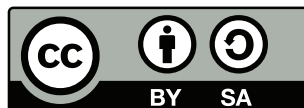


A light gray curve starts near the origin and curves upwards and to the right, resembling an exponential growth function. It is overlaid on a coordinate system with a horizontal axis and a vertical axis, both featuring tick marks. The title 'Curiosa Mathematica' is centered over the curve.

# Curiosa Mathematica

**Jens Bossaert**



(CC BY-SA 4.0)

Dit werk valt onder een Creative Commons Attribution-ShareAlike 4.0 International.

---

**You are free to:**

- **Share**—copy and redistribute the material in any medium or format
- **Adapt**—remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms.

**Under the following terms:**

- **Attribution**—you must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **ShareAlike**—if you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions—you may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

**Notices:**

- You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation.
  - No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material.
-



<b>Voorwoord</b>	3	32.7 Vermoeden van Firoozbakht . . . . .	23
<b>I Getaltheorie</b>		33 Aritmetisch getal . . . . .	23
1 Priemgetalstelling . . . . .	5	34 Vermoeden van Gilbreath . . . . .	24
2 Kleine stelling van Fermat . . . . .	6	35 Stelling van Euler . . . . .	24
3 Kwadraatvrije getallen . . . . .	6	36 Harshadgetallen . . . . .	24
4 Formule van Stirling . . . . .	7	37 <i>abc</i> -vermoeden . . . . .	25
5 Stelling van Wilson . . . . .	7	38 15-stelling . . . . .	26
6 Inversieformule van Möbius . . . . .	8	39 Fordcirkels . . . . .	27
7 Freshman's dream . . . . .	8	40 Kwadratische reciprociteit . . . . .	28
8 Stelling van Nicomachus . . . . .	8	41 Vermoeden van Collatz . . . . .	29
9 $\mathbb{N}$ -piramide . . . . .	9	42 <i>p</i> -adische getallen . . . . .	30
10 Onaanraakbare getallen . . . . .	9	43 Kerstmisstelling van Fermat . . . . .	32
11 Stelling van Midy . . . . .	9	44 AKS-priemtest . . . . .	33
12 Eulers totiëntfunctie $\varphi$ . . . . .	10	45 Gemiddelden . . . . .	34
13 Perfect totiëntgetal . . . . .	11	46 Moessners magie . . . . .	36
14 $\varphi$ , $\mu$ en de gulden snede . . . . .	11	47 Fermatpriemgetallen . . . . .	36
15 Probleem van Prouhet-Tarry-Escott . . . . .	11	48 Tweelingpriemgetallen . . . . .	37
16 Zeef van Erdős . . . . .	12	49 Vermoeden van Fortune . . . . .	38
17 Vermoeden van Catalan . . . . .	12	50 Eulerblok . . . . .	38
18 Juzuks vierdemachtsgroepjes . . . . .	12	51 Vermoeden van de eenzame loper . . . . .	39
19 Fareysequenties . . . . .	13	52 Stelling van Hurwitz . . . . .	40
20 Eigenschap van Proizvolov . . . . .	14	53 Rekenkundige afgeleide . . . . .	40
21 Constante van Landau-Ramanujan . . . . .	14	54 Probleem van Brocard . . . . .	41
22 Kettingbreuken . . . . .	14	55 Constante van Niven . . . . .	41
23 Kettingbreuken van Ramanujan . . . . .	16	56 Constante van Khinchin . . . . .	42
24 Vermoeden van Pólya . . . . .	16	57 Lifting the exponent . . . . .	43
25 <i>n</i> -hoeksgetalstelling van Fermat . . . . .	17	58 Harmonische getallen van Ore . . . . .	43
26 Perfecte getallen . . . . .	18	59 Stelling van Lucas . . . . .	43
27 Overvloedige en gebrekkige getallen . . . . .	18	60 Machtige getallen . . . . .	44
28 Vermoeden van Goldbach . . . . .	19	<b>II Algebra</b>	
29 Egyptische breuken . . . . .	20	61 Formules van Vieta . . . . .	47
30 Vermoeden van Erdős-Straus . . . . .	21	62 Tekenregel van Descartes . . . . .	47
31 Constante van Mills . . . . .	21	63 Stelling van Mason-Stothers . . . . .	47
32 Priemgetalhiaten . . . . .	21	64 Stelling van Gelfond-Schneider . . . . .	48
32.1 Postulaat van Bertrand . . . . .	21	65 Criterium van Eisenstein . . . . .	48
32.2 Priemgetallen van Ramanujan . . . . .	22	66 Criterium van Cohn . . . . .	49
32.3 Vermoeden van Legendre . . . . .	22	67 Sturmketens . . . . .	49
32.4 Vermoeden van Andrica . . . . .	22	68 Stelling van Gauss-Lucas . . . . .	50
32.5 Vermoeden van Oppermann . . . . .	23	69 Constante van Liouville . . . . .	50
32.6 Vermoeden van Cramér . . . . .	23	70 Methode van Gräffe . . . . .	50

71	Carlylecirkels . . . . .	51	116	Monster van Weierstrass . . . . .	87
72	$x^{105} - 1$ . . . . .	52	117	Riemanns reeksenstelling . . . . .	88
73	Cirkeltheorema van Gerschgorin . . . . .	53	118	Universele koordestelling . . . . .	89
74	Kuratowski's 14-stelling . . . . .	53	119	Borweinintegralen . . . . .	90
<b>III Rijen</b>			<b>V Geometrie</b>		
75	Rij van Golomb . . . . .	57	120	Dissectie van Duijvestijn . . . . .	93
76	Rij van Recamán . . . . .	57	121	Haberdasherpuzzel . . . . .	94
77	Diatomische reeks van Stern . . . . .	58	122	Tegelpatroon van Voderberg . . . . .	95
78	Rij van Thue-Morse . . . . .	58	123	Formule van Pick . . . . .	95
79	RATS . . . . .	59	124	Stelling van Jung . . . . .	96
80	Look-and-say . . . . .	60	125	Stelling van Holditch . . . . .	96
81	Rij van Gijswijt . . . . .	60	126	Stelling van Pappus . . . . .	97
82	Hofstadter-Conways \$10.000-rij . . . . .	61	127	Vlinderstelling . . . . .	97
83	Kimberlings fractale rij . . . . .	61	128	Probleem van prins Rubert . . . . .	97
84	Signatuurrijen . . . . .	62	129	Rep-tiles . . . . .	98
85	Rij van Connell . . . . .	62	130	Probleem van Langley . . . . .	99
86	Rij van Mian-Chowla . . . . .	62	131	Dissectie van Blanche . . . . .	99
87	Hofstadters $G$ -rij . . . . .	63	132	Stelling van Pascal . . . . .	100
88	Rij van Kolakoski . . . . .	63	133	Driehoek van Morley . . . . .	101
89	Schizofrene getallen . . . . .	64	134	Fermats halvecirkelprobleem . . . . .	101
90	Rij van Sylvester . . . . .	64	135	Stelling van Monsky . . . . .	102
91	Fibonaccigetallen . . . . .	65	136	Gauss' zeventienhoek . . . . .	102
92	Geluksgetallen . . . . .	67	137	Negenpuntscirkel . . . . .	103
93	Papiergevouwen rij . . . . .	68	138	Tegelpatroon van Penrose . . . . .	104
<b>IV Analyse</b>			139	Punten van Brocard . . . . .	106
94	Harmonische rij . . . . .	71	140	Probleem van Malfatti . . . . .	107
95	Constante van Euler . . . . .	71	141	Stelling van Van Aubel . . . . .	108
96	Gammafunctie . . . . .	73	142	Stelling van Napoleon . . . . .	109
97	Popcornfunctie . . . . .	74	143	Graf van Archimedes . . . . .	109
98	Van Cusa's $\pi$ -formule . . . . .	74	144	Krommen met constante breedte . . . . .	110
99	Al-Kashi's $\pi$ -formule . . . . .	75	145	Stelling van Ptolemaeus . . . . .	111
100	Power Tower . . . . .	75	146	Stelling van Laisant . . . . .	112
101	Sophomore's dream . . . . .	75	147	Veelvlak van Szilassi . . . . .	113
102	Fourierreeksen . . . . .	75	148	Stelling van Desargues . . . . .	113
103	Parkeerconstante van Rényi . . . . .	76	149	Arbelos . . . . .	114
104	Constante van Gauss . . . . .	77	149.1	Tweelingcirkels van Archimedes . . . . .	115
105	Formule van Wallis . . . . .	78	149.2	Pappusketen . . . . .	115
106	Een, twee, drie, $\pi$ . . . . .	78	149.3	Cirkel van Bankoff . . . . .	115
107	Hoorn van Gabriël . . . . .	78	149.4	Cirkels van Schoch . . . . .	116
108	Conways 13-functie . . . . .	79	149.5	Cirkels van Woo . . . . .	118
109	Volterra's functie . . . . .	79	150	Passer-en-liniaalconstructies . . . . .	118
110	Elliptische krommen . . . . .	81	151	Maantjes van Hippocrates . . . . .	119
111	Vraagtekenfunctie van Minkowski . . . . .	82	152	Luciferconstructies . . . . .	120
112	Stelling van McMullin . . . . .	83	153	Bollen van Dandelin . . . . .	120
113	Algoritme van Gauss-Legendre . . . . .	84	154	Rechte van Euler . . . . .	121
114	Omschreven veelhoeken . . . . .	84	155	Vermoeden van Toeplitz . . . . .	122
115	Lorenz attractor . . . . .	85	156	Spiraal van Theodorus . . . . .	123

157	Stelling van Viviani . . . . .	124
158	Driehoek van Calabi . . . . .	124
159	Taximeetkunde . . . . .	125
160	Stelling van Monge . . . . .	127
161	Vlak van Hilbert . . . . .	127
162	Stelling van Sylvester-Gallai . . . . .	128
163	Hyperbolische meetkunde . . . . .	128
164	Cirkel van Conway . . . . .	130
165	Kleins vierdegraadskromme . . . . .	131
166	Tarski's cirkelkwadratuur . . . . .	133
167	Parallelogram van Varignon . . . . .	134
168	Veelhoeken effenen . . . . .	134
169	Gömböc . . . . .	135
170	Monostatisch veelvlak . . . . .	136
171	Kekeyverzamelingen . . . . .	137
172	Weaire-Phelanschuim . . . . .	139
173	Criterium van Conway . . . . .	140
174	Pizzastelling . . . . .	141
175	Veelvlak van Schönhardt . . . . .	141
176	Kussende cirkels . . . . .	142
177	Japanse cirkelstelling . . . . .	143
178	Probleem van Regiomontanus . . . . .	144
179	Kusgetallen . . . . .	144
180	Penroses onverlichte kamer . . . . .	145
181	Stelling van de zeven cirkels . . . . .	146
182	Schoenveterformule . . . . .	146
183	Stelling van Cross . . . . .	147
184	Stelling van de Britse vlag . . . . .	147

## VI Bijzondere krommen

185	Cycloïde . . . . .	151
186	Cardioïde . . . . .	151
187	Nefroïde . . . . .	152
188	Deltoïde . . . . .	152
189	Tractrix . . . . .	152
190	Astroïde . . . . .	152
191	Heks van Agnesi . . . . .	152
192	Hypocycloïde . . . . .	153
193	Epicycloïde . . . . .	153
194	Lemniscaat van Bernoulli . . . . .	153
195	Strofoïde . . . . .	153
196	Cissoïde van Diocles . . . . .	154
197	Folium van Descartes . . . . .	154
198	Slakkenlijn van Pascal . . . . .	154
199	Eulerspiraal . . . . .	155

## VII Fractals

200	L-systemen en Turtle Graphics . . . . .	158
201	Driehoek van Sierpiński . . . . .	160
202	Sneeuwvlok van Koch . . . . .	162
203	Drakenkromme . . . . .	162
204	Mandelbrotverzameling . . . . .	163
205	Juliaverzameling . . . . .	165
206	Blanc-mangerkromme . . . . .	165
207	Cantorstof . . . . .	166
208	Vlakvullende krommen . . . . .	166
209	Sneeuwvlok van Vicsek . . . . .	168
210	Conways molentje . . . . .	169
211	Cesàro's gescheurd vierkant . . . . .	169
212	Pythagorasbomen . . . . .	169
213	Varen van Barnsley . . . . .	169
214	T-Square . . . . .	169
215	Lévy C-curve . . . . .	169
216	Worst van Minkowski . . . . .	170
217	Tapijt van Sierpiński . . . . .	171
218	Spons van Menger . . . . .	171

## VIII Topologie

219	Topologische handboeien . . . . .	174
220	Möbiusband . . . . .	174
221	Tangles van Conway . . . . .	175
222	Gehoornde sfeer van Alexander . . . . .	178
223	Knopen . . . . .	179
223.1	Knoopnotatie . . . . .	180
223.2	Reidemeisterbewegingen . . . . .	180
223.3	Driekleurbaarheid . . . . .	181
223.4	Samengestelde en priemknopen . . . . .	181
223.5	Alexander-Conwayveelterm . . . . .	182
223.6	Jonesveelterm . . . . .	183
223.7	HOMFLY-veelterm . . . . .	184
223.8	Andere invarianten . . . . .	184
223.9	Seifertoppervlakken . . . . .	184
224	Brouwers dekpuntstelling . . . . .	184
225	Antoinies ketting . . . . .	185
226	Diracs touwtruc . . . . .	186
227	Meren van Wada . . . . .	186

## IX Combinatoriek

228	Catalangetallen . . . . .	190
229	Subfaculteiten . . . . .	192
230	Schaakbordcombinatoriek . . . . .	193
231	Bellgetallen . . . . .	194
232	Alternerende en zigzagpermutaties . . . . .	195
233	Damesdominantie . . . . .	196
234	Motzkingetallen . . . . .	196

235	Combinatoriek en $n^{\text{de}}$ -machtswortels . . .	197
236	Langfords blokken . . . . .	198
237	Driehoeken van Kobon . . . . .	198
238	Het pannenkoekprobleem . . . . .	199
239	Happy ending problem . . . . .	199
240	Stellingen van Dilworth en Mirsky . . .	200
241	Stelling van Van der Waerden . . . . .	201
242	Sperners lemma . . . . .	201
243	Tuckers lemma . . . . .	202
244	Ladenprincipe . . . . .	202
245	Getal van Graham . . . . .	203
246	Driehoek van Pascal . . . . .	204
247	Pakkingsstellingen van de Bruijn . . .	207
248	Harmonische driehoek van Leibniz . .	208

## X Kansrekenen

249	Dobbelstenen van Efron . . . . .	212
250	Driedeurenprobleem . . . . .	212
251	Buffons naald . . . . .	213
252	Driehoedenprobleem . . . . .	213
253	Percolatietheorie . . . . .	214
254	Chevalier de Mérés dobbelprobleem . .	215
255	Paradox van Bertrand . . . . .	216
256	Sint-Petersburgparadox . . . . .	217
257	Wet van Benford . . . . .	217
258	Eindeloos typende apen . . . . .	218
259	Stokjes breken . . . . .	219
260	Parrondo's paradox . . . . .	219
261	<b>Willekeurige wandelingen</b> . . . . .	220

## XI Grafentheorie

262	Bruggen van Koningsbergen . . . . .	225
263	Vierkleurenstelling . . . . .	226
264	Stelling van Beineke . . . . .	228
265	Hamiltonpaden . . . . .	229
266	Stelling van Grinberg . . . . .	229
267	Stelling van Steinitz . . . . .	230
268	Deelbaarheidsgrafien . . . . .	231
269	Vermoeden van Tait . . . . .	232
270	Stelling van Frieze . . . . .	233
271	Stelling van Vizing . . . . .	233
272	Matrix-boomstelling van Kirchhoff . .	234
273	<b>Stelling van BEST</b> . . . . .	234
274	Formule van Cayley . . . . .	235
275	Max-flow-min-cut . . . . .	236
276	Kruskals boomstelling . . . . .	237
277	Gracieuze bomen . . . . .	238

## XII Magische vierkanten

278	Melencolia I . . . . .	241
279	Eulers magische paardenrondgang . .	241
280	Magische zeshoek . . . . .	242
281	Siamese methode . . . . .	242
282	Geomagische vierkanten . . . . .	243

## XIII Cellulaire automaten

283	Elementaire cellulaire automaten . . .	246
284	Mier van Langton . . . . .	254
285	Game of Life . . . . .	255
286	Wormen van Paterson . . . . .	262
287	Critters . . . . .	264
288	WireWorld . . . . .	265

## XIV Logica en verzamelingenleer

289	MU-puzzel . . . . .	270
290	Paradox van Russell . . . . .	270
291	Blauwogige eilandbewoners . . . . .	271
292	NAND-poorten . . . . .	272
293	Halting problem . . . . .	273
294	Hotel van Hilbert . . . . .	273
295	<b>Ordinaalgetallen</b> . . . . .	274
295.1	Stelling van Goodstein . . . . .	275
295.2	Hercules vs. de Hydra . . . . .	276
296	<b>Lambdacalculus</b> . . . . .	276
296.1	Aritmetica . . . . .	277
296.2	Logica . . . . .	278
296.3	Koppels . . . . .	279
296.4	Recuratieve functies . . . . .	279
296.5	Visualisatie . . . . .	280

## XV Groepentheorie

297	Behangpatroongroepen . . . . .	285
298	Quaternionengroep . . . . .	287
299	Rubik's Cube . . . . .	288
300	Permutatiegroepen . . . . .	290
301	15-puzzel . . . . .	290
302	Schilderijen ophangen . . . . .	292
303	Groepenwet op elliptische krommen .	293
304	Vlechtgroepen . . . . .	294

## XVI Varia

305	Knuths pijlomhoognotatie . . . . .	298
306	Hyperoperatie . . . . .	298
307	De indringer . . . . .	299
308	Boom van Pythagorasdrietallen . . . .	299
309	Vier-9's-puzzel . . . . .	300
310	18-puntenprobleem . . . . .	301

311	Conways soldaten . . . . .	301	327	Bézierkrommen . . . . .	319
312	Russisch vermenigvuldigen . . . . .	302	328	Ballistische ellips . . . . .	321
313	Origamistellingen . . . . .	302	329	Lexicodes . . . . .	321
	313.1 Stelling van Maekawa . . . . .	303	330	Gulden rondgang . . . . .	323
	313.2 Stelling van Kawasaki . . . . .	303	331	Doolhoven . . . . .	324
	313.3 Stelling van Justin . . . . .	303	332	Paradox van Braess . . . . .	325
314	Eulers 36 officieren . . . . .	304	<b>XVII Wiskundige spellen</b>		
315	Kiessystemen . . . . .	305	333	Sprouts . . . . .	329
316	Baguenaudier . . . . .	308	334	Pong Hau K'i . . . . .	330
317	Conways pijlenketen . . . . .	308	335	Phutball . . . . .	330
318	Axioma's van Huzita-Justin . . . . .	309	336	Chomp . . . . .	331
319	Bord van Galton . . . . .	310	337	Lineair schaken . . . . .	331
320	<b>Boom van Calkin-Wilf</b> . . . . .	311	338	<b>Black Path Game</b> . . . . .	332
321	RSA . . . . .	311	339	<b>Nim</b> . . . . .	332
322	<b>P vs. NP</b> . . . . .	313	<b>Quotes</b>		335
323	FRACTRAN . . . . .	314	<b>Bibliografie</b>		340
324	Sierpiński-Mazurkiewicz . . . . .	315	<b>Index</b>		345
325	Surreële getallen . . . . .	315			
326	Gulden snede in fylloaxis . . . . .	317			





# Voorwoord

De *Curiosa Mathematica* is de heilige graal in mijn queeste naar wiskundige juwelen. Elk deelgebied van de wiskunde bevat fascinerende onderwerpen, of het nu de visuele meetkunde of de abstracte algebra is, de speelse combinatoriek of de strenge analyse, en de doelstelling van dit boek is een overzicht te bieden van de aantrekkelijkste resultaten uit die grenzeloze wiskundige speeltuin.

Geniet van de wonderen van de wiskunde!

Jens Bossaert

“*The greatest mathematics has the simplicity and inevitableness of supreme poetry and music, standing on the borderland of all that is wonderful in Science, and all that is beautiful in Art.*”

Robert Turnbull



## 1 Priemgetalstelling

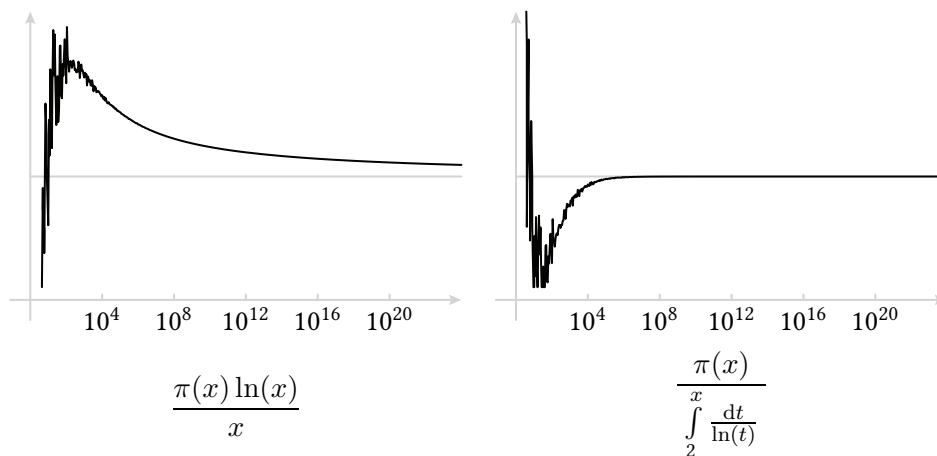
Priemgetallen, de bouwstenen van de getaltheorie, lijken onregelmatig verspreid te liggen tussen samengestelde getallen, maar voldoen desondanks aan sterke wetmatigheden. Het klassieke voorbeeld van zo'n wetmatigheid is de priemgetalstelling, waarvan de eerste notie opdaagde bij Carl Friedrich Gauss. In 1792 (op vijftienjarige leeftijd) stelde hij na een studie van priemgetalstabellen vast dat het aantal priemgetallen ten hoogste  $n$ , genoteerd  $\pi(n)$ , benaderd wordt door de uitdrukking:

$$\pi(n) \sim \frac{n}{\ln(n)}$$

Gauss heeft - zoals meerdere van zijn ontdekkingen - deze vaststelling nooit gepubliceerd. Hij vermeldde hem pas in een brief naar Johann Encke in 1849 en kwam tevens met een verfijning:

$$\pi(x) \sim \int_2^x \frac{dt}{\ln(t)}$$

Uit onderstaande logaritmische plots blijkt het quotiënt van Gauss' tweede asymptotische formule inderdaad sneller te convergeren naar één.



Onwetend van Gauss' eerdere ontdekking kwam Adrien-Marie Legendre een vergelijkbare schatting uit:

$$\pi(n) \sim \frac{n}{A \ln(n) - B}$$

In 1808 expliciteerde Legendre zijn vermoeden door te stellen dat  $A = 1$  en  $B \approx 1,08366$ . De waarde van  $B$  (soms de constante van Legendre genoemd) schatte hij uit toentertijd bekende gegevens maar Charles-Jean de la Vallée-Poussin toonde uiteindelijk aan dat  $B = 1$  feitelijk de beste benadering geeft. Merk op dat de waarde van de constante  $B$  geen invloed heeft op het asymptotisch gedrag, maar alleen op de snelheid waarmee de benadering convergeert.

$$B = \lim_{n \rightarrow \infty} \left( \ln(n) - \frac{n}{\pi(n)} \right) = 1$$

Zonder twijfel het belangrijkste artikel omtrent de verdeling van priemgetallen is Bernhard Riemanns *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*, waarin hij hun interconnectiviteit met de zëtafunctie (zie ??, blz. ??) beschreef. Uit zijn ideeën konden Jacques Hadamard en Charles-Jean de la Vallée-Poussin het eerste

rigoureuze bewijs van de priemgetalstelling geven.

Een gevolg van de priemgetalstelling is dat de kans dat een willekeurig, voldoende groot, geheel getal  $N$  een priemgetal is, bij benadering  $1/\ln(N)$  is; hoe groter  $N$ , hoe nauwkeuriger. Anders gezegd liggen twee opeenvolgende priemgetallen rond  $N$  bij benadering  $\ln(N)$  uit elkaar.

## 2 Kleine stelling van Fermat

Pierre de Fermat heeft als amateurwiskundige meerdere stellingen geponeerd, vaak zonder effectief een bewijs te geven. De stelling die later zou bekendstaan als de “kleine stelling van Fermat” vermeldde hij oorspronkelijk in een brief aan zijn vriend Frénicle de Bessy, in 1640, met bijgevoegd de opmerking:

*Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers;  
de quoi je vous enverrois la démonstration, si je n’appréhendois d’être trop long.*

Geen bewijs dus. Het eerste officiële bewijs werd gepubliceerd door Euler in 1736, in een artikel *Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio*. Leibniz vond echter eerder al vrijwel hetzelfde bewijs in een onverschenen manuscript vóór 1683.

De kleine stelling van Fermat beweert dat als  $p$  een priemgetal is en  $a$  een geheel getal, dan  $a^p - a$  deelbaar is door  $p$ ; in modulaire notatie:

$$a^p \equiv a \pmod{p}$$

Of, equivalent, wanneer  $a$  geen veelvoud is van  $p$ :

$$a^{p-1} \equiv 1 \pmod{p}$$

Het omgekeerde van de stelling geldt niet. Er bestaan namelijk ook zogenaamde pseudopriemgetallen: samengestelde getallen  $n$  waarvoor er een  $a$  bestaat met de eigenschap dat  $a^n \equiv a \pmod{n}$ . Er komen zelfs samengestelde natuurlijke getallen voor die aan deze gelijkheid voldoen voor *elke* mogelijke  $a$ -waarde, relatief priem met  $n$ ; deze staan bekend als de Carmichaelgetallen, naar Robert Carmichael:

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633 . . . (OEIS A002997)

Alwin Korselt gaf volgend criterium: een positief samengesteld getal  $n$  is een Carmichaelgetal als en slechts als  $n$  kwadraatvrij is en voor elke priemfactor  $p$  van  $n$  geldt dat  $p - 1 \mid n - 1$ .

## 3 Kwadraatvrije getallen

Een kwadraatvrij getal  $n$  is een geheel getal dat niet deelbaar is door een volkomen kwadraat, behalve 1. Equivalente definities eisen dat in de priemfactorontbinding van  $n$  elke factor juist één keer voorkomt, voor elke deler  $p$  geldt dat  $p^2 \nmid n$  of voor elke ontbinding  $n = a \cdot b$  geldt dat  $a$  en  $b$  relatief priem zijn.

1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 33, 34, 35, 37, 38, 39, 41 . . . (OEIS A005117)

Paul Erdős vermoedde dat de binomiaalcoëfficiënt  $\binom{2n}{n}$  nooit kwadraatvrij zou zijn als  $n > 4$ , wat in 1996 bewezen werd door Olivier Ramaré en Andrew Granville.

De verdeling van kwadraatvrije getallen geeft aanleiding tot een merkwaardige formule, die deze getallen linkt

aan Riemanns zetafunctie  $\zeta$  (zie ??, blz. ??). Noemen we  $Q(x)$  het aantal kwadraatvrije getallen tussen 1 en  $x$ , dan geldt:

$$\lim_{x \rightarrow \infty} \frac{Q(x)}{x} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$$

We kunnen het concept der kwadraatvrije getallen ook uitbreiden naar  $n^{\text{de}}$ -machten; als we  $Q_n(x)$  noteren als het aantal  $n^{\text{de}}$ -machtsvrije getallen tussen 1 en  $x$ , herleidt bovenstaande formule zich tot:

$$\lim_{x \rightarrow \infty} \frac{Q_n(x)}{x} = \frac{1}{\zeta(n)}$$

## 4 Formule van Stirling

De formule van Stirling is een benadering voor de faculteit van grote natuurlijke getallen, waarbij de recursiviteit van de faculteit veel te veel rekentijd zou vergen. Hoe groter het getal, hoe beter de schatting.

Een eerste versie van Stirlings formule werd ontdekt door Abraham de Moivre, in de vorm  $n! \sim c \cdot n^{n+1/2} \cdot e^{-n}$ , waarbij  $c$  een nog nader te bepalen constante was. De bijdrage van Schots wiskundige James Stirling bestond erin de waarde van  $c$  vast te stellen; hij ontdekte dat  $c = \sqrt{2\pi}$ , waardoor de uiteindelijke formule wordt:

$$n! \sim \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n$$

Sterker nog, met big- $\mathcal{O}$ -notation:

$$n! = \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \cdot \left(1 + \mathcal{O}\left(\frac{1}{n}\right)\right)$$

In applicaties wordt echter standaard deze asymptotisch gelijkwaardige formule gebruikt.

$$\ln(n!) \sim n \ln n + n$$

De Moivre publiceerde zijn resultaat in 1730 in zijn werk *Miscellanea Analytica* en gebruikte de afschatting om aan te tonen dat een binomiaalverdeling een normaalverdeling benadert. Nadat Stirling de constante bepaalde, kende de Moivre in zijn tweede editie in 1738 de verbeterde formule toe aan Stirling.

## 5 Stelling van Wilson

Al rond het jaar 1000 kende Perzisch astronoom en wiskundige Ibn al-Haytham (ook bekend als Alhazen) als eerste deze stelling. Ruim 700 jaar later werd hij herontdekt door John Wilson, student van wiskundige Edward Waring, die in 1770 de stelling bekendmaakte. Wilson noch Waring konden hem bewijzen; het was Lagrange die in 1773 het eerste bewijs gaf. Ook Leibniz zou dezelfde stelling een eeuw eerder al gekend hebben, maar hij heeft hem nooit gepubliceerd.

$$p \text{ is priem} \quad \Leftrightarrow \quad (p-1)! \equiv -1 \pmod{p}$$

Merk op dat de stelling in twee richtingen geldt; de omgekeerde implicatie geldt ook. Wilsons stelling geeft dus feitelijk een sluitend criterium voor het al dan niet priem zijn van een getal  $n$ , ware het niet dat de faculteitsfunctie uitrekenen voor grote waarden computationeel gezien onhaalbaar is.

## 6 Inversieformule van Möbius

August Ferdinand Möbius introduceerde in 1832 zijn Möbiusfunctie  $\mu(n)$ , een aritmetische functie die vaak terugkeert in getaltheorie en combinatoriek, en waarmee Möbius tevens een merkwaardige formule presenteerde.

$$\mu(n) = \begin{cases} 0 & \text{als } n \text{ niet kwadraatvrij is} \\ 1 & \text{als } n \text{ kwadraatvrij is en een even aantal verschillende priemfactoren heeft} \\ -1 & \text{als } n \text{ kwadraatvrij is en een oneven aantal verschillende priemfactoren heeft} \end{cases}$$

De Möbiusfunctie is multiplicatief, wat inhoudt dat  $\mu(a \cdot b) = \mu(a) \cdot \mu(b)$ , als  $a$  en  $b$  relatief priem zijn.

$n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1	1	0	-1	0	-1	0	1

$\mu(0)$  wordt ongedefinieerd gelaten. De functiewaarden staan in OEIS A008683.

Met behulp van  $\mu(n)$  verkondigde Möbius deze inversieformules. Voor een aritmetische functie  $g$  verkregen uit  $f$  als in het linkerlid, kan  $f$  als volgt omgekeerd verkregen worden uit  $g$ :

$$g(n) = \sum_{d|n} f(d) \quad \Leftrightarrow \quad f(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right)$$

De transformatieformules kunnen ook worden toegepast op producten i.p.v. sommen.

$$g(n) = \prod_{d|n} f(d) \quad \Leftrightarrow \quad f(n) = \prod_{d|n} \left(\frac{n}{d}\right)^{\mu(d)}$$

## 7 Freshman's dream

Ondanks het feit dat machtsverheffing niet algemeen distributief is ten opzichte van de optelling, maakt men soms de fout de macht van een som  $(a + b)^n$  uit te werken tot de som van de machten  $a^n + b^n$ , voor gehele  $a$  en  $b$  en natuurlijke  $n$ . Uiteraard fout, een dergelijke macht moet worden uitgewerkt via merkwaardige producten of het binomium van Newton.

Deze uitdrukking is echter wél geldig voor priemgetallen  $p$  als exponent, modulo  $p$ :

$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

Meer nog, een soortgelijk resultaat stelt dat  $n$  priem is als en slechts als volgende eigenschap geldt. Deze gelijkheid vormt een sleutelstelling in moderne priemtests.

$$(x + a)^n \equiv x^n + a \pmod{n} \text{ met } a \text{ en } n \text{ copriem} \quad \Leftrightarrow \quad n \text{ is priem}$$

## 8 Stelling van Nicomachus

Grieks wiskundige Nicomachus, die leefde ca. 60 tot 120 na Christus, was zeer geïnteresseerd in getaltheorie. Als neopythagoreër schreef hij bijvoorbeeld, in navolging van Pythagoras, over mystieke eigenschappen van getallen. In zijn beroemdste werk *Ἀριθμητικὴ εἰσαγωγή* (*Inleiding tot de Aritmetica*) beschrijft hij op filosofische wijze de goddelijke aard van getallen en hun voorkomen in wiskunde en wetenschap.

Naar Nicomachus vernoemd is gelijkheid tussen de som van de eerste  $n$  derdemachten en het kwadraat van het  $n^{\text{de}}$  driehoeksgetal.

$$\sum_{i=1}^n i^3 = \left( \sum_{i=1}^n i \right)^2$$

Deze eigenschap volgt uit volgende gelijkheden.

$$1^3 = 1$$

$$2^3 = 3 + 5$$

$$3^3 = 7 + 9 + 11$$

$$4^3 = 13 + 15 + 17 + 19$$

$$5^3 = 21 + 23 + 25 + 27 + 29 \text{ etc.}$$

De rij uit de kwadraten van driehoeksgetallen komen ook voor in enkele combinatorische problemen, bijvoorbeeld als het aantal rechthoeken dat op een  $n \times n$ -rooster kan worden getekend.

0, 1, 9, 36, 100, 225, 441, 784, 1296, 2025, 3025, 4356, 6084, 8281, 11025, 14400, 18496 . . . (OEIS A000537)

## 9 $\mathbb{N}$ -piramide

Een simpel maar opvallend patroon in de natuurlijke getallen:

$$1 + 2 = 3$$

$$4 + 5 + 6 = 7 + 8$$

$$9 + 10 + 11 + 12 = 13 + 14 + 15$$

$$16 + 17 + 18 + 19 + 20 = 21 + 22 + 23 + 24$$

$$25 + 26 + 27 + 28 + 29 + 30 = 31 + 32 + 33 + 34 + 35$$

$$36 + 37 + 38 + 39 + 40 + 41 + 42 = 43 + 44 + 45 + 46 + 47 + 48 \text{ etc.}$$

De linkergetallen in elk linkerlid zijn de natuurlijke kwadraten, de rechtergetallen in het linkerlid de dubbele driehoeksgetallen. Een bewijs van deze eigenschap volgt eenvoudig via volledige inductie.

## 10 Onaanraakbare getallen

Paul Erdős noemde een getal “onaanraakbaar” als het niet kan worden uitgedrukt als de som van alle echte delers van een bepaald natuurlijk getal (het onaanraakbare getal zelf inbegrepen). Erdős bewees tevens dat er oneindig veel zulke getallen bestaan. Ze vormen de rij:

2, 5, 52, 88, 96, 120, 124, 146, 162, 188, 206, 210, 216, 238, 246, 248, 262, 268, 276, 288, 290 . . . (OEIS A005114)

Het nog onbewezen vermoeden van Goldbach (zie 28, blz. 19) zou impliceren dat 5 het enige oneven onaanraakbare getal is.

## 11 Stelling van Midy

De stelling van Midy bestudeert een opmerkelijk verband in de decimale expansie van bepaalde breuken. Als een breuk  $\frac{a}{p}$ , in zijn eenvoudigste vorm en met  $p$  een priemgetal, een periode heeft met even lengte, dan tellen



de twee helften ervan op tot een tekenreeks van 9's.

$$\frac{a}{p} = 0, \overline{a_1 a_2 a_3 \dots a_{2n}} \quad \Rightarrow \quad \overline{a_1 a_2 a_3 \dots a_n} + \overline{a_{n+1} a_{n+2} a_{n+3} \dots a_{2n}} = 10^n - 1$$

Nemen we als voorbeeld de breuk  $\frac{1}{17}$ :

$$\frac{1}{17} = 0, \overline{0588235294117647} \quad \text{en} \quad 05882352 + 94117647 = 99999999$$

De stelling is gemakkelijk uit te breiden naar andere grondtallen: in grondtal  $t$  geeft ze dan een tekenreeks van opeenvolgende  $(t - 1)$ 's. Ze wordt vernoemd naar Frans wiskundige Etienne Midy, die zijn artikel hieromtrent in 1836 publiceerde.

## 12 Eulers totiëntfunctie $\varphi$

In de getaltheorie is de indicator of totiënt van natuurlijke getallen een belangrijke eigenschap. Ze werd intensief bestudeerd door Leonhard Euler, die hem in 1760 introduceerde. De notatie  $\varphi(n)$  werd gebruikt door Carl Friedrich Gauss in zijn getaltheoretisch opus *Disquisitiones Arithmeticae* in 1801.

De indicator van  $n$  (OEIS A000010) stelt het aantal natuurlijke getallen voor (zonder 0) ten hoogste  $n$ , die onderling ondeelbaar zijn met  $n$ . Zo is 10 onderling ondeelbaar met 1, 3, 7 en 9, dus  $\varphi(10) = 4$ . Deze aritmetische functie is multiplicatief, wat inhoudt dat  $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$  voor twee onderling ondeelbare getallen  $m$  en  $n$  (alhoewel dit kan worden veralgemeend; zie verder). Er bestaat een enorme hoeveelheid formules en eigenschappen die gebruik maken van  $\varphi$ . Eulers klassieke productformule maakt gebruik van alle priemgetallen  $p$  die  $n$  delen:

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

$\varphi$  kan evenzeer berekend worden door middel van goniometrische functies:

$$\varphi(n) = \sum_{k=1}^n \text{ggd}(k, n) \cdot \cos\left(\frac{2\pi k}{n}\right)$$

Door middel van Möbius' inversieformule (zie 6, blz. 8) vinden we:

$$\varphi(n) = n \cdot \sum_{d|n} \frac{\mu(d)}{d}$$

De eigenschappen zijn overweldigend, zowel qua aantal als qua schoonheid. Een kleine selectie:

$$\sum_{d|n} \varphi(d) = n \quad \varphi(mn) = \varphi(m) \cdot \varphi(n) \cdot \frac{\text{ggd}(m, n)}{\varphi(\text{ggd}(m, n))} \quad \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)}$$

De totiëntfunctie keert terug bij vele wiskundige concepten, zoals de Riemann-zètafunctie (zie ??, blz. ??), het vermoeden van Goldbach (zie 28, blz. 19) en de Euler-Mascheroniconstante  $\gamma$ . Enkele voorbeelden:

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} \quad (\text{voor } s > 2)$$

Het verband met de Euler-Mascheroniconstante is lastiger.

$$\liminf_{n \rightarrow \infty} \frac{\varphi(n) \cdot \ln(\ln n)}{n} = e^{-\gamma}$$

Een andere leuke eigenschap vormen deze onder- en bovengrens, waarbij  $\sigma(n)$  de som van alle positieve delers van  $n$  voorstelt,  $n$  zelf uitgezonderd.

$$\frac{6}{\pi^2} < \frac{\varphi(n) \cdot \sigma(n)}{n^2} < 1 \quad (\text{voor } n > 1)$$

### 13 Perfect totiëntgetal

Pas herhaaldelijk Eulers totiëntfunctie uit het vorige hoofdstuk toe op een natuurlijk getal  $n$ , tot het getal 1 bereikt wordt. Wanneer de verkregen rij getallen optelt tot het begingetal  $n$ , noemt men  $n$  een perfect totiëntgetal. Een voorbeeld van zo'n getal is 243:

$$\varphi(243) = 162, \varphi(162) = 54, \varphi(54) = 18, \varphi(18) = 6, \varphi(6) = 2, \varphi(2) = 1 \quad \text{en} \quad 162 + 54 + 18 + 6 + 2 + 1 = 243$$

De volledige rij perfecte totiëntgetallen begint als volgt:

3, 9, 15, 27, 39, 81, 111, 183, 243, 255, 327, 363, 471, 729, 2187, 2199, 3063, 4359, 4375 . . . (OEIS A082897)

Het is opvallend dat heel wat getallen uit deze rij veelvoudig zijn van drie; het kan eenvoudig worden aangetoond dat alle exacte machten van drie voldoen aan de definitie. Perez Cacho toonde aan dat  $3^p$  een perfect totiëntgetal is als en slechts als ook  $n$  dat is, voor een priemgetal  $p = 4n + 1$ . Er zijn diverse andere criteria bekend:  $3^2p$  is een perfect totiëntgetal wanneer zowel  $q = 83^b + 1$  als  $p = 2q + 1$  priem zijn, en  $3^3p$  is er eentje voor  $r = 43^b + 1$ ,  $q = 16r + 1$  en  $p = 4q + 1$  priem. Het is een open probleem of er getallen met deze eigenschap bestaan van de vorm  $3^k p$  voor  $k \geq 4$ .

### 14 $\varphi$ , $\mu$ en de gulden snede

Robert Schneider ontdekte en bewees in 2011 het volgende verband tussen de gulden snede  $\phi = \frac{1}{2}(1 + \sqrt{5})$ , de Möbiusfunctie  $\mu$  (zie 6, blz. 8), Eulers totiëntfunctie  $\varphi$  (zie 12, blz. 10) en de natuurlijke logaritme.

$$\begin{aligned} \phi &= - \sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \cdot \ln \left( 1 - \frac{1}{\phi^k} \right) \\ \frac{1}{\phi} &= - \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \cdot \ln \left( 1 - \frac{1}{\phi^k} \right) \end{aligned}$$

### 15 Probleem van Prouhet-Tarry-Escott

Dit probleem werd voor het eerst bestudeerd door Eugène Prouhet in 1851 en later door Gaston Tarry en Edward Escott begin de jaren 10:

VIND TWEE DISJUNCTE VERZAMELINGEN  $A$  EN  $B$  MET ELK  $n$  GEHELE GETALLEN, ZODAT DE SOM VAN DE  $i^{\text{DE}}$ -MACHTEN VAN ALLE ELEMENTEN UIT  $A$  EN DIE UIT  $B$  GELIJK IS, VOOR ELKE  $i$  VAN 1 TOT EN MET EEN GEGEVEN  $k$ .

$$\forall i \in \{1, 2, \dots, k\} : \sum_{a \in A} a^i = \sum_{b \in B} b^i$$

De grootste  $k$ -waarde waarvoor er tot nu toe oplossingen zijn gevonden, is 11, met bijhorende verzamelingen  $A = \{22, 61, 86, 127, 140, 151\}$  en  $B = \{35, 47, 94, 121, 146, 148\}$ .

$$\begin{aligned} 22 + 61 + 86 + 127 + 140 + 151 &= 35 + 47 + 94 + 121 + 146 + 148 \\ 22^2 + 61^2 + 86^2 + 127^2 + 140^2 + 151^2 &= 35^2 + 47^2 + 94^2 + 121^2 + 146^2 + 148^2 \\ 22^3 + 61^3 + 86^3 + 127^3 + 140^3 + 151^3 &= 35^3 + 47^3 + 94^3 + 121^3 + 146^3 + 148^3 \\ 22^4 + 61^4 + 86^4 + 127^4 + 140^4 + 151^4 &= 35^4 + 47^4 + 94^4 + 121^4 + 146^4 + 148^4 \end{aligned}$$

Enzovoort, voor alle exponenten  $\in \{1, 2, 3, \dots, 11\}$ .

Een heleboel oplossingen zijn online te vinden op <http://euler.free.fr/eslp/TarryPrb.htm>.

## 16 Zeef van Erdős

Kies een natuurlijk getal  $n$  als startwaarde  $u_0$ , verschillend van 0. Bepaal vervolgens  $u_1$  als het kleinste veelvoud van  $(n - 1)$  dat niet kleiner is dan  $u_0$ , daarna  $u_2$  als het kleinste veelvoud van  $(n - 2)$  niet kleiner dan  $u_1$ , en blijf dit herhalen totdat  $u_{n-1}$  bepaald is.

Bijvoorbeeld voor  $n = 10$ :  $10 \xrightarrow{9} 18 \xrightarrow{8} 24 \xrightarrow{7} 28 \xrightarrow{6} 30 \xrightarrow{5} 30 \xrightarrow{4} 32 \xrightarrow{3} 33 \xrightarrow{2} 34 \xrightarrow{1} 34$ .

Deze eindwaarde noemen we  $f(n)$ . Wanneer we elk natuurlijk getal  $n$  aldus op  $f(n)$  afbeelden, verkrijgen we de rij: 1, 2, 4, 6, 10, 12, 18, 22, 30, 34, 42, 48, 58, 60, 78, 82, 102, 108 . . . (OEIS A002491).

Paul Erdős en Eri Jabotinsky vonden een constructie die dezelfde rij oplevert. Omdat hun methode vergelijkbaar is met de zeef van Eratosthenes (zie ??, blz. ??), wordt ze de zeef van Erdős genoemd.

- Begin met de rij der natuurlijke getallen: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 . . .
- Begin met  $k = 2$ .
- Schrap elke  $k^{\text{de}}$  term uit de (resterende) rij, te beginnen bij de term met volgnummer  $(2k - 1)$ .
- Herhaal stap 3 met  $k = 3, 4, 5 . . .$

Nu geldt deze verbazingwekkende eigenschap:

$$\lim_{n \rightarrow \infty} \frac{n^2}{f(n)} = \pi$$

## 17 Vermoeden van Catalan

In 1844 opperde de Belgische wiskundige Eugène Charles Catalan het vermoeden dat  $2^3$  en  $3^2$  de enige twee opeenvolgende natuurlijke machten zijn, op triviale machten na, m.a.w. de volgende diophantische vergelijking zou slechts één natuurlijke, niet-triviale oplossing hebben.

$$x^a - y^b = 1, \quad \text{met } x, y, a, b > 1$$

In deze lijst van alle perfecte machten (natuurlijke getallen  $n^k$  met  $n, k \in \mathbb{N}, k > 1$ ) betekent dat dus dat 8 en 9 het enige paar opeenvolgende getallen vormen.

1, 4, **8**, **9**, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, 169, 196, 216, 225, 243, 256 . . . (OEIS A001597)

Er werd belangrijke vooruitgang geboekt door Robert Tijdeman, die bewees dat het aantal oplossingen eindig is en een bovengrens gaf. Catalans vermoeden werd uiteindelijk pas in 2002 (na bijna 160 jaar) volledig bewezen door Preda Mihăilescu, en wordt sindsdien soms de stelling van Mihăilescu genoemd.

## 18 Juzuks vierdemachtsgroepjes

In 1939 stelde Dov Juzuk een interessante manifestatie van de vierdemachten vast. Schrijf de natuurlijke getallen op in groepjes, van één, twee, drie . . . getallen, en schrap elk tweede groepje:

1,     ~~2,3~~,     4, 5, 6,     ~~7,8,9,10~~,     11, 12, 13, 14, 15,     ~~16,17,18,19,20,21~~,     . . .

De som van de eerste  $n$  resterende groepjes is dan gelijk aan  $n^4$ .

## 19 Fareysequenties

In 1816 werd een artikel gepubliceerd in het *Philosophical Magazine*, afkomstig van geoloog John Farey, over wat nu bekendstaat als de Fareysequenties. Farey kreeg de ingeving om alle breuken  $\frac{a}{b}$  tussen 0 en 1, die niet verder vereenvoudigd kunnen worden en waarbij  $b$  kleiner is dan een bepaald getal, in stijgende volgorde op te schrijven. Dit geeft:

$$\begin{aligned}
 F_1 &= \frac{0}{1}, \frac{1}{1} \\
 F_2 &= \frac{0}{1}, \frac{1}{2}, \frac{1}{1} \\
 F_3 &= \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1} \\
 F_4 &= \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1} \\
 F_5 &= \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1} \\
 \dots &= \dots
 \end{aligned}$$

Een eerste eigenschap van deze Fareysequenties betreft een bewerking  $\oplus$  op breuken, de zogenaamde mediant, die als volgt gedefinieerd wordt. Merk op dat deze afhankelijk is van de representatie van de breuk en dus niet eenduidig gedefinieerd is op de rationale getallen.

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}$$

Het viel Farey op dat in zijn sequenties elke term de mediant is van zijn twee burens, zonder dat hij dit kon bewijzen. Augustin-Louis Cauchy gaf hiervan een bewijs in zijn *Exercices de Mathématique*, waarin hij zijn inspiratie toeschreef aan Farey. Eerder al, in 1802, werd echter een soortgelijk resultaat gepubliceerd door Charles Haros, zonder dat iemand het was opgevallen.

Er zitten nog meer eigenschappen verborgen in de Fareysequenties. Zo kan de lengte van  $F_n$ , genoteerd als  $|F_n|$ , recursief worden uitgedrukt door middel van Eulers totiëntfunctie  $\varphi(n)$  (zie 12, blz. 10):

$$|F_n| = |F_{n-1}| + \varphi(n)$$

Asymptotisch gedraagt  $|F_n|$  zich als:

$$|F_n| \sim \frac{3n^2}{\pi^2}$$

Er bestaat een eenvoudig algoritme om de volgende termen van een sequentie  $F_n$  te genereren. Steunend op de twee voorgaande breuken  $\frac{a}{b}$  en  $\frac{c}{d}$  en de eigenschap van de mediant kan de volgende breuk zo berekend worden.

$$\dots \frac{a}{b}, \frac{c}{d}, \frac{\left\lfloor \frac{n+b}{d} \right\rfloor \cdot c - a}{\left\lfloor \frac{n+b}{d} \right\rfloor \cdot d - b}, \dots$$

Fareysequenties komen vaak voor in getaltheorie en kennen rijke toepassingen in andere domeinen als chaostheorie of brute-forcealgoritmes voor rationale oplossingen van diophantische vergelijkingen. Ze kunnen ook worden gelinkt aan de Riemannhypothesen. Een visualisatie ervan is mogelijk via Fordcirkels (zie 39, blz. 27).

## 20 Eigenschap van Proizvolov

Deze eigenschap werd in 1985 ontdekt door Russisch wiskundige Vyacheslav Proizvolov en als opgave gesteld in de All-Union Soviet Student Olympiads. Neem de eerste  $2n$  natuurlijke getallen samen en splits deze in twee deelverzamelingen  $A$  en  $B$  met evenveel elementen. Rangschik de getallen van  $A$  in stijgende volgorde en die van  $B$  in dalende volgorde.

$$\{1, 2, 3, \dots, 2n-1, 2n\} \quad \mapsto \quad \begin{cases} A_1 < A_2 < \dots < A_n \\ B_1 > B_2 > \dots > B_n \end{cases}$$

Tel nu de (absolute) verschillen tussen de overeenkomstige elementen op; de som daarvan is dan  $n^2$ .

$$|A_1 - B_1| + |A_2 - B_2| + \dots + |A_n - B_n| = n^2$$

## 21 Constante van Landau-Ramanujan

Beschouw de getallen die te schrijven zijn als een som van twee volkomen kwadraten, zoals  $13 = 2^2 + 3^2$ .

0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50, 52, 53 ... (OEIS A001481)

Noteer  $N(x)$  voor het aantal getallen uit deze rij, ten hoogste  $x$ , die dus zo'n som van kwadraten zijn. Onafhankelijk van elkaar bewezen de Duitse Edmund Landau en de Indische Srinivasa Ramanujan dat de volgende limiet dan convergeert, zij het uiterst traag:

$$\lim_{x \rightarrow \infty} \frac{N(x) \cdot \sqrt{\ln x}}{x} = 0,76422365358922066299\dots$$

Deze constante (soms genoteerd als  $\lambda$ ) is vermoedelijk irrationaal. Ze kan als volgt exact worden uitgedrukt, waarbij het product loopt over alle priemgetallen  $p$  congruent met 1 of 3 modulo 4:

$$\lambda = \frac{1}{\sqrt{2}} \prod_{\substack{p \equiv 3 \\ (\text{mod } 4)}} \frac{p}{\sqrt{p^2 - 1}} = \frac{\pi}{4} \prod_{\substack{p \equiv 1 \\ (\text{mod } 4)}} \frac{\sqrt{p^2 - 1}}{p}$$

De decimale expansie van de constante van Landau-Ramanujan staat in OEIS A064533.

## 22 Kettingbreuken

In zijn werk *Arithmetica infinitorum* introduceerde John Wallis in 1653 de term “kettingbreuken” voor het eerst. Dit zijn uitdrukkingen van de volgende vorm, die een reëel getal  $x$  kunnen representeren.

$$x = a_0 + \frac{b_1}{a_1 + \frac{b_2}{a_2 + \frac{b_3}{a_3 + \frac{b_4}{a_4 + \dots}}}}$$

Wanneer één van de  $b_i$ 's gelijk zou zijn aan 0, spreekt men van een eindige kettingbreuk; hierbij geldt dat een getal rationaal is als en slechts als zijn voorstelling als een kettingbreuk eindig is. De zogenaamde enkelvoudige of reguliere kettingbreuken zijn die waarbij alle  $b_i$ 's gelijk zijn aan 1; elk reëel getal kan worden geschreven als

juist één reguliere kettingbreuk. Vanwege de uniciteit wordt dan vaak de verkorte notatie  $[a_0; a_1, a_2, a_3, a_4 \dots]$  gebruikt.

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots}}}}$$

Voor elke willekeurige  $x$ -waarde kan zijn reguliere kettingbreuk gevonden worden door dit algoritme.

$$r_0 = x, \quad r_n = \frac{1}{r_{n-1} - a_{n-1}} \quad \Rightarrow \quad a_n = \lfloor r_n \rfloor$$

Er bestaan enkele opmerkelijke kettingbreuken met betrekking tot belangrijke constanten.

$$\varphi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\ddots}}}} \quad e - 1 = 1 + \frac{2}{2 + \frac{3}{3 + \frac{4}{4 + \frac{5}{\ddots}}}}$$

$$\frac{1}{e - 1} = \frac{1}{1 + \frac{2}{2 + \frac{3}{3 + \frac{4}{\ddots}}}} \quad \frac{1}{\sqrt{e} - 1} = 1 + \frac{2}{3 + \frac{4}{5 + \frac{6}{7 + \frac{8}{\ddots}}}}$$

$$\pi = \frac{4}{1 + \frac{1^2}{2 + \frac{3^2}{2 + \frac{5^2}{\ddots}}}} = \frac{4}{1 + \frac{1^2}{3 + \frac{2^2}{5 + \frac{3^2}{\ddots}}}} = 3 + \frac{1^2}{6 + \frac{3^2}{6 + \frac{5^2}{6 + \frac{7^2}{\ddots}}}}$$

Voor  $\pi$  volgt de reguliere kettingbreuk (OEIS A001203) helaas geen begrijpelijk patroon. Voor  $e$  wel:

$$\begin{aligned} e &= [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, \dots] \\ \sqrt[n]{e} &= [1; n - 1, 1, 1, 3n - 1, 1, 1, 5n - 1, 1, 1, 7n - 1, \dots] \\ \sqrt[n]{e^2} &= [1; \frac{1}{2}(n - 1), 6n, \frac{1}{2}(5n - 1), 1, 1, \frac{1}{2}(7n - 1), 18n, \frac{1}{2}(11n - 1), 1, 1, \frac{1}{2}(13n - 1), 30n, \frac{1}{2}(17n - 1), \dots] \end{aligned}$$

Wanneer een kettingbreuk die een irrationaal getal  $x$  voorstelt, wordt “afgebroken” na  $n$  termen, verkrijg je de zogenaamde  $n^{\text{de}}$  convergent. Deze convergenten vormen een rij met in zekere zin de “beste benaderingen” voor  $x$ . Uiteraard convergeert zo’n rij naar  $x$ .

De vierkantswortel uit een kwadraatvrij geheel getal  $N$  (zie 3, blz. 6) heeft een periodieke kettingbreuk van de volgende vorm, waarbij tevens geldt dat  $0 < a_n < 2\sqrt{N}$ .

$$\sqrt{N} = [a_0; \overline{a_1, \dots, a_n, 2a_0}]$$

Tot slot kunnen kettingbreuken soms gebruikt worden om functies weer te geven, zoals hier het geval voor de tangens en de tangens hyperbolicus.

$$\tan x = \frac{x}{1 - \frac{x^2}{3 - \frac{x^2}{5 - \frac{x^2}{\ddots}}}} \quad \tanh x = \frac{x}{1 + \frac{x^2}{3 + \frac{x^2}{5 + \frac{x^2}{\ddots}}}}$$

## 23 Kettingbreuken van Ramanujan

De geniale Indische wiskundige Srinivasa Ramanujan staat bekend vanwege zijn drie notitieboekjes, die hij volgekrabbeld heeft met zijn ontdekkingen. Voornamelijk uit economische motieven vermeldde hij uitsluitend zijn resultaten, zonder bewijs of zelfs maar een aanwijzing hoe hij eraan gekomen is, en dan vaak nog niet in standaardnotatie. Heel wat formules blijven tot op vandaag een mysterie, maar desondanks geeft Ramanujan hiermee een blik binnenin diepere wiskunde.

Deze kettingbreuk legt een verband tussen  $e$ ,  $\pi$  en de gulden snede  $\varphi$ .

$$\frac{1}{1 + \frac{e^{-2\pi}}{1 + \frac{e^{-4\pi}}{1 + \frac{e^{-6\pi}}{1 + \frac{\ddots}}}}}} = \left( \sqrt{\varphi \cdot \sqrt{5}} - \varphi \right) \cdot e^{\frac{2\pi}{5}}$$

Een andere, nog mooiere formule van Ramanujan maakt eveneens gebruik van kettingbreuken:

$$\frac{1}{1 + \frac{1}{1 + \frac{2}{1 + \frac{3}{1 + \frac{4}{1 + \frac{\ddots}}}}}}} + \frac{1}{1} + \frac{1}{1 \cdot 3} + \frac{1}{1 \cdot 3 \cdot 5} + \frac{1}{1 \cdot 3 \cdot 5 \cdot 7} + \dots = \sqrt{\frac{\pi \cdot e}{2}}$$

## 24 Vermoeden van Pólya

Een natuurlijk getal wordt “van het even type” genoemd als zijn ontbinding in priemgetallen een even aantal factoren kent, anders “van het oneven type”. Definieer 1 hierbij van het even type. Noem  $E(n)$  nu het aantal positieve gehele getallen van het even type kleiner dan of gelijk aan  $n$ , en  $O(n)$  het aantal positieve gehele getallen van het oneven type kleiner dan of gelijk aan  $n$ .

George Pólya vermoedde nu in 1919 dat voor elke  $n \geq 2$ , geldt dat  $O(n) \geq E(n)$ . Nadat de eerste miljoenen getallen geverifieerd waren, geloofden velen in de juistheid van dit vermoeden. Niettemin vormt het controleren van een heleboel gevallen geen bewijs...

Pólya's vermoeden bleek niet te kloppen! In 1958 bewees Colin Haselgrove dat er een tegenvoorbeeld bestaat in de buurt van  $1,845 \cdot 10^{361}$ . Een expliciet tegenvoorbeeld werd door Russell Lehman in 1960 gegeven voor

$n = 906.180.359$ . In 1980 legde Minory Tanaka het kleinste tegenvoorbeeld vast voor  $n = 906.150.257$ .

Een andere manier om dit vermoeden uit te drukken, is met behulp van de Liouvillefunctie. De Liouvillefunctie  $\lambda(n)$  wordt gedefinieerd als  $(-1)^{\Omega(n)}$ , waarbij  $\Omega(n)$  het aantal priemfactoren van  $n$  voorstelt, multiplicititeit meegerekend. De functie is volledig multiplicatief. Concreet betekent dit dus dat  $\lambda(n) = 1$  voor elke  $n$  van het even type, en  $\lambda(n) = -1$  voor elke  $n$  van het oneven type. Volgens Pólya gold dan (onterecht dus) voor elke  $n \in \mathbb{N}$ :

$$L(n) = \sum_{k=1}^n \lambda(k) \stackrel{?}{\leq} 0$$

Verwant hiermee is de volgende som  $T(n)$ , waarvoor een tijdlang een analoog vermoeden gold.

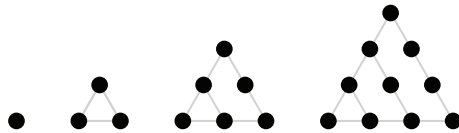
$$T(n) = \sum_{k=1}^n \frac{\lambda(k)}{k} \stackrel{?}{\geq} 0$$

Helaas toonde Haselgrove aan dat  $T(n)$  oneindig vaak van teken verandert; zoals Pál Turán aantoonde, zou een positief bewijs van dit vermoeden tot een bewijs voor de Riemannhypothesen (zie ??, blz. ??) geleid hebben. Het is overigens nog onduidelijk of ook  $L(n)$  oneindig vaak van teken zou veranderen.

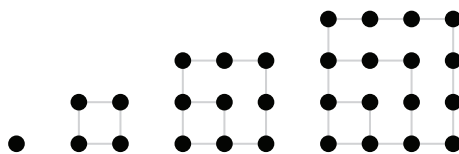
## 25 $n$ -hoeksgetalstelling van Fermat

Zoals Pierre de Fermat wel vaker deed, stelde hij in 1638 dit resultaat zonder bewijs, maar met de belofte dat hij die zou uitschrijven in een apart werk dat echter nooit verscheen. Volgens deze stelling kan elk natuurlijk getal geschreven worden als de som van maximaal  $n$  niet noodzakelijk verschillende  $n$ -hoeksgetalen.

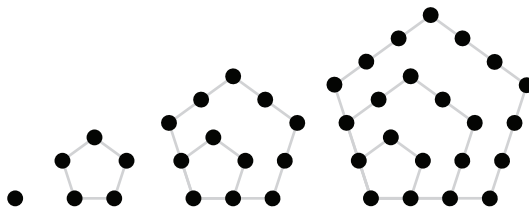
De driehoeksgetalen 0, 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, 120, 136, 153 . . . (OEIS A000217)



De vierhoeksgetalen 0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256 . . . (OEIS A000290)



De vijfhoeksgetalen 0, 1, 5, 12, 22, 35, 51, 70, 92, 117, 145, 176, 210, 247, 287, 330, 376 . . . (OEIS A000326)



Joseph Louis Lagrange bewees de stelling voor het geval  $n = 4$ , dus dat elk getal de som is van maximaal vier volkomen kwadraten. Carl Friedrich Gauss bewees in 1796 het geval  $n = 3$ , publiceerde dit resultaat in zijn *Disquisitiones Arithmeticae* en noteerde in zijn dagboek de cryptische regel “EYPHKA! num =  $\triangle + \triangle + \triangle$ ”. Sindsdien staat dit geval ook bekend als de Eureka-stelling.

Pas in 1813 gaf Augustin-Louis Cauchy een volledig bewijs voor alle  $n$ -hoeksgetalen.



## 26 Perfecte getallen

Nogal wat antieke culturen begiftigden bepaalde getallen met religieuze of magische eigenschappen. Een bekend voorbeeld daarvan zijn de zogenaamde perfecte getallen, die in het bijzonder werden bestudeerd door de Grieken, waaronder Euclides.

Perfecte getallen zijn de natuurlijke getallen  $n$  die gelijk zijn aan de som van hun echte delers ( $n$  zelf dus uiteraard uitgezonderd), ofwel de getallen  $n$  zodat  $\sigma_1(n) = 2n$ . De Grieken kenden slechts de eerste vier perfecte getallen, namelijk 6, 28, 496 en 8128. De volgende (33.550.336) werd pas geïdentificeerd door een onbekende wiskundige rond 1460. Daarna werden 8.589.869.056 en 137.438.691.328 ontdekt in 1588 door Pietro Cataldi. De volledige lijst bekende perfecte getallen staan in OEIS A000396.

Euclides kon bewijzen dat wanneer  $2^p - 1$  priem is, dan  $2^{p-1} \cdot (2^p - 1)$  noodzakelijkerwijze een perfect getal is. Leonhard Euler bewees zelfs dat deze formule alle mogelijke even perfecte getallen genereert. Priemgetallen van de vorm  $2^p - 1$  heten Mersennepriemgetallen (zie ??, blz. ??), en aangezien het nog onbekend is of er oneindig veel Mersennepriemgetallen zijn, geldt dit ook voor perfecte getallen. Een gevolg van deze formule is dat perfecte getallen binair uitgeschreven worden met  $p$  enen en  $p - 1$  nullen:

- $6 = 110_2$
- $28 = 11100_2$
- $496 = 111110000_2$
- $8128 = 1111111000000_2$
- $33550336 = 111111111111100000000000_2$

Een andere open kwestie is de pariteit van perfecte getallen: men vermoedt dat er geen oneven bestaan, maar bewijzen of tegenvoorbeelden zijn nog gevonden. Een oneven perfect getal moet wel groter zijn dan  $10^{1500}$ .

## 27 Overvloedige en gebrekkige getallen

Nauw in relatie met de perfecte getallen (zie 26, blz. 18) staan de overvloedige en gebrekkige getallen. Daar waar voor een perfect getal  $n$  geldt dat de som van de echte delers juist gelijk is aan  $n$ , is die voor een overvloedig of abundant getal juist groter ( $\sigma_1(n) > 2n$ ) en voor een gebrekkig getal kleiner ( $\sigma_1(n) < 2n$ ). Beide categorieën werden voor het eerst beschreven door Nicomachus in zijn *Ἀριθμητικὴ εἰσαγωγή* (*Inleiding tot de Aritmetica*); het was diezelfde Nicomachus die opmerkte dat 8128 een perfect getal is.

De overvloedige getallen staan in OEIS A005101:

12, 18, 20, 24, 30, 36, 40, 42, 48, 54, 56, 60, 66, 70, 72, 78, 80, 84, 88, 90, 96, 100, 102, 104, 108, 112, 114, 120 . . .

Er bestaan wel degelijk ook oneven overvloedige getallen, oneindig veel zelfs: de kleinste is 945. Een andere eigenschap is dat elk geheel getal groter dan 20.161 kan worden geschreven als de som van twee overvloedige getallen. Marc Deléglise toonde in 1998 aan dat de dichtheid van deze getallen in  $\mathbb{N}$  tussen 0,2474 en 0,2480 ligt, waarmee ze “zeldzamer” zijn dan de gebrekkige getallen.

De gebrekkige getallen staan in OEIS A005100:

1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 19, 21, 22, 23, 25, 26, 27, 29, 31, 32, 33, 34, 35, 37, 38, 39, 41, 43 . . .

Ook in deze categorie zitten er oneindig veel getallen, zowel even als oneven.

## 28 Vermoeden van Goldbach

Christian Goldbach beschreef op 7 juni 1742 in een brief naar Leonhard Euler een beroemd probleem, dat nu bekend staat als het vermoeden van Goldbach en nog steeds onopgelost is. In zijn originele versie merkte Goldbach op dat elk geheel getal dat kan worden geschreven als de som van twee priemgetallen, ook kan worden geschreven als de som van willekeurig veel priemgetallen totdat alle termen eenheden zijn. Equivalent daarmee stelde hij dat elk geheel getal  $n > 2$  kan worden geschreven als de som van drie priemgetallen.

Goldbach beschouwde het getal 1 ook als priem, maar deze conventie werd ondertussen aangepast. Een aangepaste, moderne versie van het “zwakke” vermoeden van Goldbach is dus:

ELK GEHEEL GETAL  $n > 5$  IS TE SCHRIJVEN ALS DE SOM VAN DRIE PRIEMGETALLEN.

Euler repliceerde hierop in een tweede brief en maakte Goldbach erop attent dat dit nog sterker uit te drukken is als de “sterke” vorm waaronder ze vandaag bekend staat:

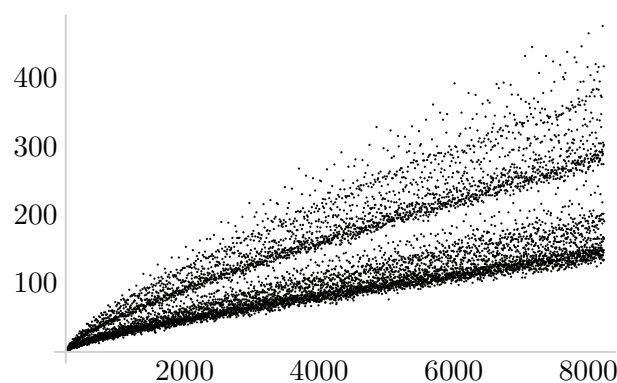
ELK EVEN GEHEEL GETAL  $n > 2$  IS TE SCHRIJVEN ALS DE SOM VAN TWEE PRIEMGETALLEN.

In zijn brief merkte Euler ook op dat hij overtuigd was van de waarheid van het vermoeden, maar dat hij er desondanks geen bewijs voor vond. Tot op vandaag blijft het probleem onbeantwoord.

*Dass... ein jeder numerus par eine summa duorum primorum sey,  
halte ich für ein ganz gewisses theorema, ungeachtet ich dasselbe necht demonstiren kann.*

Heuristische berekeningen maken het zeer waarschijnlijk dat het vermoeden klopt: grote getallen kunnen vaak op vele manieren in een som van twee priemgetallen ontbonden worden. Het aantal dergelijke partities staat in OEIS A045917, en een plot ervan staat bekend als “de komeet van Goldbach”. Ondertussen zijn alle getallen tot aan  $4 \cdot 10^{18}$  gecontroleerd, zonder dat er een tegenvoorbeeld gevonden werd.

0, 1, 1, 1, 2, 1, 2, 2, 2, 2, 3, 3, 3, 2, 3, 2, 4, 4, 2, 3, 4, 3, 4, 5, 4, 3, 5, 3, 4, 6, 3, 5, 6, 2, 5, 6, 5, 5, 7, 4 . . . (OEIS A045917)



Het vermoeden van Goldbach oplossen behoort niet tot de zeven Millenniumproblemen, maar de Britse uitgever Tony Faber loofde, bij wijze van reclame voor Apostolos Doxiadis’ novel *Uncle Petros and Goldbach’s Conjecture*, een prijs uit van \$1.000.000 als er een bewijs werd ingediend vóór april 2002. De prijs werd niet opgeëist.

Nog vermeldenswaardig in deze context is de stelling van Chen: Chinees wiskundige Chen Jingrun toonde in 1966 aan dat elk voldoende groot even getal kan worden geschreven als de som van twee priemgetallen OF een priemgetal en een semipriemgetal (een natuurlijk getal met twee priemfactoren). Olivier Ramaré toonde in 1995 aan dat elk even getal  $n > 2$  de som is van maximaal zes priemgetallen. Tot slot garandeert de in 1937 bewezen stelling van Vinogradov dat elk voldoende groot oneven getal te schrijven is als de som van drie priemgetallen.

## 29 Egyptische breuken

Het systeem van de Egyptische breuken werd ontwikkeld tijdens het Egyptische Middenrijk, rond 2000 v.Chr. Een later en ondertussen beroemd document, het Rhindpapyrus, voerde verbeteringen in notatie in; deze werd geschreven door Ahmes en is thans het oudst bekende wiskundige geschrift. In zijn Rhindpapyrus beschrijft Ahmes 84 praktische problemen, met hun oplossing, naast een tabel met expansies voor rationale getallen  $\frac{2}{n}$  naar Egyptische breuken - alles bedoeld voor dagdagelijkse situaties.

Egyptische breuken zijn voorstellingen van rationale getallen als een som van stambreuken (met teller 1). Een rationaal getal als  $\frac{17}{29}$  werd door de Egyptenaren genoteerd als  $\frac{1}{2} + \frac{1}{12} + \frac{1}{348}$ . Enkel  $\frac{2}{3}$  en  $\frac{3}{4}$  waren uitzonderingen en hadden hun eigen symbool.

Fibonacci beschreef een methode om rationale getallen te converteren naar een som van stambreuken in zijn beroemde werk *Liber Abaci*. Hij beseftte echter ook dat zijn gretige algoritme niet altijd een optimale oplossing gaf en daarom bood hij deze methode aan voor noodgevallen, wanneer zijn andere technieken faalden. Het algoritme herhaalt deze substitutie, totdat alle termen stambreuken zijn:

$$\frac{x}{y} = \frac{1}{\lceil \frac{y}{x} \rceil} + \frac{(-y) \bmod x}{y \cdot \lceil \frac{y}{x} \rceil}$$

Toegepast op bijvoorbeeld  $\frac{7}{15}$  geeft dit  $\frac{1}{3} + \frac{1}{8} + \frac{1}{120}$ . Voor sommige breuken echter levert het algoritme onbruikbare resultaten:  $\frac{31}{311}$  is relatief eenvoudig uit te drukken als  $\frac{1}{12} + \frac{1}{63} + \frac{1}{2799} + \frac{1}{8708}$ , terwijl Fibonacci's methode een expansie zou geven in tien termen, waarvan de noemer van de laatste meer dan 500 decimalen lang is!

Als praktische toepassing wist Gottfried Stratemeyer in 1930 een benaderingsmethode op te stellen voor nulpunten van polynomen gebaseerd op Fibonacci's algoritme.

Ook getallen werden in het oude Egypte weergegeven met behulp van hiërogliefen. Hun stelsel is gebaseerd op machten van 10 tot een miljoen; zie de tabel en het voorbeeld hieronder.

1	10	100	1.000	10.000	100.000	1.000.000
	∩	∩∩	∩∩∩	∩∩∩∩	∩∩∩∩∩	∩∩∩∩∩∩

$$= 21.237$$

Op deze manier konden de Egyptenaren voor het dagelijks leven voldoende grote getallen noteren. Optellingen en aftrekkingen werden genoteerd met behulp van de volgende symbolen; wanneer de voetjes in de leesrichting wezen stelden ze een optelling voor, anders een aftrekking.

∩ of ∩

Het volgende symbool boven een getal genoteerd, stelt de inverse ervan voor; letterlijk betekent het "deel".



Bijvoorbeeld:

$$= \frac{1}{331}$$

## 30 Vermoeden van Erdős-Straus

In 1948 uitten Paul Erdős en Ernst Straus het vermoeden dat het rationaal getal  $\frac{4}{n}$  steeds kan worden geschreven als de som van juist drie stambreuken (zie 29, blz. 20), voor elk natuurlijk getal  $n \geq 2$ . Met andere woorden, volgende vergelijking zou steeds oplossingen hebben in  $\mathbb{N}$ :

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

Er zijn enkele patronen bekend voor even  $n$  en voor  $n$  congruent met 3 modulo 4, en computerberekeningen verifieerden alle natuurlijke getallen tot  $10^{14}$ , maar het probleem is nog niet algemeen opgelost.

- $\frac{4}{2k} = \frac{1}{2k} + \frac{1}{2k} + \frac{1}{k}$
- $\frac{4}{4k+3} = \frac{1}{2(k+1)} + \frac{1}{2(k+1)} + \frac{1}{(k+1)(4k+3)}$

Het aantal oplossingen voor  $n$  staat in OEIS A073101.

## 31 Constante van Mills

De constante van Mills, hier  $\theta$ , is het kleinste positieve reële getal  $\theta$  zodat de uitdrukking  $\lfloor \theta^{3^n} \rfloor$  uitsluitend priemgetallen genereert voor natuurlijke getallen  $n$ . Het bestaan van deze constante werd bewezen door William Mills in 1947; in feite bestaan er oneindig veel reële getallen met deze eigenschap. Onder aanname van de Riemann-hypothese (zie ??, blz. ??) bedraagt de waarde van de kleinste ongeveer 1,3063778838630806904686144926...

De priemgetallen gegenereerd door deze functie worden priemgetallen van Mills genoemd. Opnieuw onder aanname van de Riemannhypothese, zijn Mills' priemgetallen de volgende. Ze kunnen zonder  $\theta$  worden gevonden als het kleinste priemgetal dat volgt na de derdemacht van het vorige, te beginnen bij 2.

2, 11, 1361, 2521008887, 16022236204009818131831320183... (OEIS A051254)

Jammer genoeg kent het resultaat van Mills geen praktische toepassingen: om priemgetallen te vinden met behulp van deze formule, moet eerst een voldoende nauwkeurige waarde voor  $\theta$  bekend zijn, en deze waarde valt slechts te berekenen uit reeds gekende priemgetallen. Er is geen gesloten vorm voor  $\theta$  bekend, noch is bewezen of  $\theta$  al dan niet rationaal is.

## 32 Priemgetalhiaten

De klassieke priemgetalstelling van Gauss (zie 1, blz. 5) impliceert dat het gemiddelde priemgetalhiaat (het verschil tussen twee opeenvolgende priemgetallen) ongeveer  $\ln n$  bedraagt in de buurt van  $n$ . Desondanks kunnen deze hiaten willekeurig groot worden; de rij  $m!+2, m!+3 \dots m!+m$  bestaat namelijk uit  $m-1$  opeenvolgende, samengestelde natuurlijke getallen voor willekeurige  $m$ .

Er zijn verscheidene andere stellingen en nog meer vermoedens met betrekking tot de verdeling van de priemgetallen, die nauwkeurigere resultaten voor deze priemgetalhiaten geven.

### 32.1 Postulaat van Bertrand

In 1845 uitte Joseph Bertrand het niet zo verwonderlijke vermoeden dat er zich telkens minstens één priemgetal bevindt tussen elk natuurlijk getal en het dubbele ervan. Hij verifieerde zelf alle getallen tussen 2 en  $3 \times 10^6$ , en

Pafnuty Chebyshev bewees vijf jaar later de stelling volledig.

$$\forall n \in \mathbb{N} \setminus \{0, 1\} : \exists p \in \mathbb{P} : n < p < 2n$$

Paul Erdős verbeterde de stelling van Chebyshev door te bewijzen dat voor elk natuurlijk getal  $k$ , er een getal  $N$  bestaat zodanig dat wanneer  $n > N$ , er zich minstens  $k$  priemgetallen bevinden tussen  $n$  en  $2n$ .

$$\forall k \in \mathbb{N} : \exists N \in \mathbb{N} : \forall n \in \mathbb{N} : \exists p_1, p_2 \dots p_k \in \mathbb{P} : n > N \rightarrow n < p_1 < p_2 < \dots < p_k < 2n$$

In 2006 bewees Mohamed El Bachraoui het bestaan van een priemgetal tussen  $2n$  en  $3n$ ; Andy Loo bewees hetzelfde voor  $3n$  en  $4n$  in 2011.

### 32.2 Priemgetallen van Ramanujan

Srinivasa Ramanujan gaf in 1919 een nieuw bewijs van Bertrands postulaat en een generalisatie ervan. Hij definieerde de naar hem vernoemde priemgetallen als de kleinste natuurlijke getallen  $R_n$  zodanig dat voor alle  $x \geq R_n$  geldt dat  $\pi(x) - \pi\left(\frac{x}{2}\right) \geq n$  (met  $\pi(x)$  de priemgetal-telfunctie). Deze getallen zijn zelf noodzakelijkerwijze priem, omdat de functie  $x \mapsto \pi(x) - \pi\left(\frac{x}{2}\right)$  slechts kan toenemen op een priemgetal  $x$ .

2, 11, 17, 29, 41, 47, 59, 67, 71, 97, 101, 107, 127, 149, 151, 167, 179, 181, 227, 229, 233 . . . (OEIS A104272)

Wanneer  $n$  naar oneindig gaat, nadert het  $n^{\text{de}}$  priemgetal van Ramanujan tot het  $2n^{\text{de}}$  priemgetal.

### 32.3 Vermoeden van Legendre

Net als het postulaat van Bertrand lijkt het vermoeden van Legendre nogal voor de hand liggend, maar tot op vandaag blijft deze onbewezen. Het stelt dat er zich minstens één priemgetal bevindt tussen elke twee opeenvolgende volkomen kwadraten. Het aantal dergelijke priemgetallen staat in OEIS A014085, en het vermoeden werd gecontroleerd tot  $10^{18}$ .

$$\forall n \in \mathbb{N}_0 : \exists p \in \mathbb{P} : n^2 < p < (n+1)^2$$

Legendres vermoeden zou impliceren dat de priemgetalhiaten in  $\mathcal{O}(\sqrt{p_n})$  zitten.

$$p_{n+1} - p_n = \mathcal{O}(\sqrt{p_n})$$

Zowel het vermoeden van Andrica, Opperman als Cramér impliceren het vermoeden van Legendre.

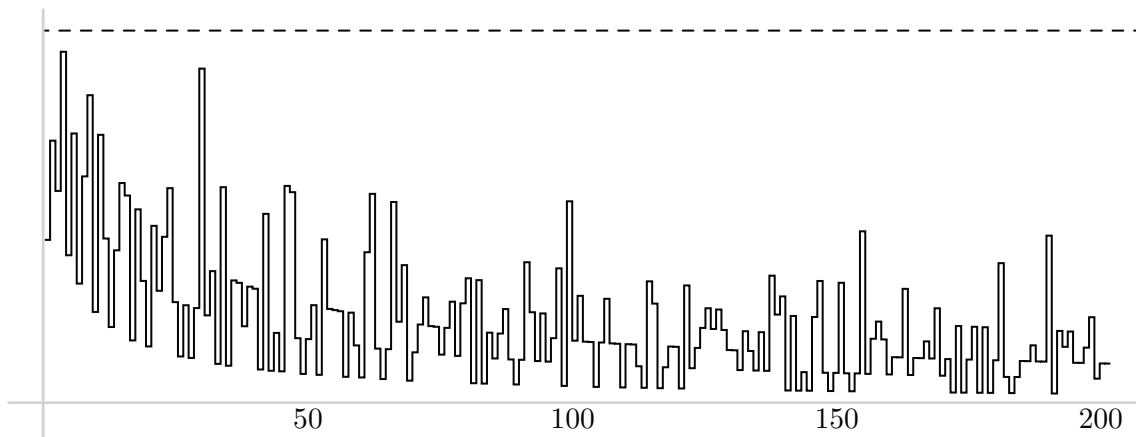
### 32.4 Vermoeden van Andrica

Het vermoeden van Dorin Andrica stelt de volgende ongelijkheid over het  $n^{\text{de}}$  priemgetal  $p_n$ :

$$\sqrt{p_{n+1}} - \sqrt{p_n} < 1$$

$$p_{n+1} - p_n < 2\sqrt{p_n} + 1$$

Tot op  $1,3002 \times 10^{16}$  werd het vermoeden bevestigd, maar er is nog geen bewijs of tegenvoorbeeld gevonden. Een plot voor de eerste 200 priemgetallen blijft duidelijk onder de kritieke lijn op 1.



### 32.5 Vermoeden van Oppermann

Deens wiskundige Ludvig Oppermann publiceerde in 1882 een sterker vermoeden dan dat van Legendre, namelijk dat er voor elk natuurlijk getal  $n > 1$  een eerste priemgetal te vinden is tussen  $n(n-1)$  en  $n^2$ , en een tweede priemgetal tussen  $n^2$  en  $n(n+1)$ .

$$\forall n \in \mathbb{N} \setminus \{0, 1\} : \exists p_1, p_2 \in \mathbb{P} : n(n-1) < p_1 < n^2 < p_2 < n(n+1)$$

### 32.6 Vermoeden van Cramér

In 1936 bewees Zweeds wiskunde en statisticus Harald Cramér dat, onder aanname van de Riemannhypothese,  $p_{n+1} - p_n = \mathcal{O}(\sqrt{p_n} \cdot \ln p_n)$ . Daaruit vermoedde Cramér een sterker resultaat, namelijk:

$$p_{n+1} - p_n = \mathcal{O}((\ln p_n)^2)$$

### 32.7 Vermoeden van Firoozbakht

Farideh Firoozbakht, vrouwelijk wiskundige aan de Universiteit van Isfahan in Iran, vermoedde in 1982 dat de functie  $n \mapsto \sqrt[n]{p_n}$  strikt dalend is. Dit relatief sterke resultaat zou het vermoeden van Cramér impliceren en blijft onbewezen, hoewel positief bevonden tot  $4,444 \times 10^{12}$ .

$$\forall n \in \mathbb{N}_0 : \sqrt[n+1]{p_{n+1}} < \sqrt[n]{p_n}$$

$$p_{n+1} - p_n < \ln p_n \cdot (\ln p_n - 1)$$

## 33 Aritmetisch getal

Men zou misschien verwachten dat elk geheel getal “aritmetisch” genoemd kan worden, omdat de aritmetica of rekenkunde nu eenmaal over getallen gaat. Het begrip *aritmetisch getal* duidt echter die natuurlijke getallen aan waarvan het rekenkundig gemiddelde van zijn delers, zelf ook natuurlijk is. In het bijzonder is elk oneven priemgetal aritmetisch.

1, 3, 5, 6, 7, 11, 13, 14, 15, 17, 19, 20, 21, 22, 23, 27, 29, 30, 31, 33, 35, 37, 38, 39, 41, 42, 43 . . . (OEIS A003601)

De getallen waarvoor deze eigenschap niet geldt worden steeds schaarser; het kan worden aangetoond dat de aritmetische getallen een asymptotische dichtheid gelijk aan 1 hebben, en dus voldoen aan de volgende eenvoudige relatie, met  $A(n)$  het aantal aritmetische getallen ten hoogste  $n$ .

$$A(n) \sim n$$

## 34 Vermoeden van Gilbreath

Norman Gilbreath ontdekte in 1958 een patroon in de priemgetallen, gedroedeld op een servet. Tachtig jaar eerder werd hetzelfde patroon opgemerkt door François Proth, die er zelfs een bewijs voor dacht te kunnen geven, dat later echter onjuist bleek te zijn. Ondertussen is het vermoeden nog steeds niet bewezen.

Beschouw de alom bekende rij van priemgetallen (OEIS A000040):

- 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103 . . .

Bereken nu de verschillen tussen de opeenvolgende priemgetallen. Elk van deze termen is dan even, omdat alle priemgetallen oneven zijn, behalve de allereerste term - deze is gelijk aan 1 (OEIS A001223):

- 1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, 4, 2, 4, 2, 4, 14, 4, 6, 2, 10, 2, 6, 6, 4 . . .

Daarna berekende Gilbreath opnieuw de verschilrij van deze termen, en bleef hij deze stap herhalen. Wat hij uiteindelijk opmerkte, en Proth dacht bewezen te hebben, is dat elke verschilrij begint met 1.

- 1, 0, 2, 2, 2, 2, 2, 4, 4, 2, 2, 2, 0, 4, 4, 2, 2, 4, 2, 2, 2, 4, 2, 2, 2, 2, 10, 10, 2, 4, 8, 8, 4, 0, 2 . . .
- 1, 2, 0, 0, 0, 0, 0, 2, 0, 2, 0, 0, 0, 2, 4, 0, 2, 0, 2, 2, 0, 0, 2, 2, 0, 0, 8, 0, 8, 2, 4, 0, 4, 4, 2 . . .
- 1, 2, 0, 0, 0, 0, 2, 2, 2, 2, 0, 0, 2, 2, 4, 2, 2, 2, 0, 2, 0, 2, 0, 2, 0, 0, 8, 8, 6, 2, 4, 4, 0, 2 . . .
- 1, 2, 0, 0, 0, 2, 0, 0, 0, 2, 0, 2, 0, 2, 2, 0, 0, 2, 2, 2, 2, 2, 2, 0, 8, 0, 2, 4, 2, 0, 4, 2 . . .
- . . .

In 1993 heeft Andrew Odlyzko het vermoeden geverifieerd voor de eerste  $10^{13}$  priemgetallen met een ingenieuze methode om niet alle rijen apart te hoeven uitrekenen; de eerste 635 volstonden.

## 35 Stelling van Euler

De stelling van Euler vormt een belangrijke getaltheoretische uitbreiding van de kleine stelling van Fermat (zie 2, blz. 6), bewezen door Euler in 1736. Wanneer  $a$  en  $n$  onderling ondeelbaar zijn, en  $\varphi(n)$  de totiënt van  $n$  voorstelt (zie 12, blz. 10), geldt de volgende modulaire gelijkheid:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Ook het omgekeerde is waar: als bovenstaande gelijkheid geldt, dan zijn  $a$  en  $n$  relatief priem. Een gevolg is dat elk oneven getal  $m$  verheven tot de vierde macht, op hetzelfde cijfer eindigt als  $m$  (dit volgt uit het feit dat  $\varphi(10) = 4$ ). Anderzijds kan de stelling gebruikt worden om een modulaire macht te reduceren (voor  $a$  en  $n$  copriem):

$$x \equiv y \pmod{\varphi(n)} \quad \Rightarrow \quad a^x \equiv a^y \pmod{n}$$

De stelling van Euler vormt een van de basisprincipes van het RSA-algoritme (zie 321, blz. 311).

## 36 Harshadgetallen

Wanneer een natuurlijk getal deelbaar is door de som van de cijfers in een bepaalde basis, noemt men deze een Harshadgetal. Ze werden door Dattaraya Kaprekar gedefinieerd en vernoemd naar het Sanskriet *harṣa da*, vrij vertaald “geluksbrenger”. Ze staan ook bekend als de Nivengetallen (naar Ivan Niven).

De rij Harshadgetallen voor basis 10 begint bij:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 18, 20, 21, 24, 27, 30, 36, 40, 42, 45, 48, 50, 54, 60, 63, 70, 72 . . . (OEIS A005349)

Helen Grundman bewees in 1994 dat er geen 21 opeenvolgende Harshadgetallen bestaan in basis 10. Ze vond ook de 20 kleinste opeenvolgende getallen die dat wel zijn; een indrukwekkende prestatie aangezien de getallen in kwestie  $10^{44363342786}$  overschrijden.

Ook opvallend is dat de rij faculteiten begint met een heleboel Harshadgetallen (in basis 10). Dit patroon gaat echter niet op:  $432!$  is de kleinste niet-Harshad faculteit.

De dichtheid van de Harshadgetallen werd voor het eerst formeel geschat door Jean-Marie de Koninck en Nicolas Doyon. Noteer  $N(x)$  voor het aantal Harshadgetallen ten hoogste  $x$ ; zij toonden aan dat voor  $N(x)$  en voor elke reële  $\varepsilon > 0$  geldt:

$$x^{1-\varepsilon} \ll N(x) \ll \frac{x \ln(\ln x)}{\ln x}$$

Bovendien bewezen ze samen met Imre Kátai dat (met little- $o$ -notatie):

$$N(x) = \left( \frac{14}{27} \cdot \ln 10 + o(1) \right) \cdot \frac{x}{\ln x}$$

### 37 *abc*-vermoeden

Er bestaat een vruchtbare analogie tussen  $\mathbb{Z}$ , de verzameling gehele getallen, en  $\mathbb{C}[x]$ , de complexe veeltermen. Een krachtig voorbeeld is de gelijkheid tussen de ontbinding van gehele getallen in priemfactoren, en de ontbinding van complexe veeltermen tot lineaire factoren. Het is dan ook interessant na te gaan of stellingen in het ene gebied ook in het andere gebied te formuleren zijn, zoals de stelling van Mason-Stothers (zie 63, blz. 47): de getaltheoretische variant hiervan werd voorgesteld door David Masser in 1985 en Joseph Oesterlé in 1988 en is sindsdien berucht als het “*abc*-vermoeden”.

Net als bij Mason-Stothers wordt het radicaal van een geheel getal  $p$  gedefinieerd als het product van al zijn verschillende priemfactoren, bijvoorbeeld  $59535 = 3^5 \cdot 5 \cdot 7^2$  heeft radicaal  $3 \cdot 5 \cdot 7 = 105$ . We beschouwen de eenvoudige vergelijking  $a + b = c$  (vandaar de naam), met  $a, b, c \in \mathbb{Z}$  en allen onderling ondeelbaar. Bij de meeste sommen blijken er in het linkerlid meer priemfactoren te staan dan in het rechterlid, bijvoorbeeld  $2^{10} + 3^4 = 5 \cdot 13 \cdot 17$  geeft er veertien links en slechts drie rechts. Dit kan technisch worden beschreven als  $\max(|a|, |b|, |c|) < \text{rad}(abc)$ , of  $c < \text{rad}(abc)$  in  $\mathbb{N}$ , wat geldig is in de meeste gevallen. Het *abc*-vermoeden gaat nu net om met de uitzonderingen op deze algemene tendens.

Eerst en vooral moeten we opmerken dat er voor  $\max(|a|, |b|, |c|) < \text{rad}(abc)$  oneindig veel uitzonderingen zijn, zoals Cameron Stewart en Robert Tijdeman opmerkten in 1986. Een enkel voorbeeld is  $3 + 5^3 = 2^7$ . Voor een hele familie tegenvoorbeelden, kies  $a = 3^{2^n}$  en  $b = -1$ . Dan zal altijd gelden dat  $2^n \mid 3^{2^n} - 1$ , zodat wanneer  $n$  groot genoeg is, hieruit volgt:

$$\max(|a|, |b|, |c|) = 3^{2^n} > 3 \cdot 1 \cdot \frac{3^{2^n} - 1}{2^{n-1}} = \text{rad}(abc)$$

De vergelijking  $\max(|a|, |b|, |c|) < \text{rad}(abc)$  kan echter lichtjes worden aangepast, met drastische gevolgen. Wanneer we de volgende wijziging beschouwen, stelt het *abc*-vermoeden dat het aantal uitzonderingen plots *eindig* wordt, voor gelijk welke positieve  $\varepsilon$  (hoe klein ook):

$$\max(|a|, |b|, |c|) < \text{rad}(abc)^{1+\varepsilon}$$

Anders geformuleerd, bestaat er voor elke  $\varepsilon > 0$  een coëfficiënt  $K_\varepsilon$  zodat voor alle  $a, b, c \in \mathbb{N}$  geldt:

$$\max(|a|, |b|, |c|) < K_\varepsilon \cdot \text{rad}(abc)^{1+\varepsilon}$$



Dit toch wel verrassende vermoeden heeft zware consequenties. Omdat het zo algemeen is, zijn er een heleboel stellingen en vermoedens die direct bewezen zouden zijn als gevolg van het *abc*-vermoeden, zoals de laatste stelling van Fermat. Hoewel het anders uitdraaide, dacht men in feite zelfs in de jaren 80 dat via het *abc*-vermoeden het eerste bewijs geleverd zou worden voor deze notoire stelling. Andere gevolgen zijn te vinden op [http://en.wikipedia.org/wiki/Abc\\_conjecture#Some\\_consequences](http://en.wikipedia.org/wiki/Abc_conjecture#Some_consequences).

Groot was de opschudding toen zeer recentelijk (in augustus 2012) de Japanse wiskundige Shinichi Mochizuki beweerde een bewijs gevonden te hebben voor het *abc*-vermoeden. Hij bouwde daarvoor een heel eigen theorie op (“interuniversele Teichmüllertheorie”) en bewees daarmee tevens enkele andere open problemen, het vermoeden van Szpiro en dat van Vojta. Probleem is nog dat bijna niemand thuis is in deze theorie; wiskundigen zijn momenteel bezig het bewijs te verifiëren.

## 38 15-stelling

Kwadratische vormen zijn veeltermen, eventueel in meerdere variabelen, waarvan de graad in alle termen gelijk is aan twee. Ze worden vaak voorgesteld via een symmetrische matrix, op de volgende manier:

$$w^2 + 2x^2 + 2y^2 + 11z^2 + 4wz + 2wy - 4xz \quad \longrightarrow \quad \begin{array}{c} w \quad x \quad y \quad z \\ \begin{array}{c} w \\ x \\ y \\ z \end{array} \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 2 & 0 & -2 \\ 1 & 0 & 2 & 0 \\ 2 & -2 & 0 & 11 \end{bmatrix} \end{array}$$

John Conway en William Schneeberger bewezen in 1993 dat wanneer een kwadratische vorm met geheelwaardige, positief-definiëte matrix alle positieve getallen tot en met 15 kan uitdrukken, ze dan *elke* positieve waarde vertegenwoordigt. Positief-definiëte houdt in dat elk resultaat positief moet zijn, ongeacht welke waarden de variabelen aannemen. Het bewijs was zeer technisch en werd nooit gepubliceerd, tot Manjul Bhargava een eenvoudiger bewijs vond en dit uitgaf in 2000.

Om preciezer te zijn, volstaat het dat de getallen  $\{1, 2, 3, 5, 6, 7, 10, 14, 15\}$  bereikt worden. Voor elk van deze negen getallen bestaat er een kwadratische vorm die alle positieve getallen aanneemt, behalve dit ene getal, zoals bijvoorbeeld het geval is voor 15 met  $w^2 + 2x^2 + 5y^2 + 5z^2$ .

Het voorbeeld van daarnet is een kwadratische vorm die aan de voorwaarden voldoet en dus elk positief geheel getal aanneemt; zo'n vorm wordt universeel genoemd.

$$w^2 + 2x^2 + 2y^2 + 11z^2 + 4wz + 2wy - 4xz \quad \longrightarrow \quad \begin{array}{c} w \quad x \quad y \quad z \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 5 \\ 6 \\ 7 \\ 10 \\ 14 \\ 15 \end{array} \begin{array}{c} w \\ x \\ y \\ z \end{array} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & -1 & 0 & -1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 2 & 0 \end{bmatrix} \end{array}$$

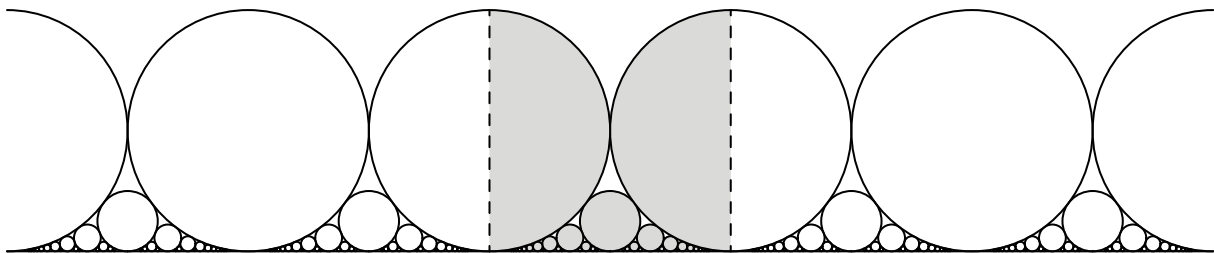
Een bescheidener voorbeeld is de vierkwadratenstelling van Lagrange (zie 25, blz. 17); de bijhorende matrix is eenvoudigweg de identiteitsmatrix van orde 4. Conways 15-stelling vormt echter geen alternatief bewijs omdat Lagranges stelling gebruikt wordt als hulpstelling voor die van Conway.

Naast een eenvoudiger bewijs gaf Manjul Bhargava ook enkele gerelateerde versies. Zijn 290-stelling garandeert dat een kwadratische vorm met gehele coëfficiënten elk positief getal representeert als dat zo is voor  $\{1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290\}$ ; de voorwaarde dat de bijhorende matrix geheelwaardig is, valt hiermee weg. En voor elk van deze 29 getallen bestaat er een kwadratische vorm die alleen dat getal niet kan weergeven.

Indien van kracht voor  $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 67, 73\}$  geeft een kwadratische vorm alle priemgetallen weer, en voor  $\{1, 3, 5, 7, 11, 15, 33\}$  alle oneven getallen.

## 39 Fordcirkels

Beschouw de reële getallen  $\frac{p}{q}$  en teken boven elke breuk  $\frac{p}{q}$  in zijn eenvoudigste vorm, een cirkel met straal  $\frac{1}{q^2}$ . Men zou verwachten dat dit een chaotisch zootje oplevert liggen, maar in feite vormen ze een mooi ordelijk systeem van oneindig veel onderling rakende cirkels.

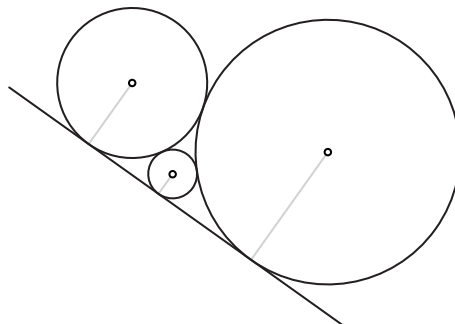


Deze cirkels worden vernoemd naar Lester Ford en voor een breuk  $\frac{p}{q}$  genoteerd als  $C[p, q]$ . Twee Fordcirkels  $C[p, q]$  en  $C[r, s]$  raken elkaar als en slechts als  $ps$  en  $qr$  opeenvolgende gehele getallen zijn, of de bijhorende breuken elkaars buur zijn in een bepaalde Fareysequentie (zie 19, blz. 13). De cirkel ingeklemd tussen twee rakende Fordcirkels  $C[p, q]$  en  $C[r, s]$  is die horende bij de mediant van de breuken,  $C[p + r, q + s]$ .

De oppervlakte  $A$  van alle Fordcirkels tussen twee gehele getallen (het aangeduide gebied op de tekening) kan worden uitgedrukt met behulp van Eulers totiëntfunctie (zie 12, blz. 10) of Riemanns zètafunctie (zie ??, blz. ??):

$$A = \frac{\pi}{4} \cdot \sum_{q=1}^{\infty} \frac{\varphi(q)}{q^4} = \frac{\pi \zeta(3)}{4 \zeta(4)} = \frac{45 \zeta(3)}{2 \pi^3}$$

De eigenschappen van deze cirkels komen al voor in Japanse sangaku's, geometrische stellingen in de vorm van puzzels. Een typisch probleem, uit 1824, beschrijft drie rakende cirkels met een gemeenschappelijke raaklijn. Gegeven de stralen  $r_1$  en  $r_3$  van de buitenste grote cirkels, wat is dan de straal  $r_2$  van de kleinere ertussen? Het antwoord kan worden afgeleid uit de constructie van de Fordcirkels:



$$\frac{1}{\sqrt{r_2}} = \frac{1}{\sqrt{r_1}} + \frac{1}{\sqrt{r_3}}$$

## 40 Kwadratische reciprociteit

De wet van kwadratische reciprociteit is een zeer krachtig getaltheoretisch resultaat, vermoed door Leonhard Euler en Adrien-Marie Legendre en bewezen door Carl Friedrich Gauss. Gauss omschreef de wet in zijn *Disquisitiones Arithmeticae* als de “fundamentele stelling” en refereerde er heimelijk naar als de “gulden stelling”. Hij publiceerde zes bewijzen ervoor en hield er nog twee voor zichzelf; momenteel zijn er al meer dan 200 bewijzen gekend.

Kwadratische reciprociteit is het eenvoudigst te omschrijven met behulp van de zogenaamde Legendresymbolen. Deze worden als volgt gedefinieerd voor een oneven priemgetal  $p$ :

$$\left[ \begin{array}{c} a \\ p \end{array} \right] = \begin{cases} 1 & \text{als } x^2 \equiv a \pmod{p} \text{ oplossingen heeft} \\ 0 & \text{als } p \mid a \\ -1 & \text{als } x^2 \equiv a \pmod{p} \text{ geen oplossingen heeft} \end{cases}$$

Een getal  $a$  waarvoor  $x^2 \equiv a \pmod{p}$  oplosbaar is, heet een kwadratische rest modulo  $p$ , anders een kwadratische niet-rest modulo  $p$ . De volgende eenvoudige rekenregels, samen met de wet van kwadratische reciprociteit verderop, zijn erg handig om Legendresymbolen van grote getallen, waarvoor de kwadratische congruentie rechtstreeks oplossen te veel werk is, te herleiden naar kleinere waarden:

$$a \equiv b \pmod{p} \Rightarrow \left[ \begin{array}{c} a \\ p \end{array} \right] = \left[ \begin{array}{c} b \\ p \end{array} \right]$$

Daarenboven is het Legendresymbool volledig multiplicatief in zijn bovenste argument:

$$\left[ \begin{array}{c} a \cdot b \\ p \end{array} \right] = \left[ \begin{array}{c} a \\ p \end{array} \right] \cdot \left[ \begin{array}{c} b \\ p \end{array} \right]$$

Als lemma's voor de kwadratische reciprociteitswet zijn er nog twee supplementen. De eerste stelt dat  $x^2 \equiv -1 \pmod{p}$  oplosbaar is als en slechts als  $p \equiv 1 \pmod{4}$ . De tweede stelt dat  $x^2 \equiv 2 \pmod{p}$  oplosbaar is als en slechts als  $p \equiv \pm 1 \pmod{8}$ . Deze concrete waarden zijn handig omdat in feite de berekening van elk Legendresymbool kan herleid worden naar deze twee vormen. De uiteindelijke kwadratische reciprociteit stelt nu, voor oneven priemgetallen  $p$  en  $q$ :

$$\left[ \begin{array}{c} p \\ q \end{array} \right] = \begin{cases} \left[ \begin{array}{c} q \\ p \end{array} \right] & \text{als } p \equiv 1 \text{ of } q \equiv 1 \pmod{4} \\ -\left[ \begin{array}{c} q \\ p \end{array} \right] & \text{als } p \equiv 3 \text{ en } q \equiv 3 \pmod{4} \end{cases}$$

Of equivalent, in één formule:

$$\left[ \begin{array}{c} p \\ q \end{array} \right] \cdot \left[ \begin{array}{c} q \\ p \end{array} \right] = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Vele bewijzen voor deze eigenschap steunen op van Gauss' lemma, een theoretisch significante voorwaarde voor kwadratische resten. Gauss bewees zijn lemma voor het eerst in zijn derde bewijs van kwadratische reciprociteit en gebruikte hem opnieuw in zijn vijfde bewijs. Beschouw een oneven priemgetal  $p$  en een copriem getal  $a$ , bereken de serie getallen  $\{a, 2a, 3a \dots \frac{p-1}{2}a\}$  en noem  $n$  het aantal van deze waarden groter dan  $\frac{p}{2}$ . Volgens het lemma van Gauss geldt dan:

$$\left[ \begin{array}{c} a \\ p \end{array} \right] = (-1)^n$$

Er zijn ook (complexere) uitbreidingen naar derde- en vierdegraadsreciprociteitswetten.

## 41 Vermoeden van Collatz

Het vermoeden van Collatz, vernoemd naar Lothar Collatz die het probleem voorstelde in 1937, is een intrigerend open probleem dat ondanks zijn eenvoudige formulering zeer moeilijk op te lossen blijkt, als het al oplosbaar is. Paul Erdős zei zelfs dat “de wiskunde nog niet rijp was voor zulke problemen” en bood \$500 voor een oplossing. Het probleem staat ook bekend als het vermoeden van Ulam, het vermoeden van Thwaites, het probleem van Kakutani of het probleem van Syracuse, en de getallen die erin voorkomen als hagelsteengetallen.

Begin met een willekeurig geheel getal  $n$  en pas er herhaaldelijk de volgende functie op toe:

$$f(n) = \begin{cases} \frac{n}{2} & \text{voor } n \text{ even} \\ 3n + 1 & \text{voor } n \text{ oneven} \end{cases}$$

Uitgevoerd met bijvoorbeeld  $n = 11$  verkrijgen we dit:

$$11 \rightarrow 34 \rightarrow 17 \rightarrow 52 \rightarrow 26 \rightarrow 13 \rightarrow 40 \rightarrow 20 \rightarrow 10 \rightarrow 5 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1 \rightarrow 4 \rightarrow 2 \rightarrow 1 \rightarrow \dots$$

Enmaal op 1 terechtgekomen, belandt het systeem in een cykel  $1 \rightarrow 4 \rightarrow 2 \rightarrow 1$ . Het vermoeden van Collatz stelt dat *elke* initiële waarde ooit in deze cykel terechtkomt, zodat er geen patronen met onbegrensde groei of andere cycli zouden voorkomen. Het vermoeden wordt algemeen als correct beschouwd, en werd gecontroleerd voor alle  $n \leq 19 \cdot 2^{58} \approx 5,48 \times 10^{18}$ , maar er is nog geen bewijs bekend.

De banen van de verschillende getallen kunnen schematisch worden weergegeven in een boomdiagram zoals hieronder; we zien inderdaad dat alle knooppunten in deze boom naar de wortel ervan (1) leiden, en dat er geen niet-triviale cycli voorkomen.



Er is al lichte vooruitgang geboekt: Jeffrey Lagarias bewees dat er geen cycli voorkomen met lengte kleiner dan 275.000, buiten  $1 \rightarrow 4 \rightarrow 2 \rightarrow 1$  natuurlijk. Stuart Kurtz en Janos Simon bewezen dat een natuurlijke generalisatie van de functie  $f$  tot een algoritmisch onbeslisbaar probleem leidt; helaas kan hun bewijstechniek niet toegepast worden op het originele probleem van Collatz, maar de mogelijkheid bestaat dus dat ook deze onbeslisbaar is.

Een andere leuke manier om de hagelsteengetallen uit te rekenen is via dit algoritme.

- Schrijf het begingetal  $n$  binair.
- Schrijf hetzelfde getal eronder, maar met een 1 toegevoegd achteraan (dit geeft  $2n + 1$ ).
- Tel de twee getallen op (dit geeft  $3n + 1$ ).
- Schrap elke nul achteraan de som (dit deelt zover als mogelijk door 2) en herhaal vanaf stap 2.

$$\begin{array}{r}
1 \ 1 \ 1 = 7 \\
+ \ 1 \ 1 \ 1 \ 1 \\
\hline
1 \ 0 \ 1 \ 1 \ \emptyset = 11 \\
+ \ 1 \ 0 \ 1 \ 1 \ 1 \\
\hline
1 \ 0 \ 0 \ 0 \ 1 \ \emptyset = 17 \\
+ \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \\
\hline
1 \ 1 \ 0 \ 1 \ \emptyset \ \emptyset = 13 \\
+ \ 1 \ 1 \ 0 \ 1 \ 1 \\
\hline
1 \ 0 \ 1 \ \emptyset \ \emptyset \ \emptyset = 5 \\
+ \ 1 \ 0 \ 1 \ 1 \\
\hline
1 \ \emptyset \ \emptyset \ \emptyset \ \emptyset = 1
\end{array}$$

Het Collatzsysteem kan ook worden toegepast op de gehele getallen  $\mathbb{Z}$  i.p.v.  $\mathbb{N}_0$ . In dit geval wordt vermoed dat er vijf cykels zijn, en dat alle beginwaarden uiteindelijk in één ervan terechtkomen. De gekende cykels zijn:

- $1 \rightarrow 4 \rightarrow 2 \rightarrow 1 \rightarrow \dots$
- $0 \rightarrow 0 \rightarrow \dots$
- $-1 \rightarrow -2 \rightarrow -1 \rightarrow \dots$
- $-5 \rightarrow -14 \rightarrow -7 \rightarrow -20 \rightarrow -10 \rightarrow -5 \rightarrow \dots$
- $-17 \rightarrow -50 \rightarrow -25 \rightarrow -74 \rightarrow -37 \rightarrow -110 \rightarrow -55 \rightarrow -164 \rightarrow -82 \rightarrow -41$   
 $\rightarrow -122 \rightarrow -61 \rightarrow -182 \rightarrow -91 \rightarrow -272 \rightarrow -136 \rightarrow -68 \rightarrow -34 \rightarrow -17 \rightarrow \dots$

## 42 $p$ -adische getallen

De  $p$ -adische getallen vormen een alternatieve uitbreiding van het veld der rationale getallen. Kurt Hensel was de eerste die ze beschreef, in 1897, hoewel eerder werk van Ernst Kummer er al impliciet gebruik van maakte. De clou van de opbouw is een andere metriek te kiezen dan die van de klassieke velduitbreiding van  $\mathbb{Q}$  naar  $\mathbb{R}$ , die gebruikmaakt van de absolute waarde, ook wel de Euclidische metriek genoemd. In tegenstelling tot reële getallen met grondtal  $p$  liggen  $p$ -adische getallen dichter bij elkaar naarmate hun verschil een *grotere* macht van  $p$  is. Ondanks dat ze er raar uitzien, maakt dit ze (met name in getaltheorie) tot een krachtig hulpmiddel, omdat ze zo bepaalde informatie van congruentie coderen. Andrew Wiles' bewijs van de Laatste Stelling van Fermat bijvoorbeeld baat deze handige eigenschap uit.

In  $\mathbb{R}$  kunnen dezelfde reële getallen uitgedrukt worden in verschillende grondtallen. Een eerste belangrijke verschil met de  $p$ -adische getallen is dat voor verschillende waarden van  $p$ , de geconstrueerde systemen in essentie verschillend zijn: 2-adische en 3-adische getallen bijvoorbeeld kunnen niet zomaar “vertaald” worden, terwijl reële getallen eenvoudig van grondtal 2 naar grondtal 3 te converteren zijn. Nog een conventie daaromtrent: zonder expliciete vermelding over welk systeem  $\mathbb{Q}_p$  er wordt gewerkt, wordt er een subscript  $p$  extra genoteerd achteraan het getal.

De nieuwe  $p$ -adische norm  $|x|_p$  wordt als volgt gedefinieerd, voor een zeker priemgetal  $p$ :

$$|x|_p = \begin{cases} 0 & \text{voor } x = 0 \\ p^{-n} & \text{voor } x = p^n \cdot \frac{a}{b} \text{ met } a \text{ en } b \text{ copriem met } p \end{cases}$$

In deze definitie is  $n$  dus de exponent van de grootste macht van  $p$  die  $x$  nog deelt. De afstand tussen twee  $p$ -adische getallen  $x$  en  $y$  wordt dan gegeven door  $|x - y|_p$ . Deze is inderdaad een metriek, want ze is positief-definiet, enkel gelijk aan nul als haar argument nul is, symmetrisch en ten slotte voldoet ze ook aan de driehoeksongelijkheid:  $|x + y|_p \leq |x|_p + |y|_p$ . In feite geldt zelfs nog de sterkere eigenschap dat  $|x + y|_p \leq \max(|x|_p, |y|_p)$ .

Hieruit volgt meteen dat  $|nx|_p \leq |x|_p$  voor  $n \in \mathbb{N}$ ; dit maakt de  $p$ -adische norm “niet-Archimedisch”.

Het blijkt nu dat het klassieke veld der rationale getallen uitgerust met deze norm niet compleet is: niet elke Cauchyrij, een rij waarvan de termen willekeurig dicht bij elkaar komen te liggen, convergeert naar een rationaal getal. Het  $p$ -adische systeem is een uitbreiding van  $\mathbb{Q}$  in de zin dat deze Cauchyrijen wél steeds convergeren naar een  $p$ -adisch getal en dat  $\mathbb{Q} \subset \mathbb{Q}_p$ .

Hoe zien  $p$ -adische getallen er nu uit? We kunnen weer vergelijken met reële getallen: getallen uit  $\mathbb{R}$  hebben telkens een eindig aantal cijfers voor de komma en eventueel oneindig veel cijfers na de komma, al dan niet met een voortgezet patroon. In de verzameling  $p$ -adische getallen echter, genoteerd als  $\mathbb{Q}_p$ , is het net andersom:  $p$ -adische getallen kunnen eindeloos verdergaan vóór de komma! Genoteerd met coëfficiënten  $a_i \in \{0, 1, \dots, p-1\}$  worden beide soorten als volgt gerepresenteerd in grondtal  $p$  of  $p$ -adisch:

$$\mathbb{R} \ni x = \pm \sum_{i=-\infty}^n a_i p^i \quad \leftrightarrow \quad \mathbb{Q}_p \ni x = \sum_{i=n}^{+\infty} a_i p^i$$

Hierin kan  $n$  zowel een positief als negatief geheel getal zijn. Het concept van afstand tussen  $p$ -adische getallen is nu verrassend anders tussen reële getallen: in  $\mathbb{R}$  met grondtal 7 liggen 66665 en 66666 dichter bij elkaar dan 56666 en 66666, terwijl het in  $\mathbb{Q}_p$  net omgekeerd is! Er geldt daar namelijk dat  $|66666 - 56666|_7$  kleiner is dan  $|66666 - 66665|_7$ .

Een volgende frappant verschil met  $\mathbb{R}$  is dat  $\mathbb{Q}_p$  geen mintekens kent; negatieve  $p$ -adische getallen worden geschreven met een doorlopende reeks cijfers voor de komma, want het  $p$ -adische systeem maakt “oneindig doorlenen” in het cijferen mogelijk. Met reële getallen lukt dit niet, omdat er uiteindelijk domweg geen cijfers meer bestaan om te lenen aan de linkerkant, en er dus nood is aan een minteken. Beschouw als voorbeeld  $3 - 4$  in 5-adisch:

$$\begin{array}{r} \dots \quad 4 \quad 4 \quad 4 \quad 4 \quad 13 \\ \dots \quad \emptyset \quad \emptyset \quad \emptyset \quad \emptyset \quad \cancel{3} \\ - \\ \dots \quad 4 \quad 4 \quad 4 \quad 4 \quad 4 \end{array}$$

Voor de rest werkt optellen en aftrekken van  $p$ -adische getallen op dezelfde maniers als van reële getallen, net als vermenigvuldigen. Delen levert echter problemen op: als reëel getal kan  $\frac{1}{3}$  geschreven worden als  $0,3333\dots$  maar dit is niet toegestaan in  $p$ -adisch. Een tweede complicatie is dat delen in  $\mathbb{Q}_p$  enkel mogelijk blijkt voor een priemgetal  $p$ , anders vormt  $\mathbb{Q}_p$  geen veld. Een mooie illustratie daarvoor is dat in  $\mathbb{Q}_{10}$  er vier getallen zijn die gelijk zijn aan hun eigen kwadraat, nl.  $0, 1, \dots, 12890625$  en  $\dots, 87109376$ !

Als we bijvoorbeeld in  $\mathbb{Q}_5$  de inverse van 3 zoeken, vinden we  $\dots, 131313132$ . Vermenigvuldigd met 3 levert dit immers inderdaad 1 op:

$$\begin{array}{r} \dots \quad 2 \quad 1 \quad 2 \quad 1 \\ \dots \quad 1 \quad 3 \quad 1 \quad 3 \quad 2 \\ \times \\ \dots \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \end{array}$$

Het algemene algoritme waarmee inversen kunnen worden bepaald, op voorwaarde dat ze bestaan, verloopt analoog als in  $\mathbb{R}$ . Beschouw een  $p$ -adische deling  $\frac{a}{b}$ , dan wordt die als volgt berekend:

- Noteer  $n$  voor het meest rechtse cijfer van  $a$ .
- Zoek het kleinste getal  $d$  dat vermenigvuldigd met  $b$  eindigt op  $n$ . Deze  $d$  is het meest rechtse cijfer van het te berekenen quotiënt, schrijf deze dus op.

- Trek  $b \cdot d$  af van  $a$  en laat de 0 achteraan de uitkomst vallen. Deze waarde wordt  $a'$ .
- Herhaal deze stappen met  $\frac{a'}{b}$  en schrijf de gevonden  $d$ 's steeds links van de eerdere.

Men kan ook de  $p$ -adische gehele getallen beschouwen: naar analogie zijn deze juist de  $p$ -adische getallen waarvan het gedeelte na de komma 0 is, of equivalent, waarvan de  $p$ -norm ten hoogste 1 is. Ze vormen een commutatieve ring die wordt genoteerd als  $\mathbb{Z}_p$  (niet te verwarren met de notatie voor restklassenringen). Zo te zien in de voorbeelden hierboven is de waarde van  $3 - 4$  inderdaad zelf ook element van  $\mathbb{Z}_5$ , hoewel dit wellicht niet echt verrassend is. Opmerkelijker is dat  $\frac{1}{3}$  óók een 5-adisch geheel getal is! In feite ligt elke deling van  $p$ -adische gehele getallen zelf weer in  $\mathbb{Z}_p$ , behalve als de noemer een veelvoud van  $p$  is: de deling  $\frac{1}{p}$  geeft bijvoorbeeld  $\dots 000,1$ .  $\mathbb{Z}_p$  is trouwens overaftelbaar oneindig.

Er gebeuren nog gekkere dingen in deze velden. Zo kan het worden aangetoond dat  $i$ , de imaginair eenheid die voldoet aan  $i^2 = -1$ , niet kan worden uitgedrukt in  $\mathbb{Q}_2$ , noch in  $\mathbb{Q}_3$ , maar wel in  $\mathbb{Q}_5$ ! Er geldt daar dat  $i = \dots 14223032431212$ . Merk op dat dit getal niet in  $\mathbb{Q}$  zit, dus het is geoorloofd om  $i$  irrationaal te noemen, maar klaarblijkelijk is het ook een 5-adisch geheel getal. Wanneer we dit getal met zichzelf vermenigvuldigen, merken we inderdaad (voor het gemak zijn de grijze carries weggelaten):

$$\begin{array}{r}
 \dots 3 \ 2 \ 4 \ 3 \ 1 \ 2 \ 1 \ 2 \\
 \times \dots 3 \ 2 \ 4 \ 3 \ 1 \ 2 \ 1 \ 2 \\
 \hline
 \dots 2 \ 0 \ 4 \ 1 \ 2 \ 4 \ 2 \ 4 \\
 \dots 2 \ 4 \ 3 \ 1 \ 2 \ 1 \ 2 \\
 \dots 4 \ 1 \ 2 \ 4 \ 2 \ 4 \\
 \dots 3 \ 1 \ 2 \ 1 \ 2 \\
 \dots 4 \ 1 \ 4 \ 1 \\
 \dots 4 \ 0 \ 3 \\
 \dots 2 \ 4 \\
 + \dots 1 \\
 \hline
 \dots 4 \ 4 \ 4 \ 4 \ 4 \ 4 \ 4 \ 4 = -1
 \end{array}$$

In feite is  $p$ -adisch rekenwerk eenvoudiger dan de conventionele reële getallen. Alles gaat van rechts naar links. Door hun uniformiteit werd er zelfs voorgesteld  $p$ -adische getallen te gebruiken voor computerhardware, omdat die gemakkelijker handelbaar zijn! Daarenboven is een  $p$ -adische schrijfwijze uniek, terwijl bijvoorbeeld het reële getal  $1,0000\dots$  ook geschreven kan worden als  $0,9999\dots$

Het  $p$ -adische getallensysteem geeft ook aanleiding tot een alternatieve vorm van analyse, waarin sterke resultaten gelden. Als gevolg van het niet-Archimedisch zijn van de  $p$ -adische norm geldt bijvoorbeeld dat een  $p$ -adische reeks  $\sum a_i$  convergeert als en slechts als zijn algemene term  $a_n$  naar 0 nadert voor  $n \rightarrow \infty$ , in schril contrast met reële reeksen, waar de grens tussen convergentie en divergentie veel subtieler is (denk maar aan de harmonische reeks).

Een voorbeeld van een reeks die convergeert binnen  $\mathbb{Q}_5$ , maar niet in  $\mathbb{R}$ , is de reeks  $1 + 5 + 25 + 125 + \dots$  (of  $1 + 10 + 100 + 1000 + \dots$  in grondtal 5) met algemene term  $5^n$ . Het blijkt immers dat  $5^n$  in dit systeem naar nul gaat: de afstand ertussen is  $|5^n - 0|_5 = |5^n|_5 = 5^{-n}$ , en deze wordt inderdaad willekeurig klein. De limiet van deze som is het getal  $\dots 1111$ , dat net  $\frac{-1}{4}$  voorstelt. Algemeen kunnen we in  $\mathbb{Q}_p$  stellen:

$$1 + p + p^2 + p^3 + \dots = \frac{1}{1 - p}$$

## 43 Kerstmisstelling van Fermat

Albert Girard zag als eerste een patroon in de priemgetallen uit te drukken als een som van twee kwadraten, in 1632. Pierre de Fermat was de eerste die beweerde er een bewijs voor te hebben, en schreef een brief daaromtrent

naar Marin Mersenne op 25 december 1640; vanwege de datum wordt het resultaat vaak aangeduid als de kerstmisstelling. Zoals doorgaans publiceerde Fermat echter geen bewijs; het eerste gekende werd na veel moeite door Leonhard Euler gegeven en maakt gebruik van oneindige afdaling, Fermats favoriete bewijsprincipe. Een later bewijs via kwadratische vormen werd gegeven door Joseph Lagrange en vereenvoudigd door Carl Friedrich Gauss. Ook Richard Dedekind gaf minstens twee bewijzen, via Gaussiaanse gehele getallen (zie ??, blz. ??).

Girard en Fermat merkten op dat  $5 = 1^2 + 2^2$ ,  $13 = 2^2 + 3^2$ ,  $17 = 1^2 + 4^2$  etc. Aan de andere kant kunnen de priemgetallen 3, 7, 11 en 19 niet worden geschreven als een som van twee kwadraten. De kerstmisstelling zegt nu dat een oneven priemgetal  $p$  (het geval 2 is triviaal) zo'n som van twee kwadraten is, en bovendien op juist één manier, als en slechts als  $p$  één meer is dan een viervoud. Fermat zelf schreef in zijn brief:

TOUT NOMBRE PREMIER, QUI SURPASSE DE L'UNITÉ UN MULTIPLE DU QUATERNAIRE EST UNE SEULE FOIS LA SOMME DE DEUX CARRÉS, ET UNE SEULE FOIS L'HYPOTÉNUSE D'UN TRIANGLE RECTANGLE.

$$\exists x, y \in \mathbb{N} : p = x^2 + y^2 \text{ voor } p \text{ priem en oneven} \quad \Leftrightarrow \quad p \equiv 1 \pmod{4}$$

Veertien jaar later maakte Fermat twee gerelateerde resultaten bekend, voor oneven priemgetallen  $p$ :

$$\begin{aligned} \exists x, y \in \mathbb{N} : p = x^2 + 2y^2 \text{ voor } p \text{ priem, } \neq 2 &\quad \Leftrightarrow \quad p \equiv 1 \pmod{8} \quad \vee \quad p \equiv 3 \pmod{8} \\ \exists x, y \in \mathbb{N} : p = x^2 + 3y^2 \text{ voor } p \text{ priem, } \neq 2 &\quad \Leftrightarrow \quad p \equiv 1 \pmod{3} \end{aligned}$$

Euler voegde er daar nog enkele aan toe als vermoeden:

$$\begin{aligned} \exists x, y \in \mathbb{N} : p = x^2 + 5y^2 \text{ voor } p \text{ priem, } \neq 2 &\quad \Leftrightarrow \quad p \equiv 1 \pmod{20} \quad \vee \quad p \equiv 9 \pmod{20} \\ \exists x, y \in \mathbb{N} : 2p = x^2 + 5y^2 \text{ voor } p \text{ priem, } \neq 2 &\quad \Leftrightarrow \quad p \equiv 3 \pmod{20} \quad \vee \quad p \equiv 7 \pmod{20} \end{aligned}$$

Zowel Fermats bewering als Eulers vermoeden werden bevestigd door Lagrange.

## 44 AKS-priemtest

In 2002 losten Manindra Agrawal en zijn studenten Neeraj Kayal en Nitin Saxena aan het Indian Institute of Technology van Kanpur, een al lang openstaand probleem op: een deterministisch algoritme dat in redelijke tijd kan bepalen of een getal priem is of niet (zie 322, blz. 313). Hun algoritme, gepubliceerd in een artikel *PRIMES is in P*, is het eerst bekende dat voldoet aan de volgende vier eigenschappen (i.t.t. tot eerdere priemtesten):

- **Algemeen:** de test kan voor *elk* getal het al dan niet priem zijn verifiëren. Vele relatief snelle priemtesten werken alleen voor priemgetallen van een bepaalde vorm, zoals de Lucas-Lehmer test voor Mersenne-priemgetallen (zie ??, blz. ??).
- **Polynomiaal:** de maximale looptijd is uit te drukken als een polynoom over het aantal cijfers van het te testen getal. Er bestaan ook andere priemtesten die meestal werken in polynomiale tijd (zelfs sneller), maar waarvan niet gekend is of ook de worst case scenario's polynomiaal lopen.
- **Deterministisch:** de test geeft 100% uitsluitel. De Miller-Rabintest bijvoorbeeld geeft eveneens in polynomiale tijd een antwoord, maar slechts een bepaalde zekerheid (99, . . . %).
- **Onvoorwaardelijk:** AKS steunt niet op onbewezen resultaten. De Millertest is deterministisch en polynomiaal, maar hangt af van de nog onbewezen Riemannhypothese (zie ??, blz. ??).

In het algoritme komt de Eulerfunctie  $\varphi(n)$  voor (zie 12, blz. 10). Het symbool  $o_r(n)$  staat voor de (multiplicatieve) orde van het  $n$  modulo  $r$ , de kleinste waarde  $k \neq 0$  waarvoor  $n^k \equiv 1 \pmod{r}$ . Tot slot houdt  $(x+a)^n \equiv x^n + a \pmod{x^r - 1, n}$  hier in dat  $(x-a)^n - (x^n - a) - q(x) \cdot (x^r - 1)$  een  $n$ -voud is, voor een zekere  $q(x)$ . Het uiteindelijke algoritme loopt als volgt:



**AKS( $n$ )****input** : integer  $n$ **output** : boolean, naargelang  $n$  priem is of niet**if**  $n = a^b$  met  $a, b \in \mathbb{N}, b > 1$  **then**| **return** false**else**| zoek minimale  $r$  zodat  $o_r(n) > {}^2\log n$ | **if**  $1 < \text{ggd } an < n$  voor een zekere  $a \leq r$  **then**| | **return** false| **else if**  $n \leq r$  **then**| | **return** true| **else**| | **for**  $a = 1$  **to**  $\lfloor \sqrt{\varphi(r)} \cdot {}^2\log n \rfloor$  **do**| | | **if**  $(x+a)^n \not\equiv x^n + a \pmod{x^r - 1, n}$  **then**| | | | **return** false| | **return** true

Alle stappen in het proces kunnen uitgevoerd worden in polynomiale tijd. De centrale stap is de modulaire congruentie, waarbij de Indiase onderzoekers bewezen dat er een voldoende kleine verzameling mogelijke  $a$ 's bestaat om primaliteit te kunnen garanderen; deze stap werkt in polynomiale tijd t.o.v. het aantal cijfers van  $n$ . In het oorspronkelijke artikel werd daarmee aangetoond dat het gehele algoritme  $\mathcal{O}(\sqrt{\log^{21} n})$  is, wat onder tusschen verbeterd werd tot  $\mathcal{O}(\log^6 n)$ . Afhankelijk van een, weliswaar zeer aannemelijk, vermoeden kan dit nog gereduceerd worden tot  $\mathcal{O}(\log^3 n)$ .

Agrawal, Kayal en Saxena's baanbrekende onderzoek werd in 2006 beloond met de Gödel- en Fulkersonprijs en betekende een belangrijke stap voorwaarts in het P-NP-probleem (zie 322, blz. 313).

## 45 Gemiddelden

Een gemiddelde wordt algemeen gedefinieerd over een reëel interval  $I \subset \mathbb{R}$  als een functie  $\mathcal{M} : I^n \rightarrow I$ , die voldoet aan de volgende eigenschappen voor al zijn invoerwaarden:

- **Behoud van waarde:**  $\mathcal{M}(a, a, \dots, a) = a$ .
- **Homogeniteit:**  $\mathcal{M}(ba_1, ba_2, \dots, ba_n) = b \cdot \mathcal{M}(a_1, a_2, \dots, a_n)$ .
- **Permutatie-invariantie:**  $\mathcal{M}(a_1, a_2, \dots, a_n) = \mathcal{M}(a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(n)})$  voor elke permutatie  $\sigma$ .
- **Middeling:**  $\min(a_1, a_2, \dots, a_n) \leq \mathcal{M}(a_1, a_2, \dots, a_n) \leq \max(a_1, a_2, \dots, a_n)$ .

Het bekendste voorbeeld van een gemiddelde is het rekenkundig gemiddelde  $\mathcal{A}$ , als volgt gedefinieerd:

$$\mathcal{A} : I^n \rightarrow I : (a_1, a_2, \dots, a_n) \mapsto \frac{a_1 + a_2 + \dots + a_n}{n}$$

De pythagoreeërs en latere Griekse wiskundigen bestudeerden behalve deze klassieker ook nog enkele andere gemiddelden, zoals het meetkundig gemiddelde  $\mathcal{G}$  (over  $\mathbb{R}^+$ ):

$$\mathcal{G} : I^n \rightarrow I : (a_1, a_2, \dots, a_n) \mapsto \sqrt[n]{a_1 \cdot a_2 \cdot \dots \cdot a_n}$$

Daarnaast bestaat er nog het harmonisch gemiddelde  $\mathcal{H}$  over  $\mathbb{R}_0^+$ :

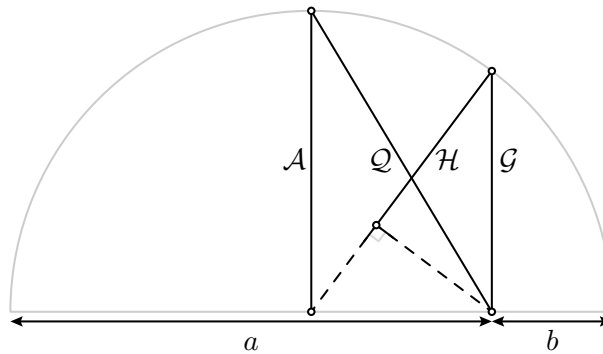
$$\mathcal{H} : I^n \rightarrow I : (a_1, a_2, \dots, a_n) \mapsto \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n}}$$

Een volgende voorbeeld is het kwadratisch gemiddelde  $\mathcal{Q}$ .

$$\mathcal{Q} : I^n \rightarrow I : (a_1, a_2, \dots, a_n) \mapsto \sqrt{\frac{a_1^2 + a_2^2 + \dots + a_n^2}{n}}$$

Merk ten slotte op dat het minimum en maximum van een  $n$ -tupel zelf ook voldoen aan de vier eisen en dus eveneens voorbeelden van gemiddelden zijn. Er bestaan oneindig veel gemiddelden, nog eentje is het rekenkundig-meetkundig gemiddelde (zie 104, blz. 77).

Pythagoras en zijn volgelingen waren niet zomaar geïnteresseerd in de eerste drie gemiddelden (die nu bekendstaan als de Pythagorische gemiddelden): Pythagoras was verzot op verhoudingen en muziek, en deze gemiddelden bleken daarin een belangrijke rol te spelen. Er is trouwens ook een opmerkelijke meetkundige interpretatie van deze gemiddelden, toegepast op een koppel  $(a, b)$ :



Er bestaat een uiterst praktisch verband tussen de hierboven beschreven gemiddelden, dat voor alle invoerwaarden of  $n$ -waarden geldig is en zijn nut bewijst in vele ongelijkheden (geliefd op olympiades).

$$\min \leq \mathcal{H} \leq \mathcal{G} \leq \mathcal{A} \leq \mathcal{Q} \leq \max$$

Gelijkheid treedt slechts op als alle invoerwaarden  $a_i$  gelijk zijn. Een mogelijkheid om de ongelijkheden te bewijzen maakt gebruik van Pythagorische drietallen  $(x, y, z)$ , waarvoor  $x^2 + y^2 = z^2$  en dus  $x, y < z$ .

$$\left( \frac{b-a}{b+a} \cdot \sqrt{ab}, \mathcal{H}(a, b), \mathcal{G}(a, b) \right)$$

Hieruit volgt dus inderdaad dat  $\mathcal{H} < \mathcal{G}$ . Gebruik voor  $\mathcal{G} < \mathcal{A}$  de volgende:

$$\left( \frac{b-a}{2}, \mathcal{G}(a, b), \mathcal{A}(a, b) \right)$$

En voor de laatste ongelijkheid:

$$\left( \frac{b-a}{2}, \mathcal{A}(a, b), \mathcal{Q}(a, b) \right)$$

Bovendien ligt het rekenkundig-meetkundig gemiddelde  $\mathcal{AG}$  tussen  $\mathcal{A}$  en  $\mathcal{G}$ .

De vier gemiddelden  $\mathcal{H}$ ,  $\mathcal{G}$ ,  $\mathcal{A}$  en  $\mathcal{Q}$  zijn speciale gevallen van een veralgemeend gemiddelde, het machtsgemiddelde, als volgt gedefinieerd voor een reële macht  $p \neq 0$ :

$$\mathcal{M}_p : I^n \rightarrow I : (a_1, a_2, \dots, a_n) \mapsto \left( \frac{a_1^p + a_2^p + \dots + a_n^p}{n} \right)^{\frac{1}{p}}$$

Voor welgekozen  $p$ -waarden verkrijgen we de bekende gemiddelden:  $\mathcal{M}_{-1} = \mathcal{H}$ , terwijl  $\mathcal{M}_1 = \mathcal{A}$  en  $\mathcal{M}_2 = \mathcal{Q}$ . Voor  $p \rightarrow 0$  convergeert  $\mathcal{M}_p$  naar  $\mathcal{G}$ , voor  $p \rightarrow -\infty$  naar het minimum en voor  $p \rightarrow +\infty$  naar het maximum.

## 46 Moessners magie

Alfred Moessner ontdekte deze verrassende manifestatie van enkele bekende getallenrijen. Noteer achtereenvolgens de natuurlijke getallen, schrap elk even getal en bereken op de rij eronder de cumulatieve som van de resterende getallen. Het resultaat zijn de volkomen kwadraten:

1	<del>2</del>	3	<del>4</del>	5	<del>6</del>	7	<del>8</del>	9	<del>10</del>	11	<del>12</del>	13	<del>14</del>	15	<del>16</del>
(1)		(4)		(9)		(16)		(25)		(36)		(49)		(64)	

Hetzelfde principe toepassen met elk derde getal en per blok het laatste schrappen, geeft de derdemachten:

1	2	<del>3</del>	4	5	<del>6</del>	7	8	<del>9</del>	10	11	<del>12</del>	13	14	<del>15</del>
1	<del>3</del>		7	<del>12</del>		19	<del>27</del>		37	<del>48</del>		61	<del>75</del>	
(1)			(8)			(27)			(64)			(125)		

Veelvouden van  $n$  in het begin wegstrepen leidt algemeen tot de  $n^{\text{de}}$ -machten aan het einde van de blokken. Bijvoorbeeld voor de vierdemachten:

1	2	3	<del>4</del>	5	6	7	<del>8</del>	9	10	11	<del>12</del>	13	14	15	<del>16</del>
1	3	<del>6</del>		11	17	<del>24</del>		33	43	<del>54</del>		67	81	<del>96</del>	
1	<del>4</del>			15	<del>32</del>			65	<del>108</del>			175	<del>256</del>		
(1)				(16)				(81)				(256)			

Variaties in de begingetallen leveren andere interessante resultaten op. Zo vind je de faculteiten wanneer je eerst de driehoeksgetallen (zie ??, blz. ??) schrapt:

(1)	2	<del>3</del>	4	5	<del>6</del>	7	8	9	<del>10</del>	11	12	13	14	<del>15</del>
	(2)		6	<del>11</del>		18	26	<del>35</del>		46	58	71	<del>85</del>	
			(6)			24	<del>50</del>			96	154	<del>255</del>		
						(24)				120	<del>274</del>			
										(120)				

Algemeen worden begingetallen van de vorm hieronder links uiteindelijk omgezet in de vorm rechts:

$$1a, 2a + 1b, 3a + 2b + 1c, 4a + 3b + 2c + 1d \dots \quad \mapsto \quad 1^a, 2^a \cdot 1^b, 3^a \cdot 2^b \cdot 1^c, 4^a \cdot 3^b \cdot 2^c \cdot 1^d \dots$$

## 47 Fermatpriemgetallen

Pierre de Fermat was de eerste die getallen van de vorm  $2^{2^n} + 1$  onderzocht. Hij vermoedde, maar gaf toe geen bewijs te kennen, dat al deze naar hem vernoemde Fermatgetallen  $F_n$  priem zijn. Leonhard Euler weerlegde dit vermoeden door aan te tonen dat  $F_5 = 4294967297 = 641 \cdot 6700417$ ; in feite zijn de eerste vijf Fermatgetallen de enige tot nog toe bekend die *wel* priem zijn.

3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, 340282366920938463463374607431768211457 ...

Fermatpriemgetallen staan in OEIS A019434, de algemene Fermatgetallen in OEIS A000215. Ze voldoen aan de

volgende recursiebetrekkingen:

$$F_0 = 3, \quad F_n = (F_{n-1} - 1)^2 + 1 = F_{n-1} + 2^{2^{n-1}} \cdot \prod_{i=0}^{n-2} F_i = F_{n-1}^2 - 2(F_{n-2} - 1)^2 = \prod_{i=0}^{n-1} F_i + 2$$

Uit de laatste relatie kan men de stelling van Goldbach afleiden, namelijk dat alle Fermatgetallen onderling ondeelbaar zijn. Hieruit volgt meteen ook dat er oneindig veel priemgetallen zijn.

De getallen van Fermat bezitten vele curieuze eigenschappen. Zo geldt dat de som van de omgekeerden van alle priemdelers van Fermatgetallen convergeert, wat toch bizar is aangezien de som over *alle* priemgetallen divergeert. Édouard Lucas bewees dat elk zo'n priemdelers van  $F_n$  van de vorm  $k \cdot 2^{n+2} + 1$  is voor  $n > 1$ .

Een eenvoudige test om vast te stellen of  $F_n$  priem is, is de priemtest van Pépin. Ondanks dat de test polynomiaal werkt, groeien Fermatgetallen zo snel (dubbelexponentieel) dat slechts een handjevol ervan in redelijke tijd getest kon worden. Tot nog toe werden maar zeven Fermatgetallen onderworpen aan de Pépintest:  $F_7$  en  $F_8$  begin 20<sup>ste</sup> eeuw,  $F_{13}$  en  $F_{14}$  rond 1960,  $F_{20}$  en  $F_{22}$  rond 1990 en  $F_{24}$  in 1999. Er wordt verwacht dat het nog decennia kan duren vooraleer nieuwe testen kunnen worden uitgevoerd; de kleinste zonder gekende priemfactoren is  $F_{33}$ , die meer dan 2,5 miljard cijfers lang is. Hoe dan ook, Pépins test garandeert de primaliteit van  $F_n$ , als en slechts als:

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

## 48 Tweelingpriemgetallen

Een koppel tweelingpriemgetallen bestaat uit twee priemgetallen die slechts twee verschillen, zoals (29, 31). Ondanks deze eenvoudige definitie is nog maar weinig erover bekend: het vermoeden dat er oneindig veel tweelingpriemgetallen zijn, wordt als een van de grotere open problemen uit de getaltheorie beschouwd.

Een analogon op de stelling van Wilson (zie 5, blz. 7) stelt dat het koppel  $(m, m + 2)$  uit twee priemgetallen bestaat als en slechts als de volgende congruentie voldaan is:

$$4(m - 1)! + 4 \equiv -m \pmod{m(m + 2)}$$

Een historisch belangrijk resultaat omtrent tweelingpriemgetallen is de stelling van Brun uit 1919, vernoemd naar Viggo Brun die er een speciale zeef voor ontwikkelde en zo de ontwikkeling van de moderne zeeftheorie in gang hielp zetten. Bruns stelling stelt dat de som van de omgekeerden van tweelingpriemgetallen convergeert naar een constante  $B$ , ook al zou hun aantal divergeren. De waarde van deze  $B$  wordt geschat op  $1,9021605823$  plusminus  $8 \times 10^{-10}$ .

$$B = \left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \left(\frac{1}{11} + \frac{1}{13}\right) + \left(\frac{1}{17} + \frac{1}{19}\right) + \left(\frac{1}{29} + \frac{1}{31}\right) + \left(\frac{1}{41} + \frac{1}{43}\right) + \left(\frac{1}{59} + \frac{1}{61}\right) + \dots$$

In december 2011 kondigde PrimeGrid aan het tot nog toe grootst bekende koppel tweelingpriemen gevonden te hebben:  $3756801695685 \cdot 2^{666669} \pm 1$ , beiden getallen van 200700 cijfers lang.

In OEIS A007534 staan de even getallen die niet te schrijven zijn als een som van twee tweelingpriemgetallen. De volledige lijst bekende getallen staat hieronder; er zijn geen andere waarden onder de  $10^9$  bekend en men vermoedt dat deze lijst compleet is, wat het tweelingpriemgetalvermoeden zou impliceren.

2, 4, 94, 96, 98, 400, 402, 404, 514, 516, 518, 784, 786, 788, 904, 906, 908, 1114, 1116, 1118, 1144, 1146, 1148, 1264, 1266, 1268, 1354, 1356, 1358, 3244, 3246, 3248, 4204, 4206, 4208

Er bestaan een aantal generalisaties van het tweelingpriemvermoeden. Een vermoeden van Alphonse de Polignac uit 1849 stelt dat er oneindig veel koppels opeenvolgende priemgetallen zijn waartussen het verschil  $k$  is, voor elk even natuurlijk getal  $k$ . Dit vermoeden is bewezen noch ontkracht, voor geen enkele  $k$ -waarde.

Een vermoeden van Godfrey Hardy en John Littlewood vormt een analogon voor de priemgetalstelling (zie 1, blz. 5). Definieer  $\pi_2(x)$  als het aantal priemgetallen  $p$  ten hoogste  $x$  zodat ook  $p + 2$  priem is, en de tweelingpriemconstante  $C_2$  als het volgende product over priemgetallen  $p \geq 3$ :

$$C_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \approx 0,660161815846869573927812110014 \dots$$

Dan zou volgens het vermoeden:

$$\pi_2(n) \sim 2C_2 \frac{n}{(\ln n)^2}$$

## 49 Vermoeden van Fortune

Reo Fortune was een Nieuw-Zeelandse sociaal antropoloog, die berucht was voor zijn labiel gedrag, op het randje van psychotisch. Zo stelde hij ooit voor om een academisch dispuut met Thomas McIlwraith te beslechten via een duel met een wapen naar keuze uit de collecties van het Royal Ontario Museum.

Analoog als faculteiten worden primorials\*  $n\#$  gedefinieerd als het product van de eerste priemgetallen ten hoogste  $n$ , zo is bijv.  $11\# = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ . Priemgetallen van de vorm  $p_n\# \pm 1$  heten primoriaalpriemgetallen en spelen een cruciale rol in Euclides' klassieke bewijs van de onbegrensde der priemgetallen. Een mooie asymptotische eigenschap:

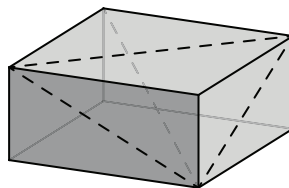
$$\lim_{n \rightarrow \infty} \sqrt[p_n]{p_n\#} = e$$

Fortune opperde dat de afstand tot het eerste priemgetal na een primoriaal, ofwel 1 is ofwel zelf een priemgetal. Ietsje sterker vermoedde hij dat  $q - p_n\#$ , waarbij  $q$  het eerste priemgetal is na  $p_n\# + 1$ , zelf priem is. Tot nog toe zijn er geen tegenvoorbeelden bekend en wordt het vermoeden algemeen aanvaard, maar een bewijs werd nog niet gevonden. De vermoedde priemgetallen in kwestie heten *fortunate primes* en staan in OEIS A005235.

Cyril Banderier vermoedde een gelijkaardig resultaat maar dan met betrekking tot de vorige priemgetallen in plaats van de volgende, en noemde zijn relevante getallen *unfortunate numbers*.

## 50 Eulerblok

Een Eulerblok is een balk waarvan alle ribben en diagonalen in een zijvlak geheeltallige lengte hebben. Het kleinste voorbeeld werd al in 1719 gevonden door Paul Halcke en heeft ribben met lengte 44, 117 en 240. De zijvlaksdagonalen worden dan 125, 244 en 267, en al deze afmetingen zijn natuurlijke getallen.



In 1740 publiceerde Nicholas Saunderson een algemene parametrische oplossing om Eulerblokken te genereren, hoewel niet alle mogelijke blokken. Leonhard Euler zelf vond in 1770 en 1772 nog minstens twee parametrisaties.

\*De benaming wordt toegeschreven aan Harvey Dubner, die *primorial* linkte met *prime* zoals *factorial* met *factor*.

De formule van Saunderson vertrekt van een Pythagorasdrietal  $(u, v, w)$  (zie 308, blz. 299) en geeft deze waarden als lengtes van de ribben  $a$ ,  $b$  en  $c$ :

$$\begin{cases} a = u(4v^2 - w^2) \\ b = v(4u^2 - w^2) \\ c = 4uvw \end{cases}$$

Door hierin nog eens de formule van Euclides (die Pythagorasdrietallen genereert) in te vullen, ontstaat deze parametrisatie van een oppervlak waarop de coëfficiënten van punten met geheeltallige parameterwaarden corresponderen met Eulerblokken.

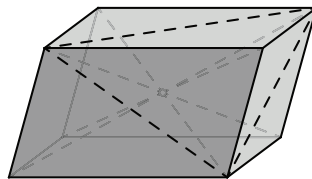
$$r(s, t) = (6ts^5 - 20t^3s^3 + 6t^5s, s^6 + 15t^2s^4 - 15t^4s^2 + t^6, 8s^5t - 8st^5)$$

Een andere manier om de Eulerblokken te interpreteren, is als oplossingen van een stelsel diophantische vergelijkingen, die volgen uit de stelling van Pythagoras:

$$\begin{cases} a^2 + b^2 = d^2 \\ b^2 + c^2 = e^2 \\ a^2 + c^2 = f^2 \end{cases}$$

Wanneer daarenboven de ruimtediagonaal een gehele lengte heeft, spreekt men van een perfect Eulerblok. Dit brengt een extra vergelijking in het stelsel hierboven mee, namelijk  $a^2 + b^2 + c^2 = g^2$ . Tussen de vele gekende Eulerblokken zijn alleen nog geen perfecte gevonden, noch is bewezen dat er geen bestaan. Een resultaat van Henry Pocklington impliceert wel dat de Saundersonparametrisatie geen perfecte Eulerblokken kan opleveren. Als zo'n perfect blok bestaat, moet zijn kortste ribbe langer zijn dan  $10^{10}$ .

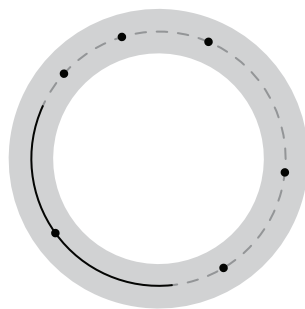
Door de eisen te verzwakken en parallellepipedum te beschouwen in plaats van balken, bestaan er wel perfecte oplossingen. Jorge Sawyer en Clifford Reiter ontdekten in 2009 een perfect parallellepipedum, wiens ribben lengte 271, 106 en 103 hebben, korte zijvlaksdagonalen 101, 266 en 255, lange zijvlaksdagonalen 183, 312 en 323 en tot slot ruimtediagonalen 374, 300, 278 en 272. Ze vonden er nog tientallen meer via brute-force algoritmen, waarbij er zelfs tussenzaten met enkele rechthoekige zijvlakken.



## 51 Vermoeden van de eenzame loper

Jorg Wills introduceerde in 1967 dit elegante vermoeden in de studie van diophantische benaderingen, het deelgebied van de getaltheorie dat zich bezighoudt met de rationale benaderingen van reële getallen. Thomas Cusick herinterpreteerde het probleem in 1974 als een geometrisch zichtobstructieprobleem. Zijn plastische naam dankt het vermoeden aan Luis Goddyn, die het in 1998 als volgt vertolkte.

Beschouw  $k$  lopers op een cirkelvormige piste. Aan de start vertrekken de lopers vanuit dezelfde positie en met constante maar onderling verschillende snelheden. In de veronderstelling dat de cirkel eenheidsomtrek heeft en afstanden langs de piste gemeten worden, en noem een loper *eenzaam* als diens afstand tot elke andere loper minstens  $\frac{1}{k}$  is. Het vermoeden van de eenzame loper stelt dan dat elke loper ooit eenzaam is.



Een handige herformulering van het probleem wijst de lopers gehele snelheden toe, niet allen deelbaar door hetzelfde priemgetal, en de loper waarvan de eenzaamheid te beschouwen is, snelheid 0. Noteer  $\|x\|$  voor de afstand van  $x$  tot het dichtstbijzijnde gehele getal. Voor elke verzameling  $D$  bestaande uit  $k - 1$  gehele getallen zonder gemeenschappelijke factoren zou dan gelden:

$$\exists t \in \mathbb{R} : \forall d \in D : \|d \cdot t\| \geq \frac{1}{k}$$

De gevallen  $k \leq 3$  bleken eenvoudig. Ulrich Betke, Jorg Wills en onafhankelijk Thomas Cusick bewezen het geval  $k = 4$ . Met de hulp van Carl Pomerance en computercontroles verifieerde Cusick het vermoeden ook voor  $k = 5$ . Pas in 2001 werd  $k = 6$  bewezen, en in 2008  $k = 7$ . Voor grotere waarden echter staat het probleem nog open. Is lopen in groep een socialere aangelegenheid?

## 52 Stelling van Hurwitz

Deze stelling uit the theorie van diophantische benaderingen, vernoemd naar Adolf Hurwitz, stelt dat voor elk irrationaal getal  $\xi$  er oneindig veel rationale getallen  $m$  en  $n$  bestaan zodanig dat de volgende ongelijkheid geldt:

$$\left| \xi - \frac{m}{n} \right| < \frac{1}{\sqrt{5} \cdot n^2}$$

De irrationaliteit van  $\xi$  is cruciaal. Daarenboven is de waarde  $\sqrt{5}$  de best haalbare: vervang deze constante door een grotere waarde en kies  $\xi = \frac{1}{2}(1 + \sqrt{5})$ , de gulden verhouding, dan bestaan er slechts eindig veel rationale  $m$  en  $n$  meer die de ongelijkheid doen opgaan.

## 53 Rekenkundige afgeleide

Edward Barbeau formaliseerde als eerste een methode om getallen “af te leiden”. Niet in de analytische betekenis (een constante afgeleid is uiteraard gewoon nul), maar een getaltheoretische functie die analoge eigenschappen vertoont als de analytische afgeleide. De aritmetische afgeleide is gebaseerd op ontbinding in priemfactoren en wordt vastgelegd met deze definitie (bemerkt de Leibnizregel):

$$\begin{cases} p' = 1 & \text{voor priemgetallen } p \\ (ab)' = a'b + ab' & \text{voor alle natuurlijke getallen } a \text{ en } b \end{cases}$$

Aldus blijkt deze functie goed gedefinieerd en impliceert ze direct dat  $0' = 1' = 0$ . Ook enkele vertrouwde eigenschappen blijven bewaard, zoals  $(n^k)' = k \cdot n^{k-1} \cdot n'$ . Een expliciete formule om getallen rechtstreeks af te leiden, zonder de recursieve definitie, verloopt als volgt (links staat de ontbinding in priemfactoren).

$$n = \prod_{i=1}^k p_i^{n_i} \quad \Rightarrow \quad n' = n \cdot \sum_{i=1}^k \frac{n_i}{p_i}$$

Als voorbeeld wordt  $120'$  als volgt uitgerekend:

$$120' = (2^3 \cdot 3 \cdot 5)' = 120 \cdot \left( \frac{3}{2} + \frac{1}{3} + \frac{1}{5} \right) = 244$$

In OEIS A003415 staan de waarden van de eerste natuurlijke afgeleiden.

0, 0, 1, 1, 4, 1, 5, 1, 12, 6, 7, 1, 16, 1, 9, 8, 32, 1, 21, 1, 24, 10, 13, 1, 44, 10, 15, 27, 32, 1, 31, 1, 80, 14, 19, 12, 60 . . .

Merk op dat lineariteit niet langer geldig is, want dat zou betekenen dat elke natuurlijke  $n$  als afgeleide nul zou hebben (immers,  $n' = (1 + 1 + \dots + 1)' \neq 1' + 1' + \dots + 1' = 0$ ). De volgende afschattingen gelden voor elke niet-prieme  $n$ , als product van  $k$  priemfactoren, met gelijkheid voor  $n = 2^k$ :

$$k \sqrt[n]{n^{k-1}} \leq n' \leq \frac{n \cdot {}^2\log n}{2}$$

Met behulp van aritmetische afgeleide kunnen we diophantische differentiaalvergelijkingen opstellen en oplossen, zoals  $n' = n$ , die enkel  $p^p$  als oplossing heeft, voor priemgetallen  $p$ . Soortgelijke differentiaalvergelijkingen kunnen gelinkt worden aan beroemde open problemen. Het vermoeden van Goldbach (zie 28, blz. 19) bijvoorbeeld garandeert dat de vergelijking  $n' = 2b$  voor elke natuurlijke  $b$  oplosbaar is: stel  $2b = p + q$  met  $p$  en  $q$  priem, dan is  $pq$  een oplossing. Het tweelingpriemvermoeden (zie 48, blz. 37) verzekert dat  $n'' = 1$  oneindig veel oplossingen heeft:  $2p$  voldoet als zowel  $p$  als  $p + 2$  priem zijn.

De rekenkundige afgeleide kan worden veralgemeend tot over gans  $\mathbb{Z}$  door middel van de voor de hand liggende regel  $(-n)' = -n'$ . De expliciete formule van hierboven blijft zelfs bruikbaar over  $\mathbb{Q}$ , waarbij sommige  $n_i$ 's negatief kunnen zijn. In beide uitbreidingen blijft de Leibnizregel geldig, in de tweede zelfs de quotiëntregel zoals gekend uit de analyse. Misschien onverwacht treden er over  $\mathbb{Q}$  plots niet-triviale oplossingen op voor  $n' = 0$ , zoals  $n = \frac{4}{27}$ , en ook de andere differentiaalvergelijkingen worden veel lastiger te begrijpen.

## 54 Probleem van Brocard

Dit probleem, voorgelegd door Henry Brocard in enkele artikels in 1876 en 1885, vraagt gehele getallen waarvoor de waarde  $n! + 1$  een volkomen kwadraat is. In 1913 bestudeerde Srinivasa Ramanujan dezelfde diophantische vergelijking onafhankelijk van Brocard.

$$n! + 1 = m^2$$

Getallenparen  $(n, m)$  die voldoen aan de vergelijking van Brocard heten Browngetallen. Er zijn slechts drie oplossingen bekend, namelijk  $(4, 5)$ ,  $(5, 11)$  en  $(7, 71)$ , en Paul Erdős vermoedde dat er geen verdere oplossingen bestaan. Bruce Berndt en William Galway voerden berekeningen uit voor  $n$  tot  $10^9$  zonder nieuwe Browngetallen te vinden. Marius Overholt toonde in 1993 aan dat het aantal oplossingen sowieso eindig is, onder aanname van het *abc*-vermoeden (zie 37, blz. 25). Andrzej Dabrowski veralgemeende dit resultaat voor diophantische vergelijkingen van de vorm  $n! + k = m^2$  met gehele  $k$ , en Florian Luca bewees nog sterker dat  $n! = P(m)$  slechts eindig veel oplossingen heeft voor een vooropgegeven veelterm  $P$  met graad minstens twee en gehele coëfficiënten.

## 55 Constante van Niven

Definieer de functies  $h(m)$  en  $H(m)$  voor een natuurlijk getal  $n$  ontbonden in priemfactoren  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  als het minimum respectievelijk maximum van de exponenten  $\alpha_1, \alpha_2, \dots, \alpha_k$ . Stel voor de volledigheid ook  $h(1) = 1$  en  $H(1) = 1$ .

Ivan Niven bewees dat de gemiddelde functiewaarde  $h(m)$  van de eerste  $n$  natuurlijke getallen gaat naar 1,



wat inhoudt dat getallen met uitsluitend hoge priem machten als factoren zeldzaam zijn. Niven toonde ook de volgende limietverhouding aan:

$$\lim_{n \rightarrow \infty} \frac{1}{\sqrt{n}} \cdot \left( \sum_{m=1}^n h(m) - n \right) = \frac{\zeta\left(\frac{3}{2}\right)}{\zeta(3)}$$

De feitelijke constante van Niven is echter de gemiddelde grootst optredende exponent in de priemfactorontbinding van een natuurlijk getal, i.e. de volgende limiet, waarvan de waarde in (OEIS A033150) staat:

$$\lim_{n \rightarrow \infty} \frac{1}{n} \cdot \sum_{i=1}^n H(i) \approx 1,705211140105367764288 \dots$$

Dat deze limiet überhaupt convergeert naar een constante  $N$ , mag al verrassend heten, maar Niven leidde ook een gesloten uitdrukking ervoor af gebruik makende van Riemanns zetafunctie (zie ??, blz. ??).

$$N = 1 + \sum_{k=2}^{\infty} \left( 1 - \frac{1}{\zeta(k)} \right)$$

## 56 Constante van Khinchin

Aleksandr Yakovlevich Khinchin bewees dat voor bijna alle reële getallen  $x$ , de coëfficiënten optredend in de regulier kettingbreuk (zie 22, blz.14) een eindig meetkundig gemiddelde hebben, dat onafhankelijk is van  $x$ ! Deze waarde heet de constante van Khinchin. Dus, schrijf  $x$  als een reguliere kettingbreuk:

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots}}}}$$

Dan geldt bijna altijd het volgende resultaat.

$$\lim_{n \rightarrow \infty} \sqrt[n]{\prod_{i=1}^n a_i} = K_0 \approx 2,6854520010 \dots$$

$K_0$  in deze formule is Khinchins constante (OEIS A002210) en kan ook exact gegeven worden als volgt:

$$K_0 = \prod_{r=1}^{\infty} \left( 1 + \frac{1}{r(r+2)} \right)^{2 \log r}$$

Voor bijna alle reële getallen gaat de stelling van Khinchin op, in de zin dat de verzameling tegenvoorbeelden maat nul heeft in  $\mathbb{R}$ . Opmerkelijk genoeg is er toch geen enkel getal bekend dat eraan voldoet; rationale getallen hebben een eindige kettingbreuk en voldoen dus zeker niet, oplossingen van kwadratische vergelijkingen (zoals de gulden snede  $\varphi$ ) evenmin en zelfs de constante van Euler  $e$  (zie 95, blz. 71) niet! Mogelijke kandidaten zijn  $\pi$ , de constante van Euler-Mascheroni  $\gamma$  (zie ??, blz. ??) of de constante van Khinchin zelf, gestaafd op numeriek bewijsmateriaal. Van geen enkel getal is de limiet echter al rigoreus bewezen. Het is ook nog ongeweten of  $K_0$  rationaal, algebraïsch of transcendent is.

## 57 Lifting the exponent

Het *lifting the exponent*-lemma is een gevierde olympiadetechniek om exponentiële diophantische vergelijkingen op te lossen. Definieer een soort “selectief logaritme”  $\nu_p(x)$  dat de grootste exponent  $n$  is waarvoor  $p^n$  nog een deler is van  $x$  (met  $p$  een priemgetal). Deze functie gedraagt zich als een logaritme, maar beschouwt slechts één priemfactor. Ze voldoet aan enkele eenvoudig te controleren eigenschappen:

- $\nu_p(1) = 0$
- $\nu_p(x^n) = n \cdot \nu_p(x)$
- $\nu_p(x \cdot y) = \nu_p(x) + \nu_p(y)$

Voor gehele getallen  $x$  en  $y$ , een natuurlijk getal  $n$ , en een oneven priemgetal  $p$  waarvoor  $p \mid x - y$  maar  $p \nmid x$  en  $p \nmid y$ , geeft lifting the exponent de volgende vereenvoudiging:

$$\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n)$$

Wanneer  $n$  oneven is, gaat bovenstaande vergelijking ook op voor sommen i.p.v. verschillen. De veronderstelling dat  $p$  verschilt van 2 is van belang; er bestaat een aparte versie van het lemma voor dit geval. Lifting the exponent zoals hierboven blijft gelden op voorwaarde dat  $4 \mid x - y$ :

$$\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(n)$$

Op voorwaarde dat  $2 \mid x - y$  stelt een andere variant voor even  $n$ :

$$\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(x + y) + \nu_2(n) - 1$$

## 58 Harmonische getallen van Ore

In 1948 definieerde Øystein Ore zijn harmonische getallen als die natuurlijke getallen wiens delers een geheel getal als harmonisch gemiddelde (zie 45, blz. 34) hebben. De eerste harmonische getallen zijn:

1, 6, 28, 140, 270, 496, 672, 1638, 2970, 6200, 8128, 8190, 18600, 18620, 27846, 30240, 32760 . . . (OEIS A001599)

Het valt eenvoudig uit te rekenen dat het harmonisch gemiddelde van de delers van  $n$  gegeven wordt door  $\frac{n\tau(n)}{\sigma(n)}$ , met  $\tau(n)$  het aantal delers en  $\sigma(n)$  de som van de delers van  $n$ . Wanneer deze uitdrukking een geheel getal is, is  $n$  een harmonisch getal van Ore.

Ore toonde aan dat elk perfect getal (zie 26, blz. 18) voldoet aan deze definitie. Men vermoedt dat er geen oneven perfecte getallen bestaan; Ore vermoedde sterker zelfs dat geen enkele van zijn harmonisch getallen (behalve 1) oneven is! W. Mills illustreerde dat een potentieel tegenvoorbeeld een priemfactor groter dan  $10^7$  zou moeten hebben, en Graeme Cohen en Ronald Sorli verifieerden dat er geen niet-triviale oneven harmonische getallen kleiner dan  $10^{24}$  bestaan.

## 59 Stelling van Lucas

De stelling van Édouard Lucas geeft een uitdrukking voor de rest bij deling van de binomiaalcoëfficiënt  $\binom{m}{n}$  door een priemgetal  $p$ , in termen van de cijfers van  $m$  en  $n$  in grondtal  $p$  genoteerd. De stelling verscheen in 1878. Ontbind  $m$  en  $n$  als volgt:

- $m = m_k p^k + m_{k-1} p^{k-1} + \dots + m_1 p + m_0$
- $n = n_k p^k + n_{k-1} p^{k-1} + \dots + n_1 p + n_0$

Onder de conventie dat  $\binom{m}{n} = 0$  als  $m < n$ , geldt dan de volgende modulaire congruentie:

$$\binom{m}{n} \equiv \prod_{i=0}^k \binom{m_i}{n_i} \pmod{p}$$

Beschouw als voorbeeld de waarden  $m = 588$ ,  $n = 277$  en  $p = 5$ . In grondtal  $p$  is  $m = (4323)_5$  en  $n = (2102)_5$ . Hier geeft de congruentie van Lucas dus dat  $\binom{588}{277} \equiv \binom{4}{2} \cdot \binom{3}{1} \cdot \binom{2}{0} \cdot \binom{3}{2} \equiv 4 \pmod{5}$ .

Een gevolg van Lucas' stelling is dat een binomiaalcoëfficiënt  $\binom{m}{n}$  deelbaar is door een priemgetal  $p$  als en slechts als minstens één van de cijfers van  $n$  in grondtal  $p$  groter is dan het corresponderende cijfer van  $m$ .

Voor een priem  $p$  en een natuurlijk getal  $n = (n_k \dots n_1 n_0)_p$  bestaan er juist  $(n_k + 1) \cdot \dots \cdot (n_1 + 1) \cdot (n_0 + 1)$  waarden  $m$  waarvoor  $\binom{n}{m}$  géén veelvoud is van  $p$ . Dit is juist het aantal niet- $p$ -vouden in de  $n^{\text{de}}$  rij van Pascals driehoek (zie 246, blz. 204).

Een gerelateerd resultaat is de stelling van Ernst Kummer, bewezen in 1852: voor natuurlijke getallen  $n \geq m$  en een priemgetal  $p$  is de hoogste macht van  $p$  die de binomiaalcoëfficiënt  $\binom{n}{m}$  deelt precies gelijk aan het aantal benodigde *carries* bij het al cijferend optellen van  $m$  en  $n - m$  in grondtal  $p$ .

## 60 Machtige getallen

Een geheel getal  $m$  heet machtig of *powerful* wanneer alle priemgetallen in zijn priemfactorontbinding minstens gekwadrateerd voorkomen. Voor elk priemgetal  $p$  zodat  $p \mid m$  moet dus ook gelden dat  $p^2 \mid m$ . Veralgemeend naar  $k$ -machtige getallen heeft elke priemfactor minstens exponent  $k$ . De rij voor  $k = 2$  begint als volgt:

1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 72, 81, 100, 108, 121, 125, 128, 144, 169, 196, 200, 216, 225 . . . (OEIS A001694)

Het valt eenvoudig in te zien dat 2-machtige getallen precies die getallen zijn van de vorm  $a^2 \cdot b^3$ , met  $a, b \in \mathbb{Z}$ . Er bestaan duidelijk oneindig veel zulke getallen, maar ook oneindig veel paren opeenvolgende, de eerste zijnde (8, 9), (288, 289), (675, 676), (9800, 9801) . . . Paul Erdős, Richard Mollin en Gary Walsh vermoedden dat er geen *drie* opeenvolgende machtige getallen bestaan, wat tot op heden nog een openstaand probleem vormt.

Het aantal machtige getallen  $k(x)$  onder  $x$  kan als volgt afgeschat worden:

$$\frac{\zeta(\frac{3}{2})}{\zeta(3)} \sqrt{x} - 3\sqrt[3]{x} \leq k(x) \leq \frac{\zeta(\frac{3}{2})}{\zeta(3)} \sqrt{x}$$

De Riemann zètafunctie (zie ??, blz. ??) duikt ook op in de som van inversen van deze getallen.

$$\sum_{n \text{ machtig}} \frac{1}{n} = \frac{\zeta(2) \cdot \zeta(3)}{\zeta(6)}$$

Soms worden machtige getallen die geen perfecte macht zijn, vernoemd naar de Griekse held Achilles (eveneens machtig maar niet perfect) en als Achillesgetallen aangeduid. Een getal  $n$  is dus Achilles als de kleinste exponent in zijn priemfactorisatie minstens twee is én de grootste gemene deler van de exponenten gelijk aan één.





## 61 Formules van Vieta

De formules van Vieta geven een zeer handige relatie tussen de nulpunten en de coëfficiënten van polynomen. François Viète ontdekte deze eigenschap in de 16<sup>de</sup> eeuw voor positieve nulpunten, en het algemene geval werd in de 17<sup>de</sup> eeuw begrepen door Albert Girard.

Beschouw een algemene monische  $n^{\text{de}}$ -graadsveelterm,  $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ . Volgens de hoofdstelling van de algebra heeft deze veelterm dan juist  $n$ , niet noodzakelijkerwijs verschillende, complexe nulpunten  $r_1, r_2, \dots, r_n$ . Volgens de formules van Vieta geldt dan:

$$\begin{aligned} -a_{n-1} &= r_1 + r_2 + \dots + r_n \\ a_{n-2} &= r_1 r_2 + r_1 r_3 + \dots + r_{n-1} r_n \\ -a_{n-3} &= r_1 r_2 r_3 + r_1 r_2 r_4 + \dots + r_{n-2} r_{n-1} r_n \\ &\vdots \\ (-1)^i a_0 &= r_1 r_2 \dots r_n \end{aligned}$$

Voor de vierkantsvergelijking zijn deze formules welbekend en soms bruikbaar om oplossingen op het zicht te vinden. Vieta's formules veralgemenen deze eigenschap naar veeltermen met willekeurige graad. Ze geven tevens aanleiding tot een befaamde olympiadetechniek die "Vieta jumping" genoemd wordt, waarin het principe van oneindige afdaling wordt toegepast op nieuwe oplossingen voor een gegeven vergelijking, gevonden via de formules van Vieta.

## 62 Tekenregel van Descartes

René Descartes beschreef deze techniek om het aantal nulpunten van een veelterm te helpen bepalen in zijn werk *La Géométrie* uit 1637 (een appendix voor zijn belangrijkste werk *Discours de la Méthode*). De tekenregel stelt het volgende:

HET AANTAL POSITIEVE REËLE WORTELS VAN EEN REËLE VEELTERM WORDT BEGRENSD DOOR HET AANTAL WISSELINGEN VAN TEKEN IN ZIJN COËFFICIËNTEN.

Later wist Carl Friedrich Gauss deze techniek nog te verfijnen, door te stellen dat het aantal positieve wortels (multipliciteit meegerekend) dezelfde pariteit heeft als het aantal tekenwisselingen. Beschouw als voorbeeld deze veelterm, die drie wisselingen in tekens ondergaat en dus ofwel één, ofwel drie positieve nulpunten heeft:

$$P(x) = x^7 + x^6 - x^4 - x^3 - x^2 + x - 1 \quad (+ + - - - + -)$$

Door Descartes' tekenregel toe te passen op de veelterm  $P(-x)$  in plaats van  $P(x)$ , kan ook het aantal negatieve wortels gevonden worden.

## 63 Stelling van Mason-Stothers

De stelling van Mason-Stothers is de polynomiale (maar vrij eenvoudige) tegenhanger van het *abc*-vermoeden (zie 37, blz. 25). Ze wordt vernoemd naar Walter Stothers, die de stelling publiceerde en bewees in 1981, en

Richard Mason, die hem kort daarna in 1983 herontdekte.

De radicaal van een veelterm  $P$ , genoteerd als  $\text{rad } P$ , wordt gedefinieerd als de veelterm met minimale graad die dezelfde nulpunten heeft als  $P$ . Hogere multipliciteiten worden zo uit de veelterm gegooid. De stelling van Mason-Stothers beschouwt drie veeltermen over  $\mathbb{C}$ ,  $A$ ,  $B$  en  $C$ , die geen nulpunten gemeenschappelijk hebben ("copriem zijn") en zodat  $A + B = C$ ; dan geldt er:

$$\max(\deg A, \deg B, \deg C) \leq \deg(\text{rad}(A \cdot B \cdot C)) - 1$$

Merk op dat  $\deg(\text{rad } P)$  juist het aantal verschillende nulpunten van  $P$  voorstelt. Onvoorstelbaar genoeg is uit deze stelling op eenvoudige wijze de polynomiale versie van de laatste stelling van Fermat (zie ??, blz. ??) te bewijzen! Immers, voor de vergelijking  $X^n + Y^n = Z^n$  met  $X, Y, Z \in \mathbb{C}[x]$  en copriem en  $n \in \mathbb{N}$  geldt wegens Mason-Stother:

$$\deg X^n \leq \deg(\text{rad}(X^n \cdot Y^n \cdot Z^n)) - 1$$

De exponenten kunnen vooropgezet of geschrapt worden:

$$n \cdot \deg X \leq \deg(\text{rad}(X \cdot Y \cdot Z)) - 1$$

Hetzelfde geldt voor  $Y$  en  $Z$ . Omdat  $X$ ,  $Y$  en  $Z$  geen nulpunten gemeenschappelijk hebben, geldt er eveneens dat  $\deg(\text{rad}(X \cdot Y \cdot Z)) = \deg(\text{rad } X) + \deg(\text{rad } Y) + \deg(\text{rad } Z)$ . De vergelijkingen voor  $X$ ,  $Y$  en  $Z$  dan optellen geeft:

$$\begin{aligned} n \cdot (\deg X + \deg Y + \deg Z) &\leq 3(\deg(\text{rad } X) + \deg(\text{rad } Y) + \deg(\text{rad } Z)) - 3 \\ &\leq 3(\deg X + \deg Y + \deg Z) - 3 \end{aligned}$$

Beschouw de uiterste leden van deze ongelijkheid. De graad van een veelterm kan slechts positief zijn, dus moet wel gelden dat  $n - 3$  strikt negatief is. Hieruit volgt onmiddellijk dat  $n$  niet groter kan zijn dan 2, zoals de laatste stelling van Fermat beweert. Helaas is de getaltheoretische variant heel wat minder triviaal gebleken...

## 64 Stelling van Gelfond-Schneider

In 1934 werd het zevende probleem op de lijst van David Hilbert onafhankelijk opgelost door Aleksandr Gelfond en Theodor Schneider. Het resultaat dat nu naar hen vernoemd wordt, bewijst de transcendentie van een grote klasse getallen. Hilberts zevende probleem stelde specifiek:

1. Als in een gelijkbenige driehoek de verhouding van de basis- tot de tophoek algebraïsch, maar irrationaal is, is dan de verhouding tussen basis en opstaande zijde transcendent?
2. Is  $a^b$  altijd transcendent, voor elke algebraïsche  $a \notin \{0, 1\}$  en irrationale algebraïsche  $b$ ?

De bevestiging op de tweede vraag (die de eerste impliceert) werd bewezen door Gelfond en verrijnd door Schneider, hetgeen nu bekend staat als de stelling van Gelfond-Schneider. Uit deze stelling volgt ook de transcendentie van een groot aantal constanten, zoals de constante van Gelfond-Schneider  $2^{\sqrt{2}}$  of de constante van Gelfond  $e^\pi$ .

## 65 Criterium van Eisenstein

Het criterium van Eisenstein geeft een eenvoudige voldoende voorwaarde voor het al dan niet irreducibel zijn van een veelterm met gehele coëfficiënten over de rationale getallen. Theodor Schönemann was de eerste die een versie ervan publiceerde, in 1846; Gotthold Eisenstein gaf in 1850 een ietwat andere versie. Vooral begin 20<sup>ste</sup> eeuw stond het criterium dan ook bekend als de stelling van Schönemann-Eisenstein.

Gegeven een veelterm in  $\mathbb{Q}[x]$  met gehele coëfficiënten,  $Q = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ . Wanneer er een priemgetal  $p$  bestaat die aan de volgende voorwaarden voldoet, is  $Q$  irreducibel over  $\mathbb{Q}$  (niet te ontbinden in een product van niet-constante veeltermen met rationale coëfficiënten):

- $p$  deelt elke coëfficiënt  $a_i$ , behalve  $a_n$
- $p$  deelt  $a_n$  niet
- $p^2$  deelt  $a_0$  niet

Een voorbeeld waarbij het criterium rechtstreeks werkt, is voor  $Q_1 = 3x^2 + 15x^2 + 10$ ; priemgetal 5 voldoet aan alle voorwaarden om irreducibiliteit te mogen besluiten.  $Q_2 = x^2 + x + 2$  gaat niet direct, maar hier biedt de substitutie  $x' = x + 3$  een uitweg: deze transformeert  $Q_2$  in  $x'^2 + 7x' + 14$ , *et voilà*: priemgetal 7 werkt.

## 66 Criterium van Cohn

Net als het criterium van Eisenstein (zie 65, blz. ??) geeft dat van Cohn een elegante voldoende voorwaarde voor irreducibiliteit in  $\mathbb{Z}[x]$ . Arthur Cohn bewees dat de veelterm  $a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0$  irreducibel is als de coëfficiënten  $a_i$  de cijfers zijn van een priemgetal  $p$  (in grondtal 10).

Een veralgemening werd gegeven door Andrew Odlyzko, John Brillhart en Michael Filaseta. Beschouw  $b \leq 2$  en de veelterm  $P(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0$  met alle coëfficiënten tussen 0 en  $b - 1$ . Als  $P(b)$  een priemgetal oplevert, dan is  $P(x)$  irreducibel in  $\mathbb{Z}[x]$ .

Het nog onbewezen vermoeden van Bunyakovsky beweert dat de stelling ook omgekeerd geldt: wanneer  $P(x)$  irreducibel is en coprieme gehele coëfficiënten heeft, zou er een grondtal bestaan zodanig dat deze coëfficiënten de representatie van een priemgetal geven in dat grondtal.

## 67 Sturmketens

De Sturmketen van een polynoom, genoemd naar Jacques Sturm, wordt eenvoudig gevonden door een variant op Euclides' algoritme. De hierop voortbouwende stelling van Sturm drukt het aantal verschillende, reële nulpunten van deze veelterm binnen een bepaald interval uit met behulp van Sturmketens en kan gebruikt worden om deze nulpunten te lokaliseren.

De Sturmketen is een rij veeltermen met strikt dalende graad die begint bij de veelterm  $P$  zelf en zijn afgeleide. Elke volgende term is de rest bij polynomiale deling van de vorige twee, veranderd van teken, en de keten stopt bij een constante.

$$\begin{aligned} K_0 &= P \\ K_1 &= P' \\ K_2 &= -\text{rem}(P, P') \\ &\vdots \\ K_m &= -\text{rem}(K_{m-2}, K_{m-1}) \\ &\vdots \\ 0 &= -\text{rem}(K_{n-1}, K_n) \end{aligned}$$

Hier is  $\text{rem}(A, B)$  de rest bij polynomiale deling van  $A$  door  $B$ . De uiteindelijke Sturmketen  $\{K_0 \dots K_n\}$  eindigt dan met de grootste gemeenschappelijke deler van de initiële polynoom  $P$  en zijn afgeleide  $P'$ .

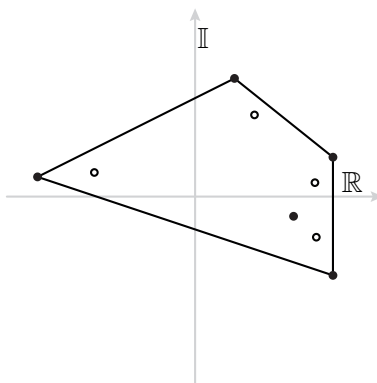
De kracht van deze Sturmketens wordt duidelijk in de stelling van Sturm. Bepaal het aantal tekenveranderingen in de keten geëvalueerd in een punt  $a$  (0 wijzigt geen teken), en doe hetzelfde voor een ander punt  $b$ . Het verschil



tussen deze aantallen komt dan overeen met het aantal verschillende, reële nulpunten van  $P$  in het interval  $]a, b]$ . Wanneer een nulpunt multipliciteit hoger dan één heeft, moet er rekening mee worden gehouden dat noch  $a$  noch  $b$  zo'n dubbele wortel mag zijn.

## 68 Stelling van Gauss-Lucas

De stelling van Gauss-Lucas geeft een geometrische relatie tussen de complexe nulpunten van een veelterm en die van zijn afgeleide. Concreet stelt die dat wanneer een convexe veelhoek in het complexe vlak alle nulpunten van een complexe polynoom  $P$  bevat, dan ook alle nulpunten van zijn afgeleide  $P'$ . Anders geformuleerd, liggen de nulpunten van  $P'$  binnen het convex omhulsel\* van de nulpunten van  $P$ .



Een opmerkelijk speciaal geval is de stelling van Marden, voor polynomen van de derde graad (zie ??, blz. ??). Deze stelling wordt vernoemd naar Carl Friedrich Gauss en Félix Lucas.

## 69 Constante van Liouville

Liouvillegetallen zijn reële getallen  $x$  zodanig dat volgende eigenschap geldt.

$$\forall n \in \mathbb{N} : \exists p, q \in \mathbb{Z} \text{ met } q > 1 : \quad 0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n}$$

Getallen die hieraan voldoen, zijn altijd irrationaal. Meer nog, in 1844 bewees Joseph Liouville dat ze ook transcendent zijn. Als concreet voorbeeld gaf Liouville zijn constante, die aan deze eigenschap voldoet en dus transcendent is: de constante bevat cijfer één op de decimale plaatsen na de komma die een faculteit zijn, de andere plaatsen bevatten cijfer nul. Het bestaan van transcendente getallen werd met dit getal voor het eerst betuigd.

$$\sum_{k=1}^{\infty} 10^{-k!} \approx 0,11000100000000000000000000001000\dots$$

## 70 Methode van Gräffe

Een van de populairste methodes uit de 19<sup>de</sup> en 20<sup>ste</sup> eeuw om nulpunten van veeltermen op te sporen, is het algoritme van Gräffe, onafhankelijk van elkaar ontdekt door Germinal Dandelin in 1826 en Karl Gräffe in 1837. Het achterliggende principe is de wortels meerdere keren impliciet te kwadrateren, zodat ze qua grootte van elkaar worden gescheiden en men ze daarna met de formules van Vieta (zie 61, blz. 47) kan benaderen. Beschouw de algemene monische veelterm:

$$P_0(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$$

\*Een convex omhulsel kan worden voorgesteld met een elastiekje dat rondom de verzameling punten losgelaten wordt: deze zal zich dan rond de punten spannen in de vorm van hun convex omhulsel.

We transformeren deze tot een nieuwe monische veelterm  $P_1$  van dezelfde graad, waarvan de wortels  $\alpha_i^2$  juist de kwadraten zijn van de wortels  $\alpha_i$  van  $P_0$ . Dit lukt door op te merken dat:

$$P_0(x) = \prod_{i=1}^n (x - \alpha_i) \quad \text{en} \quad P_0(-x) = (-1)^n \cdot \prod_{i=1}^n (x + \alpha_i)$$

Dan ziet men eenvoudig in dat de gezochte veelterm  $P_1$  als volgt berekend kan worden:

$$P_1(x^2) = \prod_{i=1}^n (x^2 - \alpha_i^2) = (-1)^n \cdot P_0(x) \cdot P_0(-x)$$

Gräffe versimpelde deze berekeningsmethode nog door  $P_0$  te splitsen in z'n even en oneven gedeelte.

$$P_0(x) = P_{0,e}(x^2) + x \cdot P_{0,o}(x^2) \quad \Rightarrow \quad P_1(x) = (-1)^n \cdot (P_{0,e}(x)^2 - x \cdot P_{0,o}(x)^2)$$

Door dit principe een aantal keer na elkaar uit te voeren, worden de wortels van  $P_0$  gescheiden. Een initiële veelterm waarvan de wortels door een factor  $\rho > 1$  gescheiden worden (dus  $|\alpha_i| \geq \rho \cdot |\alpha_j|$ ), wordt zo omgezet in een veelterm  $P_k(x) = x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0$  waarvan de wortels  $\beta_i$  minstens een snelgroeiende factor  $\rho^{2^k}$  schelen. Vervolgens passen we de formules van Vieta toe:

$$\begin{aligned} b_{n-1} &= -(\beta_1 + \beta_2 + \dots + \beta_n) \\ b_{n-2} &= \beta_1\beta_2 + \beta_1\beta_3 + \dots + \beta_{n-1}\beta_n \\ &\vdots \\ b_0 &= (-1)^n \cdot \beta_1\beta_2 \dots \beta_n \end{aligned}$$

Omdat na de voorgaande stappen de wortels flink van elkaar gescheiden zijn, zal de grootste wortel deze uitdrukkingen domineren en benaderen we de coëfficiënten enkel met de eerste termen:

$$b_{n-1} \approx -\beta_1, \quad b_{n-2} \approx \beta_1\beta_2, \quad \dots \quad b_0 \approx (-1)^n \cdot \beta_1\beta_2 \dots \beta_n$$

Hieruit volgt:

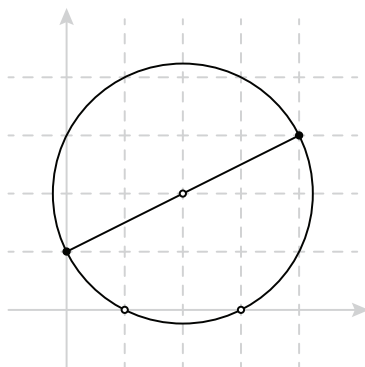
$$\beta_1 \approx -b_{n-1}, \quad \beta_2 \approx \frac{-b_{n-2}}{b_{n-1}}, \quad \dots \quad \beta_n \approx \frac{-b_0}{b_{n-1}}$$

De  $2^k$ de-machtswortels van deze  $\beta_i$ 's geven dan (op het teken na) een benadering voor de wortels  $\alpha_i$  van de oorspronkelijke veelterm, nauwkeuriger naarmate de wortels meer van elkaar gescheiden werden.

## 71 Carlylecirkels

Een cirkel van Carlyle is een welbepaalde cirkel in het Cartesisch vlak geassocieerd aan een vierkantsvergelijking. Deze cirkel heeft de eigenschap dat z'n snijpunten met de horizontale as net corresponderen met de nulpunten van de vergelijking, wat handig blijkt in bijvoorbeeld passer-en-liniaalconstructies van regelmatige veelhoeken. Het idee deze cirkels te gebruiken om tweedegraadsvergelijkingen op te lossen, wordt toegeschreven aan Thomas Carlyle.

Beschouw de algemene vergelijking  $x^2 - sx + p = 0$ , dan is de bijhorende Carlylecirkel per definitie die met als diameter het lijnstuk tussen de punten  $(0, 1)$  en  $(s, p)$ . Men rekent eenvoudig na dat deze cirkel als vergelijking  $x(x - s) + (y - 1)(y - p) = 0$  heeft. De substitutie  $y = 0$  geeft de  $x$ -waarden van de snijpunten met de  $x$ -as, die kennelijk voldoen aan  $x^2 - sx + p = 0$  en dus de oplossingen van de oorspronkelijke vierkantsvergelijking voorstellen.



Het voorbeeld hierboven geeft de vergelijking  $x^2 - 4x + 3 = 0$  weer, dus met  $(s, p) = (4, 3)$ . Inderdaad zijn de abscissen van de snijpunten met de horizontale as net 1 en 3, de wortels van de vierkantsvergelijking.

## 72 $x^{105} - 1$

Veeltermen van de vorm  $x^n - 1$  ontbonden in factoren blijken te voldoen aan de opmerkelijke regelmaat dat alle niet-nul coëfficiënten  $\pm 1$  zijn. Gedurende lange tijd probeerden wiskundigen dit te bewijzen, totdat ontdekt werd dat dit in feite niet klopt! De kleinste  $n$ -waarde waarvoor het tegendeel geldt, is 105, en de ontbinding van  $x^{105} - 1$  ziet er als volgt uit:

$$\begin{aligned} & (x - 1) \cdot (x^2 + x + 1) \cdot (x^4 + x^3 + x^2 + x + 1) \cdot (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \\ & \cdot (x^8 - x^7 + x^5 - x^4 + x^3 - x + 1) \cdot (x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1) \\ & \cdot (x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12} - x^{11} + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1) \\ & \cdot (x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - \mathbf{2}x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} \\ & - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - \mathbf{2}x^7 - x^6 - x^5 + x^2 + x + 1) \end{aligned}$$

Het gedrag van deze ontbindingen kan beter begrepen worden aan de hand van cyclotomische veeltermen. Cyclotomie betekent letterlijk “de cirkel knippen”, wat wordt bekomen door de  $n^{\text{de}}$  eenheidswortels in het complexe vlak te plotten. We weten dat voor gehele  $n \geq 1$  geldt:

$$x^n - 1 = \prod_{k=0}^{n-1} (x - e^{\frac{2\pi ik}{n}})$$

De  $n^{\text{de}}$  cyclotomische veelterm  $\Phi_n(x)$  wordt nu op een gelijkaardige manier gedefinieerd.

$$\Phi_n(x) = \prod_{\substack{k=1 \\ \text{ggd } kn=1}}^{n-1} (x - e^{\frac{2\pi ik}{n}})$$

Deze veeltermen zijn monisch en hebben steeds gehele coëfficiënten. Uitgedrukt met Eulers totiëntfunctie (zie 12, blz. 10) is de graad van  $\Phi_n(x)$  juist  $\phi(n)$ , en over het veld der rationale getallen zijn ze irreducibel. Een fundamentele formule met betrekking tot de cyclotomische polynomen is de volgende:

$$\prod_{d|n} \Phi_d(x) = x^n - 1$$

Grenzen van de optredende coëfficiënten in deze veeltermen werd al aandachtig bestudeerd. Zo toonde Adolph Migotti aan dat wanneer  $n$  ten hoogste twee verschillende oneven priemfactoren heeft, dan de coëfficiënten in  $\Phi_n(x)$  enkel  $-1$ ,  $0$  of  $1$  kunnen zijn. Het eerste afwijkende geval treedt zoals hierboven opgemerkt al op bij  $n = 105 = 3 \cdot 5 \cdot 7$  (de laatste factor in de ontbinding is  $\Phi_{105}(x)$ ). Bij meerdere oneven priemfactoren kunnen de

coëfficiënten snel toenemen: bij  $\Phi_{3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17}(x)$  manifesteert  $\pm 532$  zich al.

De irreducibiliteit van  $\Phi_n(x)$  garandeert dat er oneindig veel priemgetallen congruent met 1 modulo  $n$  bestaan, een speciaal geval van de priemgetalstelling van Dirichlet (zie ??, blz. ??).

### 73 Cirkeltheorem van Gerschgorin

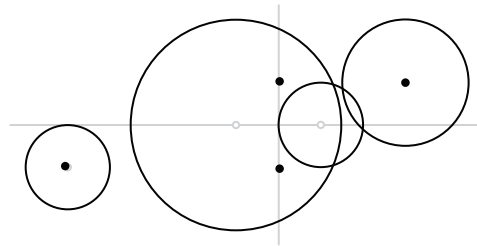
Het cirkeltheorem van Semyon Gerschgorin, gepubliceerd in 1931, geeft een afschatting voor de eigenwaarden van een complexwaardige matrix. Beschouw een matrix  $A$  van grootte  $n \times n$  met elementen  $a_{ij}$  en noteer  $R_i$  voor de som van absolute waarden van alle niet-diagonaalelementen in rij  $i$ :

$$R_i = \sum_{j \neq i} |a_{ij}|$$

Definieer nu voor elke  $i$  een zogenaamde Gerschgorinschijf als de gesloten schijf met middelpunt  $a_{ii}$  en straal  $R_i$ . Gerschgorins meest algemene en elegante resultaat stelt dat elke eigenwaarde van  $A$  binnen zo'n Gerschgorinschijf ligt. Dit houdt in dat wanneer  $A$  vooral elementen met een kleine norm buiten zijn diagonaal bevat, zijn eigenwaarden benaderd worden door de diagonaalelementen. Dit geeft aanleiding tot een numerieke techniek die eigenwaarden bepaalt door de matrix te reduceren naar een equivalente matrix met kleinere waarden buiten de diagonaal.

Beschouw als voorbeeld de volgende matrix, met bijhorende Gerschgorincirkels:

$$A = \begin{bmatrix} 2 & -2 & 0 & 0 \\ 4 & -2 & 0 & 1 \\ 1 & 1 & 6 + 2i & 1 \\ 1 & 1 & 0 & -10 - 2i \end{bmatrix}$$



Merk hierbij op dat de aangeduide eigenwaarden zich inderdaad allen binnen deze cirkels bevinden, maar niet elke cirkel een eigenwaarde hoeft te bevatten. Binnen elke *disjuncte* cirkel ligt echter wel juist één eigenwaarde. Algemeener bevat een unie van  $k$  Gerschgorincirkels disjunct met de  $n - k$  andere, precies  $k$  eigenwaarden.

Wat ook soms handig blijkt: de unieke eigenwaarde binnen een Gerschgorincirkel die disjunct is van de andere en afstamt van een rij met een reëel diagonaalelement, is zelf ook reëel.

### 74 Kuratowski's 14-stelling

Dit algebraïsche probleem vindt haar oorsprong in de topologie en werd opgelost door Kazimierz Kuratowski in 1922: hoeveel verschillende verzamelingen kan met vormen uit een gegeven verzameling, door herhaaldelijk over te gaan op sluitingen en complementen? Deze operaties geschieden binnen een vaste topologische ruimte. Beschouw bijvoorbeeld het open eenheidsinterval  $]0, 1[$  in  $\mathbb{R}$ : na sluitingen en complementen vinden we er vier.

- $]0, 1[$
- $[0, 1]$
- $\mathbb{R} \setminus [0, 1]$
- $\mathbb{R} \setminus ]0, 1[$

Met ingewikkeldere startverzamelingen zijn er meer resultaten mogelijk. Kuratowski bewees nu dat dit proces in hoogstens 14 verschillende verzamelingen resulteert, en dat deze bovengrens bovendien bereikt kan worden.

We gebruiken vanaf hier prefixnotatie: de sluiting van een verzameling  $V$  noteren we als  $-V$  en het complement als  $cV$ . Kuratowski's resultaat volgt eenvoudig uit het feit dat de sluitingsoperator idempotent is ( $-^2 = -$ ), het complement een involutie ( $c^2 = e$ , waarbij  $e$  de eenheid voorstelt), en de volgende identiteit:

$$-c - c - c - c \equiv -c - c$$

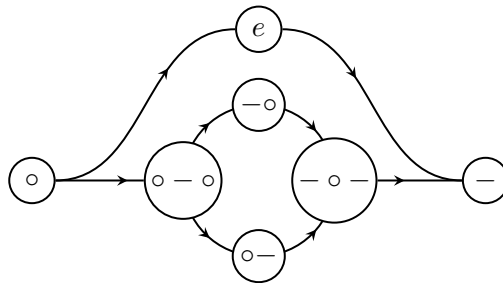
Deze laatste eigenschap volgt uit het feit dat  $(c - c)V$  het inwendige van  $V$  voorstelt, een vertrouwde operatie die we hierdoor verkort als  $\circ V$  noteren, consistent met de gebruikte prefixnotatie. De gestelde eigenschap volgt omdat  $-\circ -\circ = -\circ$  ( $-\circ$  is idempotent). Equivalent is  $-c - = -c - c - c -$ . Deze drie eigenschappen impliceren dat elke combinatie van sluitings- en complementsoperatoren equivalent moet zijn aan een van deze veertien:

- |         |               |                   |
|---------|---------------|-------------------|
| • $e$   | • $c - c$     | • $-c - c -$      |
| • $c$   | • $-c -$      | • $c - c - c -$   |
| • $-$   | • $c - c -$   | • $-c - c - c$    |
| • $c -$ | • $-c - c$    | • $c - c - c - c$ |
| • $-c$  | • $c - c - c$ |                   |

Rest nog aan te tonen dat er een topologische ruimte bestaat met een deelverzameling zodat elk van de veertien bovenstaande operatoren een ander resultaat geeft. Eén voorbeeld is de volgende in  $\mathbb{R}$ .

$$\left\{ \frac{1}{n} : n \in \mathbb{N} \right\} \cup ]2, 3[ \cup ]3, 4[ \cup \{5\} \cup [6, 7[ \cup ([8, 9[ \cap \mathbb{Q})$$

Verscheidene gerelateerde problemen werden al bestudeerd. Zo blijkt het met de operatoren  $-$  en  $\circ$ , sluiting en inwendige, mogelijk tot zeven verschillende eindverzamelingen te bekommen. In deze versie is het ook interessant na te gaan welke inclusies gelden. Deze worden in onderstaand Hassediagram gevisualiseerd; een pijl van (1) naar (2) betekent dat steeds  $(1) \subset (2)$ , voor eender welke verzameling die argument is van de operatoren.







## 75 Rij van Golomb

De rij van Golomb, vernoemd naar de Amerikaanse wiskundige Solomon Golomb, is de unieke niet-dalende rij van gehele getallen  $u$  waarbij  $u(n)$  aangeeft hoe vaak  $n$  voorkomt in de rij, startende met  $u(1) = 1$ . De rij staat ook bekend als de rij van Silverman.

1, 2, 2, 3, 3, 4, 4, 4, 5, 5, 5, 6, 6, 6, 6, 7, 7, 7, 7, 8, 8, 8, 8, 9, 9, 9, 9, 9, 10, 10, 10, 10, 10, 11, 11 ... (OEIS A001462)

De rij kan opmerkelijk genoeg ook recursief worden bepaald met het volgende voorschrift:

$$u(1) = 1, \quad u(n+1) = 1 + u(n+1 - u(u(n)))$$

Nog interessanter echter is dit expliciete voorschrift:  $u(n)$  is het gehele getal het dichtst bij  $\phi^{2-\phi} \cdot n^{\phi-1}$  gelegen, met  $\phi$  de gulden verhouding!

## 76 Rij van Recamán

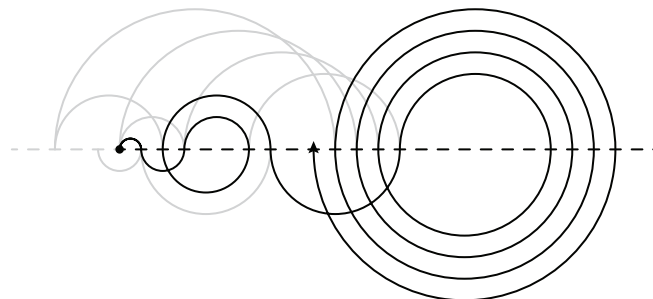
De volgende rij werd voorgesteld door de Colombiaanse wiskundige Bernardo Recamán Santos, en werd daarom door Neil Sloane (de beheerder van OEIS) aangeduid als de rij van Recamán. Ze wordt als volgt gedefinieerd:

$$u_0 = 0, \quad u_n = \begin{cases} u_{n-1} - n & \text{als } u_{n-1} - n \text{ positief is en nog niet in de rij voorkomt} \\ u_{n-1} + n & \text{anderszins} \end{cases}$$

Dit voorschrift geeft het volgende resultaat:

0, 1, 3, 6, 2, 7, 13, 20, 12, 21, 11, 22, 10, 23, 9, 24, 8, 25, 43, 62, 42, 63, 41, 18, 42, 17, 43, 16 ... (OEIS A005132)

Sloane vermoedt dat elk natuurlijk getal in de uiteindelijke reeks terug te vinden is.





## 77 Diatomische reeks van Stern

Sterns diatomische reeks wordt als volgt gedefinieerd:

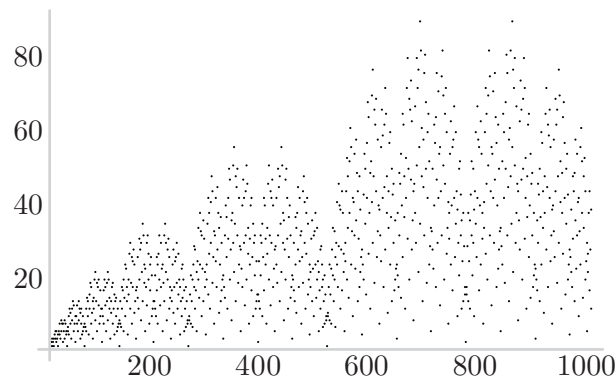
$$\begin{cases} u_0 = 0 \\ u_1 = 1 \\ u_{2n} = u_n \\ u_{2n+1} = u_n + u_{n+1} \end{cases}$$

Te beginnen met  $n = 0$  levert dit deze reeks op:

0, 1, 1, 2, 1, 3, 2, 3, 1, 4, 3, 5, 2, 5, 3, 4, 1, 5, 4, 7, 3, 8, 5, 7, 2, 7, 5, 8, 3, 7, 4, 5, 1, 6, 5, 9, 4, 11, 7, ... (OEIS A002487)

Dit voorschrift werd door Edgar Dijkstra aangeduid als de fusc-functie,  $\text{fusc}(n)$ . Ze heeft enkele interessante eigenschappen; zo is  $\text{fusc}(n+1)$  het aantal manieren om  $n$  te schrijven als een som van machten van 2, waarbij elke macht maximaal twee keer voorkomt. Dijkstra bewees ook de volgende eigenschap:

$$2 \mid \text{fusc}(n) \Leftrightarrow 3 \mid n$$



Elke twee opeenvolgende elementen zijn relatief priem. In feite geldt zelfs de verbazingwekkende eigenschap dat de verhoudingen van twee opeenvolgende termen alle positieve rationale getallen doorlopen, in hun onvereenvoudigbare vorm en juist één keer (zie 320, blz. 311)!

Schrijf de termen als volgt op in een driehoek, met in elke rij dubbel zoveel termen als in de vorige:

```

1
1 2
1 3 2 3
1 4 3 5 2 5 3 4
1 5 4 7 3 8 5 7 2 7 5 8 3 7 4 5
1 6 5 9 4 11 7 10 3 11 8 13 5 12 7 9 2 9 7 12 5 13 8 11 3 10 7 11 4 9 5 6
⋮

```

De som van de elementen in de  $k^{\text{de}}$  rij is dan gelijk aan  $3^{k-1}$ . De kolommen zijn bovendien rekenkundige rijen, waarvan de verschillen net de originele rij vormen.

## 78 Rij van Thue-Morse

De binaire rij van Thue-Morse werd het eerst bestudeerd als een toepassing in getaltheorie door Eugène Prouhet, in 1851. Hij vermeldde deze rij echter niet expliciet; dat deed Axel Thue pas in 1906, toen hij van nut bleek in

woordcombinatoriek. Dankzij Marston Morse is de rij wereldwijd beroemd geworden in 1921; Morse ontdekte een toepassing in de differentiaalmeetkunde. De rij ziet er als volgt uit:

0110100110010110100101100110100110010110011010010110100110010110100101100... (OEIS A010060)

Er zijn vele eenvoudige constructies mogelijk. Een daarvan is beginnen met 0, daarna in de volledige sequentie de 0'en en 1'en om te wisselen, deze nieuwe reeks achteraan de vorige te schakelen en dit te herhalen:

$$0 \mapsto 0 \cdot 1 \mapsto 01 \cdot 10 \mapsto 0110 \cdot 1001 \mapsto 01101001 \cdot 10010110 \mapsto \dots$$

Wat eveneens werkt, is beginnen bij 1 en herhaaldelijk 0 vervangen door 01 en 1 door 10. Een andere methode berekent expliciet de  $n^{\text{de}}$  term  $t_n$  als de som van de cijfers in de binaire voorstelling (m.a.w. het aantal 1'en in binaire notatie) modulo 2. Recursieve formules bestaan uiteraard ook:

$$t_0 = 0, \quad t_{2n} = t_n, \quad t_{2n+1} = 1 - t_n$$

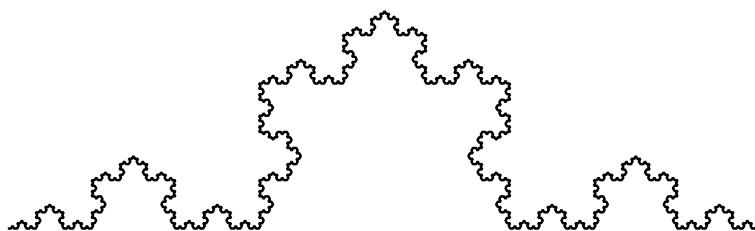
De rij  $t$  kan ook (min of meer) worden gegenereerd.

$$\prod_{k=0}^{\infty} (1 + x^{2^k}) = \sum_{k=0}^{\infty} (-1)^{t_k} \cdot x^k$$

De rij van Thue-Morse is *sterk* kubiekvrij; dit houdt in dat die geen deelrij bevat van de vorm  $xxa$ , waarbij  $x$  een eindige deelrij is en  $a$  het eerste symbool is van  $x$ . Zwakkere criteria noemen de rij ook kwadraatvrij (geen deelrij van de vorm  $xx$ ) en kubiekvrij (geen deelrij van de vorm  $xxx$ ). Schaakmeester Max Euwe gebruikte deze kubiekvrije eigenschap in een bewijs dat er schaakpartijen mogelijk zijn die oneindig lang duren, maar toch geen drie identieke zetten bevatten (en zo tot remise zouden leiden).

De rij van Thue-Morse duikt zelfs op bij fractalen! Als het volgende programma de Thue-Morserij  $t_n$  doorloopt, verkrijg je als resultaat de sneeuwvlok van Koch (zie 202, blz. 162).

- Voor  $t_n = 0$ : teken een lijnsegment één eenheid vooruit
- Voor  $t_n = 1$ : draai tegen de klok in met een hoek van  $60^\circ$



Kurt Mahler bewees in 1929 dat het binaire getal  $0,011010011001011010010110011010\dots$  (waarvan de cijfers de Thue-Morserij vormen) transcendent is. Dit getal wordt de constante van Prouhet-Thue-Morse genoemd en komt in het decimaal stelsel overeen met  $0,412454033640\dots$

## 79 RATS

De RATS-rij van John Conway wordt gedefinieerd door een simpel voorschrift: “reverse, add, then sort”! Tel gewoon telkens het getal met z'n cijfers in omgekeerde volgorde op bij zichzelf, en rangschik de cijfers van de bekomen som in opklimmende volgorde. Vertrekkend bij wortel 1 geeft dit een rij die een hardnekkig patroon vertoont, en die Conway de klimplant noemde:

1, 2, 4, 8, 16, 77, 145, 668, 1345, 6677, 13444, 55778, 133345, 666677, 1333444, 5567777, 12333445, 66666677, 133333444, 556667777, 1233334444, 5566667777, 12333334444, 55666667777 . . . (OEIS A004000)

Conway vermoedt dat ongeacht de startwaarde, elke RATS-rij uiteindelijk ofwel in deze klimplant terechtkomt, ofwel tot een cykel, zoals 111, 222, 444, 888, 1677, 3489, 12333, 44556, 111 . . .

## 80 Look-and-say

De look-and-sayrij werd geïntroduceerd en diepgaand geanalyseerd door John Conway in 1986. Het voorschrift is zeer eenvoudig doch origineel: beschrijf de voorgaande term in blokken van hetzelfde cijfer! Beginnend bij 1 geeft dit: één 1 is 11, twee 1'en is 21, één 2 en één 1 is 1211 . . .

1, 11, 21, 1211, 111221, 312211, 13112221, 1113213211, 31131211131221 . . . (OEIS A005150)

Deze rij groeit onbeperkt door ongeacht de startwaarde, behalve voor 22, die als enige getal ongewijzigd blijft. Een andere eigenschap is dat de rij uitsluitend uit 1'en, 2'en en 3'en bestaat, tenzij ook de startwaarde een groter cijfer bevat of een langere groep van eenzelfde cijfer. Conway wist nog een opmerkelijk besluit te bewijzen: als we  $L_n$  noteren als de lengte van de  $n^{\text{de}}$  term, dan convergeert de verhouding lengtes van opeenvolgende termen naar een constante  $\lambda$ , onafhankelijk van de beginwaarde:

$$\lim_{n \rightarrow \infty} \frac{L_{n+1}}{L_n} = \lambda \approx 1,303577269 \dots$$

Deze constante  $\lambda$  is, zo bewees Conway, een algebraïsch getal van graad 71! De bijhorende polynoom waarvan  $\lambda$  de unieke reële oplossing is, is:  $x^{71} - x^{69} - 2x^{68} - x^{67} + 2x^{66} + 2x^{65} + x^{64} - x^{63} - x^{62} - x^{61} - x^{60} - x^{59} + 2x^{58} + 5x^{57} + 3x^{56} - 2x^{55} - 10x^{54} - 3x^{53} - 2x^{52} + 6x^{51} + 6x^{50} + x^{49} + 9x^{48} - 3x^{47} - 7x^{46} - 8x^{45} - 8x^{44} + 10x^{43} + 6x^{42} + 8x^{41} - 5x^{40} - 12x^{39} + 7x^{38} - 7x^{37} + 7x^{36} + x^{35} - 3x^{34} + 10x^{33} + x^{32} - 6x^{31} - 2x^{30} - 10x^{29} - 3x^{28} + 2x^{27} + 9x^{26} - 3x^{25} + 14x^{24} - 8x^{23} - 7x^{21} + 9x^{20} + 3x^{19} - 4x^{18} - 10x^{17} - 7x^{16} + 12x^{15} + 7x^{14} + 2x^{13} - 12x^{12} - 4x^{11} - 2x^{10} + 5x^9 + x^7 - 7x^6 + 7x^5 - 4x^4 + 12x^3 - 6x^2 + 3x - 6 = 0$ .

Tot slot nog de "kosmologische stelling" van Conway: uiteindelijk degradeert elke rij tot zogenaamde atomische elementen, eindige deelrijen die nooit meer interageren met hun burens. Er zijn 92 dergelijke elementen die enkel de cijfers 1, 2 en 3 bevatten; John Conway vernoemde ze allen naar de chemische elementen. De volledige lijst staat op <http://mathworld.wolfram.com/CosmologicalTheorem.html>. Buiten deze klassieke elementen bestaan er voor andere cijfers telkens ook twee transuranische elementen.

## 81 Rij van Gijswijt

De rij van Gijswijt is een zeer originele en intrigerende rij. De initiële term is 1, en elke volgende term geeft aan hoeveel herhalende blokken er achteraan de rij te vinden zijn. Concreet, schrijf alle reeds gevonden termen achter elkaar in één lang woord, en ontbind dit woord als  $(x) \cdot (y)^k$  (de concatenatie van  $x$  met  $k$  kopieën van  $y$ ); de maximale  $k$ -waarde waarvoor dit mogelijk is, wordt de nieuwe term.

Bijvoorbeeld, na de eerste zes termen hebben we al 112112, wat geschreven kan worden als  $(1) \cdot (112)^2$ . Men ziet eenvoudig in dat grotere waarden voor  $k$  niet mogelijk zijn, dus de zevende term is 2. De rij begint als volgt:

1, 1, 2, 1, 1, 2, 2, 2, 3, 1, 1, 2, 1, 1, 2, 2, 2, 3, 2, 1, 1, 2, 1, 1, 2, 2, 2, 3, 1, 1, 2, 1, 1, 2, 2, 2, 3, 1, 1, 2, 1, 1, 2, 2, 2, 3, 2, 2, 2, 3, 2, 2, 2, 3, 3, 2, 2, 2, 3, 2, 1, 1, 2, 1, 1, 2, 2, 2, 3, 1, 1, 2, 1, 1, 2, 2, 2, 3, 1, 1, 2, 1, 1, 2, 2, 2, 3, 1, 1, 2, 1, 1, 2, 2, 2, 3, 2, 2, 2, 3, 2, 2, 2, 3, 3, 2, 2, 2, 3, 2, 1, 1, 2, 1, 1, 2, 2, 2, 3, 1, 1, 2, 1, 1, 2, 2, 2, 3, 2, 1, 1, 2, 1, 1, 2, 2, 2, 3, 1, 1, 2, 1, 1, 2, 2, 2, 3, 1, 1, 2, 1, 1, 2, 2, 2, 3, 1, 1, 2, 1, 1, 2, 2, 2, 3, 2, 2, 2, 3, 2, 2, 2, 3, 3,

2, 2, 2, 3, 2, 2, 2, 3, 2, 2, 2, 3, 3, 2, 2, 2, 3, 2, 2, 2, 3, 2, 2, 2, 3, 3, 3, 3, 4, 1, 1, 2, 1, 1, 2, 2, 2, 3, 1 . . . (OEIS A090822)

De rij groeit extreem traag: het getal 4 op positie 220, maar men kan miljarden termen berekenen zonder een 5 te vinden. Toch is de rij onbegrensd en duikt elk natuurlijk getal ooit in de rij van Gijswijt op! De grootteorde van de eerste optredende 5 is zo'n  $10^{10^{23}}$ , en algemeen schat me dat het getal  $t$  (voor  $t \geq 5$ ) voor het eerst voorkomt in de buurt van positie  $2 \uparrow (2 \uparrow (3 \uparrow (4 \uparrow (5 \uparrow \dots \uparrow ((t-2) \uparrow (t-1))))))$ , of:

$$2^{2^{3^{4^{\dots^{t-1}}}}}$$

De rij werd door Neil Sloane vernoemd naar Nederlands wiskundige Dion Gijswijt.

## 82 Hofstadter-Conways \$10.000-rij

De recursieve rij gedefinieerd als:

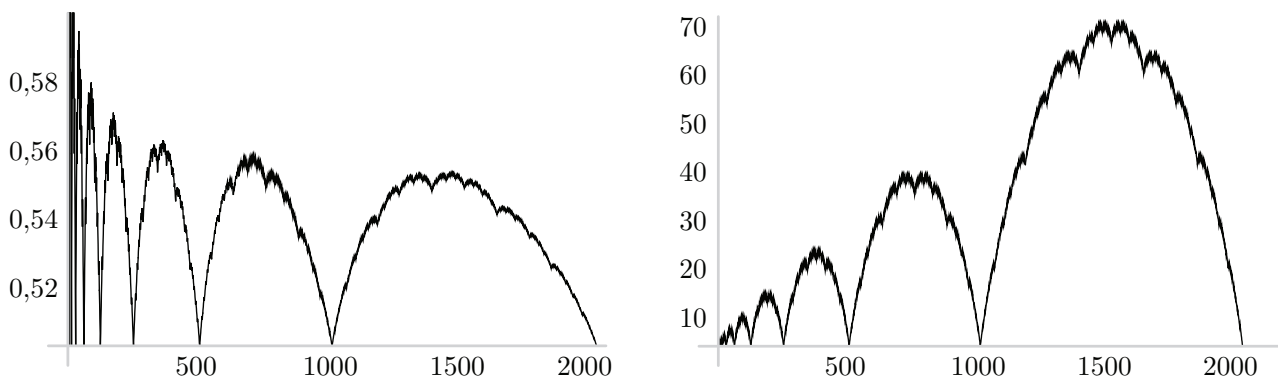
$$u(0) = 1, \quad u(1) = 1, \quad u(n) = u(u(n-1)) + u(n - u(n-1))$$

1, 1, 2, 2, 3, 4, 4, 4, 5, 6, 7, 7, 8, 8, 8, 8, 9, 10, 11, 12, 12, 13, 14, 14, 15, 15, 15, 16, 16, 16, 16, 16 . . . (OEIS A004001)

John Conway toonde aan dat de verhouding van deze termen en hun volgnummer in de limiet naar oneindig convergeert naar  $\frac{1}{2}$ . Links hieronder staat een plot van deze quotiënten.

$$\lim_{n \rightarrow \infty} \frac{u(n)}{n} = \frac{1}{2}$$

De \$10.000-rij komt aan zijn bizarre naam doordat Conway een prijs van \$10.000 aanbood voor de berekening van het volgnummer  $n$  waarvoor alle volgende quotiënten dichter bij hun limiet liggen dan  $\frac{1}{20}$ . Colin Mallows vond hiervoor  $n = 1489$  en eiste de prijs op, nadat Conway de som aanpaste naar het "beoogde" \$1.000.



Opmerkelijk genoeg blijkt de grafiek van  $u(n) - \frac{n}{2}$  een serie groeiende blanc-mangerkrommen (zie 206, blz. 165) te vormen! Zie daarvoor de rechterplot hierboven.

Voor deze rij geldt tevens nog dat  $\frac{u(n)}{n}$  telkens de limietwaarde  $\frac{1}{2}$  bereikt op termen met een tweedemacht als volgnummer (dus  $u(2^k) = 2^{k-1}$ ) en dat voor algemene volgnummers steeds geldt dat  $u(2k) \leq 2u(k)$ .

## 83 Kimberlings fractale rij

HOU EEN AANTAL KAARTEN, GENUMMERD 1, 2, 3 . . .  $n$  MET DE 1 BOVENAAN, IN JE HAND. NEEM DE BOVENSTE KAART EN PLAATS DIE ONDERAAN HET DEK; NEEM DAN DE VOLGENDE KAART EN LEG DIE OP TAFEL. HERHAAL DIT PROCES TOT ALLE  $n$  KAARTEN IN EEN BEPAALDE VOLGORDE OP TAFEL LIGGEN. DE HOEVEELSTE KAART IN DE STAPEL OP TAFEL ZAL DAN DE EERSTE KAART (GENUMMERD 1) ZIJN?

De rij gevormd door dit voorschrift is de volgende.

1, 1, 2, 1, 3, 2, 4, 1, 5, 3, 6, 2, 7, 4, 8, 1, 9, 5, 10, 3, 11, 6, 12, 2, 13, 7, 14, 4, 15, 8, 16, 1, 17, 9, 18 . . . (OEIS A003602)

Deze rij heeft de notabele eigenschap dat indien het eerste optreden van elk natuurlijk getal uit de rij geschrapt wordt, de overblijvende rij exact dezelfde is als de oorspronkelijke. Deze “zelfgelijkende” rij, opgebouwd uit kopieën van zichzelf, wordt naar analogie met de geometrische fractals een fractale rij genoemd. Zulke fractale rijen werden waarschijnlijk het eerst beschreven door Clark Kimberling in zijn artikel uit 1995 *Numeration systems and fractal sequences*.

Een extra puzzel rond de kaartenvraag: WAT MOET DE BEGINVOLGORDE VAN DE KAARTEN ZIJN OPDAT DE STAPEL OP TAFEL GERANGSCHIKT ZOU ZIJN VAN 1 TOT  $n$ ?

## 84 Signatuurrijen

Een signatuurrij kan worden bepaald voor elk positief irrationaal getal  $r$ . Orden de verzameling reële getallen van de vorm  $a + br$ , waarbij  $a$  en  $b$  natuurlijke getallen zijn, in stijgende volgorde. De rij van de  $a$ 's vormt dan de signatuurrij van  $r$ . Voor  $\sqrt{2}$  bijvoorbeeld wordt de signatuurrij:

1, 2, 1, 3, 2, 1, 4, 3, 2, 5, 1, 4, 3, 6, 2, 5, 1, 4, 7, 3, 6, 2, 5, 8, 1, 4, 7, 3, 6, 9, 2, 5, 8, 1, 4, 7, 10, 3, 6 . . . (OEIS A007336)

Net als Kimberlings rij zijn deze signatuurrijen fractaal. Verwijder het eerste optreden van elk natuurlijk getal uit de rij, of verlaag elk getal met één en schrap alle nullen; in beide gevallen verkrijg je de oorspronkelijke rij.

## 85 Rij van Connell

De rij van Connell bestaat uit het eerste oneven getal, daarna de twee volgende even getallen, de drie volgende oneven getallen, enzoverder. Ze wordt vernoemd naar Ian Connell, die in 1959 een bewijs vroeg voor de expliciete formule hieronder.

$$u_n = 2n - \left\lfloor \frac{1 + \sqrt{8n - 7}}{2} \right\rfloor$$

1, 2, 4, 5, 7, 9, 10, 12, 14, 16, 17, 19, 21, 23, 25, 26, 28, 30, 32, 34, 36, 37, 39, 41, 43, 45, 47, 49 . . . (OEIS A001614)

Zoals door Lekraj Beedassy in 2004 opgemerkt, kan de rij van Connell ook worden gegenereerd als het verschil van volgende twee rijen. De eerste rij stelt de term  $2n$  voor in de expliciete formule, de tweede rij de floorfunctie.

- De stijgende rij der even getallen: 2, 4, 6, 8, 10, 12, 14, 16, 18, 20 . . . (OEIS A005843)
- De stijgende rij waarin  $n$  juist  $n$  keer voorkomt: 1, 2, 2, 3, 3, 3, 4, 4, 4, 4 . . . (OEIS A002024)

## 86 Rij van Mian-Chowla

De rij van Mian-Chowla, vernoemd naar Abdul Majid Mian en Sarvadaman Chowla, begint met 1. Vervolgens kiest men elke nieuwe term als het kleinste natuurlijke getal zodat alle paarsgewijze verschillen tussen termen in de rij verschillend zijn. Deze gretige definitie garandeert dat geen twee koppels termen dezelfde som hebben.

1, 2, 4, 8, 13, 21, 31, 45, 66, 81, 97, 123, 148, 182, 204, 252, 290, 361, 401, 475, 565, 593, 662 . . . (OEIS A005282)

Mian en Chowla vermoedden eerst dat  $n^2$  een bovengrens vormde voor de termen  $a_n$  in hun rij, maar vanaf de

17<sup>de</sup> term wordt deze grens al overschreden. Alfred Stöhr bewees dat  $n^3$  wél een geldige bovengrens is en vroeg of deze nog verbeterd kan worden. Numerieke berekeningen wijzen erop dat de rij groeit omstreeks  $\mathcal{O}(n^{2,8})$ .

## 87 Hofstadters $G$ -rij

Douglas Hofstadter beschrijft deze rij in zijn met een Pulitzerprijs bekroonde boek *Gödel, Escher, Bach*, een ambitieuze publicatie over formele systemen en kunstmatige intelligentie. Hij geeft als recursieve voorschrift:

$$G(0) = 0, \quad G(n) = n - G(G(n - 1))$$

0, 1, 1, 2, 3, 3, 4, 4, 5, 6, 6, 7, 8, 8, 9, 9, 10, 11, 11, 12, 12, 13, 14, 14, 15, 16, 16, 17, 17, 18, 19 . . . (OEIS A005206)

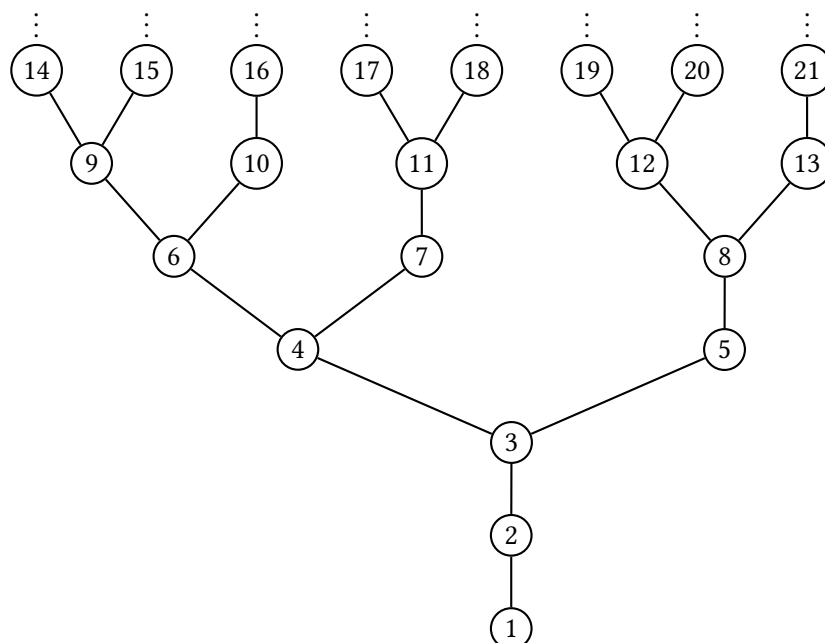
Opmerkelijk genoeg kan deze rij ook gegenereerd worden via een ander recursief voorschrift, dat gebruikmaakt van de gulden snede  $\phi = \frac{1}{2}(1 + \sqrt{5})$ .

$$G(0) = 0, \quad G(1) = 1, \quad G(n) = n - G\left(\left\lfloor \frac{n}{\phi} \right\rfloor\right)$$

Hieruit volgens tevens deze expliciete voorschriften.

$$G(n) = \left\lfloor \frac{n+1}{\phi} \right\rfloor = \lfloor (n+1) \cdot \phi \rfloor - n - 1$$

Hofstadter ontdekte ook het verband met deze boomstructuur. Elke splitsing wordt links rechtstreeks gevolgd door een nieuwe splitsing en rechts door een splitsing een niveau hoger. Wanneer de knooppunten van onder naar boven en van links naar rechts genummerd worden, vormen de getallen aan de rechterzijde van de boom de Fibonaccigetallen. Hofstadter stelde vast dat elk getal  $n$  een afsplitsing is van  $G(n)$ , bijv.  $G(6) = G(7) = 4$ , dus het vierde knooppunt vertakt zich in 6 en 7.



## 88 Rij van Kolakoski

De rij van Kolakoski is een eenvoudige doch mysterieuze rij, beschreven door William Kolakoski in 1965. Ze begint bij 1, bevat uitsluitend de getallen 1 en 2, en wordt volledig vastgelegd door de fractale eigenschap dat de lengtes van de blokken waarin de getallen voorkomen, net de originele rij vormen. Ondanks de eenvoudige



worden de termen ook Euclidesgetallen genoemd. Sylvesters rij begint bij 2 en wordt formeel bepaald als volgt:

$$u_0 = 2, \quad u_n = 1 + \prod_{i=0}^{n-1} u_i = u_{n-1}^2 - u_{n-1} + 1$$

2, 3, 7, 43, 1807, 3263443, 10650056950807, 113423713055421844361000443 . . . (OEIS A000058)

De rij van Sylvester groeit dubbelexponentieel; het kan worden aangetoond dat  $u_n$  het dichtstbijzijnde getal is bij  $E^{2^{n+1}}$ , waarin  $E$  ongeveer 1,264084735305302 is en de constante van Vardi genoemd wordt.

Nog een belangrijke eigenschap is het volgende verband met Egyptische breuken (zie 29, blz. 20): de omgekeerden van de termen uit Sylvesters rij vormen een oneindige Egyptische representatie voor één, en deze reeks eender waar afkappen en één aftrekken van de laatste noemer geeft een eindige voorstelling.

$$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{7} + \frac{1}{43} + \frac{1}{1807} + \frac{1}{3263443} + \dots$$

## 91 Fibonaccigetallen

Leonardo Pisano, thans beter bekend als Fibonacci, was de zoon van de welgestelde handelaar Guglielmo Bonacci en leerde op handelsreizen met zijn vader het Arabische talstelsel kennen. Hij realiseerde zich dat dit systeem veel eenvoudiger en efficiënter is dan het toentertijd gebruikte Romeinse stelsel en introduceerde het in Europa via zijn boek *Liber Abaci*, waarin hij tevens bij wijze van oefening de Fibonaccigetallen beschreef. De rij was al eerder bekend bij Indische wiskundigen maar werd later door Édouard Lucas naar Fibonacci vernoemd.

De Fibonaccigetallen worden bepaald door een eenvoudige recursieve relatie. De initiële waarden zijn  $F_0 = 0$  en  $F_1 = 1$ , en elk volgend getal is de som van de voorgaande twee getallen ( $F_n = F_{n-1} + F_{n-2}$ ). Dit levert op:

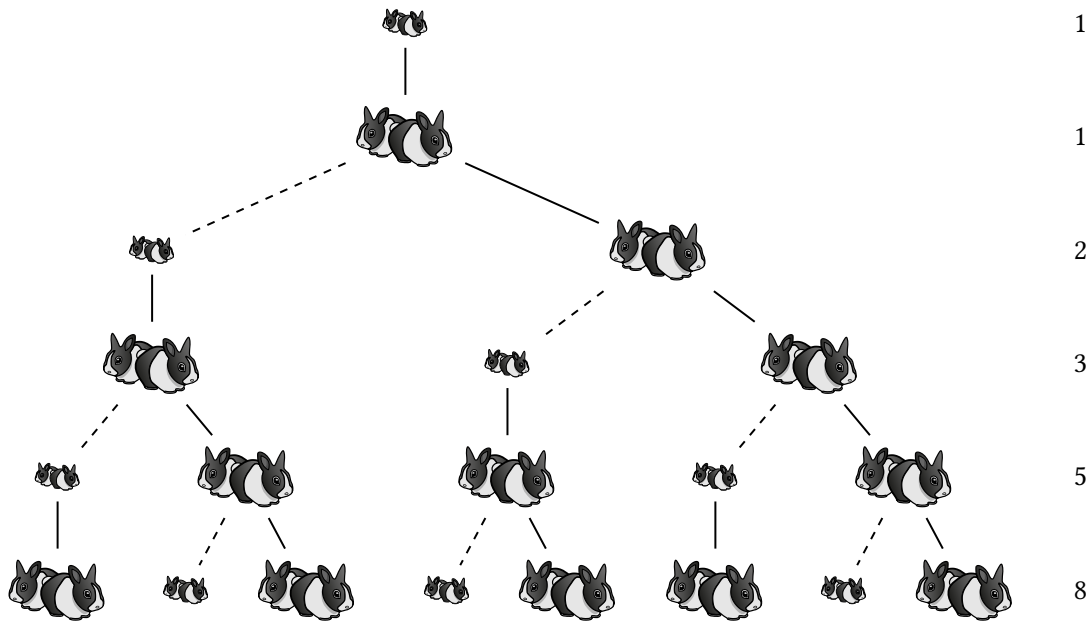
0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946 . . . (OEIS A000045)

In zijn *Liber Abaci* beschouwde Fibonacci dit (nogal onrealistische) groeimodel van een konijnenpopulatie:

- Aanvankelijk wordt een jong paar konijnen in een veld geplaatst.
- Het duurt een maand vooraleer een jong konijn volwassen wordt.
- Eenmaal volwassen plant een konijn zich elke maand voort: de nakomelingen vormen juist één jong paar.
- Er sterven geen konijnen.

Aan het einde van de  $n^{\text{de}}$  maand is het aantal konijnenparen gelijk aan het aantal dat de vorige maand overleefde, plus het aantal nieuwgeboren paren, wat net gelijk is aan het aantal paren twee maand terug. Dit resulteert dus juist in het  $n^{\text{de}}$  Fibonaccigetel.





De genererende functie voor de rij van Fibonacci is deze:

$$\sum_{n=0}^{\infty} F_n x^n = \frac{x}{1 - x - x^2}$$

Johannes Kepler was de eerste die opmerkte dat de verhouding van opeenvolgende Fibonaccigetallen convergeert naar de gulden verhouding  $\varphi$ . In feite geldt dit resultaat voor eender welke rij die voldoet aan de recursiebetrekking van Fibonacci.

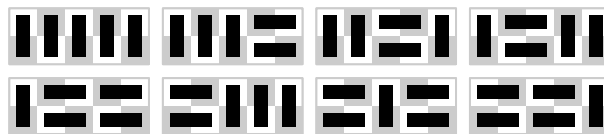
$$\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \frac{1 + \sqrt{5}}{2} = \varphi, \quad \lim_{n \rightarrow \infty} \frac{F_{n+k}}{F_n} = \varphi^k$$

Zoals elke rij gedefinieerd door een lineaire recursie met constante coëfficiënten kun je hier gemakkelijk een expliciete formule vinden. Ze staat bekend als de formule van Binet, naar Jacques Binet, hoewel Abraham de Moivre ze al eerder kende. Merk ook hier de gulden snede op!

$$F_n = \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right)$$

Uit de formule van Binet volgt eveneens dat het  $n^{\text{de}}$  Fibonaccigetal kan gevonden worden als het natuurlijke getal het dichtst gelegen bij  $\frac{\varphi^n}{\sqrt{5}}$ , aangezien de tweede term in absolute waarde steeds kleiner is dan  $\frac{1}{2}$ .

De Fibonaccigetallen treden op in de scheve diagonalen van de driehoek van Pascal (zie 246, blz. 204) en in enkele telproblemen. Zo is het aantal binaire strings met lengte  $n$  zonder opeenvolgende 1'en juist  $F_{n+2}$ , zonder oneven aantal opeenvolgende 1'en juist  $F_{n+1}$  en zonder even aantal opeenvolgende 1'en juist  $2F_n$ . Het aantal betegelingen van een  $2 \times n$ -rooster met domino's is ook een Fibonaccigetal,  $F_{n-1}$ .



Een interessante voorstelling van  $F_n$  maakt gebruik van matrices. Uit de recursie volgt immers:

$$\begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} F_n \\ F_{n-1} \end{bmatrix} \quad \Rightarrow \quad \begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Er bestaat een eenvoudige test om te controleren of een bepaald getal  $n$  Fibonacci is, gegeven door Ira Gessel in 1972:  $n$  is een Fibonaccigetel als en slechts als  $5n^2 + 4$  of  $5n^2 - 4$  een volkomen kwadraat is.

Combinatorische identiteiten met betrekking tot de Fibonaccigetallen bestaan er legio. Zo is er bijv. de identiteit van Cassini en een veralgemening ervan, de identiteit van Catalan.

$$F_n^2 - F_{n-1}F_{n+1} = (-1)^n, \quad F_n^2 - F_{n-r}F_{n+r} = (-1)^{n-r}F_r^2$$

Hier is een algemene formule om snel van index  $n$  over te stappen naar veelvoud van ervan e.d.:

$$F_{kn+c} = \sum_{i=0}^k \binom{k}{i} \cdot F_{c-i} \cdot F_n^i \cdot F_{n+1}^{k-i}$$

Ook de som van inversen van  $F_n$  werd al aandachtig bestudeerd.

$$\sum_{k=0}^{\infty} \frac{1}{1 + F_{2k+1}} = \frac{\sqrt{5}}{2}, \quad \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{\sum_{j=1}^k F_j^2} = \frac{\sqrt{5} - 1}{2}, \quad \sum_{k=0}^{\infty} \frac{1}{F_{2^n}} = \frac{7 - \sqrt{5}}{2}$$

Opmerkelijk genoeg is er nog geen gesloten formule bekend voor de som van inversen van alle Fibonaccigetallen, hoewel Richard André-Jeannin de irrationaliteit ervan toch al kon bewijzen.

$$\sum_{k=1}^{\infty} \frac{1}{F_k} \approx 3,359885666243 \dots$$

Een laatste leuke eigenschap is dat  $\text{ggd } F_m F_n = F_{\text{ggd } mn}$ .

Fibonaccigetallen komen wegens hun intieme relatie met de gulden snede vaak voor in de natuur, bijvoorbeeld als het aantal blaadjes van een bloem of spiralen in een denappel. Zie daarvoor 326, blz. 317.

## 92 Geluksgetallen

De geluksgetallen of *lucky numbers* worden zo genoemd omdat ze als enige overblijven na een zeefproces, dat nogal lijkt op de zeef van Eratosthenes (zie ??, blz. ??). Het algoritme zeft als volgt:

- Schrijf de oneven getallen uit.
- Het eerste getal na 1 is 3. Schrap elk derde getal dat nog in de lijst staat, vanaf het begin.
- Het volgende overlevende getal is 7. Schrap elk zevende getal dat nog in de lijst staat.
- Blijf dit herhalen door het  $k^{\text{de}}$  getal te schrappen, met  $k$  telkens het volgende overlevende getal.

De getallen die overblijven, heten de geluksgetallen. Merk op dat ironisch genoeg 13 een geluksgetal is.

1, 3, 7, 9, 13, 15, 21, 25, 31, 33, 37, 43, 49, 51, 63, 67, 69, 73, 75, 79, 87, 93, 99, 105, 111 . . . (OEIS A000959)

De rij werd geïntroduceerd in 1956 door Verna Gardiner, Roger Lazarus, Nicholas Metropolis en Stanisław Ulam. Opmerkelijk genoeg delen de geluksgetallen nogal wat eigenschappen met priemgetallen, zoals hun asymptotische gedrag en de priemgetalstelling (zie 1, blz. 5). Ook de frequenties van geluksgetaltweelingen en priemtweelingen (zie 48, blz. 37) zijn gelijkaardig. Er blijkt zelfs een versie van het vermoeden van Goldbach (zie 28, 19) stand te houden. Dit lijkt te suggereren dat deze eigenschappen niet zozeer gebonden zijn aan de priemgetallen zelf, maar algemener aan het zeefproces dat hen voortbrengt.

Het is nog onbekend of er oneindig veel gelukspriemgetallen zijn.

### 93 Papiergevouwen rij

De papiergevouwen rij kan op vele verrassende manieren geconstrueerd worden.

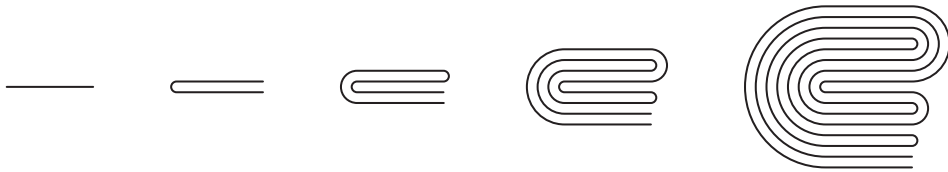
- Noteer  $n = m \cdot 2^k$  met  $m$  oneven en definieer de termen als volgt:

$$t_n = \begin{cases} 1 & \text{als } m \equiv 1 \pmod{4} \\ 0 & \text{als } m \equiv 3 \pmod{4} \end{cases}$$

- Begin met 1 en voeg in elke stap een alternerende rij van 1's en 0's toe rond de termen.

1,    1 1 0,    1 1 0 1 1 0 0,    1 1 0 1 1 0 0 1 1 1 0 0 1 0 0,    ...

- Vouw een strook papier herhaaldelijk in twee en ontvouw. Lees de geplooide richtingen af, en noteer 1 voor een bergvouw en 0 voor een dalvouw. Het is deze constructie waaraan de rij zijn naam dankt.



- Begin met 11 en pas herhaaldelijk deze substitutie toe.

$$\begin{cases} 11 \mapsto 1101 \\ 01 \mapsto 1001 \\ 10 \mapsto 1100 \\ 00 \mapsto 1000 \end{cases}$$

- Begin met 1. Elke nieuwe term wordt een 1 met links ervan de vorige term integraal toegevoegd en rechts ervan eveneens de vorige term, maar dan achterstevoren en met 0'en en 1'en geswitcht.

1,    1 1 0,    1 1 0 1 1 0 0,    1 1 0 1 1 0 0 1 1 1 0 0 1 0 0,    ...

Elk van deze constructies resulteert in de rij hieronder:

1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0 ... (OEIS A014577)





## 94 Harmonische rij

De harmonische rij wordt gedefinieerd als  $u_n = \frac{1}{n}$ , dus dit geeft de rij:  $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7} \dots$

Hoewel de algemene term steeds kleiner wordt en nadert tot nul, wordt de som van deze getallen willekeurig groot. De divergentie gaat wel ontzettend traag; zo is de som van de eerste  $10^{43}$  termen is nog steeds kleiner dan 100.

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \dots \rightarrow \infty$$

De  $n^{\text{de}}$  partieelsom van deze harmonische reeks heet het harmonische getal,  $H_n$  genoteerd. Deze harmonische getallen spelen een belangrijke rol in combinatoriek, algebra en analyse; zo zijn ze verwant met de gammafunctie  $\Gamma$  (zie 96, blz. 73) en de constante van Euler-Mascheroni  $\gamma$  (zie ??, blz. ??) volgens dit verband, dat tevens toelaat harmonische getallen te definiëren voor niet-natuurlijke  $n$ -waarden:

$$H_n - \gamma = \frac{\Gamma'(n+1)}{\Gamma(n+1)}$$

Een voortbrengende functie voor de harmonische getallen is:

$$\sum_{n=0}^{\infty} H_n x^n = \frac{-\ln(1-z)}{1-z}$$

In 2002 bewees Jeffrey Lagarias dat de vermaarde Riemannhypothes (zie ??, blz. ??) equivalent is met de onverwachte elementaire uitspraak dat  $\sigma(n) \leq H_n + \ln(H_n) \cdot e^{H_n}$  waar is voor elke natuurlijke  $n > 0$ , enkel met gelijkheid voor  $n = 1$ . Hierin staat  $\sigma(n)$  voor de som van alle delers van  $n$ .

Als we de termen uit de harmonische reeks laten alterneren, convergeert de reeks wel.

$$\sum_{k=1}^{\infty} \frac{-(-1)^k}{k} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \dots = \ln 2$$

De harmonische reeks vormt tevens de sleutel tot de oplossing van volgend raadsel:

EEN MIER BEGINT TE KRUIPEN OVER EEN RUBBEREN KOORD MET EEN LENGTE VAN 1 KM, NAAR HET ANDERE UITEINDE. ZIJN SNELHEID IS 1 CM PER SECONDE. TEGELIJKERTIJD REKT HET KOORD 1 KM PER SECONDE UIT, DUS NA 1 SECONDE IS HET 2 KM LANG, NA 2 SECONDEN 3 KM, ETC. ZAL DE MIER OOIT HET EIND VAN HET KOORD BEREIKEN?

De afstand die de mier aflegt, blijkt gelijk te zijn aan de harmonische reeks. Omdat die divergeert, moet de mier uiteindelijk, weliswaar na een kolossale tijdspanne, het uiteinde van het koort bereiken.

## 95 Constante van Euler

De eerste wiskundige die  $e$  als een welbepaalde constante beschouwde was Gottfried Leibniz, in 1690, die de notatie  $b$  gebruikte. Het was echter Leonhard Euler die de moderne notatie  $e$  introduceerde, oorspronkelijk

in een brief naar Christian Goldbach in 1731 en later in zijn werk *Introductio in Analysin Infinitorum* in 1748. Waarschijnlijk leidde hij de letter  $e$  af van “exponentieel”.

$$e = 2,7182818284590452353602874713526624977572470936999595749669676277240766303535475945 \dots$$

Al in 1737 kon Euler aantonen dat  $e$  en  $e^2$  irrationaal zijn. Johann Lambert bewees in 1768 een sterker resultaat: voor elk rationaal getal  $q \neq 0$  is  $e^q$  irrationaal. Het bewijs dat  $e$  ook transcendent is (d.w.z. geen wortel van een eindige veelterm met gehele coëfficiënten), werd pas gevonden in 1873 door Charles Hermite.

De eigenschap van  $e$  in verband met exponentiële functies is eenvoudig maar belangrijk:  $f(x) = e^x$  is de enige functie (op de triviale  $f(x) = 0$  na) die invariant blijft onder afleiden.

$$D e^x = e^x, \quad \int e^x dx = e^x + c$$

Dit impliceert de volgende eigenschap, die vaak als definitie gebruikt wordt:

$$e = \lim_{n \rightarrow +\infty} \left( 1 + \frac{1}{n} \right)^n$$

Deze klassieke definitie heeft als nadeel dat ze zeer traag convergeert. Zo is voor  $n = 10000$  de benadering slechts nauwkeurig tot drie decimalen. Met deze efficiëntere formule rekende Euler 23 correcte decimalen uit.

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

Een ongewone limiet voor  $e$ :

$$e = \lim_{n \rightarrow \infty} \left( \frac{(n+1)^{n+1}}{n^n} - \frac{n^n}{(n-1)^{n-1}} \right)$$

Er bestaan tevens verschillende oneindige producten voor  $e$ , zoals deze van Eugène Catalan uit 1873:

$$e = \frac{2}{1} \cdot \sqrt{\frac{4}{3}} \cdot \sqrt[4]{\frac{6 \cdot 8}{5 \cdot 7}} \cdot \sqrt[8]{\frac{10 \cdot 12 \cdot 14 \cdot 16}{9 \cdot 11 \cdot 13 \cdot 15}} \cdot \dots$$

Dit product convergeert echter extreem traag, net als deze gelijkaardige formule, het product van Pippenger.

$$e = 2 \cdot \sqrt{\frac{2}{1}} \cdot \sqrt[4]{\frac{2 \cdot 4}{3 \cdot 3}} \cdot \sqrt[8]{\frac{4 \cdot 6 \cdot 6 \cdot 8}{5 \cdot 5 \cdot 7 \cdot 7}} \cdot \dots$$

Nog een andere methode is via deze recursieve rij:

$$u_1 = 1, \quad u_{n+1} = (n+1) \cdot (u_n + 1), \quad e = \prod_{n=0}^{\infty} \frac{u_n + 1}{u_n}$$

$e$  heeft nog veel meer prachtige eigenschappen. Zo kun je in het rekenkundig gemiddelde  $A_n$  en het meetkundig gemiddelde  $G_n$  van de eerste  $n$  natuurlijke getallen een relatie vinden met  $e$ .

$$A_n = \frac{1 + 2 + 3 + \dots + n}{n}, \quad G_n = \sqrt[n]{1 \cdot 2 \cdot 3 \cdot \dots \cdot n}, \quad \lim_{n \rightarrow \infty} \frac{A_n}{G_n} = \frac{e}{2}$$

En zelfs bij priemgetallen  $p$  komt  $e$  om het hoekje kijken, hoewel ook deze convergentie zeer traag gaat:

$$\lim_{n \rightarrow \infty} \left( \prod_{p \leq n} \sqrt[p]{p} \right) = e$$

## 96 Gammafunctie

De faculteitsfunctie  $n!$  wordt gedefinieerd als het product van alle positieve gehele getallen ten hoogste  $n$ , waarbij  $n$  een positief geheel getal is. De faculteit wordt vaak recursief gedefinieerd en deze definitie is een typevoorbeeld voor recursie in de informatica.

$$n! = \prod_{k=1}^n k \quad \text{of} \quad n! = \begin{cases} 1 & \text{als } n = 0 \\ n \cdot (n-1)! & \text{als } n > 0 \end{cases}$$

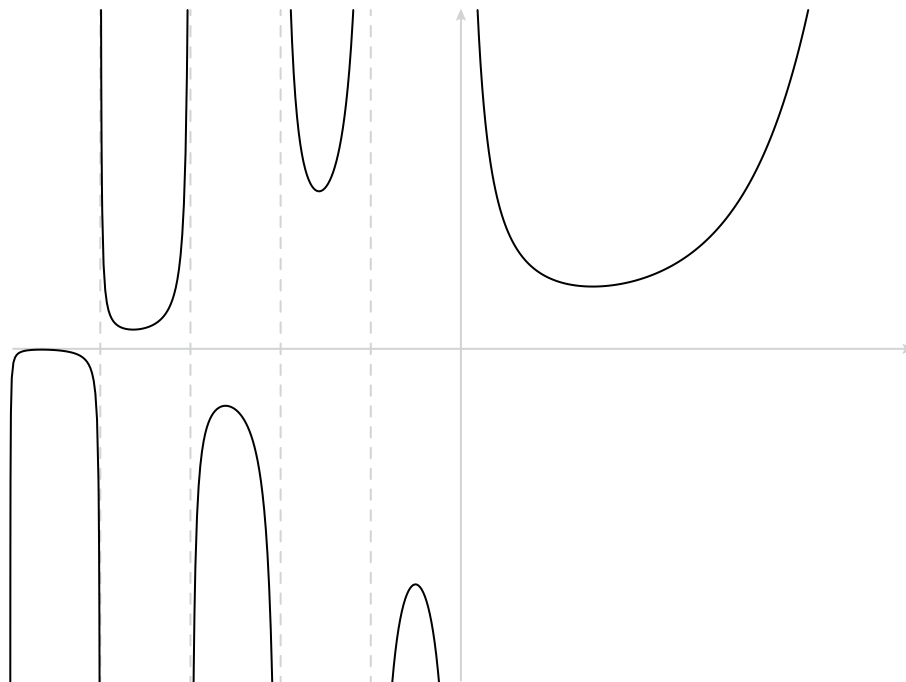
Men definieert voor de volledigheid in de combinatoriek  $0! = 1$ . De faculteiten vormen de rij:

1, 1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, 39916800, 479001600, 6227020800 . . . (OEIS A000142)

Faculteiten zijn cruciaal in de combinatoriek en in reeksontwikkelingen. Vanwege hun grote belang probeerde men het domein van de faculteitsfunctie uit te breiden van  $\mathbb{N}$  naar gans  $\mathbb{R}$  of zelfs  $\mathbb{C}$ . In het complexe vlak bestaat er juist één holomorfe functie die de discrete faculteit interpoleert, de gammafunctie geheten. Deze  $\Gamma(z)$  heeft geen nulpunten, maar wel een pool in elk negatief geheel getal (0 inclusief) en wordt vaak gedefinieerd via de volgende integraalrepresentatie:

$$\Gamma(z) = \int_0^{+\infty} t^{z-1} e^{-t} dt$$

Voor natuurlijke  $n$  geldt dan dat  $n! = \Gamma(n+1)$ , zodat de gammafunctie inderdaad samenvalt met de faculteit, op een translatie van het argument na; deze nogal ongelukkige notatie danken we aan Adrien-Marie Legendre. Carl Friedrich Gauss verkoos een alternatieve notatie  $\Pi(x)$  voor  $\Gamma(x+1)$ , zodat  $\Pi(n) = n!$  voor natuurlijke  $n$ .



De eerste die het interpolatieprobleem (gesteld door Daniel Bernoulli en Christian Goldbach rond 1720) oploste, was Leonhard Euler. Hij schreef een brief naar Goldbach in oktober 1729 over z'n eerste formule, in de vorm van een oneindig product. Goldbach ontving echter al gauw een tweede brief in januari 1730 over Eulers ontdekking van de integraalvorm.

$$\Gamma(z) = \frac{1}{z} \cdot \prod_{n=1}^{\infty} \frac{\left(1 + \frac{1}{n}\right)^z}{1 + \frac{z}{n}} \quad \text{of} \quad \Gamma(z) = \int_0^1 \left(\ln \frac{1}{t}\right)^{z-1} dt$$



De volgende formules gelden voor positieve gehele  $n$ -waarden, ter berekening van “halve gehele getallen”.

$$\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}, \quad \Gamma\left(\frac{1}{2} + n\right) = \frac{(2n)!}{4^n n!} \cdot \sqrt{\pi}, \quad \Gamma\left(\frac{1}{2} - n\right) = \frac{(-4)^n n!}{(2n)!} \cdot \sqrt{\pi}$$

Enkele symmetrie-eigenschappen:

$$\Gamma(z) \cdot \Gamma(-z) = \frac{-\pi}{z \sin(\pi z)}, \quad \Gamma(z) \cdot \Gamma(1-z) = \frac{\pi}{\sin(\pi z)}$$

Ook handig is deze verdubbelingsformule, soms de relatie van Legendre genoemd.

$$\Gamma(z) \cdot \Gamma\left(z + \frac{1}{2}\right) = 2^{1-2z} \cdot \sqrt{\pi} \cdot \Gamma(2z)$$

Tot slot geldt nog dit verband met de Riemann-zètafunctie (zie ??, blz. ??).

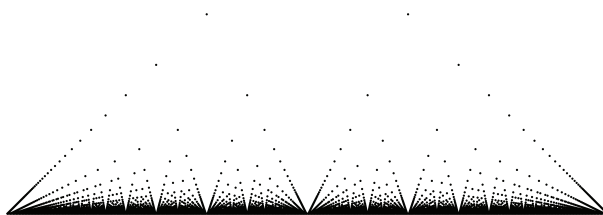
$$\Gamma\left(\frac{z}{2}\right) \cdot \frac{1}{\sqrt{\pi z}} \cdot \zeta(z) = \Gamma\left(\frac{1-z}{2}\right) \cdot \frac{1}{\sqrt{\pi^{1-z}}} \cdot \zeta(1-z)$$

## 97 Popcornfunctie

Deze functie van Duits wiskundige Carl Johannes Thomae staat bekend als de popcornfunctie, de regendruppel-functie of de “sterren boven Babylon”-functie (zo genoemd door John Conway) en wordt als volgt gedefinieerd op het open interval  $]0, 1[$ :

$$f(x) = \begin{cases} \frac{1}{q} & \text{als } x \in \mathbb{Q} \text{ en } x = \frac{p}{q} \text{ in z'n eenvoudigste vorm} \\ 0 & \text{als } x \notin \mathbb{Q} \end{cases}$$

De popcornfunctie heeft de opmerkelijke eigenschap dat ze discontinu is in elk rationaal getal, maar continu in elk irrationaal getal! Een plot ziet er als volgt uit:



## 98 Van Cusa's $\pi$ -formule

Duits theoloog en filosoof Nicolaas van Cusa was ook geboeid door wiskunde, astronomie en taalwetenschap, en liet na zijn dood in 1464 deze formule voor  $\pi$  na, die gebruik maakt van twee rijen.

$$a_0 = 0, \quad a_{n+1} = \frac{a_n + b_n}{2}$$

$$b_0 = \frac{1}{4}, \quad b_{n+1} = \sqrt{a_{n+1} \cdot b_n}$$

Merk de gelijkennis op met het rekenkundig en meetkundig gemiddelde. Het verband met  $\pi$  is eenvoudig:

$$\lim_{n \rightarrow +\infty} \frac{1}{2a_n} = \lim_{n \rightarrow +\infty} \frac{1}{2b_n} = \pi$$

## 99 Al-Kashi's $\pi$ -formule

Ghiyāth al-Dīn Jamshīd Mas'ūd al-Kāshī, beter bekend als al-Kashi, stond bekend als één van de beste wiskundigen uit de islamitische wereld en leefde van 1380 tot 1429. Zoals toen gebruikelijk was hij tevens astronoom. Dankzij zijn formule brak hij het record op decimalen van  $\pi$ ; hij vond er 16, berekend in het zestigtalig talstelsel, en dit record werd pas zo'n 200 jaar later verbroken door Ludolph van Ceulen, die er 20 kon berekenen.

De methode waarmee al-Kashi deze formule ontdekte, is gelijkaardig aan de klassieke techniek van Archimedes en steunt op omtrekken van regelmatig veelhoeken, die een cirkel (en zo  $\pi$ ) benaderen.

$$P_0 = 1, \quad P_{n+1} = \sqrt{2 - \sqrt{4 - P_n^2}}, \quad \lim_{n \rightarrow \infty} (3 \cdot 2^n \cdot P_n) = \pi$$

Al-Kashi zocht een goede benadering voor  $\pi$  om zijn astronomische benaderingen zo nauwkeurig mogelijk te kunnen berekenen. Naar eigen zeggen hield dit concreet in dat voor een cirkel 600.000 keer zo groot als de evenaar van de aarde, de benaderingsfout kleiner moest zijn dan de dikte van een paardenhaar. Helaas toonde Kepler zo'n tweehonderd jaar later aan dat de hemellichamen zich in een ellipsvormige baan bewegen, en niet in perfecte cirkelbanen zoals Al-Kashi aannam.

## 100 Power Tower

De Power Tower van  $x$  met orde  $n$  wordt gedefinieerd als  $x \uparrow\uparrow n$  (gebruik makend van Knuths pijlhoognotatie; zie 305, blz. 298). Voluit geschreven is de oorsprong van de naam duidelijk:

$$x \uparrow\uparrow n = \underbrace{x^{x^{\dots^x}}}_{n \text{ kopieën van } x}$$

Met name wat er met deze uitdrukking gebeurt als  $n$  naar oneindig nadert, is interessant. Er geldt namelijk dat deze limiet enkel convergeert voor  $e^{-e} \leq x \leq e^{\frac{1}{e}}$ , zoals Leonhard Euler ontdekte en bewees. De grenswaarden convergeren zelf respectievelijk naar  $\frac{1}{e}$  en  $e$ . Voor andere waarden krijg je bijvoorbeeld:

$$\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\dots}}} = 2$$

## 101 Sophomore's dream

"Sophomore's dream" slaat op de volgende twee gelijkheden, ontdekt door Johann Bernoulli in 1697.

$$\int_0^1 \frac{dx}{x^x} = \sum_{n=1}^{\infty} \frac{1}{n^n}, \quad \int_0^1 x^x dx = - \sum_{n=1}^{\infty} \frac{1}{(-n)^n}$$

De twee uitdrukkingen hebben als waarde, respectievelijk:

- 1, 29128599706266354040728259059560054149861936827452231731000244513 ...
- 0, 78343051071213440705926438652697546940768199014693095825541782270 ...

## 102 Fourierreeksen

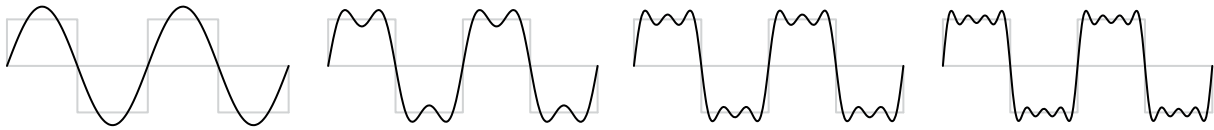
Jean-Baptiste Joseph Fourier was tot zijn dood in 1830 secretaris van de *Académie Française*. Verder werkend op een resultaat van Euler bedacht hij het principe van de Fourieranalyse, die een prominente rol speelt in de fysica door hun goniometrisch verband met golven. De Fouriertransformaties worden ook intensief gebruikt bij

bijvoorbeeld het oplossen van differentiaalvergelijkingen.

Van Leonhard Euler is volgend resultaat afkomstig, zonder vermelding hoe hij dit gevonden had of dat de reeks enkel geldig is voor  $-\pi < x < \pi$ .

$$\frac{x}{2} = \sin x - \frac{\sin 2x}{2} + \frac{\sin 3x}{3} - \frac{\sin 4x}{4} + \frac{\sin 5x}{5} - \frac{\sin 6x}{6} + \dots$$

Fourier vermoedde nu dat voor elke integreerbare functie zo'n reeks in sinussen en cosinussen kan gevonden worden, die geldt in het interval  $[-\pi, \pi]$ . Ondanks ongelovige protesten bij contemporaine wiskundigen bewees Johann Dirichlet dat dit inderdaad geldt voor periodieke functies, wat dan verder kan worden uitgebreid. De coëfficiënten bij deze sinussen en cosinussen worden Fouriercoëfficiënten genoemd en kunnen relatief eenvoudig expliciet worden uitgerekend via een bepaalde integraal.



$$f(x) = a_0 + \sum_{n=1}^{\infty} (a_n \sin nx + b_n \cos nx)$$

Fourier gaf de volgende formules voor de coëfficiënten in de Fourierreeks voor een integreerbare functie  $f(x)$  met  $x \in [-\pi, \pi]$ :

$$a_0 = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x) dx$$

$$a_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin(nx) dx$$

$$b_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos(nx) dx$$

Uit deze formules volgt dat voor even functies alle coëfficiënten bij een sinus 0 zijn, en voor oneven functies zijn die bij de cosinussen 0. Enkele voorbeelden:

- $|x| = \frac{\pi}{2} - \frac{4}{\pi} \left( \cos x + \frac{\cos 3x}{3^2} + \frac{\cos 5x}{5^2} + \frac{\cos 7x}{7^2} + \dots \right)$
- $x^2 = \frac{\pi^2}{3} - 4 \left( \cos x - \frac{\cos 2x}{2^2} + \frac{\cos 3x}{3^2} - \frac{\cos 4x}{4^2} + \frac{\cos 5x}{5^2} - \dots \right)$
- $\tan \frac{x}{2} = 2 \sin x - 2 \sin 2x + 2 \sin 3x - 2 \sin 4x + 2 \sin 5x - \dots$

## 103 Parkeerconstante van Rényi

Het parkeerprobleem van Alfréd Rényi vraagt het volgende.

GEGEVEN DE LENGTE VAN EEN STRAAT. ER PARKEREN AUTO'S (MET EENHEIDSLENGTE) OP EEN WILLEKEURIGE VRIJE POSITIE OP DE STRAAT, TOTDAT ER GEEN NIEUWE MEER BIJ KUNNEN. WAT IS DAN DE GEMIDDELDE DICHTHEID VAN DE AUTO'S?

Beschouwen we het probleem analytisch op het gesloten interval  $[0, x]$  als straat. Voor het gemiddelde aantal eendimensionale auto's met eenheidslengte,  $M(x)$ , kan dan de volgende relatie afgeleid worden

$$M(x) = \begin{cases} 0 & \text{voor } 0 \leq x < 1 \\ 1 + \frac{2}{x-1} \int_0^{x-1} M(y) dy & \text{voor } x \geq 1 \end{cases}$$

De gemiddelde dichtheid  $m$ , voor  $x$  voldoende groot, wordt dan:

$$m = \lim_{x \rightarrow \infty} \frac{M(x)}{x} = \int_0^{\infty} \exp\left(-2 \int_0^x \frac{1 - \exp(-y)}{y} dy\right) dx \approx 0,74759792025341143 \dots$$

Gemiddeld vullen de auto's dus een kleine driekwart van de straat. De decimale ontwikkeling van de parkeerconstante is terug te vinden in OEIS A050996. Ilona Palásti uitte het volgend vermoeden voor een tweedimensionale variant, maar tot op vandaag is deze bewezen noch weerlegd:

$$\lim_{x, y \rightarrow \infty} \frac{M(x, y)}{xy} = m^2$$

## 104 Constante van Gauss

De constante van Gauss, vernoemd naar de wiskundige Carl Friedrich Gauss en genoteerd als  $G$ , wordt gedefinieerd als de omgekeerde van het rekenkundig-meetkundig gemiddelde van 1 en  $\sqrt{2}$ . De decimalen staan in OEIS A014549.

$$G = \frac{1}{\mathcal{AG}(1, \sqrt{2})} \approx 0,8346268416740731 \dots$$

Het rekenkundig-meetkundig gemiddelde is lastig expliciet te bepalen. Bereken het rekenkundig gemiddelde  $\mathcal{A}_1$  en het meetkundig gemiddelde  $\mathcal{G}_1$  van twee getallen  $x$  en  $y$  (zie 45, blz. 34), en herhaal deze berekeningen met de gevonden gemiddelden. Doe dit voldoende en de twee gemiddelden zullen convergeren naar eenzelfde getal, per definitie het rekenkundig-meetkundig gemiddelde  $\mathcal{AG}(x, y)$ .

Gauss ontdekte in 1799 zijn constante via een bepaalde integraal, die een verband schept met de booglengte van de lemniscaat (zie 194, blz. 153).

$$G = \frac{2}{\pi} \cdot \int_0^1 \frac{dx}{\sqrt{1-x^4}}$$

$G$  is transcendent en kan worden gebruikt om de gammafunctie van  $\frac{1}{4}$  (zie 96, blz. 73) uit te drukken.

$$\Gamma\left(\frac{1}{4}\right) = \sqrt{2G} \cdot \sqrt{2\pi^3}$$

Volgende bepaalde integralen maken ook gebruik van Gauss' constante.

$$\frac{1}{G} = \int_0^{\frac{\pi}{2}} \sqrt{\sin x} dx = \int_0^{\frac{\pi}{2}} \sqrt{\cos x} dx$$

Ook de hyperbolische functies bevatten verbanden met  $G$ :

$$G = \prod_{n=1}^{\infty} \tanh^2\left(\frac{\pi n}{2}\right) = \int_0^{\infty} \frac{dx}{\sqrt{\cosh(\pi x)}}$$

Tot slot kan  $G$  gemakkelijk berekend worden als het kwadraat van deze snel convergerende reeks.

$$G = \left[ \sum_{n=-\infty}^{\infty} (-1)^n \cdot e^{-\pi n^2} \right]^2$$

## 105 Formule van Wallis

Deze formule, gevonden door John Wallis in 1655, drukt  $\pi$  uit als een oneindig product:

$$\frac{\pi}{2} = \left( \frac{2 \cdot 2}{1 \cdot 3} \right) \cdot \left( \frac{4 \cdot 4}{3 \cdot 5} \right) \cdot \left( \frac{6 \cdot 6}{5 \cdot 7} \right) \cdot \left( \frac{8 \cdot 8}{7 \cdot 9} \right) \cdot \left( \frac{10 \cdot 10}{9 \cdot 11} \right) \cdots$$

Vreemd genoeg convergeert dit product naar een totaal ander resultaat als elke tweede factor geschrapt wordt!

$$\sqrt{2} = \left( \frac{2 \cdot 2}{1 \cdot 3} \right) \cdot \left( \frac{6 \cdot 6}{5 \cdot 7} \right) \cdot \left( \frac{10 \cdot 10}{9 \cdot 11} \right) \cdots$$

## 106 Een, twee, drie, $\pi$

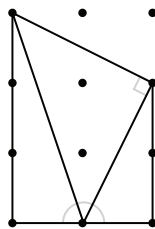
Als en slechts als  $a + b + c$  een veelvoud is van  $\pi$ , geldt de volgende identiteit voor reële variabelen:

$$\tan a + \tan b + \tan c = \tan a \cdot \tan b \cdot \tan c$$

Ook omgekeerd, als de som en het product van drie reële getallen identiek zijn (zoals voor  $\frac{21}{22}$ ,  $\frac{42}{11}$  en  $\frac{231}{128}$ ), dan zijn deze getallen de tangensen van drie hoeken die sommeren tot een veelvoud van  $\pi$ . Er bestaat precies één drietal natuurlijke getallen met deze eigenschap, namelijk (1, 2, 3). Dit impliceert dus:

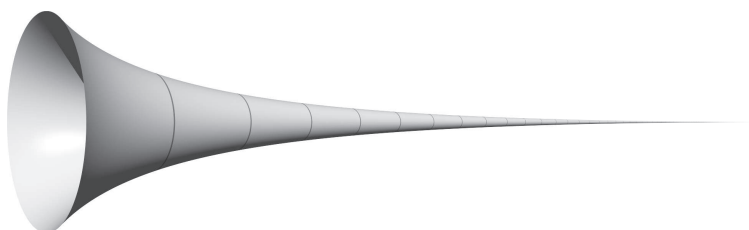
$$\text{Bgtan } 1 + \text{Bgtan } 2 + \text{Bgtan } 3 = \pi$$

Deze bekoorlijke vergelijking heeft ook een eenvoudig bewijs zonder woorden.



## 107 Hoorn van Gabriël

De hoorn van Gabriël is een bizarre meetkundige entiteit, voor het eerst beschreven door Evangelista Torricelli en daardoor ook de trompet van Torricelli genoemd. De eerste naam verwijst naar de aartsengel Gabriël, die de hoorn blaast op de Dag des Oordeels, en associeert het goddelijke (of oneindige) met het eindige. Ze wordt gevormd door de grafiek van de functie  $f(x) = \frac{1}{x}$  om de  $x$ -as te wentelen, beperkt tot het domein  $x \geq 1$  om de asymptoot op  $x = 0$  te vermijden. Het resultaat is deze oneindig lange figuur.



Torricelli wist hiervan het volume en de oppervlakte te berekenen met behulp van het principe van Cavalieri, maar dit gaat ook via de later ontdekte, analytische formules voor omwentelingslichamen en -oppervlakken. De oppervlakte van de hoorn, beperkt tot  $x \in [1, a]$  wordt:

$$A = 2\pi \int_1^a f(x) \sqrt{1 + \left(\frac{df(x)}{dx}\right)^2} dx = 2\pi \int_1^a \frac{\sqrt{1 + \frac{1}{x^4}}}{x} dx \geq 2\pi \int_1^a \frac{dx}{x} = 2\pi \ln a$$

Met andere woorden, de uiteindelijke hoorn van Gabriël (met  $a \rightarrow \infty$ ) zal een onbegrensde oppervlakte hebben. Wanneer we nu echter het volume uitrekenen, verkrijgen we iets onverwachts.

$$V = \pi \int_1^a f(x)^2 dx = \pi \int_1^a \frac{dx}{x^2} = \pi \cdot \left(1 - \frac{1}{a}\right)$$

Laat hier  $a$  naar oneindig naderen, en het volume van Gabriëls hoorn nadert naar  $\pi$ , in plaats van onbeperkt toe te nemen. Dit leidt tot de paradoxale conclusie dat het wél mogelijk is de hoorn vol te gieten met een eindige hoeveelheid verf (namelijk  $\pi$  eenheden), maar onmogelijk hem volledig te beschilderen!

## 108 Conways 13-functie

Een functie waarop de conclusie van de tussenwaardestelling\* van kracht is, wordt een Darbouxfunctie genoemd, naar Jean-Gaston Darboux. Concreet betekent de tussenwaardestelling dat continuïteit voldoende is om van een Darbouxfunctie te kunnen spreken.

Continuïteit is echter geen nodige voorwaarde, zoals John Conway illustreerde via een monsterlijke Darboux-functie, die *nergens* continu is. De constructie is nogal gesofisticeerd. Conways functie  $C_{13}$  wordt gedefinieerd als de functie die het volgende doet met een reëel argument  $x$ :

- Schrijf  $x$  uit in basis 13, met als symbolen de gebruikelijke cijfers, een plus, een min en een komma.
- Ga na of het getal eindigt in de vorm  $(x_0 x_1 x_2 \dots x_n y_0 y_1 y_2 \dots)$  waarin  $x_0$  een plus- of minsymbool is,  $y_0$  een komma en de overige cijfers beperkt zijn tot de klassieke decimale cijfers.
- Als dat wel het getal is, kan de beschouwde staart van deze representatie geïnterpreteerd worden als een reëel getal in basis 10, wat dan de functiewaarde  $C_{13}(x)$  wordt.
- Als dat niet het geval is, wordt  $C_{13}(x) = 0$ .

Een voorbeeld:

$$C_{13}(0,12-89++6+2-34,,11111\dots) = 0$$

Merk op dat de eerste komma na de nul als het normale scheidingssymbool gebruikt wordt en de overige twee als cijfers van het getal. Een getal als het volgende krijgt echter wel een speciale functiewaarde (cf. de komma):

$$C_{13}(0,12-89++6+2-34,11111\dots) = -34,11111\dots$$

Zodoende wordt elk reëel getal bereikt in elk gesloten, willekeurig klein interval  $[a, b]$ , terwijl de functie in geen enkel punt continu is. Desalniettemin worden overaftelbaar veel getallen afgebeeld op 0.

## 109 Volterra's functie

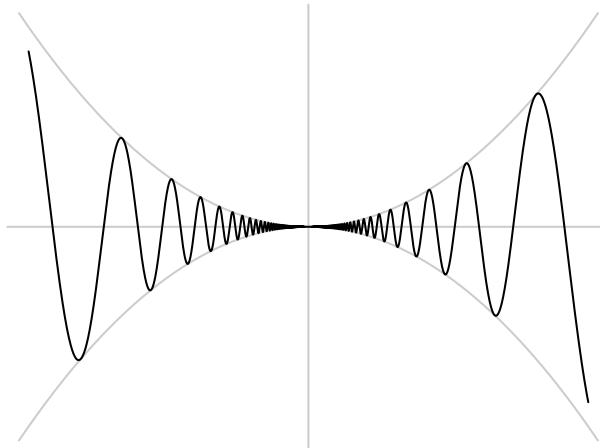
De functie van Volterra  $V$  is een bizarre reële functie, vernoemd naar de Italiaan Vito Volterra, die voldoet aan de volgende eigenschappen:

\*Een functie  $f$  continu in  $[a, b]$  neemt alle mogelijke waarden tussen  $f(a)$  en  $f(b)$  aan.

- $V$  is overal continu en afleidbaar
- $V'$  is overal begrensd
- $V'$  is *niet* Riemann-integreerbaar

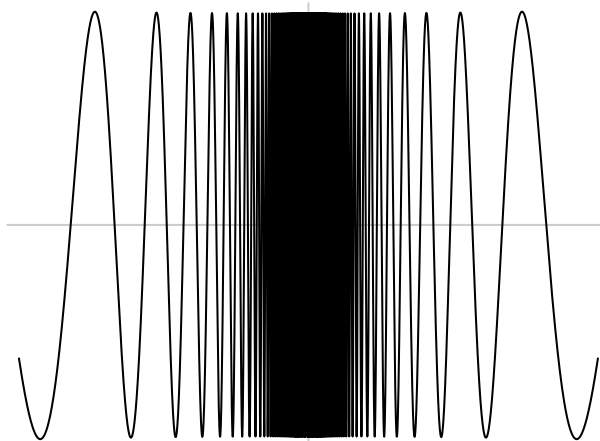
Volterra's functie is dus wel afleidbaar, maar de afgeleide ervan is niet opnieuw integreerbaar! Ze wordt geconstrueerd met behulp van de Smith-Volterra-Cantorverzameling (SVC) en de volgende functie  $h$ , die overal gedefinieerd en continu is.

$$h(x) = \begin{cases} x^2 \cdot \sin\left(\frac{1}{x}\right) & \text{voor } x \neq 0 \\ 0 & \text{voor } x = 0 \end{cases}$$

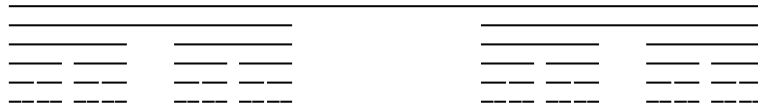


De afgeleide van deze  $h$  blijkt discontinu in de oorsprong. De rij  $\frac{1}{2\pi}, \frac{1}{4\pi}, \frac{1}{6\pi}$  etc. convergeert namelijk naar 0, maar hun functiewaarden (in  $h'$ ) naar 1 in plaats van  $h'(0)$ .

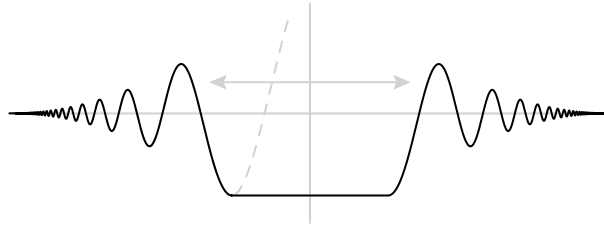
$$h'(x) = \begin{cases} 2x \cdot \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right) & \text{voor } x \neq 0 \\ 0 & \text{voor } x = 0 \end{cases}$$



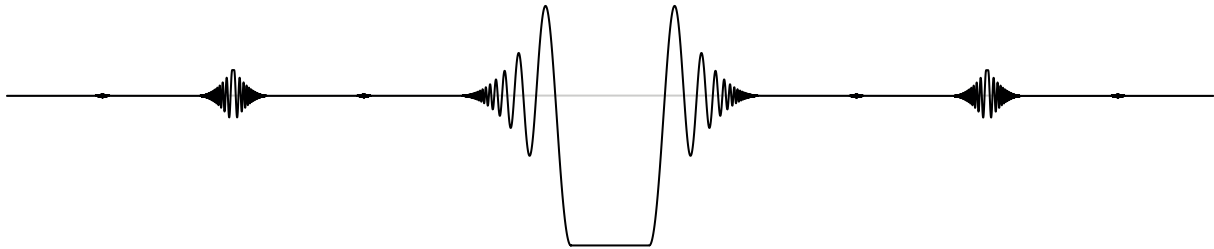
Het tweede ingrediënt voor Volterra's functie is de SVC, de Smith-Volterra-Cantorverzameling (genoemd naar Henry Smith, Vito Volterra en Georg Cantor). Deze wordt op gelijkaardige wijze opgebouwd als het klassieke Cantorstof (zie 207, blz 166), namelijk door herhaaldelijk intervallen weg te knippen uit het gesloten interval  $[0, 1]$ . Eerst wordt het centrale interval met lengte  $\frac{1}{4}$  verwijderd, daarna het centrale interval in elk van de twee stukken met lengte  $\frac{1}{16}$ , dan  $\frac{1}{64}$  en zo verder. Telkens wordt er een deelinterval met lengte  $\frac{1}{2^{2n}}$  uit de overblijvende  $2^{n+1}$  stukken gehaald. Het limietgeval van dit proces, de punten die nooit verwijderd worden, is de SVC. Echter, daar waar het Cantorstof maat 0 heeft, bezit de SVC maat  $\frac{1}{2}$ , en dit speelt een sleutelrol in de eigenschappen van Volterra's functie.



We beginnen bij een constante functie  $f_0 = 0$ . Zoek nu in de functie  $h$  de laatste  $x$ -waarde ten hoogste  $\frac{1}{8}$  waar de afgeleide 0 is en breidt die vanaf daar constant uit tot aan  $\frac{1}{8}$ . Spiegel dit gedeelte om de as  $x = \frac{1}{8}$ , en plak het stuk tussen 0 en  $\frac{1}{4}$  op  $f_0$  zoals bij de constructie van SVC: dit wordt  $f_1$ . Merk op dat  $f_1$  nog steeds afleidbaar is. Herhaal deze stappen met kleinere stukjes uit  $h$ , geplakt op de overeenkomstige SVC-gaten; het limietgeval definieert de functie  $V$  van Volterra.



De uiteindelijke functie ziet er als volgt uit:



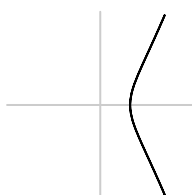
Omdat een functie slechts Riemann-integreerbaar is wanneer ze bijna overal continu is (in de zin dat de maat van eventuele discontinuïteiten 0 moet zijn), is  $V'$  niet integreerbaar. Immers, alle eindpunten van SVC leveren een discontinuïteit in  $V'$ , en hun maat is groter dan nul.

## 110 Elliptische krommen

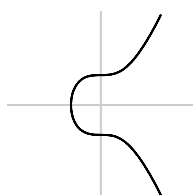
Elliptische krommen spelen een centrale rol in getaltheorie en vormen een niet te onderschatten werkterrein in huidig onderzoek. Zij vormen de sleutel tot een bewijs van de laatste stelling van Fermat, vinden toepassingen in cryptografie, kunnen gebruikt worden om gehele getallen te ontbinden in factoren, etc. Elke elliptische kromme kan worden voorgesteld als een algebraïsche kromme van de volgende vorm:

$$y^2 = x^3 + ax + b \quad \text{met } 4a^3 + 27b^2 \neq 0$$

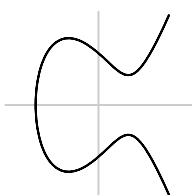
De voorwaarden op  $a$  en  $b$  zijn afkomstig van de elliptische discriminant  $\Delta = -16(4a^3 + 27b^2)$  en verzekeren dat de kromme geen keerpunten heeft en zichzelf niet snijdt. Wanneer  $\Delta$  strikt positief is, bestaat de grafiek uit twee losse componenten, terwijl bij strikt negatieve  $\Delta$  de grafiek samenhangend is. Enkele voorbeelden:



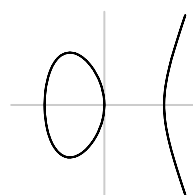
$$y^2 = x^3 - 1$$



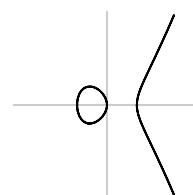
$$y^2 = x^3 + 1$$



$$y^2 = x^3 - 3x + 3$$



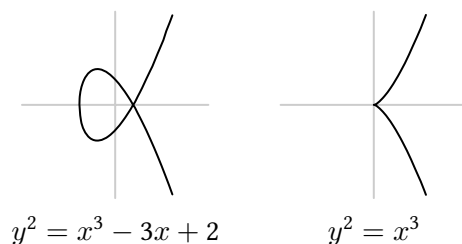
$$y^2 = x^3 - 4x$$



$$y^2 = x^3 - x$$

Voor de volgende krommen geldt  $\Delta = 0$ , waardoor ze niet singulier zijn en dus niet "elliptisch". Inderdaad, de eerste snijdt zichzelf, en de tweede bevat een keerpunt in de oorsprong.





Louis Mordell bewees dat het aantal punten op zo'n kromme met gehele coëfficiënten steeds eindig is.

Het vermoeden van Taniyama-Shimura-Weil uit 1955 legde een belangrijk verband tussen de elliptische krommen en modulaire vormen. Andrew Wiles bewees dit vermoeden in 1994 voor semistabiele krommen, wat voldoende was om de laatste stelling van Fermat (zie ??, blz. ??) te bewijzen. In 2001 breidden Christophe Breuil, Brian Conrad, Fred Diamond en Richard Taylor de technieken van Wiles uit ter bewijs voor het algemene vermoeden, sindsdien de modulariteitsstelling genoemd.

Zoals Neal Koblitz en Victor Miller in 1985 opmerkten, biedt de algebraïsche structuur van elliptische krommen (zie 303, blz. 293) over eindige velden toepassingen in public-key cryptografie. Een andere nuttige toepassing doet zich voor bij het ontbinden van gehele getallen in priemfactoren. Lenstra elliptic curve factorization of ECM is een van de snelste gekende factorisatiealgoritmen, zeker voor het opsporen van kleine priemfactoren omdat zijn runtime voornamelijk bepaald wordt door de grootte van de kleinste factor  $p$  i.p.v. het te factoriseren getal:

$$\mathcal{O}(e^{\sqrt{(2+o(1))(\ln p \ln \ln p)}})$$

## 111 Vraagtekenfunctie van Minkowski

Hermann Minkowski definieerde in 1904 zijn vraagtekenfunctie, genoteerd als  $?(x)$ , die eigenaardige eigenschappen vertoont. Kwadratisch irrationale getallen worden afgebeeld op de rationale getallen in het eenheidsinterval, terwijl de rationale getallen worden afgebeeld op dyadische rationale getallen.

De kwadratisch irrationale getallen zijn irrationale oplossingen van vierkantsvergelijkingen met gehele coëfficiënten en zijn zodoende van de onderstaande vorm. Samen met  $\mathbb{Q}$  vormen ze een deelveld van  $\mathbb{R}$ , het reëel kwadratisch veld genaamd en met  $\mathbb{Q}[\sqrt{c}]$  genoteerd. Enkel kwadratisch irrationale getallen zijn te schrijven als een periodieke kettingbreuk (zie 22, blz. 14).

$$\frac{a + b\sqrt{c}}{d} \quad \text{met } a, b, c, d \in \mathbb{Z}, b, d \neq 0, c \text{ kwadraatvrij}$$

Dyadische rationale getallen zijn breuken waarvan de noemer een macht van 2 is. Deze bepalen géén veld, daar inversen ervan over het algemeen niet van dezelfde vorm zijn, maar wel een deelring van  $\mathbb{Q}$ .

$?(x)$  voor irrationale  $x$  wordt gedefinieerd met behulp van de voorstelling als kettingbreuk:

$$?(x) = a_0 - 2 \sum_{i=1}^{\infty} \frac{(-1)^i}{2^{a_1 + \dots + a_i}} \quad \text{met } x = [a_0; a_1, a_2 \dots]$$

Voor rationale  $x$  is de definitie analoog, maar dan met een eindige kettingbreuk:

$$?(x) = a_0 - 2 \sum_{i=1}^n \frac{(-1)^i}{2^{a_1 + \dots + a_i}} \quad \text{met } x = [a_0; a_1, a_2 \dots a_n]$$

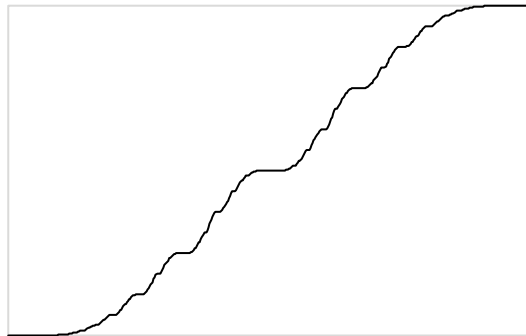
Een interessante interpretatie van  $?(x)$  bestaat erin de kettingbreuk  $[0; a_1, a_2, \dots]$  om te zetten naar een binair getal in het eenheidsinterval, als  $a_0$  nullen,  $a_1$  enen,  $a_2$  nullen,  $a_3$  enen etc.  $\frac{\sqrt{3}-1}{2}$  bijvoorbeeld, geeft de kettingbreuk  $[0; 2, 1, 2, 1, 2, 1, \dots]$ , wat overeenkomt met het binaire  $0,01001001\dots$  of  $\frac{2}{7}$  decimaal.

$$?\left(\frac{\sqrt{3}-1}{2}\right) = \frac{2}{7}$$

Voor rationale getallen kan de functie ook recursief gedefinieerd worden.

$$?\left(\frac{0}{1}\right) = 0, \quad ?\left(\frac{1}{1}\right) = 1, \quad ?\left(\frac{p+r}{q+s}\right) = \frac{1}{2}\left(?\left(\frac{p}{q}\right) + ?\left(\frac{r}{s}\right)\right) \text{ als } |ps - qr| = 1$$

Een plot van de vraagtekenfunctie illustreert de fractale aard ervan:



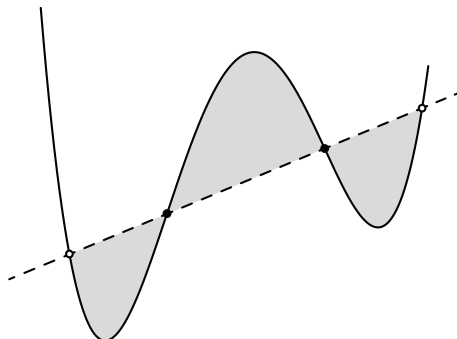
De symmetrie van de functie stemt voort uit deze functionele vergelijkingen.

$$?(x) = 1 - ?(1 - x) = 2 ?\left(\frac{x}{x+1}\right)$$

Minkowski's vraagtekenfunctie is een continue, strikt stijgende bijectie op  $[0, 1]$ , maar is niet absoluut continu. Voor "bijna alle"  $x$ -waarden is de afgeleide  $?'(x)$  0, op een verzameling met maat nul na; door deze eigenschap heet  $?(x)$  een singuliere functie.

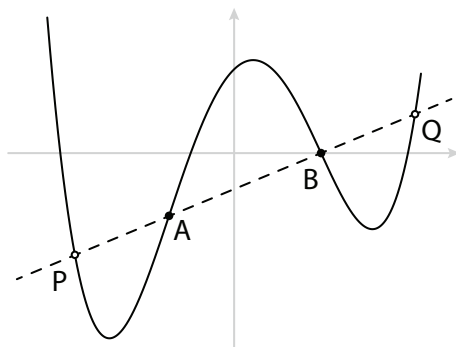
## 112 Stelling van McMullin

Lin McMullin ontdekte in 2004 een opzienbarend optreden van de gulden snede  $\varphi$  in vierdegraadspolynomen. Twee jaar eerder merkte John Mahoney op dat de rechte door de twee buigpunten van zo'n vierdegraadsfunctie drie gebieden begrenst waarvan de oppervlaktes zich verhouden als  $1 : 2 : 1$ .



McMullin ontdekte via CAS-software het volgende, nog mysterieuzere feit. Veronderstel dat de rechte door de twee buigpunten  $A$  en  $B$ , de vierdegraadsfunctie nog snijdt in de punten  $P$  en  $Q$ ; de  $x$ -coördinaten van  $P$ ,  $A$ ,  $B$  en  $Q$  heten respectievelijk  $p < a < b < q$ . Dan geldt:

$$p = \varphi \cdot a - (\varphi - 1) \cdot b \quad \text{en} \quad q = \varphi \cdot b - (\varphi - 1) \cdot a$$



Hieruit volgt dat  $b - a$  in de gulden verhouding staat tot  $a - p$  en  $q - b$ .

Op voorwaarde dat de vergelijking van de rechte op een geschikte manier wordt aangepast, blijft de stelling ook geldig voor samenvallende of zelfs complexe buigpunten: de gulden snede blijkt onvoorwaardelijk verbonden met vierdegraadspolynomen.

## 113 Algoritme van Gauss-Legendre

Het algoritme van Gauss-Legendre is een krachtige iteratiemethode om zeer snel de cijfers van  $\pi$  te berekenen. Doordat het aantal correcte decimalen per stap verdubbelt, zijn slechts 25 iteraties voldoende voor een precisie van maar liefst 45 miljoen decimalen! Een nadeel is dat deze methode geheugenintensief is. Toch werden via dit algoritme van 18 tot 20 september in 1999 de eerste 206.158.430.000 correcte decimalen berekend.

Deze versie is gebaseerd op individueel werk van Carl Friedrich Gauss en Adrien-Marie Legendre, maar wordt gecombineerd met moderne algoritmes voor vermenigvuldiging en worteltrekking. Zoals hier gepresenteerd staat ze ook bekend als het algoritme van Brent-Salamin, uitgewerkt door Richard Brent en Eugene Salamin in 1975. De beginwaarden worden als volgt ingesteld:

$$a_0 = 1, \quad b_0 = \frac{1}{\sqrt{2}}, \quad t_0 = \frac{1}{4}, \quad p_0 = 1$$

De rest van het algoritme herhaalt de volgende stappen. Merk het rekenkundig en meetkundig gemiddelde op bij de berekening van  $a_{n+1}$  respectievelijk  $b_{n+1}$ .

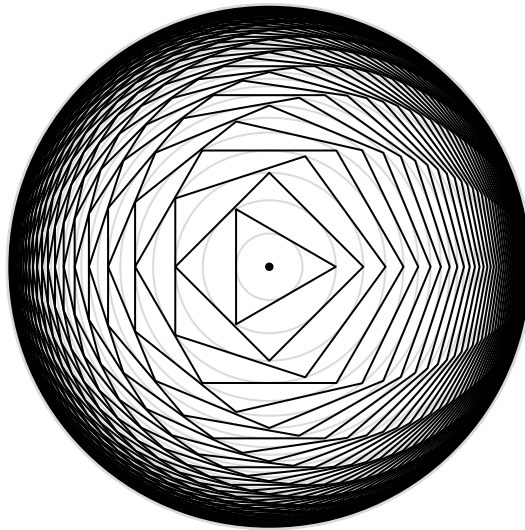
- $a_{n+1} = \frac{a_n + b_n}{2}$
- $b_{n+1} = \sqrt{a_n \cdot b_n}$
- $t_{n+1} = t_n - p_n \cdot (a_n - a_{n-1})^2$
- $p_{n+1} = 2p_n$

De waarde van  $\pi$  wordt dan vlot benaderd met de volgende limiet:

$$\pi = \lim_{n \rightarrow \infty} \frac{(a_n + b_n)^2}{4t_n}$$

## 114 Omschreven veelhoeken

Begin met een cirkel en construeer een omgeschreven regelmatige driehoek. Construeer daarna de cirkel rondom deze driehoek en een vierkant omgeschreven aan deze cirkel. Blijf dit herhalen met een regelmatige vijfhoek, zeshoek, zevenhoek, etc. De straal van deze  $n$ -hoeken wordt steeds groter, maar blijkt wel te convergeren, zoals ook de tekening hieronder suggereert.



Edward Kasner en James Newman waren de eersten die deze limietwaarde trachtten te berekenen, in hun boek *Mathematics and Imagination* uit 1940; zij bekwamen een waarde rond de 12. Vreemd genoeg werd dit voor lange tijd als correct aangenomen, totdat Christoffel Bouwkamp dit resultaat pas in 1965 weerlegde en de correcte waarde van ongeveer 8,7 gaf!

De omgeschreven straal  $R_n$  en de ingeschreven straal  $r_n$  van de regelmatige  $n$ -hoek in deze constructie kunnen als volgt berekend worden, in functie van de zijdelengte  $s$ .

$$R_n = \frac{s}{2} \cdot \csc\left(\frac{\pi}{n}\right), \quad r_n = \frac{s}{2} \cdot \cot\left(\frac{\pi}{n}\right), \quad \frac{R_n}{r_n} = \sec\left(\frac{\pi}{n}\right)$$

De limietwaarde  $K$  kan dan als volgt bepaald worden, startende met een eenheidscirkel (dus  $r_3 = 1$ ).

$$K = \prod_{k=3}^{\infty} \frac{R_k}{r_k} = \prod_{k=3}^{\infty} \sec\left(\frac{\pi}{k}\right)$$

Dit product convergeert naar 8,700036625208194503... en staat in OEIS A051762.

Omgekeerd, wanneer een driehoek wordt getekend binnen een eenheidscirkel, daarna zijn ingeschreven cirkel met daarin een vierkant, enzoverder met de verdere regelmatige  $n$ -hoeken, dan convergeert de straal van deze cirkels naar de inverse van  $K$ .

## 115 Lorenz attractor

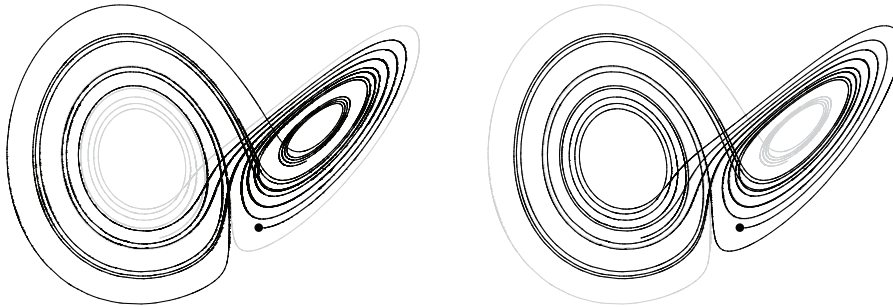
In 1963 ontwikkelde Edward Lorenz een vereenvoudigd weermodel uit de Navier-Stokes vergelijkingen. Hoewel het model zo simplistisch is dat het van weinig nut is voor praktische meteorologie, is het wiskundig belang ervan niet te onderschatten, met name in de chaostheorie. Het model stelt de toestand van de atmosfeer voor aan de hand van drie variabelen, die voldoen aan de vergelijkingen van Lorenz:

$$\begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = x(b - z) - y \\ \frac{dz}{dt} = xy - cz \end{cases}$$

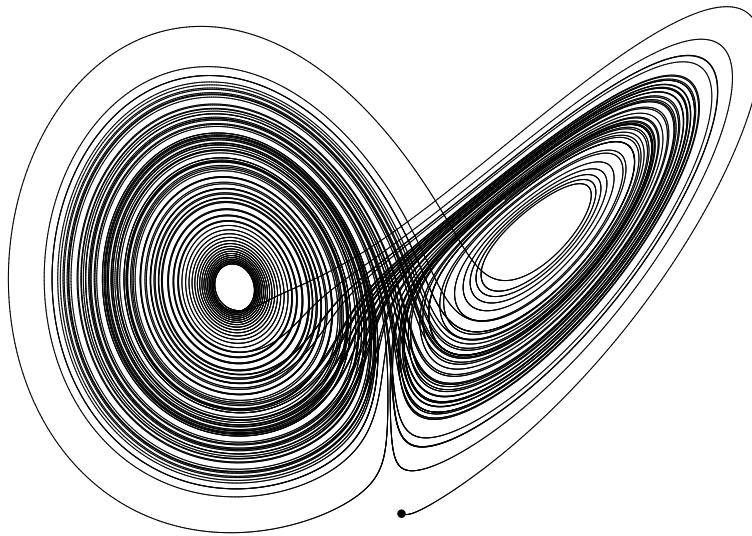
Hierin kan  $x$  geïnterpreteerd worden als de intensiteit van de convectiestromingen,  $y$  als temperatuursverschil tussen op- en neerwaartse stromingen en  $z$  als de mate waarin het verticale temperatuurverloop afwijkt van een

lineair verloop. Als waarden van de (positieve) parameters gebruikte Lorenz  $a = 10$ ,  $b = 28$  en  $c = \frac{8}{3}$ , passend bij de fysische interpretatie. Voor deze waarden vertoont het in essentie eenvoudige model al chaotisch gedrag.

Het systeem van Lorenz is deterministisch: alle toekomstige toestanden zijn volledig bepaald door de begintoestand en er is geen toeval of willekeur bij betrokken. Desondanks treedt er chaos op! Een kleine wijziging aan de begintoestanden mondt al gauw uit in een totaal verschillend baanverloop na enkele tijdseenheden. Hieronder de baan voor  $(2, 5, 10)$  en  $(2, 5 + 10^{-4}, 10)$ , met een tijdsverloop tot  $t = 15$ :



Ter vergelijking, de grijze baan erachter is die van de zeer dichtbijgelegen beginpositie. Initieel vallen hun banen nagenoeg samen, maar na enkele omlopen splitsen ze uiteen en gaan ze elk een andere richting op. Daarna gaat alle gelijkheid verloren. Het systeem is dus zeer gevoelig voor beginvoorwaarden. Toch is er een zekere orde in de chaos: het blijkt dat de banen worden aangetrokken tot een vlindervormige figuur met twee vleugels, de Lorenz attractor.

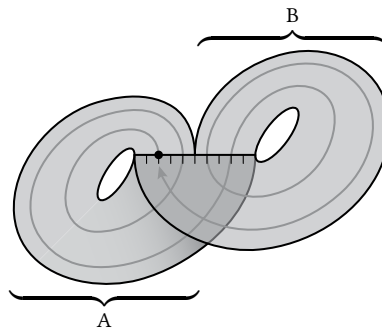


In 1972 gaf Lorenz een presentatie voor de American Association for the Advancement of Science, maar omdat hij had nagelaten een titel te voorzien, bedacht de organisator er zelf een. Het werd *Does the flap of a butterfly's wings in Brazil set off a tornado in Texas?* Sindsdien werd dit poëtische beeld, een kleine vlinder die invloed heeft op het weer, een geliefde metafoer in de populaire wetenschap en spreekt men vaak van het vlindereffect.

De ontdekking van Lorenz, dat zelfs in zeer vereenvoudigde wiskundige modellen naburige punten al vlug kunnen divergeren, veroorzaakte een schok in de meteorologie. Het is met huidige computercapaciteiten immers praktisch onmogelijk voldoende accurate gegevens te verzamelen om het weer met hoge nauwkeurigheidsgraad te voorspellen voor enkele dagen, laat staan weken of maanden!

Joan Birman, Robert Williams en John Guckenheimer stelden in de jaren 70 een verduidelijkend, simplistischer model voor de dynamiek van de Lorenz attractor voor. Hun papieren vlinder bestaat uit twee stroken waarvan het ene uiteinde half zo breed is als het andere, samengevoegd zoals op de figuur. Het centrale segment waar de

stroken bijeenkomen wordt gecoördinatiseerd van 0 tot 1. Een punt met abscis  $x$  loopt langs de linkerlus naar het punt met abscis  $2x$  en langs de rechterlus naar het punt met abscis  $2x - 1$ .



Op die manier kan men zeer gemakkelijk berekenen welke sequentie lussen een bepaald punt doorloopt, bijvoorbeeld op de figuur:  $\frac{1}{5} \rightarrow \frac{2}{5} \rightarrow \frac{4}{5} \rightarrow \frac{3}{5} \rightarrow \frac{1}{5}$ . Dit geeft dus een periodieke baan met periode 4,  $AABB$ . Een andere periodieke baan vinden we bij  $\frac{1}{3}$ , die afwisselend linker- en rechterlus doorloopt. De berekening van zo'n baan komt in feite neer op het bepalen van de binaire schrijfwijze: een binair cijfer 0 correspondeert met de lus  $A$  en een binair cijfer 1 met de lus  $B$ . Dit betekent dat juist die punten met rationale abscis een periodieke baan hebben. Een ander gevolg is dat voor elke mogelijke sequentie van linker- en rechterlussen er precies één punt bestaat die deze rij volgt.

Pas in 2001 bewees Warwick Tucker dat het model van Birman, Williams en Guckenheimer de feitelijke Lorenz-attractor goed beschrijft, in die zin dat voor elke baan op de Lorenz-attractor er een baan op het papieren model correspondeert die zich op dezelfde manier gedraagt.

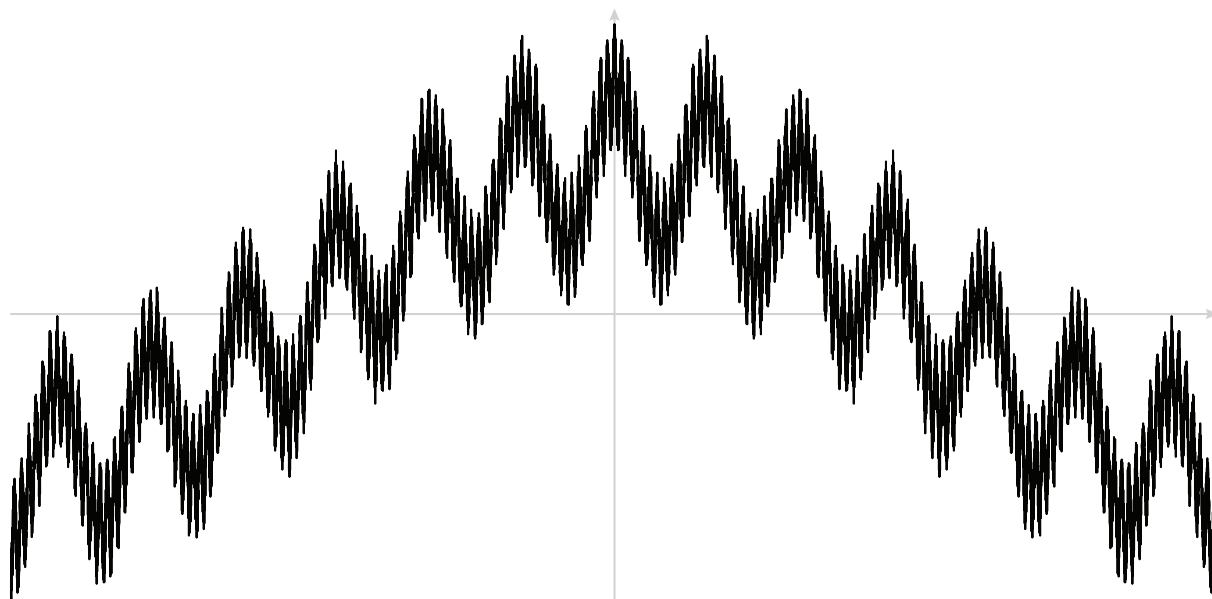
## 116 Monster van Weierstrass

In 1872 presenteerde Karl Weierstrass in een lezing voor de Königlich Akademie der Wissenschaften in Berlijn een bizarre functie, die de wiskundige gemeenschap met verstomming deed staan. Voorheen heerste de algemene intuïtieve aanname dat een continue functie bijna overal differentieerbaar was, op eventueel enkele geïsoleerde uitzonderingspunten na. André-Marie Ampère probeerde daar zelfs een theoretische rechtvaardiging voor te geven met de toen gekende middelen. De pathologische functie van Weierstrass is echter een voorbeeld van een overal continue, maar *nergens* afleidbare functie!

$$W(x) = \sum_{k=0}^{\infty} a^k \cos(b^k \pi x)$$

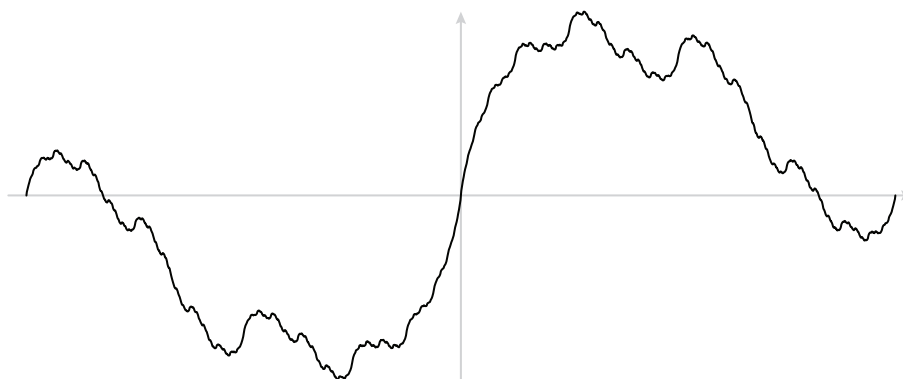
De parameter  $a$  is een reëel getal te kiezen uit  $]0, 1[$  en  $b$  een oneven natuurlijk getal zodat  $ab > 1 + \frac{3\pi}{2}$ .

Een plot met  $a = \frac{1}{2}$  en  $b = 13$ :



Weierstrass bewees de contra-intuïtieve eigenschappen van zijn functie tijdens diezelfde lezing en schreef z'n inspiratie toe aan Bernhard Riemann, die in zijn colleges een tegenvoorbeeld voor Ampères vermoeden suggereerde. In feite stuitte Bernard Bolzano rond 1830 al op een soortgelijke, als een fractaal gedefinieerde functie. Ook Charles Cellérier beschreef een mooie, rond 1860:

$$C(x) = \sum_{k=1}^{\infty} \frac{\sin(a^k x)}{a^k} \quad \text{met } a > 1$$



Vele wiskundigen voelden zich ongemakkelijk door deze pathologische functies. Door Henri Poincaré werden ze bijvoorbeeld “monsters” genoemd, en Charles Hermite schreef in een brief naar Thomas Stieltjes:

JE ME DÉTOURNE AVEC EFFROI ET HORREUR DE CETTE PLAIE LAMENTABLE DES FONCTIONS CONTINUES  
QUI N'ONT POINT DE DÉRIVÉE.

## 117 Riemanns reeksenstelling

Convergentie is een fragiele eigenschap. Zo zijn er betrekkelijk convergente reeksen, die op zich wel convergeren, maar de absolute waarden van hun termen niet. Een klassiek voorbeeld is de alternerende harmonische reeks, die convergeert naar de natuurlijk logaritme van 2:

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \frac{1}{7} - \dots \rightarrow \ln 2$$

Inderdaad, de absolute waarden van de termen geven de harmonische reeks (zie 94, blz. 71) waarvan bekend is dat deze divergeert. Conditionele convergentie is in zekere zin inferieur aan absolute, daar dergelijke reeksen niet

aan wenselijke eigenschappen als associativiteit of commutativiteit voldoen. Herschik bijvoorbeeld de termen van de reeks hierboven als volgt:

$$\left(1 - \frac{1}{2}\right) - \frac{1}{4} + \left(\frac{1}{3} - \frac{1}{6}\right) - \frac{1}{8} + \left(\frac{1}{5} - \frac{1}{10}\right) - \frac{1}{12} + \dots$$

De termen tussen haakjes berekenen resulteert dan in de alternerende harmonische reeks waarvan de termen gehalveerd zijn, zodat deze herschikking niet langer convergeert naar  $\ln 2$ , maar naar  $\frac{\ln 2}{2}$ !

$$\frac{1}{2} - \frac{1}{4} + \frac{1}{6} - \frac{1}{8} + \frac{1}{10} - \frac{1}{12} + \dots \rightarrow \frac{\ln 2}{2}$$

Bernhard Riemann toonde in 1854 aan dat een gepaste herschikking een betrekkelijk convergente reeks kan doen convergeren naar eender welk gewenst reëel getal, of doen divergeren naar oneindig. Een absoluut convergente reeks heeft daarentegen een limietwaarde die onafhankelijk is van de volgorde van de termen.

## 118 Universele koordestelling

Definieer een koorde van een functie als een *horizontaal* lijnstuk met eindpunten op de grafiek van de functie. Een opmerkelijke stelling van Paul Lévy, veralgemeend door Heinz Hopf, geeft het volgende resultaat:

BESCHOUW EEN CONTINUE REËELWAARDIGE FUNCTIE  $f$  OP HET EENHEIDSINTERVAL  $[0, 1]$ , WAARVOOR  $f(0) = f(1)$ . DAN IS HET ENKEL GEGARANDEERD DAT ER KOORDEN BESTAAN VAN LENGTE  $\frac{1}{n}$  MET  $n \in \mathbb{N}$ , EN VOOR ALLE  $\alpha$  NIET DE INVERSE VAN EEN NATUURLIJK GETAL, BESTAAT ER EEN FUNCTIE  $f$  ZONDER KOORDEN VAN LENGTE  $\alpha$ .

Algemener: als  $f$  een koorde bereikt van lengte  $\ell$ , dan ook van lengte  $\frac{\ell}{n}$  voor alle natuurlijke  $n$ , en dit geldt niet per se voor andere lengtes. Een expliciet tegenvoorbeeld van Lévy:

$$f : [0, 1] \rightarrow \mathbb{R} : x \mapsto \sin^2\left(\frac{\pi x}{r}\right) - x \sin^2\left(\frac{\pi}{r}\right)$$

Mocht deze functie een koorde van lengte  $r$  hebben, dan moet  $f(x) = f(x+r)$  voor zekere  $x$ , waaruit volgt dat  $r \sin^2\left(\frac{\pi}{r}\right) = 0$ , en dus dat  $r$  de inverse van een natuurlijk getal moet zijn. Omgekeerd, als  $r$  niet van deze vorm is, dan heeft  $f$  geen koorde van lengte  $r$ .



## 119 Borweinintegralen

Nog een bewijs dat schijnbaar herhalende waarden niet altijd wijzen op patronen.

$$\int_0^{\infty} \frac{\sin x}{x} dx = \frac{\pi}{2}$$

$$\int_0^{\infty} \frac{\sin x}{x} \cdot \frac{\sin \frac{x}{3}}{\frac{x}{3}} dx = \frac{\pi}{2}$$

$$\int_0^{\infty} \frac{\sin x}{x} \cdot \frac{\sin \frac{x}{3}}{\frac{x}{3}} \cdot \frac{\sin \frac{x}{5}}{\frac{x}{5}} dx = \frac{\pi}{2}$$

$$\int_0^{\infty} \frac{\sin x}{x} \cdot \frac{\sin \frac{x}{3}}{\frac{x}{3}} \cdot \frac{\sin \frac{x}{5}}{\frac{x}{5}} \cdot \frac{\sin \frac{x}{7}}{\frac{x}{7}} dx = \frac{\pi}{2}$$

$$\int_0^{\infty} \frac{\sin x}{x} \cdot \frac{\sin \frac{x}{3}}{\frac{x}{3}} \cdot \frac{\sin \frac{x}{5}}{\frac{x}{5}} \cdot \frac{\sin \frac{x}{7}}{\frac{x}{7}} \cdot \frac{\sin \frac{x}{9}}{\frac{x}{9}} dx = \frac{\pi}{2}$$

$$\int_0^{\infty} \frac{\sin x}{x} \cdot \frac{\sin \frac{x}{3}}{\frac{x}{3}} \cdot \frac{\sin \frac{x}{5}}{\frac{x}{5}} \cdot \frac{\sin \frac{x}{7}}{\frac{x}{7}} \cdot \frac{\sin \frac{x}{9}}{\frac{x}{9}} \cdot \frac{\sin \frac{x}{11}}{\frac{x}{11}} dx = \frac{\pi}{2}$$

$$\int_0^{\infty} \frac{\sin x}{x} \cdot \frac{\sin \frac{x}{3}}{\frac{x}{3}} \cdot \frac{\sin \frac{x}{5}}{\frac{x}{5}} \cdot \frac{\sin \frac{x}{7}}{\frac{x}{7}} \cdot \frac{\sin \frac{x}{9}}{\frac{x}{9}} \cdot \frac{\sin \frac{x}{11}}{\frac{x}{11}} \cdot \frac{\sin \frac{x}{13}}{\frac{x}{13}} dx = \frac{\pi}{2}$$

De volgende integraal evalueert echter tot een verrassende waarde:

$$\int_0^{\infty} \frac{\sin x}{x} \cdot \frac{\sin \frac{x}{3}}{\frac{x}{3}} \cdot \frac{\sin \frac{x}{5}}{\frac{x}{5}} \cdot \frac{\sin \frac{x}{7}}{\frac{x}{7}} \cdot \frac{\sin \frac{x}{9}}{\frac{x}{9}} \cdot \frac{\sin \frac{x}{11}}{\frac{x}{11}} \cdot \frac{\sin \frac{x}{13}}{\frac{x}{13}} \cdot \frac{\sin \frac{x}{15}}{\frac{x}{15}} dx = \frac{467807924713440738696537864469\pi}{935615849440640907310521750000}$$

Het verschil van deze waarde met het verwachte  $\frac{\pi}{2}$  is slechts zo'n  $2,31 \cdot 10^{-11}$ . Gelijkoortige integralen blijven evalueren tot  $\frac{\pi}{2}$  wanneer de getallen 3, 5, etc. vervangen worden door positieve reële getallen waarvoor dat de som van hun inversen kleiner is dan 1. In het laatste voorbeeld geldt echter:

$$\frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{13} < 1 \quad \text{en} \quad \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{13} + \frac{1}{15} > 1$$

Het resultaat is nog verrassender als een factor  $2 \cos x$  wordt toegevoegd in het integrandum. Dan blijven de integralen veel langer evalueren tot  $\frac{\pi}{2}$ : de eerste keer dat er een kleinere waarde wordt gevonden, is dan pas bij  $\frac{x}{113}$  in plaats van  $\frac{x}{15}$ !

Nadat David en Jonathan Borwein deze numerieke curiositeit gevonden hadden, verifieerden ze dat het computeralgebrapakket Maple alle correcte waarden van deze integralen berekende, en rapporteerden ze dit bij wijze van grap als een bug in de software. Maple-informaticus Jacques Carette verklaarde later dat hij zeker drie dagen had gependeerd aan een poging de bug te traceren vooraleer hij doorhad dat Borwein hem beet had.

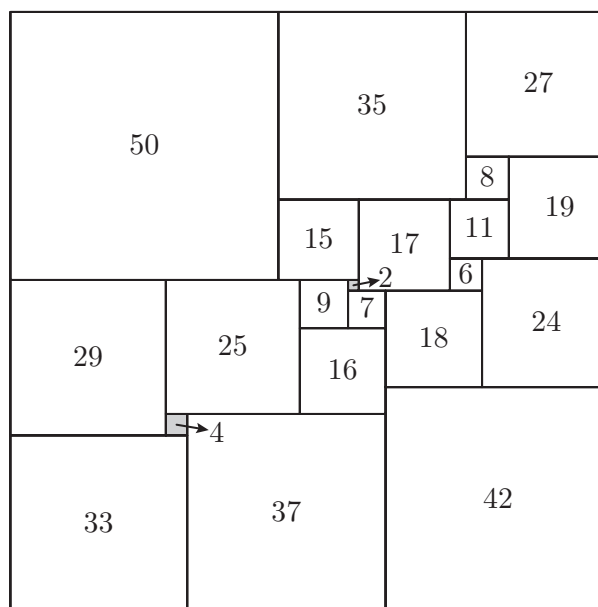




## 120 Dissectie van Duijvestijn

De kwadratuur van het vierkant is een wiskundige puzzel die vraagt een vierkant met zijden van gehele lengte te verknippen in kleinere vierkanten met gehele zijden. Op zich zeer eenvoudig totdat men extra voorwaarden oplegt; voor een *perfect* vierkant wordt geëist dat de afmetingen van de kleinere vierkanten allemaal verschillen.

Ondanks het vermoeden van Nikolai Lusin dat perfecte vierkanten niet zouden bestaan, ontdekte Roland Sprague in 1939 het eerste perfecte vierkant, onderverdeeld in 55 kleinere. Het perfecte vierkant met het kleinste aantal deelvierkanten werd door Adrianus Duijvestijn geconstrueerd met behulp van computerberekeningen in 1978. Zijn betegeling telt 21 vierkanten en dit is het absolute minimum.



Men hanteert vaak de Bouwkampcode als notatie voor perfecte vierkanten. Tussen vierkante haakjes worden de groepen aaneensluitende vierkanten genoteerd, rij per rij, van linksboven naar rechtsonder (het hoogstgelegen vierkant heeft voorrang op het meest linkse). Duijvestijns dissectie bijvoorbeeld wordt dan genoteerd als:

$$[50, 35, 27], [8, 19], [15, 17, 11], [6, 24], [29, 25, 9, 2], [7, 18], [16], [42], [4, 37], [33]$$

Hoewel Duijvestijns vierkant het laagste aantal subvierkanten heeft, is deze niet van de minimale grootte, 110. De drie kleinste perfecte vierkanten hebben 22 en 23 deelvierkanten en worden in Bouwkampcode:

- $[60, 50], [23, 27], [24, 22, 14], [7, 16], [8, 6], [12, 15], [13], [2, 28], [26], [4, 21, 3], [18], [17]$
- $[60, 50], [27, 23], [24, 22, 14], [4, 19], [8, 6], [3, 12, 16], [9], [2, 28], [26], [21], [1, 18], [17]$
- $[44, 29, 37], [21, 8], [13, 32], [28, 16], [15, 19], [12, 4], [3, 1], [2, 14], [5], [10, 41], [38, 7], [31]$

Ook enkele uitbreidingen van het probleem werden al bestudeerd. In 1975 stelde Solom Golomb de vraag of het volledige vlak kan worden betegeld met vierkanten, zodanig dat elk natuurlijk getal juist één keer voorkomt als zijdelengte. Recent, in 2008, wisten James en Frederick Henle dit inderdaad klaar te spelen.

Het probleem uitbreiden naar drie dimensies is echter onmogelijk. Geen enkele kubus kan worden onderverdeeld

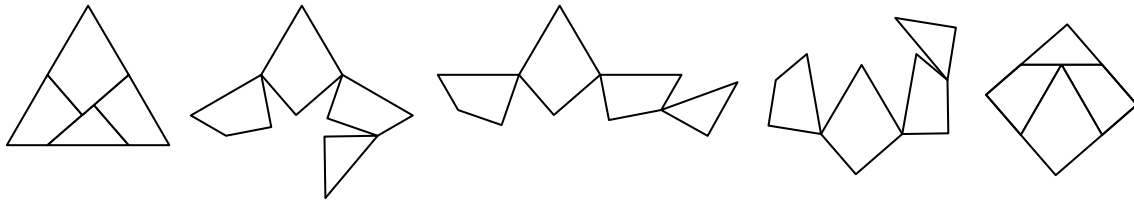
in een eindig aantal kleinere, niet-congruente kubussen met gehele ribbelengte. Veronderstel namelijk dat dit wel zou lukken, dan is diens bodemvlak alvast een perfect vierkant, waarop op elk van de deelvierkanten een kubus staat. Het kleinste kubusje van deze collectie wordt aan alle kanten omringd door uittorende kubussen, dus kunnen er enkel kleinere kubussen op staan, zodat het topvlak van dit kubusje óók een perfect vierkant is. Uit Fermats principe van oneindige afdaling volgt dat zo'n perfecte kubus dus niet kan bestaan.

## 121 Haberdasherpuzzel

Henry Ernest Dudeney was een Engels wiskundige met een voorliefde voor logicapuzzels en wiskundige spellen. Een van zijn grootste ontdekkingen is de Haberdasherpuzzel, die hij eerst publiceerde in de *Weekly Dispatch* in 1902 en daarna in zijn puzzelepos *The Canterbury Puzzles* in 1907. Het probleem gaat als volgt:

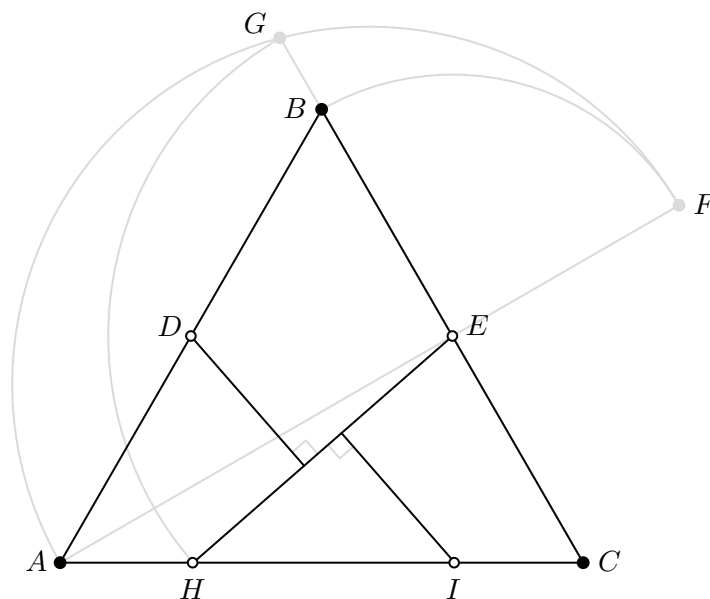
VERDEEL EEN GELIJKZIJDIGE DRIEHOEK IN VIER STUKKEN DOOR MIDDEL VAN DRIE SNEDEN, DIE DAARNA HERSCHIKT KUNNEN WORDEN TOT EEN PERFECT VIERKANT.

De oplossing staat hieronder. Bovendien kunnen de vier stukken van de dissectie aan elkaar bevestigd worden via scharnieren: draai de stukken de ene kant op en ze passen ineen tot een vierkant, terwijl ze langs de andere kant in elkaar passen tot een driehoek!



Een passer-en-liniaalconstructie vinden is haast een puzzel op zich.

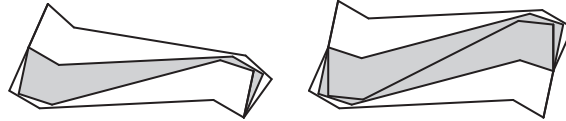
- Start met de gelijkzijdige driehoek  $ABC$ .
- Construeer  $D$  als het middelpunt van zijde  $[AB]$  en  $E$  als het middelpunt van zijde  $[BC]$ .
- Verleng  $[AE]$  en pas  $F$  af zodat  $|EF| = |BE|$ .
- Construeer de halfcirkel met diameter  $|AF|$ .
- Verleng  $[BC]$  en noem het snijpunt met de zonet geconstrueerde cirkelboog,  $G$ .
- Construeer de cirkel met middelpunt  $E$  en straal  $|EG|$ , en noem het snijpunt met zijde  $[AC]$ ,  $H$ .
- Meet  $I$  af op zijde  $[AC]$  zodat  $|HI| = |BE|$ .
- Verbind  $E$  met  $H$  en construeer vanuit  $D$  en  $I$  loodrechten op  $EH$ .



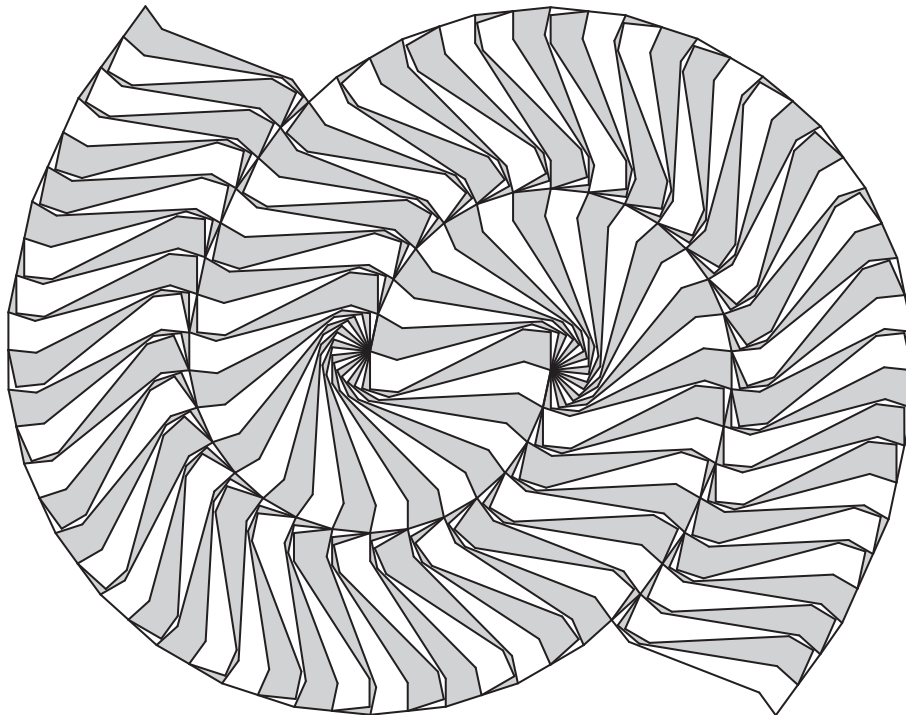
## 122 Tegelpatroon van Voderberg



Hans Voderberg ontdekte en beschreef deze bovenstaande opmerkelijke tegel in 1936. Met deze concave, negenhoekige figuur kan een spiraalvormige tessellatie van congruente tegels aangelegd worden. Dit wordt mogelijk gemaakt doordat twee tegels zowel één als twee andere tegels kunnen omsluiten:



De uiteindelijk indrukwekkende spiraal van Voderberg heeft twee armen, die draaien rond twee middelpunten. Elke arm wordt opgebouwd uit halve cirkels van telkens 12 clusters van tegels. In de eerste draaiing bevatten de clusters losse tegels, in de volgende drie tegels die alterneren in oriëntatie, daarna vijf tegels, dan zeven etc. De twee armen passen dan juist in elkaar en leveren volgende figuur op:

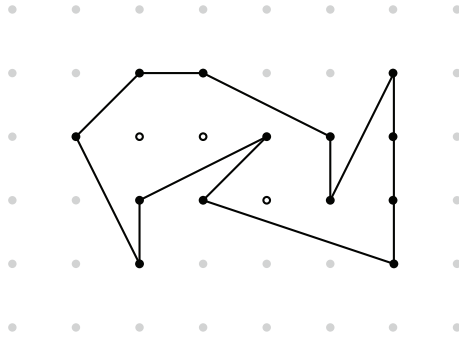


Sinds Voderbergs ontdekking zijn er al veel meer tegels met dezelfde eigenschappen ontdekt, zoals de *versatile* van Branko Grünbaum en Geoffrey Shephard of het Hirschhornpatroon van Michael Hirschhorn.

## 123 Formule van Pick

Georg Pick beschreef in 1899 een bijzonder elegante en algemene formule voor de oppervlakte van veelhoeken met hoekpunten op een regelmatig eenheidsrooster. De oppervlakte  $A$  kan dan worden uitgedrukt in functie van het aantal roosterpunten  $O$  op de omtrek van de veelhoek en het aantal roosterpunten  $I$  erbinnenin:

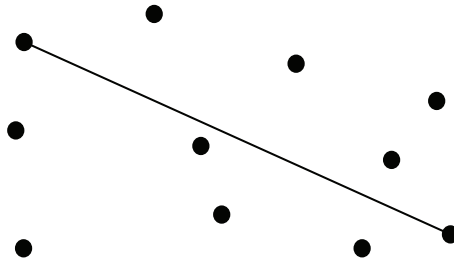
$$A = \frac{O}{2} + I - 1$$



## 124 Stelling van Jung

Beschouw een aantal punten in het vlak met diameter (de maximale afstand tussen twee punten)  $d$ . De stelling van Jung stelt nu dat alle punten binnen een cirkel met straal  $r$  kunnen worden verzameld, waarbij de volgende bovengrens geldt en gelijkheid slechts optreedt als de uiterste punten op een gelijkzijdige driehoek liggen.

$$r \leq \frac{d}{\sqrt{3}}$$



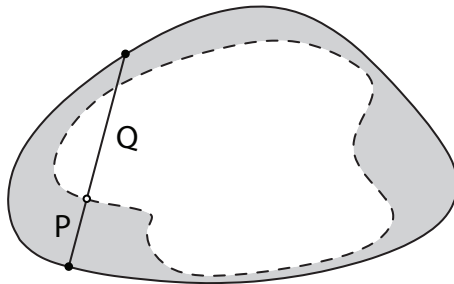
De originele stelling van Jung is een veralgemeende versie in een  $n$ -dimensionale ruimte.

$$r \leq d \cdot \sqrt{\frac{n}{2(n+1)}}$$

De stelling wordt vernoemd naar Heinrich Jung, die de ongelijkheid in 1901 bestudeerde.

## 125 Stelling van Holditch

Beschouw een gesloten, gladde en convexe kromme. Kies een koorde van de kromme en een willekeurig punt  $P$  erop, die de koorde verdeelt in twee stukken met lengtes  $p$  en  $q$ . Laat vervolgens de koorde langsheen de kromme glijden zodanig dat de lengte van de koorde constant blijft. Het punt  $P$  beschrijft dan zelf ook een kromme, de Holditchkromme genoemd.



Nu geldt volgens de stelling van Holditch, dat de oppervlakte tussen de initiële kromme en de Holditchkromme niet afhangt van hun vorm of grootte, maar enkel van  $p$  en  $q$ . Concreet is de ingesloten oppervlakte gelijk aan:

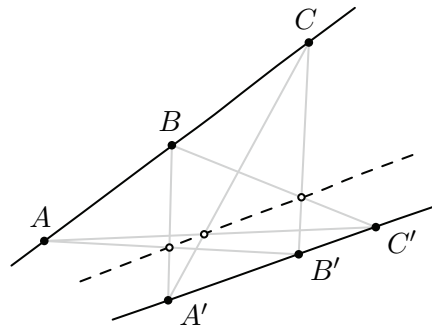
$$A = \pi pq$$

Hoewel Holditch het niet expliciet vermeldde, vereist zijn bewijs de aanname dat de koorde kort genoeg is om te garanderen dat de Holditchkromme zichzelf niet snijdt.

## 126 Stelling van Pappus

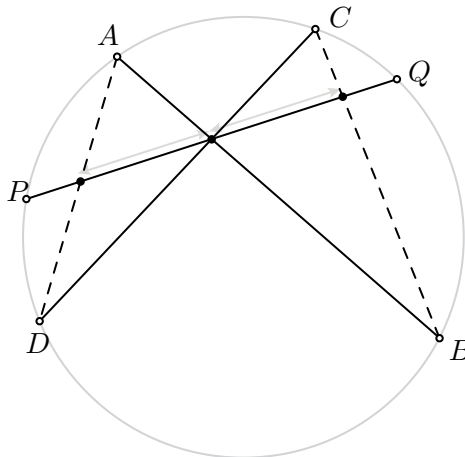
De stelling van Pappus, toegeschreven aan een van de laatste klassieke Griekse wiskundigen Pappus van Alexandrië, kan worden beschouwd als een speciaal geval van de stelling van Pascal (zie 132, blz. 100). Ze is het krachtigst in de projectieve meetkunde, waar ze gemakkelijk gedualiseerd kan worden.

Gegeven zijn drie collineaire punten  $A$ ,  $B$  en  $C$ , evenals drie collineaire punten  $A'$ ,  $B'$  en  $C'$ . De doorsneden van respectievelijk  $AB'$  en  $A'B$ , van  $AC'$  en  $A'C$  en van  $BC'$  en  $BC'$  zullen dan ook collineair zijn.



## 127 Vlinderstelling

De vlinderstelling is een klassieke stelling uit de Euclidische meetkunde. Kies een koorde  $[PQ]$  van een cirkel, en laat  $[AB]$  en  $[CD]$  twee andere koorden van de cirkel zijn die door het middelpunt  $M$  van  $[PQ]$  gaan. Noem nu  $X$  het snijpunt van  $[AD]$  met  $[PQ]$ , en  $Y$  het snijpunt van  $[BC]$  met  $[PQ]$ ; dan is  $M$  het midden van  $[XY]$ .



## 128 Probleem van prins Rupert

Ruprecht van de Palts was de hertog van Cumberland in de 17<sup>de</sup> eeuw. Als prins Rupert bekleedde hij de posten commandant en admiraal in respectievelijk de Engelse Burgeroorlog en Tweede Nederlands-Engelse Oorlog. Hij was tevens zeer geïnteresseerd in fysica, chemie en techniek. Zo demonstreerde hij in 1661 de *prince Rupert's drops* voor de Royal Society: druppelvormige glasobjecten die bestand zijn tegen hamerslagen, maar exploderen als hun puntvormige uiteinde wordt afgebroken.

Van prins Rupert is volgend probleem afkomstig.

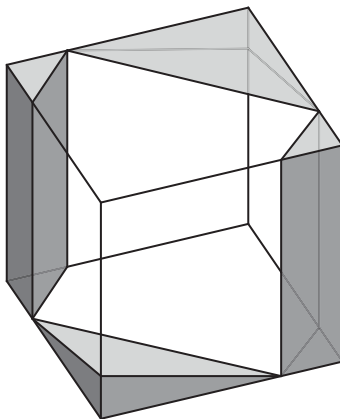


WAT IS DE GROOTSTE KUBUS DIE DOOR EEN GEGEVEN KUBUS KAN WORDEN GESCHOVEN?

Misschien verrassend blijkt dat een kubus te zijn, die lichtjes groter is dan de gegeven kubus! Pieter Nieuwland was de eerste die het probleem oploste; hij beschreef dat voor de eenheidskubus de oplossing wordt:

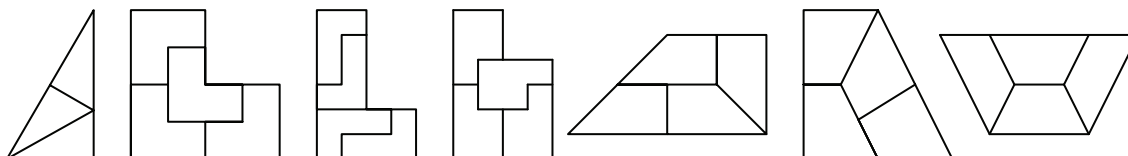
$$\frac{3\sqrt{2}}{4} \approx 1,0606601\dots$$

De zijden van de eenheidskubus worden dan verdeeld volgens de verhoudingen  $\frac{1}{3}$  en  $\frac{3}{13}$ .

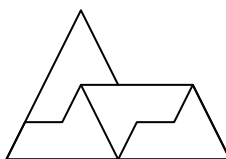


## 129 Rep-tiles

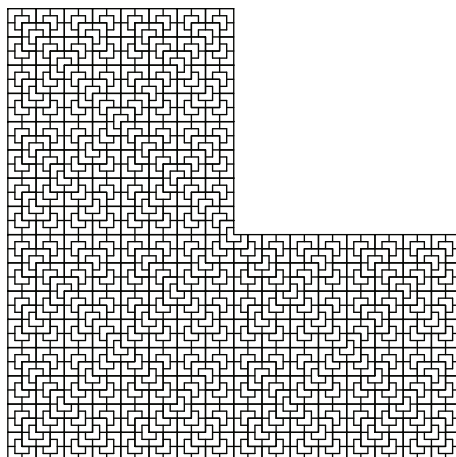
Een rep- $n$ -tile is de informele benaming voor een veelhoek die kan worden betegeld met of gedissecteerd in  $n$  kleinere, gelijkvormige veelhoeken. Triviale voorbeelden zijn alle driehoeken en parallellogrammen; boeiendere voorbeelden zijn deze.



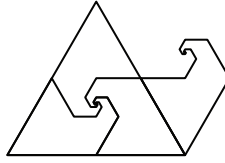
Tot nog toe bekend bestaat er maar één vijfhoekig rep-tile, bijgenaamd de sfinx:



Door herhaaldelijk de onderverdelingen weer te dissecteren in kleinere rep-tiles, kan een fractale, vlakvullende figuur worden gemaakt, zoals geïllustreerd bij deze rep-tile.



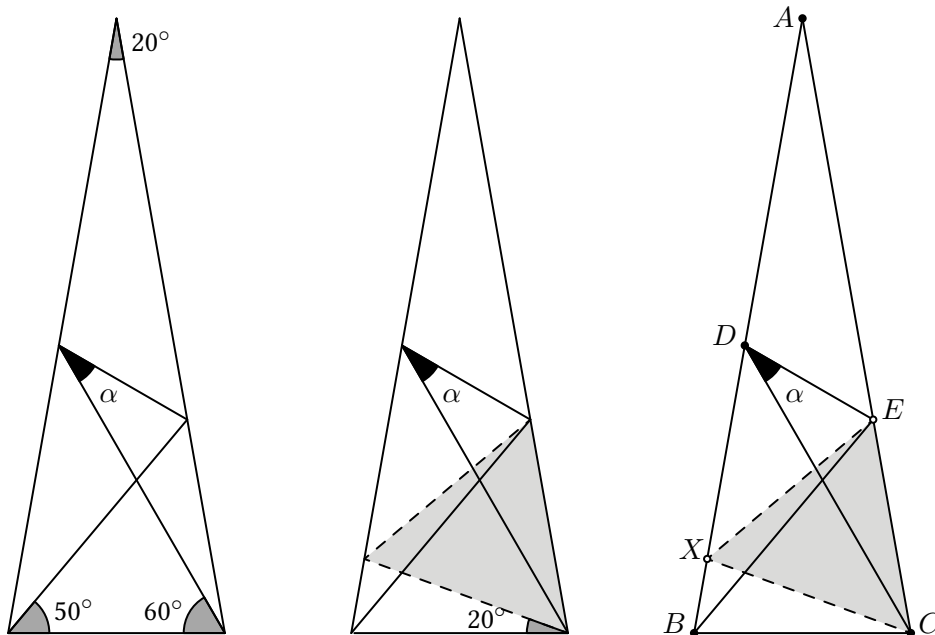
Fractalen kunnen zelf ook een rep-tile zijn, zoals deze slakkenfiguur.



### 130 Probleem van Langley

Een klassieker in de mathematische folklore! Deze opgave lijkt eenvoudig, maar is hemeltergend lastig, en werd gepubliceerd door Edward Langley in *The Mathematical Gazette* in 1922 onder de bescheiden naam "A problem".

BEPAAAL, ENKEL DOOR GEBRUIK TE MAKEN VAN ELEMENTAIRE GEOMETRIE EN DUS ZONDER GONIOMETRIE, DE WAARDE VAN DE HOEK  $\alpha$  IN DE GELIJKBENIGE DRIEHOEK LINKSONDER.



Construeer voor de oplossing het punt  $X$  op zijde  $AB$  zodat  $\widehat{BCX} = 20^\circ$ . Dan geldt omdat  $\triangle EBC$  gelijkbenig is met top  $C$  dat  $|CE| = |BC|$ , en omdat  $\triangle BCX$  gelijkbenig is met top  $C$  dat  $|BC| = |CX|$  (ze zijn gelijkbenig wegens even grote basishoeken).

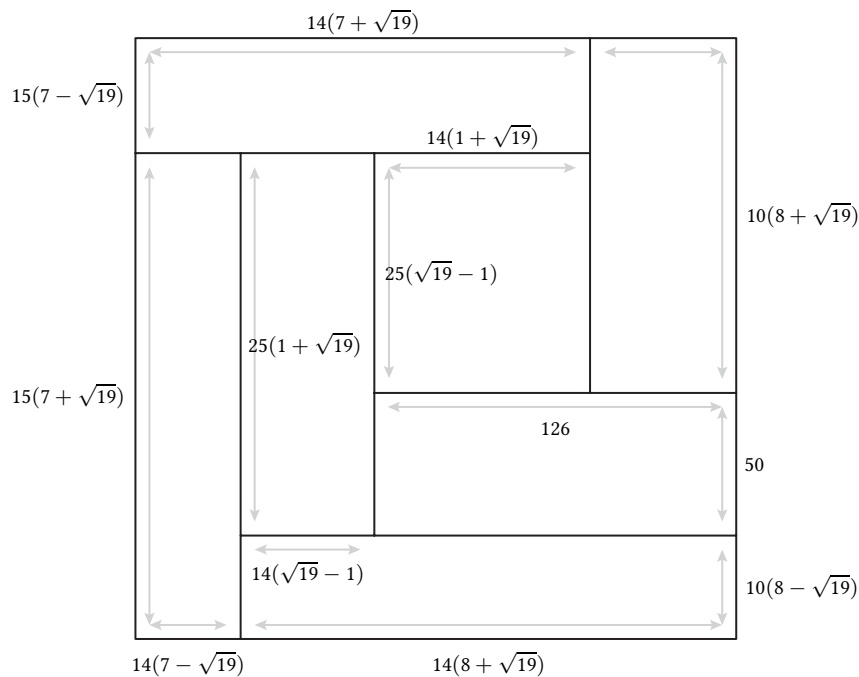
Aangezien  $|CX| = |CE|$  en  $\widehat{ECX} = 60^\circ$  is  $\triangle CEX$  gelijkbenig. Door hoekenjagen kan ook gevonden worden dat  $\triangle CDX$  even grote basishoeken heeft en dus gelijkbenig is. Dus  $|DX| = |EX|$ , en  $\triangle DEX$  is óók gelijkbenig. Hoekenjagen levert eveneens op dat  $\widehat{DXE} = 40^\circ$ , zodat  $\widehat{EDX} = 70^\circ$ . Tot slot is  $\widehat{XDC} = 40^\circ$  en vinden we voor  $\widehat{CDE}$  zelf de waarde  $30^\circ$ .

Een soortgelijk probleem vraagt de waarde van diezelfde hoek met  $60^\circ$  en  $70^\circ$  als onderste hoeken.

### 131 Dissectie van Blanche

In 1935 sloten vier wiskundestudenten Rowland Brooks, Arthur Stone, Cedric Smith en William Tutte zich aan bij de Trinity Mathematical Society en begonnen ze onder elkaar te werken aan wiskundige problemen. Ze gaven hun genootschap de naam "Blanche Descartes", oorspronkelijk BLAC uit de initialen van hun bijnamen (Bill, Leonard, Arthur en Cedric), uitgebreid naar Blanche, met de woordspeling verwijzend naar *carte blanche*.

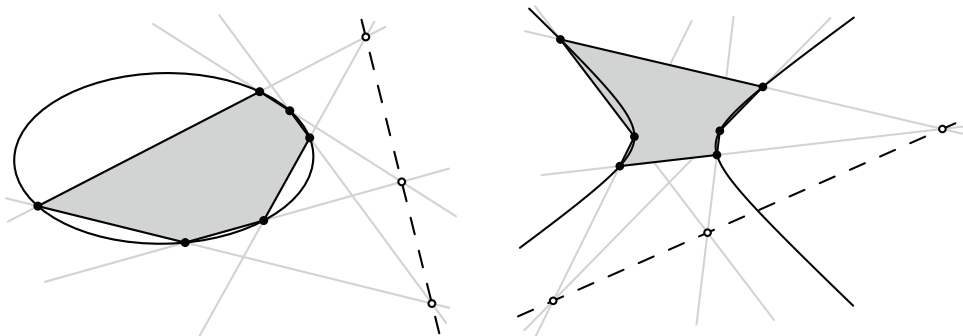
Onder deze naam gaven ze een dissectie uit van een vierkant, verdeeld in rechthoeken met dezelfde oppervlakte, maar met verschillende afmetingen. Deze dissectie van Blanche is de eenvoudigste en bevat zeven rechthoeken.



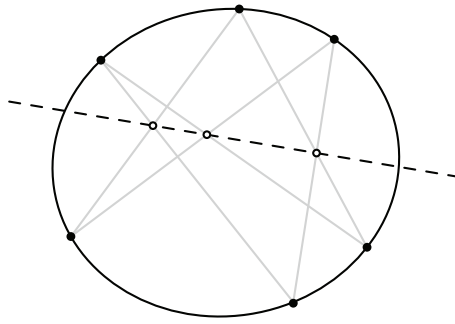
## 132 Stelling van Pascal

Frans wiskundige Blaise Pascal ontdekte en publiceerde deze verrassende stelling op 16-jarige leeftijd in een werk *Essai pour les Coniques*. Zijn interesse voor kegelsneden dankt hij waarschijnlijk aan de samenwerking met Girard Desargues, aan wie hij zijn dank betuigt in zijn *Essai*. Hij bewees zijn stelling zelf niet expliciet, maar verklaarde dat die volgde uit resultaten van Desargues.

De stelling van Pascal verkondigt dat wanneer een willekeurige zeshoek wordt ingeschreven in een kegelsnede, de snijpunten van de tegenoverliggende zijden concurrent zijn. De lijn door deze snijpunten heet de Pascallijn. In het Euclidische vlak zijn er uitzonderingen, bijvoorbeeld omdat rechten daar niet altijd snijden; daarom is de stelling het krachtigst en algemeenst in het projectieve vlak.



Omdat de stelling ook geldt voor een zichzelf snijdende zeshoek, wordt het diagram vaak anders getekend.

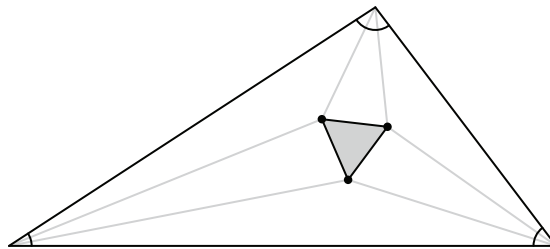


De stelling van Pappus (zie 126, blz. 97) kan worden beschouwd als een speciaal geval van deze stelling, daar twee rechten een ontaarde kegelsnede vormen.

### 133 Driehoek van Morley

Tijdens onderzoek naar cardioïden stuitte Frank Morley in 1899 op deze wonderlijke, voorheen nog onbekende stelling, die in de wiskundige folklore zelfs bekendstaat als *Morley's miracle*. Ze wordt algemeen beschouwd als een van de mooiste wiskundige stellingen.

Teken een willekeurige driehoek en verdeel diens hoeken in drie. De snijpunten van de aanliggende trisectrices vormen dan de hoekpunten van een gelijkzijdige driehoek!



De stelling van Morley is eveneens berucht als schijnbaar eenvoudig, maar weerbarstig te bewijzen. Het eerste deugdelijke bewijs werd pas gegeven 15 jaar nadat Morley zijn stelling publiceerde! De meeste vroege bewijzen steunen op delicate goniometrische manipulaties.

De zijdelengte  $z$  van de driehoek van Morley kan worden berekend uit deze formule, waarin  $\alpha$ ,  $\beta$  en  $\gamma$  de hoekgroottes van de originele driehoek voorstellen en  $R$  de straal van de omschreven cirkel:

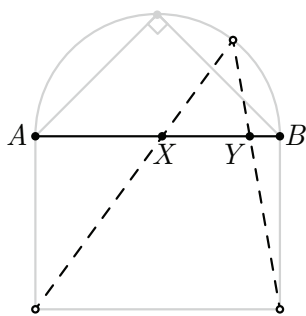
$$z = 8R \cdot \sin\left(\frac{\alpha}{3}\right) \cdot \sin\left(\frac{\beta}{3}\right) \cdot \sin\left(\frac{\gamma}{3}\right)$$

### 134 Fermats halvecirkelprobleem

Pierre de Fermat beschreef dit probleem in een brief naar Kenelm Digby, waarschijnlijk in 1658.

Construeer een halfcirkel  $ANB$ , waarbij  $N$  de cirkelboog in twee deelt, en plaats die op een rechthoek met afmetingen  $|AB|$  en  $|AN|$ . Kies een punt op de halve cirkel. Noem dan de snijpunten van de bovenzijde van de rechthoek met de lijnstukken die het punt op de halve cirkel verbinden met de onderhoeken, respectievelijk  $X$  en  $Y$ . Fermat beweerde nu dat de volgende uitdrukking geldt, ongeacht welk punt op de halve cirkel:

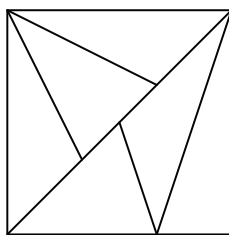
$$|AY|^2 + |BX|^2 = |AB|^2$$



Fermat zelf gaf geen bewijs. Deze werd pas in de 18<sup>de</sup> eeuw opgelost door Leonhard Euler, die een klassiek, puur geometrisch bewijs gaf omdat hij een bewijs via analytische meetkunde te voor de hand liggend vond.

## 135 Stelling van Monsky

De studie der equidissecties (dissecties van veelhoeken in driehoeken met dezelfde oppervlakte) begon bij Fred Richman, toen hij in 1965 een masterexamen opstelde aan de New Mexico State University. Tijdens het zoeken naar een meetkundevraag, ontdekte hij dat het niet voor de hand lag een vierkant te verdelen in een oneven aantal driehoeken met dezelfde oppervlakte; een even aantal is triviaal. Richman kon bewijzen dat zulke verdelingen in drie of vijf driehoeken onmogelijk zijn, maar niet algemeen en hij nam de vraag niet op in het examen.



Richmans probleem wekte de interesse van zijn vriend John Thomas, die bewees dat een oneven equidissectie onmogelijk is als de coördinaten van de hoekpunten rationale getallen zijn met oneven noemers. Pas in 1970 bewees Paul Monsky het algemene geval, in een elegant bewijs dat gebruik maakt van Spencers lemma (zie 242, blz. 201), 2-adische getallen (zie 42, blz. 30) en een slimme kleuring van het vierkant.

Volgens een generalisatie van de stelling van Monsky kan een  $n$ -dimensionale hyperkubus enkel worden onderverdeeld in simplexen met eenzelfde volume als het aantal simplexen een veelvoud is van  $n!$ .

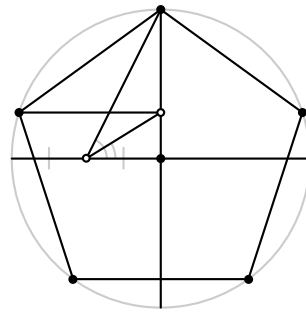
## 136 Gauss' zeventienhoek

Carl Friedrich Gauss ontdekte op 19-jarige leeftijd dat het mogelijk is een zeventienhoek te construeren uitsluitend met passer en liniaal. Dit resultaat beschouwde hij als een van zijn grootste ontdekkingen ooit en daarom, zo gaat het verhaal, verlangde hij een 17-hoek ter decoratie op zijn grafsteen. De beeldhouwer weigerde echter, omdat zo'n veelhoek niet te onderscheiden zou zijn van een cirkel. Het bewijs van construeerbaarheid werd ook gegeven in zijn monumentale werk, de *Disquisitiones Arithmeticae*.

Euclides gaf in zijn *Elementen* een constructie voor de regelmatige drie-, vier-, vijf- en zeshoek, maar de Grieken vonden geen keurige constructie voor de zevenhoek. De vraag drong zich op of algemene regelmatige  $n$ -hoeken wel altijd te construeren waren en indien niet, bij welke  $n$ -waarden. Gauss gaf een volledig antwoord op deze vraag. Als voldoende voorwaarde is een  $n$ -hoek te construeren met passer en liniaal als  $n$  een product is van verschillende Fermatpriemgetallen (zie 47, blz. 36) vermenigvuldigd met een factor  $2^k$ . Hij stelde dat dit ook een nodige voorwaarde is, maar publiceerde hiervan nooit een bewijs. In 1837 gaf Pierre Wantzel een volledig

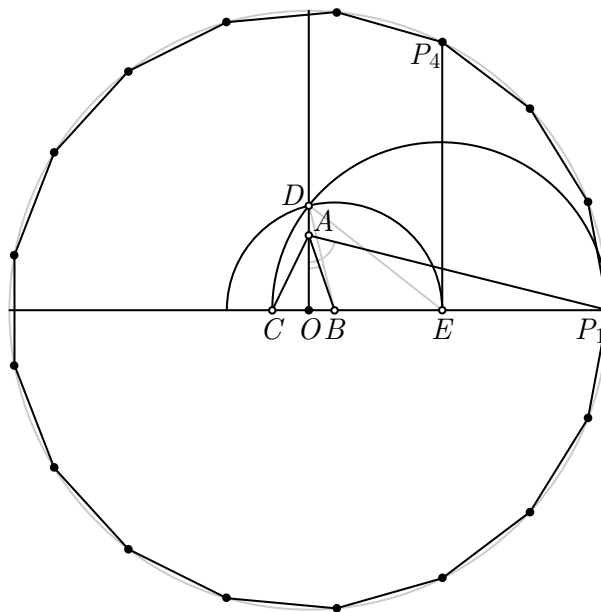
bewijs, zodat men vandaag spreekt over de stelling van Gauss-Wantzel.

Een eenvoudige constructie voor de regelmatige vijfhoek:



Gauss zelf toonde uitsluitend het theoretische resultaat aan voor zijn zeventienhoek. De eerste expliciete constructie werd gegeven door Johannes Erchinger in 1825; het volgende stappenplan is van de hand van Herbert Richmond, 1893:

- Teken een cirkel met centrum  $O$  en een diameter, eindigend op  $P_1$ .
- Teken de straal loodrecht op deze diameter en het punt  $A$  op een vierde van deze straal.
- Construeer  $B$  zodanig op  $OP_1$  dat de hoek  $O\hat{A}B$  een vierde zo groot is als de hoek  $O\hat{A}P_1$ .
- Zoek  $C$  op dezelfde diagonaal zodat  $B\hat{A}C = 45^\circ$ .
- Teken de halve cirkel met diameter  $[CP_1]$ ; deze snijdt de loodrechte straal in het punt  $D$ .
- Teken de halve cirkel met centrum  $B$  en straal  $[BD]$ .
- Het snijpunt van deze halve cirkel met  $[OP_1]$  wordt het punt  $E$ .
- Construeer de loodrechte door  $E$  op de diameter. Deze snijdt de oorspronkelijke cirkel in  $P_4$ .
- De punten  $P_1$  en  $P_4$  zijn hoekpunten van de zeventienhoek, die nu makkelijk vervolledigd wordt.



Constructies voor de 257-hoek werden gepubliceerd in 1832 door Friedrich Richelot en Hugo Schwendenwein, en Johann Hermes spendeerde tien jaar aan een constructie voor de 65537-hoek rond 1900.

## 137 Negenpuntscirkel

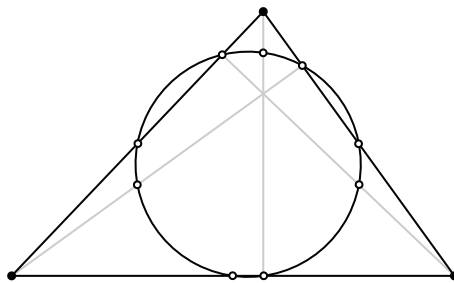
Deze opmerkelijke meetkundige curiositeit wordt toegeschreven aan Karl Feuerbach, die in 1822 een verband ontdekte tussen de voetpunten van de hoogtelijnen in een driehoek en middelpunten van zijn zijden, hoewel

Charles Brianchon en Jean-Victor Poncelet dezelfde observatie al iets eerder hadden gemaakt. Olry Terquem voegde kort na Feuerbachs ontdekking drie gerelateerde punten toe aan hun resultaat. Ook Leonhard Euler wordt tot de ontdekkers van deze eigenschappen gerekend (al in 1765); de negenpunts­cirkel staat dan ook bekend als de cirkel van Feuerbach, de cirkel van Terquem en de cirkel van Euler.

Teken de volgende punten in een willekeurige driehoek:

- de middelpunten van de drie zijden
- de voetpunten van de drie hoogtelijnen
- de middelpunten van de lijnsegmenten tussen het hoogtepunt en de drie hoekpunten

Deze negen punten liggen nu altijd op eenzelfde cirkel, die voldoet aan nog andere eigenschappen. Feuerbach bewees dat de negenpunts­cirkel uitwendig raakt aan de drie aangeschreven cirkels en inwendig aan de ingeschreven cirkel van de driehoek. Zijn middelpunt ligt ook op de rechte van Euler (zie 154, blz. 121), en zijn straal is half zo lang als die van de omgeschreven cirkel. Als een rechthoekige hyperbool (met loodrechte diagonalen) door de drie hoekpunten gaat, ligt zijn middelpunt op de negenpunts­cirkel; deze laatste eigenschap staat bekend als Feuerbachs kegelsnedestelling.



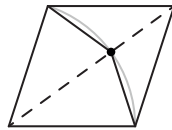
## 138 Tegelpatroon van Penrose

Periodieke betegelingen, die translatiesymmetrie vertonen, zijn triviaal te vinden. Niet-periodieke patronen zijn lastiger, zeker als de tegels allemaal dezelfde vorm en grootte moeten hebben, maar het eenvoudigst is daarbij een spiraalpatroon te ontwerpen, vanuit een centraal punt vertrekkende. Dit gaf aanleiding tot de vraag:

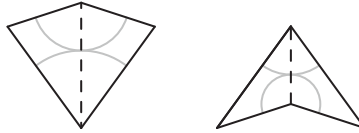
BESTAAT ER EEN VERZAMELING TEGELS ZODAT DIE HET VLAK SLECHTS *NIET-PERIODIEK* BETEGELEN?  
 GEEN ENKELE VORM UIT DEZE VERZAMELING, NOCH EEN DEELVERZAMELING, NOCH DE VOLLEDIGE VER-  
 ZAMELING MAG EEN PERIODIEKE BETEGELING KUNNEN VORMEN.

Zulke verzamelingen worden nu aperiodiek genoemd. Lange tijd geloofden wiskundigen niet in het bestaan van aperiodieke verzamelingen; zelfs twee tegels van Voderberg (zie 122, blz. 95) kunnen naast elkaar gelegd worden tot een achthoek die een periodieke betegeling toelaat. In 1961 groeide de interesse in dit probleem, toen Hao Wang het dominoprobleem (zie ??, blz. ??) introduceerde. Wang vermoedde dat er geen aperiodieke verzameling van zijn domino's bestond, waaruit zou volgen dat het probleem beslisbaar was. In 1966 echter bewees Robert Berger dat het betegelingsprobleem in feite onbeslisbaar is, waarmee hij impliciet het bestaan van aperiodieke tegelsystemen bewees. Berger vond een verzameling van 20426 tegels; dit kon de latere jaren wel drastisch teruggebracht worden.

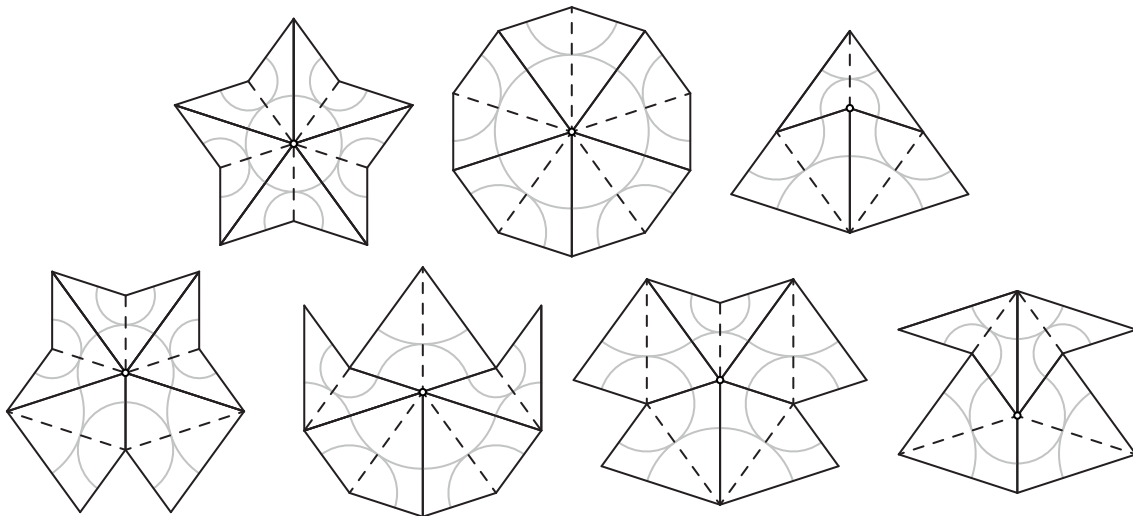
Roger Penrose bedacht een esthetischer systeem, gebaseerd op vijfhoeken i.p.v. vierkanten. Zijn eerste versie bestond uit zes tegels, die hij heeft weten te herleiden naar twee. Samen met John Conway onderzocht hij de verscheidene eigenschappen ervan, die daarna werden gepopulariseerd door Martin Gardner in zijn "Mathematical Games" in de *Scientific American*. De twee stukken worden bekomen door de lange diagonaal van een ruit, met hoeken van  $72^\circ$  en  $108^\circ$ , te verdelen volgens de gulden snede. Verbind dan dit punt met de andere hoekpunten. Een cirkelboog zoals hieronder, met een hoekpunt als centrum, werkt ook.



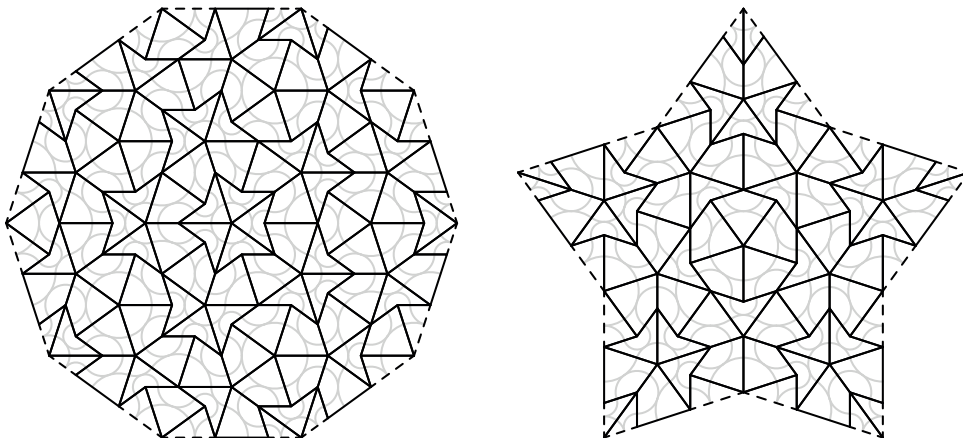
Het resultaat zijn twee tegels, door Conway aangeduid als “vliegers” (*kites*) en “pijlpunten” (*darts*). Om te voorkomen dat de stukken terug in elkaar worden gezet als de oorspronkelijke ruit (die een periodieke betegeling zou toelaten), worden er nog bogen aangebracht, die moeten doorlopen wanneer tegels aan elkaar worden gelegd.



De enige mogelijke reglementaire combinaties van vliegers en pijlen rond een punt zijn de volgende zeven.



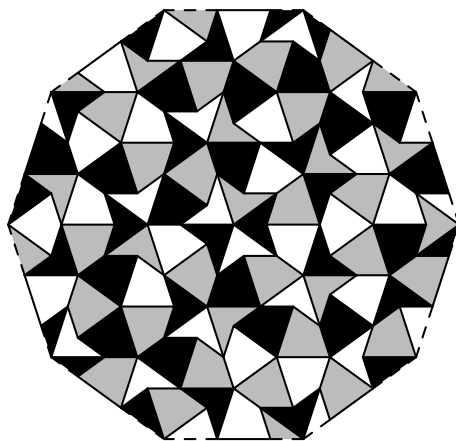
De tegels van Penrose kunnen onmogelijk het volledige vlak periodiek bedekken; translaties zullen nooit een Penrosepatroon op zichzelf afbeelden. Andere symmetrieën zijn echter nog steeds goed mogelijk; wanneer je probeert de vijfvoudige symmetrie te bewaren, word je gedwongen een van volgende twee patronen te volgen. Conway noemde ze figuratief de “zon” en de “ster”. Beiden zijn eenduidig bepaald tot in het oneindige.



In een reglementair aangelegd Penrosepatroon nadert de verhouding tussen het aantal vliegers tegenover pijlen naar de gulden verhouding  $\varphi$ , hoe groter het patroon hoe nauwkeuriger. Elke eindige regio in een betegeling komt een oneindig aantal keer voor, in eender welke oneindige Penroseconfiguratie. Een kopie van een regio is hooguit twee keer zo ver als de diameter ervan terug te vinden.

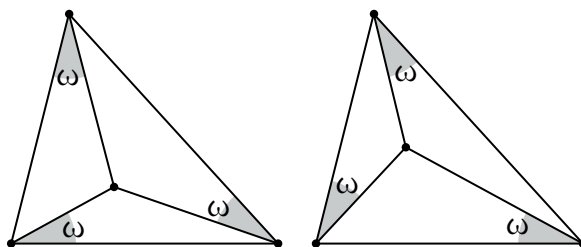
John Conway stelde de vraag of het mogelijk is Penrosepatronen in te kleuren met slechts drie kleuren, waarbij aangrenzende tegels een verschillende kleur hebben. Dit vermoeden werd bevestigd door William Paulsen.





### 139 Punten van Brocard

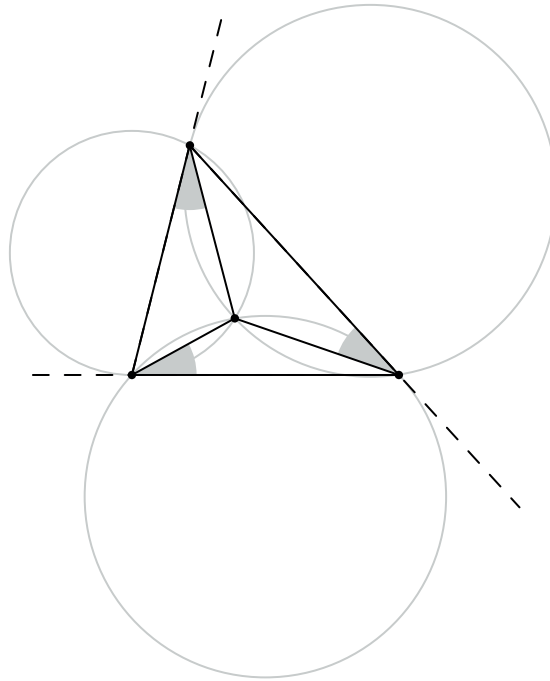
De punten van Brocard, vernoemd naar Henri Brocard, zijn de twee unieke punten in een driehoek waarvan uit de lijnstukken naar de hoekpunten onder een gelijke hoek gezien worden vanuit het volgende hoekpunt (wijzerzin of tegenwijzerzin, elk geeft een ander Brocardpunt). De figuur illustreert het concept.



De hoek  $\omega$  vastgelegd door de Brocardpunten voldoet aan de volgende elegante uitdrukking, waarbij  $\alpha$ ,  $\beta$  en  $\gamma$  de hoekgroottes van de driehoek voorstellen:

$$\cot \omega = \cot \alpha + \cot \beta + \cot \gamma$$

De Brocardpunten worden eenvoudig gevonden door de cirkel door  $A$  en  $B$  te construeren die raakt aan  $BC$ . Construeer ook de cirkel door  $B$  en  $C$  rakend aan  $AC$ , en die door  $A$  en  $C$  rakend aan  $AB$ . Deze drie cirkels zullen door één punt gaan, het eerste Brocardpunt. Het tweede punt wordt analoog gevonden door de cirkels te laten raken aan de zijde aan de andere kant.

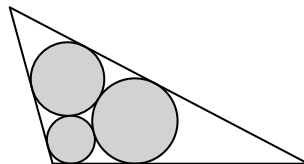


## 140 Probleem van Malfatti

In 1803 stelde Gian Francesco Malfatti het marmerprobleem:

GEGEVEN EEN BLOK MARMER IN DE VORM VAN EEN RECHT DRIEHOEKIG PRISMA, BEPAAL DAN DE DRIE GROOTST MOGELIJKE CILINDERVORMIGE ZUILEN DIE UIT DIT BLOK GEKAPT KUNNEN WORDEN.

Dit vraagt de constructie van die drie cirkels binnen een driehoek met de grootst mogelijke totale oppervlakte. Malfatti stelde zelf de cirkels voor die raken aan zowel de twee andere cirkels als twee zijden van de driehoek, waarin ook vele contemporaine wiskundigen de oplossing voor het marmerprobleem zagen. De desbetreffende cirkels worden nu de cirkels van Malfatti genoemd.

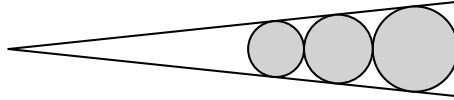


Hoewel eerder onderzoek naar de eigenschappen van de Malfatticirkels voornamelijk analytisch gebeurde, gaf Jakob Steiner in 1826 een synthetische constructie.

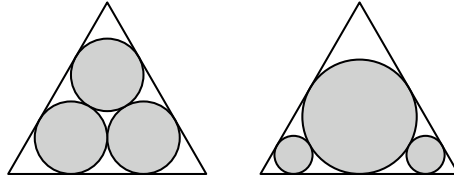
- Construeer de bissectrices van de driehoek  $\triangle ABC$ , van de hoekpunten tot hun gemeenschappelijke snijpunt (het centrum van de ingeschreven cirkel).
- Deze bissectrices verdelen de oorspronkelijke driehoek in drie kleinere driehoeken. Bepaal de ingeschreven cirkels van elk van deze driehoeken.
- Construeer van elk paar ingeschreven cirkels uit stap 2 de gemeenschappelijke raaklijn.
- Deze drie raaklijnen zullen concurrent zijn; noem hun snijpunt  $L$  en de snijpunten met de zijden tegenover hoekpunt  $A$ ,  $B$  en  $C$  respectievelijk  $A'$ ,  $B'$  en  $C'$ .
- De vierhoeken  $AB'C'L$ ,  $A'BC'L$  en  $A'B'CL$  zijn tangentiële vierhoeken. Hun ingeschreven cirkels zijn de gevraagde Malfatticirkels van de oorspronkelijke driehoek  $ABC$ .

Een amusante opmerking is dat ondanks de schijnbare vanzelfsprekendheid, de cirkels van Malfatti *niet* de meest rendabele oppervlakte geven! In 1930 illustreerden Hyman Lob en Herbert Richmond dat voor een lange smalle

driehoek, Malfatti's oplossing duidelijk niet de beste is. De gevraagde oppervlakte kan zo goed als verdubbeld worden door een gretig algoritme, dat eerst de cirkel met maximale straal binnen de driehoek selecteert, dan de tweede cirkel met maximale straal in de drie overblijvende stukjes, en daarna ook de laatste cirkel zo groot mogelijk in de restanten van de driehoek.



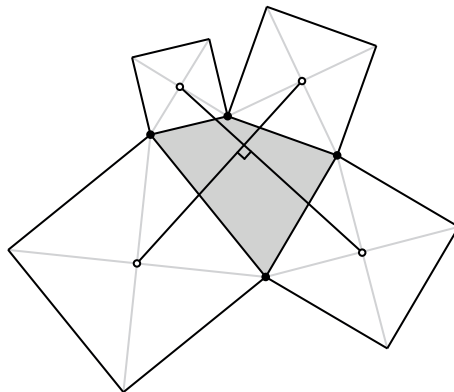
Voor een gelijkzijdige driehoek geeft de procedure van Lob-Richmond minder winst, maar desalniettemin is de aldus bekomen oppervlakte een kleine 1% groter. Michael Goldberg toonde in 1967 zelfs aan dat Malfatticirkels *nooit* de grootst mogelijke oppervlakte opleveren!



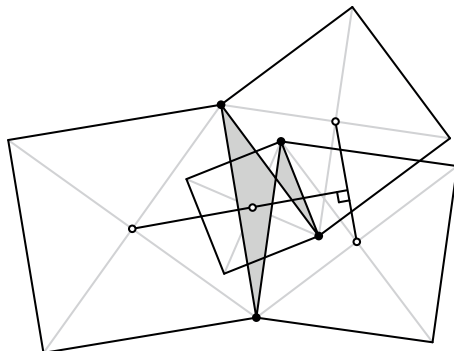
Hans Melissen vermoedde in 1997 dat voor elke  $n$ , het algoritme van Lob-Richmond de maximale oppervlakte voor  $n$  cirkels oplevert, wat nog maar voor  $n \leq 3$  geverifieerd werd.

## 141 Stelling van Van Aubel

Deze aardige stelling werd gepubliceerd door Belgisch wiskundige Henricus Hubertus van Aubel in 1878. Teken op een willekeurige gegeven vierhoek, vierkanten op de zijden naar de buitenkant toe. Deze vierhoek hoeft niet per se convex te zijn: zelfs voor complexe vierhoeken (die zichzelf snijden) geldt de stelling, mits de vierkanten in de juiste richting geconstrueerd worden. Van Aubel kon dan aantonen dat de rechten die de middelpunten van tegenoverstaande vierkanten verbinden, loodrecht op elkaar staan.



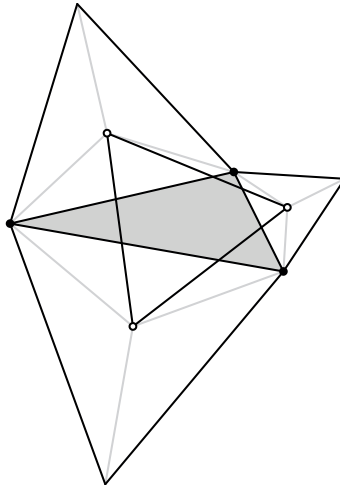
Zoals daarnet opgemerkt geldt de stelling eveneens voor zichzelf snijdende vierhoeken.



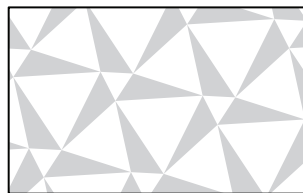
Van Aubels stelling is gerelateerd aan de stelling van Napoleon (zie 142, blz. 109).

## 142 Stelling van Napoleon

Dit item is legendarisch als een van de meest herontdekte stellingen uit de wiskunde. Of Napoleon Bonaparte dit resultaat ontdekte, of zelfs maar kende, is twijfelachtig; de thans oudste bekende referentie (*The Ladies Diary* van William Rutherford) dateert van 1825, vier jaar na Napoleons dood, en noemt hoegenaamd geen ontdekker. Aureliano Faifofer droeg als eerste de stelling op aan de Franse keizer, in zijn *Elementi di Geometria* uit 1911. Toch dient gezegd te worden dat Napoleon een degelijke wiskundige kennis bezat: hij correspondeerde geregeld met contemporaine wiskundigen als Fourier, Monge, Laplace, Lagrange...



Hoe dan ook, de stelling van Napoleon beweert dat wanneer op een willekeurige driehoek, drie gelijkzijdige driehoeken getekend worden (allen naar buiten toe of allen naar binnen toe), dat dan de middelpunten ook een gelijkzijdige driehoek vormen. De omcirkels van de driehoeken op de zijden, of de lijnstukken tussen overstaande hoekpunten, snijden elkaar daarenboven in de punten van Fermat (zie ??, blz. ??). De twee resulterende gelijkzijdige driehoeken worden de binnenste en buitenste driehoek van Napoleon gedoopt; het verschil tussen hun oppervlaktes is verrassend genoeg ook gelijk aan de oppervlakte van de oorspronkelijke driehoek. De eigenschap fundeert het volgende patroon:



Bewijzen van de stelling zijn niet moeilijk te vinden. Er bestaan analytische en goniometrische bewijzen, via symmetrie en via complexe getallen. Analytisch is aan te tonen dat de zijden van Napoleons driehoek, voor een begindriehoek met zijden  $a$ ,  $b$  en  $c$ , allen zoveel bedragen als:

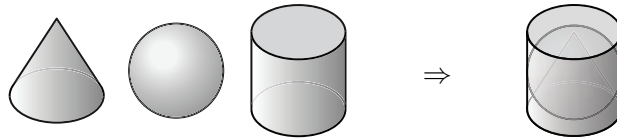
$$z = \sqrt{\frac{a^2 + b^2 + c^2}{6} + \frac{\sqrt{(a+b+c)(a+b-c)(a-b+c)(-a+b+c)}}{2\sqrt{3}}}$$

## 143 Graf van Archimedes

Tijdens de Tweede Punische Oorlog, rond 212 voor Christus, vielen Romeinse troepen de stad Syracuse binnen waar op dat moment de legendarische wis- en natuurkundige Archimedes verbleef. Ondanks uitdrukkelijk bevel van generaal Marcus Claudius Marcellus zijn leven te sparen, ontstak een van de soldaten in woede toen hij Archimedes aantrof, wiskundige diagrammen tekenend in het zand en klagend dat zijn werk verstoord werd. Zijn laatste woorden waren: “Breng mijn cirkels toch niet in de war” (*μή μου τοὺς κύκλους τάραττε*), waarop

de soldaat hem neerstak met zijn zwaard.

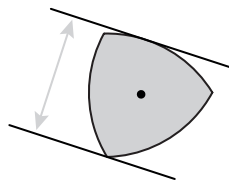
Archimedes' grafsteen draagt een gravure van zijn favoriete wiskundige ontdekking, omtrent een bol ingeschreven in een cilinder. De bol raakt zowel de mantel als de onder- en bovenvlakken van de cilinder. Archimedes toonde aan dat het volume en de oppervlakte van de bol zich verhouden tot die van de cilinder als twee derde. In feite kan dit elegante resultaat nog sterker gemaakt worden door ook de kegel in de cilinder erbij te beschouwen: in dat geval verhouden de volumes van kegel, bol en cilinder zich tot elkaar als  $1 : 2 : 3$  en hun respectievelijke oppervlaktes als  $3 : 4 : 6$ .



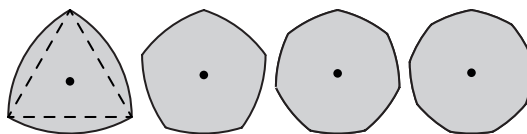
Toen Marcus Tullius Cicero, aangesteld als quaestor in Sicilië, in het jaar 75 het graf wou bezoeken, kon niemand de juiste locatie aanwijzen. Uiteindelijk werd het graf nog teruggevonden, totaal verwaarloosd en overwoekerd; Cicero liet het graf opknappen en kon de aangebrachte inscripties lezen. Charles Edwards verkondigde in *The Historical Development of the Calculus* dat deze daad allicht de grootste wiskundige bijdrage van de Romeinen was, gezien hun zeer beperkte interesse in pure wiskunde. Momenteel is de exacte locatie opnieuw onbekend.

## 144 Krommen met constante breedte

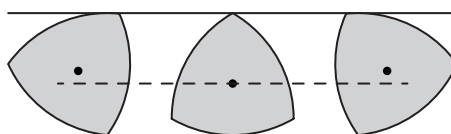
Een kromme met constante breedte is een convexe vlakke figuur waarvan de breedte in alle richtingen hetzelfde is. Met "breedte" in een bepaalde richting wordt de kleinst mogelijke afstand bedoeld tussen twee rechten in deze richting, die geen innerlijke punten van de figuur bevatten (de figuur hieronder verduidelijkt dit). Een voor de hand liggende kromme die hieraan voldoet, is de cirkel, maar er bestaan ook niet-triviale voorbeelden.



De bekendste familie krommen met constante breedte zijn de veelhoeken van Reuleaux, vernoemd naar Duits ingenieur Franz Reuleaux. Zijn klassieke driehoek wordt gemaakt door een cirkelboog te trekken tussen elke twee hoekpunten op een gelijkzijdige driehoek met het derde hoekpunt als centrum. Analoge krommen kunnen geconstrueerd worden uit  $n$ -hoeken voor oneven  $n$ .

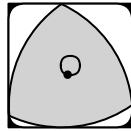


Objecten op rollers met een veelhoek van Reuleaux als doorsnede, zouden probleemloos (zonder hoppen) rollen. Als wiel zijn ze echter niet praktisch, omdat ze niet rond een vast rotatiecentrum draaien en er dus geen vaste as aan bevestigd kan worden.



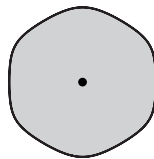
Een ander concreet gebruik is als vorm van geldstukken. Britse munten van 20 en 50 pence bijvoorbeeld, hebben een Reuleauxzevenhoekige vorm, wat het gebruik in muntautomaten toelaat.

Reuleauxdriehoeken kennen nog een onvoorstelbaardere toepassing: het boren van vierkante gaten! Een speciaal mechanisme zorgt ervoor dat de driehoek niet rond een vaste as rondbeweegt. Op deze manier kunnen zo goed als vierkante gaten geboord worden met zo'n driehoek als boor. Enkel de hoekpunten zijn lichtjes afgerond, maar het uitgeboorde gat beslaat toch zo'n 99,87% van de oppervlakte van het volledige vierkant.



De familie krommen hierboven hebben scherpe hoeken, een soort van knikpunten. De krommen in de volgende familie, gedefinieerd met behulp van parametervergelijkingen, zijn echter overal glad. Voor de parameters geldt dat  $a, b \geq 0$  en dat  $k$  oneven is. Het is wel mogelijk dat de resulterende krommen hiermee niet convex zijn.

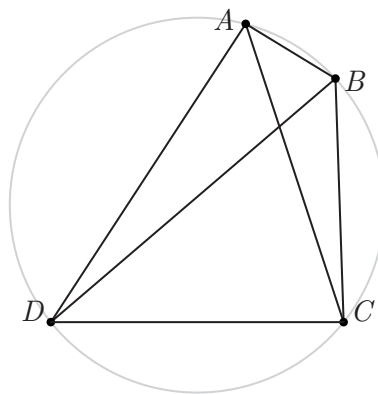
$$\begin{cases} x = p(\theta) \cdot \cos \theta - p'(\theta) \cdot \sin \theta \\ y = p(\theta) \cdot \sin \theta + p'(\theta) \cdot \cos \theta \end{cases} \quad \text{met } p(\theta) = a \cos^2\left(\frac{k\theta}{2}\right) + b$$



Van alle krommen met eenzelfde constante breedte  $s$  is de grootste oppervlakte die van de cirkel, en volgens de stelling van Blaschke-Lebesgue heeft de Reuleauxdriehoek de kleinste oppervlakte, namelijk  $\frac{1}{2}(\pi - \sqrt{3}) \cdot s^2$ . Ook opmerkelijk is dat al deze krommen dezelfde omtrek hebben! De stelling van Barbier garandeert dat deze steeds  $\pi \cdot s$  is, ongeacht de vorm van de kromme.

## 145 Stelling van Ptolemaeus

Deze klassieke stelling speelt een centrale rol in de Euclidische meetkunde. Verschillende eigenschappen, zoals de stelling van Pythagoras, de cosinusregel, de gulden snede in het pentagram en een heleboel goniometrische identiteiten kunnen eruit afgeleid worden. Ze wordt vernoemd naar Claudius Ptolemaeus, Grieks astronoom en wiskundige, die de stelling gebruikte voor astronomische doeleinden en goniometrische tabellen.



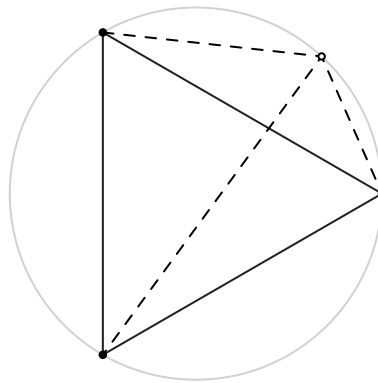
In een koordenvierhoek  $ABCD$  (waarvan de hoekpunten op dezelfde cirkel liggen) geldt de volgende relatie.

$$|AB| \cdot |CD| + |BC| \cdot |AD| = |AC| \cdot |BD|$$

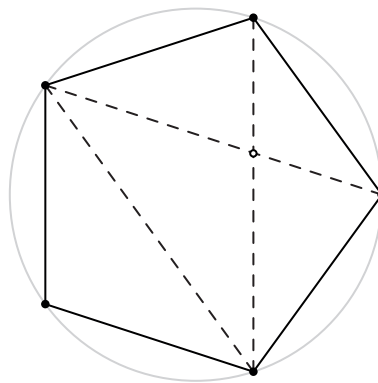
De stelling geldt ook in de andere richting: als en slechts als de bovenstaande gelijkheid optreedt, is de vierhoek ingeschreven in een cirkel. Een veralgemeende eigenschap stelt dat de volgende ongelijkheid steeds opgaat, met gelijkheid als en slechts als  $ABCD$  een koordenvierhoek is.

$$|AB| \cdot |CD| + |BC| \cdot |AD| \geq |AC| \cdot |BD|$$

Een eerste mooie gevolg is dat voor een punt op de omgeschreven cirkel van een gelijkzijdige driehoek, de afstand tot het verst afgelegen hoekpunt gelijk is aan de som van de afstanden tot de twee dichtstbijzijnde hoekpunten.

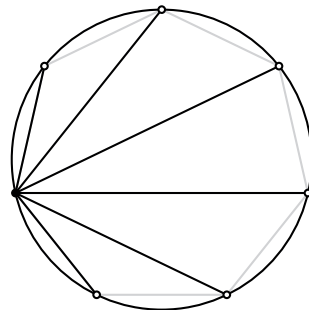


Toegepast op een rechthoek geeft Ptolemaeus de stelling van Pythagoras als gevolg, op een gelijkbenig trapezium de cosinusregel. In een vijfhoek dan, met zijde  $z$  en diagonaal  $d$ , geldt dat  $d^2 = z^2 + dz$ . Hieruit volgt dat  $\frac{d}{z} = \varphi$ , de gulden snede als verhouding tussen diagonaal en zijde.



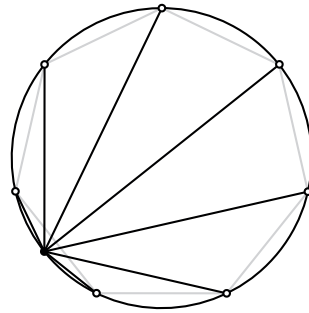
## 146 Stelling van Laisant

Charles-Ange Laisant, militair ingenieur aan de École Polytechnique, wordt de volgende verrassende ontdekking toegeschreven. Teken een regelmatige  $n$ -hoek, ingeschreven in de eenheidscirkel, en trek alle lijnstukken vanuit één hoekpunt naar alle  $n - 1$  andere (dus twee zijden en  $n - 3$  diagonalen). Het product van alle lengtes van deze lijnstukken is dan steevast gelijk aan  $n$ .



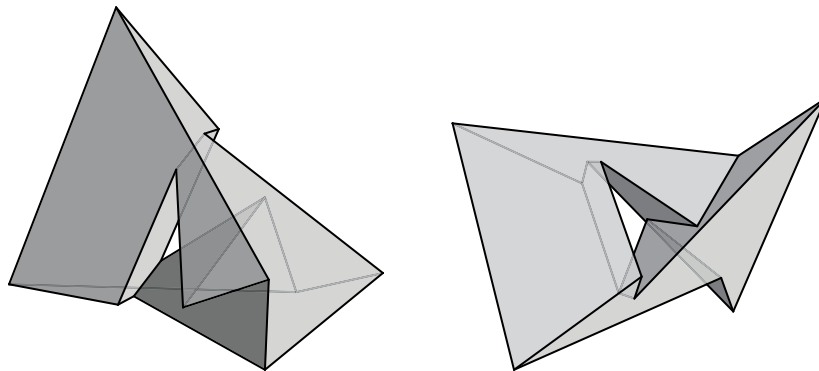
Het totale product van alle zijden en diagonalen is bijgevolg gelijk aan  $\sqrt{n^n}$ .

Een eveneens opmerkelijke variant van de stelling van Laisant is dat wanneer de verbindingslijnen vanuit een punt op de cirkel, halverwege twee punten van de  $n$ -hoek, getekend worden, het product van hun lengtes steeds 2 is, onafhankelijk van  $n$ ! Dit kan eenvoudig aangetoond worden door de originele stelling toe te passen op de uitgebreide  $2n$ -hoek en de regelmatige  $n$ -hoek met deze tussenpunten.



## 147 Veelvlak van Szilassi

Het veelvlak van Szilassi, vernoemd naar en in 1977 ontdekt door Hongaars wiskundige Lajos Szilassi, is naast de tetraëder het enige gekende veelvlak met de eigenschap dat elke twee zijden een ribbe gemeenschappelijk hebben. Hij bestaat uit 7 zeshoekige zijden, 14 toppen en 21 ribben. Topologisch gezien is Szilassi's veelvlak isomorf met een torus, omdat er een gat in zit.



Eulers veelvlakformule (zie ??, blz.??) voor een veelvlak met  $V$  toppen,  $E$  ribben,  $F$  zijvlakken en  $H$  gaten, stelt dat  $V - E + F = 2 - 2H$ . De voorwaarde dat elk paar zijden een ribbe deelt, betekent tevens dat er uit elke tophoek drie ribben moeten vertrekken. Dus gelden de volgende betrekkingen op deze parameters.

$$E = \frac{F \cdot (F - 1)}{2} \quad \text{en} \quad V = \frac{2E}{3} \quad \Rightarrow \quad H = \frac{(F - 4) \cdot (F - 3)}{12}$$

De tetraëder voldoet aan deze voorwaarde met  $H = 0$  en  $F = 4$ ; Szilassi's veelvlak correspondeert met  $H = 1$  en  $F = 7$ . Het is nog onbekend (maar onwaarschijnlijk) of verdere gehele oplossingen tot een geldig veelvlak met meerdere gaten leiden.

Het analogon van de vierkleurenstelling (zie 263, blz. 226) op een torus, stelt dat er ten hoogste zeven kleuren nodig zijn om een toroidale landkaart in te kleuren; het veelvlak van Szilassi bewijst dat minder dan zeven kleuren niet altijd volstaan.

Het duale veelvlak van Szilassi's is dat van Ákos Császár, ontdekt in 1949. Deze heeft 7 toppen, 21 zijden, en 14 driehoekige zijden, en heeft de eigenschap geen enkele ruimtediagonaal te bezitten: elke twee toppen worden verbonden door een zijde.

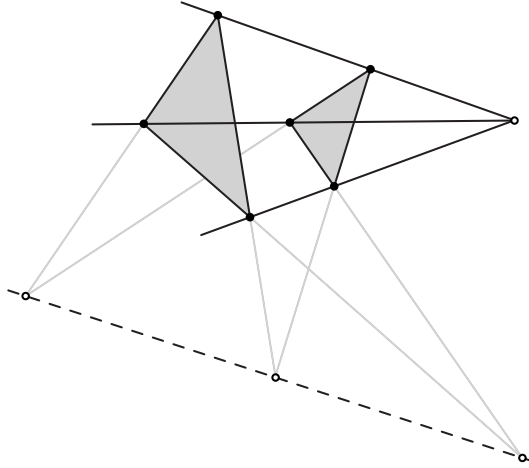
## 148 Stelling van Desargues

De stelling van Desargues wordt vernoemd naar wiskundige en ingenieur Girard Desargues, pionier in de projectieve meetkunde, hoewel het zijn vriend en leerling Abraham Bosse was die de stelling voor het eerst publiceerde, in een praktisch boek omtrent perspectief in 1648.



Twee driehoeken  $\triangle ABC$  en  $\triangle A'B'C'$  staan in lijnperspectief (of zijn coaxiaal) als de snijpunten van de overeenkomstige lijnenparen collineair zijn. De driehoeken heten in puntperspectief (of copolair) als de rechten door de overeenkomstige hoekpunten concurrent zijn.

Volgens Desargues zijn twee driehoeken in lijnperspectief als en slechts als ze ook in puntperspectief zijn:

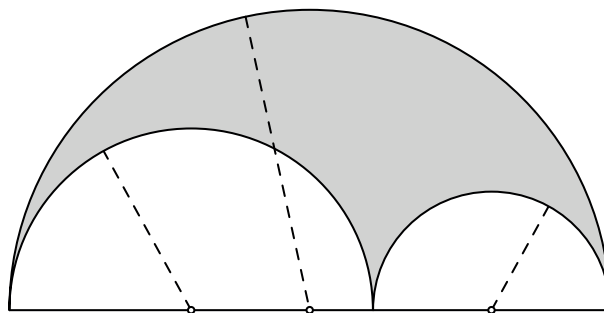


De stelling is uiteraard het krachtigst in de projectieve meetkunde, omdat er uitzonderingsgevallen optreden in het klassieke Euclidische vlak wanneer bepaalde zijden van de driehoeken parallel zijn.

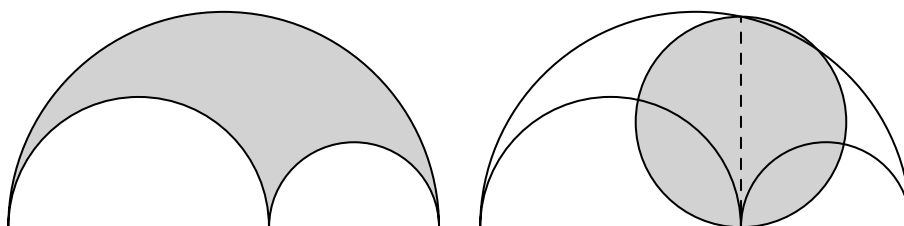
## 149 Arbelos

Deze ronduit wonderbaarlijke meetkundige figuur werd besproken in *Liber Assumptorum* (het boek der lemma's) dat wordt toegeschreven aan Archimedes van Syracuse, hoewel het auteurschap betwistbaar is. Desalniettemin worden de arbelos en diens de tweelingcirkels (zie verder) aan Archimedes toegewezen. De benaming "arbelos" is afkomstig uit het Grieks en betekent schoenmakersmes.

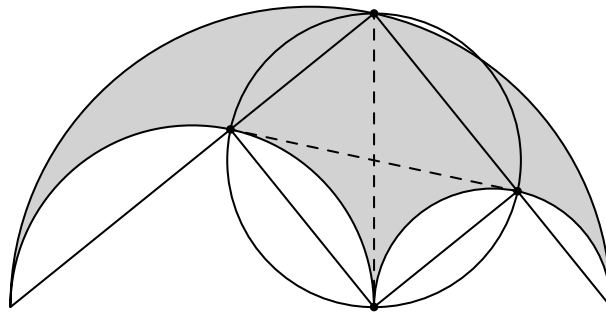
De arbelos wordt begrensd door drie onderling rakende halfcirkels, waarvan er twee volledig omsloten worden door de derde en de raakpunten op een rechte liggen (de basislijn):



Een eerste boeiende eigenschap betreft oppervlakte. Archimedes toonde aan dat deze gelijk is aan de oppervlakte van de cirkel met als diameter de loodrechte op de basislijn tussen de halfcirkels, begrens binnen de arbelos. Zijn omtrek is gelijk aan die van de cirkel met de basislijn als diameter.

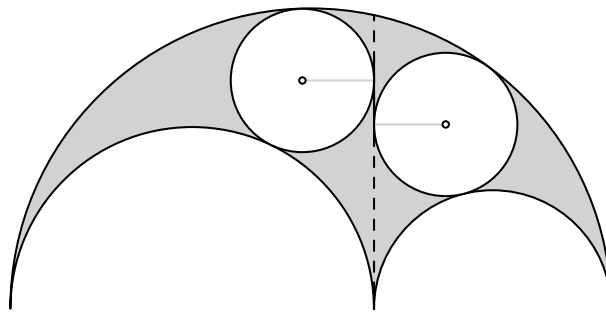


De volgende constructie resulteert in een rechthoek, waarvan beide diagonalen liggen op de gemeenschappelijke raaklijnen van de binnenste halve cirkels.



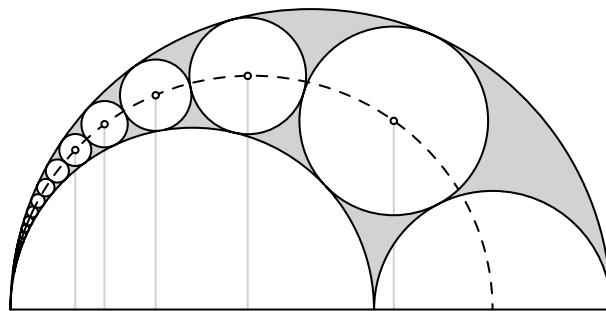
### 149.1 Tweelingcirkels van Archimedes

Er zijn nog heel wat meer sublieme eigenschappen terug te vinden in een arbelos. Archimedes' tweede bekende resultaat is de ontdekking dat zijn zogenaamde tweelingcirkels, die raken aan de loodrechte tussen de binnenste halve cirkels en de arbelos zelf, even groot zijn:



### 149.2 Pappusketen

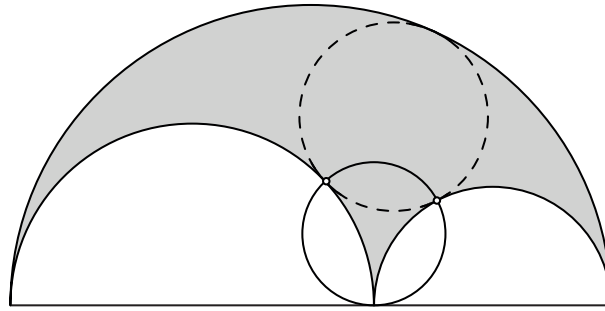
Een ander verbazingwekkend resultaat wordt vernoemd naar Pappus van Alexandrië. Teken in de arbelos een keten van elkaar rakende cirkels, te beginnen bij een van de kleine halfcirkels en rakend aan de andere twee:



Pappus ontdekte nu dat het middelpunt van de  $n^{\text{de}}$  cirkel in de keten, op een hoogte ligt van  $n$  keer zijn diameter boven de basislijn. Daarnaast geldt tevens dat de middelpunten van al deze cirkels op een ellips liggen, wiens brandpunten de middelpunten zijn van de twee halfcirkels waaraan alle Pappuscirkels raken. De onderlinge raakpunten echter liggen allemaal op een cirkel.

### 149.3 Cirkel van Bankoff

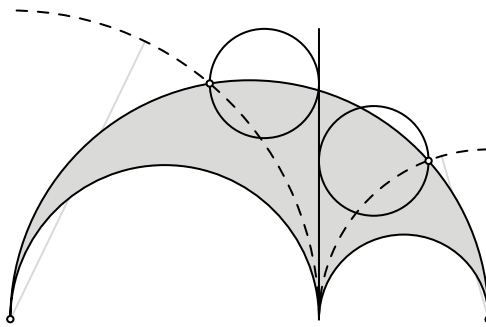
In 1974 construeerde Leon Bankoff een nieuwe cirkel in de arbelos die dezelfde grootte heeft als de oorspronkelijke tweelingcirkels. Dergelijke cirkels worden nu begrijpelijkerwijs Archimedis ch genoemd. Construeer de ingeschreven cirkel van de arbelos. De drie onderlinge raakpunten van de binnenste halfcirkels en deze ingeschreven cirkel bepalen dan een nieuwe cirkel: de cirkel van Bankoff.



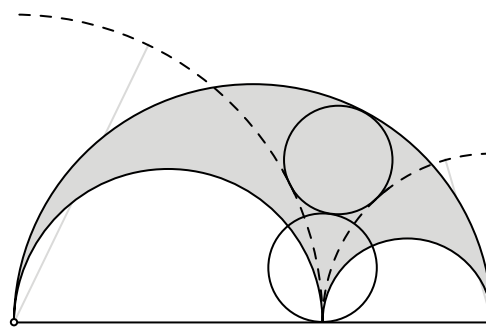
#### 149.4 Cirkels van Schoch

In 1979 (meer dan twee millennia na Archimedes' ontdekkingen) ontdekte Thomas Schoch een dozijn nieuwe Archimedische cirkels. Schoch stuurde zijn vondsten door naar Martin Gardner, die ze verder doorzond naar Leon Bankoff. Deze was van plan een artikel te publiceren over de arbelos, de Schochcirkels inclusief, dat nooit verwezenlijkt werd door Bankoffs overlijden het jaar daarop.

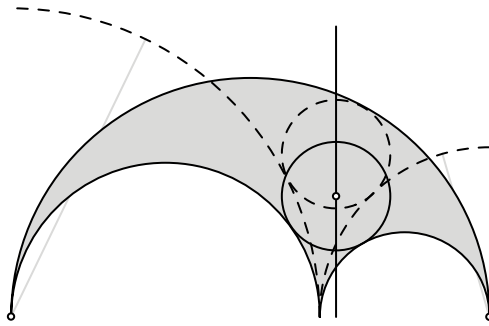
Construeer de cirkels met de uiterste punten van de basislijn als middelpunt, rakend aan de binnenste halfcirkels. Zij snijden de buitenste halfcirkel in twee punten. De kleinste cirkels door deze punten, rakend aan de loodrechte op de basislijn tussen de binnenste halfcirkels, zijn de eerste twee cirkels van Schoch.



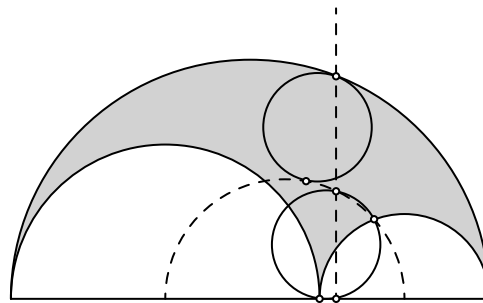
De cirkel ingeschreven in het gebied tussen de buitenste halfcirkel en de twee grote cirkels van daarnet, is Archimedisch. De kleinste cirkel hieraan rakend aan door het middenste punt op de basislijn ook.



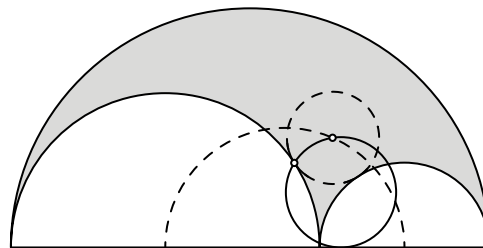
De middellijn van de derde Schochcirkel die loodrecht op de basislijn staat, wordt de rechte van Schoch genoemd. De vijfde cirkel van Schoch is diegene met middelpunt op deze rechte rakend aan de binnenste halfcirkels.



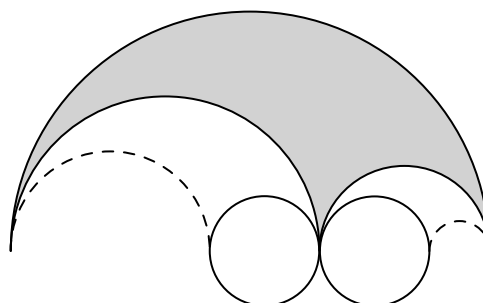
Construeer nu de halfcirkel door de middelpunten van de binnenste halve cirkels. De cirkel hieraan rakend en aan de buitenste halfcirkel in een punt op de rechte van Schoch, is Archimedisches. De rechte van Schoch snijdt ook deze zopas geconstrueerde halfcirkel en de basislijn; de cirkel door deze punten en het punt tussen de middenste halfcirkels vormt de zevende cirkel van Schoch.



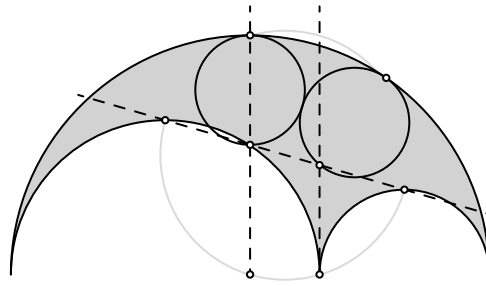
Teken nog een hulpcirkel met middelpunt op de halfcirkel uit de vorige constructie, rakend aan de binnenste halve cirkels. Door het middelpunt van deze hulpcirkel en rakend aan de basislijn, gaat de achtste Schochcirkel.



Teken in de binnenste halfcirkels twee nieuwe arbelossen, gelijkvormig aan de originele. De kleinste nieuwe halfcirkel onder de grootste oorspronkelijke halfcirkel en omgekeerd bepalen de negende en tiende cirkels van Schoch.



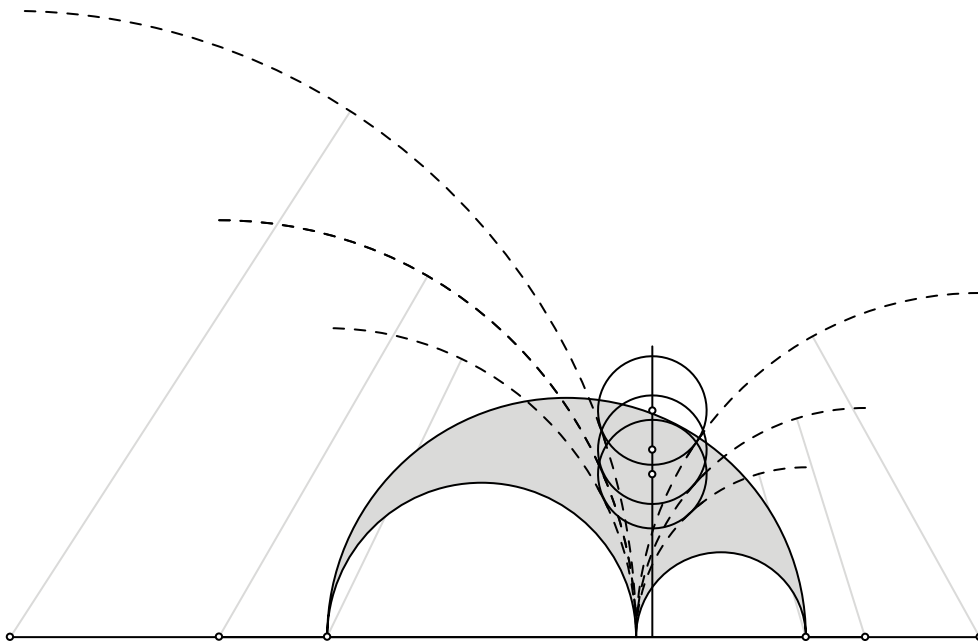
Construeer de rechte  $r$  door de toppunten van de binnenste halfcirkels, en de middellijn van de buitenste halve cirkel loodrecht op de basislijn. De elfde Archimedisches cirkel is de kleinste door het snijpunt van  $r$  met de zonet geconstrueerde middellijn, rakend aan de buitenste halfcirkel. De twaalfde is analoog te vinden, maar dan via de vertrouwde loodlijn door het raakpunt van de binnenste halfcirkels.



De laatste configuratie heeft bovendien de eigenschap dat zes constructiepunten op dezelfde cirkel liggen, waarvan het middelpunt op  $r$  ligt.

### 149.5 Cirkels van Woo

Peter Woo vond nog een oneindige familie Archimedische cirkels. Construeer twee hulpcirkels, met middelpunt op de basislijn, en rakend aan elkaar in hetzelfde punt en met dezelfde verhouding diameters als de middenste halfcirkels van de arbelos. De cirkel met middelpunt op de Schochlijn uitwendig rakend aan zo'n koppel hulpcirkels, is Archimedisch. Andere hulpcirkels betekenen een andere Archimedische cirkel.



## 150 Passer-en-liniaalconstructies

De Griekse meetkundigen beoogden hun constructies uit te voeren met uitsluitend passer en liniaal. Deze spelregels zijn tot zeer veel in staat, maar kennen hun beperkingen; zie ??, blz. ??.

- De passer kan enkel een cirkel construeren met een geconstrueerd punt als middelpunt en de lengte van een geconstrueerd lijnstuk als straal.
- De liniaal, die geen merkpunten heeft, kan enkel een rechte construeren door elke twee geconstrueerde punten en eventueel verlengen.
- Een snijpunt van twee geconstrueerde rechten, een rechte en een cirkel, of twee cirkels, geldt als nieuw geconstrueerd punt.

Elke constructie moet exact zijn en eindigen na een eindig aantal stappen. De enige benodigheid om een geldige passer-en-liniaalconstructie te kunnen starten, zijn twee punten met onderlinge afstand 1.

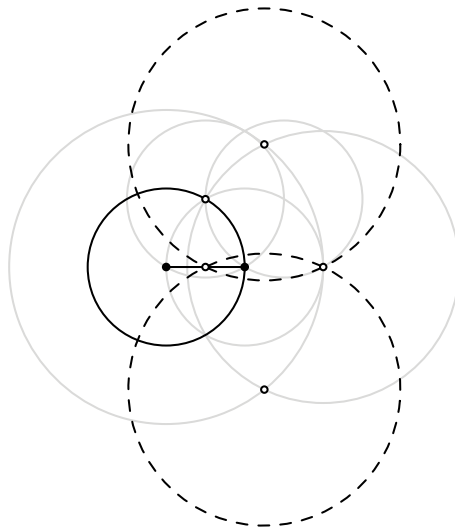
Wanneer de beginpunten abscis 0 en 1 hebben op de reële getallenas, zijn de abscissen van de punten die op deze manier te construeren zijn, juist die getallen die te bereiken zijn door eindige optellingen, vermenigvuldigingen of worteltrekkingen vanuit gehele getallen. Deze getallen heten construeerbaar en vormen een deelveld van  $\mathbb{R}$ . De verwezenlijking van Gauss' 17-hoek bijvoorbeeld (zie 136, blz. 102) steunt op het feit dat het volgende getal construeerbaar is:

$$\cos \frac{2\pi}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

Jean-Victor Poncelet suggereerde in 1882 dat er in feite geen passer nodig is voor deze constructies. Jakob Steiner bevestigde dit met een bewijs in 1833, zolang er een vaste cirkel en diens middelpunt gegeven is. Twee snijdende cirkels zonder middelpunt voldoen ook, of drie niet-snijdende cirkels zonder middelpunt. Dergelijke constructies, die uitsluitend een liniaal gebruiken, heten Steinerconstructies.

Misschien nog verwonderlijker is dat het ook met uitsluitend een passer mogelijk is om de construeerbare punten te construeren, zoals Georg Morh en Lorenzo Mascheroni onafhankelijk van elkaar bewezen. Het probleem van Napoleon bijvoorbeeld verlangt het middelpunt van een gegeven cirkel via zo'n Mascheroniconstructie (zonder liniaal) en is moeilijk, maar wel degelijk oplosbaar.

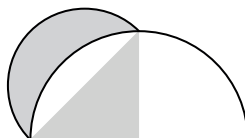
Hier volgt de constructie voor het middelpunt van een lijnstuk zonder gebruik te maken van een liniaal:



## 151 Maantjes van Hippocrates

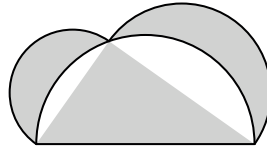
De maantjes van Hippocrates ontvlamden bij velen de hoop op een oplossing voor de cirkelkwadratuur. Hoewel dit probleem onoplosbaar is voor de cirkel (zie ??, blz. ??), lukt het voor deze maantjes wel. Hippocrates van Chios, de Oud-Grieks wiskundige die de figuren beschreef, was de eerste die een systematische en geordende aanpak van de meetkunde verkondigde, in een leerboek genaamd *Stoicheia* (Elementen). Het is zeer waarschijnlijk dat Euclides veel uit zijn latere meetkundig opus baseerde op dat van Hippocrates.

Er is slechts één fragment overgeleverd uit de oorspronkelijke *Stoicheia*, waarin de oppervlakte berekend wordt van de maantjes van Hippocrates. Deze maantjes worden begrensd door twee cirkelbogen:



Hippocrates toonde aan dat zijn maantje dezelfde oppervlakte heeft als de driehoek tussen de diameter en de rechte hoek van daarnet, in het diagram hierboven gekleurd weergegeven.

Naar de Arabische Alhazen vernoemd zijn de volgende maantjes, die een veralgemening geven van de originele van Hippocrates. Deze twee maantjes hebben samen dezelfde oppervlakte als de driehoek.



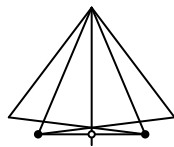
## 152 Luciferconstructies

In 1939 bewees Thomas Dawson een alternatieve manier om de construeerbare punten te bereiken. Hij toonde aan dat alle punten te vinden met passer-en-lijnaal (zie 150, blz. 118), en geen andere punten, ook te vinden zijn via “luciferconstructies”. Dawsons spelregels zijn als volgt, met lucifers van eenheidslengte:

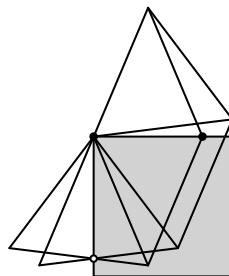
- Een lucifer mag zo geplaatst worden dat die door een geconstrueerd punt gaat, of met zijn uiteinde aan een geconstrueerd punt.
- Lucifers door twee geconstrueerde punten kunnen enkel geplaatst worden als de afstand ertussen ten hoogste 1 is.
- Lucifers mogen niet overlappen, i.e. maximaal één punt gemeenschappelijk hebben.
- Als een punt dicht genoeg ligt bij een geconstrueerde lijn, kan een lucifer zodanig geplaatst worden met z'n ene uiteinde op het punt en z'n andere uiteinde op de lijn.
- Twee lucifers kunnen samengelegd worden tot een gelijkbenige driehoek, waarbij twee van hun uiteinden samenvallen en de andere twee op geconstrueerde punten liggen waartussen de afstand kleiner dan 2 is.

De derde regel dient om te voorkomen dat lijnstukken al te gemakkelijk verlengd kunnen worden. Net als met passer-en-lijnaalconstructies zijn er twee initiële punten nodig, die hier op een afstand van elkaar kleiner dan 1 moeten liggen.

De volgende constructie bepaalt het middelpunt van een lijnstuk.



Een rechte hoek, die dan uit te breiden is naar een volledig vierkant, gaat als volgt:

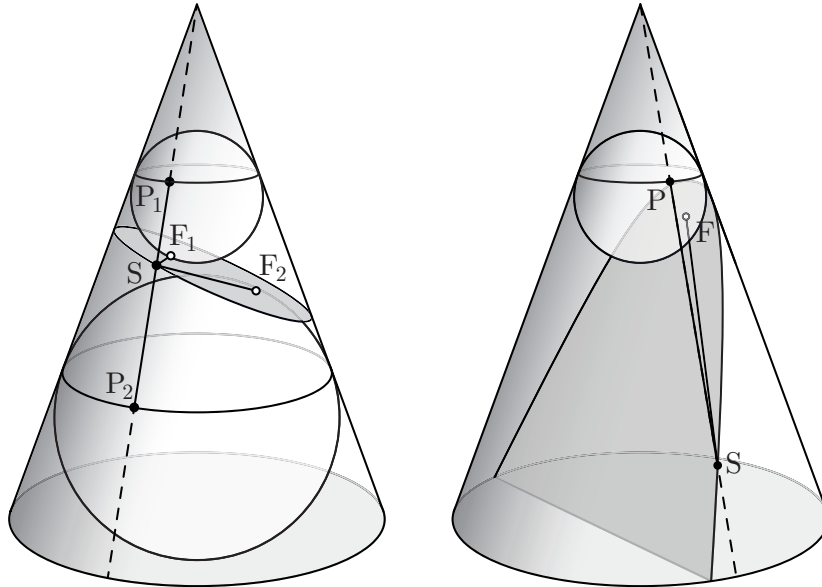


## 153 Bollen van Dandelin

Belgisch wiskundige Germinal Dandelin ontdekte dat meerdere eigenschappen van kegelsnedes in het vlak, terug te vinden zijn in de driedimensionale kegel zelf. Met deze ontdekking formuleerde Dandelin eenvoudige

bewijzen voor eerder gekende resultaten.

Beschouw een kegel en een vlak dat de mantel ervan snijdt, de top vermijdend; hun doorsnede bepaalt dan een kegelsnede. De bollen van Dandelin zijn de bollen die zowel de kegel inwendig raken in een cirkel als het snijvlak. Een ellips zal twee Dandelinbollen hebben, beiden gelegen in dezelfde kegelhelft. Een hyperbool heeft er eveneens twee, maar deze liggen elk in één halve kegel. De parabool ten slotte heeft maar één Dandelinbol.

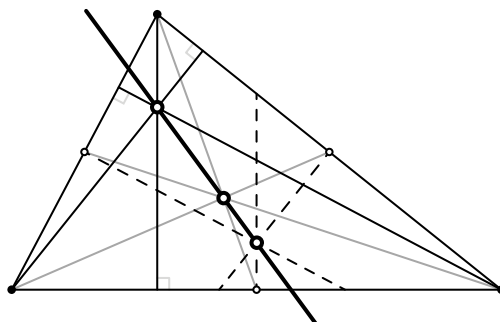


Dandelin toonde aan dat de raakpunten van zijn bollen met het snijvlak, net de brandpunten van de kegelsnede zijn! Daarnaast geldt dat de afstand  $|SF_1|$  in het linkerdiagram gelijk is aan  $|SP_1|$  (omdat beide dragers raken aan dezelfde bol) en dat  $|SF_2|$  gelijk is aan  $|SP_2|$ . Omdat de afstand  $|P_1P_2|$  niet wijzigt wanneer de rechte rond de kegel gaat, is ook de som van de afstanden  $|SF_1| + |SF_2|$  constant. Hetzelfde geldt voor de hyperbool. Bij de parabool rechtsboven zijn de afstanden  $|SF|$  en  $|SP|$  gelijk.

Ook de richtlijnen van de kegelsneden zijn terug te vinden met behulp van Dandelinbollen. De cirkels waarin de bollen raken aan de kegel bepalen een vlak; de snijlijnen tussen deze vlakken en het vlak waarin de kegelsnede ligt zijn diens richtlijnen.

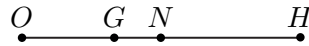
## 154 Rechte van Euler

Leonhard Euler bewees in 1765 dat in een willekeurige driehoek, het zwaartepunt, hoogtepunt en middelpunt van de omgeschreven cirkel stevast collineair zijn. Bij een gelijkzijdige driehoek vallen deze punten samen. Later werden er nog heel wat belangrijke punten toegevoegd aan deze bevinding, zoals het middelpunt van de negenpunts cirkel (zie 137, blz. 103), het punt van Schiffler, het punt van Exeter etc. De gemeenschappelijke rechte waar al deze punten op liggen, heet de rechte van Euler.

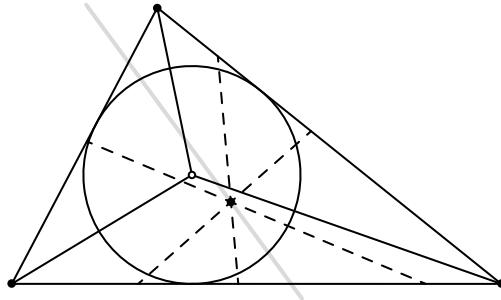




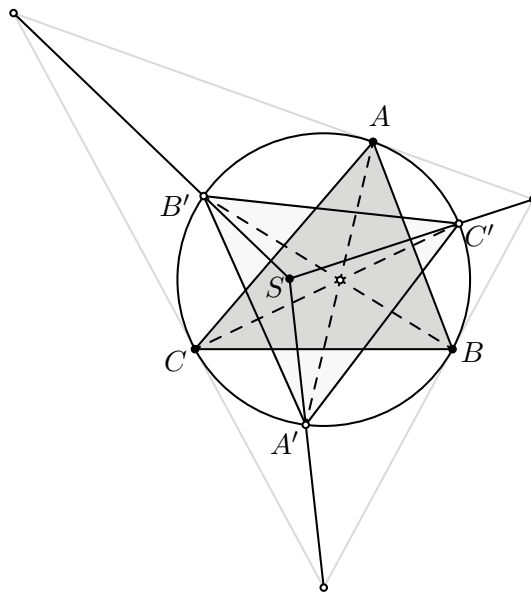
Daarboven vormen het middelpunt  $O$  van de omschreven cirkel, het zwaartepunt  $G$ , het middelpunt  $N$  van de negenpunts cirkel en het hoogtepunt  $H$ , een harmonisch viertal en is de onderlinge relatieve afstand ertussen respectievelijk 2, 1 en 3.



Een ander punt dat ook op de rechte van Euler blijkt te liggen, is het punt van Schiffler. Trek in een driehoek de drie lijnstukken vanuit het middelpunt van de ingeschreven cirkel tot zijn hoekpunten, zodat er een partitie in drie nieuwe driehoeken ontstaat. Construeer in elk van deze driehoeken de rechte van Euler. De stelling van Schiffler stelt dat deze drie rechten concurrent en hun snijpunt, het punt van Schiffler, ligt ook op de Eulerrechte van de originele driehoek.



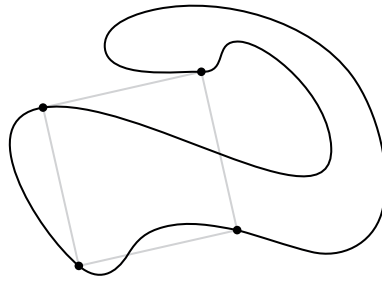
Het punt van Exeter wordt geconstrueerd door de snijpunten  $A'$ ,  $B'$  en  $C'$  van de zwaartelijnen van de driehoek  $\triangle ABC$  met zijn omschreven cirkel. De raaklijnen van de omcirkel met  $A$ ,  $B$  en  $C$  leggen een nieuwe driehoek vast. De verbindingslijnen van zijn hoekpunten met  $A'$ ,  $B'$  en  $C'$  zijn concurrent; hun snijpunt is het punt van Exeter, pas ontdekt in 1986 tijdens een computerworkshop aan de Phillips Exeter Academy.



## 155 Vermoeden van Toeplitz

In 1911 gaf Otto Toeplitz een opmerkelijk eenvoudig te verwoorden, maar lastig op te lossen probleem.

BEVAT ELKE JORDANKROMME (EEN GESLOTEN, CONTINUE LUS IN HET VLAK) VIER PUNTEN DIE DE HOEK-PUNTEN VAN EEN VIERKANT VORMEN?



Welbepaalde figuren (zoals vierkanten en cirkels), bevatten oneindig veel zulke vierkanten; andere (zoals een stomphoekige driehoek) juist één. Een eerste doorbraak voor het algemene geval kwam in 1913 al, toen Arnold Emch de vraag affirmatief beantwoordde voor convexe figuren. Emch verbeterde zijn resultaat twee jaar later, toen hij aantoonde dat het vermoeden klopt voor een kromme die uit eindig veel analytische stukjes opgedeeld kan worden.

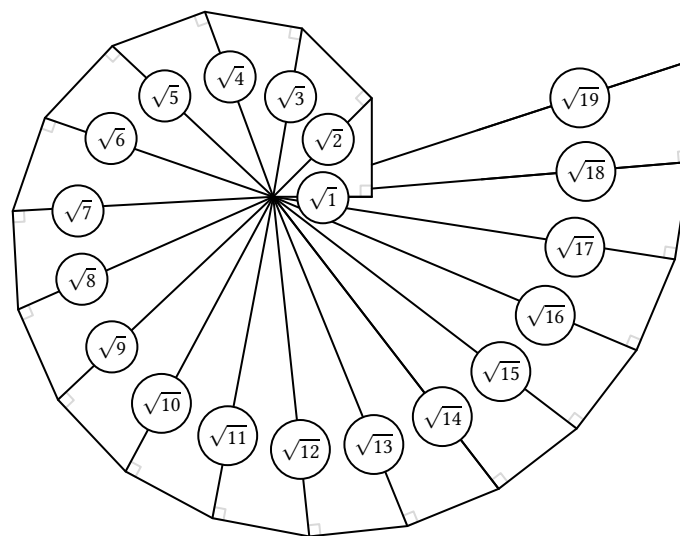
Lev Schnirelmann gaf een bewijs voor krommen die twee maal afleidbaar zijn en een continue tweede afgeleide hebben. Schnirelmanns bewijs bevatte echter een fout, maar werd gecorrigeerd door Heinrich Guggenheimer. Walter Stromquist versoepelde deze eis in 1989 tot eenmaal afleidbaar zijn.

Het beste resultaat tot nog toe bekend werd eveneens gegeven door Stromquist, die aantoonde dat een kromme zeker een vierkant omschrijft als ze lokaal monotoon is, d.w.z. lokaal als een functie  $f(x)$  kan worden weergegeven. Eenvoudigere criteria zijn er nog niet bekend.

Het specifieke geval waarbij de kromme centraal symmetrisch is, werd wel al bevestigd.

## 156 Spiraal van Theodorus

Theodorus van Cyrene was de eerste die deze spiraalstructuur construeerde, die bestaat uit aanliggende rechthoekige driehoeken. Begin bij een driehoek die twee rechthoekszijden met eenheidslengte heeft, en voeg telkens een nieuwe rechthoekige driehoek toe op de vorige zoals op de figuur. Zo heeft de  $n^{\text{de}}$  driehoek dan drie zijden met lengtes  $1$ ,  $\sqrt{n}$  en  $\sqrt{n+1}$ .

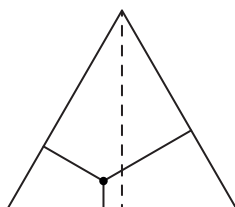


Theodorus stopte zelf bij  $\sqrt{17}$ , waarschijnlijk omdat de volgende driehoek dan de vorige overlapt. Wanneer de spiraal wordt verdergezet zullen de richtingen van twee hypotenusa's nooit samenvallen, zoals Erich Teuffel in 1958 aantoonde. Daarenboven zullen ook de segmenten met eenheidslengte nooit door andere andere hoekpunten op de spiraal gaan als ze verlengd worden.

De afstand tussen twee opeenvolgende windingen convergeert snel naar  $\pi$ , wat impliceert dat de spiraal van Theodorus een Archimedische spiraal benadert.

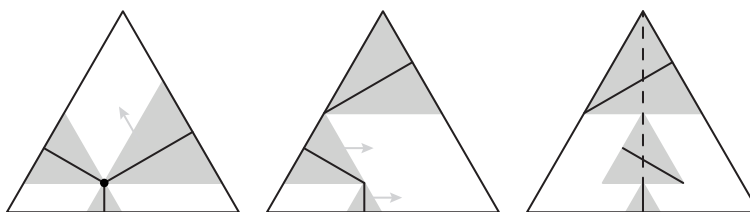
## 157 Stelling van Viviani

De stelling van Vincenzo Viviani, leerling van Galileo Galilei en Evangelista Torricelli, beweert dat de som van de afstanden van eender welk punt binnen een gelijkzijdige driehoek tot diens zijden, constant is. Meer bepaald is die som juist gelijk aan de hoogte van de driehoek, wat dan volgt als limietgeval door het punt te verschuiven naar een hoekpunt.



Omgekeerd geldt eveneens dat wanneer de afstanden tot de zijden van een driehoek optellen tot een som die constant is, onafhankelijk van het gekozen punt binnen de driehoek, dan is deze gelijkzijdig.

De stelling is eenvoudig aan te tonen met behulp van de volgende voorstelling:



Een formeler bewijs volgt door de gelijkzijdige driehoek  $\triangle ABC$  met hoogte  $h$  en zijde  $z$  op te delen. Noem  $P$  het punt binnenin,  $d_a$  de afstand ervan tot de zijde  $a$  (tegenover  $A$ ) en analoog voor de andere zijden. Beschouw dan de driehoeken  $\triangle PBC$ ,  $\triangle APC$ ,  $\triangle ABP$ . Omdat de oppervlakte van  $\triangle ABC$  gelijk is aan die van de drie driehoeken in deze dissectie samen, volgt eenvoudig:

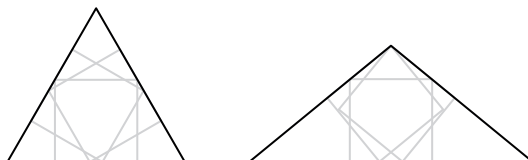
$$\frac{1}{2} zh = \frac{1}{2} zp_a + \frac{1}{2} zp_b + \frac{1}{2} zp_c$$

Oftewel:

$$h = p_a + p_b + p_c$$

## 158 Driehoek van Calabi

Beschouw het grootst mogelijke vierkant ingeschreven in een willekeurige driehoek. Alle vier de hoekpunten zullen dan op de zijden van de driehoek liggen, en bij een gelijkzijdige driehoek zijn er drie zulke grootste vierkanten (zie hieronder links). Eugenio Calabi ontdekte dat er een unieke tweede driehoek bestaat die aan deze eigenschap voldoet, dus waarbij het grootste vierkant op drie verschillende manieren in de driehoek gepositioneerd kan worden:



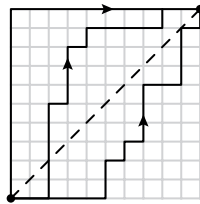
De verhouding tussen de lengtes van de basis en de opstaande zijden is uit te drukken als de grootste wortel van de veelterm  $2x^3 - 2x^2 - 3x + 2$ , of voluit geschreven:

$$\frac{1}{3} + \frac{\sqrt[3]{-23 + 3\sqrt{237}i}}{3\sqrt[3]{4}} + \frac{11}{3\sqrt[3]{-46 + 6\sqrt{237}i}}$$

## 159 Taximeetkunde

Deze alternatieve vorm van meetkunde werd verkend door Hermann Minkowski aan het eind van de 19<sup>de</sup> eeuw. De klassieke Euclidische notie van afstand wordt hier vervangen door een nieuwe metriek, informeel bekend als de Manhattanmetriek vanwege de gelijkenis met het roostervormige stratenplan van Manhattan.

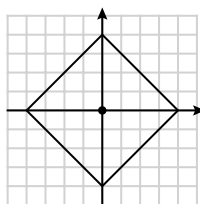
De nieuwe afstand tussen twee punten is de afstand afgelegd via een pad langsheen een rooster:



Deze interpretatie is van toepassing op *discrete* taximeetkunde, waarin er effectief sprake is van punten gerangschikt in een rooster. Steeds fijnere roosters geven in het limietgeval aanleiding tot *continue* taximeetkunde. Formeler wordt de Manhattanmetriek  $d(A, B)$  gedefinieerd als de som van de lengtes van de projecties van het lijnstuk  $[AB]$  op de coördinaatassen. Voor  $A = (a_1, a_2 \dots a_n)$  en  $B = (b_1, b_2 \dots b_n)$ :

$$d(A, B) = \sum_{i=1}^n |a_i - b_i|$$

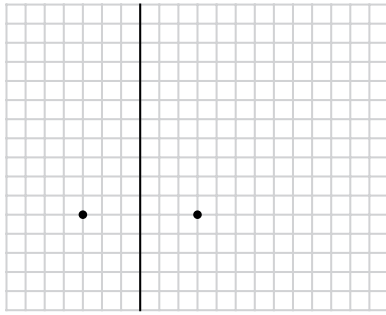
Deze nieuwe afstand heeft verrassende consequenties voor de vorm van vertrouwde meetkundige objecten zoals cirkels. Een cirkel wordt gewoonlijk gedefinieerd als de verzameling van alle punten waarvoor de afstand tot een gemeenschappelijk middelpunt hetzelfde is. Met de Manhattanafstand ziet een "cirkel" om de oorsprong er dan als volgt uit. Alle punten op deze cirkel liggen even ver tot de oorsprong!



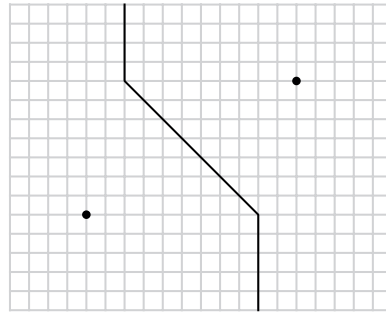
Bemerk dat de verhouding omtrek-diameter hier niet gelijk is aan  $\pi$ , maar aan 4. Hoeken variëren hier kennelijk tussen 0 en 8 en er is eveneens een hele alternatieve taximeetkundige goniometrie af te leiden.

Middelloodlijnen zien er nog vreemder uit. Tussen punten die op eenzelfde horizontale of verticale rechte liggen merken we niks nieuws, maar tussen andere punten bestaat de middelloodlijn (als verzameling van alle punten even ver gelegen van twee gegeven punten) uit drie segmenten, of beslaat ze zelfs twee kwartvlakken! Algemeen wordt de vergelijking van de middelloodlijn tussen  $A(a_1, a_2)$  en  $B(b_1, b_2)$ :

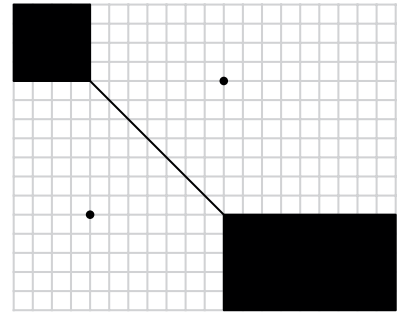
$$|x - a_1| + |y - a_2| = |x - b_1| + |y - b_2|$$



$$\begin{aligned} &|x - 4| + |y - 5| \\ &= |x - 10| + |y - 5| \end{aligned}$$



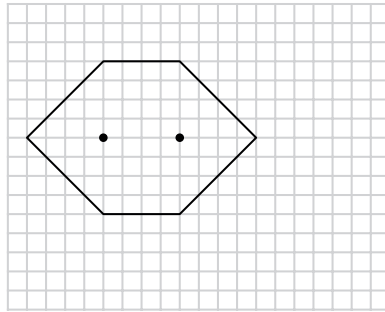
$$\begin{aligned} &|x - 4| + |y - 5| \\ &= |x - 15| + |y - 12| \end{aligned}$$



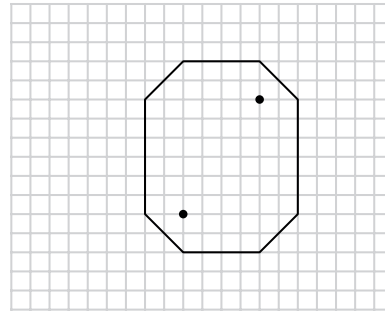
$$\begin{aligned} &|x - 4| + |y - 5| \\ &= |x - 11| + |y - 12| \end{aligned}$$

Per definitie is een ellips de verzameling punten waarvan de som van de afstanden tot twee gegeven brandpunten  $A(a_1, a_2)$  en  $B(b_1, b_2)$  gelijk is; dit resulteert in de volgende vormen en algemene vergelijking:

$$|x - a_1| + |y - a_2| + |x - b_1| + |y - b_2| = c$$



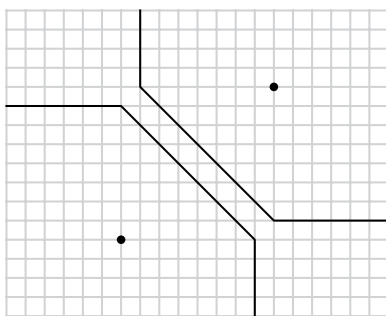
$$\begin{aligned} &|x - 5| + |y - 9| \\ &+ |x - 9| + |y - 9| = 12 \end{aligned}$$



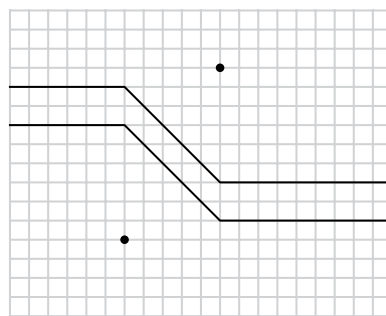
$$\begin{aligned} &|x - 9| + |y - 5| \\ &+ |x - 13| + |y - 11| = 14 \end{aligned}$$

Ook met hyperbolen gebeurt iets bizar. Analoog als de ellips is een hyperbool de verzameling punten waarvan het verschil van de afstanden tot twee gegeven brandpunten  $A(a_1, a_2)$  en  $B(b_1, b_2)$  gelijk is, dus:

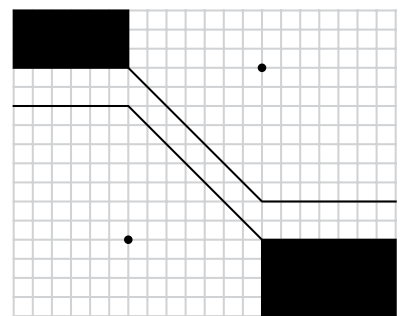
$$||x - a_1| + |y - a_2| - |x - b_1| - |y - b_2|| = c$$



$$\begin{aligned} &||x - 6| + |y - 4| \\ &- |x - 14| - |y - 12|| = 2 \end{aligned}$$



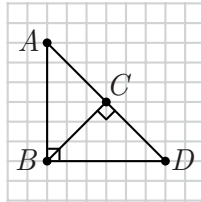
$$\begin{aligned} &||x - 6| + |y - 4| \\ &- |x - 11| - |y - 13|| = 2 \end{aligned}$$



$$\begin{aligned} &||x - 6| + |y - 4| \\ &- |x - 13| - |y - 13|| = 2 \end{aligned}$$

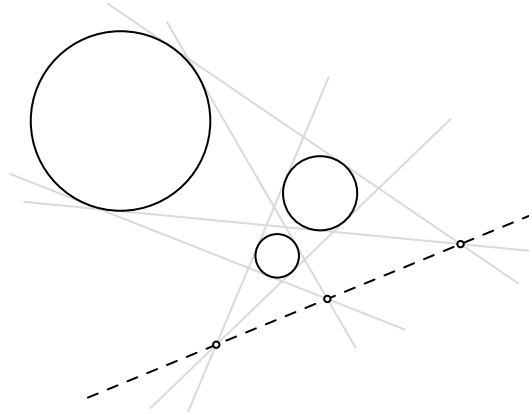
Naargelang de parameters krijgen hyperbolen dus een verschillend uiterlijk.

Zelfs taximeetkundige driehoeken verkrijgen bizarre trekjes:  $\triangle ABD$  hieronder is rechthoekig en heeft zijdelengtes 6, 6 en 12, terwijl  $\triangle BCD$  eveneens rechthoekig is en zijden 6, 6 en 6 heeft (een rechthoekige gelijkzijdige driehoek!). Het congruentiekenmerk zijde-hoek-zijde gaat dus niet op.



## 160 Stelling van Monge

Beschouw drie cirkels in een vlak, met verschillende stralen en niet in elkaar gelegen, en construeer van elk paar cirkels de gemeenschappelijke uitwendige raaklijnen. De stelling van Monge, vernoemd naar Gaspard Monge, stelt dat de snijpunten van deze koppels raaklijnen collineair zijn.



Het verhaal gaat dat toen ingenieur John Sweet deze stelling voor het eerst zag, hij ze “perfect vanzelfsprekend” vond. Zijn argument was tevens de manier waarop Monge zijn resultaat bewees, hoewel het ook klassieker kan met behulp van de stelling van Desargues (zie 148, blz. 113) of Menelaos (zie ??, blz. ??). Sweet stelde de cirkels voor als bollen die op een oppervlak liggen, en hun raaklijnen als kegels errond gewikkeld. De toppen van de kegels liggen dan vanzelfsprekend in het vlak. Leg vervolgens een tweede vlak op de drie bollen; dit vlak moet dan noodzakelijkerwijs de bollen raken en zal dus eveneens de drie toppen van de kegels bevatten. Bijgevolg liggen deze drie punten in de snijlijn van beide vlakken, waarmee hun collineariteit bewezen is.

Monge publiceerde zijn resultaat in 1798 in zijn *Géométrie Descriptive*.

## 161 Vlak van Hilbert

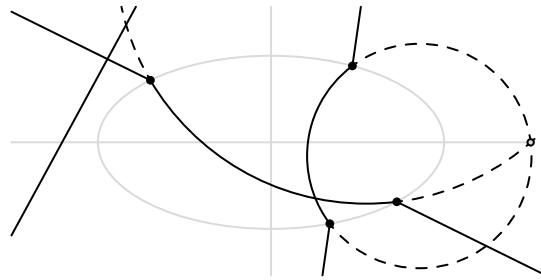
David Hilbert publiceerde in 1899 de *Grundlagen der Geometrie* een geheel nieuw axiomatisch systeem voor de Euclidische meetkunde. Hij gaf oorspronkelijk een stelsel van 21 axioma's, waarvan er één overtoellig bleek en de overige 20 standhielden. Hilberts modernere benadering voor meetkunde nam bijvoorbeeld in tegenstelling tot Euclides het concept congruentie op in de axioma's.

Naast eenvoud, volledigheid\* en consistentie spendeerde Hilbert ook veel tijd en aandacht aan de onafhankelijkheid van de axioma's. Om aan te tonen dat bepaalde clusters axioma's onafhankelijk zijn, construeerde hij expliciet modellen die aan alle axioma's voldoen, behalve één. Een mooi model diende ter illustratie dat de stelling van Desargues (zie 148, blz. 113) niet af te leiden is zonder hulp van de vooropgestelde congruentieaxioma's.

Hilberts model vertrekt van het Euclidische vlak  $\mathbb{R}^2$  waarin de ellips met vergelijking  $x^2 + 4y^2 = 1$  getekend

\*Volledigheid in de zin dat alle tot dan toe bekende meetkunde uit deze axioma's af te leiden diende te zijn. Gödels onvolledigheidsstellingen (zie ??, blz. ??) vernietigden Hilberts droom dat *alle* meetkunde uit zijn systeem zou volgen.

is. Punten ondergaan geen transformatie, rechten buiten de ellips evenmin, maar rechten die de ellips snijden wel: construeer de cirkel door het punt  $(\frac{3}{2}, 0)$  en de twee snijpunten tussen de rechte en de ellips, en definieer de vervormde rechte in het vlak van Hilbert als de unie van de twee halfrechten buiten de ellips met de cirkelboog binnen de ellips. In feite kun je de ellips beschouwen als een soort lens op  $\mathbb{R}^2$ .



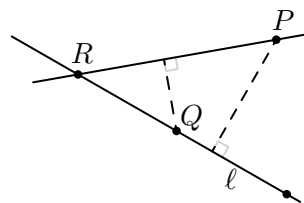
Zoals eenvoudig te controleren is, zijn in deze nieuwe meetkunde de eerste axioma's van kracht, zoals de uniciteit van de rechte door twee gegeven punten of de uniciteit van de rechte door een gegeven punt die een gegeven rechte niet snijdt. Desalniettemin gaat de stelling van Desargues (zie 148, blz. 113) niet op, waarmee Hilbert aantoonde dat het onmogelijk is deze stelling te bewijzen enkel vanuit deze grondbeginselen, zonder congruentie. De congruentieaxioma's zijn dus wel degelijk onafhankelijk.

## 162 Stelling van Sylvester-Gallai

In 1893 stelde James Sylvester dit probleem als een puzzel. Een betrekkelijk moeilijke puzzel, blijktens het feit dat het eerste concrete bewijs pas gegeven werd zo'n 40 jaar later door Tibor Gallai, nadat Paul Erdős het vermoeden herontdekte in 1943. Twee jaar eerder had Eberhard Melchior wel al de projectieve duale versie bewezen (in feite zelfs een iets sterker resultaat).

De stelling van Sylvester-Gallai garandeert dat voor elke eindige configuratie punten in het Euclidische vlak, er altijd een rechte gevonden kan worden die exact twee punten bevat, tenzij al deze punten collineair zouden zijn.

Het mooiste bewijs werd volgens Erdős gegeven door Leroy Kelly. Veronderstel dat elke rechte minstens drie punten zou bevatten, en zoek het koppel  $(P, \ell)$  zijnde het punt  $P$  en de rechte  $\ell$  in de configuratie waartussen de afstand het kleinst is. Beschouw de loodlijn op  $\ell$  door  $P$ . Aangezien  $\ell$  minstens drie punten bevat, kunnen we er zeker twee vinden aan dezelfde kant van deze loodlijn (mogelijks is één punt juist het voetpunt). Noem het punt het verst van de loodrechte gelegen  $R$  en het dichtere punt  $Q$ . Maar dan ligt het punt  $Q$  dicht bij de rechte  $PR$  dan  $P$  ligt bij  $\ell$ : contradictie. Er kan dus geen kleinste positieve afstand bestaan, zodat elk punt op afstand 0 moet liggen van elke rechte, m.a.w. de punten moeten collineair zijn als elke rechte minstens drie punten bevat.



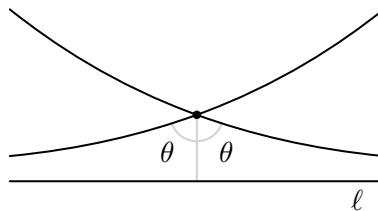
## 163 Hyperbolische meetkunde

Euclides' parallellenpostulaat gaf lange tijd aanleiding tot een flinke controverse. In de Euclidische meetkunde is dit postulaat equivalent met de uitspraak dat er door een gegeven punt juist één rechte gaat die een andere gegeven rechte niet snijdt. Euclides' oorspronkelijke axioma was nog complexer en daarom probeerden velen

tevergeefs de juistheid ervan af te leiden uit andere axioma's. Pas in de 19<sup>de</sup> eeuw werd duidelijk dat het parallellenpostulaat wel degelijk onafhankelijk is, door constructie van een nieuwe consistente meetkunde waarin er door een gegeven punt *minstens twee* rechten gaan die een gegeven rechte niet snijden. Vergelijk dit met de bolmeetkunde (zie ??, blz. ??), waarin er *geen enkele* parallelle rechte door een ander punt gaat.

Deze vernieuwende meetkunde werd later door Felix Klein aangeduid als hyperbolische meetkunde. Pioniers waren János Bolyai (1832) en Nikolai Lobachevsky (1830), die het gebied onafhankelijk van elkaar onderzochten. Carl Friedrich Gauss maakte eerder al observaties maar vond zijn bevindingen nog te ruw om te publiceren.

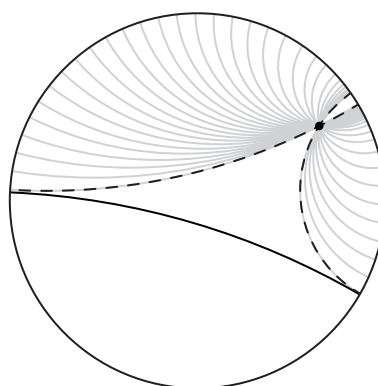
Het vervallen van het parallellenpostulaat geeft hier aanleiding tot twee klassen van parallelisme. Teken de loodlijn door het gegeven punt op de rechte  $\ell$ , en zoek de twee rechten door het punt die  $\ell$  niet snijden en zodat hun hoek  $\theta$  met de loodlijn zo klein mogelijk is, m.a.w. zodanig dat kleinere hoeken rechten opleveren die  $\ell$  wel snijden. Deze twee unieke rechten heten asymptotisch, de oneindig vele rechten ertussen noemt men ultraparallel. Het belangrijkste verschil is dat de afstand tussen een rechte en zijn asymptotische rechten nadert tot nul, terwijl voor ultraparallelle rechten deze afstand in beide richtingen oneindig groot wordt. Er bestaat trouwens wel steeds een unieke rechte die loodrecht staat op twee gegeven ultraparallelle rechten.



Er bestaan vier veelgebruikte modellen voor het hyperbolische vlak. Ondanks hun namen werden de eerste drie geïntroduceerd door Eugenio Beltrami, die ze gebruikte om de equiconsistentie van de hyperbolische meetkunde met de Euclidesche aan te tonen; Felix Klein en Henri Poincaré populariseerden de modellen.

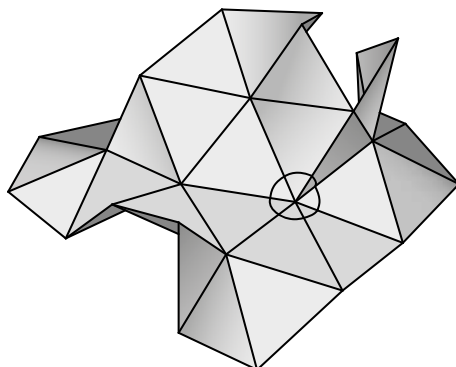
- Het Kleinmodel of het projectieve schijfmodel visualiseert het hyperbolische vlak als het binnengebied van een schijf en hyperbolische rechten als koorden van de cirkel. Als afstand in dit model wordt de dubbelverhouding gebruikt. Deze voorstelling heeft het nadeel dat hoeken vervormd worden.
- Het schijfmodel van Poincaré of het conforme schijfmodel werkt eveneens met het binnengebied van een schijf, maar rechten worden hier voorgesteld als diameters of cirkelbogen loodrecht op de grenscirkel. Deze voorstelling bewaart de hoekgroottes, maar vervormt rechten.
- Het halfvlakmodel van Poincaré gebruikt een halfvlak begrensd door een rechte  $B$ , waarop hyperbolische rechten voorgesteld worden als halfcirkels of halfrechten loodrecht op  $B$ .
- Het Lorentzmodel stelt het hyperbolische vlak voor als een halve tweebledige hyperboloïde.

Een illustratie van Poincaré's schijfmodel met daarop aangeduid asymptotische en ultraparallelle rechten:





William Thurston gaf een model dat duidelijk illustreert hoe er zich meer hyperbolische ruimte rond een punt bevindt dan Euclidische. Knip een aantal gelijkzijdige driehoeken uit en plak deze zodanig aan elkaar dat er zeven driehoeken rond elk hoekpunt zitten. Deze configuratie vormt dan uiteraard geen plat vlak maar een nogal wiebelige structuur, minder vlak naarmate verder van het centrum verwijderd. Dit model is echter nogal onhandig voor rechten en andere concrete meetkunde.



Een andere welbekende hyperbolische eigenschap is dat de hoeken van een driehoek niet meer sommeren tot  $180^\circ$ , maar minder. Driehoeken waarvan de hoekpunten op oneindig liggen, hebben zelfs drie nulhoeken! Deze worden “ideaal” genoemd en bestaan uit drie onderling asymptotische zijden.

Afhankelijk van de Gausskromming  $K$  van het hyperbolische vlak, negatief is en gestandaardiseerd  $-1$ , veranderen ook de afmetingen van meetkundige figuren. Vaak worden afmetingen gemeten in een eenheid  $R = \frac{1}{\sqrt{-K}}$ . Een hyperbolisch analogon voor de stelling van Pythagoras wordt dan, voor een rechthoekige driehoek met rechthoekszijden  $a$  en  $b$ , hypothenusa  $c$ , en tegenoverliggende hoeken  $\alpha$ ,  $\beta$  en  $\gamma$ :

$$\cosh a \cdot \cosh b = \cosh c$$

Veralgemeend gelden deze cosinusregel en zijn duale:

$$\begin{cases} \cosh c = \cosh a \cdot \cosh b - \sinh a \cdot \sinh b \cdot \cos \gamma \\ \cos \gamma = -\cos \alpha \cdot \cos \beta + \sin \alpha \cdot \sin \beta \cosh c \end{cases}$$

Er bestaat ook een hyperbolische sinusregel.

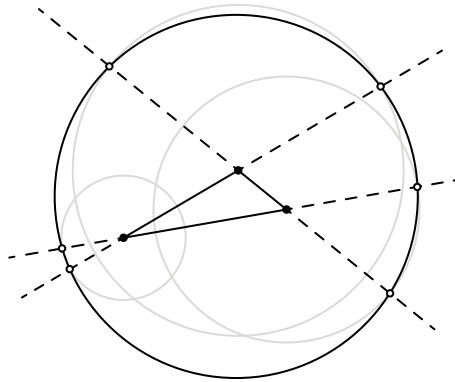
$$\frac{\sin \alpha}{\sinh a} = \frac{\sin \beta}{\sinh b} = \frac{\sin \gamma}{\sinh c}$$

De oppervlakte van een hyperbolische driehoek wordt gegeven door  $(\pi - \alpha - \beta - \gamma) \cdot R^2$ . Merk op dat een ideale driehoek een maximale oppervlakte bereikt. Overigens zijn hyperbolische driehoeken enkel gelijkvormig als ze ook congruent zijn, een eigenschap die ook voorkomt in bolmeetkunde.

Cirkels met straal  $r$  hebben een omtrek van  $2\pi R \sinh \frac{r}{R}$  en een oppervlakte van  $2\pi R^2 (\cosh \frac{r}{R} - 1)$ .

## 164 Cirkel van Conway

Nog een mooie stelling van John Conway. Verleng de zijden van een driehoek en meet vanuit elk hoekpunt een afstand af gelijk aan de lengte van de overstaande zijde. De zes geconstrueerde punten liggen dan op één cirkel.



## 165 Kleins vierdegraadskromme

Het complexe projectieve vlak wordt beschreven door drie complexe coördinaten  $(z_1, z_2, z_3) \in \mathbb{C}^3$ , waarbij de drie coördinaten niet tegelijk nul mogen zijn en drietallen die slechts een constante factor verschillen met gelijke punten corresponderen. In de klassieke projectieve meetkunde zijn dit homogene coördinaten.

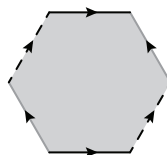
In deze habitat beschouwde Felix Klein in 1878 volgende homogene vierdegraadsvergelijking:

$$z_1^3 \cdot z_2 + z_2^3 \cdot z_3 + z_3^3 \cdot z_1 = 0$$

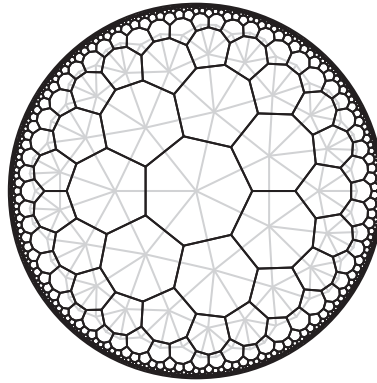
Het oppervlak gedefinieerd door deze vergelijking is topologisch tweedimensionaal, maar wordt lokaal beschreven door slechts één complexe parameter. Daarom spreekt men eerder van een kromme i.p.v. een oppervlak.

Klein toonde aan dat zijn moeilijk te visualiseren vierdegraadskromme genus 3 heeft (m.a.w. eruitziet als een torus met drie gaten) en ongelooflijk symmetrisch is: 168 oriëntatiebewarende symmetrieën, of dubbel zoveel als ook spiegelingen toegelaten zijn. Een stelling van Adolf Hurwitz klasseert dit zelfs als het maximum haalbare! Een gewone sfeer heeft duidelijk oneindig veel symmetrieën, net als een torus. Hurwitz toonde in 1893 echter aan dat vanaf genus  $g \geq 2$  dit aantal eindig wordt, en naar boven begrensd door  $84(g - 1)$ , spiegelingen niet inbegrepen. Met  $g = 3$  wordt dat juist 168. De vreemde coëfficiënt 84 is te verklaren vanuit Eulers veelvlakformule (zie ??, blz. ??).

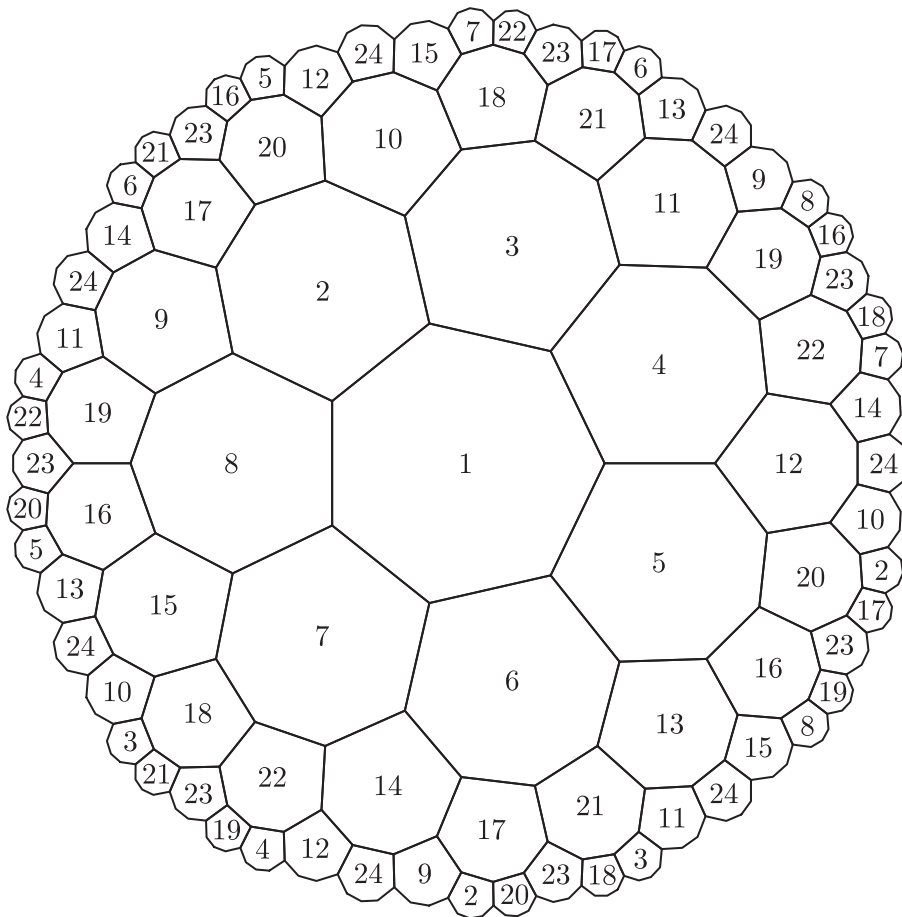
Een andere manier om de vierdegraadskromme van Klein te bestuderen is via hyperbolische betegelingen. Neem een aantal gelijkzijdige driehoeken en plak ze aan elkaar, met drie rond één hoek: het resultaat is een tetraëder (zie ??, blz. ??). Met vierkanten en regelmatige vijfhoeken levert dat respectievelijk een kubus en een dodecaëder op, maar met zeshoeken een betegeling van het vlak in een honingraatpatroon. Om een eindige structuur te verkrijgen, kan een deel van zo'n betegeling opgerold worden tot een torus. Dit kan op vele manieren; in feite lukt het zelfs al met één zeshoek als volgt:



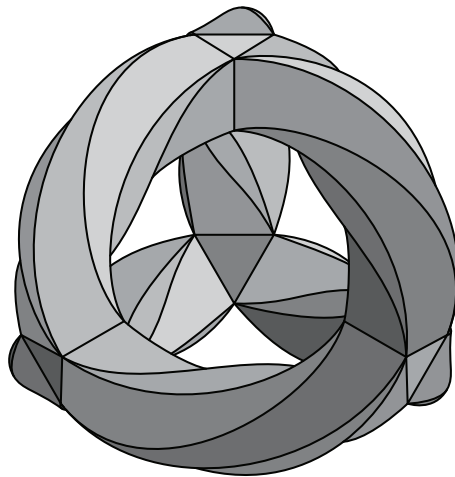
Regelmatige zevenhoeken, gerangschikt met drie rond één hoekpunt, passen niet in de klassieke Euclidische ruimte. Ze resulteren in een hyperbolische betegeling, die er als volgt uitziet in het model van Klein (zie 163, blz. 128). Opmerkelijk is dat de aantallen zevenhoeken even ver van de centrale zevenhoek, gegeven worden door 7, 7, 14, 21, 35, 56, 91... oftewel zeven keer de Fibonaccigetallen (zie 91, blz. 65)!



Het is niet mogelijk om een deel van deze tessellatie uit te knippen en op te rollen tot een torus met één gat. Een torus met drie gaten lukt wel, uitsluitend met precies 24 zevenhoeken. Het diagram hieronder illustreert hoe: zorg dat alle zevenhoeken met hetzelfde getal op elkaar geplakt worden, en het resultaat komt overeen met de vierdegraad van Klein, die dus betegeld kan worden met 24 congruente, regelmatige hyperbolische zevenhoeken.



Zonder de zevenhoeken te vervormen wordt dit een knoeiboel. Beschouw daarom de duale tessellatie: verbind de middelpunten van aanliggende zevenhoeken en het resultaat is een betegeling van driehoeken met telkens zeven driehoeken gerangschikt rond elk hoekpunt. Greg Egan wist daarmee met hulp van Mike Stay en Gerard Westendorp de volgende voorstelling te construeren, weliswaar sterk vervormd maar duidelijker qua symmetrie. Merk de tetraëderstructuur op!



De zevenvoudige symmetrie van Kleins vierdegraadskromme is het eenvoudigst te visualiseren als rotaties in de zevenhoekige tessellatie. De voorstelling als tetraëder onthult een extra twaalfvoudige symmetrie. Daarenboven kan deze structuur ook “binnenstebuiten” gekeerd worden. De 168 combinaties hiervan beschrijven alle mogelijke symmetrieën van de vierdegraadskromme van Klein.

Kleins kromme komt in verschillende wiskundige concepten terug. Zo kan het geval  $n = 7$  van de laatste stelling van Fermat (zie ??, blz. ??) ermee bewezen worden, of de stelling van Stark-Heegner (zie ??, blz. ??), en blijken er connecties te zijn met de vermenigvuldiging van octonionen.

## 166 Tarski's cirkelkwadratuur

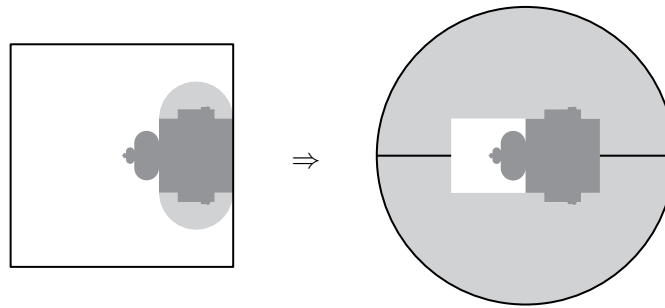
Geïnspireerd door het probleem van de cirkelkwadratuur (zie ??, blz. ??) poneerde Alfred Tarski in 1925 een gelijkaardig vraagstuk.

IS HET MOGELIJK EEN CIRKELSCHIJF IN EEN EINDIG AANTAL STUKKEN TE PARTITIONEREN EN DIE TE TERUG SAMEN TE VOEGEN TOT EEN VIERKANT VAN DEZELFDE GROOTTE?

Anders dan het klassieke passer-en-liniaalprobleem is de cirkelkwadratuur van Tarski wél realiseerbaar, zoals Miklós Laczkovich in 1990 aantoonde. Laczkovich' bewijs steunt hevig op het keuzeaxioma en is daardoor niet-constructief, maar zijn decompositie verdeelt de cirkel in zo'n  $10^{50}$  stukken! Deze zijn echter niet meetbaar; in het bijzonder is het effectief onmogelijk om een cirkel aldus te “verknippen” in stukken met een Jordankromme (??, blz. ??) als grens.

In feite bewees Laczkovich een sterker resultaat: de stukken terug samenvoegen tot een vierkant lukt met uitsluitend translaties; rotaties zijn niet vereist! Daarenboven geldt dit niet alleen voor een cirkel, maar voor eender welk eenvoudig veelvlak. De gerelateerde stelling van Wallace-Bolyai-Gerwien stelt dat zo'n veelvlak bovendien in *polygonale* stukken verdeeld kan worden, mits de reassemblage ook rotaties toelaat. Uit een resultaat van Trevor Wilson uit 2005 volgt trouwens nog dat het mogelijk is de stukken in Tarski's decompositie zodanig te kiezen dat ze continu verschoven kunnen worden zonder te overlappen.

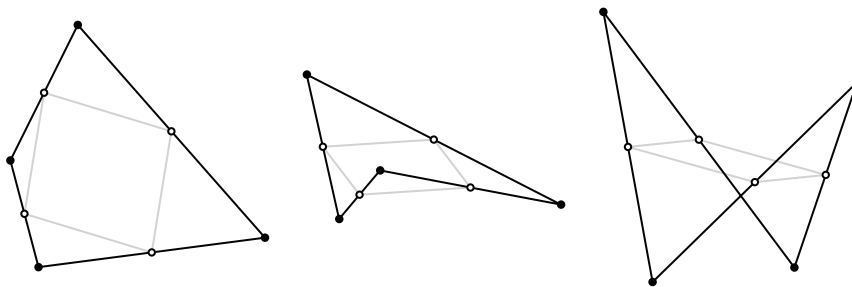
Als de stukken herschaald mogen worden tijdens het reassemblageproces, is een zeer elegante verknipping in vier fractale stukken mogelijk.



## 167 Parallellogram van Varignon

Pierre Varignon publiceerde in 1731 volgende elegante stelling. Vertrek vanuit een willekeurige vierhoek en verbind de middens van diens zijden; het resultaat is dan steeds een parallellogram. Daarenboven is de oppervlakte van dit parallellogram net de helft van de oorspronkelijke vierhoek.

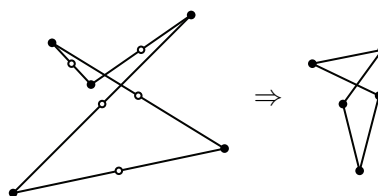
Het parallellogram van Varignon duikt ook op bij concave of zichzelf snijdende vierhoeken, maar in het tweede geval gaat de oppervlakte-eigenschap verloren (behalve bij een soort “georiënteerde oppervlakte”). Zelfs als de hoekpunten van de vierhoek niet in één vlak liggen blijft de stelling geldig, en is het parallellogram toch planair.



Het parallellogram van Varignon is een ruit als en slechts als de twee diagonalen van de originele vierhoek even lang zijn, en een rechthoek als en slechts als de diagonalen loodrecht op elkaar staan.

## 168 Veelhoeken effenen

Adam Elmachtoub en Charles Van Loan bestudeerden een interessante methode om veelhoeken uit te middelen. In hun artikel *From random polygon to ellipse: an eigenanalysis* definieerden ze het “gemiddelde” van een veelhoek als de nieuwe veelhoek verkregen door de middelpunten van opeenvolgende zijden te verbinden.



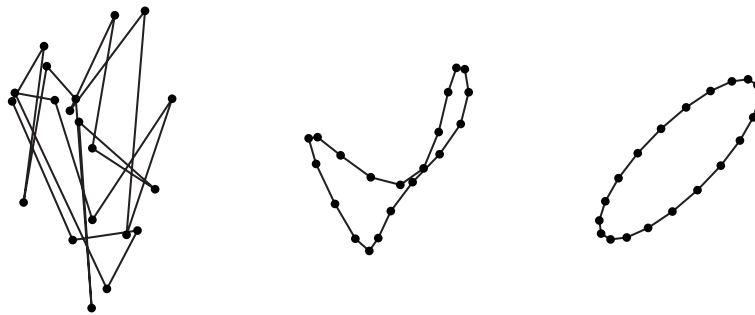
De beschouwde veelhoeken hoeven bijlange niet convex te zijn en mogen zelfs zichzelf snijden. Elmachtoub en Van Loan onderzochten wat er gebeurt als een willekeurig gegenereerde veelhoek steeds opnieuw uitgemiddeld wordt. Zoals de titel van hun artikel uitwijst, lukte dit hen via matrices: noteer de  $n$ -hoek als  $\mathcal{P}(x, y)$ , waarin  $x$  de kolomvector voorstelt met als componenten de  $x$ -waarden van de hoekpunten en  $y$  die met de corresponderende

$y$ -waarden. De gemiddelde veelhoek  $\mathcal{P}(\hat{x}, \hat{y})$  vindt men dan d.m.v. een lineaire afbeelding  $M_n$ :

$$\hat{x} = M_n \cdot x \quad \text{met } M_n = \frac{1}{2} \begin{bmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 & 0 \\ 0 & 0 & \dots & \dots & 1 & 1 \\ 1 & 0 & \dots & \dots & 0 & 1 \end{bmatrix}$$

Deze lineaire afbeelding bewaart het zwaartepunt. Na herhaaldelijke toepassing blijkt de rij veelhoeken te convergeren naar een enkel punt, dat dan wel het zwaartepunt moet zijn. Opmerkelijker is dat als de veelhoeken na elke stap herschaald worden zodat de verkleining geen rol speelt, blijkt dat elke willekeurige veelhoek (hoe chaotisch ook) uiteindelijk “ontwart” en diens hoekpunten zich leggen volgens een ellips, precies  $45^\circ$  gedraaid ten opzichte van de coördinaatassen!

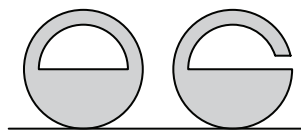
Het proces toegepast op zo'n willekeurige veelhoek, met daarbij het effect na 18 en 200 uitmiddelingen:



Een animatie is te vinden op <http://www.jasondavies.com/random-polygon-ellipse>.

## 169 Gömböc

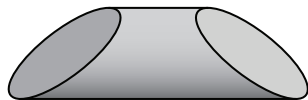
Tuimelaars, speelgoedjes die vanzelf terug rechtop bewegen als ze worden scheefgeduwd, fascineren niet alleen kinderen maar ook wiskundigen. Deze tuimelaars zijn eenvoudig te construeren door hun ronde onderkant te verzwaren, of hun binnenkant uit te hollen als op de figuur.



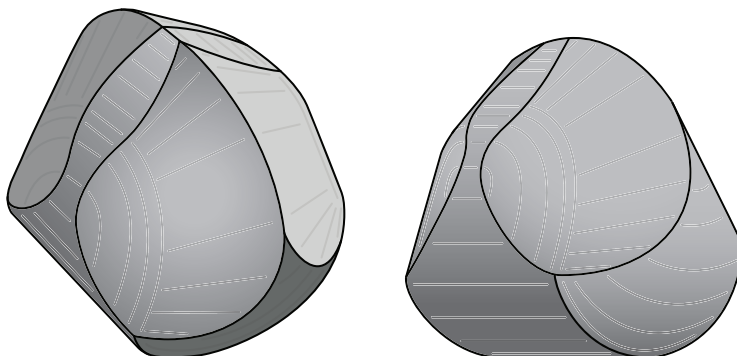
Wiskundigen vroegen zich ook af of er een “eerlijke” tuimelaar bestaat, zonder holtes of verzwaarde zijden. Concreet zoekt men een convex, homogeen, mono-monostatisch lichaam, waarbij die laatste eigenschap betekent dat het juist één stabiel en één instabiel evenwichtspunt moet bezitten. Zo'n lichaam werd een gömböc gedoopt, als /'gomböts/ uitgesproken en Hongaars voor plomp of bolvormig.

In twee dimensies is de kwestie aanschouwelijker. Een vierkant staat in stabiel evenwicht op elk van zijn zijden, maar ook op zijn hoekpunten, zij het instabiel: bij de kleinste beroering valt hij om. Een driehoek doet het met drie stabiele en drie instabiele evenwichtspunten beter, en een ellips heeft er van elk slechts twee. Een gevolg van de viertoppenstelling (zie ??, blz. ??) is dat het beter dan dat niet kan: de krommingsfunctie van een gesloten, eenvoudige, gladde en planaire kromme heeft minstens vier extrema, meer bepaald minstens twee minima en twee maxima, die corresponderen met respectievelijk stabiele en instabiele evenwichtspunten. Tweedimensionale gömböcs bestaan dus niet.

Het lijkt verleidelijk dat een analoog resultaat opgaat in drie dimensies. Daar is echter meer variatie mogelijk, zoals Gábor Domokos met het tegenvoorbeeld hieronder inzag. Deze scheef afgezaagde cilinder heeft juist één stabiel evenwichtspunt (zoals hij afgebeeld staat), en daarnaast zijn er ook drie instabiele evenwichten, met name op z'n kop of balancerend op een puntig uiteinde.



Het bestaan van een waarachtige gömböc werd pas in 1995 door Russisch wiskundige Vladimir Arnold vermoed en in 2006 door Gábor Domokos en Péter Várkonyi bevestigd. De eerste gömböc die het vermoeden van Arnold bewees, geleek door de convexiteitseis echter zoveel op een bol dat Domokos en Várkonyi een karakteristiekere vorm zochten. Uiteindelijk vonden ze dit model.



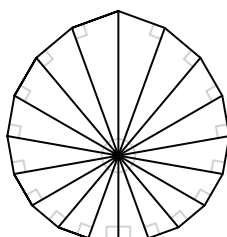
Hoe je dit lichaam ook positioneert, hij rolt altijd terug naar dezelfde evenwichtspositie, rechts afgebeeld. Opmerkelijk genoeg waren de twee Hongaarse wiskundigen niet de eerste ontdekkers: bepaalde soorten schildpadden maken gebruik van een bij benadering gömböcvormig schild om zonder moeite terug juist te rollen wanneer ze omgekeerd verzeild geraken!

Winnaars van de Stephen Smaleprijs, om de drie jaar uitgereikt aan jonge talenten in computationele wiskunde, krijgen een gegraveerde gömböc als trofee.

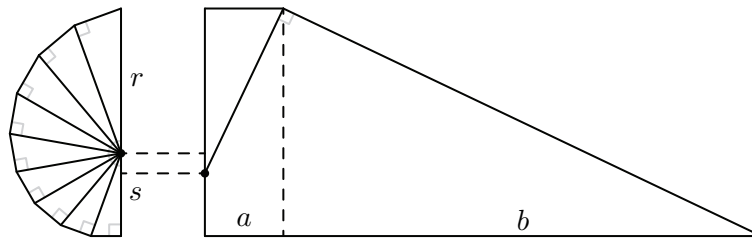
## 170 Monostatisch veelvlak

Een vergelijkbare kwestie als de gömböc (zie 169, blz. 135) vraagt naar een convex, homogeen veelvlak dat maar op één zijvlak stabiel staat. Als zo'n monostatisch veelvlak of *unistable polyhedron* op een andere zijde gelegd wordt, rolt deze dan terug naar die unieke stabiele positie. Een meetkundige karakterisatie stelt dat het zwaartepunt van uitsluitend zo'n veelvlak bij orthogonale projectie op zijn zijvlakken binnen juist één zijvlak ligt.

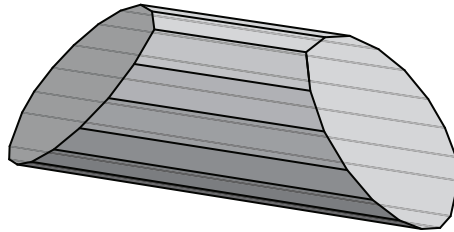
Richard Guy en John Conway waren de eerste die een veelvlak vonden dat aan de vereisten voldoet. Hun vondst vertrekt vanuit een prisma, waarvan de dwarsdoorsnede geconstrueerd wordt met  $2m$  rechthoekige driehoeken, die met gelijke hoeken rond het centrum zitten zoals in de figuur hieronder. Noteer de afstand centrum-top als  $r$  en de afstand centrum-bodem als  $s$ . Met wat straightforward goniometrie volgt hieruit zonder veel moeite dat  $s = r \cdot \cos^m\left(\frac{2\pi}{m}\right)$ .



Daarna dient deze bilateraal symmetrische  $(2m - 1)$ -hoek als grondvlak van een prisma, die scheef wordt afgezaagd en zo nog twee nieuwe zijvlakken oplevert. Op de figuur hieronder staat een half zijaanzicht.



Opdat aan de karakterisering voldaan is, is het van belang de parameters  $a$ ,  $b$  en  $m$  zodanig te kiezen dat het zwaartepunt van het resulterende lichaam enerzijds onder het centrale punt in de doorsnede valt (dan valt de projectie van het zwaartepunt enkel binnen de onderste zijde) en anderzijds boven de loodrechten op de zaagvlakken (dan mist de projectie van het zwaartepunt ook deze twee vlakken). Conway en Guy konden uitrekenen dat dit slechts lukt vanaf  $m = 9$ , wanneer  $b$  voldoende groot is ten opzichte van  $a$ , en gaven daarmee een monostatisch veelvlak met 19 vlakken, thans nog altijd het record.



Wanneer het veelvlak hol verondersteld wordt, als een polyhedraal oppervlak, dan bestaat er wel een soortgelijk uitzienend monostatisch veelvlak met slechts 15 zijvlakken. Wanneer enkel de ribben massa hebben, wordt dit nog verbeterd door een polyhedraal skelet met 13 vlakken.

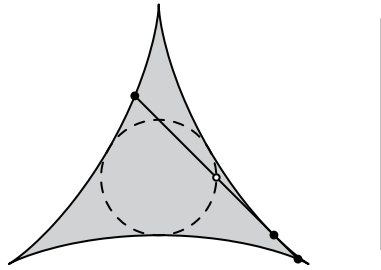
Door reductie tot de viertoppenstelling (zie ??, blz. ??) kon Vladimir Arnold bewijzen dat monostatische veelhoeken (in twee dimensies) niet bestaan. Er is ook bewezen dat monostatische simplices niet bestaan tot in acht dimensies, maar wel vanaf tien dimensies!

## 171 Kakeyaverzamelingen

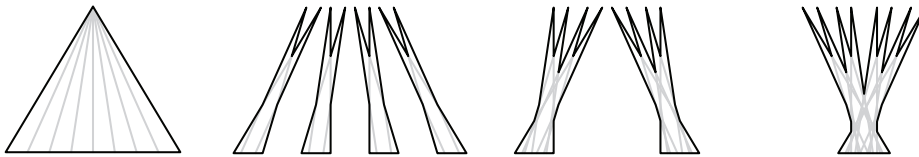
Kakeyaverzamelingen zijn verzamelingen punten in de Euclidische ruimte die een lijnstuk met eenheidslengte in elke mogelijke richting bevatten. Als daarenboven een lijnstuk met eenheidslengte erbinnenin continu kan worden geroteerd over  $360^\circ$ , spreekt men van een Kakeya-naaldverzameling (*needle set*). Een eenheidsschijf is een duidelijk voorbeeld. Beide concepten zijn vernoemd naar de Japanse wiskundige Sōichi Kakeya.

Kakeya stelde in 1917 ook de vraag hoe groot de *kleinste* naaldverzameling is. Wanneer convexiteit vereist is, vermoedde Kakeya dat de gelijkzijdige driehoek met hoogte één de verzameling met minimale oppervlakte is, wat inderdaad enkele jaren later bewezen werd door Julius Pál. Daarnaast speculeerde Kakeya dat de deltoïde (zie 188, blz. 152) hieronder afgebeeld de algemene oplossing is, waarin de naald net kan roteren en op elk moment van de rotatie de omhullende deltoïde in drie punten aanraakt: de twee uiteinden van het lijnstuk en één raakpunt. Het middelpunt van de naald beschrijft juist een cirkel met een diameter half zo lang als de naald.

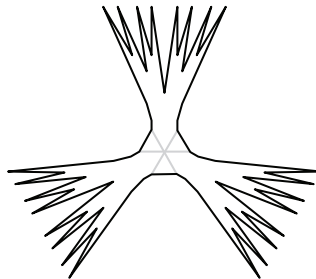




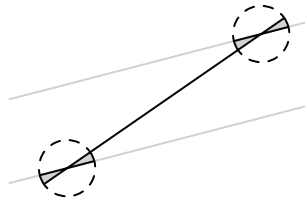
Door de isolatie tussen de Sovjet-Unie en de Westerse wereld was Russisch wiskundige Abram Besicovitch niet op de hoogte van Kakeya's naaldenvraagstuk totdat hij Rusland verliet. Tijdens zijn onderzoek naar integreerbaarheid stuitte Besicovitch echter eveneens op het concept van de Kakeyaverzamelingen (soms ook naar hem vernoemd) en wist hij aan te tonen dat er zulke verzamelingen bestaan met willekeurig kleine maat. Zijn constructie maakt gebruik van zogenaamde Perronbomen:



De gelijkzijdige driehoek links met hoogte één bevat duidelijk een eenheidslijnstuk in elke richting tussen de linker- en rechterzijde. Dissecteer deze driehoek door zijn basis onder te verdelen in  $2^n$  even lange stukken en overlap elk opeenvolgend paar driehoekjes. Blijf dit herhalen tot er één boomachtige structuur overblijft; deze voldoet evenzeer aan Kakeya's criterium als de initiële driehoek maar heeft een kleinere oppervlakte, die steeds meer afneemt naarmate  $n$  toeneemt. Stel dan drie zulke Perronbomen samen om een waarachtige Kakeyaverzameling te vormen, die naalden in elke mogelijke richting bevat en willekeurig kleine maat heeft. Besicovitch kon aantonen dat er ook bestaan met exact maat nul.



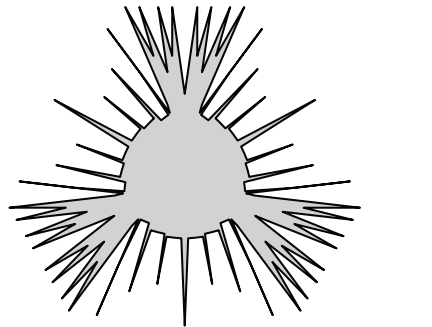
Dankzij een trucje van Pàl, een constructie van een verzameling met willekeurig kleine maat (een Pàlkoppeling) waarin een lijnstuk zich tussen twee parallelle rechten kan verplaatsen, liet Besicovitch zien dat er ook Kakeya-naaldenverzamelingen bestaan met willekeurig kleine maat! Pàlkoppelingen zijn eenvoudig te construeren:



Verklein de hoek tussen de rechten en de verbindingslijn voor een kleinere oppervlakte. Merk op dat door deze koppelingen de figuur niet langer enkelvoudig samenhangend is en een zeer grote diameter kan hebben.

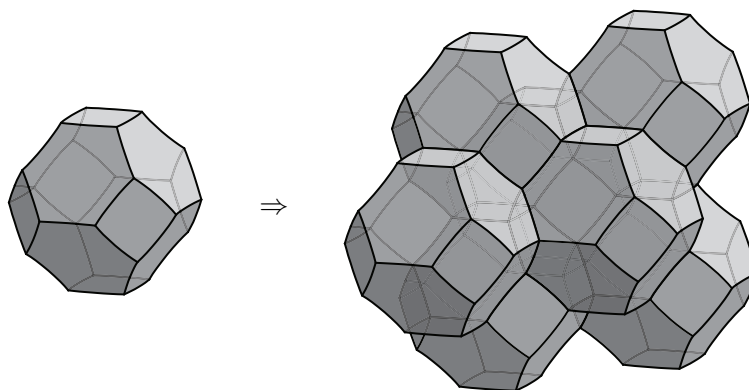
Van Alphen bewees in 1941 het bestaan van onbeperkt kleine Kakeya-naaldenverzamelingen binnen een schijf met straal  $2 + \varepsilon$ . Melvin Bloom en Isaac Schoenberg presenteerden enkelvoudig samenhangende naaldenverzamelingen waarvan de oppervlaktes convergeren naar de constante  $\frac{\pi}{24}(5 - 2\sqrt{2})$ . Schoenberg vermoedde dat

dit de minimale oppervlakte was bij deze criteria, maar Frederick Cunningham kwam met een opnieuw verrassend antwoord: voor elke  $\varepsilon > 0$  bestaat er een enkelvoudig samenhangende Kakeya-naaldenverzameling met oppervlakte kleiner dan  $\varepsilon$ , binnen een eenheidsschijf. Maat nul kan echter niet.

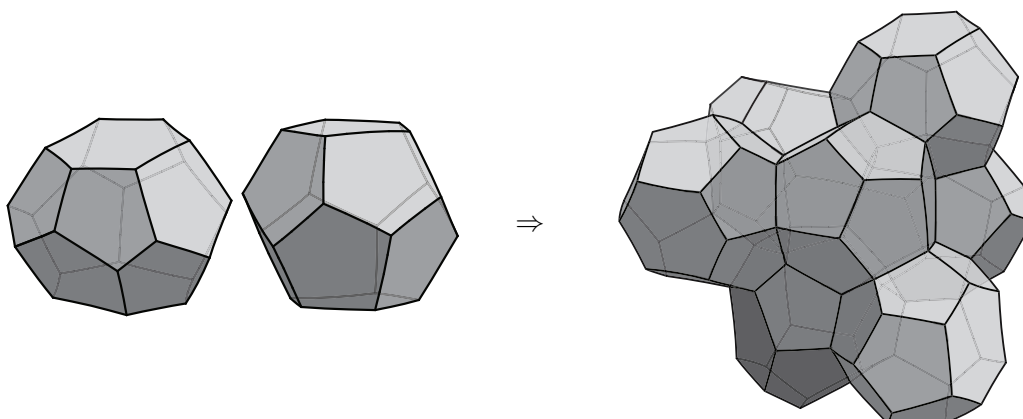


## 172 Weaire-Phelanschuim

De natuurkundige William Thomson, bekender als Lord Kelvin, overpeinsde hoe de ruimte moest worden gepartitioneerd in cellen met hetzelfde volume zodat de oppervlakte ertussen minimaal is, of met andere woorden, wat het meest efficiënte zeepbellenschuim is. In 1887 stelde hij als plausibele oplossing een structuur voor bestaande uit kopieën van eenzelfde basiscel, een afgeknotte octaëder, met zes vierkantige en acht zeshoekige zijvlakken. Om te voldoen aan de wetten van Plateau (zie ??, blz. ??), die schuimstructuren modelleren, zijn de zeshoekige zijvlakken lichtjes gebogen.



Kelvin vermoedde dat zijn structuur optimaal was, wat wijd en zijd aangenomen werd. Meer dan honderd jaar lang werd er geen efficiënter schuim gevonden. Pas in 1993 werd Kelvins vermoeden ontkracht: Denis Weaire en zijn student Robert Phelan vonden via computersimulaties een betere oplossing. Hun structuur is eveneens periodiek maar bestaat uit twee basiscellen: een onregelmatige dodecaëder met twaalf vijfhoekige zijvlakken en een tetradecaëder met twee extra zeshoekige zijvlakken. Ook hun (vijfhoekige) zijvlakken zijn lichtjes gekromd.



De relevante oppervlakte in het Weaire-Phelanschuim is slechts 0,3% kleiner dan in het originele Kelvinschuim. Het is nog niet bewezen dat dit optimaal is, maar experimenteel ordenen zeepbellen onder gunstige randvoorwaarden zich spontaan in een Weaire-Phelanachtig rooster. De strakke, polyhedrale vorm was al langer bekend als chemische kristalstructuur maar toepassing in het vraagstuk van Kepler werd over het hoofd gezien.

De vorm van dit schuim werd gebruikt in het ontwerp voor het Beijing National Aquatics Center in China voor de Olympische Spelen in 2008. Diens architecturale structuur is daardoor inherent sterk en toch licht.

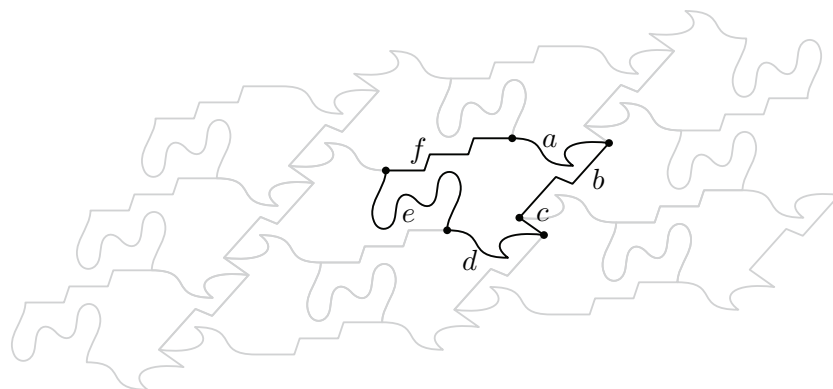
## 173 Criterium van Conway

Het tessellatiecriterium van John Conway biedt een verrassend efficiënte methode om monohedrale Escherachtige betegelingen te construeren, en drukt een voldoende voorwaarde uit om het vlak te kunnen betegelen. Het criterium is eenvoudig maar zeer krachtig.

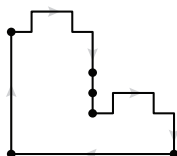
Een vlakke figuur (topologisch een gesloten schijf) voldoet aan Conways criterium als diens rand verdeeld kan worden in zes segmenten  $a$ ,  $b$ ,  $c$ ,  $d$ ,  $e$  en  $f$ , gelabeld met de klok mee, waarop het volgende geldt:

- Het randsegment  $a$  is congruent met  $d$  via een translatie, die de zin omkeert: als de rand in een bepaalde richting doorlopen wordt, moeten  $a$  en  $d$  een verschillende oriëntatie krijgen.
- De vier andere segmenten zijn symmetrisch t.o.v. een puntspiegeling om hun centrum.

De voorwaarden kunnen worden verzwakt door lege segmenten toe te laten. De punten die de rand afbakenen mogen eventueel samenvallen, zolang minstens één segment in elk van de aanliggende koppels  $(b, c)$  en  $(e, f)$  niet ontbreekt. Ook  $a$  en  $d$  mogen ledig zijn, zolang minstens drie van de resterende vier segmenten niet ledig zijn. Elke exotische tegel die voldoet aan deze voorwaarden, is in staat het vlak te betegelen.



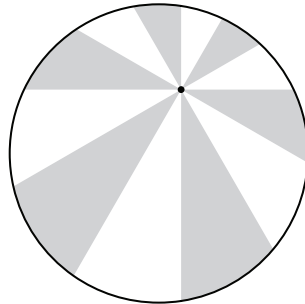
Het is cruciaal dat de oriëntatie van de twee getranslateerde randsegmenten wordt omgekeerd. De tegel hieronder bijvoorbeeld voldoet aan alle andere voorwaarden maar laat geen betegeling van het vlak toe, juist omdat de translatie de oriëntatie in de oploopzin bewaart.



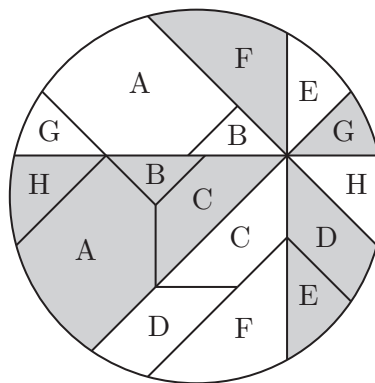
Van de 104 heptomino's (veralgemeende domino's uit zeven identieke vierkanten) die het vlak betegelen, herkent Conways criterium er 101, en van de 343 octomino's worden er slechts 23 over het hoofd gezien. Dit maakt het een uiterst handig hulpmiddel bij polyominocatalogi, daar het aantal  $n$ -omino's exponentieel toeneemt met  $n$ .

## 174 Pizzastelling

Beschouw een schijfvormige pizza en een willekeurig punt erbinnenin. Kies een viervoud  $n \geq 8$ , en verdeel de pizza in  $n$  stukken langs een willekeurige snede doorheen het gekozen punt en rotaties errond over  $\frac{2\pi}{n}$  radialen. Nummer de aldus verkregen pizzapunten met de klok mee. De pizzastelling garandeert dan dat de stukken pizza met even nummer samen even grote oppervlakte hebben als die met oneven nummer.



Michael Goldberg gaf het eerste bewijs, dat rechtstreeks algebraïsche uitdrukkingen voor de oppervlakte van de sectoren manipuleert. Greg Frederickson gaf een familie dissectiebewijzen voor alle toegestane  $n$ , waarin de sectoren in kleinere stukken gesneden worden zodanig dat elke stuk in een evengelabelde sector een congruent stuk in een onevengelabelde sector heeft, zoals voor  $n = 8$  hieronder.

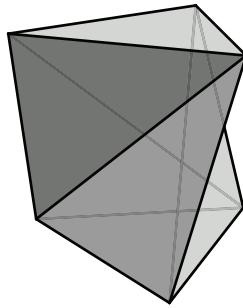


Jeremy, Michael, Jeremy, Andrew en Philip Hirschhorn toonden aan dat een pizza gesneden in  $n$  sectoren met gelijke middelpuntshoeken, met  $n$  een viervoud, ook eerlijk verdeeld kan worden tussen  $\frac{n}{4}$  personen.

## 175 Veelvlak van Schönhardt

Het veelvlak van Schönhardt is het eenvoudigste niet-convexe veelvlak dat niet in tetraëders kan worden getrianguleerd zonder nieuwe hoekpunten toe te voegen. Het veelvlak wordt vernoemd naar Erich Schönhardt, die er een eerste beschrijving van gaf in 1928.

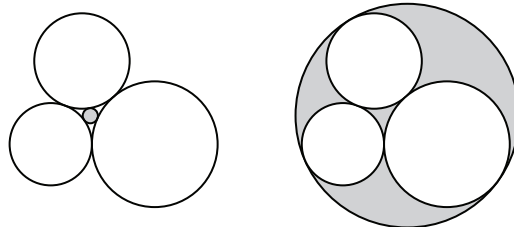
Schönhardts polyhedron wordt geconstrueerd met twee congruente gelijkzijdige driehoeken in parallelle vlakken, zodat de rechte door hun centra loodrecht staat op deze vlakken. De driehoeken moeten wat gedraaid zijn t.o.v. elkaar. Verbind vervolgens hun hoekpunten zoals op de figuur; geen enkele ruimtediagonaal ligt dan nog bevat binnen het veelvlak. Het uiteindelijke resultaat heeft de eigenschap dat geen enkele tetraëder met hoekpunten gemeenschappelijk met het Schönhardtveelvlak volledig binnen dit veelvlak ligt.



Jim Ruppert en Raimund Seidel gebruikten het veelvlak van Schönhardt als basis voor hun bewijs dat bepalen of een niet-convex veelvlak al dan niet getrianguleerd kan worden, NP-compleet is.

## 176 Kussende cirkels

Wat is het maximale aantal cirkels in het vlak die elkaar allemaal onderling raken? Het antwoord op dit probleem (het *kissing circles problem*) is vier: gegeven drie zulke cirkels kan er altijd nog een vierde geconstrueerd worden ertussen of errond, maar daar blijft het bij. Het drietal gegeven cirkels vormt een Steinerketen (zie ??, blz. ??) van de twee nieuwe, die de Soddy-cirkels heten.



Frederick Soddy ontdekte een elegante formule die de stralen van een viertal kussende cirkels verbindt en goot dit in een gedicht in 1936. Na publicatie bleek echter dat René Descartes in een brief naar prinses Elizabeth van Bohemen in 1643 hetzelfde verband afgeleid had. De formule staat daarom bekend als Descartes' cirkelformule.

### The Kiss Precise

(Frederick Soddy, *Nature*, juni 1936)

Four circles to the kissing come.  
The smaller are the benter.  
The bend is just the inverse of  
the distance from the center.  
Though their intrigue left Euclid dumb  
there's now no need for rule of thumb.  
Since zero bend's a dead straight line  
and concave bends have minus sign,  
the sum of the squares of all four bends  
is half the square of their sum.

To spy out spherical affairs  
an oscular surveyor  
might find the task laborious,  
the sphere is much the gayer,  
and now besides the pair of pairs  
a fifth sphere in the kissing shares.  
Yet, signs and zero as before,  
for each to kiss the other four  
the square of the sum of all five bends  
is thrice the sum of their squares.

Noteer  $k_i$  (de *bend* of kromming waarvan sprake in het gedicht) voor de inversen van de stralen van de cirkels, positief als de andere cirkels hem uitwendig raken en negatief anderszijds. De stelling van Descartes geeft dus:

$$2 \cdot (k_1^2 + k_2^2 + k_3^2 + k_4^2) = (k_1 + k_2 + k_3 + k_4)^2$$

Zoals in de tweede strofe van het gedicht te lezen, gaf Soddy ook een driedimensionaal analogon voor sferen. Daar kunnen er maximaal vijf elkaar onderling raken, en wordt de bijhorende formule:

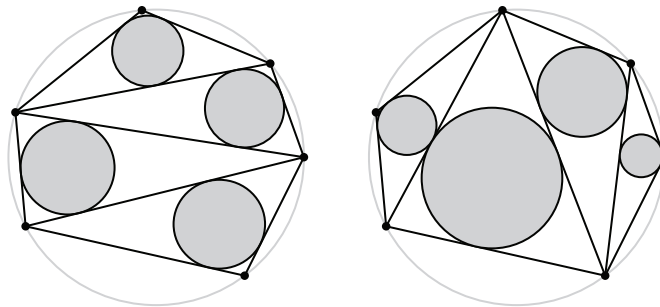
$$3 \cdot (k_1^2 + k_2^2 + k_3^2 + k_4^2 + k_5^2) = (k_1 + k_2 + k_3 + k_4 + k_5)^2$$

Thorold Gosset veralgemeende de formule tot willekeurige  $n$ -dimensionale ruimtes, waar maximaal  $n + 2$  sferen elkaar kunnen raken en hun krommingen aan de volgende betrekking voldoen:

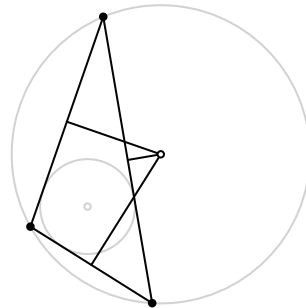
$$n \cdot (k_1^2 + k_2^2 + \dots + k_{n+2}^2) = (k_1 + k_2 + \dots + k_{n+2})^2$$

## 177 Japanse cirkelstelling

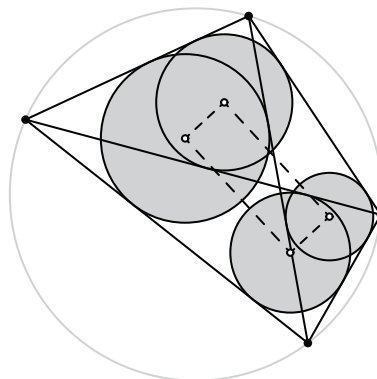
Beschouw een koordenveelhoek (wiens hoekpunten op een cirkel liggen) en een willekeurige triangulatie ervan. De Japanse cirkelstelling, die aan z'n naam komt omdat het resultaat in de vorm van een sangaku gepresenteerd werd, garandeert dan dat de som van de stralen van de ingeschreven cirkels constant is, onafhankelijk van de gekozen triangulatie.



Omgekeerd geldt eveneens dat een veelhoek een koordenveelhoek is als de som van de stralen onafhankelijk is van de triangulatie. Het resultaat volgt eenvoudig uit de stelling van Carnot, naar Lazare Carnot; de som van de afstanden van het middelpunt van de omgeschreven cirkel tot elk van de zijden van een driehoek is gelijk aan de som van de straal van de in- en omgeschreven cirkel. Een afstand wordt negatief beschouwd als hij volledig buiten de driehoek ligt, zoals in dit voorbeeld het geval is.



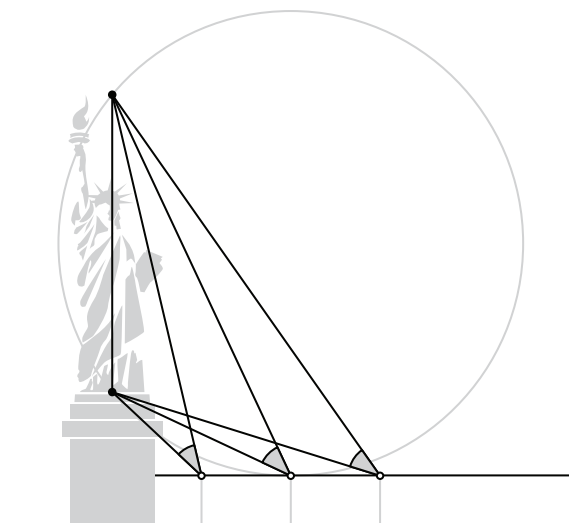
Een andere bewijstechniek maakt gebruik van volgende eigenschap. Verdeel een koordenveelhoek in twee driehoeken volgens een diagonaal en construeer diens ingeschreven cirkels, en herhaal dit met de tweede diagonaal. De middelpunten van deze vier cirkels vormen dan de hoekpunten van een rechthoek.



## 178 Probleem van Regiomontanus

Een standbeeld staat op een sokkel, zo hoog dat diens bovenkant nog boven ooghoogte uittorent, of een schilderij hangt aan de muur zodat de onderkant van de lijst zich nog boven ooghoogte bevindt. Proefondervindelijk is het duidelijk dat als je je vlakbij of te ver van het standbeeld of schilderij bevindt, het te klein zal lijken. Johannes Müller (ook bekend als Regiomontanus) vroeg zich af op welke afstand een waarnemer zich moet bevinden om het kunstwerk optimaal te bewonderen, d.i. onder een maximale hoek.

Uiteraard biedt analyse een mogelijkheid, maar er bestaat ook een zuiver meetkundige interpretatie om dit onder-tussen beroemde optimalisatieprobleem op te lossen. Construeer de unieke cirkel door de uiterste punten van het schilderij of standbeeld, die tevens raakt aan de rechte op ooghoogte:



Aangezien omtrekshoeken op dezelfde boog even groot zijn, lijkt het kunstwerk even groot vanuit punten op de cirkel; erbuiten wordt de waarnemingshoek kleiner. De enige manier om de hoek nog groter te maken, is kijken vanuit een punt *binnen* de cirkel, wat onmogelijk is voor een waarnemer op de grond. De optimale positie is dus precies het punt waar de cirkel raakt aan de rechte op ooghoogte.

Via calculus kan het als volgt. Definieer de volgende parameters:

- $a$ : de (verticale) hoogte van het onderste punt van het standbeeld boven ooghoogte
- $b$ : de (verticale) hoogte van het bovenste punt van het standbeeld boven ooghoogte
- $x$ : de (horizontale) afstand van de waarnemer tot het standbeeld
- $\alpha$ : de hellingshoek van het onderste punt van het standbeeld, gezien vanuit de positie van de waarnemer
- $\beta$ : de hellingshoek van het bovenste punt van het standbeeld, gezien vanuit de positie van de waarnemer

Het probleem van Regiomontanus vraagt de maximale waarde van  $\beta - \alpha$ . Daartoe is het voldoende  $\tan(\beta - \alpha)$  te maximaliseren, wat na uitwerking geeft:

$$\tan(\beta - \alpha) = \frac{\tan \beta - \tan \alpha}{1 + \tan \alpha \cdot \tan \beta} = \frac{\frac{b}{x} - \frac{a}{x}}{1 + \frac{b}{x} \cdot \frac{a}{x}} = (b - a) \frac{x}{x^2 + ab}$$

Deze uitdrukking afleiden en gelijk aan nul stellen geeft inderdaad een maximum, meer bepaald op  $x = \sqrt{ab}$ , het meetkundig gemiddelde (zie 45, blz. 34) van  $a$  en  $b$ .

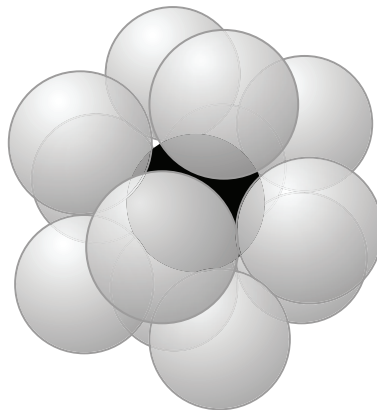
## 179 Kusgetallen

Het volgende probleem is afkomstig van Isaac Newton.

HOEVEEL TWEEDIMENSIONALE EENHEIDSSFEREN PASSEN ER MAXIMAAL ROND EEN CENTRALE SFEER,  
ZODANIG DAT DEZE ELKAAR NIET OVERLAPPEN EN ZE ALLEN RAKEN AAN DE CENTRALE SFEER?

Hoewel het probleem in één en twee dimensies zeer eenvoudig is en ook het driedimensionale geval met fysieke bollen eenvoudig te conceptualiseren valt, leidde het vraagstuk tot een verhitte discussie tussen Isaac Newton en David Gregory. Noteer het maximale aantal sferen waarvan sprake in  $n$  dimensies (het  $n^{\text{de}}$  kusgetal) als  $\kappa_n$ . Wanneer de bollen op een lijn geplaatst worden, is  $\kappa_1$  duidelijk gelijk aan 2. Voor het vlak geldt  $\kappa_2 = 6$ .

In drie dimensies is het gemakkelijk om 12 bollen rond een centrale bol te positioneren, door hun middelpunten op de hoekpunten van een icosaeëder te plaatsen. In die symmetrische configuratie blijft echter vrij veel ruimte onbenut, voldoende zelfs om twee willekeurige bollen van plaats te verwisselen zonder dat ergens het contact met de centrale bol verbroken hoeft te worden. Gregory beweerde daarom dat er een extra bol bij paste, terwijl Newton van het tegendeel overtuigd was. Geen van beide kon echter een demonstratie of bewijs geven.



Newton bleek het bij het rechte eind te hebben, maar een bewijs dat  $\kappa_3 = 12$  werd pas in 1953 gegeven door Kurt Schütte en Bartel van der Waerden. Drie jaar later gaf John Leech ook een eenvoudiger bewijs.

In hogere dimensies hebben 2-sferen meer vrijheid en passen er meer rond een gegeven sfeer. Philippe Delsarte vond in 1972 dat  $24 \leq \kappa_4 \leq 25$ . Alhoewel ook hier de meest symmetrische verdeling met 24 bollen veel ruimte openlaat (meer zelfs dan in drie dimensies), bewees Oleg Musin in 2003 dat  $\kappa_4 = 24$ . De volgende kusgetallen zijn nog onbekend, op twee uitzonderingen na: dankzij enkele uitermate symmetrische roosters (het  $E_8$ - resp. Leechrooster) kon men ook besluiten dat  $\kappa_8 = 240$  en  $\kappa_{24} = 196560$ . Zoals John Conway, die de symmetrieën van het Leechrooster in detail analyseerde en er enkele nieuwe sporadische groepen (zie ??, blz. ??) in ontdekte, de situatie in 24 dimensies treffend verwoordde:

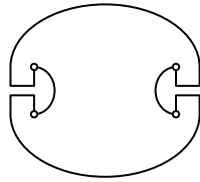
*There's a lot of room up there.*

## 180 Penroses onverlichte kamer

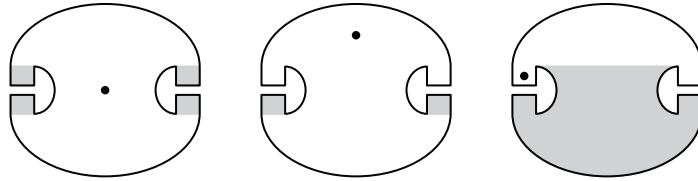
Begin de jaren 50 vroeg Ernst Straus of een kamer met bespiegelde wanden steeds volledig verlicht kan worden met een enkele puntvormige lichtbron, waarbij lichtstralen willekeurig vaak terugkaatsen via de wanden.

Roger Penrose zag in de eigenschappen van de ellips een methode om een kamer met gebogen wanden te construeren waarin geen enkele lichtbron de volledige kamer zou kunnen verlichten. De kamer van Penrose (1958) bestaat uit twee halve ellipsen en twee paddenstoelvormige uitstulpingen, die op hun beurt opgebouwd zijn uit lijnsegmenten en twee kleinere halve ellipsen, tussen de brandpunten van de grote halve ellipsen.

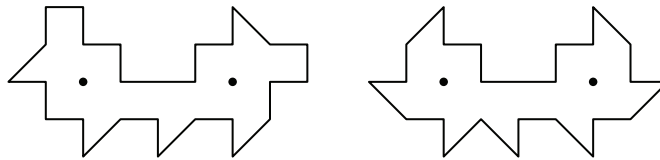




Ongeacht de positie van een lichtbron, zullen er steeds bepaalde ruimtes pikdonker blijven:

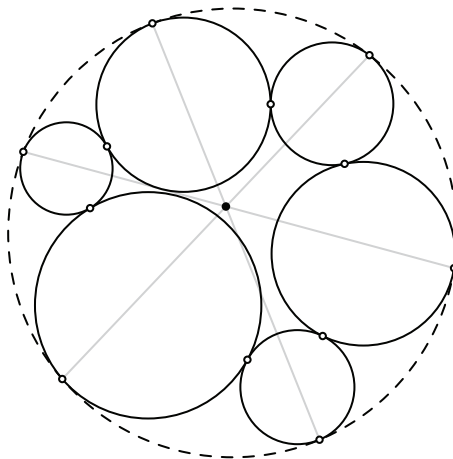


Bij kamers met vlakke wanden ligt het wat lastiger. George Tokarsky toonde aan dat er ook polygonale kamers bestaan in twee en drie dimensies, die vanuit een bepaald punt niet elk ander punt verlichten, zoals zijn voorbeeld met 26 vlakken hieronder links aantoont; stralen vanuit een lichtbron geplaatst in één van de aangeduide punten bereiken het andere punt nooit. Dit grensgeval werkt dus enkel vanuit bepaalde punten en laat slechts singuliere punten onverlicht. Het staat nog open of er kamers te vinden zijn zonder deze beperkingen. Castro kon wel een eenvoudiger voorbeeld met 24 wanden geven, hieronder rechts.



## 181 Stelling van de zeven cirkels

Beschouw een ketting van zes cirkels die allen raken aan een zevende cirkel en aan twee van hun buren. Verbind de raakpunten tussen overstaande raakpunten in deze ketting met de centrale cirkel. Deze drie lijnen snijden dan steeds in één punt.



Er zijn vele variaties mogelijk, bijvoorbeeld met zes cirkels die uitwendig raken aan de centrale, of combinaties. Deze op zich elementaire stelling werd pas in 1974 ontdekt door C. Evelyn, G. Money-Coutts en John Tyrrell.

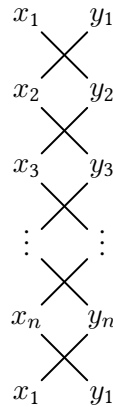
## 182 Schoenveterformule

De schoenveterformule biedt een gewiekste methode om snel de oppervlakte van een veelhoek te berekenen als de coördinaten van diens hoekpunten bekend zijn. De formule kan worden afgeleid uit de stelling van Green

(zie ??, blz. ??). Noteer de coördinaten van de hoekpunten  $(x_1, y_1)$ ,  $(x_2, y_2)$ , tot en met  $(x_n, y_n)$ , in wijzerzin doorlopen; de schoenveterformule geeft dan de oppervlakte  $A$  van de veelhoek in functie van deze coördinaten:

$$A = \frac{1}{2} \left| \sum_{i=1}^n x_i y_{i+1} - \sum_{i=1}^n x_{i+1} y_i \right| = \frac{1}{2} \left| \sum_{i=1}^n \det \begin{bmatrix} x_i & x_{i+1} \\ y_i & y_{i+1} \end{bmatrix} \right|$$

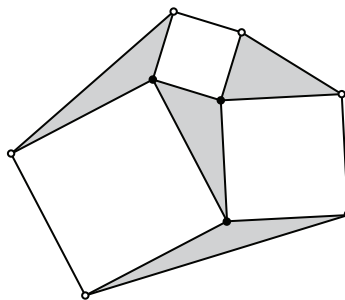
In deze formule worden  $x_{n+1} = x_1$  en  $y_{n+1} = y_1$  gesteld. De volgende visuele representatie verduidelijkt de benaming. Noteer de paren coördinaten onder elkaar, sluit af met het initiële punt, en voeg diagonalen toe:



Vermenigvuldig elk paar getallen verbonden door een dalende diagonaal en tel deze allemaal op, en doe hetzelfde voor de stijgende diagonalen. De helft van het absolute verschil tussen deze sommen geeft dan de oppervlakte.

### 183 Stelling van Cross

David Cross vond als 14-jarige schooljongen dit resultaat terug, dat aldus in het Verenigd Koninkrijk bekendstaat als de stelling van Cross. Construeer drie vierkanten op de zijden van een willekeurige driehoek en verbind diens hoekpunten als op de figuur. De vier gearceerde driehoeken hebben dan allen gelijke oppervlakte.



### 184 Stelling van de Britse vlag

Kies een willekeurig punt  $P$  binnen een rechthoek  $ABCD$ . De stelling van de Britse vlag stelt dan dat de som van de kwadraten van de afstanden van  $P$  tot twee overstaande hoeken van de rechthoek gelijk is aan diezelfde som tot de overige twee. In een vergelijking:

$$|AP|^2 + |CP|^2 = |BP|^2 + |DP|^2$$

De stelling blijft geldig als  $P$  buiten de rechthoek gekozen wordt, of zelfs willekeurig in een Euclidische ruimte waarin de rechthoek ingebed zit. Er is ook een veralgemening tot parallellogrammen: de twee sommen zijn dan over het algemeen niet gelijk, maar het verschil ertussen hangt uitsluitend af van de vorm van het parallellogram en niet van de keuze van  $P$ .

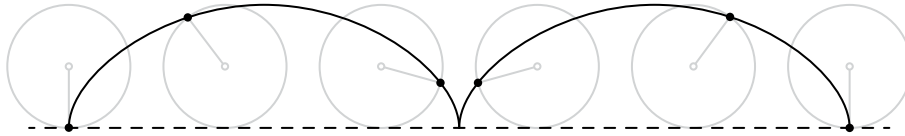
De stelling ontleent zijn naam aan het feit dat de configuratie, samen met de loodrechten vanuit  $P$  op de zijden (handig ter bewijs), enigszijns doet denken aan de vlag van het Verenigd Koninkrijk.



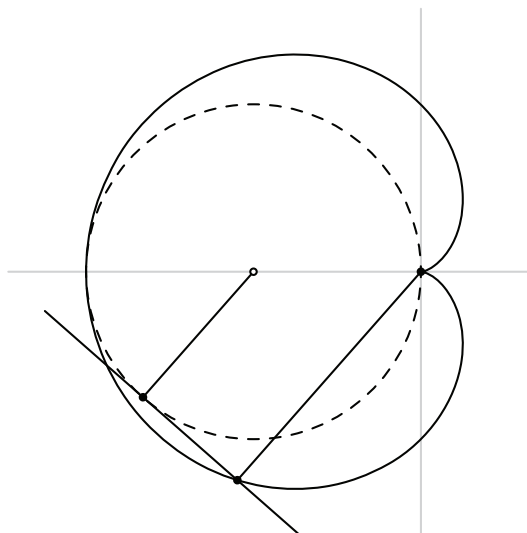
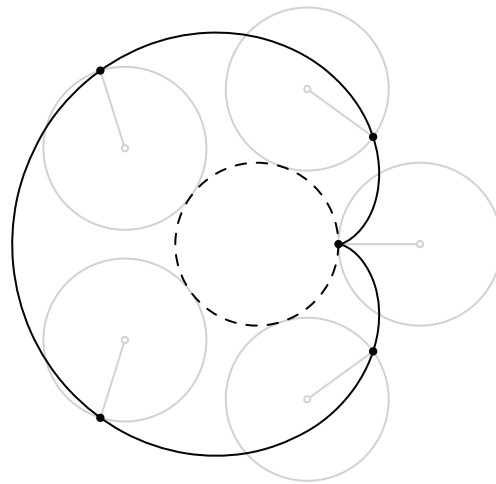


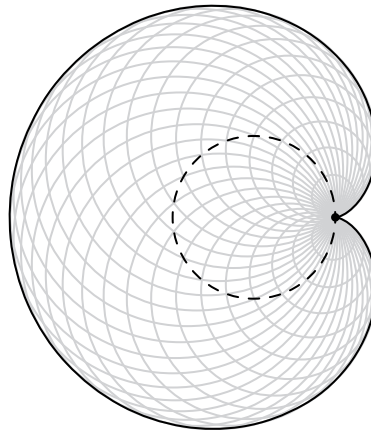
# VI Bijzondere krommen

## 185 Cycloïde

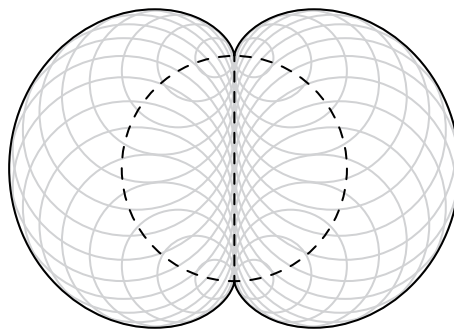


## 186 Cardioïde



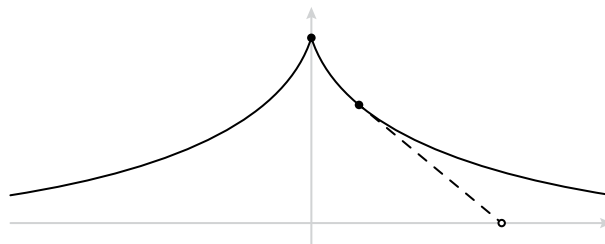


**187 Nefroïde**



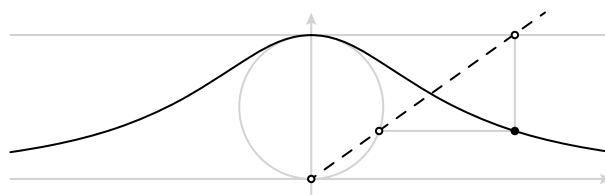
**188 Deltoïde**

**189 Tractrix**



**190 Astroïde**

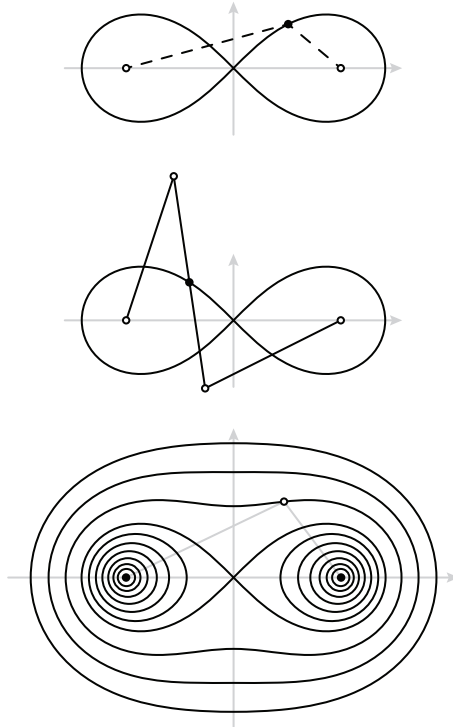
**191 Heks van Agnesi**



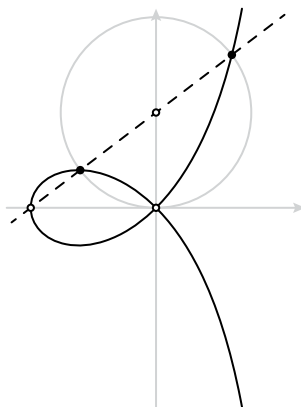
192 **Hypocycloïde**

193 **Epicycloïde**

194 **Lemniscaat van Bernoulli**

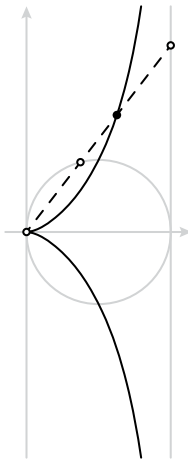


195 **Strofoïde**

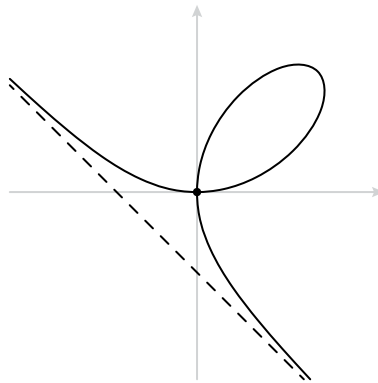




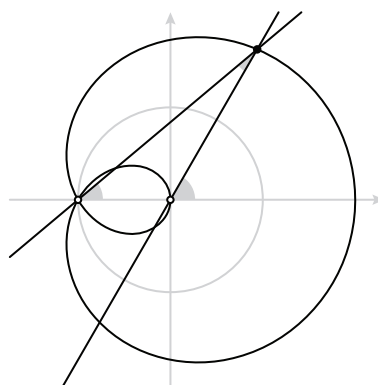
**196 Cissoïde van Diocles**

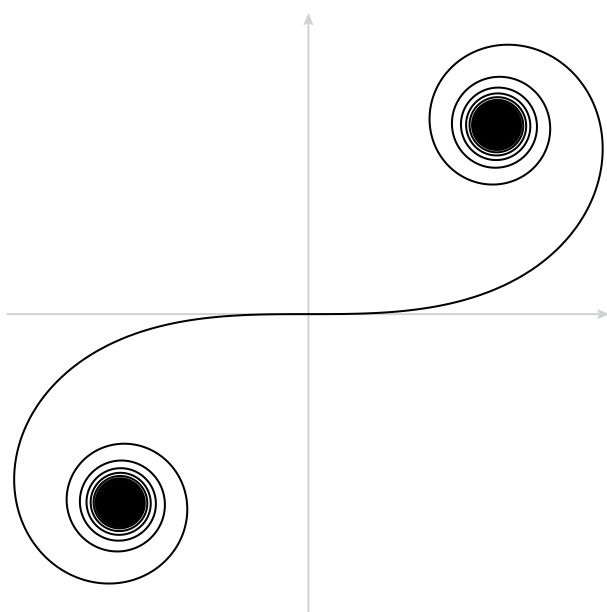


**197 Folium van Descartes**



**198 Slakkenlijn van Pascal**



**199 Eulerspiraal**





Een fractal is een meetkundige figuur die *zelfgelijkend* is, d.w.z. opgebouwd uit delen die (min of meer) gelijkvormig zijn met de figuur zelf. Daardoor bevatten ze een oneindige hoeveelheid details en steeds terugkerende patronen. De belangrijkste genereermethoden voor fractals zijn IFS (*Iterated Function Systems*) en Lindenmayersystemen. De meest visuele techniek is basis-en-motief, wat gemakkelijk om te zetten is naar een L-systeem.

## 200 L-systemen en Turtle Graphics

Lindenmayersystemen of L-systemen werden ontwikkeld door theoretisch bioloog en botanicus Aristid Lindenmayer in 1968, als formele fundering voor een axiomatische benadering van biologische evolutie.

Een Lindenmayersysteem  $L$  wordt formeel gedefinieerd als een tupel  $L = \{V, \omega, P\}$ .

- $V$  (het alfabet): de verzameling variabelen en constanten.
- $\omega$  (het axioma): de tekenreeks bestaande uit symbolen uit  $V$ , die de begintoestand van  $L$  definieert.
- $P$  (de producties): de verzameling regels die vastleggen hoe een variabele moeten worden vervangen door een tekenreeks uit  $V$ . Voor een symbool  $A$  dat wel in  $V$  zit maar geen productieregel ondergaat, wordt  $A \rightarrow A$  verondersteld; zo'n symbool heet een constante.

Het concept is zeer krachtig, vooral in combinatie met de zogenaamde Turtle Graphics. Die vertalen elk symbool in een tekenreeks naar een bepaalde grafische handeling, en visualiseren aldus het groeiproces in een L-systeem.

### Lindenmeyers algen

Met zijn originele L-systeem beschreef Lindenmayer de groei van algen.  $B$  stelt een cel in groeifase voor, die zal groeien tot de reproductietoestand  $A$ . Een cel  $A$  zal splitsen in twee cellen, één groeistoestand en één reproductietoestand.

- $V: A, B$
- $\omega: A$
- $P: (A \rightarrow AB), (B \rightarrow A)$

De productieregels herhaaldelijk toepassen levert op:

$$A \rightarrow AB \rightarrow ABA \rightarrow ABAAB \rightarrow ABAABABA \rightarrow ABAABABAABAAB \rightarrow \dots$$

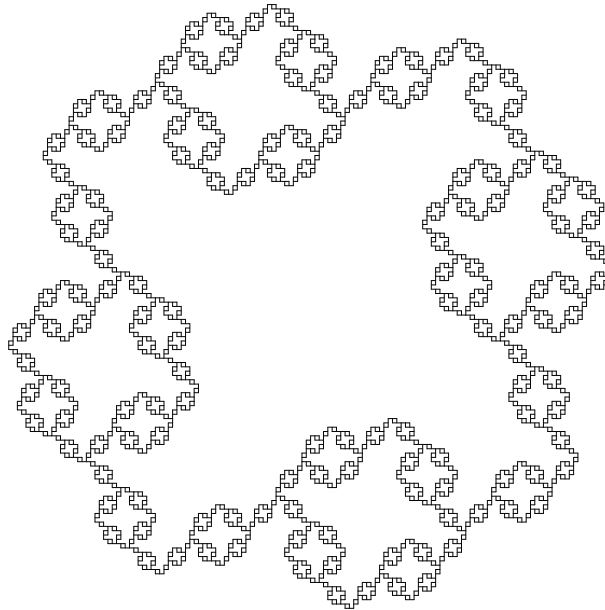
De som van het aantal variabelen in elke generatie is steeds een Fibonaccigetel. Als we de  $n^{\text{de}}$  generatie noteren als  $L_n$ , dan kan  $L_n$  als een aaneenschakeling  $L_{n-1} \cdot L_{n-2}$  van de vorige twee generaties worden geschreven.

### Fractals

Lindenmayersystemen in combinatie met Turtle Graphics kunnen gemakkelijk fractale vormen genereren.

- $V: F, +, -$
- $\omega: F + F + F + F$
- $P: (F \rightarrow FF - F - F - F - F - F + F)$
- Turtle Graphics:

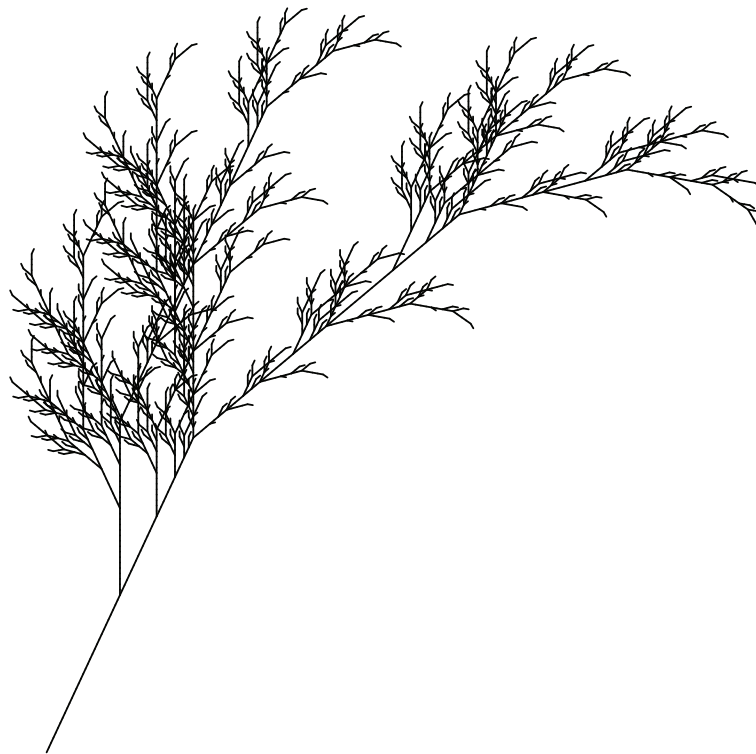
- $F$ : teken een eenheid vooruit
- $+$ : draai  $90^\circ$  naar links
- $-$ : draai  $90^\circ$  naar rechts



## Planten

Lindenmeyersystemen kennen een belangrijke toepassing in de game-industrie, omdat ze eenvoudige, snel laadbare en toch gedetailleerde en realistische figuren als planten en bomen kunnen genereren.

- $V$ :  $X, F, +, -, [, ]$
- $\omega$ :  $X$
- $P$ :  $(X \rightarrow F - [[X] + X] + F[+FX] - X), (F \rightarrow FF)$
- Turtle Graphics:
  - $F$ : teken een eenheid vooruit
  - $+$ : draai  $25^\circ$  naar rechts
  - $-$ : draai  $25^\circ$  naar links
  - $[$ : sla huidige positie en hoek op (push)
  - $]$ : keer terug naar de laatst opgeslagen positie en hoek (pop)



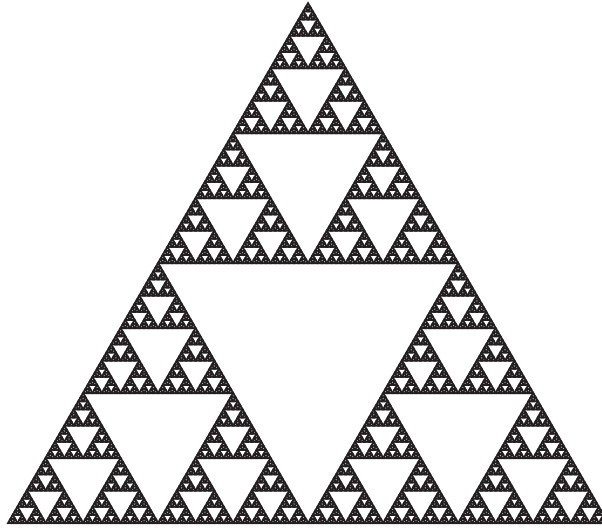
Er zijn nog veel meer L-systemen te bedenken voor zowel andere fractals als voor bijv. of vlakvullende krommen of Penrosebetegelingen (zie 138, blz. 104). Op [http://www-user.uni-bremen.de/~schmuhl/fractals/fractal\\_curves.html](http://www-user.uni-bremen.de/~schmuhl/fractals/fractal_curves.html) staan nog meer voorbeelden.

Uiteraard zijn er vele uitbreidingen en variaties op de Lindenmeyersystemen. Zo heb je versies die bepaalde kansen meegeven in de productieregels (stochastische systemen), andere versies geven parameters mee (parametrische systemen) en nog andere gebruiken contextsensitieve productieregels, waarbij de productie van een variabele afhangt van de variabelen errond.

## 201 Driehoek van Sierpiński

Deze klassieke fractal werd in 1915 besproken door Pools wiskundige Waclaw Sierpiński. De patronen komen echter al voor in 13<sup>de</sup>-eeuwse Italiaanse kunst.

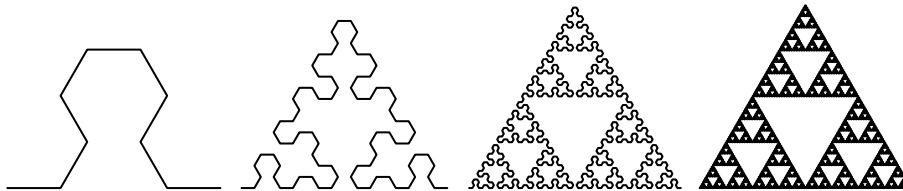
De meest eenvoudige constructie vertrekt vanuit een gelijkzijdige driehoek, verdeelt deze in vier kleinere gelijkzijdige driehoeken, verwijdert de middenste driehoek en herhaalt het proces op de resterende driehoeken. Het limietgeval van dit proces heet de driehoek of de zeef van Sierpiński. Na elke stap verkleint het oppervlak van de figuur met een factor  $\frac{3}{4}$ , zodat het oppervlak van de uiteindelijke figuur naar 0 nadert.



Een Lindenmeyersysteem:

- $V: A, B, +, -$
- $\omega: A$
- $P: (A \rightarrow B - A - B), (B \rightarrow A + B + A)$
- Turtle Graphics:
  - $A$  en  $B$ : teken een eenheid vooruit
  - $+$ : draai  $60^\circ$  naar links
  - $-$ : draai  $60^\circ$  naar rechts

Het teken van de hoek moet na elke iteratie gewisseld worden voor een driehoek waarvan de basis steeds aan dezelfde kant ligt. Het resultaat wordt hier getekend na 2, 4, 6 en 8 iteraties:

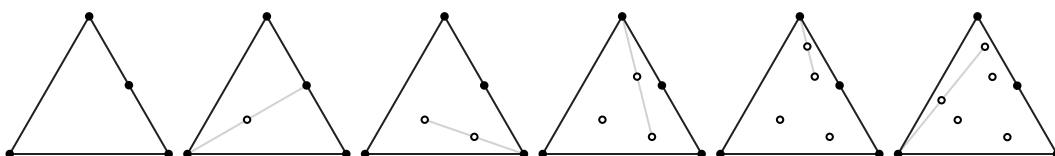


Een ander L-systeem voor de driehoek van Sierpiński is deze. Hierbij worden dezelfde Turtle Graphics gebruikt als bij de eerste versie, maar met een hoek van  $120^\circ$ .

- $V: A, B, +, -$
- $\omega: A - B - B$
- $P: (A \rightarrow A - B + A + B - A), (B \rightarrow BB)$

Nog een prachtige genereermethode is via een zogenaamde chaos game, zo genoemd door Michael Barnsley. Hij gaf nog een voorbeeld van deze techniek voor zijn beroemde varen (zie 213, blz. 169).

- Teken de hoekpunten van de omhullende gelijkzijdige driehoek en kies één ervan als beginpunt  $P_0$ .
- Bepaal een nieuwe punt  $P_{n+1}$  door willekeurig één van de oorspronkelijke hoekpunten te kiezen, en het middelpunt tussen dit hoekpunt en  $P_n$  te nemen.
- Herhaal stap 2 *ad infinitum*.



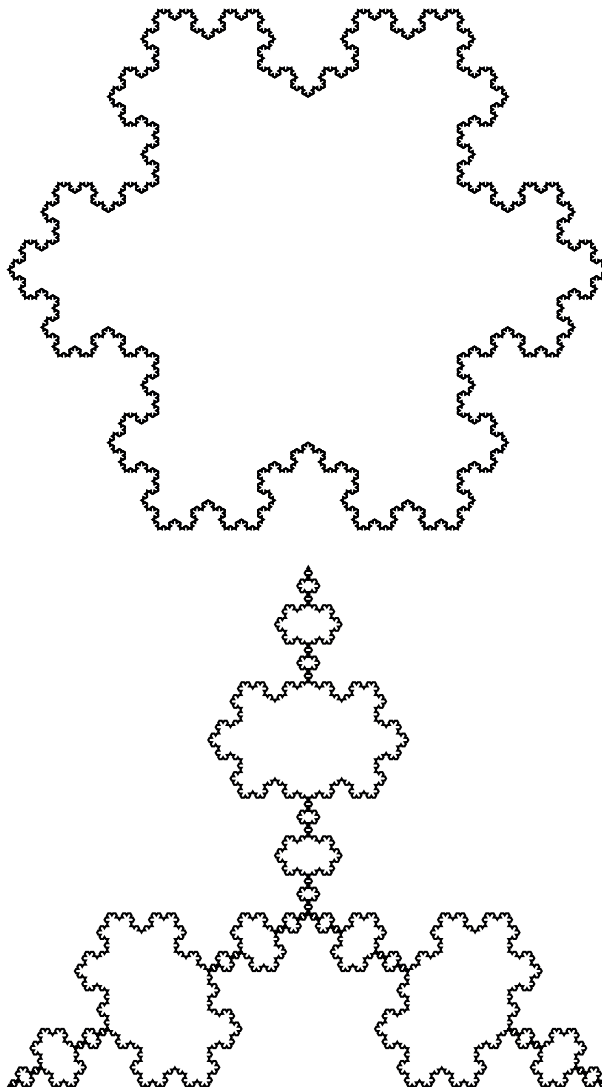


Bij meerdere elementaire cellulaire automaten (zie 283, blz. 246) ontstaat er een Sierpińskidriehoek tijdens hun evolutie. Zelfs in de Game of Life (zie 285, blz. 255) kan de driehoek geprogrammeerd worden!

Kleur  $2^n$  rijen uit de driehoek van Pascal in, zwart bij oneven en wit bij even (ofwel modulo 2); het resultaat is een benadering van Sierpiński's driehoek. Het limietgeval  $n \rightarrow \infty$  geeft de exacte fractal.

## 202 Sneeuwvlok van Koch

- $V: F, +, -$
- $\omega: F ++F ++F$
- $P: (F \rightarrow F - F ++F - F)$
- Turtle Graphics:
  - $F$ : teken een eenheid vooruit
  - $+$ : draai  $120^\circ$  naar links
  - $-$ : draai  $120^\circ$  naar rechts

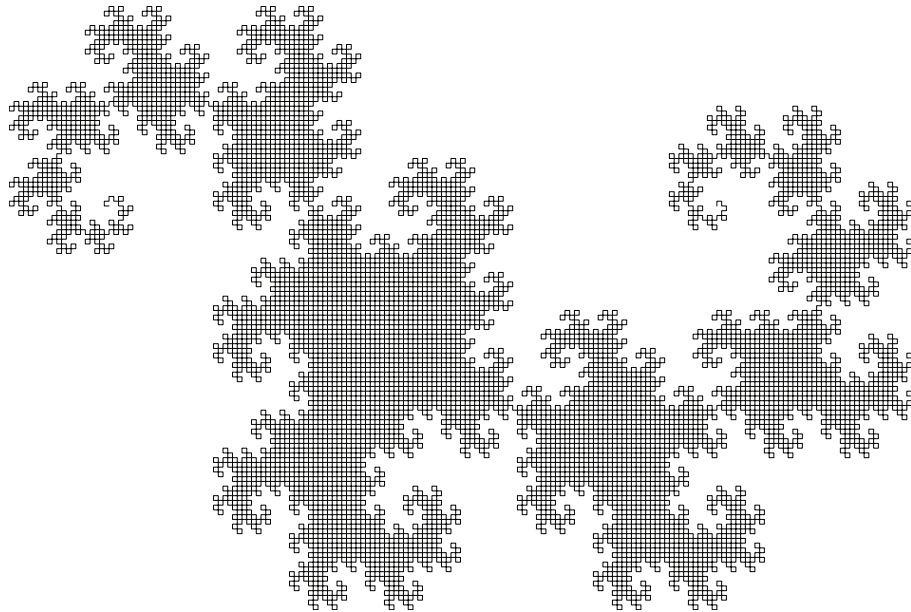


## 203 Drakenkromme

- $V: X, Y, F, +, -$
- $\omega: FX$

- $P: (X \rightarrow X + YF), (Y \rightarrow FX - Y)$
- Turtle Graphics:
  - $F$ : teken een eenheid vooruit
  - $+$ : draai  $90^\circ$  naar rechts
  - $-$ : draai  $90^\circ$  naar links

Merk op dat in deze Turtle Graphics  $X$  en  $Y$  geen grafische betekenis hebben, ze dienen enkel ter controle over de evolutie van de kromme. De drakenkromme levert dit spectaculaire resultaat op na 14 iteraties:



## 204 Mandelbrotverzameling

De Mandelbrotverzameling is een verzameling punten in het complexe vlak waarvan de rand een karakteristieke fractale vorm heeft. Ze vindt haar oorsprong in de studie van complexe dynamische systemen, een veld dat begin 20<sup>ste</sup> eeuw verkend werd door de Franse wiskundigen Pierre Fatou en Gaston Julia. De fractal wordt vernoemd naar Benoit Mandelbrot, die de verzameling onderzocht en populariseerde.

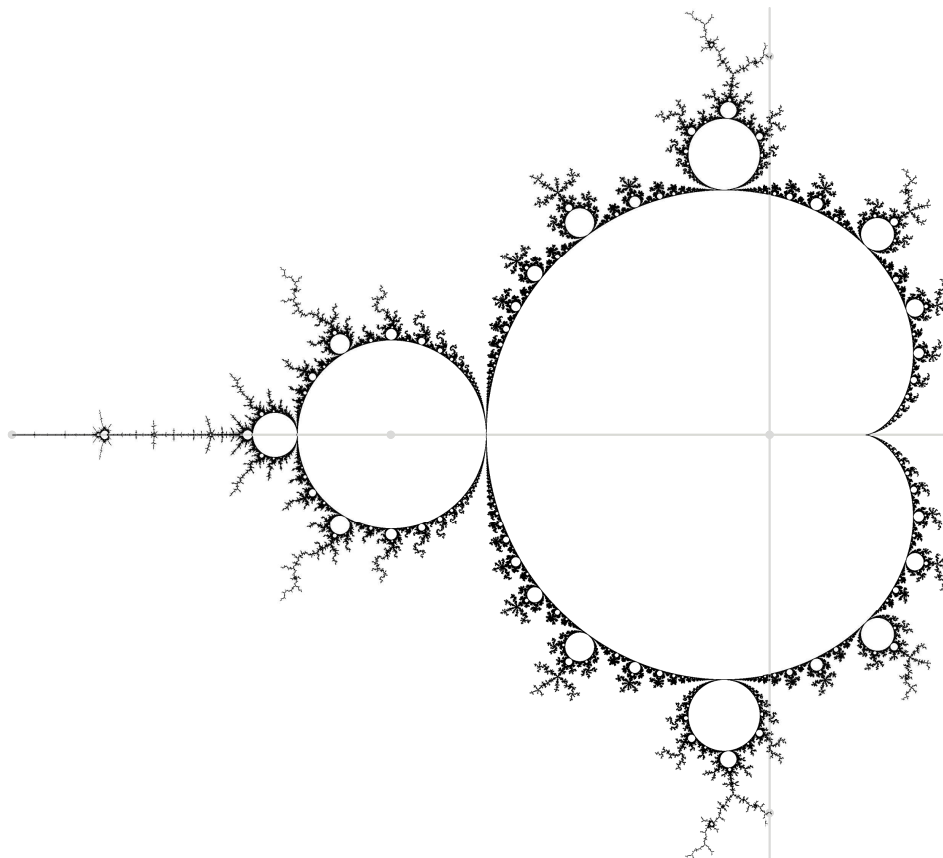
Beschouw het dynamisch systeem  $P_c : \mathbb{C} \rightarrow \mathbb{C} : z \mapsto z^2 + c$ , waarin  $c$  een complexe parameter is. Itereer nu deze functie startende vanuit het kritische punt nul, m.a.w. bereken de baan van nul:

$$0 \rightarrow P_c(0) \rightarrow P_c(P_c(0)) \rightarrow P_c(P_c(P_c(0))) \rightarrow \dots \rightarrow P_c^n(0) \rightarrow \dots$$

Er zijn drie mogelijkheden voor een dergelijke rij: divergentie naar oneindig, attractie naar een periodieke cykel, of convergentie. De Mandelbrotverzameling wordt dan gedefinieerd als de verzameling van juist die complexe parameters  $c$  waarvoor de baan van nul begrensd blijft en dus niet divergeert naar oneindig.

De imaginaire eenheid  $i$  als waarde voor  $c$  doet nul al gauw in een 2-cykel belanden:  $0, i, i - 1, -i, i - 1, -i \dots$ . Deze rij is duidelijk begrensd, zodat bijvoorbeeld  $i$  in de Mandelbrotverzameling wordt opgenomen. Het getal 1 daarentegen doet de baan divergeren ( $0, 1, 2, 5, 26 \dots$ ), zodat 1 niet in deze verzameling zit.

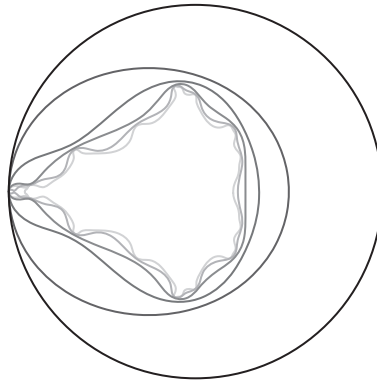
Ondanks deze eenvoudige constructie blijkt de Mandelbrotverzameling een zeer complexe structuur te vormen! In feite konden de eerste afbeeldingen van deze fractal pas worden getekend in 1978 via computerberekeningen, door Robert Brooks en Peter Matelski. Gedetailleerdere illustraties werden sindsdien alsmaar populairder in de folklore, ook buiten de wiskunde.



Op deze figuur is duidelijk te zien dat het centrale gebied van de Mandelbrotfractal de vorm van een cardioïde heeft (zie 186, blz. 151)). Deze cardioïde bevat de parameters  $c$  waarvoor  $P_c$  een aantrekkend fixpunt bezit, oftewel de  $c$ 's van de vorm  $\frac{\mu}{2} \cdot (1 - \frac{\mu}{2})$  voor welbepaalde  $\mu$  in de open eenheidsschijf. Direct links van deze centrale cardioïde bevindt zich een perfecte cirkel, met centrum  $-1$  en straal  $\frac{1}{4}$ , die de  $c$ -waarden bevat waarvoor  $P_c$  een aantrekkende 2-cykel bezit. Errond vertakken zich nog oneindig veel kleinere, bijna-cirkelvormige lobjes. De doorsnede van de Mandelbrotverzameling met de  $x$ -as is precies het interval  $[-2, \frac{1}{4}]$ .

Mandelbrot vermoedde uit de eerste, ruwe figuren dat zijn verzameling niet samenhangend was, maar op fijnere figuren was te zien dat verschillende delen wel degelijk verbonden waren door dunne filamenten. Zoals Adrien Douady en John Hubbard expliciet aantoonde is de gehele Mandelbrotfractal inderdaad samenhangend.

Op basis van hoe snel de banen convergeren, kunnen vertrouwde gekleurde illustraties van de fractal gemaakt worden. Een andere manier om met kleuren te werken maakt gebruik van zogenaamde Mandelbrotlemniscaten: krommen waarvan de punten aan dezelfde snelheid een vooropgestelde  $r_{\max}$  bereiken. Gewoonlijk wordt een natuurlijk getal  $n$  gedefinieerd die de grootste  $n$  is zodat  $P_c^n(0) < r_{\max}$ , waarbij deze maximale  $r$  vaak als 2 gekozen wordt. Punten met dezelfde  $n$ -waarde worden dan in hetzelfde kleur gekleurd, en de scheidingslijnen tussen deze gebieden vormen dan een serie Mandelbrotlemniscaten met de fractal als limiet. De eerste worden hieronder weergegeven.

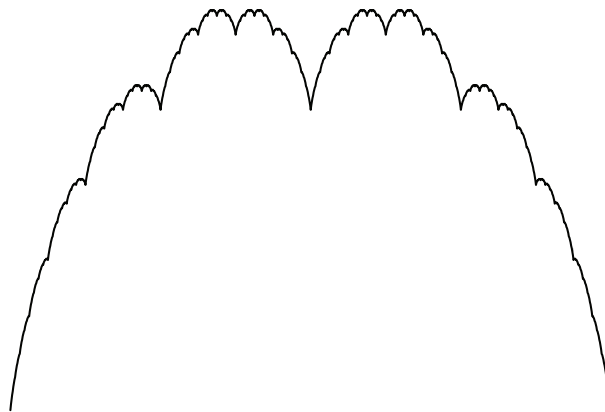


Allerlei regio's in de fractal hebben een eigen naam gekregen, zoals bijvoorbeeld de “zeepaardjesvallei” tussen de centrale cardioïde en de cirkel links ervan.

## 205 **Juliaverzameling**

### 206 **Blanc-mangerkromme**

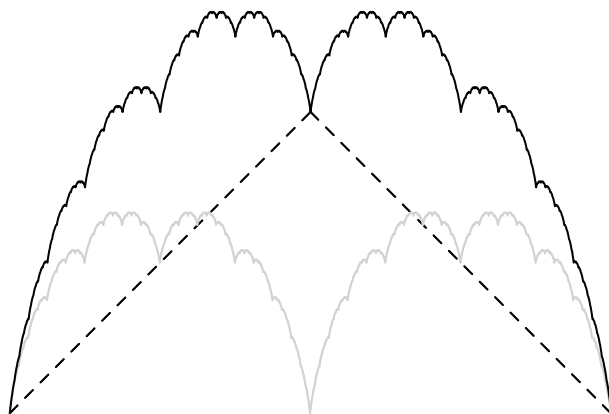
De blanc-mangerkromme werd in 1903 beschreven door Teiji Takagi en staat ook bekend als de Takagikromme, maar wordt meestal vernoemd naar een gelijkende pudding. Een veralgemening ervan is de kromme van Takagi-Landsberg.



Meetkundig kan de kromme worden geconstrueerd uit zigzaglijnen zoals hieronder. Neem een oneindige serie zigzaglijnen, waarbij elke kromme steeds half zo hoog is als de vorige, en tel ze allemaal op; het resultaat is de blanc-mangerkromme. De eerste vier stadia:



Een mooie eigenschap van de fractale blanc-mangerkromme: teken twee krommen naast elkaar, construeer een overspannende zigzag en tel deze drie krommen samen: het resultaat is een enkele, grotere blanc-manger.



Algebraïsch kan de kromme ook als een functie op het eenheidsinterval  $[0, 1]$  gedefinieerd worden. Deze pathologische functie is overall continu, maar nergens afleidbaar, zoals het monster van Weierstrass (zie 116, blz. 87). Merk op dat in het functievoorschrift  $\min_{n \in \mathbb{Z}} |\alpha - n|$  de afstand voorstelt van  $\alpha$  tot het dichtstbijzijnde gehele getal.

$$B(x) = \sum_{k=0}^{\infty} \frac{\min_{n \in \mathbb{Z}} |2^k x - n|}{2^k}$$

Het oppervlak onder de kromme wordt eenvoudig berekend als een meetkundige reeks met limiet  $\frac{1}{2}$ .

## 207 Cantorstof

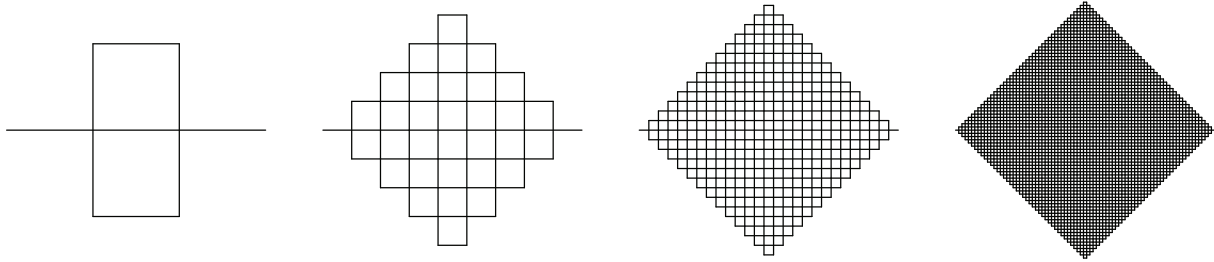
- $V: A, B$
- $\omega: A$
- $P: (A \rightarrow ABA), (B \rightarrow BBB)$
- Turtle Graphics:
  - $A$ : teken een eenheid vooruit
  - $B$ : ga een eenheid vooruit



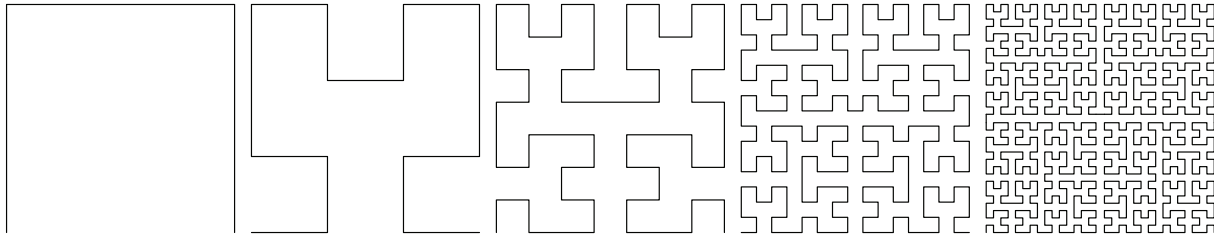
Cantor set =  $D(n) \bmod 3$ : <http://mathworld.wolfram.com/CantorSet.html>

## 208 Vlakvullende krommen

Intuïtief kan een continue kromme worden gezien als het pad van een continu bewegend punt. Een strengere definitie in de analytische meetkunde noemt een kromme een continue afbeelding van een ééndimensionale ruimte naar een  $n$ -dimensionale ruimte ( $n \geq 2$ ). Het lijkt aannemelijk dat een vlakke kromme slechts een deel van dat vlak kan beslaan; Euclides zei al in de derde eeuw voor Christus dat “het geheel steeds groter is z’n delen”. In 1887 echter vond Giuseppe Peano als eerste een vlakvullende kromme, die een volledig tweedimensionaal vierkant beslaat; de fractale kromme in kwestie is het limietgeval van onderstaand proces.



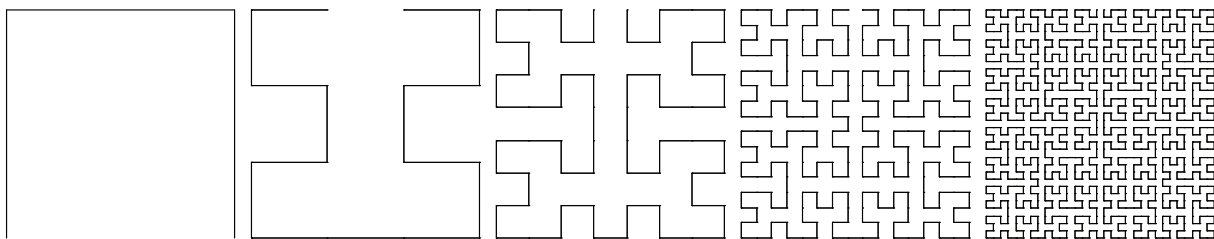
Een jaar na Peano's constructie, publiceerde David Hilbert een variatie op de techniek, waarbij hij een afbeelding voegde ter visualisatie. De kromme van Hilbert begint met een open vierkant waarop herhaaldelijk een fractaal proces wordt toegepast:



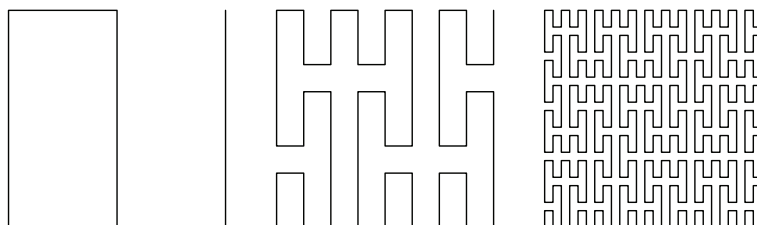
Elk open vierkant wordt vervangen door vier nieuwe open vierkanten, die drie keer zo klein zijn. Vervolgens worden de vierkanten opnieuw met elkaar verbonden en wordt deze stap herhaald. De regels ter vervanging zijn als volgt:

$$\begin{array}{cccccccc}
 \square & \Rightarrow & \sqcup & \rightarrow & \square & \downarrow & \square & \leftarrow & \sqcap \\
 \sqcup & \Rightarrow & \square & \downarrow & \sqcup & \rightarrow & \sqcup & \uparrow & \square \\
 \square & \Rightarrow & \sqcap & \leftarrow & \square & \uparrow & \square & \rightarrow & \sqcup \\
 \sqcap & \Rightarrow & \square & \uparrow & \sqcap & \leftarrow & \sqcap & \downarrow & \square
 \end{array}$$

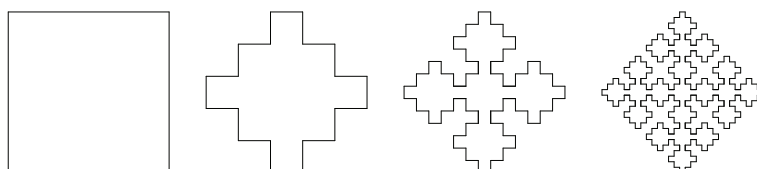
Het limietgeval van dit proces omvat dan uiteindelijk elk punt binnen het oorspronkelijke vierkant. Op deze constructie zijn er veel variaties denkbaar en zodus zijn er al veel meer vlakvullende krommen gevonden; enkele aanpassingen leveren bijvoorbeeld de curve van Moore op:



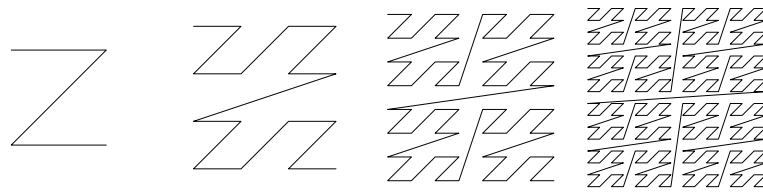
Als verwijzing naar hun ontdekker worden vlakvullende krommen ook vaak Peanokrommen genoemd.



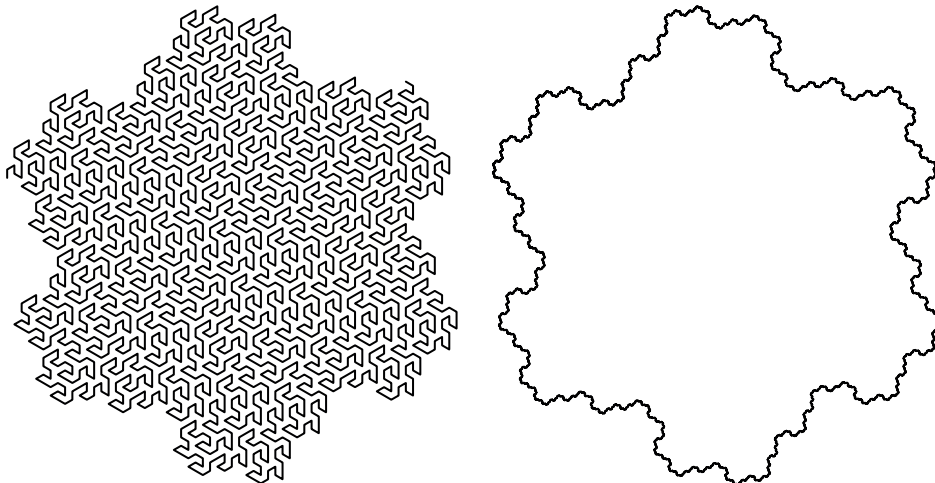
Ook Waclaw Sierpiński, bekend van de naar hem vernoemde driehoek (zie 201, blz. 160), vond er één.



Deze Z-kromme, geïntroduceerd door George Manuel Morton in 1966, heeft nuttige toepassingen in de informatica, om multidimensionale informatie (arrays) af te beelden op ééndimensionale data.

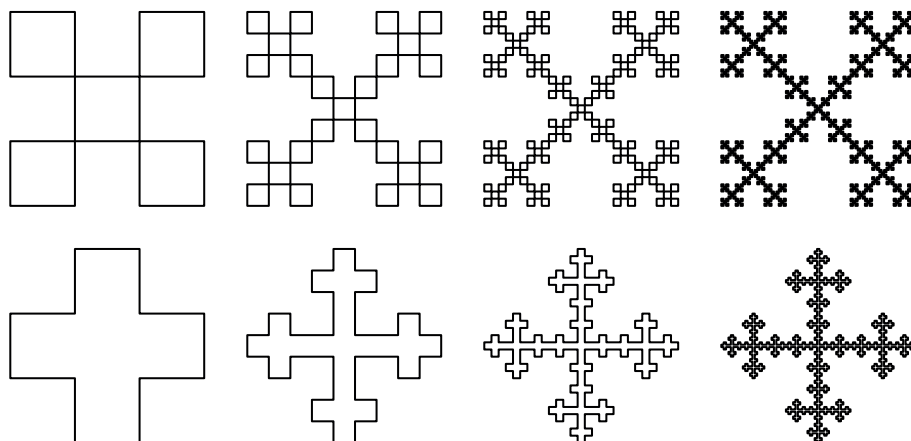


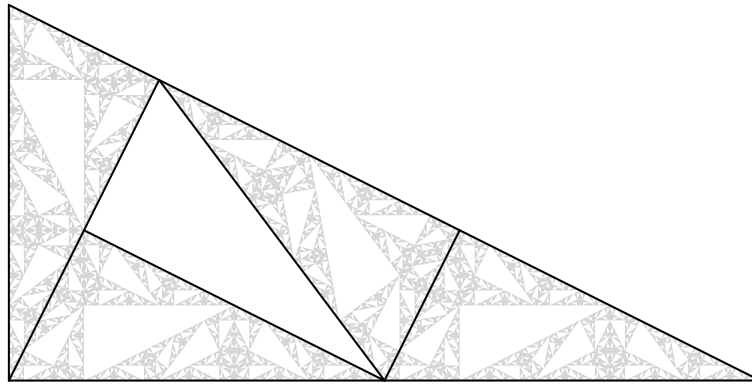
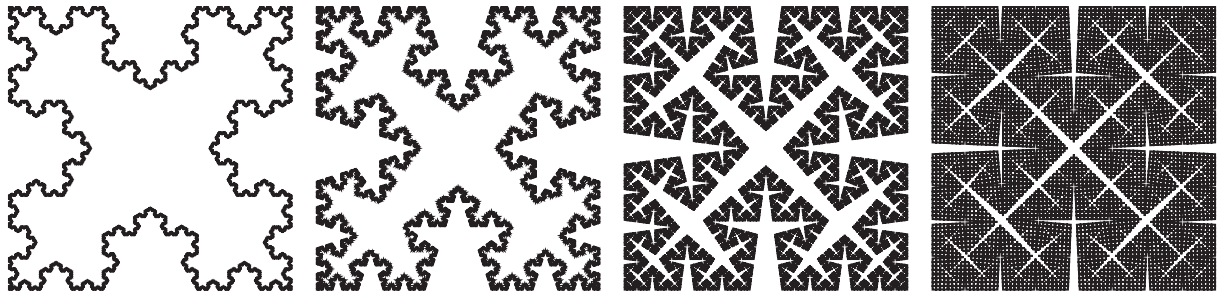
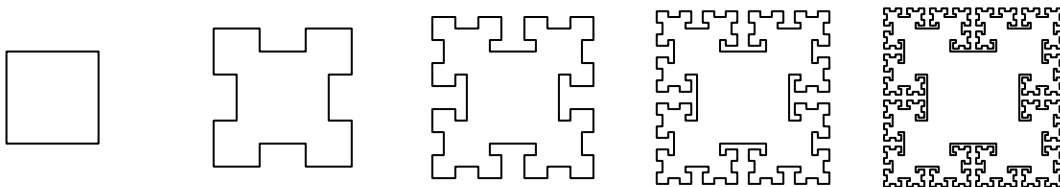
Vlakvullende krommen hoeven niet per se beperkt te blijven tot een vierkant; de kromme van Gosper bijvoorbeeld ligt ingesloten in een fractale figuur (het eiland van Gosper of de *flowsnake*) die gelijkenissen vertoont met de sneeuwvlok van Koch (zie 202, blz. 162).



Ten slotte kunnen vlakvullende krommen nog worden uitgebreid naar meerdere dimensies. Een kromme kan niet alleen een tweedimensionaal vlak vullen, maar mits enkele wijzigingen ook een kubus (een ruimtevullende kromme) of zelfs een  $n$ -dimensionale hyperkubus. Het is ook mogelijk om een kromme zodanig te definiëren dat hij het volledige Euclidische vlak vult.

## 209 Sneeuwvlok van Vicsek

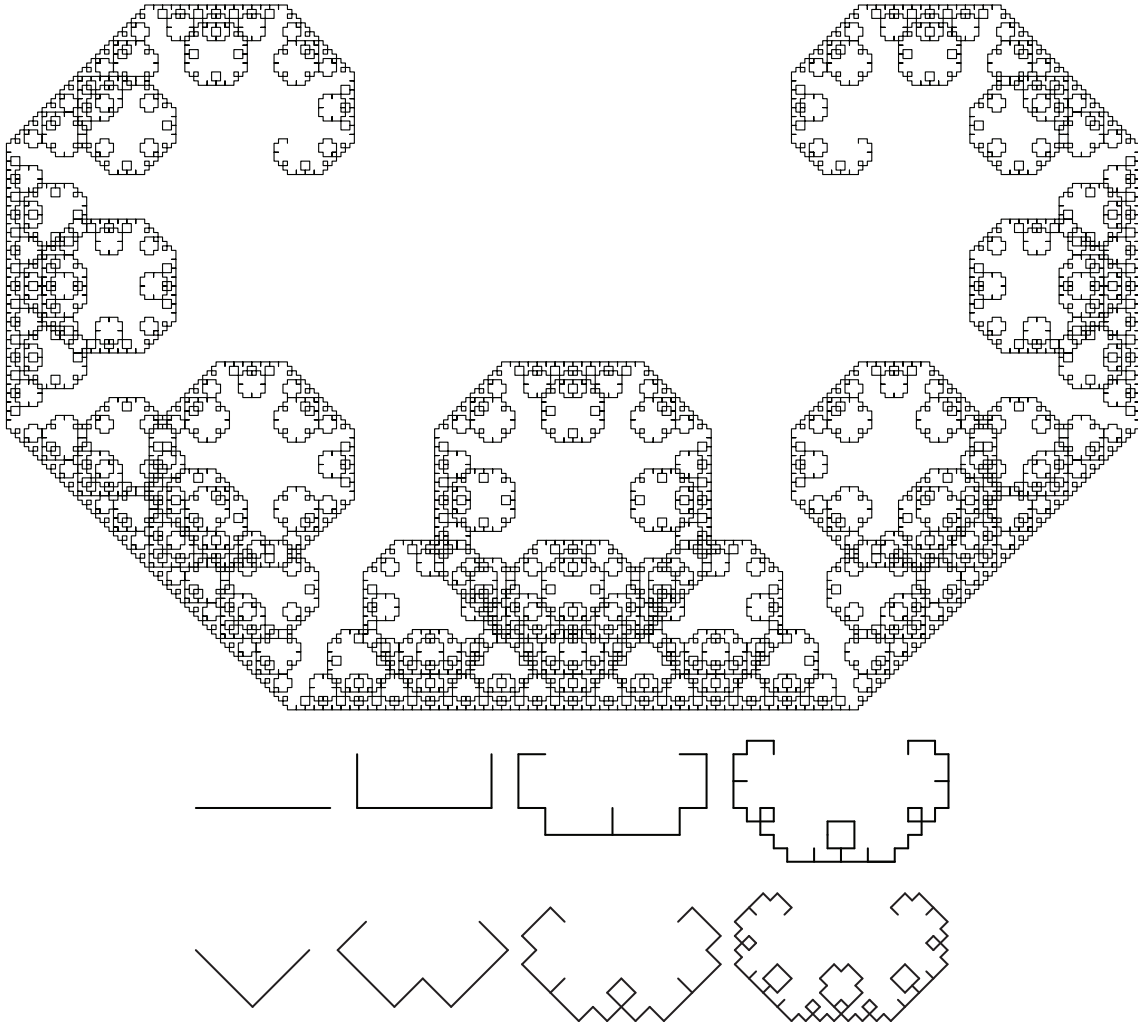


210 **Conways molentje**211 **Cesàro's gescheurd vierkant**212 **Pythagorasbomen**213 **Varen van Barnsley**214 **T-Square**215 **Lévy C-curve**

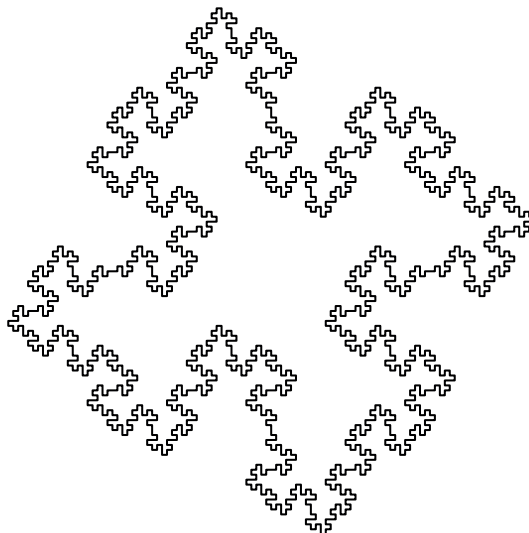
- $V: F, +, -$
- $\omega: F$

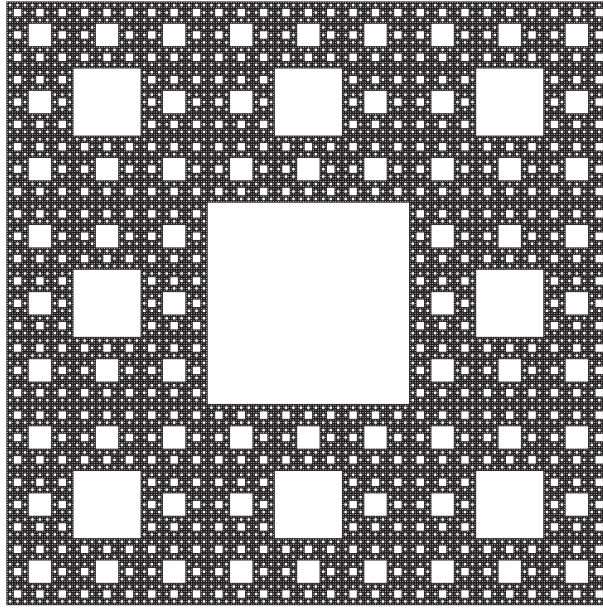


- $P: (F \rightarrow +F - F+)$
- Turtle Graphics:
  - $F$ : teken een eenheid vooruit
  - $+$ : draai  $45^\circ$  naar rechts
  - $-$ : draai  $45^\circ$  naar links



**216 Worst van Minkowski**



**217 Tapijt van Sierpiński****218 Spons van Menger**

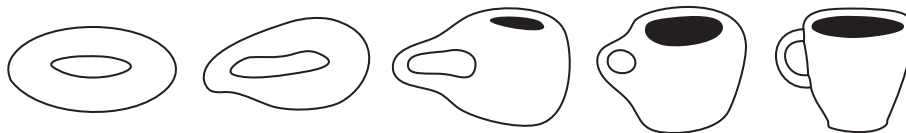




## 219 Topologische handboeien

Topologie is een betrekkelijk nieuw deelgebied. Ze werd pas eind 19<sup>de</sup> eeuw ontwikkeld, maar bloeide sindsdien op tot een belangrijke tak van de wiskunde en kent op haar beurt weer vele deelgebieden. Topologie houdt zich bezig met de eigenschappen van de ruimte die bij (continue) vervorming bewaard blijven; topologische objecten mogen vervormd worden als hoopjes klei, maar niet gescheurd of geplakt. Een dergelijke continue vervorming wordt een homeomorfisme genoemd.

Een klassiek voorbeeld van zo'n continue vervorming is die van een donut tot een koffiekop, wat leidde tot de populaire anekdote dat een topoloog het verschil tussen beide niet zou kunnen herkennen.



Zulke homeomorfismen kunnen tot opmerkelijke transformaties leiden. Zo zijn twee in elkaar gehaakte, met elkaar verbonden ringen topologisch equivalent aan diezelfde ringen, los van elkaar:



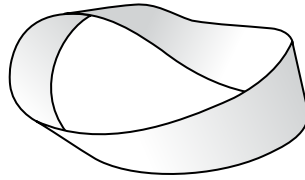
Een soortgelijke transformatie is die waarbij de twee ringen vastzitten rond een derde ring:



## 220 Möbiusband

Deze opmerkelijke topologische structuur werd in 1858 geïntroduceerd door August Ferdinand Möbius en onafhankelijk in datzelfde jaar door Johann Listing. De Möbiusband is een strook wiens uiteinden aan elkaar zijn bevestigd, maar met een halve draai erin, waardoor hij heeft slechts één zijde en één rand heeft. De op zich tweedimensionale band kan diensgevolge enkel in drie dimensies ingebed worden, en is tevens niet-oriënteerbaar: het is mogelijk een chirale\* figuur via een continue beweging over het oppervlak van een Möbiusband af te beelden op zijn spiegelbeeld, wat niet lukt op vertrouwde oriënteerbare oppervlakken als een sfeer of een torus.

\*Chiraliteit (in twee dimensies) houdt in dat een figuur niet kan worden afgebeeld op zijn spiegelbeeld via uitsluitend translaties en rotaties over een vlak. Deze twee versies van de figuur heten dan *enantiomorf*. De term is afgeleid van Oud-Griekse  $\chi\epsilon\lambda\rho$  (wat verwijst naar "hand", het meest bekende chirale object) en speelt tevens een belangrijke rol in de chemie.

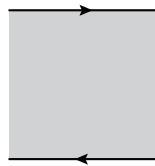


Het is opmerkelijk wat er gebeurt bij het over de lengte doormidden knippen van Möbiusbandachtige structuren. De klassieke geeft bijvoorbeeld een enkele, dubbel zo lange band, waarin een volledige draai zit. Een band met een oneven aantal halve draaien resulteert algemeen in een langere band, met een even aantal halve draaien in twee onderling verbonden banden (elk met evenveel draaien als het origineel). Doormidden knippen op een derde van de rand, geeft een even lange, maar dunnere Möbiusband samen met een dubbel zo lange band met twee volledige draaien erin.

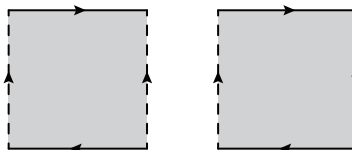
De Möbiusband (met breedte en straal van binnenste cirkel één) kan worden geparаметriseerd in  $\mathbb{R}^3$ :

$$\begin{cases} x(u, v) = \left(1 + \frac{v}{2} \cdot \cos \frac{u}{2}\right) \cdot \cos u \\ y(u, v) = \left(1 + \frac{v}{2} \cdot \cos \frac{u}{2}\right) \cdot \sin u \\ z(u, v) = \frac{v}{2} \cdot \cos \frac{u}{2} \end{cases} \quad \text{met } u \in [0, 2\pi] \text{ en } v \in [-1, 1]$$

Topologisch kan de Möbiusband ook gezien worden als het vierkant  $[0, 1] \times [0, 1]$  waarbij de bovenste en onderste zijde geïdentificeerd worden volgens de relatie  $(x, 0) \sim (1-x, 1)$  voor  $0 \leq x \leq 1$ , zoals in onderstaand diagram. Concreet komt dit neer op deze zijden volgens de pijltjes “aan elkaar te plakken”.



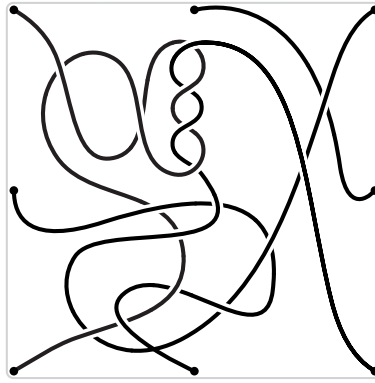
Een gerelateerde figuur is de fles van Klein, die ontstaat door twee Möbiusbanden langs hun rand aan elkaar te plakken, of via het linkerdiagram hieronder. Ook het projectieve vlak bevat soortgelijke eigenschappen als een Möbiusband; door een cirkel te knippen uit dit vlak houd je een Möbiusband over, en omgekeerd, wanneer je een cirkelschijf vastplakt aan de rand van zo'n band, verkrijgt je het projectieve vlak (zie ook het rechterdiagram). Beide figuren kunnen niet worden weergegeven in drie dimensies zonder zichzelf te snijden.



Ook buiten de wiskunde is het concept bekend: in de 19<sup>de</sup> eeuw gebruikten veel stoommachines een Möbiusband als drijfriem, zodat ze gelijkmatig en tweezijdig afsleten en dus dubbel zo lang meegingen.

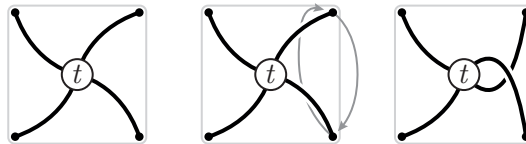
## 221 Tangles van Conway

John Conway beschreef zijn *tangles* tijdens onderzoek naar knopen. Tangles bestaan uit  $n$  lussen binnen een bol, die in een knoopachtige structuur met elkaar verweven kunnen zitten. Door de lussen langsheen de buitenkant van de bol met elkaar te verbinden, ontstaat dan een klassieke knoop, en Conway hoopte met een goed begrip van deze tangles tot een beter begrip van knopen (zie 223, blz. 179) te komen.

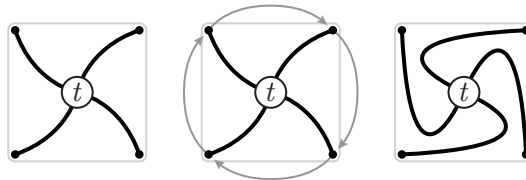


Tangles met twee lussen die te “ontwarren” zijn door hun eindpunten over de bol te verschuiven, heten *rational tangles*, omdat er een prachtig verband met de rationale getallen opgaat: met elke rational tangle is een rationaal getal geassocieerd. Conway stelde deze tangles voor als vier dansers, die elk een einde van een touw vasthouden en twee bewegingen kunnen uitvoeren: een *twist'em up* en een *turn'em roun'*.

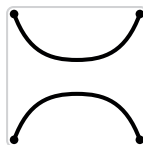
Bij de eerste actie, de *twist'em up*, worden de twee rechtse uiteinden over elkaar één slag om elkaar gewenteld. De onderste gaat onder de bovenste. Deze actie komt overeen met één optellen bij zijn waarde,  $t \rightarrow t + 1$ .



De tweede actie, *turn'em roun'*, betekent niks meer dan gewoon de hele tangle één positie klokgewijs roteren. De waarde van de tangle wordt daarmee omgekeerd en tegengesteld,  $t \rightarrow \frac{-1}{t}$ .

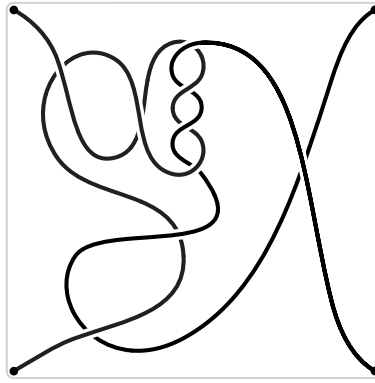


Om te kunnen starten, wordt aan deze tangle de waarde 0 toegekend:



We korten vanaf hier een *twist'em up* af als  $T$ , een *turn'em roun'* als  $R$  en samenstelling van dezelfde acties met een exponent. Vertrekkende vanaf 0 kan de volgende tangle verkregen worden door de acties  $T^4 \cdot R \cdot T^2 \cdot R \cdot T^2 \cdot R \cdot T$ , waardoor deze tangle de waarde  $\frac{3}{10}$  verkrijgt.

$$0 \xrightarrow{T} 1 \xrightarrow{T} 2 \xrightarrow{T} 3 \xrightarrow{T} 4 \xrightarrow{R} \frac{-1}{4} \xrightarrow{T} \frac{3}{4} \xrightarrow{T} \frac{7}{4} \xrightarrow{R} \frac{-4}{7} \xrightarrow{T} \frac{3}{7} \xrightarrow{T} \frac{10}{7} \xrightarrow{R} \frac{-7}{10} \xrightarrow{T} \frac{3}{10}$$



Merk op dat de twee bewegingen maar in één richting gelden en er dus niet zomaar teruggekeerd kan worden! Een legitieme mogelijkheid om opnieuw 0 te bekomen, is bijvoorbeeld  $R \cdot T^4 \cdot R \cdot T^2 \cdot R \cdot T^2$ .

$$\frac{3}{10} \xrightarrow{R} \frac{-10}{3} \xrightarrow{T} \frac{-7}{3} \xrightarrow{T} \frac{-4}{3} \xrightarrow{T} \frac{-1}{3} \xrightarrow{T} \frac{2}{3} \xrightarrow{R} \frac{-3}{2} \xrightarrow{T} \frac{-1}{2} \xrightarrow{T} \frac{1}{2} \xrightarrow{R} -2 \xrightarrow{T} -1 \xrightarrow{T} 0$$

Hoe kan je nu berekenen welke reeks manipulaties je moet uitvoeren om een tangle te verkrijgen, horende bij een gegeven breuk? Dit is eenvoudig af te lezen uit de volgende voorstelling als kettingbreuk (zie 22, blz. 14):

$$\frac{p}{q} = n_0 + \frac{-1}{n_1 + \frac{-1}{n_2 + \frac{-1}{\ddots + \frac{-1}{n_k}}}}$$

De gewenste *twist'em ups* en *turn'em rounds* (vanaf 0) worden dan:

$$T^{n_k} \cdot R \dots R \cdot T^{n_2} \cdot R \cdot T^{n-1} \cdot R \cdot T^{n_0}$$

Het berekenen van deze kettingbreukvoorstelling komt in feite neer op het algoritme van Euclides in vormomming. De waarden  $n_i$  blijken namelijk overeen te komen met de coëfficiënten in dit lichtjes gewijzigde algoritme (let op de mintekens):

$$\begin{aligned} p &= n_0 \cdot q - r_1 \\ q &= n_1 \cdot r_1 - r_2 \\ r_1 &= n_2 \cdot r_2 - r_3 \\ &\vdots \\ r_{k-1} &= n_k \cdot r_k \end{aligned}$$

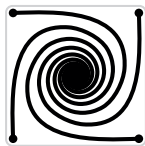
Tot slot merkte Conway nog een subliem detail op, een finishing touch aan de analogie met de rationale getallen. Als op de tangle met waarde 0 een *turn'em roun'* wordt toegepast, wordt zijn waarde het onzinnige  $\frac{-1}{0}$ . Omdat de bijhorende tangle zelf geen problemen geeft, lijkt het wel geoorloofd ermee te rekenen als  $\pm\infty$ . En wat gebeurt er wanneer bij oneindig één wordt opgeteld? Voer een *twist'em up* uit:

$$\begin{array}{ccc} \begin{array}{|c|} \hline \text{Diagram 1: Two strands, one on the left, one on the right, facing each other.} \\ \hline \end{array} & \longrightarrow & \begin{array}{|c|} \hline \text{Diagram 2: Two strands, one on the left, one on the right, facing each other, with a small loop on the right strand.} \\ \hline \end{array} \\ \pm\infty & \longrightarrow & \pm\infty + 1 \end{array} = \begin{array}{|c|} \hline \text{Diagram 3: Two strands, one on the left, one on the right, facing each other.} \\ \hline \end{array} \pm\infty$$

De analogie tussen tangles en breuken blijft geldig tot in oneindig!

Tot slot nog wat spelerei. Aangezien het imaginaire getal  $i = \frac{-1}{i}$ , zou een tangle horende bij  $i$  invariant moeten zijn onder een *turn'em roun'*, en deze oneindige tangle blijkt te voldoen:





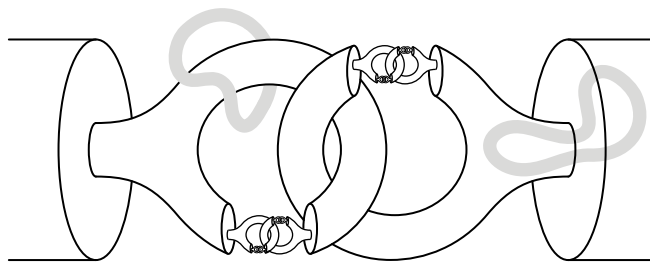
## 222 Gehoornde sfeer van Alexander

De hoornde sfeer van Alexander is een pathologische inbedding van een sfeer in de driedimensionale ruimte, waarvoor het lastig is een “binnenkant” en een “buitenkant” te definiëren. James Alexander beschreef het ding in 1924 en toonde ermee aan dat een intuïtief lijkende veralgemening van de stelling van Jordan (zie ??, blz. ??) niet opgaat in drie dimensies.

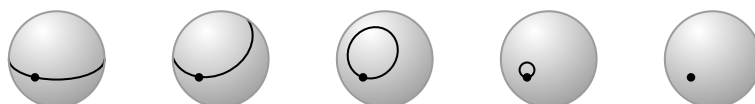
De hoornde sfeer wordt geconstrueerd vanuit een gewone torus:

- Verwijder een schijfje uit de torus.
- Verbind een nieuwe getopte torus aan beide kanten van de snede, door elkaar verbonden.
- Herhaal stap 1 en 2 *ad infinitum*.

Een close-up van het limietproces, zoals getekend door Alexander zelf:

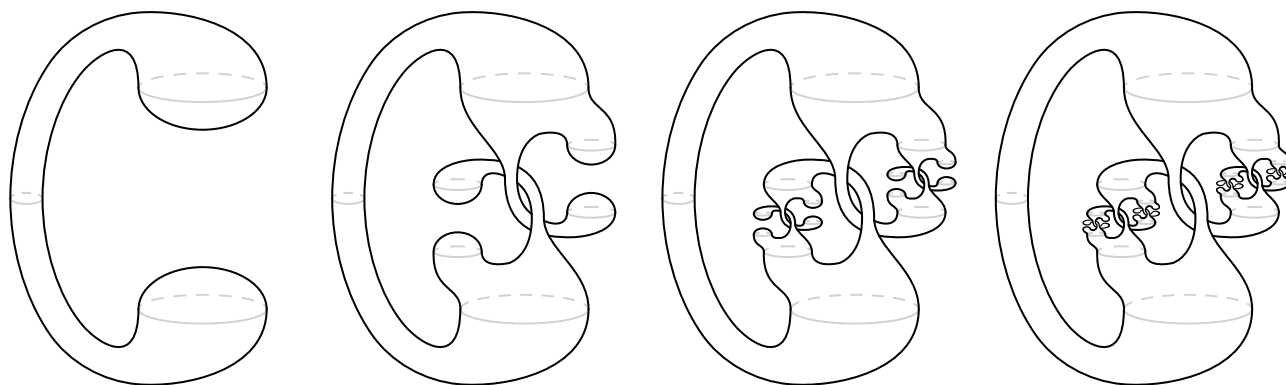


Deze fractale structuur samen met zijn binnenkant is topologisch equivalent (homeomorf) aan een gewone bal, want ze is enkelvoudig samenhangend: teken een willekeurige lus volledig binnen de hoornde sfeer gelegen, zoals de rechterlus op het diagram hierboven, en hij kan worden samengetrokken tot een punt. Deze eigenschap hebben enkel topologische structuren die uit één stuk bestaan en geen gaten bevatten.



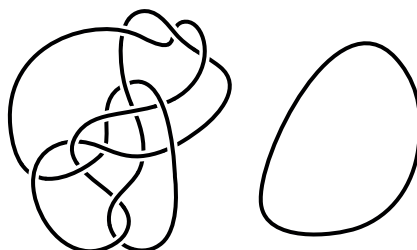
Nochtans is de buitenkant van de hoornde sfeer *niet* enkelvoudig samenhangend: teken een willekeurige lus rond de hoorns en deze kan nooit tot een punt slinken zonder de structuur te snijden, zelfs niet in een oneindig aantal stappen!

Alexander vermoedde eerst dat de stelling van Jordan-Schönflies, die stelt dat een eenvoudige gesloten kromme het vlak verdeelt in een binnen- en buitenkant beide homeomorf met de binnen- en buitenkant van een gewone cirkel, ook zou opgaan in drie dimensies; zijn hoornde sfeer bewees echter het tegendeel.



## 223 Knopen

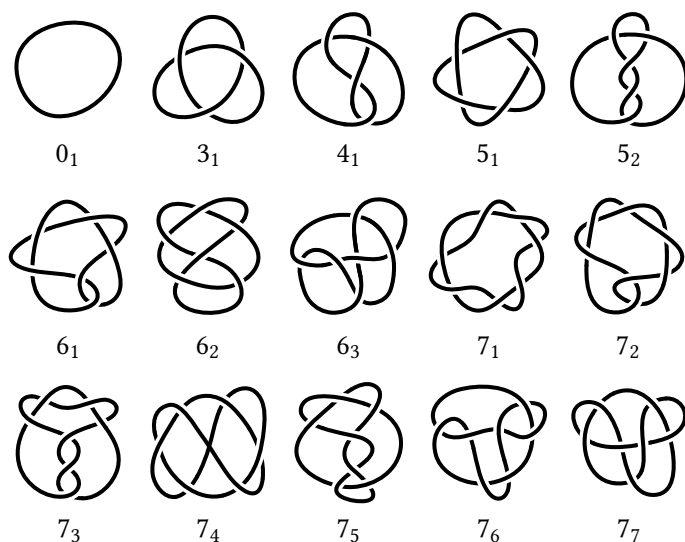
Knopentheorie vormt een zeer interessant domein binnen de topologie, dat ook belangrijke toepassingen kent in bijvoorbeeld DNA-analyse. Ondanks dat iedereen met knopen vertrouwd is, blijkt een goed begrip van deze wiskundige structuren heel wat lastiger dan verwacht. Wiskundig wordt een knoop gedefinieerd als een inbedding van een cirkel in de driedimensionale Euclidische ruimte, oftewel een gesloten kromme die zichzelf niet snijdt; merk op dat dit niet volledig correspondeert met het dagelijkse woordgebruik aangezien deze wiskundige knopen geen eindpunten mogen hebben.



Het simpelste voorbeeld van een knoop is de triviale knoop of onknoop (Engels: *unknot*), die niets meer is dan een gesloten lus zonder kruisingen. Diens standaardvorm staat rechts hierboven. Minder voor de hand liggend is dat de knoop hierboven links óók een onknoop in vermomming is! Door op het model de juiste manipulaties uit te voeren, wordt die teruggebracht naar een ongeknootte lus. Het centrale probleem, de heilige graal van de knopentheorie is het vinden van een invariant om knopen te kunnen onderscheiden van elkaar of juist te bepalen of verschillende projecties dezelfde knoop voorstellen, en dit blijkt een verrassend moeilijk probleem.

Bekende knopeninvarianten maken gebruik van veeltermen, waarvan de coëfficiënten bepaalde eigenschappen van de knoop coderen. James Alexander gaf als eerste een polynomiale invariant in 1923, maar het belang ervan werd pas duidelijk toen John Conway een alternatieve aanpak opmerkte via *skein relations*. In 1984 gaf Vaughan Jones een nieuwe invariant, waarna er nog ontdekt werden zoals de HOMFLY-veelterm. Geen enkele van deze invarianten geeft echter al een 100% sluitend resultaat als het gaat om identificatie van verschillende knopen.

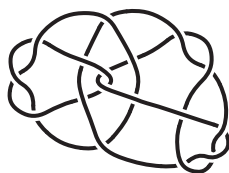
Peter Tait was de eerste die begon met een catalogisering van de mogelijke knopen. Zijn werk werd verdergezet door Charles Little en Thomas Kirkman. Hun tabellen bevatten de priemknopen (zie verder), op reflectie na, in de representatie die het minste aantal kruisingen vergt. De knopen staan op dit aantal geklasseerd en worden voorzien van een index, die geen verdere betekenis heeft. Deze traditionele notatie heet de Alexander-Briggsnotatie; hieronder staat de tabel tot op zeven kruisingen.



Omdat het aantal priemknopen met  $n$  kruisingen zeer snel toeneemt met  $n$  wordt verdere catalogisering al gauw onhoudbaar en hoeft het niet te verwonderen dat er meerdere fouten gevonden zijn in eerdere knopentabellen. Het aantal van deze priemknopen staat in OEIS A002863; hoewel er exponentiële onder- en bovengrenzen bekend zijn, is het nog niet aangetoond of deze rij strikt stijgend zou zijn.

0, 0, 1, 1, 2, 3, 7, 21, 49, 165, 552, 2176, 9988, 46972, 253293, 1388705 . . . (OEIS A002863)

Algemener bestudeert de knopentheorie ook de structuur van linken of schakels. Dit zijn collecties knopen, die elkaar niet snijden, maar wel onderling vernesteld kunnen zitten, zoals de 2-link hieronder.



### 223.1 Knoopnotatie

...

Een andere manier om knopen te beschrijven is bijvoorbeeld via de generatoren van vlechtgroepen (zie 304, blz. 294).

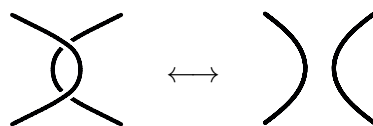
### 223.2 Reidemeisterbewegingen

Een eerste belangrijk hulpmiddel in de studie van knopen zijn de Reidemeisterbewegingen. Onafhankelijk van elkaar toonden Kurt Reidemeister in 1926 en James Alexander en Garland Briggs het jaar daarop aan dat twee knopendiagrammen die horen bij dezelfde knoop, in elkaar om te zetten zijn door een serie van de volgende drie elementaire bewegingen.

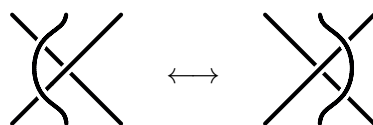
- Verwijder een kink in een lus of voeg er één toe:



- Haal een lus volledig over een andere heen:



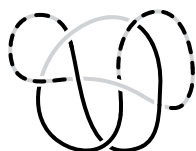
- Beweeg een lus over of onder een bestaande kruising:



Deze Reidemeisterbewegingen maken het mogelijk aan te tonen dat twee knopendiagrammen effectief dezelfde knoop representeren, maar het blijft lastig aan te tonen dat er geen eindige serie van deze bewegingen bestaat om te bewijzen dat twee knopen verschillen.

### 223.3 Driekleurbaarheid

Een eenvoudige invariant waarmee knopen kunnen worden onderscheiden van triviale knopen is driekleurbaarheid. Dit houdt in dat er een kleuring van de strengen moet bestaan met drie kleuren, waarbij de drie strengen rond elke kruising ófwel allemaal dezelfde, ófwel allemaal verschillende kleuren hebben.



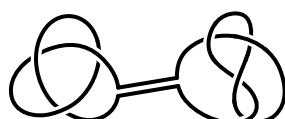
Zoals eenvoudig gecontroleerd kan worden, blijft deze eigenschap behouden onder Reidemeisterbewegingen, zodat driekleurbaarheid onafhankelijk is van het beschouwde diagram. Als concreet gevolg hiervan kan een driekleurbare knoop geen triviale knoop zijn, omdat de triviale knoop niet driekleurbaar is. Veel verdere praktische toepassingen heeft deze invariant echter niet.

Uit driekleurbaarheid volgt tevens dat de klaverbladknoop de kleinste niet-triviale knoop is, waarvan de twee oriëntaties bovendien wel degelijk verschillend (enantiomorf) zijn; de linker- en rechtvariant zijn niet in elkaar om te zetten door een serie Reidemeisterbewegingen.



### 223.4 Samengestelde en priemknopen

Er bestaat een boeiende operatie op knopen, die een mooi verband legt met priemgetallen. De samenstelling of som van twee knopen (traditioneel genoteerd met #) creëert een nieuwe knoop als volgt, door de twee gegeven knopen elk in een boog door te knippen en deze eindpunten onderling te verbinden.



Het is duidelijk dat de triviale knoop hier de rol van eenheid speelt, daar een samenstelling ermee exact dezelfde knoop oplevert. Minder voor de hand liggend is dat het niet uitmaakt op welke lussen de operatie plaatsgrijpt; dit geldt omdat de toegevoegde knoop ook het diagram van de oorspronkelijke knoop kan volgen en zodoende op elke lus hetzelfde resultaat zou opleveren.



Desondanks bestaat de mogelijkheid dat twee knopen op verschillende manieren kunnen worden samengesteld! De bogen recht of kruiselings terug aaneenschakelen kan resulteren in twee verschillende resultaten. Dit probleem kan worden opgelost door de knopen te oriënteren, d.w.z. een vaste richting te geven waarin het diagram doorlopen wordt en die moet matchen bij een samenstelling.

Knopen aldus te construeren uit niet-triviale knopen (factoren) heten samengesteld. Een knoop verschillend van de onknoop die niet kan worden gevormd door niet-triviale knopen samen te stellen, heet priem. Net als bij gehele getallen bestaan er oneindig veel priemknopen en zijn de factoren van samengestelde knopen uniek op volgorde na. Deze laatste eigenschap werd bewezen door Horst Schubert in 1949.

De samenstelling van georiënteerde knopen is een commutatieve en associatieve bewerking, maar het kan worden aangetoond dat geen enkele niet-triviale knoop een inverse heeft, m.a.w. samenstelling van niet-triviale knopen kan nooit een triviale knoop opleveren.

### 223.5 Alexander-Conwayveelterm

Zoals eerder opgemerkt ontdekte James Alexander als eerste een polynomiale knoopinvariant in 1923. Deze naar hem vernoemde Alexanderveelterm werkt ook voor linken en werd later verbeterd door John Conway in 1969, hoewel later bleek dat Alexander al op de hoogte was van deze vorm.

Conways constructie maakt gebruik van een *skein relation* tussen diagrammen van georiënteerde knopen, waarin één welbepaalde kruising in verband staat met andere. De Alexander-Conwaypolynoom  $\nabla \in \mathbb{Z}[t]$  kan dan recursief berekend worden met behulp van de volgende relaties. Er kan worden aangetoond dat hij invariant blijft onder Reidemeisterbewegingen en dus niet afhangt van de gekozen knoopprojectie.

$$\nabla(\bigcirc) = 1, \quad \nabla(\text{X}) - \nabla(\text{Y}) = t \cdot \nabla(\text{Z})$$

Deze relaties maken het mogelijk om Alexander-Conwayveeltermen voor willekeurige knopen uit te rekenen: beschouw een goedgekozen kruising en gebruik de tweede eigenschap om de berekening te herleiden naar twee eenvoudigere knopen of linken, en herhaal dit tot er onknoten optreden, waarvoor dan  $\nabla = 1$ .

Bij wijze van voorbeeld wordt hier de Alexander-Conwayveelterm berekend van een klaverbladknoop met telkens de kruising aangeduid waarop de relatie wordt toegepast.

$$\nabla(\text{Klaverblad}) = \nabla(\text{Hopf}) + t \cdot \nabla(\text{Hopf})$$

Links herkennen we een onknoop, rechts staat de eenvoudigste niet-triviale schakel genaamd de Hopfschakel (naar Heinz Hopf). Deze rekenen we verder uit:

$$\nabla(\text{Hopf}) = \nabla(\text{Hopf}) + t \cdot \nabla(\text{Hopf})$$

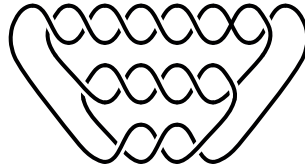
In de rechterterm zien we weer de triviale knoop opduiken, maar bij de linkerterm (de triviale link met twee componenten) schuilt er nog een addertje onder het gras. Er geldt immers:

$$\nabla(\text{Hopf}) = \nabla(\text{Hopf}) + t \cdot \nabla(\text{Hopf})$$

De eerste twee polynomen in deze gelijkheid zijn die voor de triviale knoop, waaruit we kunnen concluderen dat die voor de triviale 2-link gelijk moet zijn aan nul. Terugwerkend naar de klaverbladknoop vinden we dus:

$$\nabla\left(\text{Klaverbladknoop}\right) = 1 + t \cdot (0 + t \cdot 1) = 1 + t^2$$

Ook al zijn linker- en rechtersvariant van de klaverbladknoop verschillend, toch blijken hun Alexander-Conway-polynomen exact gelijk te zijn. Er bestaan zelfs niet-triviale knopen die dezelfde polynoom opleveren als de onknoop, zoals die hieronder. De Alexander-Conwaypolynoom is dus wel praktisch, maar kent beperkingen.



### 223.6 Jonesveelterm

De Jonesveelterm werd ontdekt in 1984 door Vaughan Jones en kent vele interessante toepassingen. Zo is ze bijvoorbeeld oriëntatieonafhankelijk, kan ze sterk veralgemeend worden en blijkt ze beter in staat om knopen te identificeren dan de Alexanderveelterm. De eenvoudigste manier om de polynoom van Jones te definiëren is via een gerelateerde invariant, Kauffmans bracketpolynoom. Ook hier wordt er een *skein relation* gebruikt:

$$\langle \bigcirc \rangle = 1, \quad \langle K \sqcup \bigcirc \rangle = -(A^{-2} + A^2)\langle K \rangle, \quad \langle \text{X} \rangle = A\langle \text{>} \rangle + A^{-1}\langle \text{<} \rangle$$

Met  $K \sqcup \bigcirc$  wordt een diagram bedoeld bestaande uit het diagram van een knoop  $K$  samen met een onknoop, die geen kruisingen bevat (noch met zichzelf noch met  $K$ ). De rechtse relatie is analoog te interpreteren als bij de Alexanderpolynoom.

Zoals eenvoudig te verifiëren blijft de bracketpolynoom ongewijzigd bij Reidemeisterbewegingen van het tweede of derde type, maar *niet* van het eerste type. Een dergelijke Reidemeisterbeweging verandert de bracketveelterm als volgt:

$$\langle \text{><} \rangle = -A^3 \langle \text{V} \rangle, \quad \langle \text{<>} \rangle = -A^{-3} \langle \text{V} \rangle$$

Mits een kleine aanpassing kan de Kauffmanpolynoom onafhankelijk van alle Reidemeisterbewegingen vastgelegd worden. Voorzie daartoe de knoop  $K$  van een oriëntatie en definieer zijn verdraaiing\*  $w(K)$  als het aantal positieve kruisingen min het aantal negatieve. Dit is de conventie:

$$\begin{array}{cc} \begin{array}{c} \nearrow \\ \searrow \end{array} & \begin{array}{c} \nwarrow \\ \swarrow \end{array} \\ +1 & -1 \end{array}$$

Ook de verdraaiing blijft enkel behouden onder Reidemeisterbewegingen van tweede en derde type, maar als volgt samengesteld met de bracketpolynoom van Kauffman verkrijgen we een knoopinvariant, geldig voor elke link  $K$  en voor eender welke projectie  $D$  ervan. Zet in deze uitdrukking  $A$  om naar  $t$  via de substitutie  $A^{-2} = t^{\frac{1}{2}}$  om de standaardvorm van de Jonesveelterm  $V \in \mathbb{Z}[t^{\frac{1}{2}}, t^{-\frac{1}{2}}]$  te bekomen.

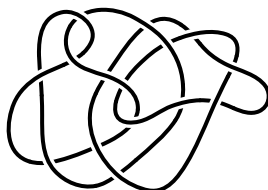
$$V(K) = (-A)^{-3w(D)} \cdot \langle D \rangle \Big|_{A^{-2}=t^{\frac{1}{2}}}$$

De *skein relation* geüpdatet voor de Jonesveelterm ziet er als volgt uit:

$$\langle \bigcirc \rangle = 1, \quad (t^{-\frac{1}{2}} - t^{\frac{1}{2}}) \cdot V(\text{><}) = t \cdot V(\text{><}) - t^{-1} \cdot V(\text{<>})$$

\*Engels: *writhe*

Voor knopen (of algemener, linken met een oneven aantal componenten) bevat de Jonespolynoom uitsluitend gehele machten van  $t$ . Om het spiegelbeeld van een knoop te berekenen volstaat het om  $t$  overal te vervangen door  $t^{-1}$ . Het is nog ongeweten of de Jonesveelterm in staat is elke knoop te onderscheiden van de onknoop, m.a.w. of er een niet-triviale knoop bestaat met triviale  $V$ . Er bestaat wel zo'n niet-triviale 2-link:



### 223.7 HOMFLY-veelterm

De HOMFLY-polynoom is een veralgemening van die van Alexander en Jones, en combineert de initialen van de ontdekkers: Jim Hoste, Adrian Ocneanu, Kenneth Millett, Peter Freyd, William Lickorish en David Yetter. Om onafhankelijk werk van Józef Przytycki en Paweł Traczyk te erkennen wordt HOMFLY soms ook HOMFLY-PT genoemd.

HOMFLY is een polynoom in twee veranderlijken, hier  $\alpha$  en  $z$ , en wordt uniek vastgelegd door de volgende *skein relation* op georiënteerde linken:

$$P(\bigcirc) = 1, \quad \alpha \cdot P(\text{crossing}) - \alpha^{-1} \cdot P(\text{crossing}) = z \cdot P(\text{split})$$

Op dit polynoom  $P$  gelden enkele handige rekenregels, zoals voor een samengestelde knoop  $K_1 \# K_2$ :

$$P(K_1 \# K_2) = P(K_1) \cdot P(K_2)$$

Een analoge regel bestaat voor een gescheiden unie\*  $K_1 \sqcup K_2$ , d.w.z. twee onderling onvernestelde knopen:

$$P(K_1 \sqcup K_2) = \frac{-(l + l^{-1})}{m} \cdot P(K_1) \cdot P(K_2)$$

Om de HOMFLY-polynoom van het spiegelbeeld van een knoop te berekenen, volstaat het om overal  $\alpha$  te vervangen door  $\alpha^{-1}$  en  $z$  ongewijzigd te laten.

Een gepaste substitutie van de variabelen van de HOMFLY-polynoom resulteert in de veelterm van Alexander ( $\nabla$ ) of Jones ( $V$ ). Ze zijn als volgt gerelateerd voor elke knoop  $K$ :

- $V(K) = P(K) \Big|_{\alpha=t^{-1}, z=t^{\frac{1}{2}-t^{-\frac{1}{2}}}}$
- $\nabla(K) = P(K) \Big|_{\alpha=1, z=t}$

Tot nog toe is de HOMFLY-veelterm de krachtigste bekende knoopinvariant, ondanks het feit dat er hele families verschillende knopen bestaan met dezelfde HOMFLY.

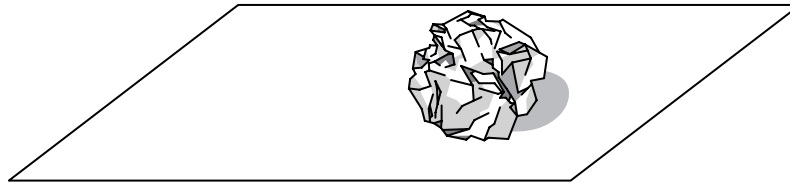
### 223.8 Andere invarianten

### 223.9 Seifertoppervlakken

## 224 Brouwers dekpuntstelling

Neem twee identieke bladen papier, verfrommel het eerste en plaats het bovenop het tweede. Volgens Brouwers dekpuntstelling zal er steeds, hoe je het blad ook vervormt, plooit of verplaatst, een punt van het bovenste blad direct boven het corresponderende punt op het onderste blad liggen!

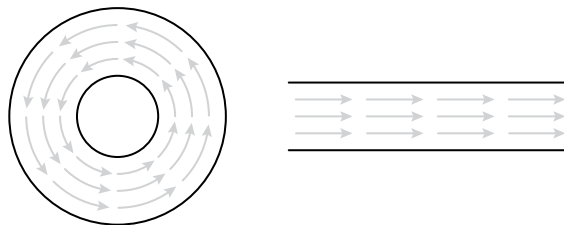
\*Engels: *split union*



Formeler en algemener zegt de stelling, vernoemd naar Nederlands wiskundige Luitzen Brouwer, dat voor elke continue functie  $f$  die een convexe compacte deelverzameling van  $\mathbb{R}^n$  op zichzelf afbeeldt, minstens één punt  $x$  bestaat dat voldoet aan  $f(x) = x$ . Dit punt wordt een fixpunt of dekpunt genoemd. Een andere illustratie: leg een landkaart uit op een tafel in dat bepaalde land. Dan ligt er steeds een punt op de kaart precies boven het gerepresenteerde punt.

Brouwers dekpuntstelling was een van de eerste prestaties van de algebraïsche topologie, en legt de basis voor complexere fixpuntstellingen. Ze vindt toepassingen in allerlei domeinen van de wiskunde, van differentiaalvergelijkingen tot evenwichten in markteconomie. Een eerste versie voor  $n = 3$  werd bewezen door Piers Bohl in 1904 maar bleef onopgemerkt. Luitzen Brouwer bewees hetzelfde geval in 1909, het jaar daarop toonde Jacques Hadamard het algemene geval aan en gaf Brouwer nog een bewijs. Brouwer werd geïnspireerd door het roeren in een kopje koffie (er bleek steeds een bewegingloos punt op het oppervlak). De naar hem vernoemde stelling impliceert dat er zich een punt in de koffie bevindt dat na het roeren niet van positie veranderd is, en als je dit punt dan toch verplaatst in een volgende roerbeweging, zal je automatisch een nieuw fixpunt creëren.

De voorwaarden zijn wel degelijk van belang. Als de deelverzameling van  $\mathbb{R}^n$  gaten bevat of onbegrensd is, zoals de voorbeelden hieronder, is het bestaan van een dekpunt niet langer waarborgd. De beschouwde verzameling moet ook gesloten zijn: de functie  $f : ] - 1, 1[ \rightarrow ] - 1, 1[ : x \mapsto \frac{x+1}{2}$  is bijvoorbeeld continu maar heeft geen vaste punten. Als we het domein sluiten tot  $[-1, 1]$  is er wel een dekpunt (1). Tot slot is ook continuïteit vereist: de beweringen hierboven gaan niet op als je het blad papier scheurt of de koffie over de rand morst.

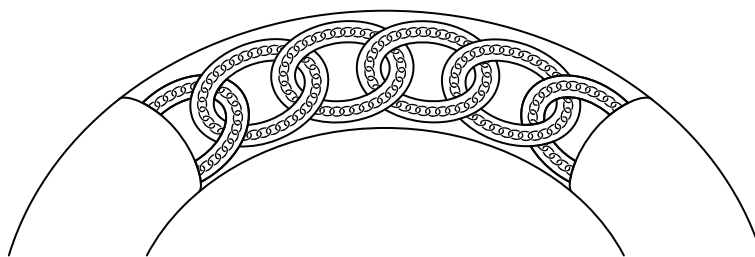


Brouwer zelf mag de grondlegger van het intuïtionisme genoemd worden, en aldus de filosofische tegenpositie van Hilbert, die het formalisme belichaamde. In het intuïtionisme is de uitspraak  $P$  bijvoorbeeld sterker dan  $\neg(\neg P)$  en wordt de wet van de uitgesloten derde (*tertium non datur*) als ongeldig beschouwd. Voor een intuïtionist bestaat een object met bepaalde eigenschappen pas als het zodanig geconstrueerd kan worden, i.t.t. tot Hilberts visie, waarin een object ook bestaat als zijn niet-bestaan ontkend kan worden. Ironisch genoeg was Brouwer niet in staat een constructief bewijs te geven voor zijn dekpuntstelling; zijn bewijzen geven enkel aan dat een dergelijk punt bestaat maar geven geen methode om het ook effectief te vinden.

## 225 Antoinettes ketting

Louis Antoine construeerde dit bizarre topologische object in 1921. Vertrek vanuit een een solide torus, vervang deze door een aantal kleinere aaneengeschakelde torussen en herhaal dit. Blijf schakels vervangen door een nieuwe ketting van schakels. Na aftelbaar veel zulke stadia heet het resultaat de ketting van Antoine.

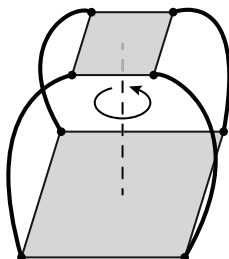




Aangezien de schakels willekeurig klein worden, zijn de verbonden componenten van Antoine's ketting enkelvoudige punten. Daarenboven is ze gesloten, bevat ze geen geïsoleerde punten en heeft ze de kardinaliteit van het continuüm. Deze eigenschappen zijn voldoende om te besluiten dat de ketting homeomorf is met de Cantor-verzameling (zie 207, blz. 166), hoewel het complement van deze inbedding niet enkelvoudig verbonden is.

## 226 Diracs touwtruc

Verbind de hoekpunten van een vierkant met die van een groter vierkant door middel van lang, los touw zoals op de figuur hieronder. Roteer dit vierkant één keer rond (over  $360^\circ$ ) over een verticale as. De touwtjes raken enigzins verstrikt en kunnen niet ontward worden zonder de vierkanten nog te verdraaien.



Draai nu het vierkant nog eens rond, over  $360^\circ$  in dezelfde richting. Verrassend genoeg raken de touwtjes nu niet nog meer in de war, maar kunnen ze ontward worden door ze over het bovenste vierkant te halen!

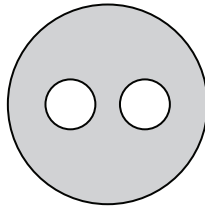
Een variant van dit concept heet de Filipijnse wijnglastruc. Een glas water vastgehouden in één hand kan over  $720^\circ$  gerooteerd worden zonder water te morsen, puur door het glas onder en boven de elleboog te wentelen. Een rotatie over  $360^\circ$  is echter onmogelijk op die manier.

Dit principe, voorgesteld door Paul Dirac, is een van de eerste toepassingen van de algebraïsche topologie in de kwantumfysica en illustreert het kwantumspingetal  $\frac{1}{2}$  van elektronen. Onder een rotatie van  $360^\circ$  keert zijn amplitude om, die weer hersteld wordt onder een rotatie van  $720^\circ$ . De achterliggende algebraïsche structuren in hun algemeenheid (zogenaamde spinoren) ontdekte Élie Cartan in 1913.

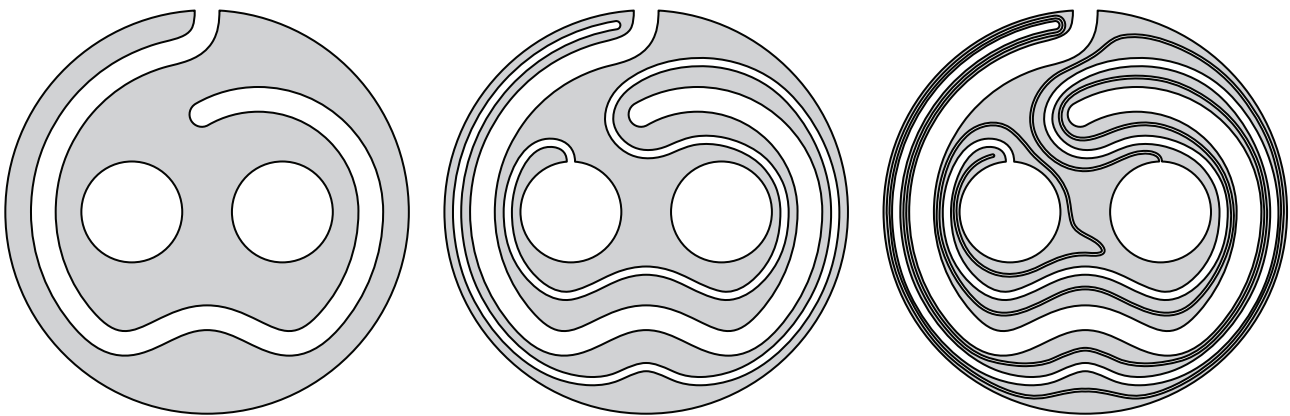
## 227 Meren van Wada

Kunnen meerdere onderling disjuncte, samenhangende, open verzamelingen in het vlak dezelfde grens hebben? De open binnen- en buitenzijde van een cirkel zijn voor de hand liggende voorbeelden, maar het lijkt intuïtief onmogelijk dat er méér dan twee zulke gebieden voldoen of dat deze voorbeelden begrensd kunnen zijn.

Kunizō Yoneyama publiceerde echter in 1917 een constructie voor dergelijke bizarre gebieden! Hij schreef de ontdekking toe aan zijn leraar Takeo Wada, zodat de geconstrueerde gebieden thans bekendstaan als de meren van Wada. Vertrek vanuit een eiland waarin een aantal meren liggen, zegge  $k$  (hier dus  $k = 2$ ):



Leg vanuit de zee een kanaal aan doorheen het eiland, zodat elk punt van het drooggebleven land op een afstand ten hoogste 1 van het zeewater ligt. Dit moet zodanig gebeuren dat het binnengebied van het resterende land verbonden blijft en de zee open. Vervolgens wordt een nieuw kanaal aangelegd vanuit het eerste meer, dat nog dichter van elk resterend punt op het eiland ligt, etc. Algemeen wordt in de  $n^{\text{de}}$  stap een kanaal toegevoegd vanuit het  $(n \bmod k)^{\text{de}}$  meer, die het eiland zodanig irrigeert dat elk punt op het land hoogstens  $\frac{1}{n}$  ver ligt van het water uit dat meer. De zee telt mee als het  $0^{\text{de}}$  meer.



In het limiet van dez procedure vormt het resterende droge land de grens van zowel de zee als elk van de meren. De constructie uitvoeren op eilanden met meerdere meren geeft uiteraard meerdere gebieden met dezelfde grens; via een iets gewijzigde methode kunnen zelfs aftelbaar veel gebieden met Wada's eigenschap gevonden worden.

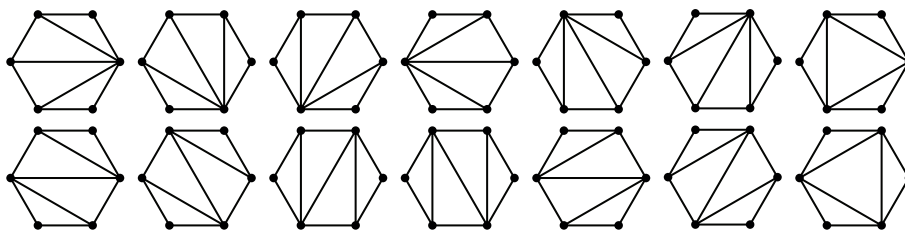




## 228 Catalangetallen

De geschiedenis van de Catalangetallen (genoteerd als  $C_n$ ) begint bij Leonhard Euler, die via een brief in 1751 Christian Goldbach volgend vraagstuk voorlegde:

OP HOEVEEL MANIEREN KAN EEN REGELMATIGE  $n$ -HOEK DOOR ZIJN DIAGONALEN IN DRIEHOEKEN VERDEELD WORDEN? DE DIAGONALEN MOGEN ELKAAR NIET SNIJDEN EN DRAAIINGEN OF SPIEGELINGEN WORDEN APART GETELD.



Euler vond een inductief bewijs voor de oplossing van zijn delingsprobleem, waarvan hij zij dat het hem “heel wat inspanning kostte”. Desondanks worden de getallen die uit het probleem voortvloeien, vernoemd naar de Belgische wiskundige Eugène Catalan, die een verband ontdekte met combinaties van haakjes toen hij werkte aan de torens van Hanoi (zie ??, blz. ??). Een reglementaire verdeling van de  $n$ -hoek kan op  $C_{n-2}$  manieren.

1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012, 742900, 2674440, 9694845 . . . (OEIS A000108)

Enkele expliciete formules voor de Catalangetallen:

$$C_n = \frac{1}{n+1} \binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1} = \frac{(2n)!}{(n+1)!n!} = \prod_{k=2}^n \frac{k+n}{n}$$

De Catalangetallen kunnen ook recursief berekend worden:

$$C_0 = 1, \quad C_{n+1} = \sum_{i=0}^n (C_i \cdot C_{n-i}) = \frac{2(2n+1)}{n+2} \cdot C_n$$

Asymptotisch groeit  $C_n$  als:

$$C_n \sim \frac{4^n}{\sqrt{\pi n^3}}$$

In de combinatoriek hebben allerlei telproblemen de Catalangetallen als oplossingen.

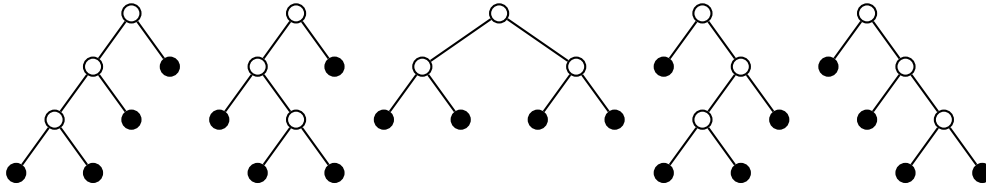
- $C_n$  is zoals eerder opgemerkt het aantal manieren om een convexe veelhoek met  $n + 2$  zijden te verdelen in driehoeken via niet-snijdende diagonalen (Eulers delingsprobleem).
- $C_n$  is het aantal correcte manieren om  $n$  paren haakjes op te schrijven, zodat de haakjes matchen.

((( )))   ()( )   ()( )   ()( )   ()( )

- $C_n$  is het aantal verschillende mogelijkheden om  $n + 1$  factoren volledig tussen haakjes te zetten (of het aantal mogelijkheden om een binaire operator toe te passen op  $n + 1$  argumenten).

$$((ab)c)d \quad (a(bc))d \quad (ab)(cd) \quad a((bc)d) \quad a(b(cd))$$

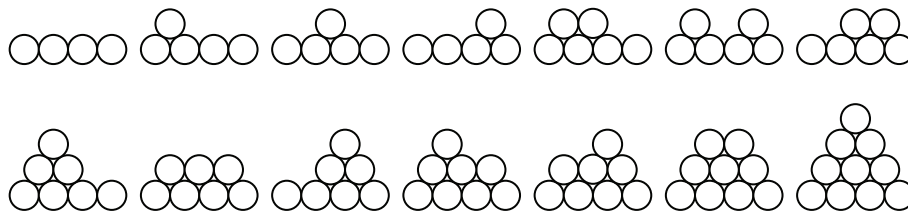
- $C_n$  is het aantal binaire bomen vanuit één punt met  $n + 1$  bladeren.



- $C_n$  is het aantal monotone paden langs een  $n \times n$ -rooster, die de diagonaal niet kruisen (vertrekkend vanuit één hoekpunt naar het tegenoverliggende hoekpunt, het rooster following).

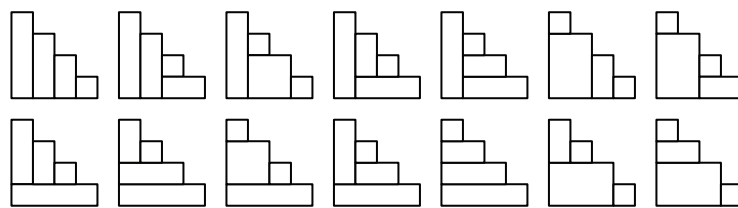


- $C_n$  is het aantal “fonteinen” waarvan de basis  $n$  cirkels breed is.



- $C_n$  is het aantal mogelijkheden om  $2n$  punten op een cirkel te verbinden met  $n$  niet-snijdende koorden.

- $C_n$  is het aantal manieren om een trapvorm van hoogte  $n$  te betegelen met  $n$  rechthoeken.



- $C_n$  is het aantal permutaties van  $\{1, 2, \dots, n\}$  waarbij in geen enkele deelrij drie opeenvolgende, stijgende termen voorkomen (bijvoorbeeld 1324, die uitgesloten wordt omdat die deelrij 124 bevat).

$$\{1, 2, 3, 4\} \longmapsto 1432, 2143, 2413, 2431, 3142, 3214, 3241, 3412, 3421, 4132, 4213, 4231, 4312, 4321$$

- $C_n$  is het aantal manieren waarop de getallen  $1, 2, \dots, 2n$  kunnen worden gerangschikt in een  $n \times 2$ -rooster, zodanig dat elke rij en elke kolom een stijgende rij vormt.

$$\{1, 2, 3, 4, 5, 6\} \longmapsto \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & 4 \\ \hline 5 & 6 \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & 5 \\ \hline 4 & 6 \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 4 \\ \hline 5 & 6 \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 5 \\ \hline 4 & 6 \\ \hline \end{array} \quad \begin{array}{|c|c|} \hline 1 & 4 \\ \hline 2 & 5 \\ \hline 3 & 6 \\ \hline \end{array}$$

De driehoek van Catalan is een soortgelijke constructie als de driehoek van Pascal (zie 246, blz.204) maar genereert de Catalangetallen i.p.v. binomiaalgetallen, en wordt als volgt gedefinieerd:

- Begin met een rij met 1 als enige element.
- Begin een nieuwe rij met 1 als eerste element.
- Elk element is de som van het getal links en het getal erboven; reken ontbrekende getallen als 0.
- Herhaal stap 2 en 3 voor het vormen van nieuwe rijen (telkens één element meer dan de vorige).
- Het Catalangetal  $C_n$  komt tevoorschijn als het laatste element van rij  $n$ , of als de som van rij  $n - 1$ .

$$\begin{array}{ccccccc}
 & & & & & & 1 \\
 & & & & & & 1 & 1 \\
 & & & & & & 1 & 2 & 2 \\
 & & & & & & 1 & 3 & 5 & 5 \\
 & & & & & & 1 & 4 & 9 & 14 & 14 \\
 & & & & & & 1 & 5 & 14 & 28 & 42 & 42 \\
 & & & & & & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
 \end{array}$$

Deze functie brengt de Catalangetallen voort:

$$\sum_{n=0}^{\infty} C_n \cdot x^n = \frac{2}{1 + \sqrt{1 - 4x}}$$

Tot slot geldt nog deze eigenschap, ongeacht de waarde van  $n$ .

$$\begin{vmatrix} C_0 & C_1 & C_2 & \cdots & C_n \\ C_1 & C_2 & C_3 & \cdots & C_{n+1} \\ C_2 & C_3 & C_4 & \cdots & C_{n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ C_n & C_{n+1} & C_{n+2} & \cdots & C_{2n} \end{vmatrix} = \begin{vmatrix} C_1 & C_2 & C_3 & \cdots & C_{n+1} \\ C_2 & C_3 & C_4 & \cdots & C_{n+2} \\ C_3 & C_4 & C_5 & \cdots & C_{n+3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ C_{n+1} & C_{n+2} & C_{n+3} & \cdots & C_{2n+2} \end{vmatrix} = 1$$

## 229 Subfaculiteiten

Definieer een derangement als een permutatie zonder fixpunten, dus een permutatie die geen enkel element op z'n oorspronkelijke positie afbeeldt. Er zijn bijvoorbeeld negen zulke derangementen op vier elementen:

$$\{1, 2, 3, 4\} \mapsto \begin{array}{lll} \{2, 1, 4, 3\}, & \{2, 3, 4, 1\}, & \{2, 4, 1, 3\}, \\ \{3, 1, 4, 2\}, & \{3, 4, 1, 2\}, & \{3, 4, 2, 1\}, \\ \{4, 1, 2, 3\}, & \{4, 3, 1, 2\}, & \{4, 3, 2, 1\} \end{array}$$

Het aantal derangementen op  $n$  elementen wordt voorgesteld door  $!n$  (niet te verwarren met de faculteit  $n!$ ). De  $!n$ -waarden worden de subfaculiteiten of de de Montmortgetallen genoemd, naar Pierre Raymond de Montmort die in 1708 als eerste het probleem beschouwde en het in 1713 ook oploste. Ook Nicholas Bernoulli hield zich gelijktijdig met de subfaculiteiten bezig.

1, 0, 1, 2, 9, 44, 265, 1854, 14833, 133496, 1334961, 14684570, 176214841, 2290792932, ... (OEIS A000166)

Voor de subfaculiteiten zijn verscheidene formules gekend. De volgende recursieve formule werkt ook voor de vertrouwde faculteiten, het enige verschil ligt in de definitie van de grondwaarden  $!1$  en  $1!$ .

$$\begin{array}{lll} !0 = 1, & !1 = 0, & !n = (n - 1) \cdot (!(n - 1) + !(n - 2)) \\ 0! = 1, & 1! = 1, & n! = (n - 1) \cdot ((n - 1)! + (n - 2)!) \end{array}$$

Expliciet kan  $!n$  berekend worden als volgt.

$$!n = n! \cdot \sum_{k=0}^n \frac{(-1)^k}{k!}$$

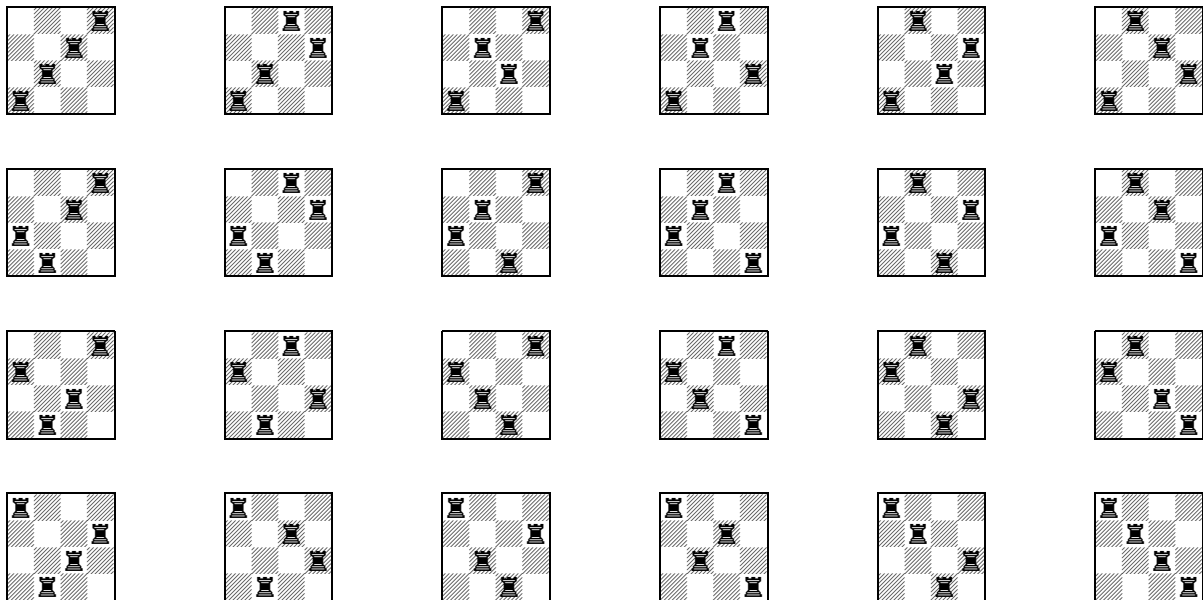
Er is echter een nog veel opmerkelijker verband tussen derangementen en permutaties:

$$\lim_{n \rightarrow \infty} \frac{n!}{!n} = e$$

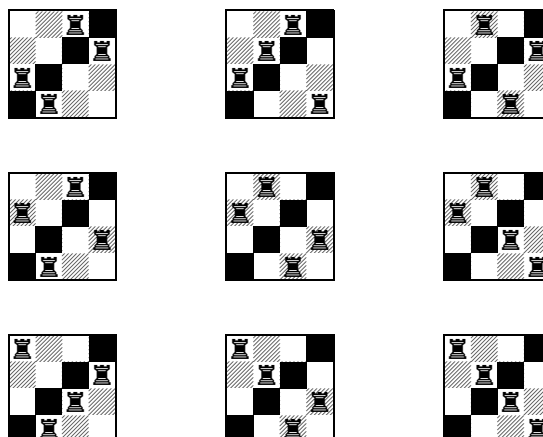
Dit impliceert dat de kans dat een willekeurige permutatie tevens een derangement is, ongeveer gelijk is aan  $\frac{1}{e}$ , hoe groter het aantal elementen, hoe nauwkeuriger. Deze limiet convergeert relatief snel.

## 230 Schaakbordcombinatoriek

Permutaties en derangementen (zie 229, blz. 192) zijn gemakkelijk te visualiseren op een schaakbord. De permutatie  $n!$  vormt juist het aantal manieren waarop  $n$  torens kunnen worden geplaatst op een  $n \times n$ -bord, waarbij geen enkele toren een andere aanvalt. De mogelijkheden vallen eenvoudig te berekenen door elke permutatie van  $\{1, 2, \dots, n\}$  te combineren met  $\{a, b, c, \dots\}$  en zo op het schaakbord te plaatsen. Dus voor  $n = 4$ :



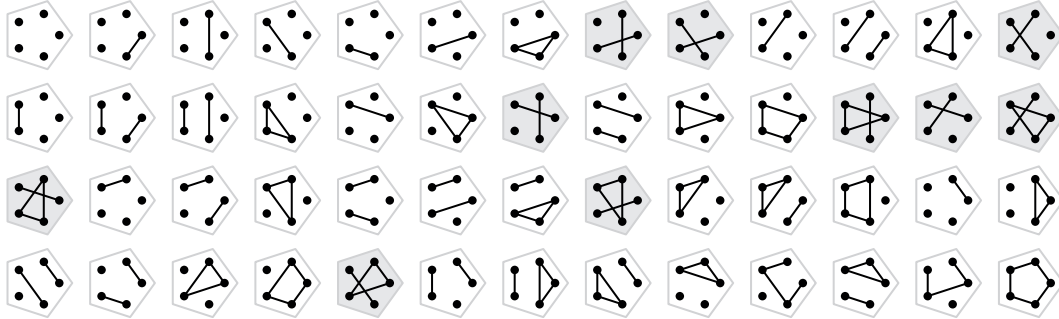
De derangementen kunnen op een soortgelijke manier worden gevisualiseerd, omdat  $!n$  het aantal mogelijke manieren vormt waarop  $n$  torens het  $n \times n$ -bord bezetten zonder dat twee torens elkaar aanvallen, met de extra beperking dat er geen torens op één van de diagonalen mogen staan. Dus voor  $n = 4$ :





## 231 Bellgetallen

Eric Bell beschreef in de jaren 30 deze Bellgetallen, gerelateerd aan o.a. de getallen van Catalan (zie 228, blz. 190). Het Bellgetal  $B_n$  geeft het totaal aantal mogelijke partities weer van een verzameling met  $n$  elementen, terwijl het Catalangetal  $C_n$  het aantal “niet-kruisende” partities uitdrukt. In de figuur hieronder wordt dit duidelijk gemaakt; de tien gekleurde partities worden niet meegerekend door  $C_n$ , wel door  $B_n$ .



1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, 27644437, 190899322 . . . (OEIS A000110)

Een recursieformule voor de Bellgetallen is deze:

$$B_0 = 1, \quad B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k$$

Een expliciete formule wordt gegeven door de formule van Dobiński:

$$B_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}$$

Ook de Bellgetallen hebben een genererende functie en een elegantere exponentiële genererende functie.

$$\sum_{n=0}^{\infty} B_n \cdot x^n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{1}{(1 - kx)k!}, \quad \sum_{n=0}^{\infty} \frac{B_n}{n!} \cdot x^n = e^{(e^x - 1)}$$

Ernesto Cesàro vond in 1885 de volgende verbazingwekkende complexe integraalrepresentatie, waarin  $\Im(z)$  het imaginaire gedeelte van  $z$  voorstelt.

$$B_n = \frac{2n!}{\pi e} \cdot \Im \left( \int_0^{\pi} e^{e^{e^{i\theta}}} \sin(n\theta) \, d\theta \right) = \frac{2n!}{\pi e} \cdot \int_0^{\pi} e^{e^{\cos(\theta)} \cos(\sin \theta)} \sin(e^{\cos(\theta)} \sin(\sin \theta)) \sin(n\theta) \, d\theta$$

Net als de Catalan- en binomiaalgetallen kunnen ook de Bellgetallen gegenereerd worden in een driehoek, die de driehoek van Bell, of ook wel de array van Aitken of de driehoek van Peirce genoemd wordt.

- Begin met een rij met 1 als enige element.
- Begin een nieuwe rij met het laatste element van de vorige rij als eerste element.
- Elk niet-eerste element in een rij is de som van het getal links en het getal linksboven.
- Herhaal stap 2 en 3 voor het vormen van nieuwe rijen (telkens één element meer dan de vorige).
- Het eerste getal in rij  $n$  is het Bellgetal  $B_n$ .

1					
1	2				
2	3	5			
5	7	10	15		
15	20	27	37	52	
⋮	⋮	⋮	⋮	⋮	⋱

Een laatste opmerkelijke eigenschap van de Bellgetallen is deze:

$$\begin{vmatrix} B_0 & B_1 & B_2 & \cdots & B_n \\ B_1 & B_2 & B_3 & \cdots & B_{n+1} \\ B_2 & B_3 & B_4 & \cdots & B_{n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ B_n & B_{n+1} & B_{n+2} & \cdots & B_{2n} \end{vmatrix} = \prod_{k=0}^n k!$$

## 232 Alternerende en zigzagpermutaties

Dit type van permutaties werd voor het eerst bestudeerd door Désiré André in de 19<sup>de</sup> eeuw. Een alternerende permutatie is een permutatie van de eerste  $n$  getallen naar de volgorde  $c_1, c_2, \dots, c_n$ , waarbij geen enkele  $c_i$  tussen zijn burens  $c_{i-1}$  en  $c_{i+1}$  ligt. Concreet houdt dit in dat de getallen afwisselend op en af moeten springen. Een bijkomende eis is nog dat  $c_1 < c_2$ ; als deze eis achterwege wordt gelaten, verkrijgen we de zogenaamde zigzagpermutaties en wordt het aantal mogelijkheden verdubbeld. Op de verzameling  $\{1, 2, 3, 4\}$  zijn er zo vijf alternerende permutaties:

$$\begin{aligned} 1 &< 3 > 2 < 4 \\ 1 &< 4 > 2 < 3 \\ 2 &< 3 > 1 < 4 \\ 2 &< 4 > 1 < 3 \\ 3 &< 4 > 1 < 2 \end{aligned}$$

Het probleem van André vraagt nu algemeen hoeveel mogelijke alternerende permutaties er zijn op een verzameling met  $n$  elementen. Deze aantallen worden genoteerd als  $A_n$  en staan bekend als de Euler-zigzaggetallen of op-neergetallen.

1, 1, 1, 2, 5, 16, 61, 272, 1385, 7936, 50521, 353792, 2702765, 22368256, 199360981 ... (OEIS A000111)

Een mooi algoritme ter berekening van  $A_n$  is deze recursieve relatie, waarbij de som loopt over elke natuurlijke  $r$  en  $s$  waarvoor  $r + s = n - 1$ .

$$a_0 = 1, \quad a_1 = 1, \quad a_n = \frac{1}{2n} \cdot \sum_{r,s} (a_r \cdot a_s) \quad \Rightarrow \quad A_n = a_n \cdot n!$$

De getallen  $A_n$  met even index (1, 1, 5, 61, 1385, 50521 ...) worden ook wel zig- of secansgetallen genoemd, die met oneven index (1, 2, 16, 272, 7936, 353792 ...) zag- of tangensgetallen. Er geldt namelijk volgend verband met de goniometrische functies.

$$\sec x = \frac{A_0}{0!} x^0 + \frac{A_2}{2!} x^2 + \frac{A_4}{4!} x^4 + \dots, \quad \tan x = \frac{A_1}{1!} x + \frac{A_3}{3!} x^3 + \frac{A_5}{5!} x^5 + \dots$$

Gecombineerd geeft dit de stelling van André, een elegante genererende exponentiële functie van  $A_n$ .

$$\sum_0^{\infty} \frac{A_n}{n!} x^n = \sec x + \tan x$$

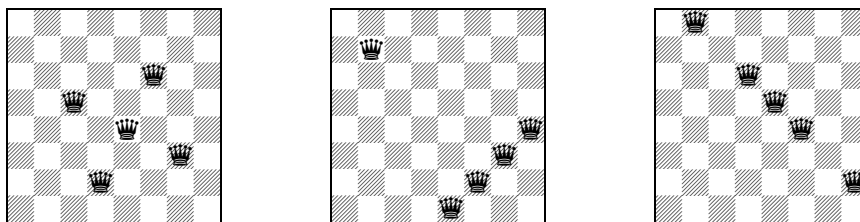
Tot slot heeft  $A_n$  nog een verbluffende andere eigenschap met betrekking tot  $\pi$ .

$$\lim_{n \rightarrow \infty} (2n + 2) \cdot \frac{A_n}{A_{n+1}} = \pi$$

## 233 Damesdominantie

HOEVEEL SCHAAKSTUKKEN (VAN DEZELFDE SOORT) HEEFT MEN MINSTENS NODIG OM TE GARANDEREN DAT ÉLK VAKJE OP HET SCHAAKBORD KAN WORDEN AANGEVALLEN? DE STUKKEN MOGEN EVENTUEEL OOK ELKAAR AANVALLEN.

Dit dominantieprobleem is het interessantst voor de dame. Ondanks vele vooruitgangen blijkt het een opmerkelijk weerbarstig probleem te zijn, dat nog steeds verre van opgelost is. Het klassieke  $8 \times 8$ -bord werd al intensief bestudeerd; zo weet men dat vijf dames genoeg zijn om het hele bord bezet te houden en Isaak en Akiva Yaglom stelden vast dat dit op 4860 verschillende manieren mogelijk is. Bijvoorbeeld:



Het minimum aantal dames nodig om een  $n \times n$ -bord te domineren wordt genoteerd als  $\gamma(Q_{n \times n})$ . De eerste waarden zijn eenvoudig na te gaan en staan in OEIS A140858. Voor  $n = 14$  zijn er al opstellingen met 8 dames bekend, maar het is nog niet bewezen of het al dan niet mogelijk is met 7 stukken. Hetzelfde probleem geldt voor  $n = 15, 16, 19, 20, 22, 23, 24 \dots$

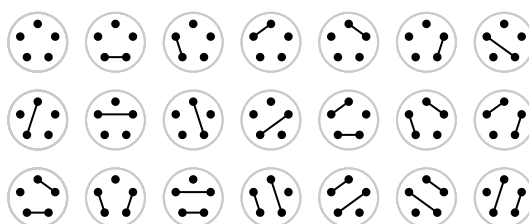
- $\gamma(Q_{1 \times 1}) = 1$
- $\gamma(Q_{2 \times 2}) = 1$
- $\gamma(Q_{3 \times 3}) = 1$
- $\gamma(Q_{4 \times 4}) = 2$
- $\gamma(Q_{5 \times 5}) = 3$
- $\gamma(Q_{6 \times 6}) = 3$
- $\gamma(Q_{7 \times 7}) = 4$
- $\gamma(Q_{8 \times 8}) = 5$
- $\gamma(Q_{9 \times 9}) = 5$
- $\gamma(Q_{10 \times 10}) = 5$
- $\gamma(Q_{11 \times 11}) = 5$
- $\gamma(Q_{12 \times 12}) = 6$
- $\gamma(Q_{13 \times 13}) = 7$

Lonnie Welch gaf een constructie die een bovengrens impliceerde, terwijl P. Spencer een ondergrens gaf:

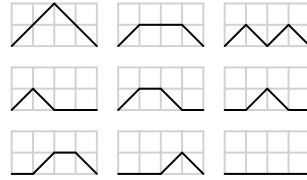
$$\frac{n-1}{2} \leq \gamma(Q_{n \times n}) \leq n - \left\lfloor \frac{n}{3} \right\rfloor$$

## 234 Motzkingetallen

De Motzkingetallen  $M_n$ , vernoemd naar Theodore Motzkin, stellen het aantal mogelijkheden voor om  $n$  punten op een cirkel te verbinden met niet-snijdende koorden. Ze duiken ook op in allerlei andere telproblemen.



1, 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188, 5798, 15511, 41835, 113634, 310572, 853467 . . . (OEIS A001006) De Motzkingetallen kunnen tevens worden gevisualiseerd als het aantal mogelijke paden op een  $n \times n$ -rooster, vertrekkend van de linkeronderhoek en eindigend in de rechteronderhoek, door enkel en alleen gebruik te maken van de richtingen  $\rightarrow$ ,  $\nearrow$  en  $\searrow$ . Omdat een dergelijk pad slechts over de onderste helft van het rooster kan lopen, staan hier de voorstellingen op een  $\frac{n}{2} \times n$ -rooster.



De Motzkingetallen kunnen als volgt recursief worden berekend.

$$M_0 = 1, \quad M_1 = 1, \quad M_{n+1} = M_n + \sum_{i=0}^{n-1} M_i \cdot M_{n-1-i} = \frac{2n+3}{n+3} \cdot M_n + \frac{3n}{n+3} \cdot M_{n-1}$$

Een genererende functie:

$$\sum_{n=0}^{\infty} M_n \cdot x^n = \frac{2}{1-x+\sqrt{1-2x-3x^2}} = \frac{1}{1-x-\frac{x^2}{1-x-\frac{x^2}{1-x-\frac{x^2}{\dots}}}}$$

## 235 Combinatoriek en $n^{\text{de}}$ -machtswortels

Vele combinatorische getallen voldoen aan een interessant patroon. Kijk bijvoorbeeld naar de Catalangetallen (zie 228, blz. 190) en bereken het aantal cijfers van  $C_{10^n}$ . Deze aantallen geven de rij hieronder en bevatten duidelijk een patroon, dat eruitziet als de decimale ontwikkeling van  $\log 4 \approx 0,6020599913$ .

1, 5, 57, 598, 6015, 60199, 602051, 6020590, 60205987, 602059978, 6020599899 . . . (OEIS A114466)

Dit kan worden teruggebracht tot de volgende limiet voor algemene  $n$ :

$$\bullet \lim_{n \rightarrow \infty} \sqrt[n]{C_n} = 4$$

Een soortgelijk resultaat gaat op voor de Motzkingetallen (zie 234, blz. 196):

$$\bullet \lim_{n \rightarrow \infty} \sqrt[n]{M_n} = 3$$

De Delannoygetallen en Schrödergetallen (zie ??, blz. ??) hebben eveneens zo'n limietwaarde.

$$\bullet \lim_{n \rightarrow \infty} \sqrt[n]{D_n} = 3 + 2\sqrt{2}$$

$$\bullet \lim_{n \rightarrow \infty} \sqrt[n]{S_n} = 3 + 2\sqrt{2}$$

De Mersennegetallen (zie ??, blz. ??) zijn niet zo zeer combinatorisch, maar ook hier geldt deze eigenschap.

$$\bullet \lim_{n \rightarrow \infty} \sqrt[n]{M_n} = 2$$

Ook bij de Fibonacci- en Lucasgetallen (zie 91, blz. 65) duikt zo'n limiet op, gekoppeld aan de gulden snede.

$$\bullet \lim_{n \rightarrow \infty} \sqrt[n]{F_n} = \varphi$$

$$\bullet \lim_{n \rightarrow \infty} \sqrt[n]{L_n} = \varphi$$

Zelfs bij de harmonische getallen (zie 94, blz. 71) komt deze eigenschap voor en blijkt de limiet gerelateerd aan Eulers constante (zie 95, blz. 71). Noteer  $T_n$  voor de teller van het  $n^{\text{de}}$  harmonische getal en  $N_n$  voor zijn noemer.

$$\bullet \lim_{n \rightarrow \infty} \sqrt[n]{T_n} = e$$

$$\bullet \lim_{n \rightarrow \infty} \sqrt[n]{N_n} = e$$

## 236 Langfords blokken

Nadat zijn zoontje een blokkentoren gebouwd had, merkte Dudley Langford iets speciaals op aan de configuratie. Van elk kleur waren er twee blokjes, en ze waren zodanig gestapeld dat er tussen het rode koppel juist één blok zat, tussen het blauwe koppel twee en tussen het gele koppel drie.



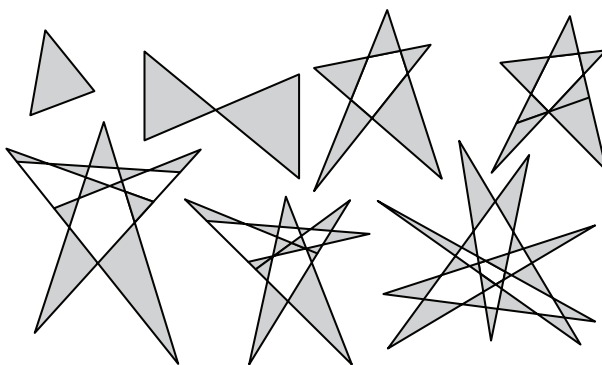
Dit inspireerde Langford tot de Langfordsequenties. Dit zijn permutaties van  $2n$  getallen  $(1, 1, 2, 2, \dots, n, n)$  zodanig dat er één getal zit tussen de 1'en, twee getallen tussen de 2'en, enzovoort. De sequentie voor het geval  $n = 3$  bijvoorbeeld is 231213 (zoals de blokjes hierboven), en deze oplossing is op omkering na uniek.

Langfordsequenties bestaan alleen voor  $n$ -waarden congruent met 0 of 3 modulo 4. Wanneer we omgekeerde sequenties niet apart meetellen, staat het aantal oplossingen voor  $n$  in OEIS A014552; er is nog geen algemene formule voor bekend. De sequenties zelf staan in OEIS A050998.

0, 0, 1, 1, 0, 0, 26, 150, 0, 0, 17792, 108144, 0, 0, 39809640, 326721800, 0, 0, 256814891280 ... (OEIS A014552)

## 237 Driehoeken van Kobon

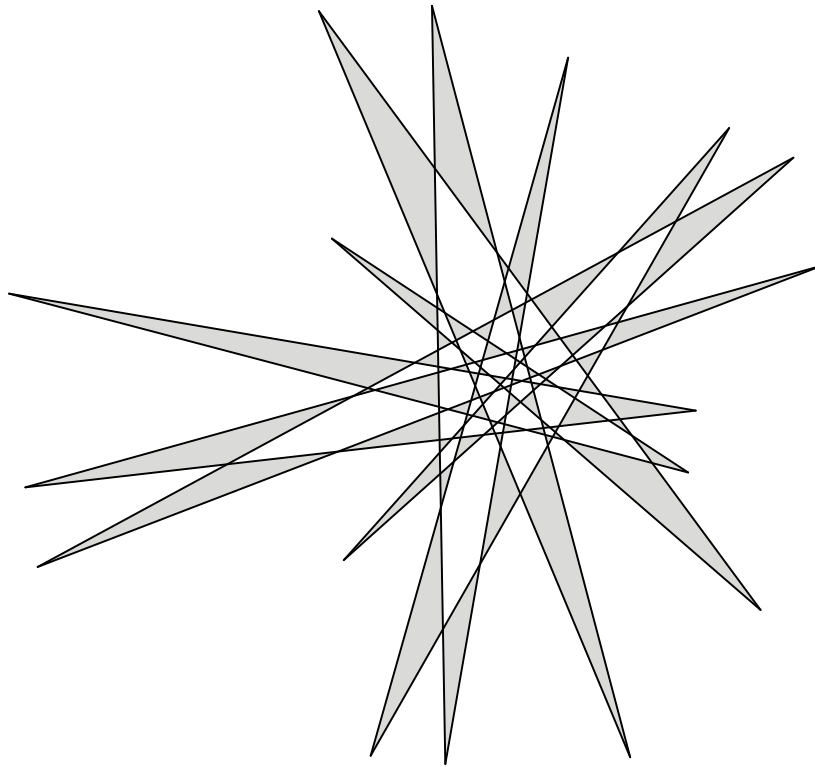
Bekend gemaakt door Martin Gardner in 1983, vraagt het probleem van Kobon Fujimura het grootst mogelijke aantal niet-overlappende driehoeken die worden begrensd door  $n$  rechte lijnsegmenten. Voor kleine waarden van  $n$  is dit niet moeilijk op te lossen, maar voor grotere waarden is er nog geen algemene oplossing bekend.



De eerste oplossingen (vanaf  $n = 3$ ) zijn: 1, 2, 5, 7, 11, 15, 21 ... (OEIS A006066).

Volgende waarden zijn nog onbekend! Voor  $n = 10$  is het maximale aantal driehoeken 25 of 26, maar welken juist is nog ongeweten. Hetzelfde voor  $n = 11$ , daar is 32 of 33 mogelijk. De grootste  $n$ -waarde waarvoor de oplossing gekend is, is  $n = 17$ ; daarvoor werd een configuratie met 85 driehoeken gevonden, wat overeenkomt met een bovengrens gegeven door Saburo Tamura. Algemeen wordt die bovengrens gegeven door:

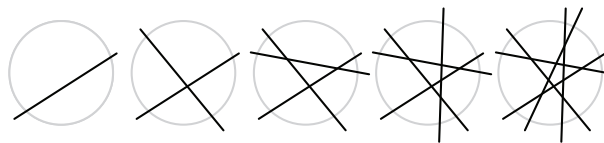
$$\left\lfloor \frac{n \cdot (n + 2)}{3} \right\rfloor$$



## 238 Het pannenkoekprobleem

Het pannenkoekprobleem (of het probleem van de luie traiteur) vraagt hoeveel stukken er maximaal kunnen worden gesneden uit een pannenkoek of pizza, met een gegeven aantal rechte lijnen. Deze stukken hoeven niet dezelfde grootte of vorm te hebben. De oplossing wordt gemakkelijk gevonden: met  $n$  rechte lijnen kunnen er  $\frac{1}{2}(n^2 + n + 2)$  stukken uit een cirkel worden afgebakend; juist de driehoeksgetallen plus één.

1, 2, 4, 7, 11, 16, 22, 29, 37, 46, 56, 67, 79, 92, 106, 121, 137, 154, 172, 191, 211, 232, 254 . . . (OEIS A000124)

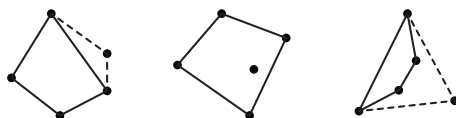


Deze oplossing volgt direct uit de recursieve betekenis van de sneden; als het aantal stukken met  $n$  sneden genoteerd wordt als  $f(n)$ , voegt de laatste snede  $n$  stukken toe en geldt dus dat  $f(n) = f(n - 1) + n$ . De eerste snede snijdt de pannenkoek in twee stukken, dus volgt daaruit dat  $f(n) = 1 + (1 + 2 + \dots + n)$ , het  $n^{\text{de}}$  driehoeksgetal vermeerderd met één.

## 239 Happy ending problem

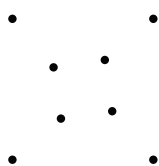
Het probleem van de goede afloop (of het happy ending problem) komt aan z'n ludieke naam via Paul Erdős, doordat de twee onderzoekers die het probleem voor het eerst uitwerkten, Ester Klein en George Szekeres, verloofd werden en later trouwden. Hun resultaten waren een van de eerste stappen in de ontwikkeling van Ramseytheorie (zie ??, blz. ??). Het originele probleem werd door Klein en Szekeres opgelost en begint vrij simpel, maar veralgemeningen bleken zeer moeilijk. In feite staat het algemene probleem nog steeds open.

Het basisgeval stelt dat een algemene configuratie van vijf punten, steeds vier punten bevat die de hoekpunten zijn van een convexe vierhoek. Met “algemeen” wordt bedoeld dat geen drie punten op eenzelfde rechte liggen.



Erdős en Szekeres bewezen een sterker resultaat, namelijk dat voor elke natuurlijke  $N \geq 3$ , een voldoende grote, maar eindige verzameling punten in het vlak in algemene positie een convexe  $N$ -hoek bevat. Het minimale aantal punten  $M$  waarvoor steeds zo'n veelhoek gevonden kan worden, is echter lastig te vinden: voor  $N > 6$  zijn de waarden nog onbekend.

Voor een vijfhoek zijn acht punten onvoldoende, zoals onderstaand diagram bewijst; Endre Makai bewees dat negen punten wél voldoen. De bekende minimale aantallen met zeker een convexe driehoek, vierhoek, vijfhoek en zeshoek zijn respectievelijk 3, 5, 9 en 17.



Naast hun stelling toonden Szekeres en Erdős enkele grenzen voor  $M$  aan:

$$2^{n-2} + 1 \leq M \leq \binom{2n-4}{n-2} + 1$$

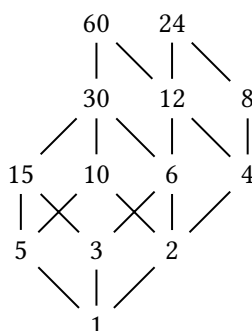
De bovengrens is sindsdien verbeterd tot  $\binom{2n-5}{n-2} + 2$ . De twee onderzoekers menen echter dat hun ondergrens in feite de exacte waarde is, een vermoeden dat gestaafd wordt door de ondertussen gekende waarde voor  $n = 6$ , die pas veel later (in 2006) gevonden werd door Szekeres met behulp van computers. Kort voor zijn overlijden heeft Erdős nog een prijs van \$500 gezet op een bewijs van dit nog steeds open probleem.

## 240 Stellingen van Dilworth en Mirsky

Een partiële orderrelatie  $\preceq$  voldoet aan drie voorwaarden, voor alle  $x, y$  en  $z$ :

- **Reflexiviteit:**  $x \preceq x$ .
- **Antisymmetrie:**  $x \neq y$  en  $x \preceq y$  impliceren  $y \not\preceq x$ .
- **Transitiviteit:**  $x \preceq y$  en  $y \preceq z$  impliceren  $x \preceq z$ .

Verzameling uitgerust met een partiële orderrelatie heten *posets* (*partially ordered sets*). Voorbeelden van posets zijn een aantal natuurlijke getallen geordend op deelbaarheid, een machtsverzameling geordend op inclusie, of de toppenverzameling van een gerichte acyclische graaf geordend op bereikbaarheid. Een visualisatie van zo'n poset gebeurt vaak via een Hassediagram zoals die hieronder, die de deelbaarheidsrelatie weergeeft tussen de delers van 60 en 24.



In een poset kunnen er koppels optreden die niet te vergelijken zijn, zoals 5 en 12 in het voorbeeld hierboven. Een verzameling van zulke onderling onvergelijkbare elementen, heet een antiketen (zoals  $\{6, 8, 10, 15\}$ ), terwijl een keten een verzameling elementen is die wel onderling te vergelijken zijn (zoals  $\{1, 2, 12, 60\}$ ).

De stelling van Dilworth, vernoemd naar Robert Dilworth (1950), stelt nu dat de maximale lengte van een antiketen gelijk is aan het minimale aantal ketens, nodig om alle elementen te bedekken. Deze gemeenschappelijke waarde heet de breedte van de partiële orderrelatie.

Het is daarenboven waar dat de maximale lengte van een keten gelijk is aan het minimale aantal antiketens die de hele verzameling bedekt. Deze waarde wordt de hoogte van de relatie genoemd. Dit gerelateerde resultaat staat bekend als de stelling van Mirsky, naar Leon Mirsky (1971).

De stellingen kunnen als volgt gereformuleerd worden: een poset met  $ab + 1$  elementen bevat zeker een keten van lengte  $a + 1$  of een antiketen van lengte  $b + 1$ .

## 241 Stelling van Van der Waerden

Voor elke gegeven gehele getallen  $k$  en  $r$  bestaat er een welbepaald getal  $N$  zodanig dat wanneer de getallen  $\{1, 2, \dots, N\}$  elk gekleurd worden in een van  $r$  verschillende kleuren, het bestaan van  $k$  getallen die een rekenkundige rij vormen en dezelfde kleur hebben, verzekerd is. De kleinste  $N$  die hieraan voldoet heet het Van der Waerdengetal  $W(r, k)$ .

Voor  $k = 3$  en  $r = 2$  is  $N$  zeker groter dan 8, want er bestaat een 2-kleuring die geen drie getallen bevat die dezelfde kleur hebben en een rekenkundige rij vormen. Het blijkt dat 9 de kleinste waarde is waarvoor er wél steeds een rekenkundige rij gevonden kan worden, dus  $W(2, 3) = 9$ .

1	2	3	4	5	6	7	8
---	---	---	---	---	---	---	---

Nog maar weinig Van der Waerdengetallen zijn gekend. Er is wel een bovengrens bekend, gegeven door Timothy Gowers, die echter zo immens is dat er prijzen zijn gezet op terugbrengingen ervan naar een “redelijke” functie.

$$W(r, k) \leq 2^{2^{r \cdot 2^{2^k+9}}}$$

Dit resultaat uit de Ramseytheorie (zie ??, blz. ??) wordt vernoemd naar Nederlands wiskundige Bartel van der Waerden, die in 1927 het vermoeden van Baudet ermee bewees. Dit vermoeden stelde dat wanneer de unie van een eindig aantal verzamelingen  $C_1 \cup C_2 \cup \dots \cup C_n$  gelijk is aan  $\mathbb{N}$ , er dan een  $C_i$  is die willekeurig lange rekenkundige voortzettingen bevat.

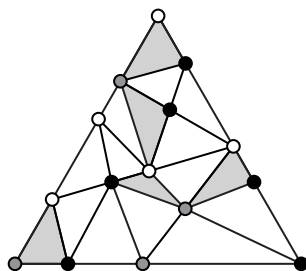
## 242 Sperners lemma

Emanuel Sperner bewees deze combinatorische versie van Brouwers dekpuntstelling (zie 224, blz. 184) in 1928. Het lemma vindt concrete applicaties in berekeningen van dekpunten of wortels van functies.

In één dimensie is het lemma een discrete variant van de tussenwaardstelling en betekent deze in essentie dat een discrete functie die enkel de waarden 0 en 1 aanneemt, een oneven aantal keren moet wisselen.

De tweedimensionale variant is het bekendst. Verdeel een driehoek in kleinere driehoeken zoals op de figuur, en kleur dan de drie hoekpunten van de oorspronkelijke driehoek in drie verschillende kleuren in. De punten op de zijden mogen enkel gekleurd worden in de kleuren van de aanliggende hoekpunten, niet in de kleur van het hoekpunt ertegenover. Op de kleuren van de punten binnenin de driehoek zijn er geen beperkingen.





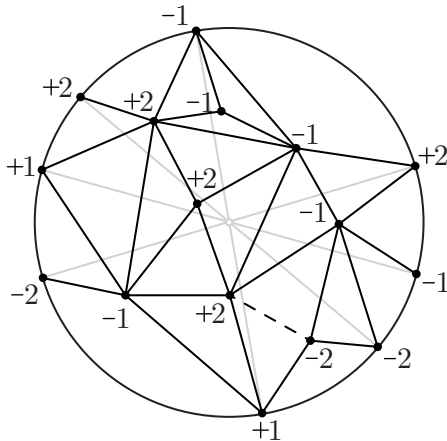
Sperners lemma beweert dat in een dergelijke configuratie, er zeker één driehoekje gevonden worden met de drie verschillende kleuren in zijn hoekpunten. Meer bepaald bestaat er steeds een oneven aantal van zo'n driehoeken.

Ook in hogere dimensies blijft het lemma bruikbaar. Beschouw een triangulatie van een  $n$ -simplex in kleinere  $n$ -simplices, en kleur de hoekpunten in met  $n+1$  kleuren, analoge regels volgend als in de tweedimensionale versie. Ook hier zal er steeds een oneven aantal simplices te vinden zijn, waarvan de hoekpunten alle verschillende kleuren dragen.

## 243 Tuckers lemma

Naar Albert Tucker vernoemd is deze combinatorische versie van de stelling van Borsuk-Ulam (zie ??, blz. ??).

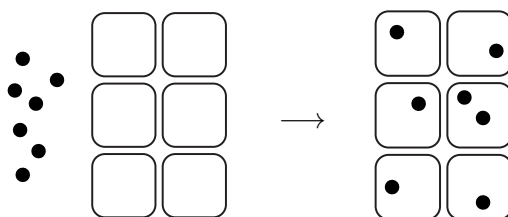
Stel een triangulatie op van de gesloten  $n$ -dimensionale bal  $B^n$ , zodanig dat elk punt op de  $(n-1)$ -sfeer ook een tegenoverstaand punt heeft. Label vervolgens de gekozen punten met de getallen  $\{1, -1, 2, -2 \dots n, -n\}$ , waarbij tegenoverstaande punten op de sfeer een tegengestelde labeling krijgen. De punten binnenin de bal ondervinden geen beperking.



Het lemma van Tucker stelt nu dat gelijk hoe de triangulatie ook genummerd werd volgens deze regels, er altijd een lijnstuk te vinden is met dezelfde getallen aan z'n uiteinden, maar met tegengesteld teken.

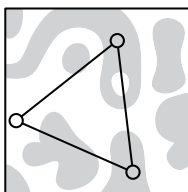
## 244 Ladenprincipe

Een van de meest elementaire en intuïtieve telprincipes is het duivenhokprincipe of ladenprincipe van Johann Dirichlet (1834). Deze stelt eenvoudigweg dat wanneer er meer dan  $k$  duiven onderverdeeld moeten worden in  $k$  hokken, er dan zeker een hok zal zijn met meer dan één duif erin.



Een algemenere verwoording: als  $n$  objecten verdeeld worden in  $k$  dozen, is er zeker een doos met minstens  $\lceil \frac{n}{k} \rceil$  en een doos met maximaal  $\lfloor \frac{n}{k} \rfloor$  objecten.

Alhoewel elementair is dit principe een niet te onderschatten hulpmiddel in allerlei telproblemen. Een niet zo triviaal voorbeeld is dit: wanneer er  $n$  mensen handen schudden (niet per se met iedereen), zijn er gegarandeerd twee mensen die met evenveel anderen handen geschud hebben.



Het ladenprincipe impliceert eveneens dat het vlak niet zodanig gekleurd kan worden in twee kleuren dat geen twee punten op eenheidslengte van elkaar dezelfde kleur hebben: op elke kleuring kan een driehoek getekend worden, met zijden van lengte 1, en dan hebben zeker twee van zijn hoekpunten dezelfde kleur.

Steunend op het duivenhokprincipe bewees Frank Ramsey in 1930 een resultaat dat de basis legde voor wat later Ramseytheorie zou heten (zie ??, blz. ??).

## 245 Getal van Graham

Het getal van Graham is een onvatbaar groot getal, dat een bovengrens aanduidt voor een probleem uit de Ramseytheorie en wordt vernoemd naar Ronald Graham. Martin Gardner beschreef het in 1977 in zijn column in de *Scientific American* als volgt, waarna het in 1980 officieel in het Guinness Book of World Records opgenomen werd.

IN AN UNPUBLISHED PROOF, GRAHAM HAS RECENTLY ESTABLISHED... A BOUND SO VAST THAT IT HOLDS  
THE RECORD FOR THE LARGEST NUMBER EVER USED IN A SERIOUS MATHEMATICAL PROOF.

Het getal vindt zijn oorsprong in deze context. Beschouw een  $n$ -dimensionale hyperkubus, en verbind elk paar hoekpunten om een complete graaf met  $2^n$  toppen te verkrijgen. Kleur elk van de bogen rood of blauw in. Wat is dan de kleinste waarde van  $n$  waarin elke kleuring gegarandeerd een complete subgraaf bevat met vier toppen, corresponderend met coplanaire hoekpunten in de kubus, en slechts één kleur?

Ronald Graham en Bruce Rothschild toonden in 1971 dat het probleem een oplossing heeft, met een bescheiden ondergrens van 6 en een gigantische bovengrens, die heel wat ingewikkelder te beschrijven is. In feite is dit getal niet te noteren met onze gebruikelijke decimale notatie, zelfs niet met Power Towers (zie 100, blz. 75). Het lukt wel met herhaaldelijke pijlomhoogoperaties van Knuth (zie 305, blz. 298): noteer  $f(n)$  voor  $2 \uparrow^n 3$ , dan is de originele bovengrens van Graham en Rothschild gegeven door  $f^7(12)$ , oftewel  $f(f(f(f(f(f(f(12)))))))$ . De ondergrens werd sindsdien verbeterd tot 11 door Geoff Exoo in 2003, en 13 door Jerome Barkley in 2008. De best gekende bovengrens blijft nog steeds deze van Graham.

Het getal dat echter bekendstaat als ‘‘Grahams getal’’ is nog veel en veel groter. In overleg met Gardner definiëerde Graham een eenvoudiger uit te leggen bovengrens, die nog groter was de oorspronkelijke, en dit was het getal dat Gardner beschreef in zijn column. Noteer  $g(n)$  voor  $3 \uparrow^n 3$ . Het aldus gekende, monsterlijke getal van Graham is dan gelijk aan  $G = g^{64}(4)$ , of voluit geschreven:

$$G = \left. \begin{array}{c} 3 \uparrow \uparrow \dots \uparrow 3 \\ \underbrace{\hspace{10em}}_{3 \uparrow \uparrow \dots \uparrow 3} \\ \vdots \\ \underbrace{\hspace{10em}}_{3 \uparrow \uparrow \dots \uparrow 3} \\ \underbrace{\hspace{10em}}_{3 \uparrow \uparrow \uparrow 3} \end{array} \right\} 64 \text{ lagen}$$

Uitgedrukt met de pijlenketens van Conway (zie 317, blz. 308) ligt de waarde van  $G$  tussen  $3 \rightarrow 3 \rightarrow 64 \rightarrow 2$  en  $3 \rightarrow 3 \rightarrow 64 \rightarrow 2$ . Decimaal uitgeschreven zijn de laatste cijfers ervan . . . 2464195387.

### 246 Driehoek van Pascal

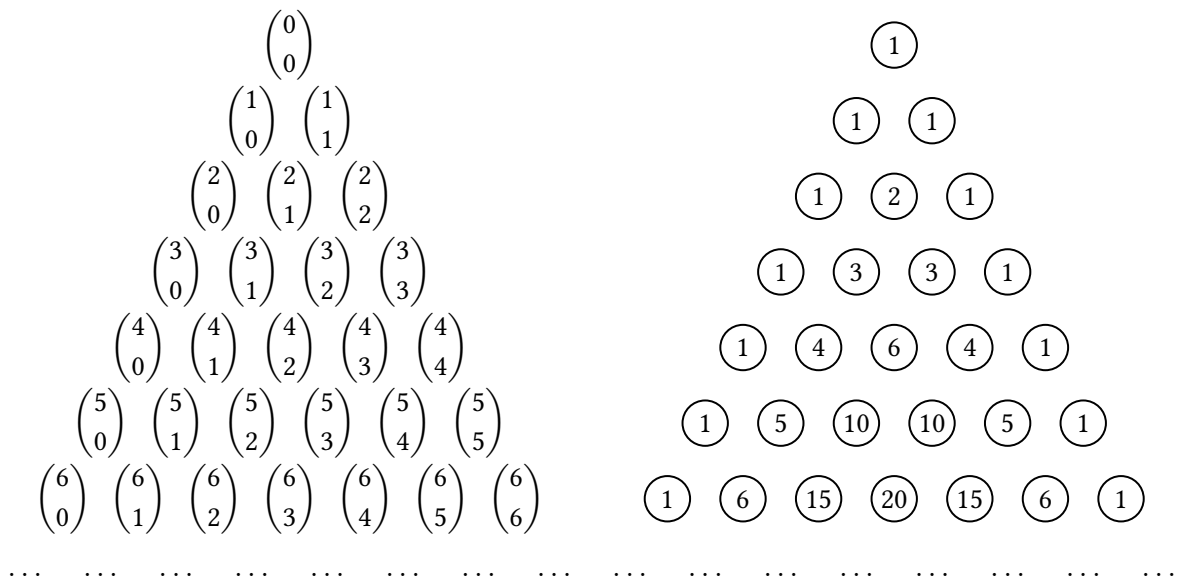
Pascals driehoek is ongetwijfeld één van de meest intrigerende wiskundige entiteiten, die ondanks zijn eenvoud barst van de verrassende patronen. De driehoek bevat de binomiaalgetallen, als  $\binom{n}{k}$  genoteerd, die het aantal mogelijke combinaties tellen met lengte  $k$  te kiezen uit  $n$  elementen (zonder herhaling en zonder vaste volgorde). Equivalent tellen deze binomiaalgetallen het aantal deelverzamelingen met  $k$  elementen uit een verzameling met  $n$  elementen. Er bestaat een welbekende, eenvoudige gesloten formule voor:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n - k)!}$$

Een eerste belangrijke eigenschap is de formule van Stifel-Pascal:

$$\binom{n}{k} = \binom{n - 1}{k} + \binom{n - 1}{k - 1}$$

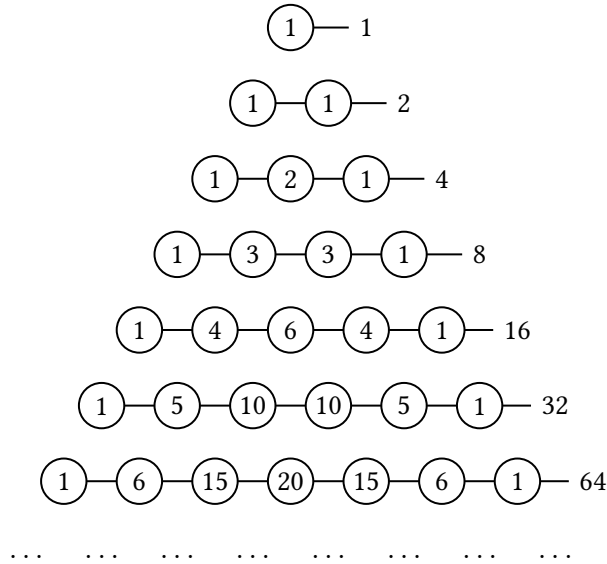
Gerangschikt met  $n$  als rijnummer en  $k$  als positie in de rij, voor alle natuurlijke getallen  $n$  en  $k$  zodat  $k \leq n$ , verkrijgen we de driehoek van Pascal. De opbouw gaat zeer eenvoudig via de eigenschap van Stifel-Pascal, die ervoor zorgt dat elk element gelijk is aan de som van de twee elementen erboven.



De  $n^{\text{de}}$  rij uit Pascals driehoek bestaat juist uit de coëfficiënten van de ontwikkeling  $(x + y)^n$ , wat volgt uit het binomium van Newton (zie ??, blz. ??). De vierde rij bijvoorbeeld correspondeert met deze ontwikkeling:

$$(x + y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

Uit het binomium van Newton, toegepast op  $(1 + 1)^n$ , volgt ook dat de elementen in rij  $n$  optellen tot  $2^n$ .



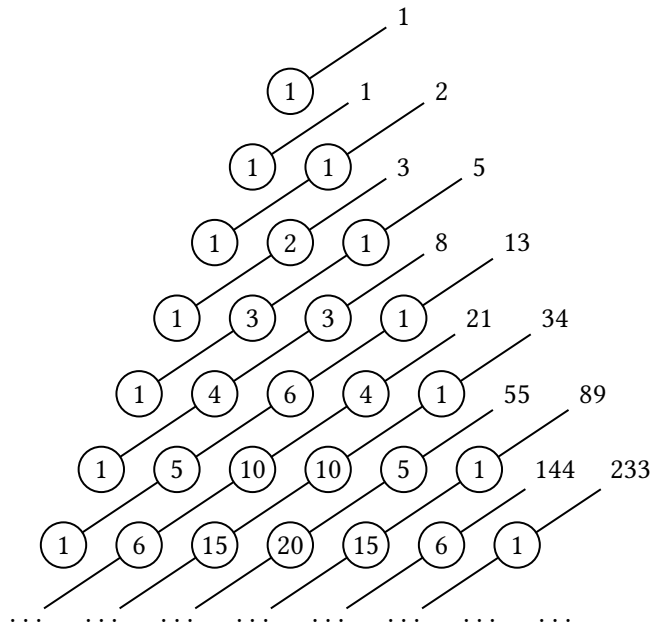
Nog een gevolg van Newtons binomium is dat de waarde van rij  $n$ , beschouwd als decimale cijfers en met overdracht als het getal meerdere cijfers bevat, gelijk is aan  $11^n$ . In de vijfde rij bijvoorbeeld, wordt  $\langle 1, 5, 10, 10, 5, 1 \rangle$  na overdracht  $161.051 = 11^5$ . Algemeener werkt dit ook als de cijfers beschouwd worden over grondtal  $d$  met  $(d + 1)^n$  als resultaat.

De som van de kwadraten van alle elementen uit rij  $n$  is net gelijk aan het middelste element van rij  $2n$ :

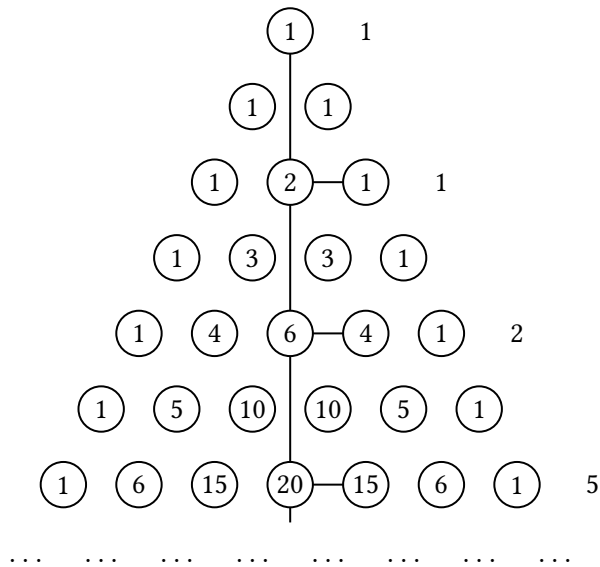
$$\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$$

De buitenste diagonalen bevatten uitsluitend het getal 1, de tweede diagonalen de natuurlijke getallen en de derde de driehoeksgetallen. Door de elementen in de derde diagonalen twee aan twee samen te tellen, kunnen ook de kwadraatgetallen gevonden worden.

In de “scheve diagonalen” treden verrassend genoeg de Fibonaccigetallen op:



De Catalangetallen (zie 228, blz. 190) kunnen in de driehoek van Pascal afgelezen worden uit de verschillen van de elementen in de middelste kolom met een van hun burenen.

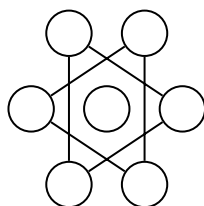


Er zitten nog een heleboel andere stellingen verborgen. Zo ontdekte Henry Gould in 1972 de “davidsterstelling”; hieronder staat een schematische weergave over de onderlinge ligging in de driehoek.

$$\binom{n-1}{k-1} \cdot \binom{n}{k+1} \cdot \binom{n+1}{k} = \binom{n-1}{k} \cdot \binom{n}{k-1} \cdot \binom{n+1}{k+1}$$

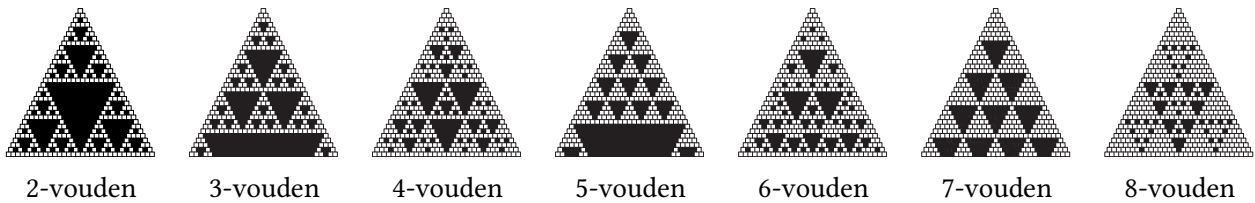
Bovendien geldt:

$$\text{ggd}\left(\binom{n-1}{k-1}, \binom{n}{k+1}, \binom{n+1}{k}\right) = \text{ggd}\left(\binom{n-1}{k}, \binom{n}{k-1}, \binom{n+1}{k+1}\right)$$

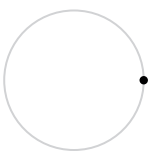
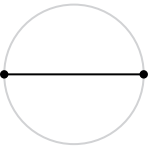
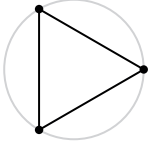
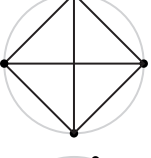
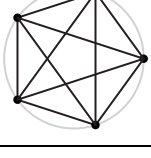


De getalwaarde van een punt op de Pascaldriehoek is het aantal mogelijke paden dat eruit vertrekt, telkens een van de twee punten erboven aandoet en uiteindelijk toekomt aan de top van de driehoek.

Kleur de oneven elementen zwart en de even elementen wit. Het resultaat is de bekende driehoek van Sierpiński (201, blz. 160). Er treden interessante patronen op wanneer de veelvouden van andere getallen gekleurd worden:



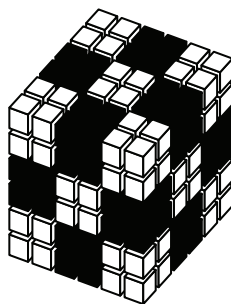
Een mooie meetkundige interpretatie is de volgende. Omdat een combinatie  $\binom{n}{k}$  correspondeert met een  $k$ -hoek vastgelegd door  $k$  punten van een  $n$ -hoek, kunnen we een tabel opstellen van  $n$ -hoeken en diens meetkundige componenten, die dan overeenkomt met de driehoek van Pascal, op de kolom 1'tjes na.

	punten	lijnstukken	driehoeken	vierhoeken	vijfhoeken
	1				
	2	1			
	3	3	1		
	4	6	4	1	
	5	10	10	5	1

De driehoek wordt vernoemd naar Blaise Pascal, hoewel hij al eeuwen eerder bekend was bij o.a. Indische, Griekse, Perzische, Chinese, Duitse en Italiaanse wiskundigen. Daardoor staat ze in andere landen bekend als de driehoek van Khayyam, Yang Hui of Tartaglia. Pascal verzamelde allerlei gegevens erover in zijn *Traité du triangle arithmétique* dat postuum gepubliceerd werd in 1653.

## 247 Pakkingsstellingen van de Bruijn

Nicolaas de Bruijn bewees in 1969 een aantal stellingen geïnspireerd op het inpakken van blokken in een groter blok. De Bruijn zag hoe zijn zoontje van zeven jaar niet in staat bleek een  $6 \times 6 \times 6$ -kubus te vullen met blokken van grootte  $1 \times 2 \times 4$ , en realiseerde zich via dat dit effectief onmogelijk is. Verdeel namelijk de kubus in  $27 \times 2 \times 2 \times 2$ -kubusjes en kleur deze in een driedimensionaal schaakbordpatroon:



Nu zijn er acht witgekleurde cellen meer dan zwartgekleurde. Echter, bij het vullen van deze kubus bedekt elk  $1 \times 2 \times 4$ -blok juist vier witte en juist vier zwarte cellen, zodat er hoogstens 26 zulke blokken in passen.

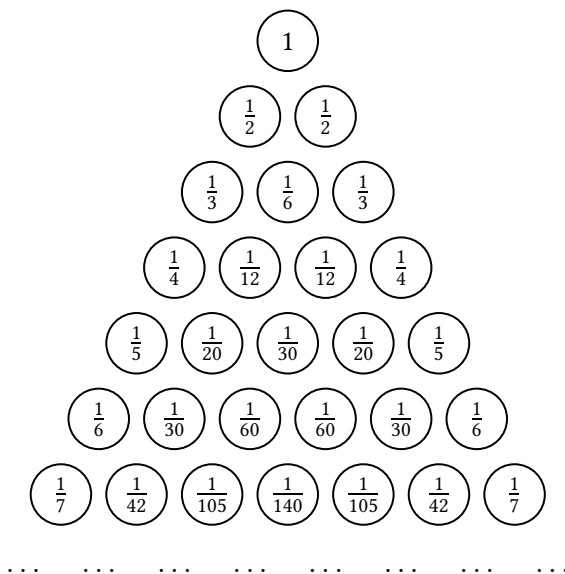
De Bruijn gaf enkele algemenere inpakstellingen. Merk eerst en vooral op dat het zeer eenvoudig is een *veelvoud* van een blok te vullen, d.i. een blok waarvan de afmetingen allen een bepaald veelvoud zijn van de afmetingen van het kleine blok. In zo'n triviale pakking hebben alle blokken dezelfde oriëntatie. Niet alleen veelvouden kunnen worden gevuld; zo passen vijf  $1 \times 2 \times 3$ -blokken bijvoorbeeld ook in een  $1 \times 5 \times 6$ -blok. Wat de Bruijn echter aantoonde, was dat als een groot blok met kopieën van een klein blok opgevuld kan worden, dat dan voor elke zijdelengte van het kleine blok minstens één van de zijdelengtes van het grote blok er een veelvoud van is.

Een tweede stelling gaat over harmonische blokken, waarin elke zijdelengte een veelvoud is van de vorige (bijv.  $1 \times 3 \times 12$ ). Volgens de Bruijn zijn de enige blokken die zo'n harmonisch blok kan opvullen, veelvouden ervan. Bovendien kan elk niet-harmonisch blok wél een blok vullen dat geen veelvoud is.

De stellingen van de Bruijn gaan op in een willekeurig aantal dimensies.

## 248 Harmonische driehoek van Leibniz

Gerelateerd aan de driehoek van Pascal (zie 246, blz. 204) is deze harmonische driehoek van Leibniz, een rangschikking van breuken waarbij de buitenste diagonalen de inversen van de rijnummers bevatten en elke breuk verkregen wordt als de som van de twee breuken eronder.



De driehoek bevat uitsluitend rationale getallen waarvan de vereenvoudigde vorm een stambreuk is, d.i. een breuk met teller 1. De noemers in de  $n^{\text{de}}$  rij sommeren juist tot  $n \cdot 2^{n-1}$ . Noteer  $a_{n,k}$  voor de waarde in rij  $n$  en

kolom  $k$  (vanaf  $n = 1$  en  $k = 1$ ), dan worden de termen dus recursief gedefinieerd als:

$$a_{n,1} = \frac{1}{n}, \quad a_{n,k} = a_{n-1,k-1} - a_{n,k-1}$$

Ze kunnen ook expliciet uitgedrukt worden in een vorm die het verband met Pascals driehoek verduidelijkt. Deze formule houdt in dat de termen in elke rij verkregen worden door de initiële term te delen door de overeenkomstige term in de driehoek van Pascal.

$$a_{n,k} = \frac{1}{k \cdot \binom{n}{k}} = \frac{1}{n \cdot \binom{n-1}{k-1}}$$

Merk op dat de noemers van de tweede diagonaal de zogenaamde pronsche getallen vormen, die het product zijn van twee opeenvolgende getallen:  $2 = 1 \cdot 2$ ,  $6 = 2 \cdot 3$ ,  $12 = 3 \cdot 4$ ,  $20 = 4 \cdot 5$ ,  $30 = 5 \cdot 6$ ,  $42 = 6 \cdot 7$  etc.

De harmonische driehoek van Leibniz kan helpen bij het vinden van particuliere oplossingen voor het vermoeden van Erdős-Straus (zie 30, blz. 21).







## 249 Dobbelstenen van Efron

Bradley Efron ontdekte deze opmerkelijke verzameling intransitieve dobbelstenen. Als je weet dat dobbelsteen  $\mathcal{A}$  een hogere winstkans heeft tegenover dobbelsteen  $\mathcal{B}$ ,  $\mathcal{B}$  een hogere winstkans tegenover  $\mathcal{C}$  en  $\mathcal{C}$  tegenover  $\mathcal{D}$ , komt het toch verrassend over dat dobbelsteen  $\mathcal{D}$  het gemiddeld wint van  $\mathcal{A}$ . Vergelijk het met blad-steen-schaar: daar wint elk element tegen één van de andere elementen en verliest die tegen de andere.

Dobbelsteen $\mathcal{A}$	0	0	4	4	4	4
Dobbelsteen $\mathcal{B}$	3	3	3	3	3	3
Dobbelsteen $\mathcal{C}$	2	2	2	2	6	6
Dobbelsteen $\mathcal{D}$	1	1	1	5	5	5

Het valt eenvoudig aan te tonen dat bij deze dobbelstenen geldt:

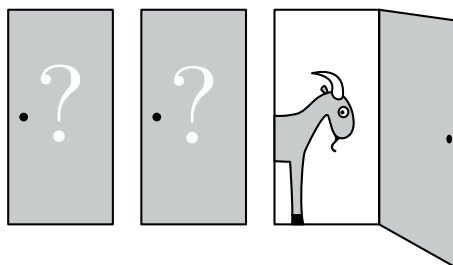
$$\mathcal{P}(\mathcal{A} \text{ wint van } \mathcal{B}) = \mathcal{P}(\mathcal{B} \text{ wint van } \mathcal{C}) = \mathcal{P}(\mathcal{C} \text{ wint van } \mathcal{D}) = \mathcal{P}(\mathcal{D} \text{ wint van } \mathcal{A}) = \frac{2}{3}$$

Intransitieve dobbelstenen bestaan niet alleen per vier. De Letse wiskundige en informaticus Rusins Freivalds toonde aan dat als er een verzameling met  $n$  dobbelstenen bestaat waarin elke de volgende verslaat met kans  $p$ , dat dan  $p$  willekeurig dicht bij (maar niet exact gelijk aan)  $\frac{3}{4}$  kan liggen voor  $n$  voldoende groot.

## 250 Driedeurenprobleem

Het driedeurenprobleem, algemener bekend als het Monty Hallprobleem, is een waarschijnlijkheidspuzzel die nogal tegen de intuïtie indruist. Het probleem gaat als volgt.

IN EEN WEDSTRIJD KRIJGT DE SPELER DE KEUZE TUSSEN DRIE DEUREN. ACHTER ÉÉN DEUR ZIT DE HOOFDPRIJS, EEN LUXE SPORTWAGEN, ACHTER DE ANDERE TWEE DEUREN ZIT ER TELKENS EEN GEIT. DE SPELER KIEST ÉÉN DEUR, WAARNA DE PRESENTATOR ÉÉN ANDERE DEUR MET EEN GEIT ERACHTER OPENT, EN DE SPELER VRAAGT OF HIJ NOG NAAR DE ANDERE DEUR WIL WISSELEN. WAT IS NU DE BESTE STRATEGIE: WISSELEN OF NIET?



Misschien verrassend is dat de speler zijn winstkans verdubbelt indien hij wél op zijn keuze terugkomt. Dit kan gemakkelijk als volgt worden ingezien: nadat de presentator een deur met een geit uit het spel heeft gehaald, blijven er nog twee deuren over (één geit en de auto). Om de prijs te winnen zónder wisselen, moet de speler al in het begin van het spel de juiste deur gekozen hebben, wat dus een kans van  $\frac{1}{3}$  geeft. Mét wisselen echter komt de speler bij de auto terecht als hij in het begin een geit koos, wat een kans  $\frac{2}{3}$  geeft. Wisselen verdubbelt

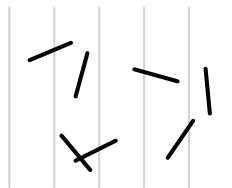
dus effectief de winstkans!

Het concept werd al wezenlijk toegepast in televisieprogramma's als het Amerikaanse *Let's make a deal* of de Nederlandse *Willem Ruisshow*.

## 251 Buffons naald

Graaf Georges-Louis Leclerc de Buffon stelde in 1733 volgend probleem:

STEL DAT WE EEN ONDERGROND HEBBEN BESTAANDE UIT EVENWIJDIGE LIJNEN, OP EEN AFSTAND  $d$  VAN ELKAAR. WAT IS DAN DE KANS DAT EEN NAALD, MET LENGTE  $\ell$ , DIE WILLEKEURIG OP DIT LIJNEN-PATROON VALT, (MINSTENS) ÉÉN VAN DEZE LIJNEN SNIJDT?



In het eenvoudige geval dat de naald korter is dan de afstand tussen de lijnen ( $\ell \leq d$ ), dan is de oplossing:

$$\mathcal{P}(\text{naald valt op een lijn} \mid \ell \leq d) = \frac{2\ell}{\pi d}$$

In het geval  $\ell > d$ , is de kans veel lastiger te berekenen.

$$\mathcal{P}(\text{naald valt op een lijn} \mid \ell > d) = \frac{2}{\pi} \cdot \left( \frac{\ell}{d} - \sqrt{\frac{\ell^2}{d^2} - 1} + \arccos \frac{d}{\ell} \right)$$

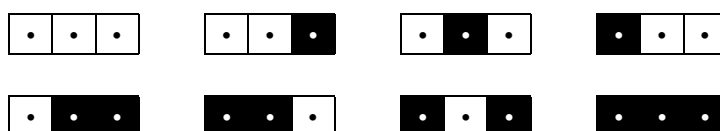
In 1901 voerde Mario Lazzarini deze Monte Carlomethode uit ter benadering van  $\pi$ , met 3408 naalden, waarbij de naaldlengte  $\frac{5}{6}$  van de afstand  $d$  was. Hij kwam de bekende rationale schatting  $\frac{355}{113}$  uit.

## 252 Driehoedenprobleem

IN EEN WEDSTRIJD MOETEN DRIE PERSONEN ELK EEN HOED OPZETTEN, EEN ZWARTE OF EEN WITTE. ELKE PERSOON KAN DE HOED VAN DE ANDERE PERSONEN ZIEN, MAAR NIET DE EIGEN HOED. NU MOET ELKE PERSOON ÓFWEL DE KLEUR VAN DE EIGEN HOED RADEN, ÓFWEL PASSEN. DE DRIE PERSONEN MOETEN TEGELIJKERTIJD ANTWOORDEN, DUS NIEMAND KAN GOKKEN OP BASIS VAN UITSPRAKEN VAN DE ANDEREN.

WANNEER NIEMAND EEN VERKEERDE GOK HEEFT UITGESPROKEN EN MINSTENS ÉÉN IEMAND CORRECT GEGOKT HEEFT (DUS GEEN DRIE PASSEN), WINT DE GROEP! WAT IS NU DE OPTIMALE STRATEGIE?

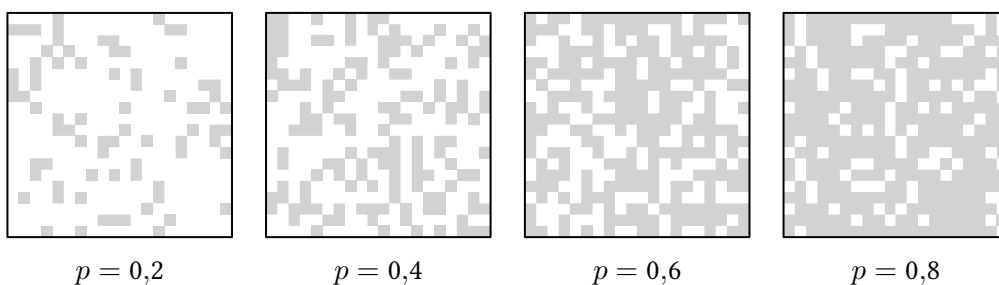
Merk op dat van alle acht mogelijke mogelijkheden er slechts twee zijn waarbij de drie hoeden dezelfde kleur hebben. Bij de andere zes gevallen zijn er telkens twee hoeden van de ene kleur en één van de andere. Er bestaat nu een schrandere strategie, die enkel faalt in de uniforme verdeling en dus 75% winstkans geeft: *wanneer je twee teamplayers dezelfde kleur van hoed dragen, gok dan voor jezelf op de andere kleur; in het andere geval pas je.*



Een algemene oplossing voor  $n$  personen blijft een open probleem. Er bestaat nochtans veel interesse in dit type problemen, door belangrijke toepassingen in communicatietechnologie: zie bijvoorbeeld “de kleur van de hoed niet kennen” als een bit verliezen in een transmissie, en “de kleur van de hoed raden” als het herstellen van zo’n bitfouten met hoge waarschijnlijkheid.

## 253 Percolatietheorie

Percolatietheorie bestudeert het ontstaan en het gedrag van verbonden clusters in willekeurige netwerken en modelleert doorsijpeling door poreus materiaal. Beschouw een vierkant rooster en vul diens cellen op met waarschijnlijkheid  $p$ . Hoeveel cellen moeten er gemiddeld bezet zijn om van één zijde van het rooster naar de tegenoverliggende zijde te kunnen lopen via aaneengrenzende cellen? Bij kleine  $p$  zijn er maar weinig cellen bezet en verwacht men dus kleine clusters, die groeien als  $p$  toeneemt. Vanaf een bepaalde kritieke waarde, de percolatiedrempel, wordt de gemiddelde cluster groot genoeg om tegenoverliggende zijden te verbinden. Een voorbeeld met enkele  $p$ -waarden:

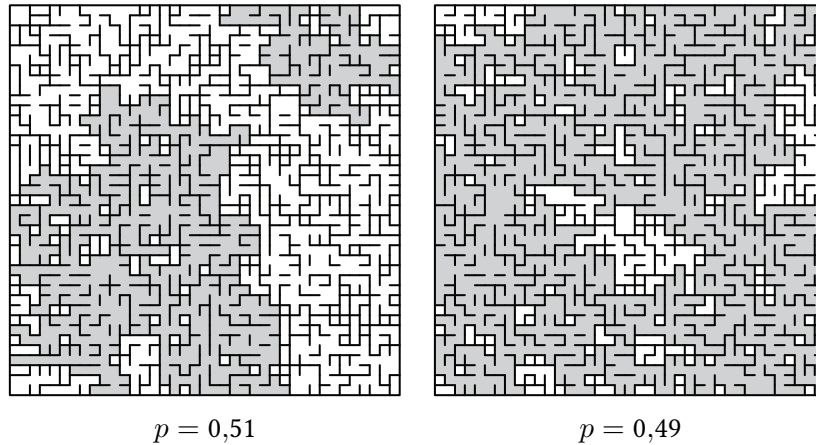


Eigenlijk is het eenvoudiger werken met oneindig grote roosters. In dit geval wordt de overeenkomstige vraag: hoeveel procent van de cellen moet er gemiddeld bezet zijn om een oneindige cluster te garanderen? Hierbij is de 0-1-wet van Kolmogorov toepasbaar, die stelt dat een gebeurtenis bepaald door een oneindige reeks onafhankelijke gebeurtenissen (hier het al dan niet vullen van een enkele cel), zelf kans 0 of 1 moet hebben. Deze kans  $\mathcal{P}_p$  (afhankelijk van  $p$ ) is duidelijk stijgend en voldoet aan  $\mathcal{P}_0 = 0$  en  $\mathcal{P}_1 = 1$ . Hieruit blijkt dus dat er een kritieke  $p$ -waarde bestaat, als  $p_c$  genoteerd en de percolatiedrempel genoemd, waarvoor geldt:

$$\begin{cases} \mathcal{P}_p = 0 & \text{als } p < p_c \\ \mathcal{P}_p = 1 & \text{als } p > p_c \end{cases}$$

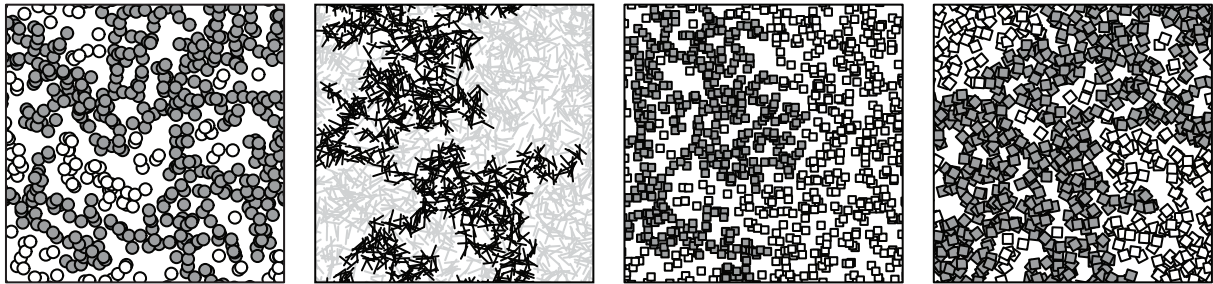
In het vorige voorbeeld werd  $p_c$  via Monte-Carloalgoritmen geschat op zo’n 0,592746, m.a.w. vanaf deze concentratie gevulde cellen komt er bijna zeker (met kans 1) een oneindige cluster aan elkaar hangende cellen voor.

Er werden al vele variaties op dit thema onderzocht, zoals het gedrag van roosters waarin niet de cellen (*site percolation*) maar de grenzen (*bond percolation*) worden bezet. In dit geval beschouwt men clusters als open paden doorheen het rooster. Bij grotere  $p$ -waarden worden de gevormde clusters kleiner, bij kleinere  $p$ -waarden ontstaat er een poreuzere, open structuur. Voor dit model heeft Harry Kesten in 1982 kunnen bewijzen dat de percolatiedrempel exact  $\frac{1}{2}$  is.

 $p = 0,51$  $p = 0,49$ 

Voor een driehoekig rooster ligt de drempel bij *site percolation* op  $\frac{1}{2}$  en bij *bond percolation* op  $2 \sin\left(\frac{\pi}{18}\right)$ .

Behalve driehoekige en vierkante roosters zijn er al tal van andere modellen onderzocht; een overzicht met gevonden percolatiedrempels is te vinden op [https://en.wikipedia.org/wiki/Percolation\\_threshold](https://en.wikipedia.org/wiki/Percolation_threshold). Enkele andere, continue voorbeelden zijn willekeurig geplaatste cirkels, stokjes of vierkanten die moeten overlappen voor clustervorming.



## 254 Chevalier de Mérés dobbelprobleem

Antoine Gombaud, Chevalier de Méré, was een Frans schrijver, ridder en gokverslaafde. Hij dobbelde veelvuldig en bedacht zijn eigen gokspel: in vier worpen met één enkele dobbelsteen wedde hij op minstens één gegooide 6. Proefondervindelijk kwam de Méré uit dat dit een rendabele gok was.

Later bedacht hij een variant, en wedde hij dat hij in 24 worpen met twee dobbelstenen minstens één dubbel 6 zou gooien. Volgens de Méré zou dit even voordelig moeten zijn: immers, voor één dobbelsteen is de kans op een zes  $\frac{1}{6}$ , dus voor vier worpen  $\frac{4}{6}$ . Analoog, een dubbel zes bij twee dobbelstenen heeft kans  $\frac{1}{36}$ , dus voor 24 worpen  $\frac{24}{36}$ . Nu is  $\frac{4}{6} = \frac{24}{36}$ , dus zouden beide spelletjes op termijn dezelfde winst moeten opbrengen.

De Méré ondervond uiteindelijk dat zijn tweede spel op lange termijn niet rendabel was. Hij vroeg hulp aan zijn vriend Blaise Pascal, die hem samen met Pierre de Fermat op een fout in zijn redenering wezen. De winstkansen moeten namelijk als volgt berekend worden:

$$\begin{aligned} \mathcal{P}(\text{bij 4 enkele worpen}) &= 1 - \left(\frac{5}{6}\right)^4 \approx 0,5177 \\ \mathcal{P}(\text{bij 24 dubbele worpen}) &= 1 - \left(\frac{35}{36}\right)^{24} \approx 0,4914 \end{aligned}$$

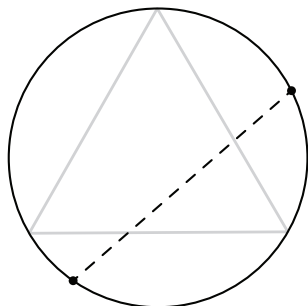
De eerste gok is dus inderdaad lucratiever dan de tweede, die op lange termijn in verlies resulteert. Toch valt op dat beide kansen niet ver van de 50% verwijderd liggen; als de Méré deze kansen effectief experimenteel bepaald heeft, moet hij hele dagen aan een stuk hebben zitten dobbelen!

Met deze analyse legden Pascal en Fermat de basis voor de moderne kansrekening.

## 255 Paradox van Bertrand

Deze klassieke paradox in de kansberekening werd geïntroduceerd door Joseph Bertrand in zijn werk *Calcul des probabilités* in 1888, ter illustratie dat wanneer het mechanisme dat de toevalsvariabele bepaalt niet goed gedefinieerd is, dan ook de kansen niet.

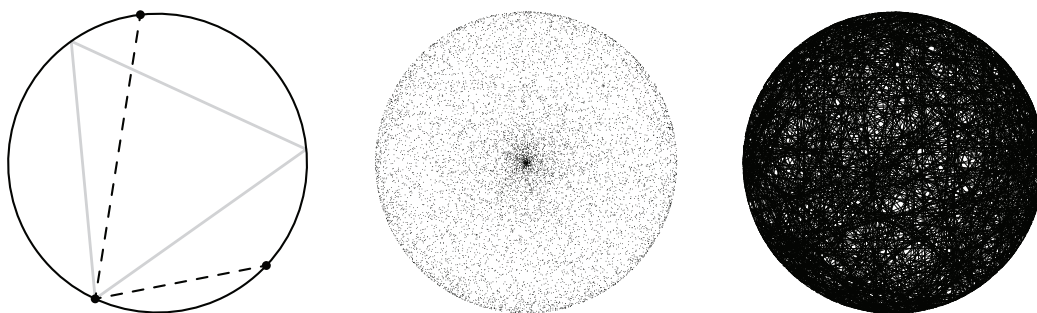
BESCHOUW EEN GELIJKZIJDIGE DRIEHOEK EN DIENS OMGESCHREVEN CIRKEL. HOE GROOT IS DE KANS DAT EEN WILLEKEURIG GEKOZEN KOORDE VAN DEZE CIRKEL, EEN GROTERE LENGTE HEEFT DAN DE ZIJDE VAN DE DRIEHOEK?



Het probleem kan op drie verschillende manieren worden opgelost, alledrie schijnbaar even correct, terwijl hun uitkomsten verschillend zijn. Na elk diagram wordt een visualisatie gegeven van de verdelingen van de koorden en hun middelpunten; elke methode geeft ook een verschillende verdeling.

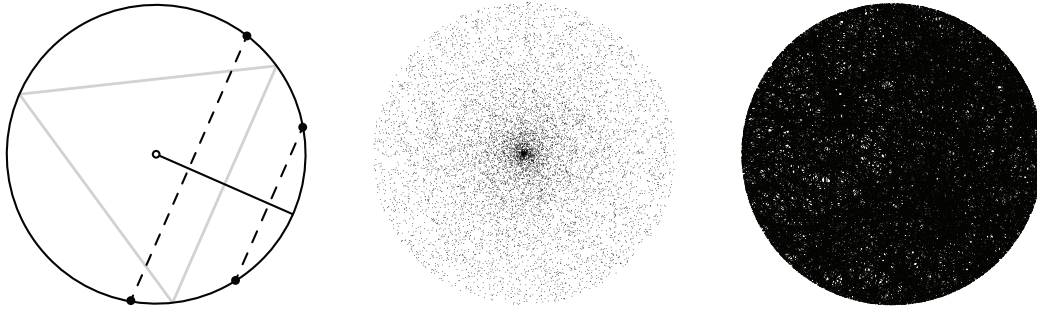
### Lukrake eindpunten.

De eerste mogelijkheid bestaat erin twee willekeurige punten op de cirkel te kiezen en de koorde die hen verbindt te beschouwen. Roteer de driehoek totdat één van zijn hoekpunten samenvalt met een eindpunt van de koorde. Enkel wanneer het andere eindpunt dan op de cirkelboog ligt tussen de twee overige hoekpunten, zal de koorde langer zijn dan de zijde. Aangezien de lengte van die boog een derde is van de omtrek van de cirkel, moet de gezochte kans gelijk zijn aan  $\frac{1}{3}$ .



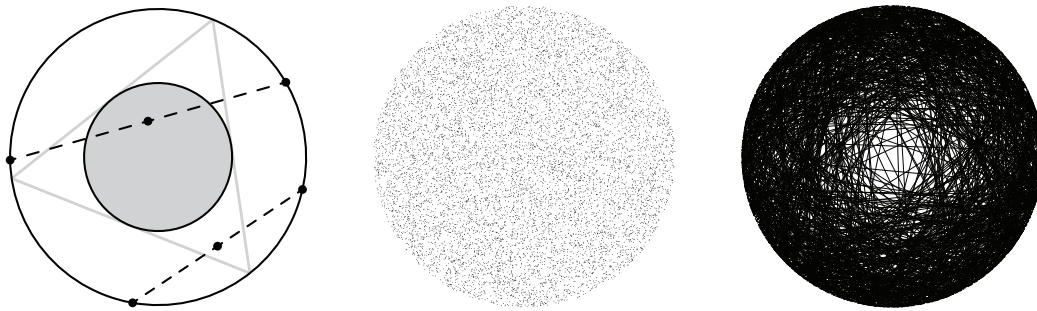
### Lukrake straal.

Een andere optie is een willekeurige straal te kiezen en op deze straal een willekeurig punt. Beschouw dan de koorde door dit punt, loodrecht door de straal, en roteer de driehoek zodat één van de zijden evenwijdig loopt met de geconstrueerde koorde. Enkel wanneer de koorde door de binnenste helft van de straal loopt, zal die langer zijn dan de zijde. De gezochte kans is dus gelijk aan  $\frac{1}{2}$ .



### Lukraak middelpunt.

Tot slot kan een willekeurige koorde ook bepaald worden door een willekeurig punt binnen de cirkel te kiezen en de unieke koorde te beschouwen die dat punt als middelpunt heeft. In dit geval wordt de koorde langer dan de zijde enkel wanneer zijn middelpunt binnen de ingeschreven cirkel van de driehoek ligt, wiens straal half zo lang is als de omgeschreven cirkel. Zo wordt de gezochte kans dus  $\frac{1}{4}$ .



## 256 Sint-Petersburgparadox

De paradox van Sint-Petersburg is een klassieke illustratie in de kansrekening voor een naïef beslissingscriterium, dat alleen de verwachte waarde van een kansspel beschouwt. Dit criterium zou een uitkomst geven die geen enkel rationeel persoon zou volgen. De paradox werd voor het eerst beschreven door Nikolaus I Bernoulli in 1713 in een briefwisseling met Pierre Raymond de Montmort, maar werd bekend gemaakt door Daniel Bernoulli en 25 jaar later gepubliceerd door de Keizerlijke Academie der Wetenschappen te Sint-Petersburg. Beschouw het volgende kansspel:

BEGIN MET €1 IN DE POT EN GOOI EEN MUNT OP. BIJ DE UITKOMST “KOP” WORDT DE INHOUD VAN DE POT VERDUBBELD EN MAG JE OPNIEUW GOOIEN, BIJ DE UITKOMST “MUNT” WIN JE DE POT.

De kans  $\mathcal{P}(X = x_k)$  dat voor het eerst “munt” gegooid wordt na  $k$  worpen, is gelijk aan  $\frac{1}{2^k}$ . De winst  $x_k$  bij deze situatie is dan  $2^{k-1}$ . De verwachtingswaarde  $E(X)$  wordt dus als volgt berekend:

$$E(X) = \sum_{k=1}^{\infty} x_k \cdot \mathcal{P}(X = x_k) = \sum_{k=1}^{\infty} \frac{1}{2^k} \cdot 2^{k-1} = \sum_{k=1}^{\infty} \frac{1}{2} \rightarrow +\infty$$

Omdat de gemiddelde winst oneindig groot wordt, zul je op termijn steeds winst maken, ongeacht hoeveel geld je dient in te leggen! In de praktijk echter zou niemand geneigd zijn meer dan een paar euro in te zetten.

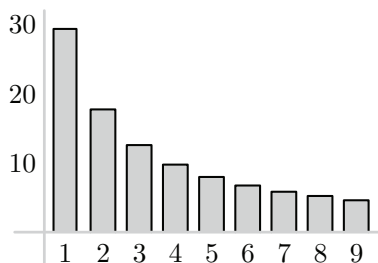
## 257 Wet van Benford

Simon Newcomb was de eerste die een curieus verschijnsel in de statistiek opmerkte. Hij observeerde in 1881 dat in de logaritmetabellen, toen intensief gebruikt voor berekeningen, de eerste pagina's meer versleten waren



dan die verderop in het boek. Newcomb ging na of getallen die beginnen met een lager cijfer, statistisch vaker zouden voorkomen dan getallen met een hoger cijfer, zoals zijn observatie van de tabellen deed vermoeden.

Newcomb onderzocht verschillende gegevensverzamelingen uit het dagelijks leven en ontdekte inderdaad dat het cijfer 1 een veel hogere frequentie heeft als begincijfer dan alle andere, zo'n 30%. De andere cijfers kwamen steeds minder vaak voor als begincijfer.



Uit deze gegevens kon Newcomb een wet opstellen die de frequentie van de begincijfers vastlegt. Frank Benford herontdekte in 1938 hetzelfde fenomeen en publiceerde een artikel met een analyse van 20 gegevensbronnen, te vinden op o.a. <http://mathworld.wolfram.com/Benford'sLaw.html>, met dezelfde formule. Hun resultaat staat vandaag bekend als de wet van Benford:

$$\mathcal{P}(n \text{ als eerste cijfer}) = \log \left( 1 + \frac{1}{n} \right)$$

Waarom de wet van Benford zo vaak opgaat, bleef lange tijd nogal onduidelijk. Wel wist men dat de gegevens niet volledig random mogen zijn, maar toch een voldoende groot bereik en variatie moeten behouden. De verdeling moet ook schaal-invariant zijn: onafhankelijk van de gebruikte maateenheid, zoals meter, voet of inch. Pas in 1995, en in 1998 met een vervolgstudie, wist Theodore Hill een afdoende verklaring voor de logaritmische verdeling te geven voor schaal-invariante gegevensverzamelingen met behulp van geavanceerde waarschijnlijkheidsrekening.

Hill bewees ook dat schaal-invariantie radix-invariantie impliceert; Benfords wet blijft geldig als van grondtal veranderd wordt, mits aanpassing van het grondtal van het logaritme (merk op dat dit voor binaire gegevens een correcte maar triviale verdeling geeft, aangezien elk getal behalve 0 daar met cijfer 1 begint). Daaruit volgt tevens dat de wet uitbreidbaar is naar tweede, derde en volgende cijfers, bijvoorbeeld  $\mathcal{P}(1 \text{ als eerste cijfer}, 2 \text{ als tweede cijfer}, 4 \text{ als derde cijfer}) = \log \left( 1 + \frac{1}{124} \right)$ .

$$\mathcal{P}(n \text{ als eerste cijfer in grondtal } d) = {}^d \log \left( 1 + \frac{1}{n} \right)$$

Exponentiële processen, Fibonaccigetallen, faculteiten, machten van twee... voldoen exact aan de wet (asymptotisch gezien), vierkantswortels en omgekeerden niet. Als praktische toepassing is de wet van Benford handig om fraude op te sporen: omdat ze zo contra-intuïtief is, zijn fraudeurs meestal geneigd uniformere gegevens te kiezen, terwijl legitieme boekhoudingen eerder voldoen aan de verdeling van Benford.

## 258 Eindeloos typende apen

In een gedachte-experiment liet Émile Borel in 1913 een aap los op een typemachine, die in willekeurige volgorde de toetsen intikt. De stelling van de eindeloos typende aap garandeert nu dat als we de aap maar lang genoeg bezig laten, hij uiteindelijk elke denkbare tekst (zoals het volledige *Hamlet* van Shakespeare) zou reproduceren!

De aap typt willekeurig en heeft dus geen voorkeur voor een bepaalde letter of lettercombinatie. In de veronderstelling dat de typemachine 50 toetsen heeft (letters, cijfers en enkele leestekens), is de kans dat de aap "banaan"

typt dan gelijk aan  $(\frac{1}{50})^6 \approx 6,4 \times 10^{-11}$ : een zeer kleine kans, maar niet nul en dus niet onmogelijk.

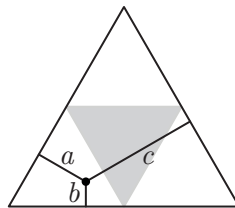
De kans dat de aap *geen* “banaan” produceert na  $n$  pogingen wordt dus  $(1 - \frac{1}{50})^n$ . Op den duur, voor  $n$  groot genoeg, nadert deze kans naar nul, en zal de aap dus met 100% waarschijnlijkheid de gevraagde uitvoer typen. Hetzelfde argument gaat op voor langere teksten, zoals *Hamlet* dat zo’n 130.000 letters bevat.

Een soortgelijke situatie beschrijft oneindig veel typende apen. Een analoge berekening wijst dan uit dat minstens één aap direct de verwachte tekst herproduceert met 100% waarschijnlijkheid.

## 259 Stokjes breken

EEN STOKJE WORDT GEBROKEN IN  $n$  STUKKEN, OP  $n - 1$  UNIFORM EN WILLEKEURIG GEKOZEN BREEK-PUNTEN. WAT IS DE KANS DAT DEZE  $n$  STUKKEN KUNNEN WORDEN SAMENGELEGD TOT EEN  $n$ -HOEK?

Probeer eerst het geval  $n = 3$ , dus de kans dat een in drie gebroken stokje een driehoek kan vormen. Onderstel voor het gemak dat het stokje voor het breken eenheidslengte heeft en noem de verkregen lengtes  $a$ ,  $b$  en  $c$ ; uit de driehoeksongelijkheid weten we dat deze tot een driehoek samengelegd kunnen worden als en slechts als  $a + b > c$ ,  $a + c > b$  en  $b + c > a$ . Een beetje prutsen met deze ongelijkheden levert op dat zowel  $a$ ,  $b$  als  $c$  kleiner dan  $\frac{1}{2}$  moeten zijn. Een mooie meetkundige manier om deze kans uit te rekenen maakt gebruik van de stelling van Viviani (zie 157, blz. 124):



Als de hoogte van de driehoek gelijk is aan de lengte van het stokje, kunnen de lengtes van de hoogtelijnen geïdentificeerd worden met  $a$ ,  $b$  en  $c$ . Elk van deze hoogtelijnen moet kleiner zijn dan  $\frac{1}{2}$ , wat enkel gebeurt als het punt waaruit de hoogtelijnen vertrekken gelegen is in het grijs gekleurde gebied op de tekening. De kans dat het punt tot dit gebied behoort bij uniforme kansverdeling is juist  $\frac{1}{4}$ , dus het antwoord voor  $n = 3$  is  $\frac{1}{4}$ .

Lastiger uit te rekenen is de kans in het algemene geval:

$$\mathcal{P}(n \text{ stukken samen te stellen tot een } n\text{-hoek}) = 1 - \frac{n}{2^{n-1}}$$

Merk op dat deze kans naar 1 nadert naarmate  $n$  toeneemt, zodat de mogelijkheid een  $n$ -hoek te construeren dan ook waarschijnlijker wordt (wat intuïtief wel te verwachten is).

## 260 Parrondo's paradox

De paradox van Juan Parrondo is een contra-intuïtief effect in de speltheorie en stelt het volgende:

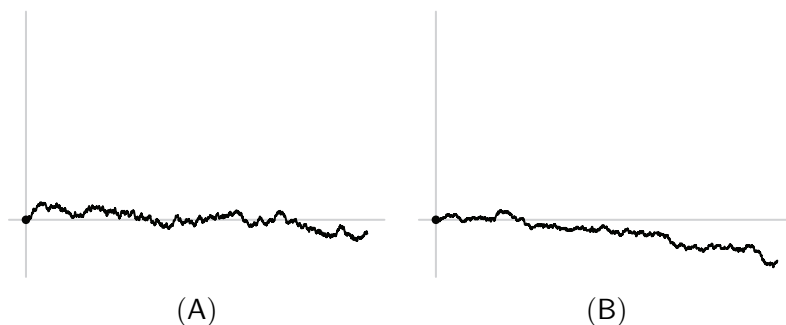
ER BESTAAN PAREN SPELLEN DIE ELK EEN GROTERE KANS OP VERLIES DAN OP WINST GEVEN, WAARVOOR HET MOGELIJK IS EEN WINNENDE STRATEGIE TE VINDEN DOOR DE SPELLEN AFWISSELEND TE SPELEN.

Deze twee gokspellen A en B vormen een concreet voorbeeld van de paradox. Winst levert één euro op, verlies kost één euro. Kies  $\varepsilon$  een kleine positieve waarde, zoals 0,005, en start met nul euro.

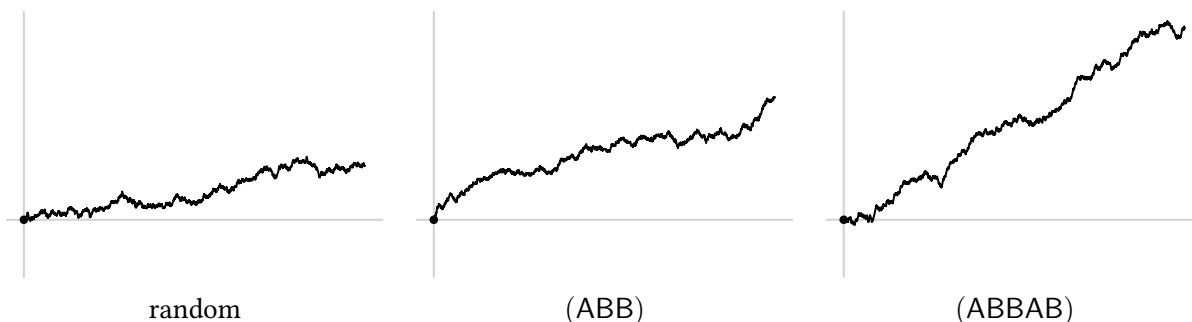
- A: gooi een munt met bias op, waarvoor de winstkans  $\frac{1}{2} - \varepsilon$  is.

- B: speel naargelang het huidige kapitaal spel  $B_1$  of  $B_2$ . Als het reeds gewonnen bedrag een veelvoud is van 3, gooi dan een munt op met winstkans  $\frac{1}{10} - \varepsilon$ , in het andere geval een munt met winstkans  $\frac{3}{4} - \varepsilon$ .

Het is duidelijk dat herhaaldelijk spel A spelen op lange termijn bijna zeker in verlies resulteert. Hetzelfde blijkt te gelden voor spel B, ook al is een van diens subspellen wel gunstig. Een simulatie na 5000 spellen:



Bepaalde periodieke combinaties van A en B geven echter een *winnend* spel! De combinaties (ABB), (AABB) en (ABBAB) bijvoorbeeld resulteren in winst op lange termijn, (AB) niet. Zelfs als de volgorde van de spellen willekeurig gekozen wordt, neemt de winst vrijwel zeker onbeperkt toe.



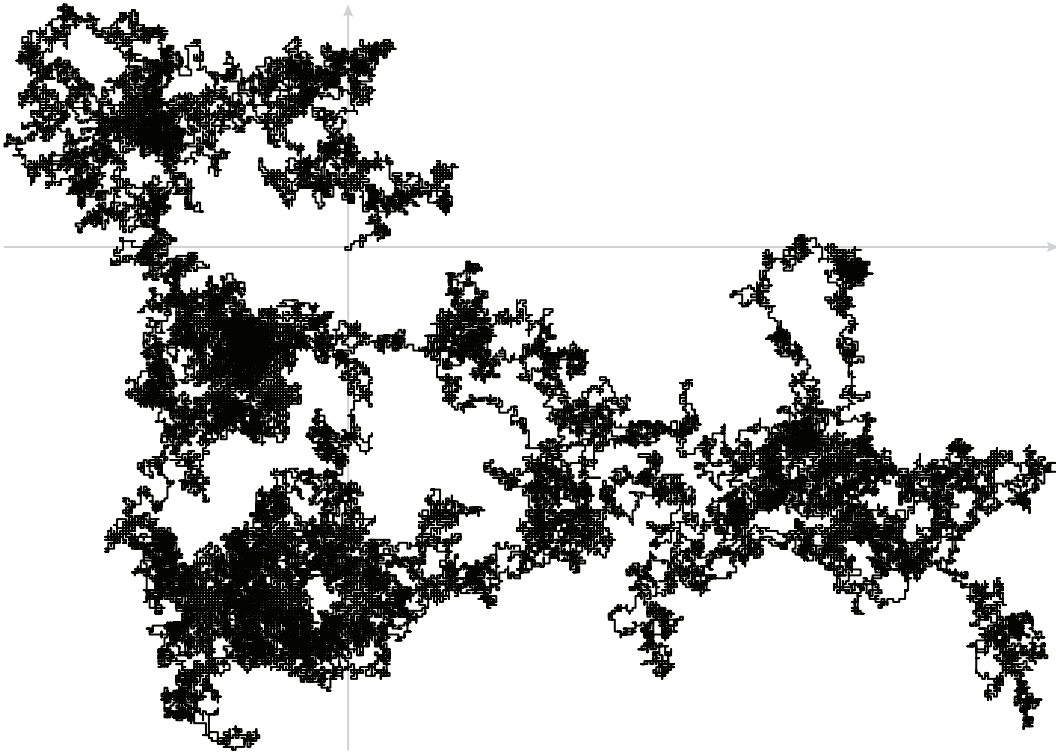
Een verklaring voor de paradox ligt in het feit dat A en B niet onafhankelijk zijn en het subspel  $B_2$  winnend is.

## 261 Willekeurige wandelingen

Beschouw een vierkant rooster en zet vanuit de oorsprong herhaaldelijk een stap naar boven, onder, rechts of links, waarbij elk van de richtingen even waarschijnlijk verondersteld wordt. Een voorbeeld van zo'n *random walk* of willekeurige wandeling met 1000 en 10000 stappen:



Bij nog grotere versies (zoals hier met 100000 stappen) gaan de structuren er steeds organischer uitzien.

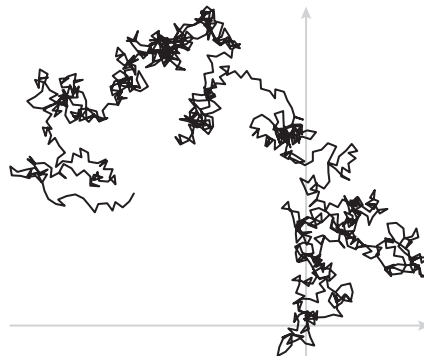


Men kan aantonen dat een tweedimensionale willekeurige wandeling “bijna zeker” (met kans 1) eender welk rasterpunt bereikt en ooit weer naar het uitgangspunt terugkeert. Opmerkelijk genoeg geldt dit niet voor driedimensionale wandelingen: daar is de kans slechts zo’n 34% dat je terug belandt op de oorsprong. Merk op dat een groot deel van die kans (25%) inhoudt dat de tweede stap de eerste ongedaan maakt; dit wil dus zeggen dat als je niet snel na het vertrek de oorsprong terugvindt, je wellicht hopeloos zal verdwalen in de ruimte. Deze kans slinkt nog verder als de dimensie toeneemt.

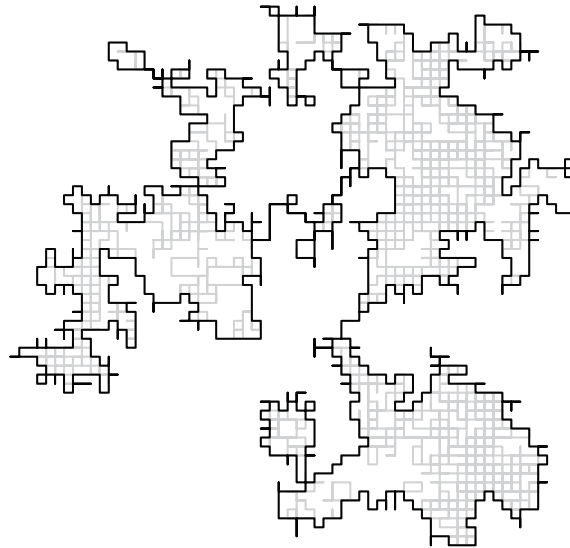
Zoals Elliott Montroll al in 1956 uitdokterde, kan de algemene kans in een  $d$ -dimensionale ruimte ( $d \geq 3$ ) exact uitgedrukt worden in de volgende spectaculaire formule, waarvoor geen gesloten vorm bekend is:

$$\mathcal{P}(\text{oorsprong teruggevonden}) = 1 - \frac{(2\pi)^d}{d \cdot \underbrace{\int_{-\pi}^{\pi} \int_{-\pi}^{\pi} \dots \int_{-\pi}^{\pi}}_d \frac{dx_1 dx_2 \dots dx_d}{d - \sum_{i=1}^d \cos x_i}}$$

Ook als de richtingen van de stappen niet langer beperkt worden tot vier, maar willekeurig te kiezen zijn uit een continu spectrum, zal elk punt van het vlak nog steeds bezocht worden met waarschijnlijkheid 1.



Benoît Mandelbrot vermoedde dat de rand van een vlakke random walk fractale dimensie  $\frac{4}{3}$  heeft, maar dit werd pas in 2002 bewezen, door Wendelin Werner die o.a. daarvoor de Fieldsmedaille werd toegekend.

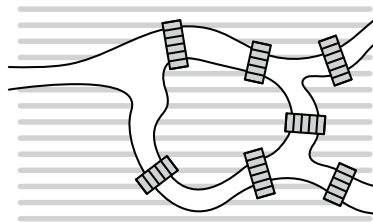






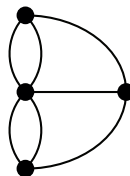
## 262 Bruggen van Koningsbergen

De stad Koningsbergen, eertijds gelegen in Duitsland maar thans gekend als Kaliningrad in Rusland, wordt door de rivier de Pregolja gescheiden in vier gebieden, verbonden door enkele bruggen. Het beroemde probleem van Koningsbergen vraagt nu of het mogelijk is tijdens een wandeling door de stad al deze bruggen juist één keer over te steken, en eventueel aan te komen op dezelfde plaats als waar de wandeling begon.

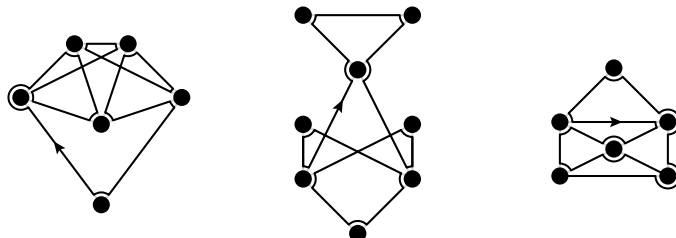


Toen Leonhard Euler in 1736 van dit probleem hoorde, bewees hij al snel dat zo'n wandeling onmogelijk is aan de hand van een diagram, waarmee hij de basis legde voor de moderne grafentheorie. Euler tekende de gebieden als punten ("toppen") en verbond de punten met een lijn ("bogen") voor elke brug tussen de desbetreffende gebieden. Geabstraheerd stelt het probleem dus:

GEGEVEN EEN GRAAF, BESTAAT ER EEN (GESLOTEN OF OPEN) TRAJECT DAT ALLE BOGEN VAN DE GRAAF JUIST ÉÉN KEER AANDOET?



Een eenvoudige observatie maakt duidelijk waarom de gezochte wandeling niet bestaat. Wanneer je via een brug een gebied betreedt, verlaat je datzelfde gebied via een andere brug, dus als zo'n wandeling mogelijk zou zijn, moet er uit elke top een even aantal bogen vertrekken. Alleen voor begin- en eindpositie is deze eis overbodig. Omdat in Koningsbergen vanuit elk van de vier gebieden een oneven aantal bruggen vertrekt, is zo'n wandeling (in moderne termen een Eulerpad) onuitvoerbaar, laat staan een gesloten (een Eulercircuit).



Als en slechts als alle toppen van de graaf  $G$  even graad hebben, bestaan er Eulercircuits in  $G$ ; bij maximaal twee toppen van oneven graad bestaan er Eulerpaden met deze toppen als eindpunt. Het aantal dergelijke circuits kan o.a. worden berekend via de stelling van BEST (zie 273, blz. 234).

Tijdens de Tweede Wereldoorlog werden twee van de zeven originele bruggen platgebombardeerd. Twee andere



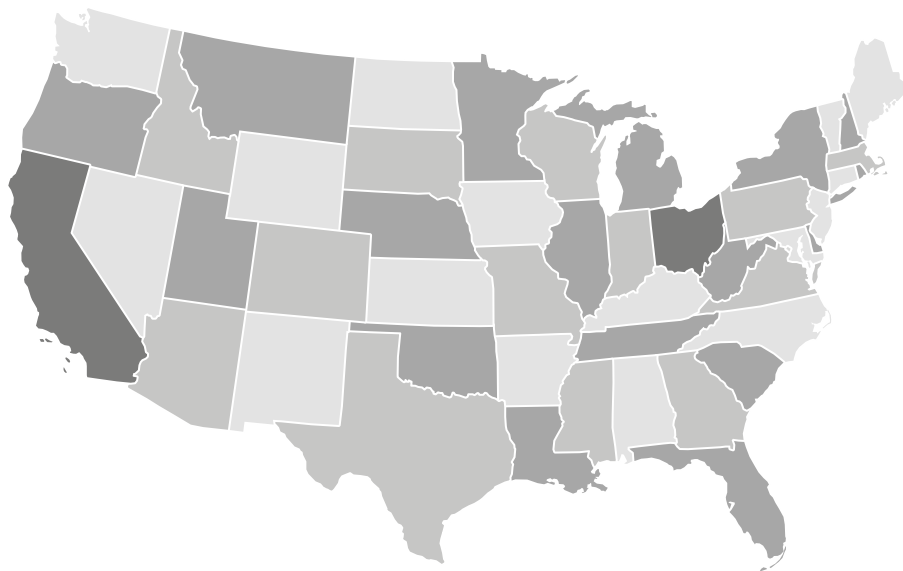
werden later verwoest en vervangen door een moderne snelweg, en de overige drie staan nog steeds overeind. Door de eliminatie van twee bruggen is een Eulerpad in Koningsbergen vandaag wél mogelijk!

## 263 Vierkleurenstelling

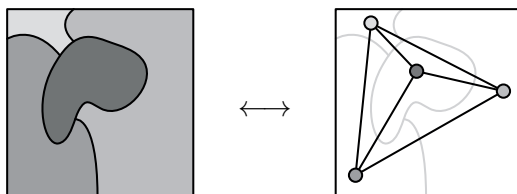
De beruchtste kwestie omtrent grafen is zonder twijfel het vierkleurenprobleem. In 1852 merkte Francis Guthrie tijdens het inkleuren van een kaart met de graafschappen van Engeland op dat dit lukte met slechts vier kleuren als aaneengrenzende graafschappen een verschillend kleur kregen, en vermoedde dat dit algemeen geldt voor elke kaart. Hij vroeg zijn broer Frederick, die op dat moment student was onder Augustus de Morgan, een verklaring hiervoor. De Morgan vond geen oplossing en schreef naar William Hamilton:

A STUDENT OF MINE ASKED ME TO DAY TO GIVE HIM A REASON FOR A FACT WHICH I DID NOT KNOW WAS A FACT - AND DO NOT YET. HE SAYS THAT IF A FIGURE BE ANY HOW DIVIDED AND THE COMPARTMENTS DIFFERENTLY COLOURED SO THAT FIGURES WITH ANY PORTION OF COMMON BOUNDARY LINE ARE DIFFERENTLY COLOURED - FOUR COLOURS MAY BE WANTED BUT NOT MORE. IF YOU RETORT WITH SOME VERY SIMPLE CASE WHICH MAKES ME OUT A STUPID ANIMAL, I THINK I MUST DO AS THE SPHYNX DID....

Een voorbeeld voor het vierkleurenprobleem op de Verenigde Staten:



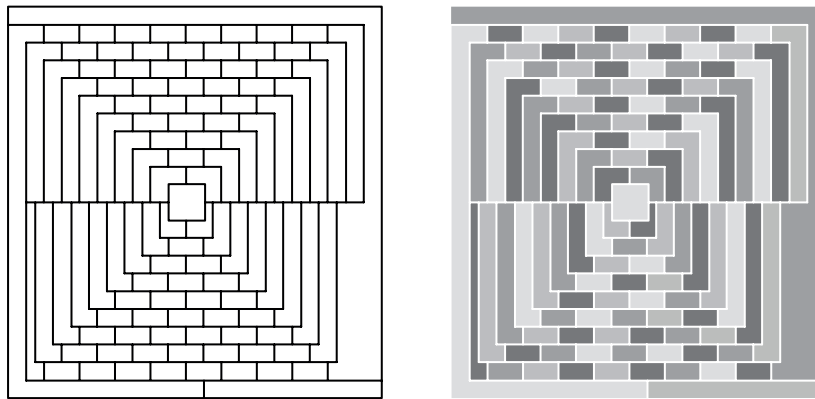
Geïnterpreteerd op grafen stelt het vierkleurenprobleem dat elke planaire graaf (die zodanig in een vlak getekend kan worden dat zijn bogen niet kruisen) zonder lussen, een chromatisch getal van ten hoogste 4 heeft.



Het ogenschijnlijk eenvoudige karakter van dit probleem strookt niet met de intrinsieke moeilijkheid ervan. Noch De Morgan, noch andere contemporaine wiskundigen konden een oplossing geven. Alfred Kempe lanceerde in 1879 een bewijspoging dat elf jaar lang als geldig aangenomen werd, tot Percy Heawood een catastrofale zwakke plek ontdekte; Kempes methode volstond daarna slechts nog ter bewijs dat *vijf* kleuren voldoende zijn. Ook in een bewijs van Peter Tait uit 1880 werd pas na elf jaar een fout gevonden, door Julius Petersen.

Martin Gardner beweerde in 1975 als een aprilgrap dat de onderstaande kaart niet reglementair in te kleuren is

met slechts vier kleuren en dus een tegenvoorbeeld voor het vermoeden vormt. Stan Wagon bekwam echter via een algoritme de kleuring rechts.



Pas in 1989 werd het vierkleurenvermoeden de vierkleurenstelling, al voelen veel wiskundigen zich nog steeds oncomfortabel tegenover het bewijs. Wolfgang Haken en Kenneth Appel gebruikten een computer om feitelijk allerlei mogelijke configuraties uit te putten. Als het vermoeden vals was, zou er een tegenvoorbeeld bestaan met het minimale aantal regio's dat vijf kleuren vereist; Haken en Appel weerlegden het bestaan van zo'n minimaal tegenvoorbeeld gebruikmakend van de volgende concepten.

- Een *onvermijdbare verzameling* omvat regio's zodat elke kaart zeker één ervan bevat.
- Een *reduceerbare configuratie* is er een die niet kan voorkomen in een minimaal tegenvoorbeeld. Als een kaart zo'n configuratie bevat, kan de kaart herleid worden naar een kleinere kaart. Deze kleinere kaart heeft bovendien de eigenschap dat als ze met vier kleuren ingekleurd kan worden, dan ook de originele kaart. Dus als voor een configuratie vier kleuren onvoldoende zijn, geldt dit ook voor de gereduceerde configuratie en dan is de originele niet minimaal.

Uiteindelijk vonden Appel en Haken een onvermijdbare verzameling van reduceerbare configuraties, waarmee het bewijs voor de vierkleurenstelling geleverd werd. Ze beperkten het oneindig aantal mogelijke kaarten tot 1936 reduceerbare configuraties (later nog teruggebracht tot 1476) die door een computer gecheckt werden. Hun onvermijdbare verzameling vereiste echter wel degelijk manuele controle, in 400 pagina's microfiche.

Wegens veel controverse en protest tegen dit bewijs, gaven Haken en Appel in 1989 een boek *Every Planar Map is Four-Colorable* uit, waarin hun bewijs volledig en gedetailleerd uitgewerkt staat.

De enige voorwaarde van kracht op de kaarten is dat de landen enkelvoudig samenhangend moeten zijn. Als landen dezelfde kleur moeten krijgen als hun eventuele exclaves (wel politiek maar niet geografisch verbonden gebieden), volstaan vier kleuren niet altijd, zoals het voorbeeld hieronder aantoont. Het aantal benodigde kleuren kan willekeurig hoog oplopen bij meerdere exclaves.



Grappig genoeg bleken de resultaten eenvoudiger aan te tonen voor ingewikkeldere oppervlakken. Heawood vermoedde dat het minimale aantal kleuren voor een oriënteerbaar oppervlak met genus  $g > 0$ , of eender welk oppervlak met Eulerkarakteristiek  $\chi$ , gegeven wordt door:

$$\left\lceil \frac{7 + \sqrt{1 + 48g}}{2} \right\rceil \quad \text{of} \quad \left\lceil \frac{7 + \sqrt{49 - 24\chi}}{2} \right\rceil$$

Gerhard Ringel en John Youngs verifieerden dit in 1968 voor alle oppervlakken, uitgezonderd voor het vlak en de fles van Klein (zie ??, blz. ??). Voor het vlak werd het bewijs geleverd met de vierkleurenstelling. De fles van Klein bleek de enige uitzondering te zijn doordat die met zes kleuren in te kleuren is i.p.v. het verwachte zeven. Voor bijvoorbeeld een torus zijn er zeven kleuren nodig (zie 147, blz. 113), zoals in het voorbeeld hieronder; de onderkant sluit aan op de bovenkant en hetzelfde geldt voor de zijkanten.

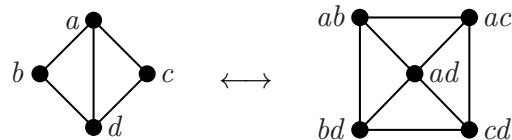


Een Möbiusband (zie 220, blz. 174) vereist zes kleuren:

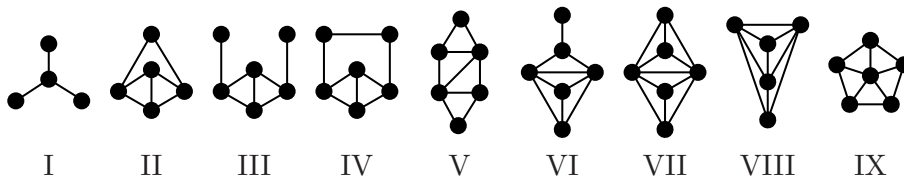


## 264 Stelling van Beineke

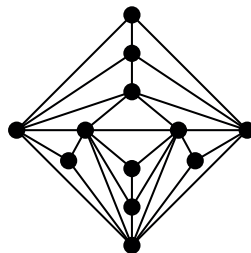
De lijngraaf van een gegeven graaf  $H$  heeft een top voor elke boog van  $H$  en een boog tussen elk paar bogen in  $H$  met een gemeenschappelijke top, bijvoorbeeld als volgt:



Lowell Beineke gaf in 1968 een karakterisatie van de mogelijke lijngraphen a.d.h.v. geïnduceerde deelgraphen (deelverzameling van de toppen van een bepaalde graaf, inclusief alle bogen die deze toppen onderling verbinden). Beineke toonde aan dat een graaf een lijngraaf is van een bepaalde graaf als en slechts als deze geen geïnduceerde deelgraaf uit deze lijst bevat:



De graaf hieronder bevat *elk* van de verboden graphen uit de lijst van Beineke (probeer ze maar terug te vinden) en is dus zeker geen lijngraaf. Hou er wel rekening mee dat een geïnduceerde deelgraaf ook alle bogen tussen de gekozen toppen meeneemt, dus de subgraaf gevormd door de twee bovenste toppen en de toppen uiterst links en rechts bijvoorbeeld, is niet de eerste verboden graaf uit de lijst!

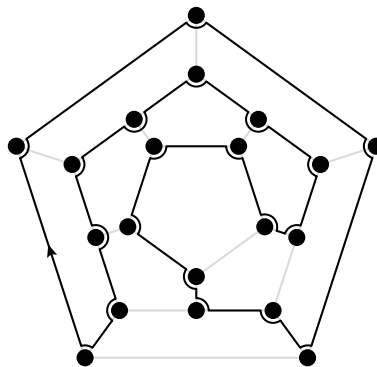


## 265 Hamiltonpaden

Een analoog probleem als de Eulerpaden (zie 262, blz. 225), maar dan met de rollen van toppen en bogen omgewisseld, wordt vernoemd naar William Hamilton, die een puzzel bedacht waarbij het de bedoeling was een gesloten pad te vinden op een icosaeëder langsheen de ribben die alle hoekpunten juist één keer aandoet.

GEGEVEN EEN GRAAF, BESTAAT ER EEN (GESLOTEN OF OPEN) TRAJEKT DAT ALLE TOPPEN VAN DE GRAAF  
JUIST ÉÉN KEER AANDOET?

Zulke trajecten heten (overeenkomstig met die van Euler) Hamiltonpaden en Hamiltoncykels. Aangezien eenvoudige criteria bekend zijn voor het al dan niet bestaan van Eulerpaden, zou men verwachten ook het probleem van de Hamiltonpaden eenvoudig op te lossen moet zijn. Dit blijkt echter niet het geval: het blijkt over het algemeen zeer moeilijk te bepalen of een willekeurige graaf Hamiltonpaden of -cykels bevat (zelfs NP-compleet, zie 322, blz. 313). Een graaf met zo'n cykel heet dan Hamiltoniaans. De icosaeëder en alle andere Platonische en Archimedische lichamen blijken wel degelijk Hamiltoniaans:



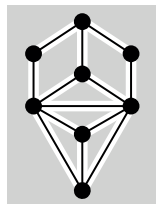
Omdat Hamiltonpaden zo lastig te vinden zijn, vormen ze een centraal onderwerp in heel wat grafentheoretische stellingen, zoals de stelling van Grinberg (zie 266, blz. 229) of het vermoeden van Tait (zie 269, blz. 232). Een voldoende voorwaarde in een eindige, eenvoudige graaf (zonder lussen of meervoudige bogen) wordt gegeven door het criterium van Øystein Ore: als elk paar niet-aanliggende toppen in een graaf samen een hogere graad hebben dan het totale aantal toppen  $n$ , bevat deze zeker een Hamiltoncykel. Gabriel Dirac toonde aan dat dit ook het geval is als elke top minstens graad  $\frac{n}{2}$  heeft.

Voor een gegeven graaf met  $n$  toppen bestaat er een unieke graaf, de sluiting genoemd, geconstrueerd door elk paar niet-aanliggende toppen  $v$  en  $w$  waarvoor  $\deg v + \deg w \geq n$  te verbinden, totdat geen zulke toppen meer gevonden worden. De stelling van Bondy-Chvátal, vernoemd naar John Bondy en Václav Chvátal, veralgemeent de stellingen van Dirac en Ore door te stellen dat een graaf Hamiltoniaans is als en slechts als ook zijn sluiting dat is. Dit resultaat is handig omdat op grafen met meer bogen gemakkelijker Hamiltoncykels gevonden kunnen worden (als ze bestaan).

## 266 Stelling van Grinberg

Deze stelling, vernoemd naar Lets wiskundige Emanuel Grinberg, geeft een nodige voorwaarde voor een planaire graaf om een Hamiltoncykel (zie 265, blz. 229) te bezitten. Ze wordt vaak gebruikt om speciale niet-Hamiltoniaanse grafen te construeren met bijkomende eigenschappen, zoals nieuwe tegenvoorbeelden voor het vermoeden van Tait (zie 269, blz. 232).

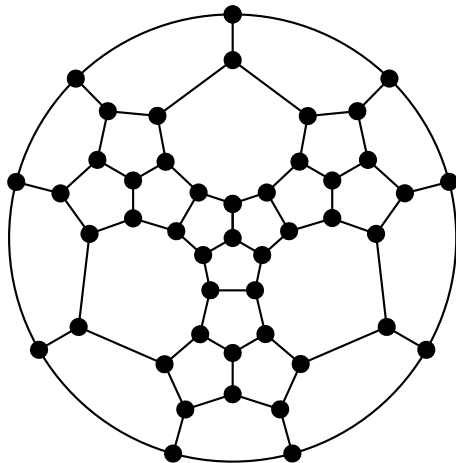
Definieer de gebieden van een planaire graaf als de regio's in het vlak volledig begrensd door bogen, waar geen andere bogen door lopen. De regio rondom de graaf is óók zo'n gebied! Deze heeft er bijvoorbeeld zeven:



Beschouw een planaire graaf die een Hamiltoncykel bevat. Noteer  $i_k$  en  $o_k$  voor het aantal  $k$ -hoekige gebieden binnen respectievelijk buiten de cykel. De stelling van Grinberg, eenvoudig af te leiden uit de formule van Euler (zie ??, blz. ??), beweert nu dat de volgende gelijkheid geldt:

$$\sum_{k \geq 3} (k - 2)(i_k - o_k) = 0$$

De stelling van Grinberg impliceert dat de onderstaande graaf geen Hamiltoncykels bevat. Beschouw de formule modulo 3 en stel dat er een Hamiltoncykel bestaat. Elk begrensde gebied heeft vijf of acht hoeken en heeft dus geen invloed op de som (immers,  $k - 2 \equiv 0 \pmod{3}$ ), ongeacht of die nu binnen of buiten een cykel zou liggen. Het onbegrensde gebied rondom de graaf heeft echter negen hoeken en draagt dus wel een term bij, zodat de gehele som verschillend is van nul, de gelijkheid niet opgaat en er dus geen Hamiltoncykel te vinden kan zijn.

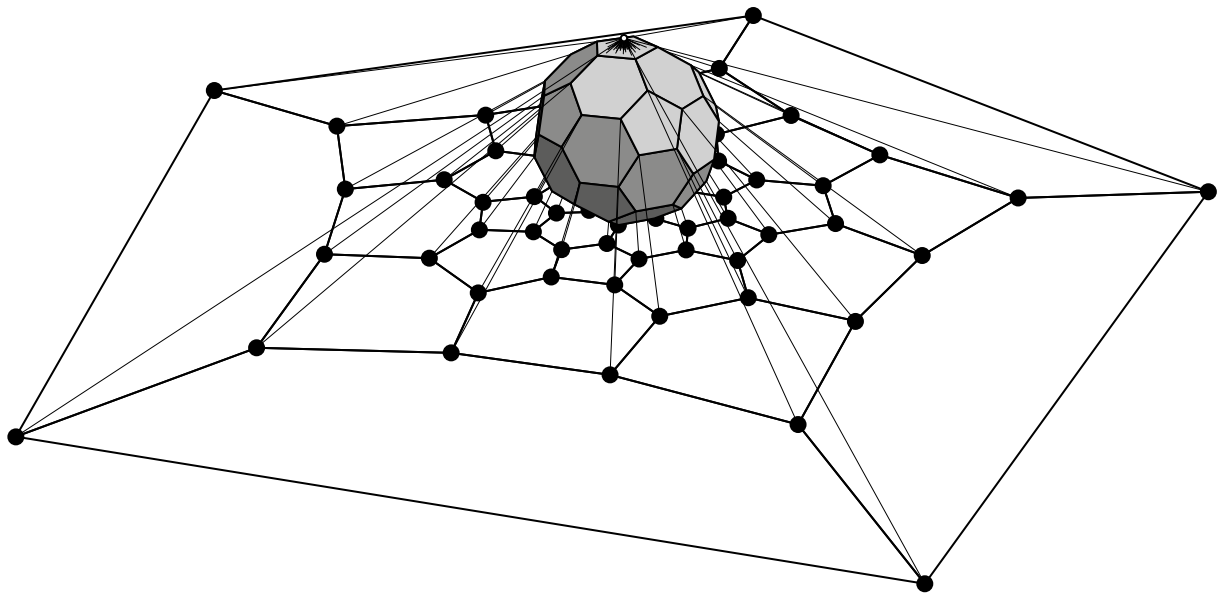


De stelling is helaas niet in twee richtingen geldig. Er bestaan bijvoorbeeld wel degelijk grafen met alleen vijf- en achthoekige gebieden, die toch geen Hamiltoncykels bevatten.

## 267 Stelling van Steinitz

Beschouw eender welk convex veelvlak en construeer de corresponderende graaf met een top voor elk hoekpunt en een boog voor elke ribbe. Het resultaat noemt men de polyhedrale graaf of het skelet van dat veelvlak. Je kunt ze ook eenvoudig verkrijgen door een Schlegeldiagram: de projectie van het veelvlak vanuit een punt voorbij diens zijden, op een vlak\*, zoals hieronder voor de afgeknotte icosäeder gebeurd is.

\*De algemene Schlegeldiagrammen zijn projecties van een  $n$ -dimensionale polytoop naar  $n - 1$  dimensies. Feitelijk worden ze frequenter gebruikt ter visualisatie van vierdimensionale polytopen.



Volgens de stelling van Balinski blijft het skelet van een  $d$ -dimensionaal veelvlak samenhangend bij verwijdering van eender welke  $d - 1$  toppen. Een graaf met deze eigenschap heet  $d$ -verbonden.

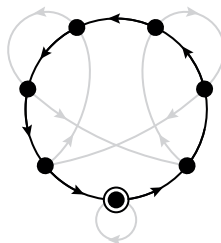
Een belangrijke karakterisatie van de polyhedrale grafen (van driedimensionale polyhedra) wordt gegeven door de stelling van Steinitz, vernoemd naar Ernst Steinitz die de stelling bewees in 1922. Steinitz bewees dat deze grafen juist de 3-verbonden planaire grafen zijn. Elk convex veelvlak heeft dus een 3-verbonden planair skelet, en omgekeerd correspondeert elke 3-verbonden planaire graaf met een welbepaald convex veelvlak.

## 268 Deelbaarheidsgrafen

David Wilson beschreef in een blog van Tanya Khovanova een zeer originele manier om deelbaarheid van gehele getallen te controleren via grafen. De graaf hieronder bijvoorbeeld codeert deelbaarheid door 7. De methode werkt als volgt voor een gegeven getal  $n$ :

- Begin bij de omcirkelde boog onderaan.
- Voor elk cijfer  $d$  in  $n$ , volg je  $d$  opeenvolgende zwarte pijlen, gevolgd door één grijze pijl.
- Herhaal de vorige stap door alle cijfers van  $n$  te overlopen (te beginnen bij het meest significante cijfer).

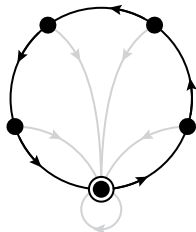
Enkel als je terug uitkomt op de omcirkelde top, is  $n$  deelbaar door 7!



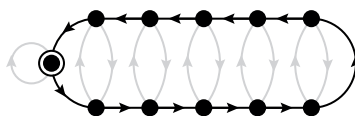
Feitelijk berekent de graaf nog iets sterkers, namelijk  $n \pmod{7}$ . De zeven toppen met de zwarte pijlen vormen een cykel; geef de omcirkelde top label "0" en elke volgende in de cykel één meer dan de vorige. Het label van de bereikte top na het doorlopen van het algoritme geeft dan weer hoeveel de rest is bij gehele deling door 7.

Een eenvoudige constructiemethode voor analoge deelbaarheidsgrafen gaat als volgt: noteer  $m$  voor de deler en begin met een  $m$ -cykel gelabeld zoals hierboven. Voor elk label  $r$  dient er een zwarte pijl te vertrekken naar zijn opvolger en een grijze pijl naar de waarde  $10 \cdot r \pmod{m}$ . Voor bijvoorbeeld 5 geeft dit een simpele graaf, die je

ongeacht welk cijfer terugstuurt naar de omcirkelde top. Merk op dat deze methode veralgemeend kan worden naar andere talstelsels; een binaire deelbaarheidsgraaf bijvoorbeeld kan dienen als een eindigetoestandsauto-maat, die de modulo-operatie in lineaire tijd berekent t.o.v. het aantal cijfers.



Voor 11 krijgen we een mooie symmetrische deelbaarheidsgraaf:



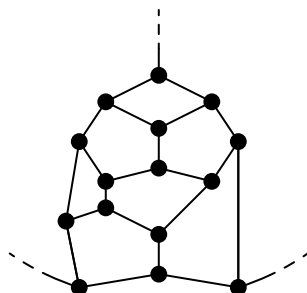
## 269 Vermoeden van Tait

Peter Tait stelde in 1884 een significant vermoeden voor dat, indien waar, de vierkleurenstelling (zie 263, blz. 226) zou impliceren. Helaas werd het in 1946 door William Tutte ontkracht a.d.h.v. een tegenvoorbeeld met 46 toppen en 69 bogen. Het vermoeden stelde:

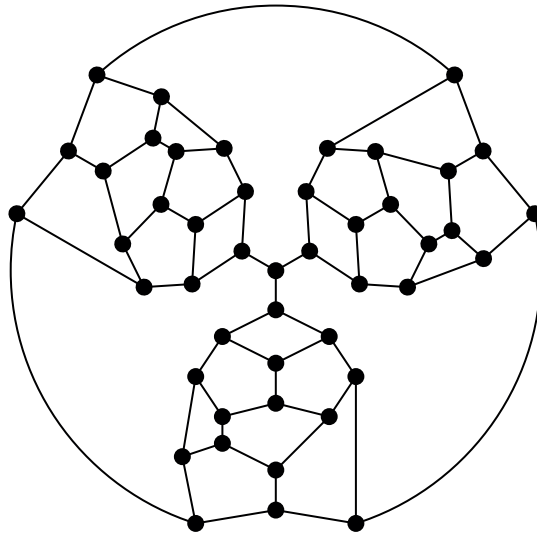
ELKE 3-VERBONDEN, PLANAIRE, KUBISCHE GRAAF BEVAT EEN HAMILTONCYKEL.

Hamiltoncyclen worden besproken in 265, blz. 229. Een graaf is  $k$ -verbonden als je minstens  $k$  toppen moet verwijderen om een niet-samenhangende graaf over te houden. Planaire grafen zijn te tekenen in het vlak zonder kruisende bogen. Tot slot is een graaf kubisch als elk van zijn toppen graad drie heeft.

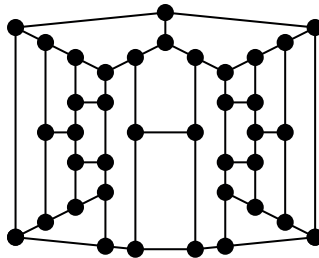
Tutte toonde aan dat het vermoeden vals is via zijn speciaal geconstrueerde graaf. De sleutel tot zijn tegenvoorbeeld is het onderdeel hieronder. Wanneer dit fragment binnen een grotere graaf zit, moet elke Hamiltoncykel het fragment binnengaan en verlaten via de bovenste top en één van de onderste twee; een Hamiltonpad met de onderste toppen als begin- en eindpunt kan niet het hele fragment aandoen. De boog bovenaan maakt dus zeker deel uit van een cykel.



Het is nu eenvoudig in te zien waarom de onderstaande graaf, bestaande uit drie zo'n Tuttefragmenten, geen Hamiltoncykel kan bezitten. Indien zo'n cykel bestaat, moet die immers langs de drie bogen rond de centrale top passeren, wat onmogelijk is.



Het kleinst gekende tegenvoorbeeld werd onafhankelijk van elkaar gegeven door Joshua Lederberg, David Bar-  
nette en Juraj Bosák rond 1965, en telt 38 toppen en 57 bogen.



## 270 Stelling van Frieze

Alan Frieze ontdekte deze stelling in 1985. Beschouw een complete graaf met  $n$  toppen waarin aan elke boog een willekeurig reëel getal tussen nul en één, onafhankelijk en uniform verdeeld, als gewicht wordt toegekend. In deze graaf observeren we de opspannende bomen; dit zijn samenhangende deelgrafën die alle toppen van de oorspronkelijke graaf bevatten, maar geen cykels. Het verwachte gewicht van een willekeurige opspannende boom in de complete graaf blijkt gelijk aan  $\frac{n-1}{2}$  en neemt dus onbeperkt toe met het aantal toppen.

Het verrassende is dat de opspannende boom met het minimale gewicht wel degelijk een begrensd gewicht heeft, dat bij grotere  $n$ -waarden bovendien convergeert naar  $\zeta(3)$ , de zètafunctie van 3 (zie ??, blz. ??)!

## 271 Stelling van Vizing

De vierkleurenstelling (zie 263, blz. 226) gaat over toppenkleuringen van planaire grafen. Een soortgelijk kleur-principe kan worden opgesteld voor de bogen; daar mogen bogen die een top delen niet dezelfde kleur hebben. Het is duidelijk dat het minimum aantal kleuren dan minstens de maximale graad  $\Delta$  van de graaf is. De stelling van Vadim Vizing stelt dat er hoogstens één extra kleur nodig is voor een legitieme kleuring van de gehele graaf.

Dit geeft aanleiding tot een indeling in twee klassen: de grafen waarbij  $\Delta$  kleuren voldoende zijn, en die waarbij er  $\Delta + 1$  nodig zijn. Vizing toonde eveneens aan dat de grafen uit klasse twee zeker drie toppen moeten hebben met maximale graad. Robin Wilson en Lowell Beineke merkten in 1973 op dat van de 143 grafen met niet meer dan zes toppen, er slechts acht waren van de tweede klasse. Wilson vermoedde dat deze schaarste in de limiet naar nul nadert bij toenemend aantal toppen, wat hij in samenwerking met Paul Erdős bewees in 1977. Bijna alle grafen zijn dus van de eerste klasse en vereisen juist evenveel kleuren als hun grootste graad.



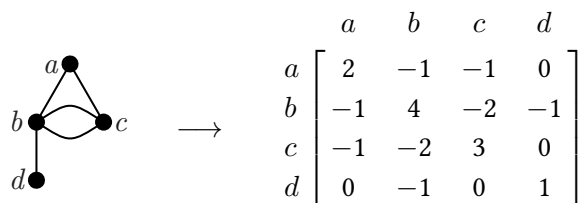
## 272 Matrix-boomstelling van Kirchhoff

Deze stelling van fysicus Gustav Kirchhoff beschrijft het aantal opspannende bomen voor een gegeven graaf via determinanten. Kirchhoff vond in zijn stelling uit 1847 een methode om elektrische schakelingen en netwerken te onderzoeken. In feite is dit een generalisatie van de formule van Cayley, die het aantal opspannende bomen in de complete graaf beschrijft (zie 274, blz. 235).

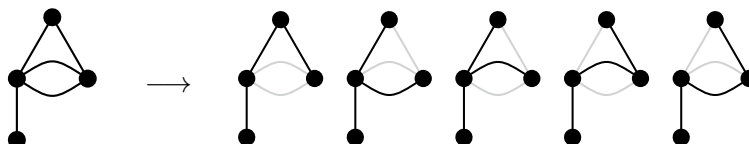
Beschouw de graaf  $G$  met  $n$  toppen. Construeer de bijhorende Laplaciaanse  $n \times n$ -matrix  $\mathbb{L}(G)$  als volgt:

$$\mathbb{L}(G) = (a_{ij})_{n \times n} \text{ met } \begin{cases} a_{ij} = -(\text{aantal bogen tussen top } i \text{ en top } j) & \text{voor } i \neq j \\ a_{ij} = \text{graad van top } i & \text{voor } i = j \end{cases}$$

Uit deze definitie volgt dat de matrix symmetrisch is en dat de som van elke rij of kolom gelijk is aan nul. Verder is  $\mathbb{L}$  steeds positief-semidefiniet en heeft ze eigenwaarde nul, wiens multipliciteit juist het aantal samenhangende componenten van de graaf is. Tot slot (en dit is belangrijk voor de uiteindelijke stelling van Kirchhoff) zijn al de minoren van  $\mathbb{L}$  in absolute waarde gelijk. Een voorbeeld:



De stelling van Kirchhoff geeft een methode om a.d.h.v. deze matrix het aantal opspannende bomen te berekenen. Deze zijn juist de maximale bomen zonder cyclen, of de minimale bomen die alle toppen verbinden en bestaan uit  $n - 1$  bogen. Volgens Kirchhoff is het aantal opspannende bomen in de graaf net gelijk aan de (unieke) minor van zijn Laplaciaan  $\mathbb{L}$  in absolute waarde. In het voorbeeld geeft dit 5, en inderdaad:



Specifiek toegepast op een complete graaf  $K_n$  resulteert de Laplaciaan in de formule van Cayley (zie 274, blz. 235), omdat onderstaande Laplaciaanse matrix steeds  $n^{n-2}$  als absolute minoren heeft:

$$\mathbb{L}(K_n) = \begin{bmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{bmatrix}$$

## 273 Stelling van BEST

Vernoemd naar Cedric Smith and Bill Tutte, die in 1941 een speciaal geval aantoonde, en Nicholaas de Bruijn en Tatyana van Aardenne-Ehrenfest, die in 1951 het algemene resultaat bekwamen, geeft de stelling van BEST een formule voor het aantal Eulercircuits (zie 262, blz. 225) in bepaalde grafen. De stelling is van toepassing op gerichte grafen (met georiënteerde bogen) waarin Eulercircuits mogelijk zijn, d.w.z. waarin de in- en uitgraad van elke top gelijk is. Voorgesteld met pijlen moeten er in elke top evenveel pijlen toekomen als eruit vertrekken. De stelling maakt gebruik van zogenaamde gewortelde bomen, waarin voor elke top een gericht pad naar een bepaalde top (de wortel) gevonden kan worden, bijvoorbeeld deze hierboven rechts.

Kies een specifieke top  $w$  uit en bepaal het aantal gewortelde bomen met wortel  $w$ , genoteerd als  $t_w$ . De in- en uitgraad van een top  $v$ , gelijk verondersteld, wordt genoteerd met  $\deg(v)$ . De stelling van BEST stelt nu dat het totaal aantal Eulercircuits gegeven wordt door:

$$t_w \cdot \prod_v (\deg(v) - 1)!$$

Hierbij loopt het product over alle toppen van de graaf. Uit de stelling blijkt direct dat het aantal bomen geworteld in  $w$  gelijk is voor elke top  $w$ , wat al totaal niet evident is. Nog minder voor de hand liggend is dat deze formule een eenvoudige methode geeft om het aantal Eulercircuits in een gerichte graaf te berekenen, in polynomiale tijd, terwijl dit voor ongerichte grafen een #P-probleem\* is!

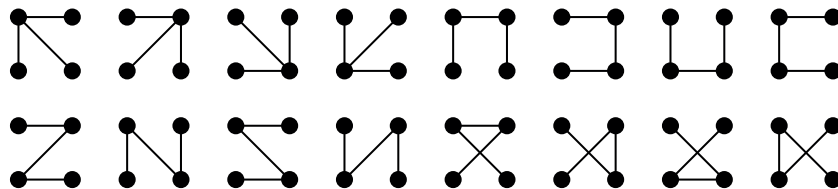
## 274 Formule van Cayley

Een van de elegantste resultaten uit de enumeratieve combinatoriek is deze formule van Cayley. Carl Borchardt beschreef ze voor het eerst en bewees ze via determinanten in 1860. In 1889 gaf Arthur Cayley een uitbreiding en ondanks zijn verwijzing naar Borchardts originele resultaat, wordt de formule vandaag naar Cayley vernoemd. Ook James Sylvester zou ze al gekend hebben.

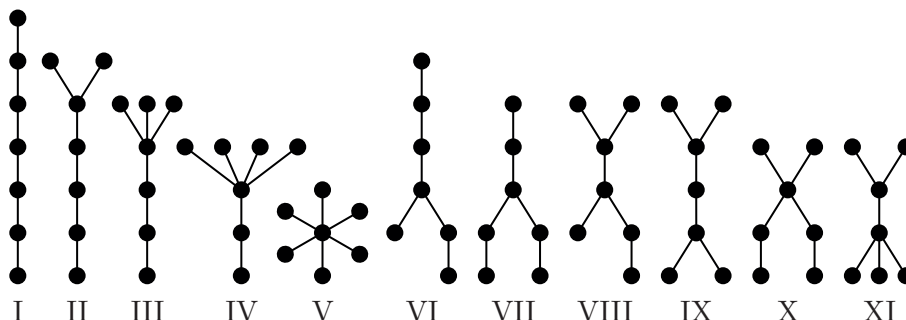
Beschouw alle gelabelde bomen met  $n$  toppen, d.w.z. waarbij de toppen onderling te onderscheiden zijn. Er zijn bijvoorbeeld drie zulke bomen met drie toppen:



Met vier toppen bestaan er al zestien gelabelde bomen:



De formule van Cayley stelt algemeen dat het totale aantal opspannende bomen op  $n$  verschillende toppen gelijk is aan  $n^{n-2}$ . Bij  $n = 7$  kun je de volgende bomen opstellen, waarbij er nog verschillende mogelijkheden zijn om de toppen te labelen:



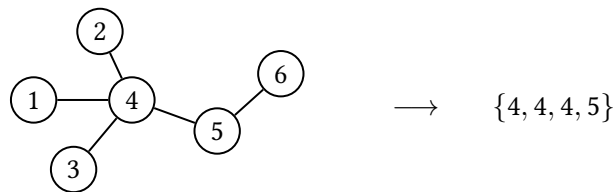
Het aantal mogelijke labelingen wordt als volgt geteld. Voor IX bijvoorbeeld, kun je de onderste twee vertakkingen permuteren zonder de boom wezenlijk te veranderen, net als de bovenste twee, of de boven- en onderkant, dus dit levert  $\frac{7!}{2 \cdot 2 \cdot 2}$  bomen op. Ook hier is aan de formule van Cayley voldaan: het totale aantal is inderdaad  $7^5$ .

\*#P-problemen zijn de overeenkomstige telproblemen van de beslissingsproblemen uit NP. Een typisch NP-probleem vraagt of er oplossingen bestaan die aan bepaalde beperkingen voldoen. Het bijhorende #P-probleem vraagt dan *hoeveel* oplossingen eraan voldoen. Klaarblijkelijk is de klasse #P nog moeilijker dan NP.

I	II	III	IV	V	VI	VII	VIII	IX	X	XI
$\frac{7!}{2}$	$\frac{7!}{2}$	$\frac{7!}{3!}$	$\frac{7!}{4!}$	7	7!	$\frac{7!}{3!}$	$\frac{7!}{2}$	$\frac{7!}{2^3}$	$\frac{7!}{2^2}$	$\frac{7!}{2 \cdot 3!}$

Er zijn verschillende elegante bewijzen voor Cayleys formule. Klassieke bewijzen maken gebruik van Kirchhoffs stelling (zie 272, blz. 234) of recursie. Jim Pitman gaf een ander bewijs (het mooiste volgens *Proofs from THE BOOK*) via dubbele telling. Een bewijs door bijjectie werd gegeven door Heinz Prüfer, via zijn Prüfersequenties.

Zo'n Prüfersequentie is een unieke sequentie van lengte  $n - 2$  horende bij een gelabelde boom met als toppen  $\{1, 2, \dots, n\}$ . Zoek telkens het "blad" (top met graad 1) met het kleinste label, knip het af van de boom en noteer het label van zijn "tak" (unieke buur) als volgende element in de sequentie. Herhaal tot er nog maar twee toppen overblijven. Beschouw het volgende voorbeeld:



Het is duidelijk dat elke boom een unieke Prüfersequentie heeft. Omgekeerd correspondeert ook elke sequentie juist met één boom. De verzameling gelabelde bomen met  $n$  toppen is dus bijjectief met de verzameling sequenties met  $n - 2$  labels gekozen uit  $\{1, 2, \dots, n\}$ ; de laatste verzameling heeft kardinaliteit  $n^{n-2}$ , en dus de eerste ook.

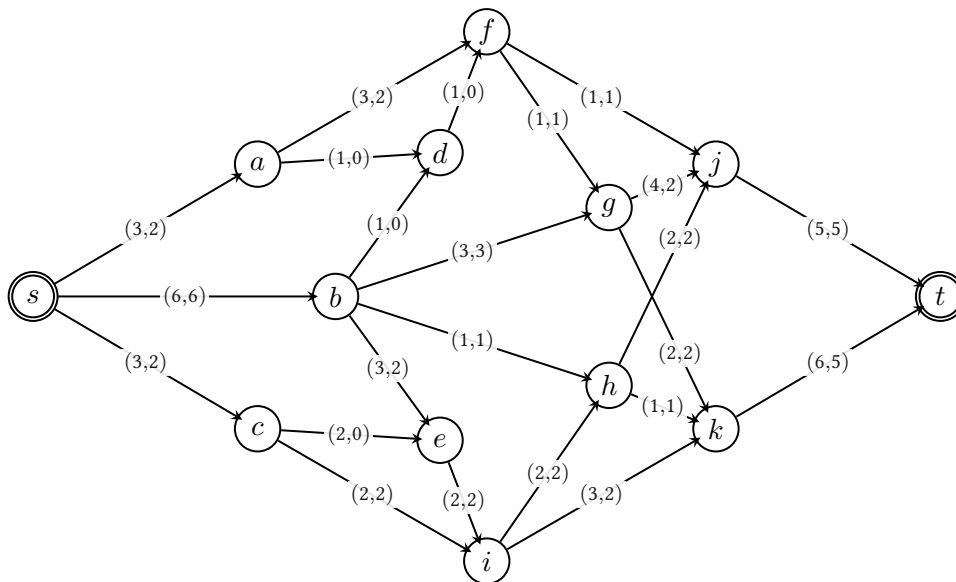
## 275 Max-flow-min-cut

Een belangrijk resultaat in optimalisatietheorie is de max-flow-min-cutstelling, die een verband legt tussen de maximale stroom in een stroomnetwerk en de minimaal af te snijden capaciteit om alle stroom te blokkeren.

In een netwerk (een gerichte graaf) heet een top met in- of uitgraad 0, een *source* respectievelijk *sink*. Behalve een richting wordt elke boog ook een capaciteit toegekend, d.i. een positief reëel getal  $c$  dat de maximale stroom (*flow*) voorstelt die doorheen de boog kan stromen. De flow zelf is dan een nieuwe afbeelding  $f$  van de bogen naar  $\mathbb{R}^+$  die voldoet aan twee voorwaarden:

- In elke boog geldt de capaciteitslimiet,  $f \leq c$ .
- In elke top (op de source en sink na) is de toestromende flow exact even groot als de uitgaande.

De totale flow, genoteerd  $|f|$ , is de hoeveelheid die vertrekt uit de source (en toekomt in de sink). Een natuurlijk probleem is nu de waarde  $|f|$  te maximaliseren in een bepaald netwerk met gegeven capaciteiten. Een voorbeeld van een dergelijk stroomnetwerk staat hieronder; de labels zijn van de vorm  $(c, f)$ . Concreet spreekt men hier van een *s-t-flow*, daar de stroom van de source  $s$  naar de sink  $t$  gaat.



Nu willen we door bogen te verwijderen, de source en de sink van elkaar scheiden. Een  $s$ - $t$ -snede is een partitie van de toppen in twee componenten, waarvan de ene  $s$  bevat en de andere  $t$ ; door de bogen tussen deze componenten weg te nemen, wordt de flow tussen source en sink afgesneden ( $|f| = 0$ ). Een praktisch probleem in deze context is de snede te bepalen die de weggesneden capaciteit minimaliseert.

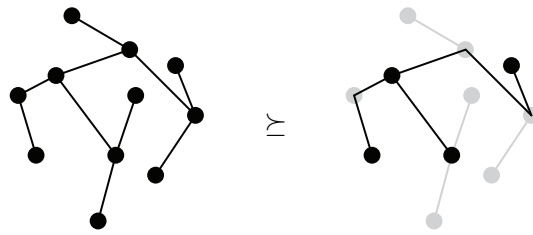
Zoals de naam al doet vermoeden, beweert de max-flow-min-cutstelling nu dat de maximale  $s$ - $t$ -flow gelijk is aan de minimale  $s$ - $t$ -snede! Wanneer men in een netwerk een flow en een snede vindt met dezelfde waarde, weet men dus dat beiden optimaal zijn. In het voorbeeld hierboven vloeit er een flow met  $|f| = 10$ , en men gaat eenvoudig na dat de snede  $\{s, a, b, c, d, e, f\} \leftrightarrow \{g, h, i, j, k, t\}$  bogen met totale capaciteit 10 wegsnijdt. Groter kan de flow in dit voorbeeld dus niet worden.

Min-cut-max-flow werd bewezen door Peter Elias, Amiel Feinstein en Claude Shannon in 1956, en onafhankelijk door Lester Ford en Delbert Fulkerson in datzelfde jaar. Het speciale geval voor ongerichte en ongewogen grafen werd echter al bewezen door Karl Menger in 1927.

## 276 Kruskals boomstelling

De boomstelling van Joseph Kruskal is een vrij technische stelling die aanleiding geeft tot een functie  $\text{Tree}(n)$ , die onvoorstelbaar snel groeit en al gigantische waarden aanneemt voor  $n = 3$ . De stelling van Kruskal gaat over zogenaamde wel-quasi-ordeningen. Dit zijn reflexieve en transitieve relaties die geen oneindige dalende keten en geen oneindige antiketen van onderling onvergelijkbare elementen toelaten, zoals de vertrouwde ordening op de natuurlijke getallen. Op  $\mathbb{Z}$  geeft dit echter geen wel-quasi-ordening, daar er oneindig dalende ketens bestaan. Nog een niet-voorbeeld is  $\mathbb{N}$  geordend op deelbaarheid: daar vormen de priemgetallen een oneindige antiketen.

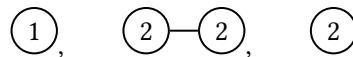
De boomstelling van Kruskal stelt nu dat de verzameling van eindige bomen waarvan de toppen gelabeld worden met termen uit een wel-quasi-geordende verzameling, zelf ook wel-quasi-geordend is volgens homeomorfe inbedding, of  $A \preceq B$  als en slechts als  $A$  een zogenaamde minor van  $B$  is (te verkrijgen door bogen en toppen te verwijderen en bogen samen te trekken). Het voorbeeld hieronder verduidelijkt de ordening:



Kruskals resultaat garandeert het bestaan van een functie die Harvey Friedman Tree noemde. Beschouw een rij van gelabelde bomen (voor het gemak labelen we met natuurlijke getallen) die voldoet aan volgende condities:

- Hoogstens een vooropgegeven aantal labels wordt gebruikt.
- Elke boom heeft hoogstens zoveel toppens als zijn index in de rij.
- Geen enkele boom is een minor (met matchende labels) van een boom die verderop in de rij staat.

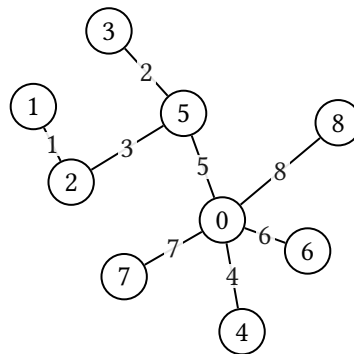
De boomstelling van Kruskal impliceert dat zo'n rij onmogelijk oneindig kan zijn. Friedman definieerde  $\text{Tree}(n)$  dus als de maximale lengte van een rij waarin  $n$  labels gebruikt mogen worden.  $\text{Tree}(1)$  is duidelijk gelijk aan 1, want de eerste boom in de rij is een enkele top gelabeld 1, en elke volgende boom zou deze als minor bevatten. Het is ook eenvoudig te verifiëren dat de langste rij met 2-gelabelde bomen een bescheiden lengte 3 heeft:



De waarde van  $\text{Tree}(3)$  explodeert echter tot een getal zo onvoorstelbaar groot dat deze min of meer volslagen onbegrijpelijk is; zelfs het getal van Graham (245, blz. 203) stelt absoluut niets voor vergeleken met  $\text{Tree}(3)$ !

## 277 Gracieuze bomen

Beschouw een samenhangende graaf met  $n$  bogen. Ken diens toppen getallen van 0 tot en met  $n$  toe zodanig dat geen twee toppen hetzelfde getal krijgen, en label vervolgens elke boog met het verschil van z'n twee eindtoppen (in absolute waarde). Als deze labels precies de waarden 1 tot en met  $n$  zijn, spreekt men van een gracieuze (*graceful*) labeling. Een voorbeeld:



De graaf wordt zelf gracieus genoemd als er een gracieuze labeling voor bestaat. Niet alle grafen voldoen hieraan; in een pionierend artikel in 1967 bewees Alex Rosa bijvoorbeeld dat Euleriaanse grafen nooit gracieus zijn als  $n$  congruent is met 1 of 2 modulo 4, en dat een cykel gracieus is precies als  $n$  congruent is met 0 of 3 modulo 4. Rosa hanteerde trouwens de benaming " *$\beta$ -valuation*"; de populaire benaming is afkomstig van Solomon Golomb.

Van verscheidene families grafen is de gracieuziteit al bewezen. Relatief eenvoudig te controleren voorbeelden zijn ster- en padgrafen. Via een computerproject onder leiding van Wenjie Fang werden alle bomen tot 35 toppen geverifieerd, in het spoor van het notoire vermoeden van Ringel-Kotzig (naar Gerhard Ringel en Anton Kotzig), dat stelt dat in feite *alle* bomen gracieuze labelings toelaten! Vorderingen voor dit open probleem geschieden zeer moeizaam; Kotzig zelf bestempelde de inspanningen als een kwaal.





## XII Magische vierkanten

### 278 Melencolia I

De befaamde Albrecht Dürer, Duits kunstenaar uit de renaissance, creëerde als een van zijn bekendste werken de gravure *Melencolia I*, waarin een beroemd magisch vierkant verwerkt zit dat barst van patronen.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

De magische constante is 34 en wordt in vele combinaties teruggevonden (rijen, kolommen, diagonalen, centrale  $2 \times 2$ -vierkant, hoeken, kwadranten ...). Centraal in de onderste rij staat "1514", het jaartal waarin Dürer *Melencolia I* maakte.

### 279 Eulers magische paardenrondgang

Een paardenrondgang is een circuit bestaande uit paardensprongen, waarbij het paard alle velden van het bord precies éénmaal aandoet. Vaak eist men ook nog dat het paard daarna weer naar in één sprong naar zijn beginveld kan terugkeren (zo'n paardenrondgang wordt dan *gesloten* genoemd, indien dit niet het geval is *open*). Voor een  $8 \times 8$ -bord zijn er vele elegante paardenrondgangen mogelijk.

Leonhard Euler vond een paardenrondgang op een  $8 \times 8$ -bord dat, als je de opeenvolgende sprongen nummert, een halfmagisch vierkant oplevert met magische som 260. De paardenrondgang is niet gesloten maar open, en de sommen in de diagonalen komen niet overeen, maar wat deze kleine tekortkomingen meer dan goedmaakt is het feit dat de vier kwadranten zelf weer halfmagische  $4 \times 4$ -vierkanten zijn, en in elk  $4 \times 4$ -kwadrant is de som van het  $2 \times 2$ -kwadrant óók constant (130).

1	48	31	50	33	16	63	18
30	51	46	3	62	19	14	35
47	2	49	32	15	34	17	64
52	29	4	45	20	61	36	13
5	44	25	56	9	40	21	60
28	53	8	41	24	57	12	37
43	6	55	26	39	10	59	22
54	27	42	7	58	23	38	11

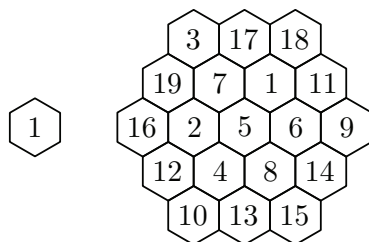
Ondertussen zijn er al andere van dit type paardenrondgangen ontdekt (zelfs gesloten), maar er wordt vermoed dat een *perfect* magisch  $8 \times 8$ -vierkant met paardenrondgang, waarbij ook de diagonalen dezelfde som hebben als de rijen en kolommen, niet bestaat.



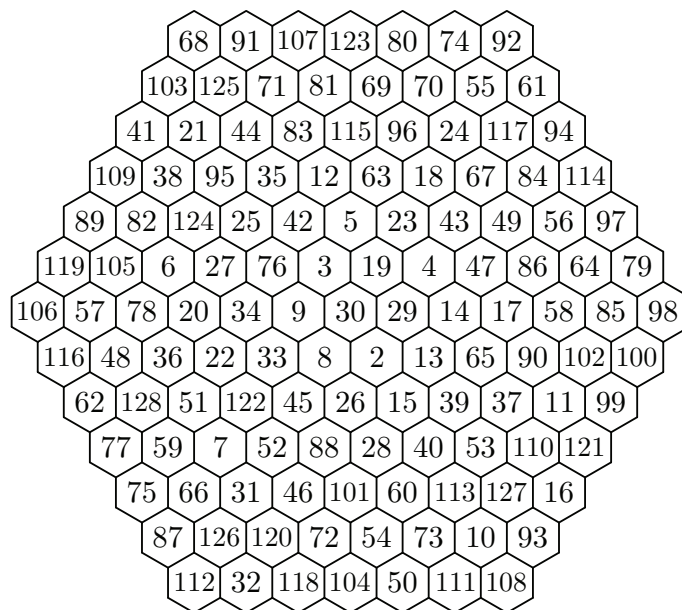
## 280 Magische zeshoek

De magische zeshoek, een variatie op het magisch vierkant, heeft de structuur van een gecentreerd hexagonaal rooster gevuld met getallen, waarbij in elke “rij” (in elke mogelijke richting) de som constant is. Analoog als bij de vierkanten wordt het aantal cellen op de rand ervan de orde  $n$ .

Een *normale* magische zeshoek bevat alle opeenvolgende gehele getallen van 1 tot  $3n^2 - 3n + 1$ . Het blijkt nu dat er maar twee normale magische zeshoeken zijn: de triviale van orde 1 en, veel interessanter, die van orde 3. Nog merkwaardiger is dat de oplossing voor orde 3 uniek is, op spiegelingen en rotaties na.



De eerste die naar deze zeshoek verwees (en mogelijk ontdekte) was Ernst von Haselberg in 1887. Ondertussen zijn er al grotere magische zeshoeken gevonden, die weliswaar uit opeenvolgende getallen bestaan, maar dan niet starten bij 1. Het huidige record staat op naam van Arsen Zahray, die via computerberekeningen op 22 maart 2006 deze zeshoek van orde 7 vond, bestaande uit  $\{2, 3, \dots, 128\}$ .



## 281 Siamese methode

De Siamese methode of de methode van de la Loubère maakt het opstellen van een magisch vierkant waarvan de orde oneven is, zeer eenvoudig. Ze werd in 1688 in Frankrijk geïntroduceerd door wiskundige en diplomaat Simon de la Loubère, toen hij terugkeerde uit Siam.

1. Kies eerst een rekenkundige rij (normaliter 1, 2, 3, 4, 5, 6, ...).
2. Vul het eerste getal in in het middelste hokje van de bovenste rij van het vierkant.
3. Elk volgende getal wordt indien mogelijk ingevuld in het hokje rechtsboven het vorige hokje ( $\nearrow$ ).
  - (a) Wanneer een hokje wordt bereikt dat buiten het vierkant ligt, vul dan die aan de tegenoverliggende kant in (alsof het vierkant een torus zou zijn).

(b) Wanneer een hokje wordt bereikt dat reeds ingevuld is, keer dan terug en vul in plaats daarvan het hokje eronder in ( $\downarrow$ ).

4. Blijf deze vorige stap herhalen totdat het hele vierkant gevuld is; dit geeft dan een magisch vierkant.

Toegepast op een  $3 \times 3$ -rooster geeft deze de Lo-Shu. Op een  $5 \times 5$ -rooster:

		1		
	5			
4				
				3
			2	

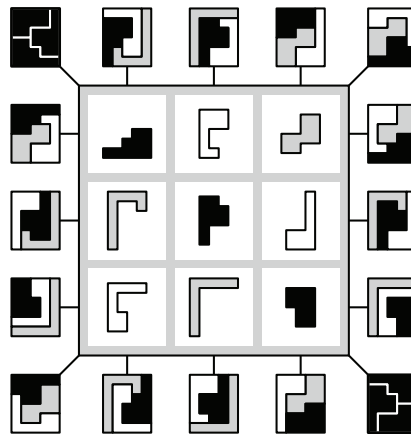
		1	8	
	5	7		
4	6			
10				3
			2	9

...

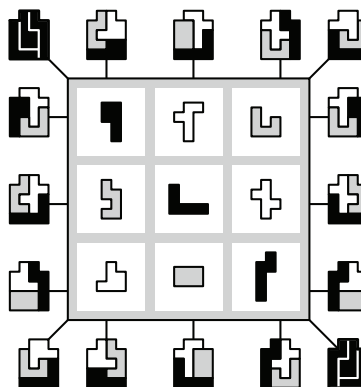
17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

## 282 Geomagische vierkanten

Door het concept van het magische vierkant op een compleet andere manier te beschouwen, introduceerde Lee Sallows recentelijk de geomagische vierkanten. Hierbij is er geen sprake van een cijferrooster met constante som in rijen, kolommen en diagonalen, maar bevat het rooster geometrische figuren, die per rij, kolom of diagonaal gecombineerd kunnen worden tot eenzelfde meetkundige “constante”.



Tallose aansprekende voorbeelden staan in de galerij van Lee Sallows, <http://www.geomagicsquares.com>. Hier geeft hij ook een introductie over en een formele definitie van de geomagische vierkanten.





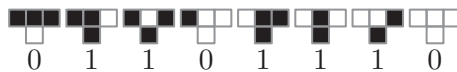


# XIII Cellulaire automaten

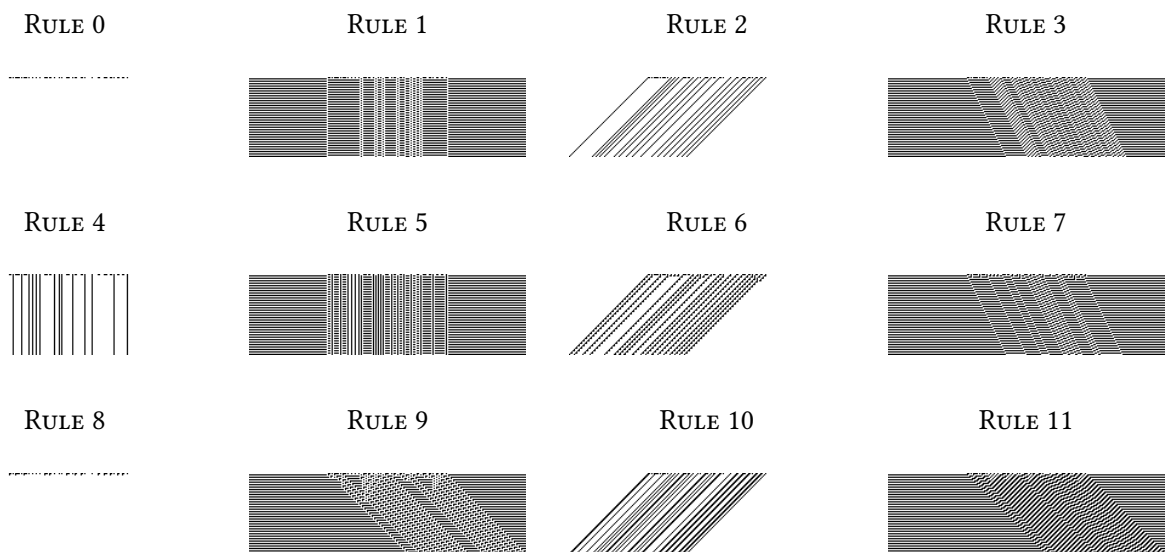
## 283 Elementaire cellulaire automaten

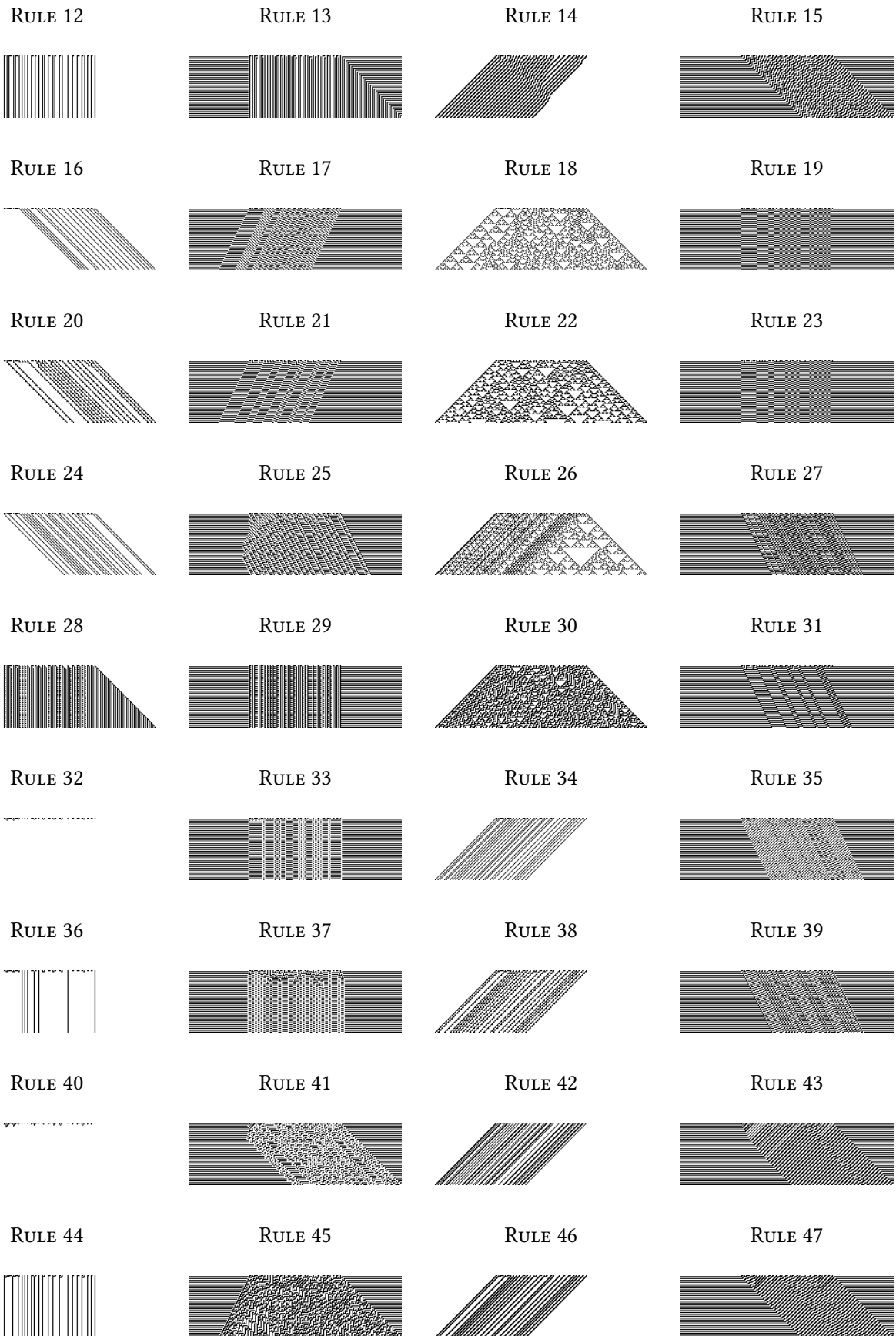
In deze familie ééndimensionale cellulaire automaten zijn er twee mogelijke toestanden en wordt de evolutie van elke cel bepaald a.d.h.v. zijn twee onmiddellijke buurcellen. Dit maakt ze tot een van de eenvoudigste modellen.

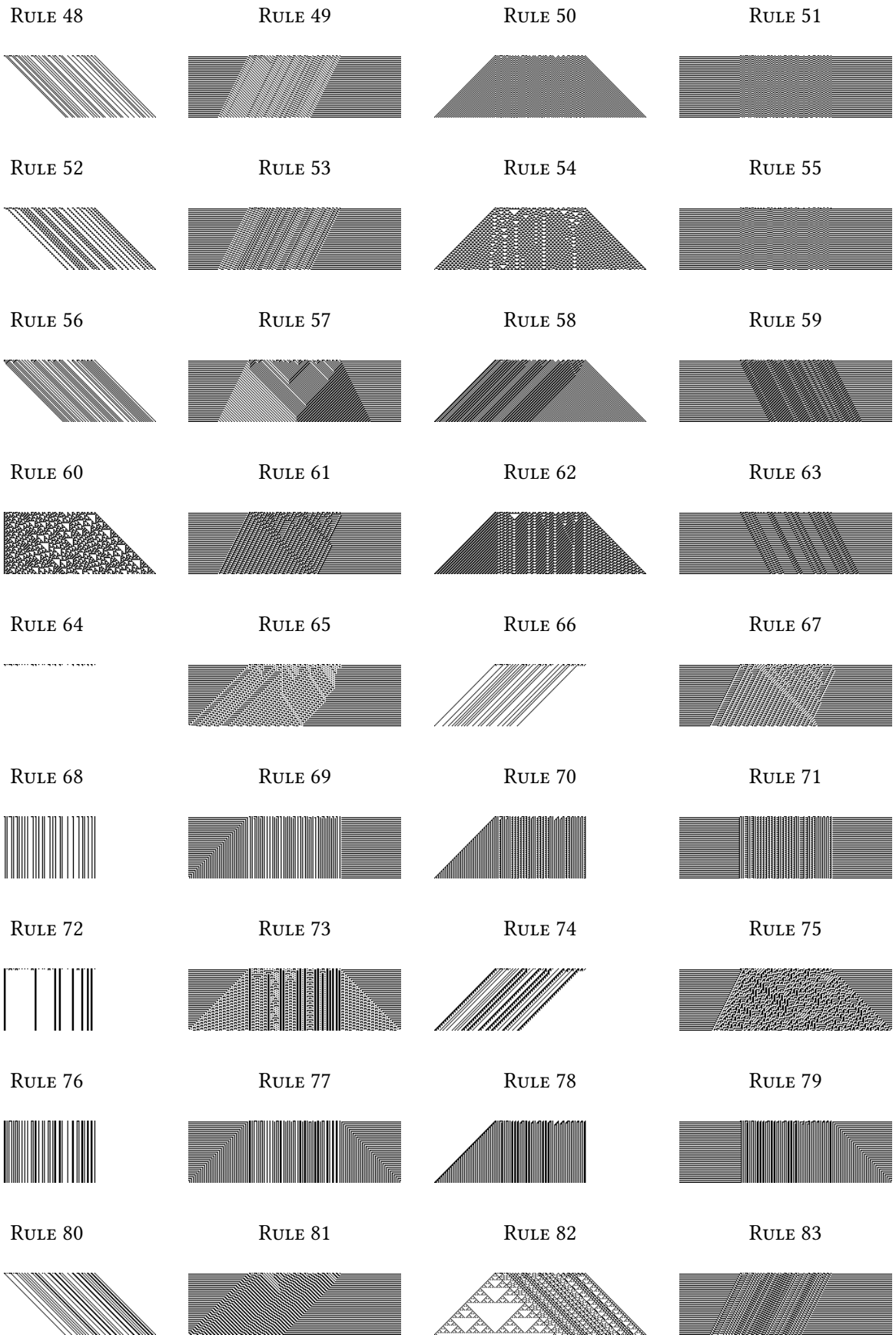
Elke automaat gebruikt acht regels: één voor elke mogelijke combinatie van buurcellen. In combinatie met twee mogelijke toestanden van de cel geeft dit  $2^8 = 256$  elementaire automaten. Ze werden aandachtig bestudeerd door Stephen Wolfram, die er in een artikel uit 1983 en in zijn *A New Kind of Science* ook een nomenclatuur voor gaf, sindsdien bekend als Wolframcode. Associeer de toestand van een cel met 0 of 1, interpreteer de acht buurcelconfiguraties als binaire getallen (dalend gerangschikt), ken elke configuratie een nieuwe toestand toe (0 of 1) en lees het gevormde binaire getal af. Het voorbeeld hieronder wordt zo RULE 110 gedoopt. Deze ziet er vrij onschuldig uit, maar is in feite in staat tot universele berekening!

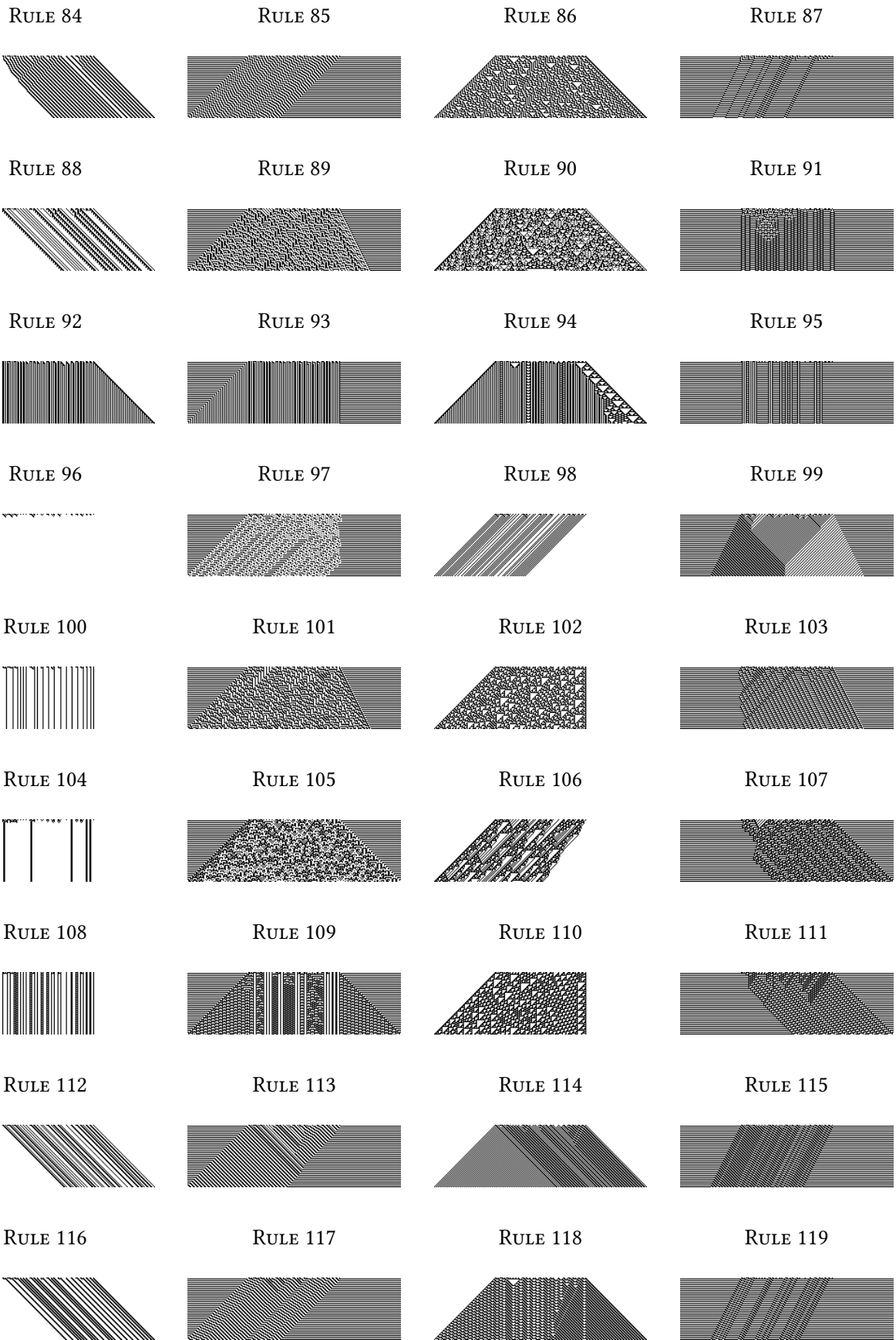


De begintoestand en de regels van de automaat zijn volledig determinerend voor de evolutie ervan. Hieronder worden alle 255 regels geïllustreerd, vertrekkende van enkele zwarte cellen als begintoestand. Wezenlijk zijn er slechts 88 fundamenteel verschillende: automaten die elkaars spiegelbeeld zijn of waarin de rol van 0 en 1 verwisseld is, vertonen hetzelfde gedrag, maar worden als verschillend beschouwd. De 64 regels die hetzelfde zijn als hun spiegelvorm, heten amfichiraal. Merk op dat de automaten zelf ééndimensionaal zijn; het is gebruikelijk elke nieuwe generatie als een nieuwe rij onder de vorige te zetten.



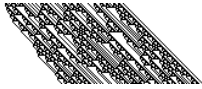




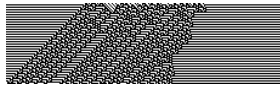




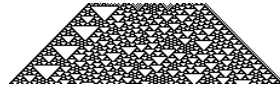
RULE 120



RULE 121



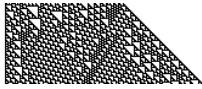
RULE 122



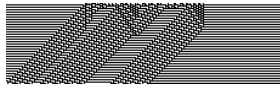
RULE 123



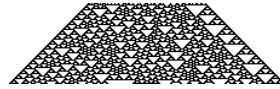
RULE 124



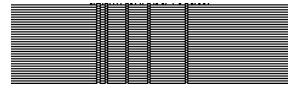
RULE 125



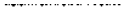
RULE 126



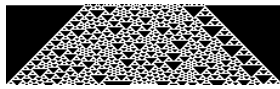
RULE 127



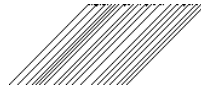
RULE 128



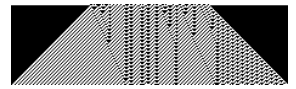
RULE 129



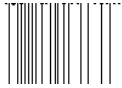
RULE 130



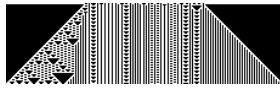
RULE 131



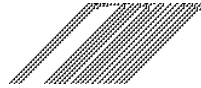
RULE 132



RULE 133



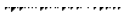
RULE 134



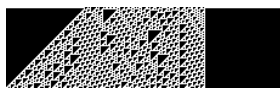
RULE 135



RULE 136



RULE 137



RULE 138



RULE 139



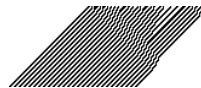
RULE 140



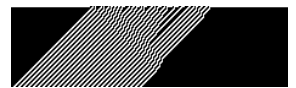
RULE 141



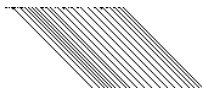
RULE 142



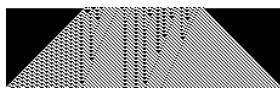
RULE 143



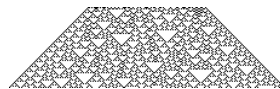
RULE 144



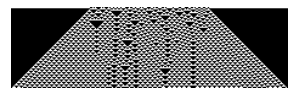
RULE 145



RULE 146



RULE 147



RULE 148



RULE 149



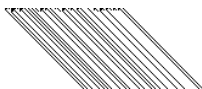
RULE 150



RULE 151



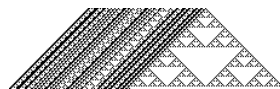
RULE 152



RULE 153



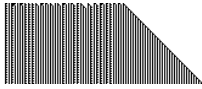
RULE 154



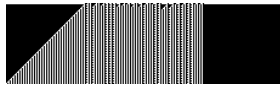
RULE 155



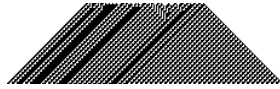
RULE 156



RULE 157



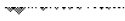
RULE 158



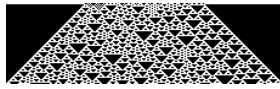
RULE 159



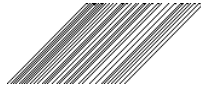
RULE 160



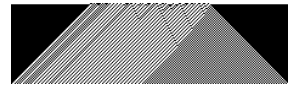
RULE 161



RULE 162



RULE 163



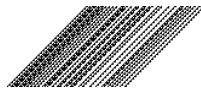
RULE 164



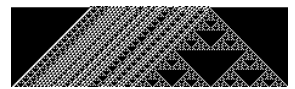
RULE 165



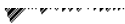
RULE 166



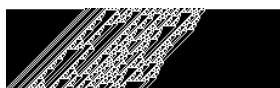
RULE 167



RULE 168



RULE 169



RULE 170



RULE 171



RULE 172



RULE 173



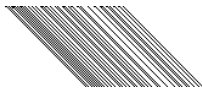
RULE 174



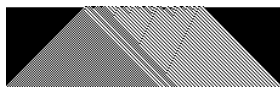
RULE 175



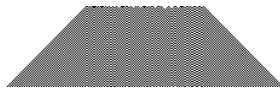
RULE 176



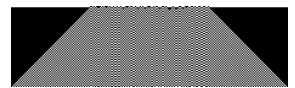
RULE 177



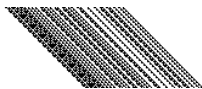
RULE 178



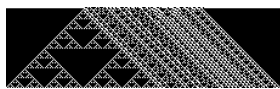
RULE 179



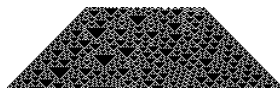
RULE 180



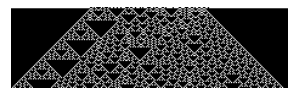
RULE 181



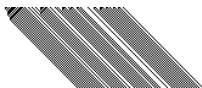
RULE 182



RULE 183



RULE 184



RULE 185



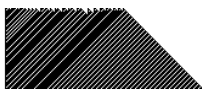
RULE 186



RULE 187



RULE 188



RULE 189

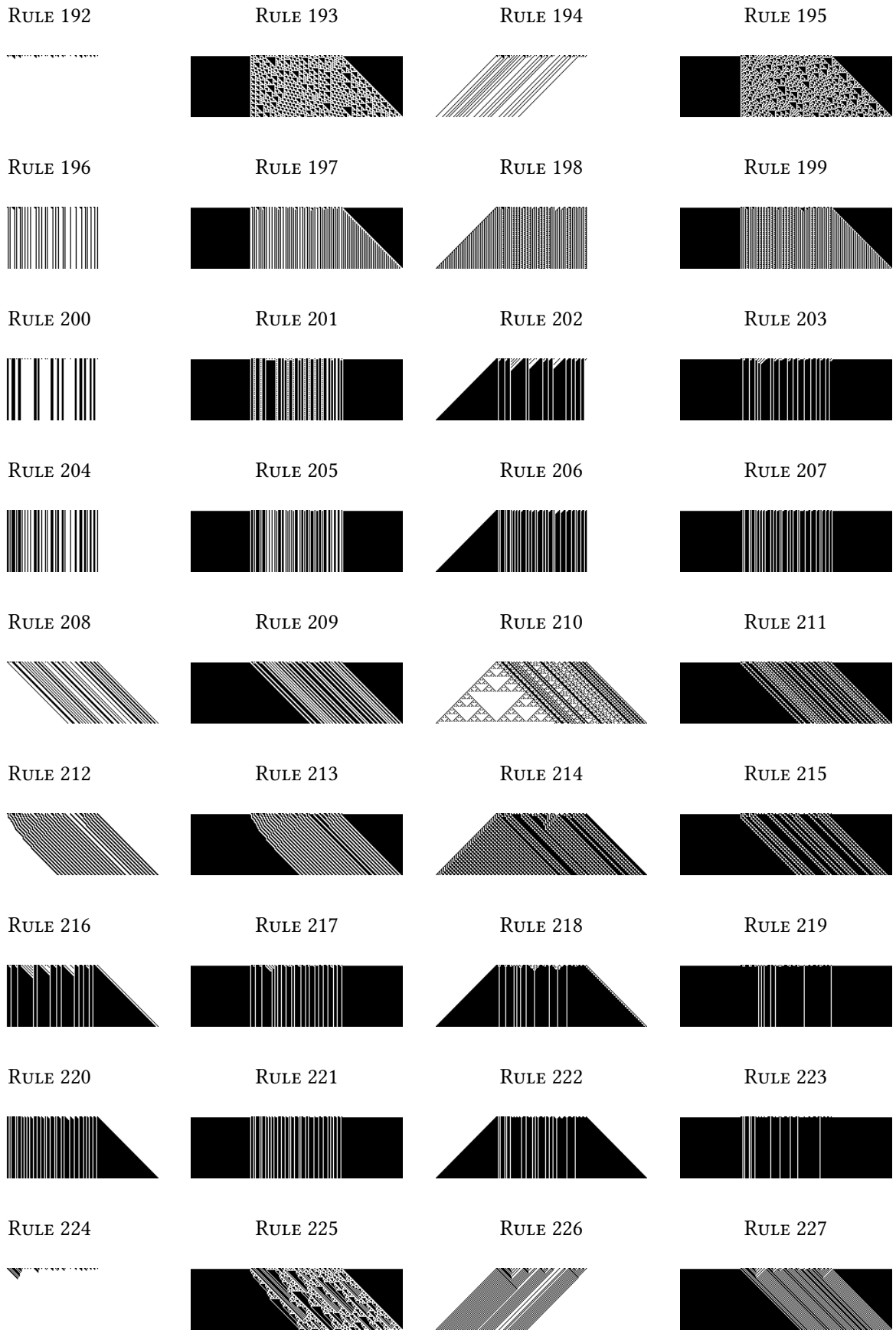


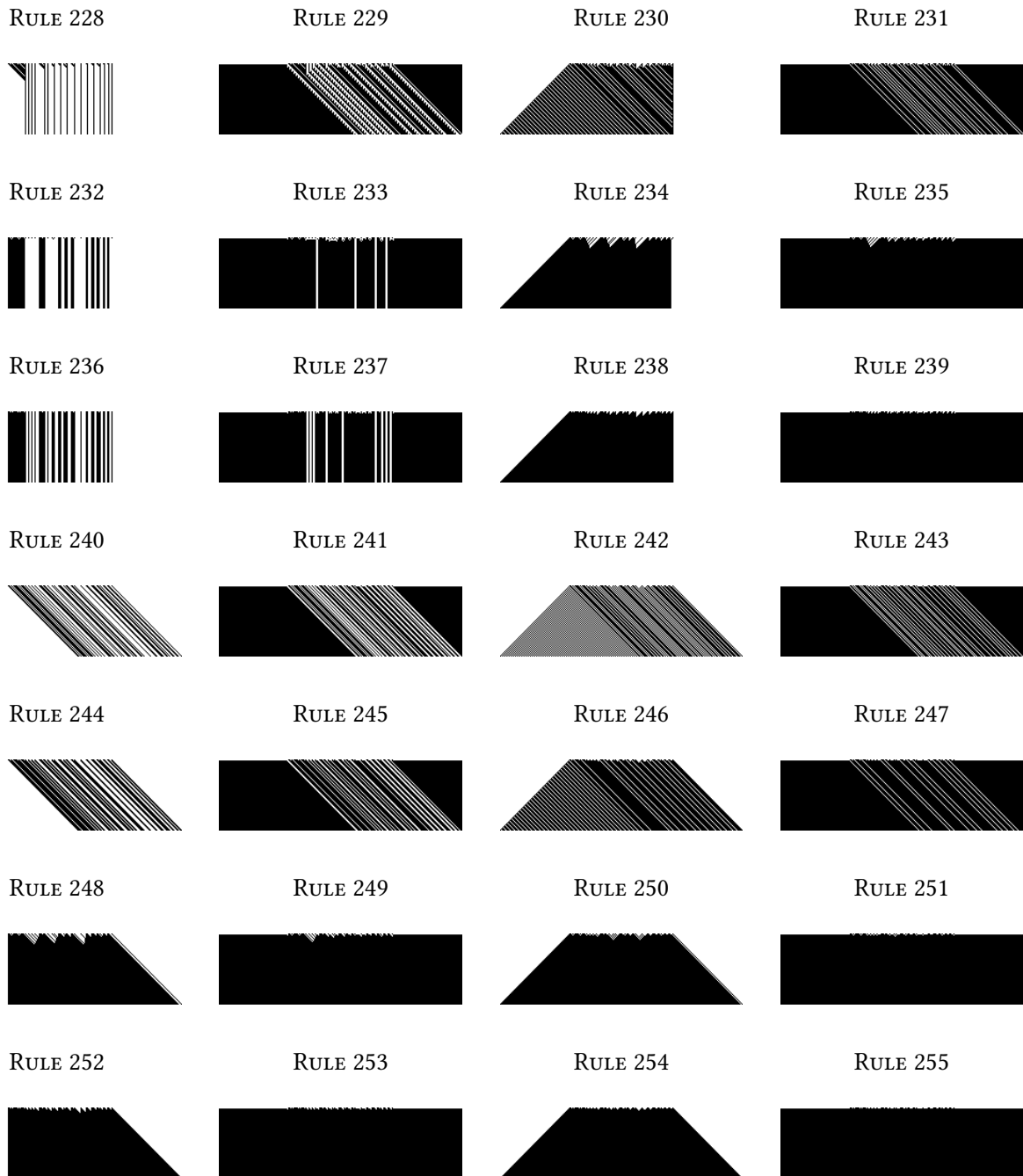
RULE 190



RULE 191

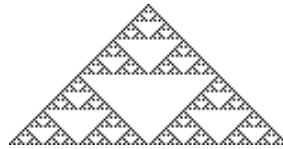




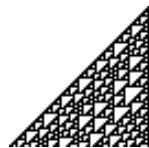


Merk op dat nogal wat regels de driehoek van Sierpiński genereren (zie 201, 160), en vertrekkende vanuit een enkel zwarte cel zouden nog meer regels Sierpińskidriehoeken doen ontstaan, zoals RULE 90 hieronder. Zoals te zien zijn helaas niet alle elementaire cellulaire automaten bijster interessant; Wolfram classificeerde ze in vier categorieën (de Wolframklassen):

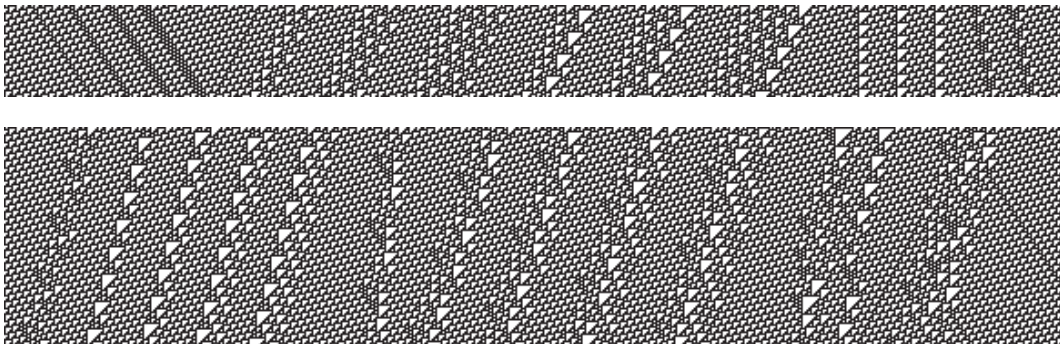
- **Klasse 1:** willekeurige begintoestanden evolueren snel naar een stabiele toestand; initiële chaos verdwijnt.
- **Klasse 2:** willekeurige begintoestanden evolueren snel naar stabiele of oscillerende patronen; lokale wijzigingen blijven lokaal.
- **Klasse 3:** willekeurige begintoestanden evolueren naar pseudorandom (chaotisch) gedrag. Stabiele patronen worden vernietigd door omliggend ruis. Lokale wijzigingen kunnen zich heel het patroon doorzetten.
- **Klasse 4:** willekeurige begintoestanden evolueren naar structuren die op complexe manieren interageren, terwijl er ook lokale structuren ontstaan die voor langere periode stabiliseren.



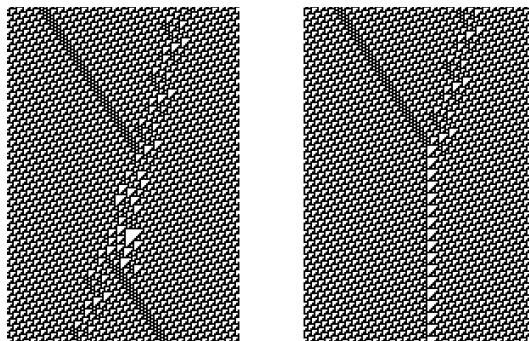
Hoewel elementaire cellulaire automaten er eenvoudig uitzien, zijn ze tot indrukwekkende prestaties in staat. Wolfram vermoedde sinds 1985 dat automaten van klasse 4 universeel zijn en elke mogelijke berekening kunnen simuleren. Voor RULE 110 werd dit inderdaad aangetoond, door Matthew Cook, assistent van Wolfram, tijdens de CA98 conferentie op het Sante Fe Institute, net voordat *A New Kind of Science* werd uitgegeven. Wolfram Research startte daarop een juridische zaak op basis van het verbreken van Cooks geheimhoudingsovereenkomst, waardoor publicatie van het bewijs voor twee jaar geblokkeerd werd. In 2004 werd het officiële bewijs uitgegeven in Wolframs tijdschrift *Complex Systems*.



De Turing-compleetheid van Rule 110 werd onderbouwd door aan te tonen dat deze een *cyclic tag system* kan simuleren, waarvan gekend is dat ze universeel is. Cook construeerde een aantal repeterende lokale patronen (*spaceships*) en combineerde die om hun interacties uit te buiten voor berekeningen. De mogelijke spaceships in het systeem staan hieronder:



Deze patronen kunnen zodanig geplaatst worden dat ze met elkaar interageren of juist niet, wat van fundamenteel belang is in slechts één dimensie en cruciaal in Cooks bewijs.

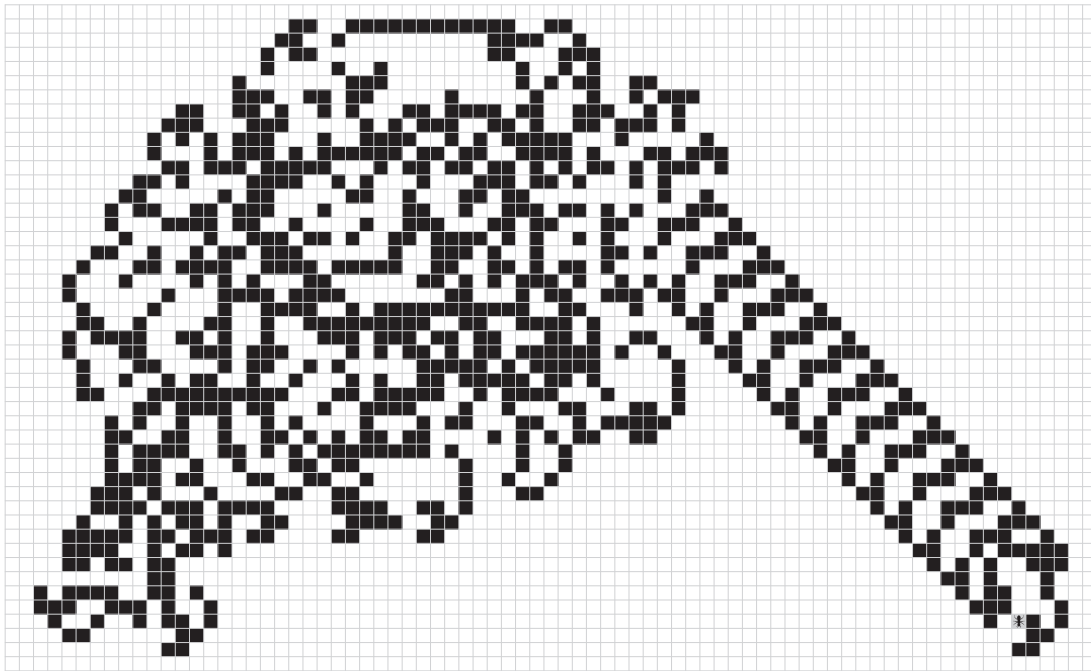


## 284 Mier van Langton

De mier van Langton is een tweedimensionale Turingmachine (zie ??, blz. ??), beschreven door Chris Langton in 1986, met zeer eenvoudige regels maar ingewikkeld gedrag. De mier beweegt zich voort op een vierkant rooster, waarvan de cellen wit of zwart kunnen zijn en van kleur veranderen naargelang de mier erop loopt:

- Als de mier op een zwarte cel staat, draait die rechtsaf en beweegt die één hokje vooruit.
- Als de mier op een witte cel staat, draait die linksaf en beweegt die één hokje vooruit.
- Wanneer de mier een hokje verlaat, keert de kleur ervan om.

In het gebruikelijke geval wordt de mier op een volledig wit veld geplaatst. Tijdens de eerste paar honderd stappen scheidt de mier eenvoudige patronen, vaak ook symmetrische, maar daarna ontstaat er een groot chaotisch patroon en uiteindelijk, na zo'n 10.000 stappen, legt de mier een "snelweg" aan: een patroon van 104 stappen dat zich eindeloos voortzet. Deze is duidelijk te zien op de onderstaande tekening.



Simulaties doen vermoeden dat Langtons mier er uiteindelijk vanuit elke willekeurige eindige startconfiguratie via zo'n snelweg vandoor gaat, zelfs als meerdere mieren met elkaar interageren. Dit is nog niet bewezen voor alle constellaties; men weet enkel met zekerheid dat het traject van de mier onbegrensd is, onafhankelijk van de beginconfiguratie, wat bekend staat als de stelling van Cohen-Kung.

In 2000 construeerden Anahí Gajardo, Jarkko Kari en Andrés Moreira met een enkele mier een volledig booleaans circuit, met operationele AND-, OR- en NOT-poorten, waarmee ze bewezen dat de mier van Langton in theorie een volledig functionele computer kan simuleren en dus Turing-compleet is.

## 285 Game of Life

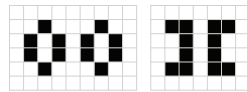
John Conways Game of Life is veruit de populairste cellulaire automaat. Game of Life is ontstaan nadat Conway experimenteerde met verschillende regels om een goede balans te vinden tussen leven en dood. Het systeem werkt met generaties op een oneindig tweedimensionaal rooster, waarvan de cellen dood (wit) of levend (zwart) kunnen zijn en acht buurcellen hebben. De volgende regels bepalen de status van een cel uit generatie  $t$  op de volgende generatie  $t + 1$ :

- **Uitsterving:** een levende cel met minder dan twee levende buurcellen in  $t$ , sterft in  $t + 1$ .
- **Overleving:** een levende cel met twee of drie levende buurcellen in  $t$ , overleeft in  $t + 1$ .
- **Overbevolking:** een levende cel met meer dan drie levende buurcellen in  $t$ , sterft in  $t + 1$ .
- **Geboorte:** een dode cel met precies drie levende buurcellen in  $t$ , leeft in  $t + 1$ .
- Cellen die niet veranderen door één van bovenstaande regels, wijzigen niet.

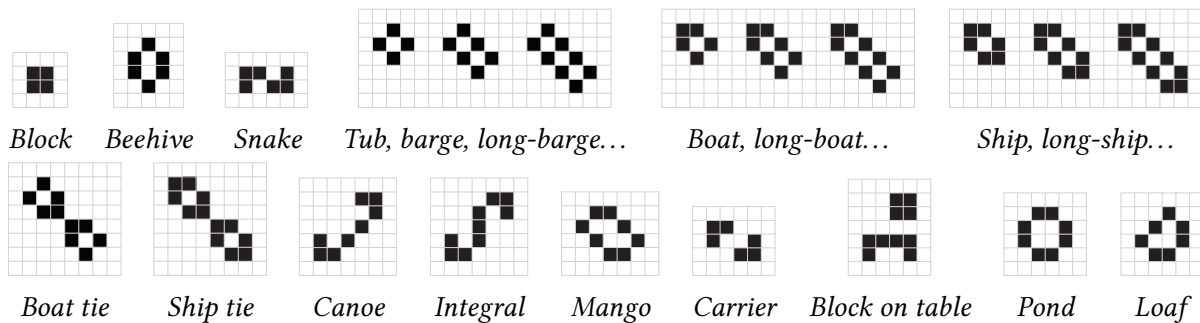
Met deze eenvoudige regels kunnen de meest fantastische patronen gecreëerd worden. Er zijn verschillende statische *still lifes* bekend, periodieke *oscillators*, zich verplaatsende *spaceships*, *guns* die steeds weer nieuwe spaceships produceren, *puffer trains* die een (statische) rookwolk achterlaten, *rakes* die zichzelf verplaatsen én spaceships uitzenden, *breeders* die guns, puffers of rakes produceren die dan zelf weer een derde patroon afvuren, *eaters* die spaceships vernietigen en daarna naar hun oorspronkelijke staat terugkeren, *reflectors* die spaceships van richting doen veranderen...

### Still lifes.

*Still lifes*, statische patronen die geen verdere evolutie vertonen, kunnen worden gecombineerd door twee patronen naast elkaar te zetten. Een *pseudo still life* bestaat uit twee of meerdere van zo'n niet-interagerende statische subpatronen, bij een *strict still life* zijn de subpatronen van elkaar afhankelijk voor hun stabiliteit. Het onderscheid is niet altijd eenvoudig (zie hieronder, het linkerpatroon is pseudo, het rechterpatroon strict). Toch is het mogelijk een in polynomiale tijd werkend algoritme te schrijven dat bepaalt tot welke categorie een gegeven still life behoort (zie 322, blz. 313).



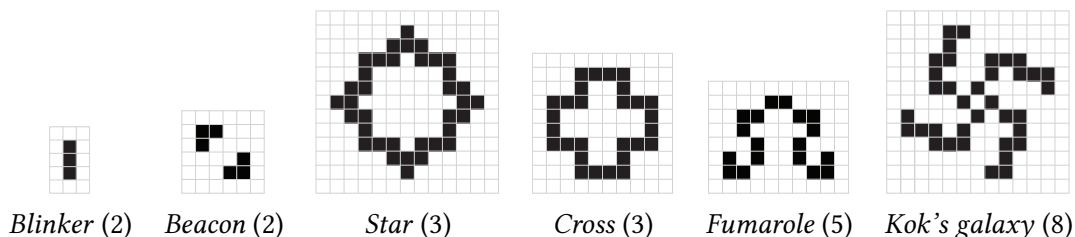
Hieronder volgt een overzicht van de meest voorkomende still lifes. Het aantal mogelijke statische patronen met  $n$  levende cellen vormt rij OEIS A019473.



### Oscillators.

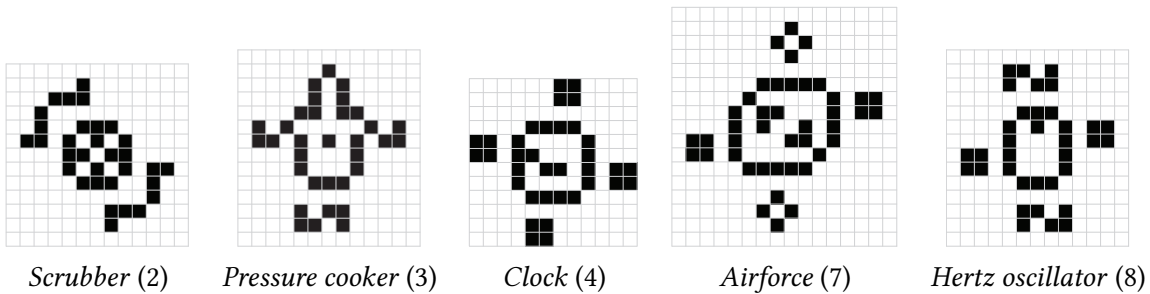
*Oscillators* zijn patronen die identiek zijn aan het beginpatroon na een aantal generaties. Het minimum aantal generaties waarna het patroon herhaald wordt, heet de periode ervan.

Men vermoedt dat er oscillators voor gelijk welke periode bestaan, hoewel er nog geen bekend zijn voor periode 19, 23, 38, 41, 43 en 53. Daarnaast zoekt men ook nog naar een niet-triviale oscillator met periode 34; de enige gekende zijn opgebouwd uit niet-interagerende oscillators van periode 2 en 17.



### Billiard tables.

Een speciaal soort oscillators zijn zogenaamde *billiard tables*. De *rotor* van een oscillator verwijst naar de cellen die op een bepaald punt in de evolutie veranderen, terwijl de *stator* de andere cellen aanduidt die de hele tijd in leven blijven. Voor een billiard table wordt de rotor nu volledig omvat door de stator. Billiard tables hebben over het algemeen niet veel belang, omdat ze geen bruikbare interacties toelaten.



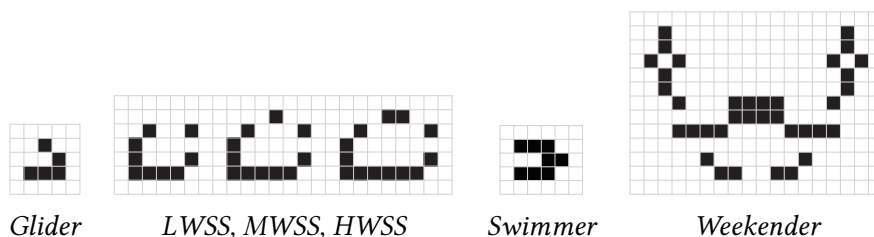
Bij een oscillator heet de proportie cellen die van status veranderen (de verhouding van het aantal cellen in de rotor op het totaal aantal cellen), de volaliteit.

### Spaceships.

*Spaceships*, patronen die na een aantal generaties in dezelfde configuratie verschijnen maar op een andere positie, spelen een cruciale rol in de Game of Life omdat ze kunnen gebruikt worden om informatie door te sturen. Hun snelheid wordt uitgedrukt in  $c$ , de metaforische lichtsnelheid die gelijkstaat aan één hokje per generatie. Zo betekent een snelheid van  $\frac{c}{4}$  dat er vier generaties nodig zijn om een spaceship één hokje op te schuiven. Algemeener kan de snelheid  $v$  van een spaceship dat na  $n$  generaties over  $(x, y)$  verplaatst wordt, bepaald worden met de volgende formule:

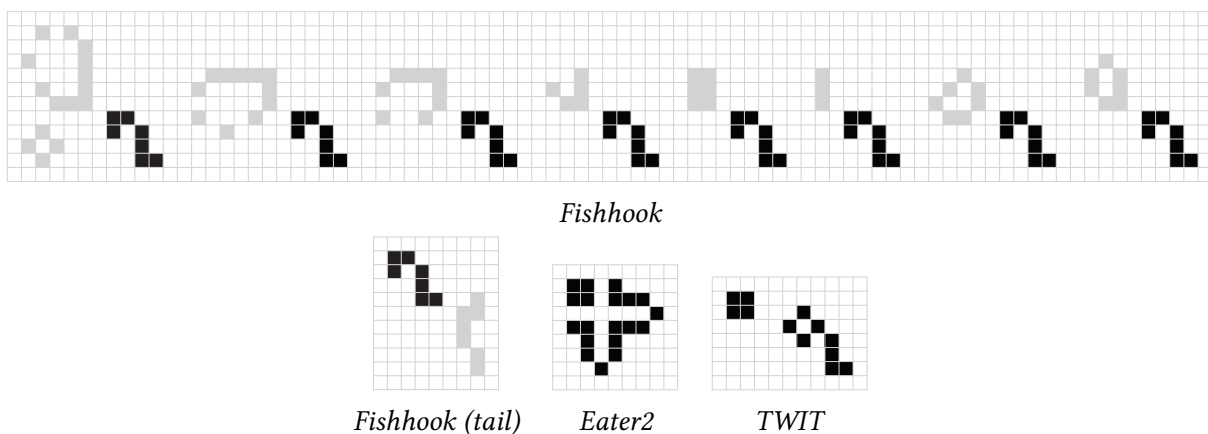
$$v = \frac{\max(|x|, |y|) \cdot c}{n}$$

De meest frequente spaceships zijn de *glider* en de *LWSS* (light-weight spaceship). Er bestaan enkele varianten van deze laatste: de *MWSS* (medium-weight) en *HWSS* (heavy-weight). Ook spaceships met diverse snelheden worden bestudeerd, zoals de *weekender* waarvoor  $v = \frac{2c}{7}$ .



### Eaters en rocks.

Still lifes die de capaciteit hebben met bepaalde patronen (meestal spaceships) te interageren zonder zelf permanente schade op te lopen, heten *eaters*. De bekendste is de *fishhook*, die verschillende objecten kan consumeren. Wanneer een eater doorheen het proces helemaal niet wijzigt, zelfs niet tijdelijk, heet die een *rock*. De staart van de fishhook kan beschouwd worden als een rock. Aanpassingen aan de fishhook kunnen gliders uit meerdere richtingen absorberen, zoals de *Tub-with-tail eater* of *TWIT*. *Eater2* is een andere eater, die gliders uit een positie kan consumeren waarin een fishhook vernietigd zou worden.

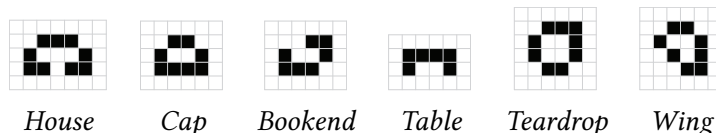




Net als spaceships zijn eaters van vitaal belang in complexe constructies, omdat ze achtergelaten afval kunnen opruimen of een datastroom van spaceships reguleren.

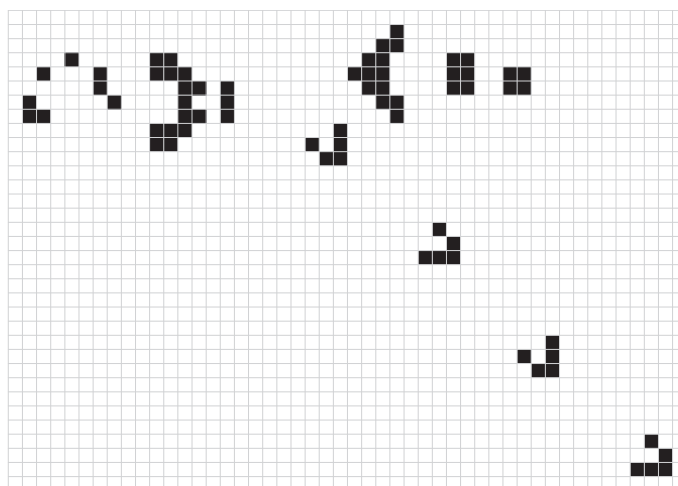
### Induction coils.

*Induction coils* zijn objecten die gebruikt worden om andere patronen te stabiliseren zonder ze aan te raken. De billiard table Airforce bijvoorbeeld, werkt dankzij de twee blocks en twee tubs die errond staan. Zowel still lifes als oscillators kunnen als induction coil gebruikt worden, maar er zijn er ook die op zich niet stabiel zijn, zoals die hieronder.



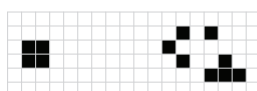
### Guns en puffers.

*Guns* zijn patronen die zichzelf herhalen zoals oscillators, maar ook met vaste regelmaat spaceships uitzenden. Hun bestaan impliceert dat eindige configuraties uiteindelijk kunnen evolueren in configuraties zonder begrensd aantal levende cellen, wat John Conway eerst onmogelijk achtte. De eerste (en thans kleinst bekende) gun werd geconstrueerd door Bill Gosper in 1970, die daarmee \$50 won van Conway.

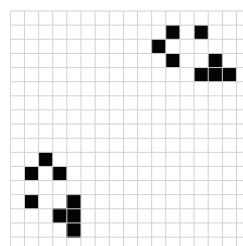


*Gosper gliding gun*

Een andere manier om aan te tonen dat oneindige groei mogelijk is, is door de *puffer trains* of *puffers*: patronen die zelf over het veld bewegen zoals spaceships, maar daarbij een rookwolk van still lifes en oscillators achterlaten. Hieronder wordt een eenvoudig patroon afgebeeld dat evolueert naar de *block-laying switch engine*, die een trap van blocks bouwt. *Noah's ark* komt aan zijn naam door de variatie aan achtergelaten puin: 42 blocks, 40 blinkers, 22 beehives, acht loaves, vier gliders, twee boats, twee block on tables, twee long boats, één ship en één beacon.



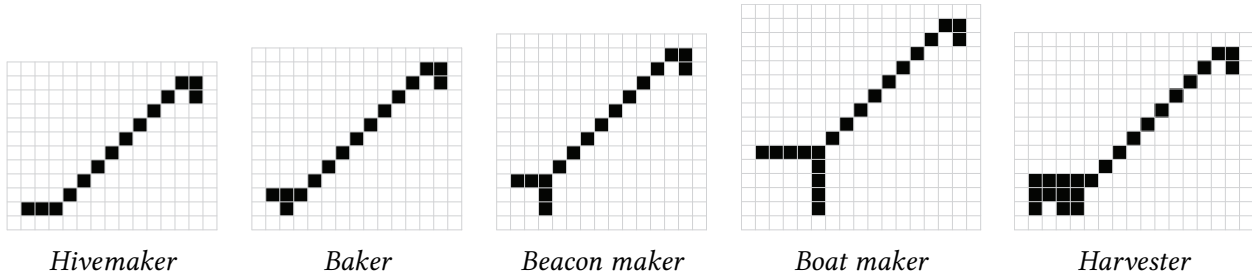
*Block-laying switch engine (predecessor)*



*Noah's ark*

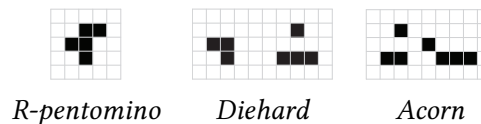
### Wicks en fuses.

*Wicks* zijn lange, in één richting herhaalde, stabiele of oscillerende patronen die “opbranden” als een uiteinde wordt aangestoken. De interessantste wicks zijn diegenen die een ordelijk spoor of helemaal geen bijproducten achterlaten, zoals deze hieronder. Eenmaal aangestoken spreekt men ook van *fuses*. Zogenaamde *wick stretchers* kunnen segmenten van wicks uitbreiden.



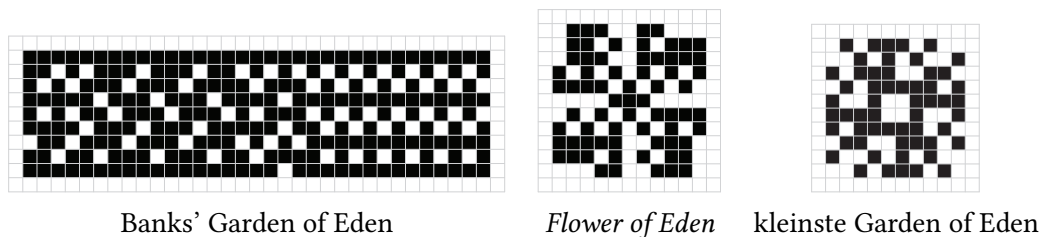
### Methuselahs.

*Methuselahs* zijn kleine initiële patronen die een relatief groot aantal generaties nodig hebben om te stabiliseren. De *R-pentomino* hieronder bestaat uit slechts vijf cellen, maar wordt pas na 1103 generaties stabiel. De *diehard* sterft volledig uit, maar pas na 130 generaties, wat het maximum is voor zeven cellen. De eveneens zevencellige *acorn* heeft 5206 generaties nodig om te stabiliseren, tijdens dewelke hij 13 gliders uitstuurt. Methuselahs worden vernoemd naar de grootvader van Noach, Methuselah, die volgens de Bijbel 969 jaar oud werd.



### Garden of Eden.

Een *Garden of Eden* is een patroon dat onmogelijk kan ontstaan uit evolutie van een bepaalde andere configuratie. Ze worden vernoemd naar de Bijbelse Tuin van Eden, die slechts door een Schepper, vanuit het niets, gecreëerd kan worden. De allereerste Garden of Eden werd gevonden in 1971 door Roger Banks en heeft afmetingen van  $9 \times 33$ . Ondertussen is bewezen dat er geen Gardens of Eden bestaan kleiner dan  $7 \times 7$ ; de thans kleinst bekende heeft afmetingen  $10 \times 10$  en bestaat uit 56 levende cellen.



Er geldt nog een mooie stelling omtrent zulke Gardens of Eden, die injectiviteit en surjectiviteit op cellulaire automaten definieert en met elkaar in verband brengt.

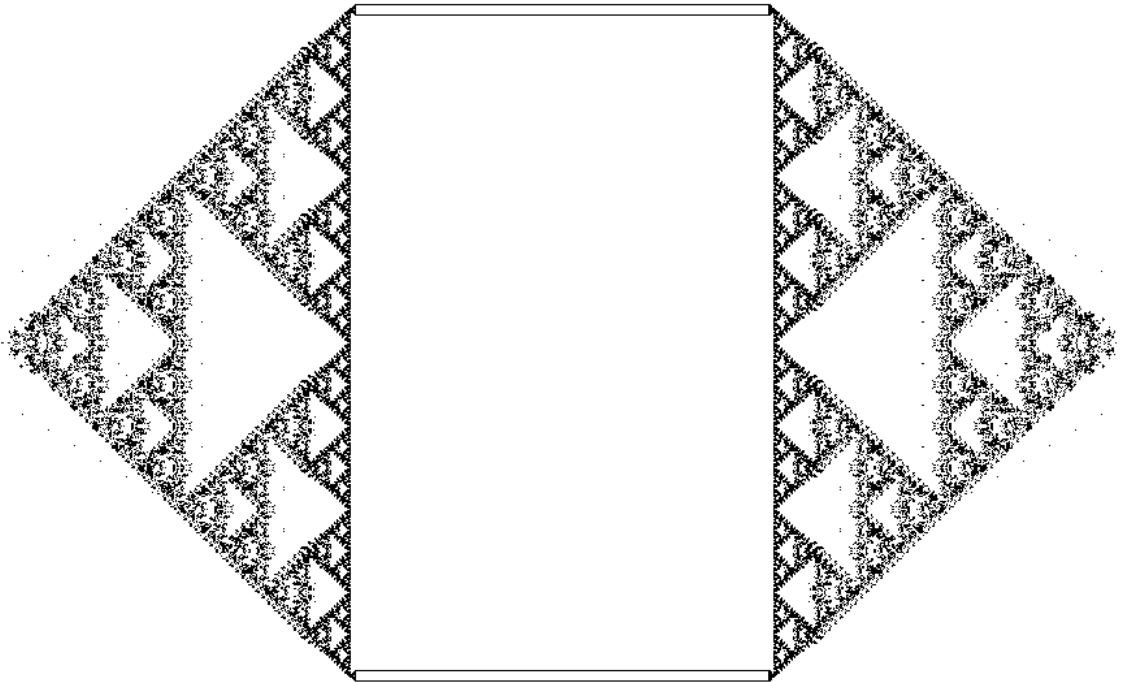
- **Injectiviteit:** geen twee verschillende, eindige patronen zijn de volgende generatie identiek.
- **Surjectiviteit:** elk mogelijk patroon is de evolutie van een bepaalde voorloper (*predecessor*)

Bemerk dat Gardens of Eden dus niet voorkomen in surjectieve automaten. De stelling van de Garden of Eden, bewezen door Edward Moore en John Myhill begin de jaren 60, stelt dat een cellulaire automaat injectief is als en slechts als ze surjectief is. Daaruit volgt dat de Game of Life, die duidelijk niet injectief is (zie hieronder), zeker een Garden of Eden bevat; het bestaan was dus al bekend vóór zo'n configuratie effectief gevonden werd.

$$\left\{ \begin{array}{l} \begin{array}{|c|c|c|} \hline \blacksquare & \blacksquare & \square \\ \hline \end{array} & \textit{Preblock} & \Rightarrow & \begin{array}{|c|c|c|} \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \end{array} & \textit{Block} \\ \begin{array}{|c|c|c|} \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \end{array} & \textit{Grin} & \Rightarrow & \begin{array}{|c|c|c|} \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \end{array} & \textit{Block} \end{array} \right.$$

### Complexe constructies.

Met behulp van deze patronen en hun eigenschappen kunnen complexere constructies gemaakt worden. Dit patroon construeert de driehoek van Sierpiński (zie 201, blz. 160):



Een tweede mooi voorbeeld is *Primer*, die een stroom van gliders afvuurt maar tevens de  $n^{\text{de}}$  glider vernietigt wanneer  $n$  een samengesteld getal is. De aan- of afwezigheid van gliders in de stroom duidt dus aan of een getal priem is of niet. Deze nieuwe versie van *Primer* werd gemaakt door Jason Summers in 2010:



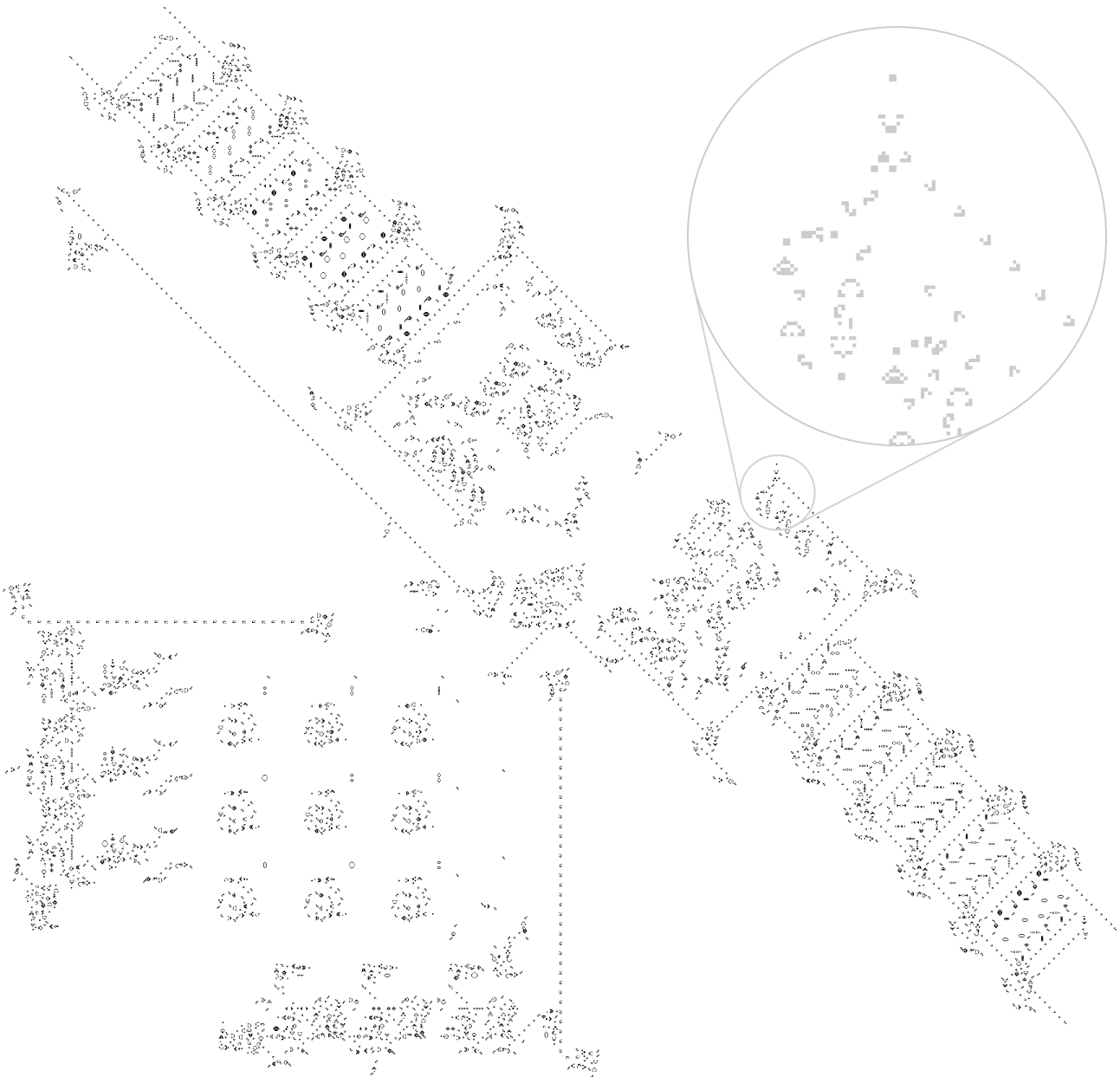
*Primer* kan worden aangepast zodat die alleen tweelingpriemgetallen (zie 48, blz. 37), Fermatpriemgetallen (zie 47, blz. 36) of Mersennepriemgetallen (zie ??, blz. ??) produceert.

Naast constructies die louter één bepaalde taak uitvoeren, kan in Game of Life een universele computer worden gebouwd, wat betekent dat Game of Life in theorie tot elke mogelijke computerberekening in staat is. Uit guns, gliders en eaters kunnen in Life logische poorten worden opgebouwd, en de opslag van registers kan gesimuleerd worden met een *sliding block memory*: een constructie waarin een stroom gliders een block één cel verder kan

duwen of terug kan trekken. Deze componenten samenstellend bewees John Conway in 1982 dat zijn Game of Life wel degelijk Turing-compleet is (zie ??, blz. ??). Een verbeterde versie van Conways sliding block memory werd in 1990 gefabriceerd door Dean Hickerson:



Aangespoord door Conways bewijs verwezenlijkte Paul Rendell in 2000 een directe implementatie van een Turingmachine, hieronder afgebeeld. Na deze gigantische prestatie werden er nog verbeteringen doorgevoerd ter vorming van bijvoorbeeld een Minskyregistermachine (equivalent met een Turingmachine, maar eindig doordat die geen oneindige band vereist).



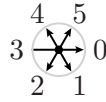
De uitgebreide wereld van Game of Life geeft aanleiding tot een weelderige woordenschat, onder meer terug te vinden op <http://www.conwaylife.com/wiki> of [http://www.argentum.freemove.co.uk/lex\\_home.htm](http://www.argentum.freemove.co.uk/lex_home.htm). Op het internet zijn tevens talrijke programma's te vinden (zoals Golly) om de Game of Life op de computer te simuleren.

## 286 Wormen van Paterson

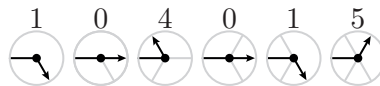
Begin jaren 70 werkten Mike Paterson en John Conway dit model uit om het gedrag van bepaalde prehistorische wormen te simuleren. De wormen worden geleid door eenvoudige regels, maar vertonen zeer complex gedrag; in feite is het lot van één worm zelfs nog steeds onbekend. Conways eerste wormen werden op een rechthoekig rooster gezet, maar dit leidde tot slechts drie, nogal saaie verschillende soorten. Paterson beschouwde een driehoekig rooster, waarop interessantere wormen leefden. In 1973 besprak Martin Gardner het systeem besproken in zijn *Mathematical Games*. Sindsdien gaven computersimulaties spectaculaire afbeeldingen voor de ingewikkeldste wormen.

De worm start op een punt ergens in een oneindig groot, driehoekig rooster. Hij beweegt langs één van de zes rasterlijnen uit dat punt vertrekkende en komt aan op een nieuw punt. De worm beslist hier op basis van

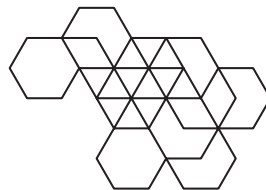
de verdeling van doorkruiste en niet-doorkruiste wegen welke richting hij uitgaat: bij een verdeling die hij al eens tegengekomen is, gaat hij dezelfde richting uit als de eerdere keer, bij een nieuwe verdeling kiest die een nieuwe richting. Wanneer er slechts één nog niet doorkruiste richting beschikbaar is, kiest hij natuurlijk die ene richting. De worm sterft wanneer hij op een kruispunt terechtkomt zonder nieuwe niet-doorkruiste richtingen. De richtingen worden (relatief t.o.v. de positie van de worm) als volgt genummerd:



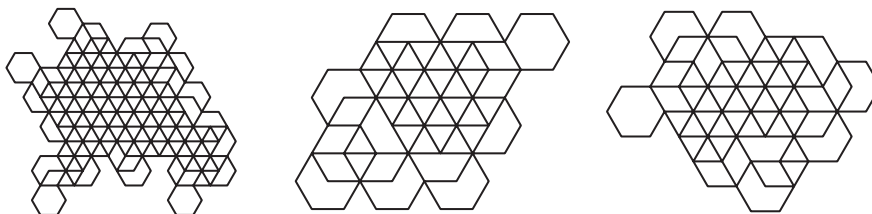
Beschouwen we als voorbeeld de worm met als DNA  $\{1, 0, 4, 0, 1, 5\}$ . De worm wordt gedropt op het driehoekig rooster, gaat één richting naar rechts, komt bij een nog onbekende configuratie terecht en besluit om richting 1 te kiezen (de eerste waarde in zijn DNA). Nu belandt de worm op een wel bekende configuratie en kiest dezelfde richting, 1. Dit gaat door tot die een volledige zeshoek doorlopen heeft. Op dat punt bevindt de worm zich in een onbekende verdeling, en kiest die richting 0 (de tweede waarde in zijn DNA). De volgende stappen vervolledigt hij weer een zeshoek. De nieuwe verdelingen van doorkruiste wegen en de gekozen richting staat hieronder afgebeeld:



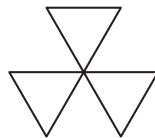
Deze worm uiteindelijk sterft na 57 stappen en laat dit spoor na:



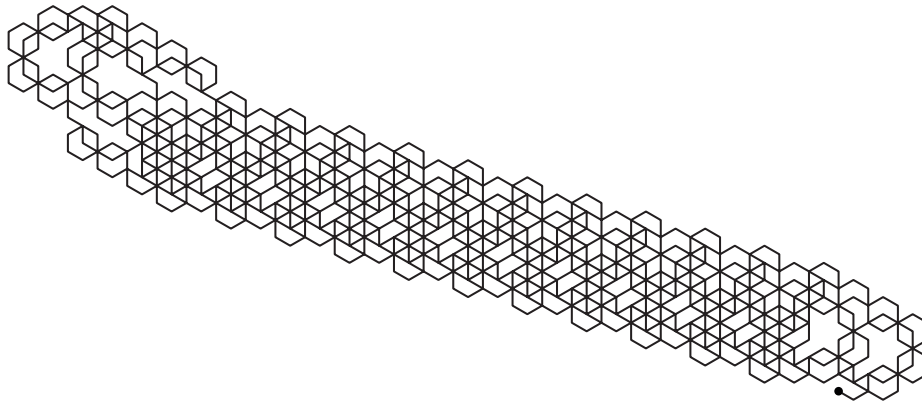
Meer wormen ( $\{1, 0, 4, 0, 1, 0, 1\}$ ,  $\{1, 0, 4, 0, 1, 0, 2\}$ , en  $\{1, 0, 4, 0, 1, 0, 5\}$ ):



Sommige wormen zijn nogal saai en sterven vrijwel direct, zoals  $\{2, 0, 0\}$ .



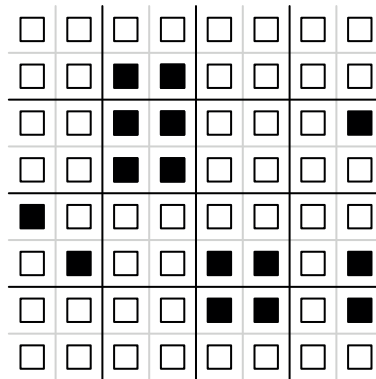
Andere wormen sterven uiteindelijk nooit, en leggen een snelweg aan zoals de mier van Langton (zie 284, blz.254). Voor het spoor hieronder vertrekt de worm met één stap naar boven i.p.v. rechts.



In totaal zijn er 1296 wormen. Velen hiervan zijn gespiegelde versies of sterven voor ze alle waarden uit hun DNA nodig hebben. In totaal blijven er slechts 411 fundamenteel verschillende over, plus de triviale worm (die de hele tijd rechtdoor gaat). 336 van hen gaan uiteindelijk dood, 73 leggen een herhalend patroon aan, van nog twee anderen wordt sterk vermoed dat ze oneindig doorgaan en het gedrag van de laatste blijft onbekend. Elf van de wormen vertonen echt gecompliceerd gedrag, zonder te sterven of een duidelijk patroon aan te leggen na miljarden stappen. Pas in 2003 ontwikkelde Benjamin Chaffin (een van de ontwerpers van de Pentium 4 chip) nieuwe methoden om hun gedrag te bepalen, zodat na uren rekenwerk negen ervan opgelost werden. Tomas Rokicki stelde vast dat de tiende,  $\{1, 0, 4, 2, 0, 2, 0\}$ , uiteindelijk sterft na zo'n 57 biljoen stappen. Volgens Rokicki is de laatste worm, waarvan nog onbekend of hij uiteindelijk sterft of niet, nog steeds actief na  $5,2 \times 10^{19}$  stappen!

## 287 Critters

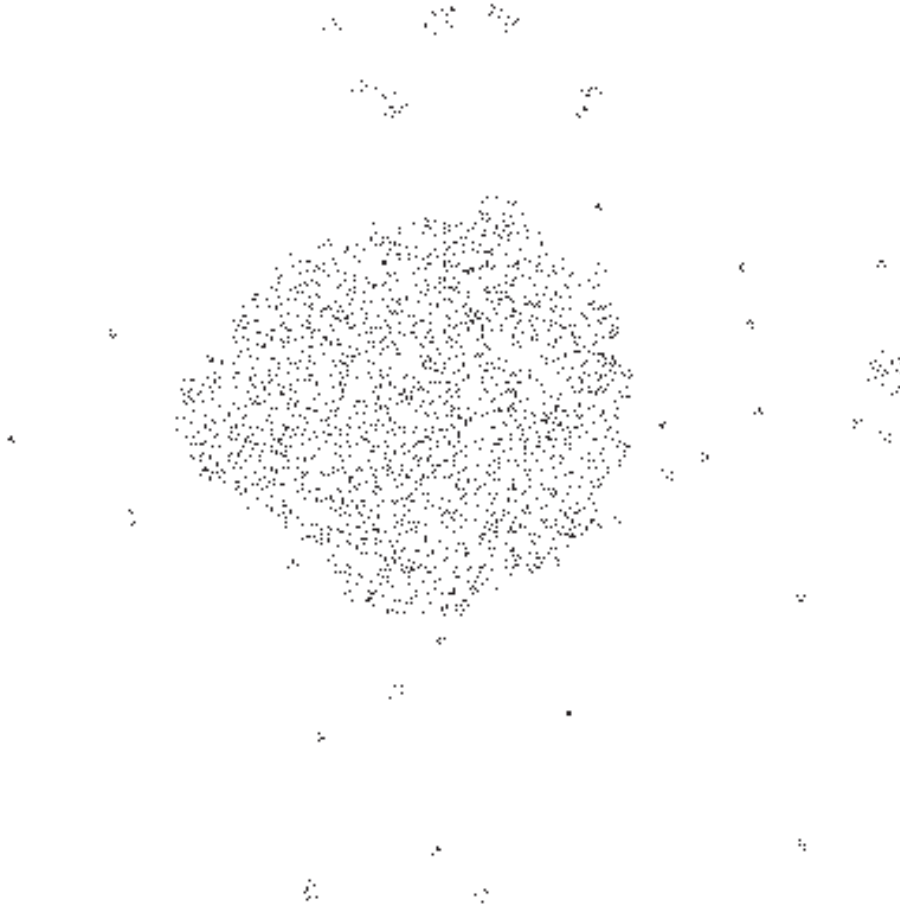
Game of Life en WireWorld (zie 285, blz. 285 en 288, blz. 288) worden gedefinieerd via de zogenaamde Moore-omgeving, de acht omliggende cellen. Men kan ook de vier direct aangrenzende cellen gebruiken (de Von Neumannomgeving). Een totaal andere manier om cellen te updaten is via de Margolusomgeving: verdeel het bord in  $2 \times 2$ -blokken, pas op elk blok de transformatieregels toe, schuif de blokken één cel in elke dimensie op en herhaal de regels. Deze wisselende blokken hebben het belangrijk voordeel dat wanneer de transformatieregels voor elk blok omkeerbaar zijn, dat eveneens zo is voor het hele veld.



Een voorbeeld van een cellulaire automaat die gebruikmaakt van de Margolusomgeving is Critters, door Tommaso Toffoli en Norman Margolus. Hierbij wisselt de toestand van elke cel in elk blok, tenzij er juist twee van elk zijn. Daarbovenop wordt een blok met drie levende cellen  $180^\circ$  gedraaid. Deze transformatieregel is omkeerbaar: elk mogelijk blok heeft juist één mogelijke voorganger, in tegenstelling tot bij Game of Life. Een extra eigenschap van Critters is dat per twee generaties het aantal levende cellen constant blijft (“behoud van deeltjes”).



In Critters komen er ook gliders en ingewikkeldere spaceships voor, net als oscillators. Een opmerkelijk verschil is echter dat in Critters, omkeerbaarheid en behoud van deeltjes ervoor zorgen dat minstens één glider bij een crash moet ontkomen.



## 288 WireWorld

WireWorld is een andere cellulaire automaat, met de intentie gemakkelijk elektrische circuits te kunnen simuleren. Het systeem is tweedimensionaal en vierkleurig en werd geïntroduceerd door Brian Silverman in 1987.

- Kleur 0 is achtergrond en blijft onveranderlijk.
- Kleur 1 is een *electron head*, en verandert de volgende generatie in een *electron tail*.
- Kleur 2 is een *electron tail*, en verandert de volgende generatie in *wire*.
- Kleur 3 is *wire* en blijft *wire*, tenzij er één of twee van de acht buurhokjes *electron head* zijn: in dat geval verandert kleur 3 de volgende generatie in een *electron head*.

Deze regels laten eenvoudig toe om stroom doorheen wires te simuleren. Ook logische poorten en ander elektronisch materiaal zijn veel gemakkelijker te programmeren dan in andere cellulaire automaten.

### Signalen.

Hieronder wordt voorgesteld hoe een *electron*, als combinatie van de lichtgrijze *head* en donkergrijze *tail*, doorheen de wire stroomt; elke generatie verplaatst die zich één cel verder.



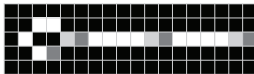
Wires kunnen ook makkelijk gesplitst worden.





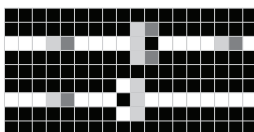
### Stroombronnen.

De stroombronnen of *pulsers* in WireWorld zijn eenvoudige lussen aangesloten op een wire, die na een bepaald aantal generaties (hieronder zes) een nieuw electron afvuurt door de wire.



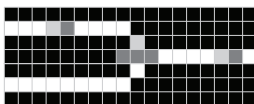
### Diodes.

Diodes zorgen ervoor dat electrons slechts in één richting doorheen een wire kunnen stromen. Omdat wires zelden gebruikt worden om signalen in twee richtingen door te sturen, worden deze diodes in praktijk niet vaak in circuits geïmplementeerd. De bovenste diode laat stroom die links binnenkomt door, anders wordt de stroom geblokkeerd.



### Logische poorten.

De volgende stap naar de constructie van complexere circuits zijn logische poorten. Een eenvoudige OR-poort, die uitvoer produceert wanneer minstens een van beide invoerwires een electron doorstuurt, is de volgende.



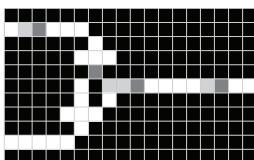
Een XOR-poort geeft pas uitvoer terug wanneer er in juist één invoerwire een electrontransmissie plaatsvindt.



Ook verscheidene AND- en NOT-poorten zijn bekend, die er wel ietwat complexer uitzien.

### Flip-flops.

Flip-flops zijn schakelementen die aan of uit gezet kunnen worden en naargelang hun status al dan niet werken als een stroombron. Een electron in de onderste wire activeert de flip-flop, terwijl de bovenste wire dient om hem te resetten. Hieronder staat een geactiveerde flip-flop.



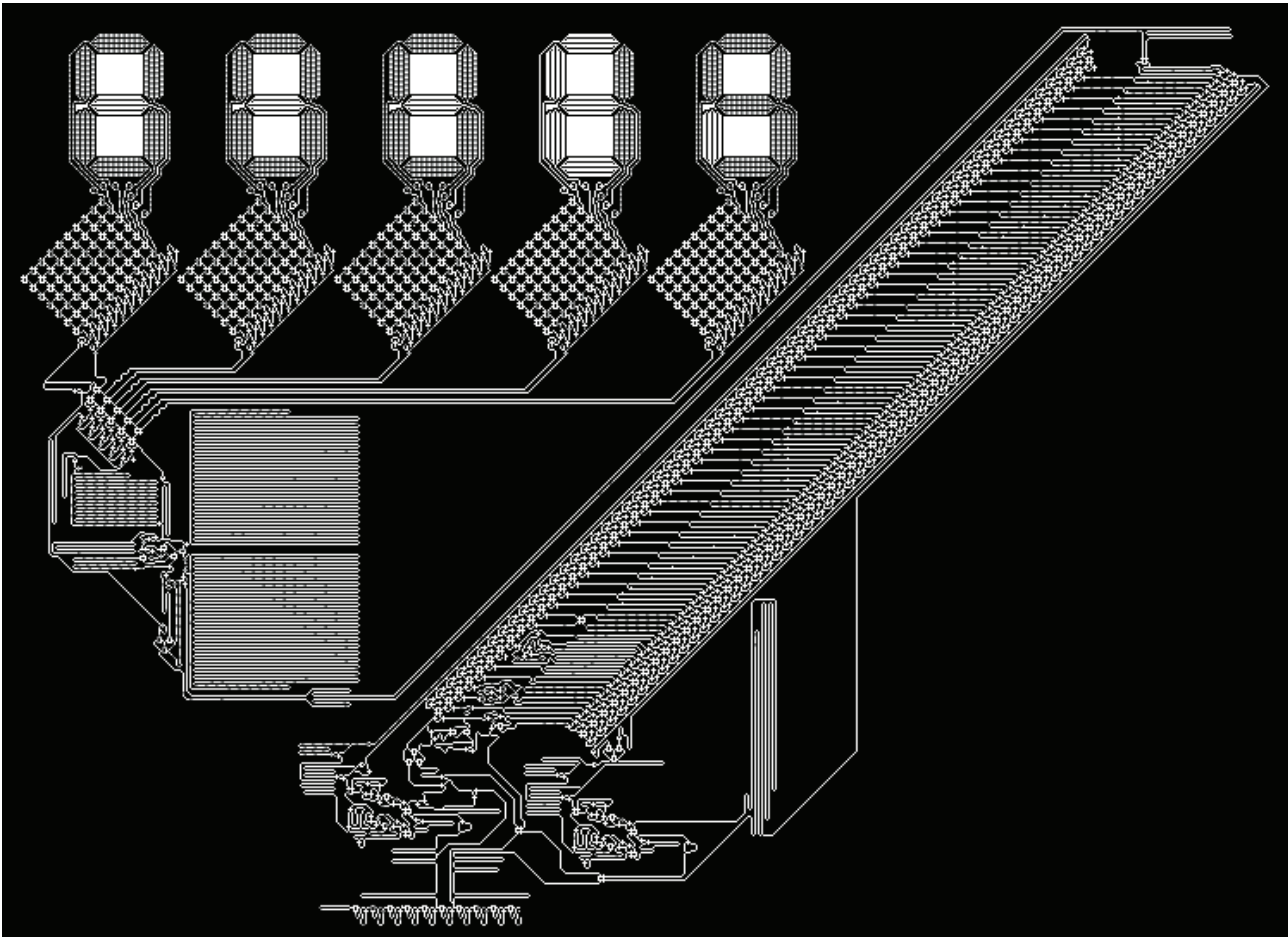
### Andere elementen.

Er kunnen in Wireworld ook circuits geprogrammeerd worden die de frequentie van een electron verdubbelen of halveren, reflectors die een electron terugsturen in de wire\*, *wire crossings*, circuits die een stroom electrons

\*Een interessant gadget, maar niet bruikbaar voor het doel van WireWorld, het eenvoudig programmeren van computers via een cellulaire automaat.

interpreteren als een binair getal en de som ervan als output produceren, een *register bank* die 16-bits getallen kan opslaan, *splitters* die data na elke cyclus in een andere outputwire richten, een mooie *binary counter* die een aantal electrons als input vereist en daarna de binaire vorm als output produceert (via een wire voor de 1, een wire voor de 2, één voor de 4 ...) enzoverder.

Door deze elementen te combineren kan, net als in Life, een Turing-complete computer gebouwd worden, die in staat is tot universele berekening. Ter illustratie staat hieronder een computer die de priemgetallen berekent en weergeeft als een LCD-scherm; Michael Fryers schreef het programma, David Moore en Mark Owen bouwden het design. Een zeer interessante link over de opbouw van de computer is <http://www.quinapalus.com/wi-index.html>.



Nog meer elementen met illustraties zijn te vinden op <http://karlscherer.com/Wireworld.html>.





## 289 MU-puzzel

Douglas Hofstadter illustreert in zijn befaamde boek *Gödel, Escher, Bach* de belangrijkste principes uit de logica en informatica via zijn MU-systeem. Dit systeem bevat de volgende transformatieregels, waarmee “stellingen” kunnen worden gebouwd vertrekkende vanuit het axiomatische woord MI.

- Voeg een U toe achteraan een woord dat eindigt op I, bijv. MI  $\rightarrow$  MIU.
- Verdubbel de tekenreeks die achter de M staat, bijv. MIU  $\rightarrow$  MIUIU.
- Vervang een tekenreeks III door U, bijv. MUIIU  $\rightarrow$  MUUU.
- Laat een tekenreeks UU weg, bijv. MUUU  $\rightarrow$  MU.

Hofstadter daagt de lezers tot de volgende puzzel uit. Is de tekenreeks MU hier een stelling? Dat wil zeggen, is het mogelijk vanuit MI door toepassing van bovenstaande regels MU te bekomen?

Verder in zijn boek geeft hij het antwoord. Door een getaltheoretische truc toe te passen op het systeem, bewijst Hofstadter dat de puzzel onmogelijk is: het aantal I's modulo 3 blijft invariant onder toepassing van de transformatieregels, terwijl dit niet zo is tussen MI en MU. Zo'n metatrucje kan ook formeel worden toegepast op serieuzere systemen, en zo illustreert Hofstadter de intuïtie achter Gödels onvolledigheidsstelling (zie ??, blz. ??).

## 290 Paradox van Russell

Begin de 20<sup>ste</sup> eeuw ontdekte Bertrand Russell een ronduit catastrofale paradox in de naïeve verzamelingenleer van Georg Cantor. In tegenstelling tot latere axiomatische theorieën werd deze naïeve theorie niet gedefinieerd op formele logica maar op informele courante taal. In dit systeem was het zinvol te spreken over de verzameling van alle verzamelingen, maar zoals Russells paradox aantoonde, leiden dergelijke beschouwingen tot inconsistenties, waardoor de grondslagen van heel de wiskunde aan het wankelen gebracht werden!

Verdeel de verzamelingen in twee categorieën onder: de “normale” die zichzelf niet bevatten, en de “abnormale” die zichzelf wél bevatten (zoals de verzameling van alle verzamelingen). Definieer dan  $R$  als de verzameling van alle normale verzamelingen:

$$R = \{x \mid x \notin x\}$$

Een natuurlijke vraag is nu of  $R$  zelf al dan niet normaal is. Als  $R$  normaal zou zijn, voldoet ze aan de voorwaarde in haar definitie en moet ze dus worden opgenomen in zichzelf, zodat ze niet normaal is. Mocht  $R$  daarentegen abnormaal zijn en zichzelf dus wél bevatten, dan bevat  $R$  een abnormale verzameling, wat niet strookt met de definitie van  $R$ !

$$R \in R \quad \Leftrightarrow \quad R \notin R$$

Als oplossing voor deze paradox stelde Ernst Zermelo in 1908 een systeem met verzwakte bestaansaxioma's voor. Nog enkele aanpassingen in de jaren 20, door Abraham Fraenkel, Thoralf Skolem en Zermelo zelf, leidden tot de standaard axiomatische verzamelingstheorie van vandaag: ZFC. In dit systeem wordt bijvoorbeeld niet aangenomen dat voor elke eigenschap er een verzameling bestaat van alle objecten die eraan voldoen, maar eerder dat voor elke verzameling, een deelverzameling gedefinieerd kan worden via eerste-orde logica, waarmee

het bestaan van een paradoxale verzameling zoals hierboven beschreven, vermeden wordt.

Russell beantwoordde zijn paradox op een andere manier, met een geheel nieuwe hiërarchie van typen. Geïnspireerd door eerder werk van Gottlob Frege publiceerden Bertrand Russell en Alfred Whitehead een driedelig opus in 1910, 1912 en 1913, de *Principia Mathematica*, met als doel een complete en consistente basis te geven waaruit dan alle wiskundige waarheid afgeleid zou kunnen worden. Helaas betekenden Gödels onvolledigheidsstellingen (zie ??, blz. ??) dat dit nobele doel gedoemd is te mislukken.

## 291 Blauwogige eilandbewoners

Op de blog van Terence Tao verscheen in 2008 de volgende amusante logicapuzzel.

OP EEN AFGELEGEN EILAND WOONT EEN PRIMITIEVE STAM. DE STAMLEDEN HEBBEN OFWEL BLAUWE, OFWEL BRUINE OGEN, MAAR DE PLAATSELIJKE RELIGIE VERBIEDT HET KENNEN VAN DE EIGEN OOGKLEUR: IEDERE OCHTEND KOMT DE STAM BIJEEN EN VRAAGT HET OPPERHOOFD OF IEMAND ZIJN OOGKLEUR ACHTERHAALD HEEFT, WAARNA DE PERSOON IN KWESTIE RITUELE ZELFMOORD DIENT TE PLEGEN VOOR DE OGEN VAN DE HELE STAM. IEDEREEN KAN ELKAARS OGEN BEKIJKEN, MAAR NIEMAND SPREEKT EROVER EN ER ZIJN GEEN SPIEGELS.

OP EEN DAG KOMT EEN ONTDEKKINGSREIZIGER (MET BLAUWE OGEN) AAN OP HET EILAND EN DEZE WORDT HARTELIJK ONTVANGEN. OP EEN AVOND ECHTER BEDANKT HIJ IEDEREEN VOOR DE GASTVRIJHEID EN VERMELDT HIJ TERLOOPS, ONWETEND VAN DE ETIQUETTE: “VREEMD OM HIER IEMAND TE ZIEN MET DEZELFDE OOGKLEUR ALS IK”...

WELK EFFECT HEEFT DEZE FAUX PAS OP DE STAM? ALLE STAMLEDEN ZIJN UITERMATE VROOM EN KUNNEN PERFECT LOGISCH DENKEN. DAARENBOVEN WETEN ALLE STAMLEDEN DAT ALLE STAMLEDEN UITERMATE VROOM EN LOGISCH ZIJN, DAT ALLE STAMLEDEN WETEN DAT ALLE STAMLEDEN UITERMATE VROOM EN LOGISCH ZIJN, ETC.

Op het eerste zicht lijkt een dergelijke uitspraak geen effect te hebben, aangezien alle stamleden kunnen zien dat er meerdere stamleden met blauwe ogen zijn en de bezoeker dus geen extra informatie gegeven heeft. Het concept *common knowledge* geeft echter aanleiding tot een tegensprekend argument.

Veronderstel dat maar één stamlid blauwe ogen heeft. Dan zal die doorhebben dat de reiziger naar hem refereert (want hij ziet uitsluitend stamleden met bruine ogen) en zelfmoord plegen. Inductief geldt dan dat als meerdere stamleden blauw als oogkleur hebben, elk ervan denkt: “Mocht ik bruine ogen hebben, dan zijn er  $n - 1$  leden met blauwe ogen, die dan allemaal zelfmoord zullen plegen na  $n - 1$  dagen.” Nadat  $n - 1$  dagen gepasseerd zijn en de hele stam nog leeft, weten deze  $n$  stamleden met zekerheid dat ze zelf blauwe ogen hebben.

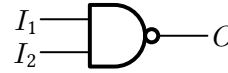
De ontdekkingsreiziger verstrekte wel degelijk nieuwe, fatale informatie. Voor zijn opmerking wist niet iedereen dat iedereen wist dat iedereen wist dat . . . dat iemand blauwe ogen heeft. Als er bijvoorbeeld twee blauwogige stamleden zijn, weten zij beide dat er iemand blauwe ogen heeft, maar niet dat die andere persoon daarvan op de hoogte is. De bezoeker maakt deze kennis echter *common knowledge*, zodat de eilandbewoners hun oogkleur kunnen beginnen deduceren.

Nadat de stamleden met blauwe ogen hun oogkleur publiek gemaakt hebben, kunnen ook de overige stamleden met bruine ogen hun oogkleur afleiden, zodat feitelijk de gehele stam wordt uitgeroeid.

## 292 NAND-poorten

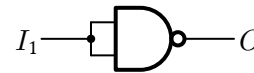
De NAND- en de NOR-poort zijn de enige logische poorten waarmee alle andere kunnen worden gebouwd; deze eigenschap maakt hen tot “universele poorten”. De schematische weergave van zo’n NAND en zijn waarheidstabel zijn:

$I_1$	$I_2$	$I_1 \text{ NAND } I_2$
0	0	1
0	1	1
1	0	1
1	1	0



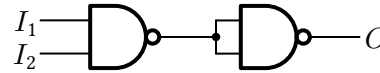
De NOT-poort is eenvoudig: sluit de invoer gewoon aan op beide ingangen van een NAND-poort.

$I_1$	NOT $I_1$
0	1
1	0



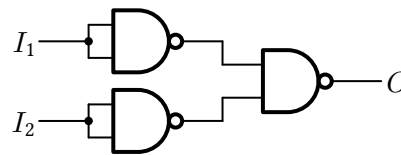
Een AND verkrijgt je door de NOT van daarnet achter een NAND te plaatsen.

$I_1$	$I_2$	$I_1 \text{ AND } I_2$
0	0	0
0	1	0
1	0	0
1	1	1



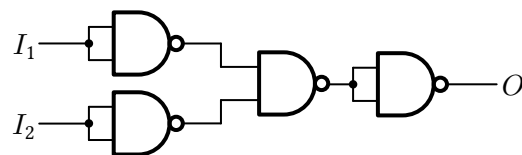
Voor een OR worden de invoerwaarden eerst omgekeerd en daarna door een NAND gestuurd.

$I_1$	$I_2$	$I_1 \text{ OR } I_2$
0	0	0
0	1	1
1	0	1
1	1	1



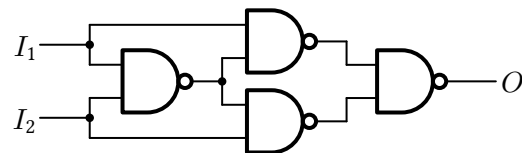
NOR is niets meer dan de OR van daarnet met omgekeerde uitvoer:

$I_1$	$I_2$	$I_1 \text{ NOR } I_2$
0	0	1
0	1	0
1	0	0
1	1	0



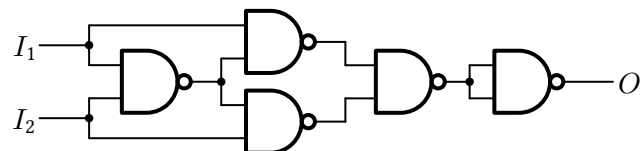
XOR-poorten zijn lastiger te construeren:

$I_1$	$I_2$	$I_1 \text{ XOR } I_2$
0	0	0
0	1	1
1	0	1
1	1	0



Tot slot, met een NOT erachter, wordt de XOR- een XNOR-poort.

$I_1$	$I_2$	$I_1 \text{ XNOR } I_2$
0	0	1
0	1	0
1	0	0
1	1	1



## 293 Halting problem

Een fenomeen berucht bij computerprogrammeurs zijn de *infinite loops* of oneindige lussen: programmeercode die zichzelf eeuwig herhaalt bij het uitvoeren. Normaliter een ongewenst effect, doordat het processorintensief is en het systeem kan doen crashen. Helaas kan de oorzaak van zo'n bug zeer subtiel en lastig op te sporen zijn. Daarom vroeg Alan Turing zich in 1936 af of het mogelijk is een algoritme  $\text{HALT}(P)$  op te stellen dat een ander programma  $P$  als invoer vraagt en kan bepalen of  $P$  al dan niet in een oneindige lus terechtkomt, zonder het effectief uit te voeren.

Jammer genoeg ontdekte Turing dat dit potentieel waardevolle programma onmogelijk kan bestaan! Veronderstel namelijk dat  $\text{HALT}(P)$  wél bestaat en kan beslissen of  $P$  al dan niet ooit stopt. Turing beschouwde dan het programma  $\text{TROUBLE}$ , dat als volgt geconstrueerd wordt:

---

```

TROUBLE( $P$ )
  input : programma  $P$ 

  if  $\text{HALT}(P)=\text{true}$  then
    | perform infinite loop
  else
    | halt

```

---

Dus, als  $P$  stopt, gaat  $\text{TROUBLE}(P)$  in een oneindige lus, en als  $P$  niet stopt, zou  $\text{TROUBLE}(P)$  zelf wel stoppen. Wat doet  $\text{TROUBLE}(\text{TROUBLE})$  dan? Een kleine analyse wijst uit dat  $\text{TROUBLE}$  stopt als en slechts als  $\text{TROUBLE}$  niet stopt! Deze absurditeit bewijst dat zo'n programma  $\text{HALT}$  helaas niet bestaat.

## 294 Hotel van Hilbert

Hilberts Hotel is een magnifieke illustratie van de ideeën van Georg Cantor en de contra-intuïtieve eigenschappen van het concept "oneindigheid" (zoals  $\infty + 1 = \infty$ ,  $2 \cdot \infty = \infty$  en  $\infty^2 = \infty$ ), gecreëerd door David Hilbert in de jaren 20. Het Hotel van Hilbert bevat oneindig veel kamers, eenvoudig genummerd volgens de natuurlijke getallen. Daardoor biedt het Hotel onderdak aan een oneindig aantal gasten, ware het niet dat het volledig volzet is: elke kamer is bezet.

Een nieuwe gast arriveert. Ook al zijn er geen kamers meer vrij, de receptionist weet kamer 1 vrij te maken door elke gast één kamernummer op te schuiven: de gast in kamer  $n$  verhuist naar kamer  $n + 1$ .

Daarna arriveert er een oneindig lange bus op de parking met een oneindig aantal gasten die een kamer willen. Opnieuw klaart de receptionist het klusje door de huidige gasten te verhuizen: deze keer van kamer  $n$  naar  $2n$ , zodat alle oneven kamernummers vrijkomen om de nieuwe gasten op te vangen.

De creativiteit van de receptionist wordt danig op de proef gesteld als er vervolgens een oneindig aantal bussen met oneindig veel gasten in elk toekomt. Ook nu verhuist iedereen van kamer  $n$  naar  $2n$ , waarna de eerste bus wordt ondergebracht in de kamers 3, 9, 27 . . . , de tweede bus in 5, 25, 125 . . . , en elke verdere bus in de kamers die een macht van het volgende priemgetal als kamernummer hebben. Zo blijven er zelfs nog een oneindig aantal kamers onbezet!

WE'RE ALWAYS FULL, BUT WE ALWAYS HAVE ROOM FOR YOU.



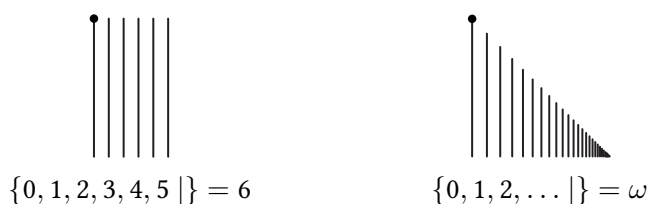
## 295 Ordinaalgetallen

Het klassieke telsysteem gebruikt natuurlijke getallen verschillend van nul om objecten te tellen, zodat het laatste gebruikte getal het te tellen aantal weergeeft. Een alternatief en algemener systeem is te tellen vanaf nul: dan stelt het kleinste niet-gebruikte getal het aantal voor. Vanuit dit principe bouwde Georg Cantor als eerste een coherente theorie op om oneindige aantallen te tellen, via ordinaalgetallen.

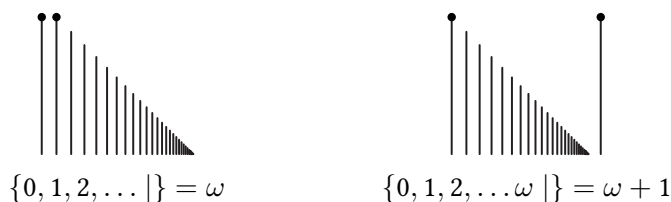
Het systeem van Cantor heeft het voordeel dat ongeacht welke verzameling ordinaalgetallen je beschouwt, er altijd een uniek bepaald, kleinste ordinaalgetal bestaat dat niet in deze verzameling zit. Een gangbare notatie voor dit getal is een streep op het einde van de verzameling. Het kleinste ordinaalgetal dat verschilt van de natuurlijke getallen heet  $\omega$  en heeft aldus de volgende representatie:

$$\omega = \{0, 1, 2, \dots | \}$$

Een visuelere weergave is de volgende:

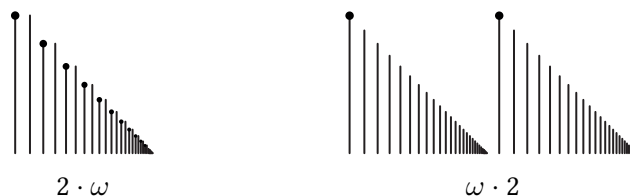


Om ordinaalgetallen op te tellen, volstaat het om hun diagrammen zoals hierboven naast elkaar te zetten en te hertellen. Merk wel op dat deze optelling niet langer commutatief is vanaf  $\omega$ ! Er geldt bijvoorbeeld dat  $1 + \omega = \omega$ , terwijl  $\omega + 1$  is wel degelijk groter dan  $1 + \omega$ :

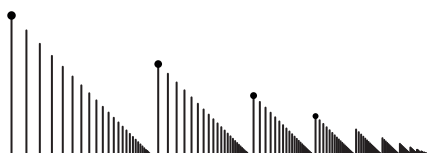


Ondanks dat deze sommen niet commutatief zijn, blijkt dat drie ordinaalgetallen niet tot zes, maar slechts tot vijf verschillende sommen opgeteld kunnen worden, m.a.w. zeker twee van de uitdrukkingen  $\alpha + \beta + \gamma$ ,  $\alpha + \gamma + \beta$ ,  $\beta + \alpha + \gamma$ ,  $\beta + \gamma + \alpha$ ,  $\gamma + \alpha + \beta$  en  $\gamma + \beta + \alpha$  zijn gelijk. Het maximale aantal verschillende sommen met  $n$  ordinaalgetallen staat in OEIS A005348.

Een product  $a \cdot b$  van ordinaalgetallen is de waarde van het diagram horende bij  $b$  kopieën van het diagram van  $a$  achter elkaar. Ook hier gaat de commutativiteit verloren, bijvoorbeeld  $2 \cdot \omega = \omega$ , maar  $\omega \cdot 2 = \omega + \omega$ .



Het ordinaalgetal  $\omega \cdot \omega$ , of  $\omega^2$ , bestaat dan uit  $\omega$  kopieën van  $\omega$ . Nogmaals  $\omega$  kopieën van dit diagram levert hogere machten van  $\omega$  op.



Het eerstvolgende ordinaalgetal achter al deze machten van  $\omega$  is dan  $\{1, \omega, \omega^2, \omega^3, \dots\} = \omega^\omega$ . Daarna gaat het systeem weer verder als voorheen.

$$0, 1, 2, \dots, \omega, \omega + 1, \omega + 2, \dots, \omega \cdot 2, \omega \cdot 2 + 1, \dots, \omega \cdot 3, \dots, \omega^2, \dots, \omega^2 + \omega, \dots, \omega^3, \dots, \omega^\omega, \dots, \omega^{\omega^\omega}, \dots$$

De “limiet” van al deze getallen is het volgende ordinaalgetal,  $\{1, \omega, \omega^\omega, \omega^{\omega^\omega}, \dots\}$ , dat Cantor met  $\epsilon_0$  aanduidde. Het is het eerste ordinaalgetal dat niet uit te drukken is met een eindig aantal optellingen, vermenigvuldigingen en machtsverheffingen van kleinere ordinaalgetallen.

$$\epsilon_0 = \underbrace{\omega^{\omega^{\omega^{\omega^{\dots}}}}}_{\omega \text{ kopieën}}$$

De ordinaalgetallen  $\epsilon$  waarvoor de Cantors vergelijking  $\omega^\epsilon = \epsilon$  opgaat, heten de epsilongetallen; het al onvoorstelbare  $\epsilon_0$  is nog maar de kleinste. De volgende is  $\epsilon_1 = (\epsilon_0 + 1) + \omega^{(\epsilon_0 + 1)} + \omega^{\omega^{(\epsilon_0 + 1)}} + \dots$

Het systeem gaat natuurlijk nog verder; zo zijn er nog  $\epsilon_2, \epsilon_3, \dots, \epsilon_\omega, \dots, \epsilon_{\omega^2}, \dots, \epsilon_{\omega^\omega}, \dots, \epsilon_{\epsilon_0}, \dots, \epsilon_{\epsilon_{\epsilon_0}}, \dots$  en uiteindelijk  $\epsilon_{\epsilon_{\epsilon_{\epsilon_{\dots}}}}$  (dat de eerste oplossing vormt van  $\epsilon_\alpha = \alpha$ ), etcetera, etcetera...

Zoals Cantor vermoedde en zijn student Ernst Zermelo in 1904 kon aantonen, zijn er genoeg ordinaalgetallen in dit systeem om elke mogelijke verzameling te tellen, ongeacht hoe groot deze is. Het bewijs van Zermelo vestigde de aandacht op het beruchte keuzeaxioma (zie ??, blz. ??), dat tot dan nog vrijwel onbekend was in de wiskundige wereld en waarop het bewijs steunt.

### 295.1 Stelling van Goodstein

De stelling van Goodstein werd ontdekt en bewezen door Reuben Goodstein in 1944. Ze is om twee redenen interessant: enerzijds is het resultaat op zich spectaculair, en anderzijds kan worden aangetoond dat de stelling onbewijsbaar is binnen de klassieke Peanorekenkunde. Het resultaat is wel degelijk bewijsbaar als men het bestaan van het ordinaalgetal  $\epsilon_0$  aanneemt.

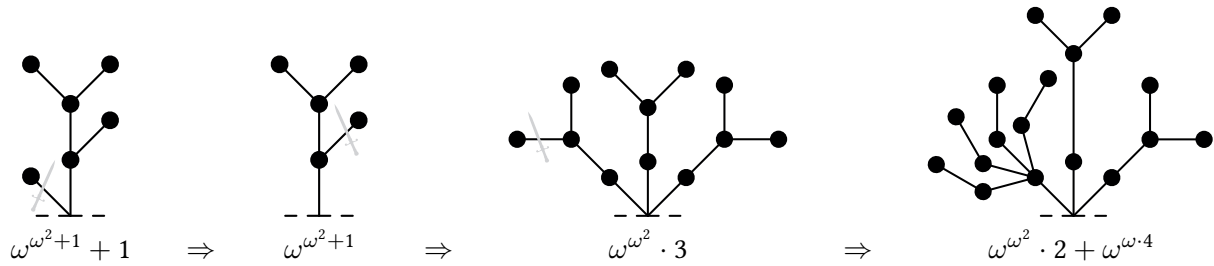
De rijen van Goodstein, waar de stelling over gaat, worden geconstrueerd met behulp van super- $n$ -notatie of notatie in strikte basis  $n$ . Om een getal te noteren in deze vorm, moet die eerst worden geschreven als een som van machten van  $n$ , waarbij de coëfficiënten kleiner dan  $n$  moeten zijn. Herhaal deze stap nu met de exponenten, totdat de volledige representatie gebruik maakt van enkel getallen ten hoogste  $n$ . Het getal 265 bijvoorbeeld, wordt in super-2-notatie:

$$265 = 2^{2^{2+1}} + 2^{2+1} + 1$$

De beginterm  $G_1$  van een Goodsteinrij is een willekeurig natuurlijk getal. Schrijf dan dit getal in super-2-notatie, verander elke 2 in 3 en verminder het resultaat met 1; deze waarde wordt  $G_2$ . Elke volgende term  $G_n$  verkrijgen we door de vorige te schrijven in super- $n$ -notatie, elke  $n$  te vervangen door  $n + 1$  en deze waarde te verminderen met 1. Zulke rijen groeien extreem snel en worden al gauw onhandelbaar groot: kies 19 als beginwaarde, en  $G_2$  is al gelijk aan 7.625.597.484.990 (om nog maar te zwijgen over  $G_3$ , zo'n  $1,3 \times 10^{154}$ ). De uiteindelijke stelling van Goodstein beweert echter dat voor elke rij, met welk begingetal dan ook, hoe groot de tussenwaarden ook groeien en hoe lang de rij ook wordt, uiteindelijk de termen stranden op 0!

Laurie Kirby en Jeff Paris demonstreerden in 1982 dat dit verrassende resultaat onbewijsbaar is binnen de Peanorekenkunde, niet af te leiden uit de axioma's van Peano. Daarmee bleek de stelling van Goodstein een concreet voorbeeld van Gödels onvolledigheidsstelling (zie ??, blz. ??). Het oorspronkelijke bewijs van Goodstein maakt gebruik van ordinaalgetallen, een concept binnen een sterker systeem.

**295.2 Hercules vs. de Hydra**



**296 Lambdacalculus**

Het systeem der lambdacalculus werd ingevoerd door Alonzo Church in de jaren 30, die er onderzoek mee deed naar de wiskundige grondslagen, meer bepaald berekenbaarheidstheorie. Church gebruikte de lambdacalculus onder andere om aan te tonen dat het Entscheidungsproblem van Hilbert (zie ??, blz. ??) onoplosbaar is, en stelde dat zijn systeem (net als de Turingmachines, zie ??, blz ??) tot alle mogelijke effectieve berekeningen in staat is. Stephen Kleene en John Rosser ontwikkelden in 1935 echter een paradox binnen het systeem, zodat Church' originele lambdacalculus logisch inconsistent bleek. In 1940 introduceerde hij daarop een computationeel zwakker maar logisch consistent systeem, de *simply typed lambda calculus*.

Lambdacalculus is gebaseerd op het concept van *abstractie* en *applicatie* van functies. Een functie die bijvoorbeeld  $x$  afbeeldt op  $5x - 1$  kan een naam krijgen, bijvoorbeeld  $f$  waardoor dan  $f(x) = 5x - 1$ , maar een anonieme variant is soms handiger om een hele waslijst aan indirecte functienamen te vermijden. Church gebruikte de Griekse letter  $\lambda$  en een punt om functies te abstraheren:

$$\lambda \text{ input} . \text{output}$$

Concreet wordt het voorbeeld van daarnet in lambdacalculus genoteerd als  $\lambda x . 5x - 1$ . Net zoals bij een klassieke functie krijgt deze lambda-expressie dus een bepaalde invoer en wordt (afhankelijk van de invoer) een bepaalde uitvoer teruggegeven. Een applicatie van zo'n expressie komt dan neer op "invullen" in de functie:

$$(\lambda \text{ input} . \text{output}(\text{input})) \text{ variabele} \Rightarrow \text{output}(\text{variabele})$$

Concreet:  $(\lambda x . 5x - 1) z^2 = 5z^2 - 1$ . Merk op dat functies in meerdere veranderlijken altijd geschreven kunnen worden d.m.v. functies in één veranderlijke die een andere functie teruggeeft; een alternatieve uitdrukking voor  $\lambda a . (\lambda b . a + b)$  is dan  $\lambda ab . a + b$ , waarbij  $a$  en  $b$  twee inputvariabelen zijn. Een dergelijke transformatie wordt vandaag *currying* genoemd, ter ere van Haskell Curry.

Tot nog toe hebben we enkel nieuwe notatie ingevoerd. Het wonderlijke aan dit systeem is echter dat voor logica en aritmetica geen cijfers of andere bewerkingen vereist zijn: uitsluitend abstractie en applicatie van functies naar andere functies (*pure lambda calculus*) volstaan! In deze context spreekt men eerder van combinatoren i.p.v. functies. Zo is er de identiteitscombinator  $\lambda a . a$ , de combinator  $\lambda a . aa$  die eender welke combinator op zichzelf toepast,  $\lambda ab . ba$  die de toepassingsvolgorde van twee combinatoren omdraait...

Een recursieve definitie van geldige lambda-expressies:

- Een variabele  $x$  op zich is een geldige expressie.
- Als  $t$  een geldige expressie is en  $x$  een variabele, is ook  $(\lambda x . t)$  een geldige expressie (abstractie).
- Als  $t$  en  $s$  geldige expressies zijn, is ook  $(t s)$  een geldige expressie (applicatie).

Lambda-expressies kunnen gereduceerd worden via drie regels:  $\alpha$ -conversie,  $\beta$ -reductie en  $\eta$ -conversie.

- $\alpha$ -conversie laat toe gebonden variabelen te hernoemen, zoals:

$$\lambda x . x \quad \xleftrightarrow{\alpha} \quad \lambda y . y$$

- $\beta$ -reductie stelt substitutie voor, wat gangbaar genoteerd wordt als  $f[x/x']$  en neerkomt op het vervangen\* van alle vrije instanties van de variabele  $x$  door de variabele  $x'$  in de expressie  $f$ . Een  $\beta$ -reductie doet dan het volgende:

$$((\lambda x . f) x') \quad \xleftrightarrow{\beta} \quad f[x/x']$$

- $\eta$ -conversie vertegenwoordigt extensionaliteit, waarbij functies als gelijk beschouwd worden als ze gelijke resultaten vertonen voor alle argumenten. Wanneer  $x$  niet vrij voorkomt in  $f$ , geldt zo:

$$\lambda x . (f x) \quad \xleftrightarrow{\eta} \quad f$$

Een term die nog vereenvoudigd kan worden door middel van een  $\beta$ - of  $\eta$ -reductie heet een redex (*reducible expression*). Een term die niet meer te reduceren valt, staat in zijn normale vorm.

Een laatste technische afspraak betreft een lichtere notatie.

- Buitenste haakjes worden vaak weggelaten:  $a b$  betekent  $(a b)$ .
- Applicaties worden links associatief verondersteld:  $a b c$  betekent  $((a b) c)$ .
- Een abstractie strekt zo ver naar rechts uit als mogelijk:  $\lambda x . a b$  betekent  $\lambda x . (a b)$ , en niet  $(\lambda x . a) b$ .
- Een sequentie abstracties kan worden ingekort:  $\lambda x y z . a$  betekent  $\lambda x . \lambda y . \lambda z . a$ , en dit betekent op zijn beurt voluit  $(\lambda x . (\lambda y . (\lambda z . a)))$ .

## 296.1 Aritmetica

Hoe is het nu mogelijk te rekenen in de lambdacalculus zonder notie van optelling of vermenigvuldiging? Church representeerde zijn getallen als functies die twee parameters vereisen,  $f$  en  $x$ , en intuïtief gezien deze  $f$  een aantal keer uitvoeren op  $x$ . Vaakvoorkomende functies zullen we vanaf nu een naam geven om ernaar te verwijzen, maar onthoud dat deze in feite niks meer dan andere lambda-expressies zijn.

$$\begin{cases} \mathbf{0} \equiv \lambda f . \lambda x . x \\ \mathbf{1} \equiv \lambda f . \lambda x . f x \\ \mathbf{2} \equiv \lambda f . \lambda x . f (f x) \\ \mathbf{3} \equiv \lambda f . \lambda x . f (f (f x)) \\ \dots \end{cases}$$

Een opvolgerfunctie voor deze “getallen”  $n$  zoals beschreven in de axioma’s van Peano wordt dan:

$$\mathbf{Succ} \equiv \lambda n . \lambda f . \lambda x . f (n f x)$$

Een functie die twee getallen optelt ziet er dan als volgt uit:

$$\mathbf{Plus} \equiv \lambda m . \lambda n . m \mathbf{Succ} n = \lambda m . \lambda n . \lambda f . \lambda x . m f (n f x)$$

---

\*Indien nodig wordt dit voorafgegaan door een  $\alpha$ -conversie om conflicterende variabelen te vermijden. Een voorbeeld is  $(\lambda x . y)[y/x]$ : dit wordt dan gesubstitueerd tot  $\lambda z . x$ .

Dit definieert wel degelijk een optelling: **Plus 2 3** bijvoorbeeld reduceert tot **5**.

$$\begin{aligned}
 & \mathbf{Plus\ 2\ 3} \\
 & \downarrow \\
 & (\lambda m . \lambda n . \lambda f . \lambda x . m\ f\ (n\ f\ x))\ \mathbf{2\ 3} \\
 & \downarrow \\
 & \lambda f . \lambda x . \mathbf{2}\ f\ (\mathbf{3}\ f\ x) \\
 & \downarrow \\
 & \lambda f . \lambda x . (\lambda f . \lambda x . f\ (f\ x))\ f\ ((\lambda f . \lambda x . f\ (f\ (f\ x)))\ f\ x) \\
 & \downarrow \\
 & \lambda f . \lambda x . (\lambda x . f\ (f\ x))\ (f\ (f\ (f\ x))) \\
 & \downarrow \\
 & \lambda f . \lambda x . f\ (f\ (f\ (f\ (f\ x)))) \\
 & \downarrow \\
 & \mathbf{5}
 \end{aligned}$$

Vermenigvuldiging:

$$\mathbf{Mult} \equiv \lambda m . n . m\ (\mathbf{Plus}\ n)\ \mathbf{0} = \lambda m . \lambda n . \lambda f . m\ (n\ f)$$

Machtsverheffing ziet er eenvoudiger uit.

$$\mathbf{Exp} \equiv \lambda m . \lambda n . m\ n$$

Een voorgangerfunctie, die 0 afbeeldt op 0 en elke andere  $n$  op  $n - 1$ , is weer heel wat lastiger.

$$\mathbf{Pred} \equiv \lambda n . \lambda f . \lambda x . n\ (\lambda g . \lambda h . h\ (g\ f))\ (\lambda u . x)\ (\lambda u . u)$$

Hiermee kan een functie geconstrueerd worden die  $m - n$  teruggeeft wanneer  $m > n$  en 0 anderszijds:

$$\mathbf{Sub} \equiv \lambda m . \lambda n . n\ \mathbf{Pred}\ m$$

## 296.2 Logica

Logica maakt gebruik van de als volgt gedefinieerde booleaanse waarden.

$$\begin{cases}
 \mathbf{True} \equiv \lambda x . \lambda y . x \\
 \mathbf{False} \equiv \lambda x . \lambda y . y
 \end{cases}$$

Merk op dat **FALSE** als dezelfde functie gecodeerd wordt als het getal **0**. Enkele logische operatoren (die gebruikmaken van prefixnotatie) zijn dan:

$$\begin{cases}
 \mathbf{And} \equiv \lambda p . \lambda q . p\ q\ p \\
 \mathbf{Or} \equiv \lambda p . \lambda q . p\ p\ q \\
 \mathbf{Not} \equiv \lambda p . \lambda a . \lambda b . p\ b\ a
 \end{cases}$$

En inderdaad, zo kunnen we bijvoorbeeld uitrekenen dat **And True False** reduceert tot **False**:

$$\begin{aligned}
 & \mathbf{And\ True\ False} \\
 & \quad \downarrow \\
 & (\lambda p . \lambda q . p\ q\ p)\ \mathbf{True\ False} \\
 & \quad \downarrow \\
 & \mathbf{True\ False\ True} \\
 & \quad \downarrow \\
 & (\lambda x . \lambda y . x)\ \mathbf{False\ True} \\
 & \quad \downarrow \\
 & \mathbf{False}
 \end{aligned}$$

Deze expressie kan gebruikt worden als predicaatstest. Ze ontvangt drie argumenten en geeft de tweede of de derde terug, afhankelijk van de eerste term.

$$\mathbf{IfThenElse} \equiv \lambda p . \lambda a . \lambda b . p\ a\ b$$

<b>IfThenElse True</b> $a\ b$	<b>IfThenElse False</b> $a\ b$
$\downarrow$	$\downarrow$
$(\lambda p . \lambda a . \lambda b . p\ a\ b)\ \mathbf{True}\ a\ b$	$(\lambda p . \lambda a . \lambda b . p\ a\ b)\ \mathbf{False}\ a\ b$
$\downarrow$	$\downarrow$
<b>True</b> $a\ b$	<b>False</b> $a\ b$
$\downarrow$	$\downarrow$
$(\lambda x . \lambda y . x)\ a\ b$	$(\lambda x . \lambda y . y)\ a\ b$
$\downarrow$	$\downarrow$
$a$	$b$

Een fundamenteel predicaat is deze test, die controleert of een getal gelijk is aan nul:

$$\mathbf{IsZero} \equiv \lambda n . n\ (\lambda x . \mathbf{False})\ \mathbf{True}$$

### 296.3 Koppels

Koppels kunnen bijgehouden worden via de volgende functie, die het paar  $(x, y)$  inkapselt:

$$\mathbf{Pair} \equiv \lambda x . \lambda y . \lambda f . f\ x\ y$$

Het eerste en tweede element van zo'n koppel kan dan verkregen worden als volgt:

$$\left\{ \begin{array}{l} \mathbf{First} \equiv \lambda p . p\ \mathbf{True} \\ \mathbf{Second} \equiv \lambda p . p\ \mathbf{False} \end{array} \right.$$

### 296.4 Recursieve functies

Voorgaande basisconstructies kunnen gecombineerd worden tot ingewikkeldere combinatoren. Een noemenswaardig voorbeeld is de recursief gedefinieerde faculteitsfunctie. In de lambdacalculus is het helaas niet mogelijk rechtstreeks te verwijzen naar een functie binnen diezelfde functie, maar dit kan wel gerealiseerd worden via de volgende constructie:  $(\lambda x . x\ x)\ y$  laat de functie  $y$  toegepast op zichzelf. We zoeken nu een combinator om algemene anonieme recursie toe te laten.

Eén stap van de faculteitsfunctie ziet er als volgt uit:

$$F = \lambda f . \lambda n . \mathbf{IfThenElse} (\mathbf{IsZero} \ n) \ \mathbf{1} \ (\mathbf{Mult} \ n \ (f \ (\mathbf{Pred} \ n)))$$

In deze formule dienen  $F$  en  $f$  als plaatshouder voor de uiteindelijke faculteit, **Fact**. De bedoeling is nu een algemene combinator **Fix** te vinden die voldoet aan  $(\mathbf{Fix} \ F) = (F \ (\mathbf{Fix} \ F))$  en die dus een fixpunt van zijn argument  $F$  opspoort: wanneer deze een lambda-expressie gegeven krijgt wiens eerste argument de recursieve functieoproep voorstelt, zal **Fix** een lambda-expressie teruggeven die de gezochte recursieve functie codeert. De faculteitsfunctie **Fact** vinden we dan bijvoorbeeld als **Fix**  $F$ :

$$\begin{aligned} & (\mathbf{Fix} \ F) \ n \\ & \quad \downarrow \\ & F \ (\mathbf{Fix} \ F) \ n \\ & \quad \downarrow \\ & \lambda f . \lambda n . \mathbf{IfThenElse} (\mathbf{IsZero} \ n) \ \mathbf{1} \ (\mathbf{Mult} \ n \ (f \ (\mathbf{Pred} \ n))) \ (\mathbf{Fix} \ F) \ n \\ & \quad \downarrow \\ & \mathbf{IfThenElse} (\mathbf{IsZero} \ n) \ \mathbf{1} \ (\mathbf{Mult} \ n \ ((\mathbf{Fix} \ F) \ (\mathbf{Pred} \ n))) \end{aligned}$$

Een willekeurige recursieve formule kan dus worden gevonden door  $F$  zoals hierboven te definiëren voor één enkele stap, en hem daarna toe te passen op een **Fix**-combinator. Rest ons nog zo'n **Fix**-combinator te vinden. De bekendste en wellicht eenvoudigste werd ontdekt door Haskell Curry.

$$\mathbf{Fix} \equiv \lambda f . (\lambda x . f \ (x \ x)) \ (\lambda x . f \ (x \ x))$$

Deze voldoet inderdaad aan de vereisten:

$$\begin{aligned} & \mathbf{Fix} \ g \\ & \quad \downarrow \\ & (\lambda f . (\lambda x . f \ (x \ x)) \ (\lambda x . f \ (x \ x))) \ g \\ & \quad \downarrow \\ & (\lambda x . g \ (x \ x)) \ (\lambda x . g \ (x \ x)) \\ & \quad \downarrow \\ & g \ ((\lambda x . g \ (x \ x)) \ (\lambda x . g \ (x \ x))) \\ & \quad \downarrow \\ & g \ (\mathbf{Fix} \ g) \end{aligned}$$

Het valt nog op te merken dat voor elke lambdaterm er steeds een expressie bestaat die geëvalueerd wordt naar diezelfde expressie, d.w.z. elke lambdaterm heeft een fixpunt, te vinden door inwerking van **Fix**.

### 296.5 Visualisatie

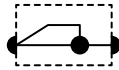
Raymond Smullyan wees erop dat het enige belangrijke aan combinatoren is hoe ze op elkaar reageren. In zijn boek *To mock a mockingbird* vergeleek hij ze met vogels, die elkaars liedjes aanhoren en daarop met een nieuw lied reageren, ter nagedachtenis van pionier Haskell Curry die vogels bestudeerde als hobby. David Keenan bouwde daarop voort en ontwikkelde een grafische notatie voor deze vogels.

De eenvoudigste is uiteraard deze *identity* (of *idiot*) *bird* **I**. Links (z'n oor) ontvangt de vogel het liedje en rechts (z'n keel) produceert hij zijn reactie erop, die hier exact dezelfde is als wat hij hoorde.



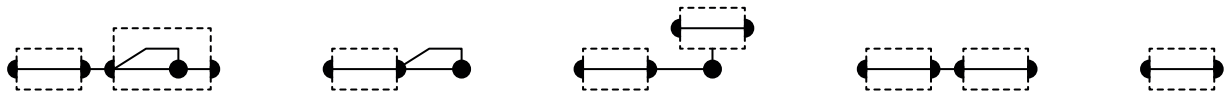
$$\mathbf{I} \equiv \lambda x . x$$

De reactie van de spotgaai  $\omega$  (*mockingbird*) op eender welke vogel is dezelfde als de reactie van die vogel op zichzelf. Binnenin het brein van de spotgaai staat de stip voor een applicatie: de van links afkomende functie wordt toegepast op de van boven ontvangen functie, en wordt uitgevoerd naar rechts.

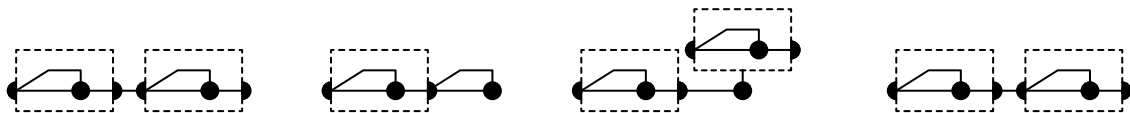


$$\omega \equiv \lambda x . x x$$

Wanneer een spotgaai een identiteitsvogel hoort, kunnen we zijn antwoord vinden door de grafische voorstellingen uit te werken, idealiter in animatie. Dit resulteert hier terug in (het liedje van) de identiteitsvogel. Bemerk dat we een vogel identificeren met zijn liedje, d.w.z. vogels en hun liedjes zijn equivalent.

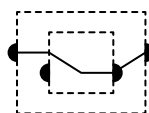


Wat gebeurt er als een spotgaai een andere spotgaai hoort?

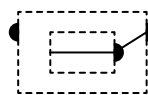


Hier blijkt dat een spotgaai in een oneindige lus terecht komt als hij een andere spotgaai hoort, omdat die steeds blijft reduceren! In deze toestand heeft een spotgaai geen normale vorm en wordt hij een *Omega bird*  $\Omega$  genoemd. In lambda-notatie:  $\Omega = (\lambda x . x x) (\lambda x . x x)$ .

De lambda-expressies die **True** en **False** voorstellen, heten in vogelvorm respectievelijk de torenvalk **K** (*kestrel*) en de wouw **KI** (*kite*). De torenvalk antwoordt op een vogel  $x$  altijd met een vogel die enkel  $x$  kan antwoorden (een *constant- $x$*  of *K $x$  bird*). De wouw negeert wat hij hoort en antwoordt steevast met de identiteit, vandaar **KI**.

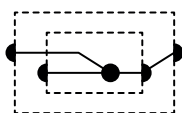


$$\mathbf{K} \equiv \lambda xy . x$$

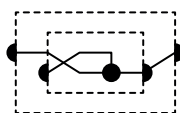


$$\mathbf{KI} \equiv \lambda xy . y$$

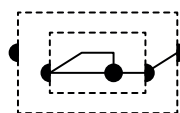
Er bestaan juist vier vogels met twee lagen en één applicator: de *idiot once removed* **I\***, de lijster **T** (*thrush*), de *constant mocker* **K $\omega$**  en de *crossed constant mocker* **C(K $\omega$ )**. De terminologie “once removed” slaat op vogels voorzien van een extra laag, verkregen door een in de bovenste zenuwcel aangebrachte applicator. Deze toestand wordt meteen ongedaan gemaakt als de vogel in kwestie een identiteitsvogel hoort.



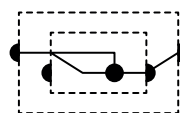
$$\mathbf{I}^* \equiv \lambda xy . x y$$



$$\mathbf{T} \equiv \lambda xy . y x$$



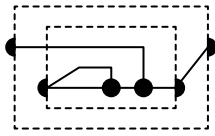
$$\mathbf{K}\omega \equiv \lambda xy . y y$$



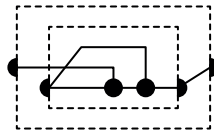
$$\mathbf{C}(\mathbf{K}\omega) \equiv \lambda xy . x x$$

Van de zestien vogels met twee lagen en twee applicatoren zijn deze de bekendste: de leeuwerik **L** (*lark*), de uil **O** (*owl*), de tjiftjaf **W** (*warbler*) en zijn gekruiste variant, de *crossed warbler* **CW**. De tjiftjaf is eigenlijk een spotgaai once removed en kon dus ook genoteerd worden als  $\omega^*$ , maar historisch gezien gaat het gebruik van **W** verder terug dan  $\omega$ . In feite werd de spotgaai zelfs lange tijd als **WI** genoteerd.

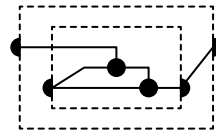




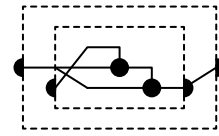
$$\mathbf{L} \equiv \lambda xy . x (y y)$$



$$\mathbf{O} \equiv \lambda xy . y (x y)$$



$$\mathbf{W} \equiv \lambda xy . (x y) y$$



$$\mathbf{CW} \equiv \lambda xy . (y x) x$$

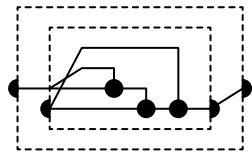
Merk op dat  $\mathbf{LI} = \mathbf{OI} = \mathbf{WI} = \omega$ . Deze figuren illustreren goed twee kenmerken die Keenan beschreef van liedjes: de rijm en het ritme. Het linkergedeelte van het brein, waar alle kruisingen en splitsingen plaatsvinden, stelt de rijm voor. Noteer  $x$  voor de input in de buitenste laag, en  $y$  voor de volgende, dan kan het rijmschema van een liedje gevonden worden door de zenuwcellen af te lezen van boven naar beneden wanneer ze weer horizontaal lopen. De uil heeft bijvoorbeeld schema  $yxy$ ; algemeen zijn er voor een vogel met  $\ell$  lagen en  $a$  applicatoren in totaal  $\ell^{a+1}$  mogelijke rijmschema's.

De sectie met de applicatoren erachter zorgt voor het ritme. De uil en de leeuwerik hebben duidelijk hetzelfde ritme, de uil en de tjiftjaf niet; het eerste ritme wordt  $(-(-))$  genoteerd tegenover  $((--)-)$  voor het tweede. Het aantal van deze uitdrukkingen met  $a$  applicatoren wordt gegeven door het  $a^{\text{de}}$  Catalangetal (zie 228, blz. 190).

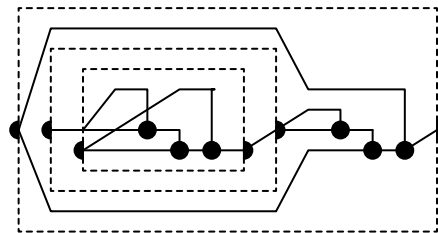
Ritme en rijm bepalen een vogel uniek, dus het totaal aantal vogels met  $\ell$  lagen en  $a$  applicatoren wordt gegeven door  $\ell^{a+1} \cdot C_a$ , oftewel:

$$\frac{\ell^{a+1}}{a+1} \cdot \binom{2a}{a}$$

Enkele belangrijke andere vogels zijn de Turingvogel  $\mathbf{U}$  en de thetavogel  $\mathbf{\Theta}$ , vanzelfsprekend vernoemd naar Alan Turing, die ze ontdekte in 1937. Beiden stellen fixpuntcombinatoren voor.



$$\mathbf{U} \equiv \lambda xy . y ((x x) y)$$



$$\mathbf{\Theta} \equiv \lambda z . ((\lambda xy . y (x x y)) (\lambda xy y (x x y)) z)$$





## 297 Behangpatroongroepen

Patronen worden over heel de wereld volop gebruikt in alle mogelijke culturen, zoals in het oude Egypte of in mozaïeken van islamitische moskeeën. De voorwaarde om van een patroon te spreken, is dat die twee translatiesymmetrieën bezit: door een horizontale of verticale verschuiving moet het patroon identiek blijven. Dit heeft als consequentie dat een patroon zich feitelijk over heel het vlak moet uitstrekken. De translaties hoeven niet loodrecht op elkaar te staan.

Door ook de andere symmetrieën (rotatie, reflectie en glijspiegeling) van deze structuren te bestuderen, slaagde Yevgrav Fyodorov er in 1891 in te bewijzen dat er slechts 17 fundamenteel verschillende patronen zijn, de zogenaamde behangpatroongroepen. George Pólya herontdekte in 1924 ditzelfde resultaat en gaf het meer bekendheid in de wiskundige wereld. De publicaties van Pólya wekten tevens de interesse van grafisch kunstenaar Maurits Escher en inspireerden hem voor diverse werken.

Ondanks het ontzaglijke en ontmoedigende aantal combinaties van symmetrieën, mogelijke posities voor middelpunten of verschillende ordes van symmetrie, worden de mogelijkheden flink beperkt door de stelling van de kristallografische restrictie. Deze stelt dat voor patronen enkel een rotatiesymmetrie van orde 2, 3, 4 of 6 mogelijk is. De stelling is ook van toepassing op driedimensionale structuren (kristallen), waarbij blijkt dat er maar liefst 230 kristallografische (ruimtelijke) groepen zijn.

De 17 behangpatroongroepen worden met diverse notaties beschreven. De meest gangbare is de IUC-notatie (door de International Union of Crystallography in 1952), die ze met vier symbolen benoemt:

- $p$  voor primitieve of  $c$  voor gecentreerde groepen
- 1, 2, 3, 4 of 6 voor de hoogste orde van rotatiesymmetrie
- $m$  voor spiegeling,  $g$  voor glijspiegeling of 1 bij afwezigheid aan spiegeling (horizontaal)
- $m$  voor spiegeling,  $g$  voor glijspiegeling of 1 bij afwezigheid aan spiegeling (verticaal)

John Conways orbifoldnotatie is niet gebaseerd op kristallografische maar op topologische eigenschappen.

- $*$  voor een spiegelsymmetrie
- 2, 3, 4 of 6 vóór de  $*$  voor de ordes van rotatiecentra niet op een spiegelas gelegen (spiralen)
- 2, 3, 4 of 6 na de  $*$  voor de ordes van rotatiecentra wél op een spiegelas gelegen (caleidoscopen)
- $\times$  voor een glijsymmetrie zonder spiegelsymmetrie
- $\circ$  voor structuren met uitsluitend translatiesymmetrie

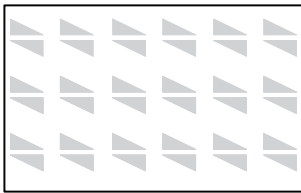
Hier volgt een overzicht van de 17 groepen.



Bevat enkel de twee translatiesymmetrieën.

**IUC:**  $p111$  of  $p1$

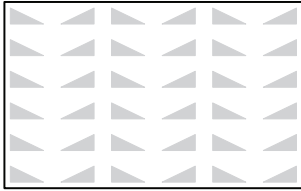
**Orbifold:**  $\circ$



Bevat vier rotatiesymmetrieën van orde 2, over  $180^\circ$ .

**IUC:**  $p211$  of  $p2$

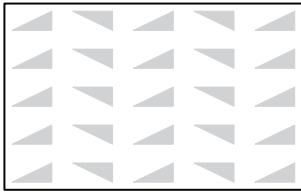
**Orbifold:** 2222



Bevat twee reflectiesymmetrieën, parallel met eenzelfde translatie.

**IUC:**  $p1m1$  of  $pm$

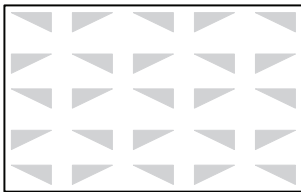
**Orbifold:** \*\*



Bevat twee glijreflecties, evenwijdig met de ene translatie en loodrecht op de andere.

**IUC:**  $p1g1$  of  $pg$

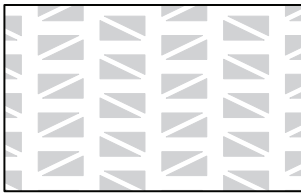
**Orbifold:**  $\times\times$



Bevat spiegelingen en glijspiegelingen, parallel met elkaar.

**IUC:**  $c1m1$  of  $cm$

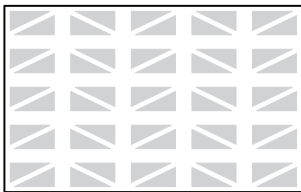
**Orbifold:**  $*\times$



Bevat glijspiegelingen in twee richtingen, loodrecht op elkaar, en twee rotatiesymmetrieën van orde 2, niet op de glijspiegelas gelegen.

**IUC:**  $p2gg$  of  $pgg$

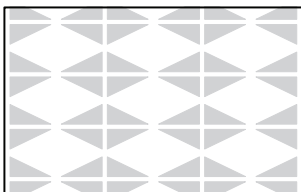
**Orbifold:**  $22\times$



Bevat spiegelingen in één richting, met glijspiegelingen loodrecht erop, en twee rotatiesymmetrieën van orde 2, op de glijspiegelas gelegen.

**IUC:**  $p2mg$  of  $pmg$

**Orbifold:**  $22*$



Bevat spiegelingen in twee richtingen, loodrecht op elkaar, en vier orde-2-rotatiesymmetrieën, op de snijpunten van de spiegellijnen gelegen.

**IUC:**  $p2mm$  of  $pmm$

**Orbifold:**  $*2222$



Bevat spiegelingen in twee richtingen, loodrecht op elkaar, met op hun snijpunten twee orde-2-rotaties, en één orde-2-rotatie, niet op een snijpunt gelegen.

**IUC:**  $c2mm$  of  $cm$

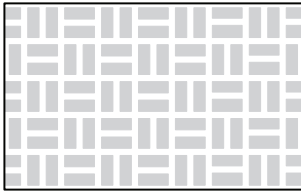
**Orbifold:**  $2*22$



Bevat naast twee rotatiesymmetrieën van orde 4 ook één rotatiesymmetrie van orde 2, zonder (glij-)spiegelsymmetrieën.

**IUC:**  $p411$  of  $p4$

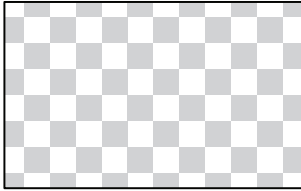
**Orbifold:** 442



Bevat twee spiegelingen, loodrecht op elkaar en met twee glijspiegelingen ertussen (op  $45^\circ$ ), één orde-2-rotatie in hun snijpunt, en één orde-4-rotatie.

**IUC:**  $p4gm$  of  $p4g$

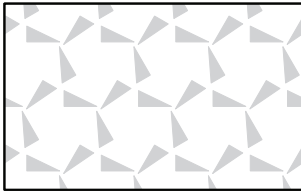
**Orbifold:**  $4*2$



Bevat reflecties in vier richtingen, glijspiegelingen, twee rotatiesymmetrieën van orde 4, en één rotatiesymmetrie van orde 2, allen op de spiegellijnen.

**IUC:**  $p4mm$  of  $p4m$

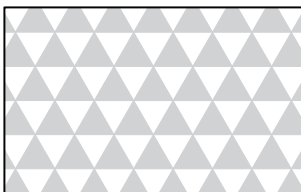
**Orbifold:**  $*442$



Bevat drie rotatiesymmetrieën, elk van orde 3.

**IUC:**  $p311$  of  $p3$

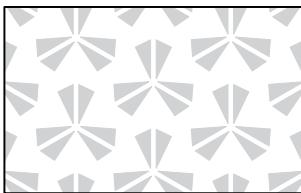
**Orbifold:**  $333$



Bevat drie rotaties van orde 3, allen gelegen op de snijpunten van de spiegellijnen, die hoeken van  $60^\circ$  met elkaar maken.

**IUC:**  $p3m1$

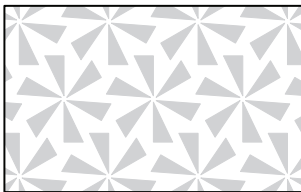
**Orbifold:**  $*333$



Bevat twee rotaties van orde 3, waarvan één gelegen op de snijpunten van de spiegellijnen, die hoeken van  $60^\circ$  met elkaar maken.

**IUC:**  $p31m$

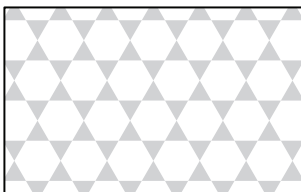
**Orbifold:**  $3*3$



Bevat drie rotatiesymmetrieën, van orde 2, 3 en 6, zonder spiegel- of glijspiegelsymmetrie.

**IUC:**  $p611$  of  $p6$

**Orbifold:**  $632$



Bevat drie rotatiesymmetrieën, van orde 2, 3 en 6, elk gelegen op snijpunten van de spiegellijnen, die zich in 6 richtingen uitstrekken.

**IUC:**  $p6mm$  of  $p6m$

**Orbifold:**  $*632$

Nauw verwant met de behangpatroongroepen zijn de strookpatroongroepen, (zie ??, blz. ??), die slechts in één richting translatiesymmetrie bevatten. Daarvan zijn er juist zeven vormen.

## 298 Quaternionengroep

De quaternionengroep  $Q_8$  of  $\mathbb{H}$  is een niet-abelse groep van orde 8, gebaseerd op de vermenigvuldiging van de basisquaternionen  $1, i, j$  en  $k$ . Ze wordt als volgt gepresenteerd, waarbij  $1$  het eenheidselement voorstelt en ook  $-1$  commuteert met de andere elementen.

$$Q_8 = \langle -1, i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle$$

Deze fundamentele quaternionenformule werd tijdens een wandeling in 1843 ontdekt door de Ier William Hamilton, die de verleiding niet kon weerstaan zijn ontdekking in een steen van de Brougham Bridge te kerven.

De Cayleytabel van  $Q_8$  ziet er als volgt uit:

$\cdot$	1	$i$	$j$	$k$	-1	$-i$	$-j$	$-k$
1	1	$i$	$j$	$k$	-1	$-i$	$-j$	$-k$
$i$	$i$	-1	$k$	$-j$	$-i$	1	$-k$	$j$
$j$	$j$	$-k$	-1	$i$	$-j$	$k$	1	$-i$
$k$	$k$	$j$	$-i$	-1	$-k$	$-j$	$i$	1
-1	-1	$-i$	$-j$	$-k$	1	$i$	$j$	$k$
$-i$	$-i$	1	$-k$	$j$	$i$	-1	$k$	$-j$
$-j$	$-j$	$k$	1	$-i$	$j$	$-k$	-1	$i$
$-k$	$-k$	$-j$	$i$	1	$k$	$j$	$-i$	-1

Een andere manier om de quaternionengroep te bekomen is via twee generatoren  $a$  en  $b$ , elk van orde 4, waar- tussen de volgende relaties gelden:

$$Q_8 = \langle a, b \mid a^2 = b^2, ab = ba^3 \rangle$$

$$1 \sim 1, \quad i \sim a, \quad j \sim b, \quad k \sim ab, \quad -1 \sim a^2, \quad -i \sim a^3, \quad -j \sim a^2b, \quad -k \sim a^3b$$

$Q_8$  kan daarenboven worden voorgesteld als een deelgroep van  $GL_2(\mathbb{C})$ , de algemene lineaire groep der inverteerbare  $2 \times 2$ -matrices over  $\mathbb{C}$ . Aangezien ze allen de eenheidsdeterminant hebben, zitten ze zelfs in de restrictie  $SL_2(\mathbb{C})$ , de speciale lineaire groep. Zie hieronder voor de corresponderende matrices.

$$1 \sim \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad i \sim \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad j \sim \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad k \sim \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

$$-1 \sim \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad -i \sim \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \quad -j \sim \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad -k \sim \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

Volgens de stelling van Cayley (zie ??, blz. ??) bestaat er ook een isomorfisme tussen de quaternionengroep en een permutatiegroep die handelt op 8 elementen. Inderdaad, de corresponderende permutaties worden hieronder weergegeven, naast de andere overeenkomstige voorstellingen. Let wel op de volgorde van de permutaties:  $a \cdot b$  in de originele quaternionen komt overeen met  $b' \circ a'$  in permutaties.

$$1 \sim (1)(2)(3)(4)(5)(6)(7)(8), \quad i \sim (1\ 2\ 3\ 4)(5\ 6\ 7\ 8), \quad j \sim (1\ 5\ 3\ 7)(2\ 8\ 4\ 6), \quad k \sim (1\ 8\ 3\ 6)(2\ 7\ 4\ 5)$$

$$-1 \sim (1\ 3)(2\ 4)(5\ 7)(6\ 8), \quad -i \sim (1\ 4\ 3\ 2)(5\ 8\ 7\ 6), \quad -j \sim (1\ 7\ 3\ 5)(2\ 6\ 4\ 8), \quad -k \sim (1\ 6\ 3\ 8)(2\ 5\ 4\ 7)$$

$Q_8$  is de kleinste niet-abelse groep waarvan alle deelgroepen wel abels zijn, en dit zijn  $\langle -1 \rangle$  met orde 2,  $\langle i \rangle$ ,  $\langle j \rangle$  en  $\langle k \rangle$  met orde 4.

## 299 Rubik's Cube

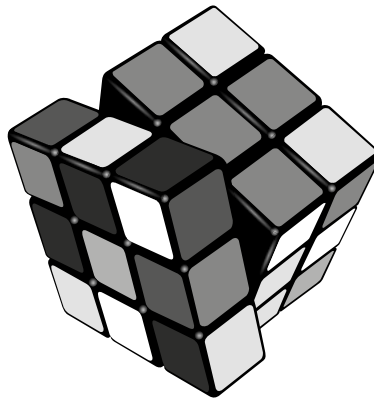
De beroemde Rubik's Cube, ontworpen door Hongaars wiskundige Ernő Rubik, geeft aanleiding tot interessante wiskundige analyses. Bijvoorbeeld, hoeveel configuraties zijn te bereiken door een opgeloste kubus te husselen?

Er zijn 8! mogelijkheden om de acht hoekblokkjes te positioneren, waarvan er zeven onafhankelijk van elkaar

geïoriënteerd kunnen worden op elk drie mogelijkheden (de oriëntering van het achtste hoekblokje ligt vast door de vorige zeven). De 12 randblokjes kunnen worden gepositioneerd op  $\frac{12!}{2}$  mogelijkheden bij vastgekozen hoekblokjes, aangezien een even permutatie van hoekblokjes enkel bij een even permutatie van randblokjes voorkomt. Elf ervan kunnen onafhankelijk van elkaar worden geïoriënteerd, daarna ligt de twaalfde ook vast. Uiteindelijk is het immense totaal aantal mogelijke posities gegeven door:

$$8! \cdot 3^7 \cdot \frac{12!}{2} \cdot 2^{11} = 43.252.003.274.489.856.000$$

Ondanks dit gigantische aantal, is elke initiële configuratie op te lossen in ten hoogste slechts 20 bewegingen\*! In 1995 bewees Michael Reid dat 20 bewegingen ook vereist zijn voor de “superflip”-positie, waarbij de hoeken correct staan en de randen omgedraaid op de goeie plaats. De moeizame ontwikkeling, de intensieve computerberekeningen en het spectaculaire resultaat waren de aanleiding voor de benaming voor 20 als “Gods getal”.



Naast combinatorisch is Rubik's Cube ook groepentheoretisch interessant, aangezien de bewegingen op de puzzel de structuur van een permutatiegroep vormen. De groep  $(G, \cdot)$  bestaat uit de verzameling legale bewegingen, onder de samenstelling ervan als bewerking. Het is duidelijk dat aan de groepsaxioma's voldaan is: de bewerking is gesloten, er bestaat een “lege” beweging  $E$  als identiteitselement, een beweging kan eenvoudigweg teruggedraaid worden als inverse, en ze zijn ook associatief. De standaardnotatie om de bewerking te beschrijven is die van wiskundige David Singmaster:

- $F$ : één kloksgewijze rotatie van het voorvlak
- $B$ : één kloksgewijze rotatie van het achtervlak
- $U$ : één kloksgewijze rotatie van het bovenzvlak
- $D$ : één kloksgewijze rotatie van het ondervlak
- $L$ : één kloksgewijze rotatie van het linkervlak
- $R$ : één kloksgewijze rotatie van het rechtervlak

De kortste manier om de superflippositie op te lossen (in HTM):

$$R \cdot L \cdot U^2 \cdot F \cdot U^{-1} \cdot D \cdot F^2 \cdot R^2 \cdot B^2 \cdot L \cdot U^2 \cdot F^{-1} \cdot B^{-1} \cdot U \cdot R^2 \cdot D \cdot F^2 \cdot U \cdot R^2 \cdot U$$

Merk op dat pakweg  $F \cdot R \neq R \cdot F$ : de groep is niet abels. Elk van deze basisbewegingen heeft orde 4, maar de grootste orde die voorkomt is 1260:  $(R \cdot U^2 \cdot D^{-1} \cdot B \cdot D^{-1})^{1260} = E$ .

Was de Rubikgroep cyclisch geweest, dan had er een vaste combinatie draaiingen bestaan die uiteindelijk altijd de opgeloste kubus teruggeeft (weliswaar na wellicht kolossaal veel draaiingen). De groepsstructuur biedt wel andere mogelijkheden om de puzzel op te lossen. Een algoritme van Morwen Thistlethwaite kan helpen een dooreengegooide kubus op te lossen, via de volgende deelgroepen:

\*Een “beweging” wordt hier gerekend in *half turn metric* (HTM), waarbij elke draai van een zijde over eender welke hoek als één beweging telt. Andere systemen, zoals *quarter turn metric* (QTM), tellen bewegingen per kwartrotatie.



- $G_0 = \langle F, B, U, D, L, R \rangle$ : alle mogelijke uitgangsposities
- $G_1 = \langle F, B, U^2, D^2, L, R \rangle$ : alle mogelijke posities te bereiken vanuit de opgeloste toestand door halve draaien aan de boven- en onderkant, en kwartdraaien aan de andere zijden
- $G_2 = \langle F^2, B^2, U^2, D^2, L, R \rangle$ : alle mogelijke posities te bereiken door kwartdraaien aan de linker- en rechterkant, en halve draaien aan de andere zijden
- $G_3 = \langle F^2, B^2, U^2, D^2, L, R \rangle$ : alle mogelijke posities te bereiken via halve draaien
- $G_4 = \{E\}$ : de opgeloste toestand

Het algoritme tracht een onopgeloste kubus uit  $G_0$  naar  $G_1$  te brengen, daarna naar  $G_2$ , etc. tot de puzzel in  $G_4$  zit en dus opgelost is. Thistlethwaites methode werd nog verbeterd door Herbert Kociemba in 1992.

### 300 Symmetrische groep en permutatiegroepen

Op een verzameling met  $n$  elementen vormen permutaties en diens samenstellingen een groepsstructuur, die niet abels is,  $n!$  als orde bezit en de symmetrische groep  $S_n$  wordt genoemd. Deelgroepen van  $S_n$  heten permutatiegroepen. Elementen van  $S_n$  kunnen worden voorgesteld met behulp van de cykelnotatie, zoals bijvoorbeeld voor deze  $f$  als permutatie op  $\{1, 2, 3, 4, 5\}$ :

$$f : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 4 \\ 3 \mapsto 5 \\ 4 \mapsto 1 \\ 5 \mapsto 3 \end{cases} \quad \Rightarrow \quad f = (1\ 2\ 4)(3\ 5)$$

In deze notatie is het direct duidelijk dat  $f$  twee cyclen bevat en de orde 6 heeft (het kleinste gemeenschappelijke veelvoud van de lengtes van de cyclen). Speciale permutaties die juist twee elementen omwisselen en de andere fixeren, heten transposities. Omdat elke cykel te schrijven is als een samenstelling van transposities, zoals voor  $(1\ 2\ 3\ 4) = (1\ 4) \circ (1\ 3) \circ (1\ 2)$ , geldt dat elke permutatie kan ontbonden worden in transposities. Zo'n ontbinding is echter niet uniek, zelfs niet op volgorde van de transposities na:

$$\begin{aligned} (136)(2457) &= (1\ 5) \circ (3\ 5) \circ (3\ 6) \circ (5\ 7) \circ (1\ 4) \circ (2\ 7) \circ (1\ 2) \\ &= (1\ 6) \circ (1\ 3) \circ (2\ 7) \circ (2\ 5) \circ (2\ 4) \end{aligned}$$

Wat wel invariant blijkt aan een permutatie is de pariteit van het aantal transposities in z'n ontbindingen. Dit geeft aanleiding tot de benaming "even" en "oneven" permutaties (verwijzend naar deze pariteit). Merk op dat de samenstelling van twee even permutaties zelf weer even is, dus vormen deze een deelgroep met orde  $\frac{n!}{2}$ , de alternerende groep  $A_n$  genoemd.

### 301 15-puzzel

De 15-puzzel werd uitgevonden door postbeambte Noyes Chapman. Vooral vanaf 1880 ontketende deze puzzel een ware rage, toen hij werd gebruikt als reclamestunt voor verscheidene producten en er geldprijzen op werden gezet. Sam Loyd, door Martin Gardner "Amerika's grootste puzzelaar en oplichter ooit" genoemd, hield tot aan zijn dood onterecht vol dat hij de feitelijke uitvinder was en de puzzel populariseerde. Loyd zette wel een prijs van \$1.000 op een oplossing van een specifieke combinatie.

De puzzel bestaat uit 15 genummerde blokjes, die door elkaar in een  $4 \times 4$ -doosje gelegd moeten worden met één lege holte. De bedoeling is nu de blokjes naar de standaardrangschikking te schuiven:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	■

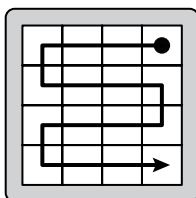
Voor verdere analyse is het zinvol om de blokjes een nieuwe nummering te geven, deze hieronder rechts. De combinatie waarvoor Sam Loyd \$1.000 zou uitreiken indien opgelost is deze links.

4	3	2	1
5	6	7	8
12	11	10	9
13	15	14	■

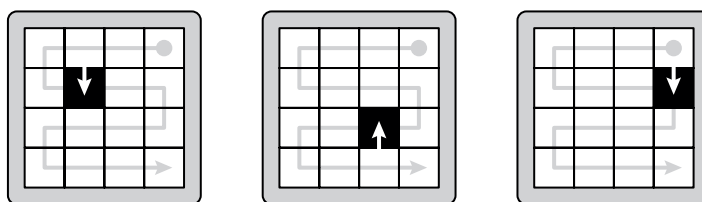
 $\Rightarrow$ 

4	3	2	1
5	6	7	8
12	11	10	9
13	14	15	■

De reden voor deze alternatieve nummering is dat we nu elke configuratie van de 15-puzzel als een permutatie kunnen opgevangen, door de blokjes volgens de pijl hieronder te overlopen en geen rekening te houden met de lege positie. Op deze manier correspondeert de opgeloste toestand juist met de identieke permutatie, op de positie van het gat na, maar deze kan dan eenvoudig doorgeschoven worden naar de plek rechtsonder.



Met behulp van deze nummering is het duidelijk dat een geldige zet van de schuifpuzzel overeenkomt met de samenstelling van de huidige permutatie met een permutatie van lengte 3 óf 5 óf 7, zoals de illustraties hieronder duidelijk maken. Aangezien deze permutaties uitsluitend te ontbinden zijn in een even aantal transposities (zie 300, blz. 290), volgt dat geen enkele oneven permutatie te bereiken is op de 15-puzzel. Dat betekent dat Loyds uitdaging, die overeenkomt met een oneven permutatie, onoplosbaar is!



Omgekeerd is elke even permutatie ook effectief te bereiken. Aangezien de cykel (345) te verkrijgen is (hierboven links) en eveneens de cykel (1 2 3 4 5 6 7) (hierboven rechts), volgt dat ook alle machten van (1 2 3 4 5 6 7) samengesteld met (3 4 5) te verkrijgen is, en dit zijn juist de 3-cykels (1 2 3), ... (5 6 7). Door dezelfde truc toe te passen op de tweede en derde wending van de pijl vinden we álle 3-cykels (1 2 3), ... (13 14 15). Aangezien deze de alternerende groep  $A_{15}$  voortbrengen, volgt inderdaad dat alle even permutaties oplosbaar zijn.

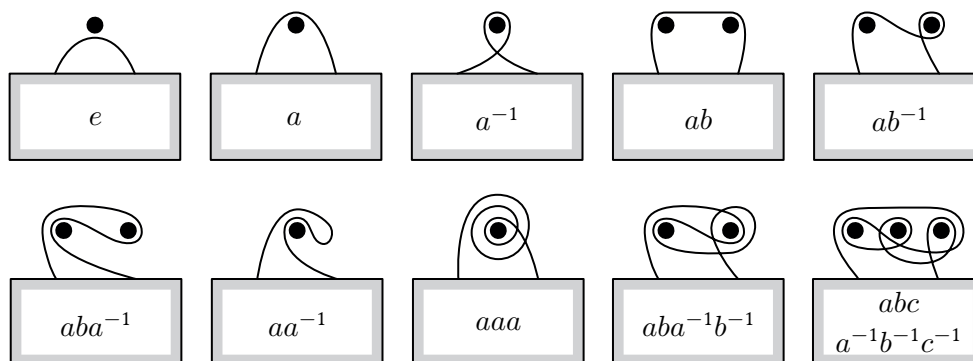
Woolsey Johnson en William Story toonden in 1879 (al voordat Loyd zijn prijsvraag bekendmaakte) via inductie aan dat algemeen, in elk  $m \times n$ -doosje, enkel even permutaties oplosbaar zijn en geen andere. Aaron Archer gaf een eleganter bewijs in 1999 dat gebruikmaakt van equivalentierelaties en Hamiltonpaden (zie 265, blz. 229).

Er werd aangetoond dat elke oplosbare configuratie maximaal 80 bewegingen vereist, of 43 als meerdere blokjes samen mogen worden doorgeschoven. Het minimale aantal zetten vinden is echter NP-moeilijk (zie 322, blz. 313).

## 302 Schilderijen ophangen

Schilderijen kunnen op verschillende manieren worden opgehangen zodat aan bepaalde eisen voldaan worden. Bijvoorbeeld ophangen aan drie spijkers zodat het schilderij valt bij weghalen van eender welke spijker, of zodat het juist blijft hangen bij verwijdering van eender welke twee spijkers; vaak is het geen eenvoudige puzzel zulke configuraties te vinden.

Groepentheorie biedt hier hulp. Noteer de gebruikte spijkers met hoofdletter en noteer  $a$  wanneer het koord kloksgewijs over  $A$  hangt. Zijn inverse,  $a^{-1}$ , betekent dat het koord tegen de klok in over  $A$  ligt. Het identiteitselement  $e$  houdt hier in dat het koord over geen enkele spijker ligt en dus sowieso zal vallen. Aldus krijgt de puzzel een groepsstructuur. De volgende configuraties geven enkele voorbeelden:

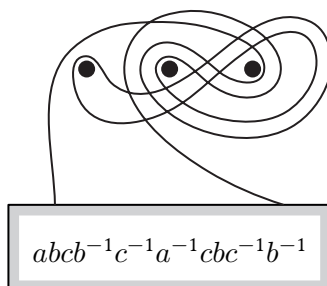


Merk op dat het schilderij direct valt bij  $aa^{-1} = e$ . Bij  $aba^{-1}b^{-1}$  is één spijker uittrekken (gelijk welken) voldoende om het te laten vallen, bij  $aba^{-1}$  blijft het enkel hangen bij verwijdering van spijker  $A$ , terwijl bij  $ab$  de configuratie solide genoeg is om het schilderij op te houden bij verwijdering van eender welke spijker. Algemeen, als de formule horende bij een ophanging herleidt naar  $e$  bij schrapping van alle  $x$  en  $x^{-1}$ , zal het kader vallen bij verwijdering van spijker  $X$ .

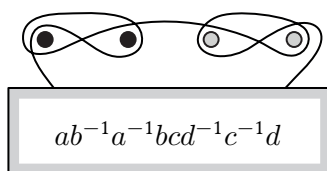
Neil Fitzgerald gaf een eenvoudige recursieve constructie voor een bevestiging aan  $n$  spijkers, waarbij het schilderij valt als eender welke spijker weggenomen wordt. De oplossing met  $n$  spijkers noteren we met  $S_n$ , noem de spijkers  $x_1$  tot  $x_n$ . Oplossingen  $S_n$  kunnen worden gevonden met de volgende recursiebetrekking:

$$S_1 = x_1, \quad S_n = S_{n-1} \cdot x_n \cdot S_{n-1}^{-1} \cdot x_n^{-1}$$

Deze oplossingen worden al gauw vrij complex: het aantal symbolen in  $S_n$  groeit exponentieel als  $2^n + 2^{n-1} - 2$ . Chris Taylor voorzag een constructie waarvan de lengte polynomiaal groeit, ten hoogste als  $2n^2$  (OEIS A073121). De illustratie hieronder beeldt een oplossing met drie spijkers af.



Algemeen kun je een schilderij zodanig om  $n$  spijkers hangen dat het valt als je  $k$  spijkers naar keuze verwijdert, maar blijft hangen bij minder dan  $k$ , voor elke  $1 \leq k \leq n!$  Een andere leuke veralgemening werkt met gekleurde spijkers. In dit voorbeeld blijft het schilderij enkel hangen als er twee spijkers van dezelfde kleur blijven zitten. Je kunt zelfs een schilderij zodanig ophangen aan  $n$  zwarte en  $n$  witte spijkers, dat het valt als je er  $k$  van elke kleur weghaalt, maar blijft hangen als je van minstens één kleur minder dan  $k$  spijkers afhaalt, voor elke  $1 \leq k \leq n$ .



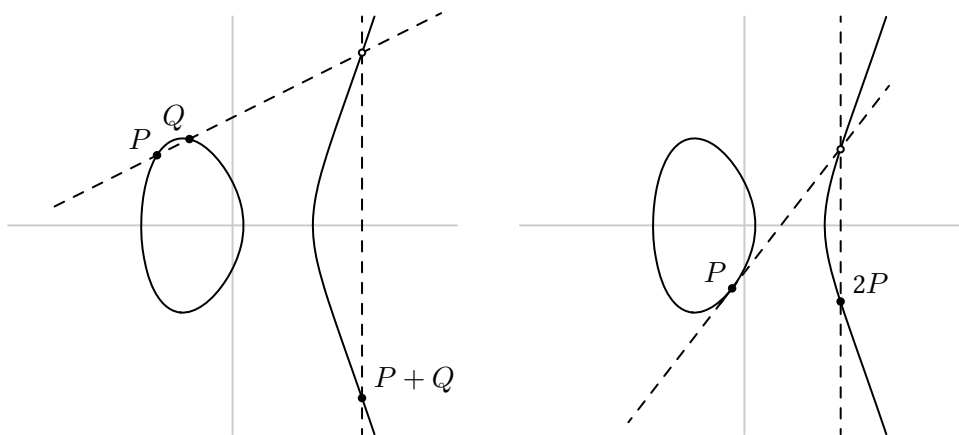
### 303 Groepenwet op elliptische krommen

Elliptische krommen worden besproken in 110, blz. 81. Wanneer we één extra, speciaal punt  $\mathcal{O}$  toevoegen aan de kromme, namelijk het punt op oneindig, verkrijgen we enkele speciale eigenschappen die het mogelijk maken een natuurlijke optelling op de punten van de elliptische kromme te definiëren.

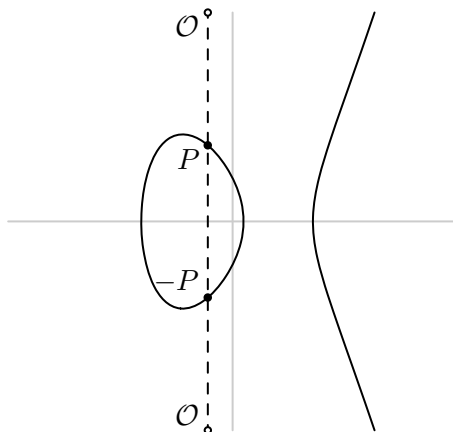
Eenmaal uitgebreid met  $\mathcal{O}$  heeft een rechte door twee punten of een raaklijn aan een punt op een elliptische kromme steeds juist één ander snijpunt. Hiermee definiëren we de optelling van twee punten  $P$  en  $Q$  als volgt:

- Construeer de rechte door  $P$  en  $Q$ .
- Bepaal het derde snijpunt.
- Spiegel dit snijpunt om de  $x$ -as. Dit punt wordt  $P + Q$ .

Een punt optellen bij zichzelf, gebeurt analoog, maar dan via de raaklijn aan  $P$ .



Deze optelling van punten herbergt een groepsstructuur: het punt op oneindig  $\mathcal{O}$  speelt hier de rol van neutraal element, de optelling is gesloten, ook aan de associativiteit is voldaan en voor elk punt  $P$  is een invers punt  $-P$  te vinden zodat de som van de twee  $\mathcal{O}$  oplevert, nl. zijn spiegelbeeld om de  $x$ -as. Dat  $P + Q$  hetzelfde resultaat oplevert als  $Q + P$  is duidelijk uit de constructie en zorgt ervoor dat de groep daarenboven abels is.



Nu is ook duidelijk waarom het snijpunt in de constructie nog gespiegeld moet worden: als dat niet gebeurde, zou de optelling  $P + \mathcal{O}$  als resultaat  $-P$  geven, en is niet voldaan aan het identiteitsaxioma.

Algebraïsch komt de optelling van een punt  $(x_P, y_P)$  met een punt  $(x_Q, y_Q)$  neer op de volgende formules:

$$\begin{cases} x_{P+Q} = s^2 - x_P - x_Q \\ y_{P+Q} = y_P + s(x_{P+Q} - x_P) \end{cases} \quad \text{met } s = \frac{y_P - y_Q}{x_P - x_Q}$$

Verdubbeling van een punt  $(x_P, y_P)$  gaat analoog. De term  $a$  is hier de coëfficiënt van  $x$  in de vergelijking van de elliptische kromme.

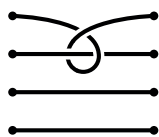
$$\begin{cases} x_{2P} = s^2 - 2x_P \\ y_{2P} = y_P + s(x_{2P} - x_P) \end{cases} \quad \text{met } s = \frac{3x_P^2 - a}{2y_P}$$

Punten met rationale coördinaten op de kromme geven ook een rationale som, zodat deze punten een deelgroep vormen. Een stelling van Louis Mordell en André Weil stelt dat deze deelgroep een eindig aantal generatoren heeft; elk rationaal punt is te bereiken vanuit optellingen van een eindige groep rationale punten.

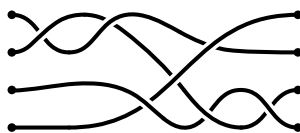
Een concrete toepassing van de groepenwet op elliptische krommen doet zich voor in de cryptografie. Als onderliggend veld wordt niet langer voor  $\mathbb{R}$  gekozen, maar voor het eindig veld  $\mathbb{F}_p$ , met karakteristiek verschillend van 2 of 3 om te garanderen dat de vorm van de vergelijking behouden blijft. Er wordt één bepaald punt  $P$  op de kromme gekozen als “generator” en boodschappen worden versleuteld met een punt  $Q = k \cdot P$ . Over eindige velden is er geen efficiënt algoritme gekend om de waarde van  $k$  te weten te komen uit de waarden van  $Q$  en  $P$ . Het naïeve algoritme is computationeel gezien onhaalbaar voor voldoende grote  $k$ -waarden. Dit geeft aanleiding tot een adequaat versleutelingsmechanisme, Elliptic Curve Cryptography of ECC, dat voordelen biedt tegenover RSA (zie 321, blz. 311): om met RSA hetzelfde beveiligingsniveau te bereiken is een veel grotere sleutel nodig: een 256-bit ECC-sleutel verschaft vergelijkbare beveiliging als een 3072-bit RSA-sleutel.

## 304 Vlechtgroepen

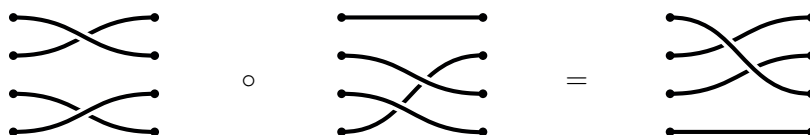
De vlechtgroepen,  $B_n$  genoteerd, zijn een familie oneindige groepen met een intuïtieve meetkundige betekenis. Ze werden voor het eerst expliciet vermeld door Emil Artin in 1925 en eerder al impliciet door Adolf Hurwitz. Begin met een kubus en plaats er  $n$  strengen in, die vertrekken aan het bovenste zijvlak en toekomen aan het onderste, elkaar niet snijden, en uitsluitend naar beneden gaan om geen knopen te bekomen. Een voorbeeld van een structuur die we willen vermijden, is deze (horizontaal getekend):



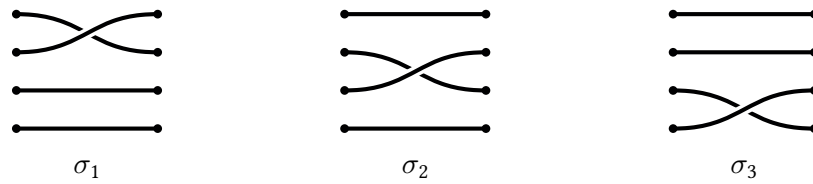
De volgende structuur stelt wel een geldige vlecht uit  $B_4$  voor. Vlechten die in elkaar om te zetten zijn door de strengen over elkaar te halen, worden als gelijk beschouwd. Vergelijk dit met de Reidemeisterbewegingen (zie 223, blz. 179) van toepassing op knopen.



Deze vlechten kunnen op een natuurlijke wijze worden samengesteld, door de vlechten achter elkaar te zetten en de overeenkomstige strengen te verbinden.



Deze samenstelling vormt een groepsstructuur, met de vlecht bestaande uit  $n$  horizontale strengen als eenheid en het spiegelbeeld van een vlecht om een verticale as als inverse. Over het algemeen is deze groep niet commutatief. De volledige groep op  $n$  strengen wordt voortgebracht door  $n - 1$  generatoren:



De relaties die de groepsstructuur volledig vastleggen kunnen zowel meetkundig als algebraïsch geïnterpreteerd worden. Er geldt duidelijk dat  $\sigma_1\sigma_3 = \sigma_3\sigma_1$  in de voorbeelden hierboven, en uitgetekend blijkt ook dat  $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$  en  $\sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3$ . Deze relaties volstaan voor  $B_4$ . Algemener:

$$B_n = \left\langle \sigma_1, \sigma_2, \dots, \sigma_{n-1} \left| \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{voor } |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & \text{voor } 1 \leq i \leq n-2 \end{array} \right. \right\rangle$$

Merk op dat  $B_1$  de triviale groep is,  $B_2$  isomorf is met  $(\mathbb{Z}, +)$  en verdere  $B_n$  niet-abels zijn. Daarenboven is  $B_n$  torsievrij: alle elementen verschillend van de identiteit hebben oneindige orde.

James Alexander bewees dat elke knoop of link in feite te beschouwen is als de sluiting van een bepaalde vlecht (het resultaat van overeenkomstige linker- en rechtereindpunten rechtstreeks te verbinden). Wegens de eenvoud om vlechten te beschrijven als woorden van hun generatoren vormt dit een handige methode om knopen te beschrijven of in te geven in computerprogramma's.







## 305 Knuths pijlomhoognotatie

Donald Knuth, grondlegger van  $\text{\TeX}$  en door velen beschouwd als de vader van de informatica, introduceerde de pijlomhoognotatie in 1976 als notatie voor enorm grote getallen, waar de klassieke decimale notatie veel te veel plaats zou innemen. Zijn idee is gebaseerd op de definities van vermenigvuldiging als een herhaalde optelling en machtsverheffing als een herhaalde vermenigvuldiging.

$$a \cdot b = \underbrace{a + a + \dots + a}_{b \text{ termen}}$$

$$a^b = \underbrace{a \cdot a \cdot \dots \cdot a}_{b \text{ factoren}}$$

De optelling kan zelf ook gedefinieerd worden op basis van een lagere-ordefunctie: Peano's opvolgerfunctie  $S(n)$ , die voorkomt in zijn axioma's voor de getaltheorie.

$$a + b = \underbrace{S(S(\dots S(a) \dots))}_{b \text{ argumenten}}$$

Deze herhaalde bewerkingen inspireerden Knuth tot een bewerking van hogere orde, gedefinieerd als een herhaalde machtsverheffing. Hij noteerde  $a \uparrow b$  voor  $a^b$ ; de uitbreiding schreef hij als een dubbele pijl.

$$a \uparrow\uparrow b = \underbrace{a^{a^{\dots^a}}}_{b \text{ kopieën van } a} = \underbrace{a \uparrow (a \uparrow (\dots \uparrow a))}_{b \text{ kopieën van } a}$$

Analoog volgde de driedubbele pijl:

$$a \uparrow\uparrow\uparrow b = \underbrace{a \uparrow\uparrow a \uparrow\uparrow \dots \uparrow\uparrow a}_{b \text{ kopieën van } a}$$

De notatie  $a \uparrow^n b$  wordt nu algemeen gebruikt voor  $a \uparrow\uparrow \dots \uparrow b$ , met  $n$  pijltjes:

$$a \uparrow^n b = \underbrace{a \uparrow^{n-1} a \uparrow^{n-1} \dots \uparrow^{n-1} a}_{b \text{ kopieën van } a}$$

Merk op dat Knuths pijlomhoogoperaties niet langer commutatief of associatief zijn, enkel rechtsassociatief. Zie ook het verband met de hyperoperatie (zie 306, blz. 298).

## 306 Hyperoperatie

De hyperoperatie  $H_n : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ , is een rekenkundige functie die twee argumenten vereist voor een bijbehorende index  $n \in \mathbb{N}$ . Het opmerkelijke eraan is dat zowel de simpele opvolgerfunctie, optelling, vermenigvuldiging, machtsverheffing en verdere pijlomhoogoperaties (zie 305, blz. 298) in één functie recursief gedefinieerd

zitten, namelijk als volgt:

$$H_n(a, b) = \begin{cases} b + 1 & \text{als } n = 0 \\ a & \text{als } n = 1, b = 0 \\ 0 & \text{als } n = 2, b = 0 \\ 1 & \text{als } n \geq 3, b = 0 \\ H_{n-1}(a, H_n(a, b - 1)) & \text{anderzijds} \end{cases}$$

Voor  $n = 0, 1, 2, 3$  levert dat bekende operaties op, voor  $n \geq 4$  de pijlomhoognotatie van Knuth (zie 305, blz. 298).

- $H_0(a, b) = b + 1$
- $H_1(a, b) = a + b$
- $H_2(a, b) = a \cdot b$
- $H_3(a, b) = a^b$
- $H_4(a, b) = a \uparrow\uparrow b$
- $H_5(a, b) = a \uparrow\uparrow\uparrow b$
- ...
- $H_n(a, b) = a \uparrow^{n-2} b$  voor  $n \geq 3$

In  $H_n(a, b)$  wordt  $n$  de graad,  $a$  het grondtal en  $b$  de (hyper-)exponent genoemd.

In 1926 definieerde Wilhelm Ackermann zijn functie  $\phi(a, b, n)$ , die vrij gelijkaardig werkt als de hyperoperatie; de laatste werd pas beschreven in 1947 door Reuben Goodstein, die tevens de nieuwe benamingen *tetratie*, *pentatie*, *hexatie* . . . voor de nieuwe bewerkingen (corresponderend met de indices 4, 5, 6 . . .) voorstelde. Ackermanns  $\phi$ -functie verschilt in de hyperoperatie omdat die in  $n = 0$  direct begint met de optelling, de opvolgerfunctie dus overslaand.

## 307 De indringer

Een klassiek probleem bij IQ-tests is het vinden van een indringer in een lijst, het symbool dat niet thuishoort in een gegeven reeks symbolen. Tanya Khovanova wist hierop een mooie variant te bouwen, geïnspireerd door Martin Gardner. Welk symbool past niet in dit rijtje?



Het standaard antwoord op deze vraag is de eerste. Die is namelijk speciaal omdat hij geen afwijkende eigenschappen bezit: de tweede heeft als enige geen onderscheiden rand, de derde is cirkelvormig, de vierde wijkt af van kleur en de vijfde van grootte. Enkel de eerste heeft geen unieke eigenschappen en is dus de indringer.

## 308 Boom van Pythagorasdrietallen

Drietallen van Pythagoras zijn 3-tupels natuurlijke getallen die lengtes van zijden van een rechthoekige driehoek kunnen vormen, dus tupels  $(a, b, c) \in \mathbb{N}^3$  waarvoor  $a^2 + b^2 = c^2$ . Wanneer  $(a, b, c)$  een Pythagorasdrietal is, dan is elk veelvoud  $(ka, kb, kc)$  daarvan dat ook; een tupel wordt primitief genoemd als z'n elementen geen gemeenschappelijke factoren hebben. Er bestaan oneindig veel primitieve Pythagorasdrietallen.

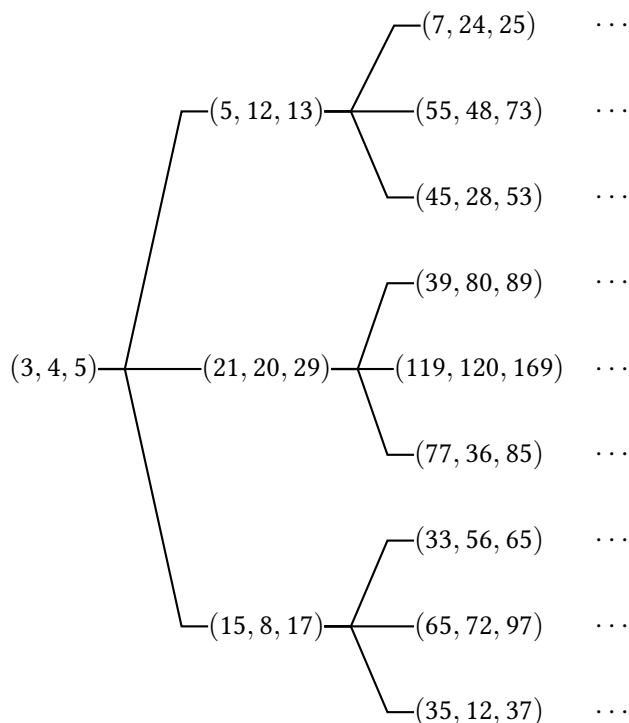
Voor natuurlijke  $m$  en  $n$  (met  $m > n$ ) kan zo'n drietal  $(a, b, c)$  gegenereerd worden via een formule van Euclides. Wanneer  $m$  en  $n$  relatief priem en niet beiden oneven zijn, wordt het resultaat bovendien een primitief drietal.

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2$$

Freek Barning beschreef in 1963 een opmerkelijke alternatieve genereermethode die gebruikmaakt van matrices. Wanneer je één van volgende matrices rechts vermenigvuldigt met een kolommatrix met een Pythagorasdrietal als elementen, zal het product nog steeds zo'n drietal zijn.

$$A = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix}, \quad C = \begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix}$$

Vertrekkend vanuit het drietal  $(3, 4, 5)$  kun je zo elk primitief Pythagorasdrietal bereiken, uitsluitend door links te vermenigvuldigen met deze matrices! Dit proces kan grafisch worden geïnterpreteerd als een ternaire boomstructuur, waarin elke tak dus een nieuw primitief drietal bevat.



Voor een vooropgesteld drietal  $(a, b, c)$  blijft het verschil tussen  $b$  en  $c$  bewaard bij vermenigvuldiging met  $A$ , het verschil tussen  $a$  en  $b$  bij vermenigvuldiging met  $B$  en tussen  $a$  en  $c$  bij vermenigvuldiging met  $C$ .

### 309 Vier-9's-puzzel

Iedereen is vertrouwd met de puzzels waarin gevraagd wordt een bepaald getal te schrijven als een uitdrukking met een aantal gegeven symbolen. Probeer bijvoorbeeld eens het getal 8 uit te drukken door middel van twee 7's en twee 9's.

$$8 = \frac{9 + 7}{9 - 7} = 7 + 7^{9-9} = 9 - 9^{7-7}$$

De bekendste versie is misschien de vier-9's-puzzel, waarin de bedoeling is de natuurlijke getallen uit te drukken met vier 9's. Oorspronkelijk mochten enkel optellen, aftrekken, vermenigvuldigen en delen gebruikt worden

(met de haakjes natuurlijk), in een modernere versie ook machtsverheffing, worteltrekking, faculteiten en bijzondere functies als de floorfunctie. Bijvoorbeeld:

$$16 = 9 + (\sqrt{9})! + \frac{9}{9}, \quad 23 = \frac{((\sqrt{9})!)!}{(\sqrt{9})! \cdot (\sqrt{9})!} + \sqrt{9}, \quad 61 = \left[ \sqrt{\sqrt{\sqrt{\sqrt{(9 \cdot \sqrt{9})!}}}]} + \frac{9}{\sqrt{9}} \right]$$

Zoals te zien aan deze voorbeelden kunnen deze uitdrukkingen al gauw vrij complex worden. Een hele lijst tot nog toe bekende oplossingen staat op <http://magicdragon.com/EmeraldCity/Nonfiction/four9s.html>.

Terry Moore bedierf de pret echter een beetje met een uitdrukking die vier 9's bevat en die *elk* natuurlijk getal kan voorstellen. Met zijn formule gaf hij dus een algemene oplossing voor de vier-9's-puzzel, voor gans  $\mathbb{N}$ .

$$\frac{\log \log 9 - \log \log \overbrace{\sqrt{\sqrt{\dots \sqrt{9}}}}^{n \text{ wortels}}}{\log(0.\overline{9} + 0.\overline{9})} = n$$

Merk op dat  $0.\overline{9}$  (repetierend) hier gebruikt wordt om 1 aan te geven, zij het nog steeds uitgedrukt door middel van één 9. Vul in de bovenstaande uitdrukking het juiste aantal worteltekens in en elk willekeurig natuurlijk getal is uitgedrukt volgens de spelregels. De logaritmes kunnen eenvoudig worden uitgewerkt ter bewijs.

Een analoge puzzel vraagt uitdrukkingen van zo veel mogelijk getallen door middel van juist één 0, 1, 2, 3, 4, 5, 6, 7, 8 en 9. Ook hier werd een algemene oplossing gevonden, door Verner Hoggatt.

$$\frac{\log \log 9 - \log \log \overbrace{\sqrt{\sqrt{\dots \sqrt{-6 + 7 + 8}}}}^{n \text{ wortels}}}{\log(0 + 1 + 2 + 3 + 4) - \log 5} = n$$

## 310 18-puntenprobleem

Martin Gardner noemde dit vreemde probleem in zijn column in de *Scientific American*. Het doel is om 18 punten te verdelen op een lijnstuk, volgens deze eenvoudige regels:

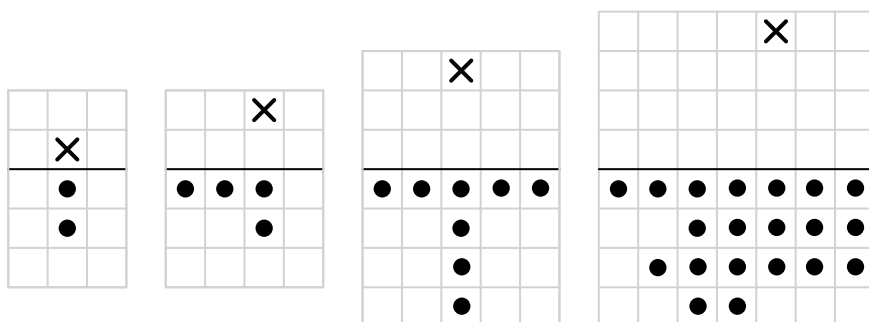
- Plaats een punt op het lijnstuk.
- Plaats een tweede punt op het lijnstuk, zodat de twee punten elk op een verschillende helft liggen.
- Plaats een derde punt erbij, zodat de drie punten elk op een verschillend derde deel liggen.
- Plaats een vierde punt erbij, zodat de vier punten elk op een verschillend kwart liggen.
- Plaats een vijfde punt erbij, zodat de vijf punten elk op een verschillend vijfde deel liggen.
- ...

Het is begrijpelijk dat de punten niet lukraak gekozen kunnen worden, of het spel loopt snel vast. Opmerkelijk genoeg, hoe zorgvuldig de punten ook geplaatst worden, is het onmogelijk verder te geraken dan 17 punten; ten laatste het 18<sup>de</sup> punt zal altijd de spelregels schenden!

## 311 Conways soldaten

Dit probleem werd geanalyseerd door John Conway, in 1961. In deze variant op het klassieke éénpersoonsspel Solitaire, krijg je beschikking over een oneindig groot speelbord, verdeeld door een horizontale lijn, en een willekeurige voorraad pionnen (soldaten) in een vrij te kiezen beginconfiguratie. Door de standaard Solitairezet

(één soldaat springt over een andere die horizontaal of verticaal aangrenst en na de sprong verwijderd wordt) is het de bedoeling zo ver mogelijk over de horizontale lijn te geraken.



Het is snel aangetoond dat er minimum twee stukken nodig zijn om de eerste lijn te bereiken, vier stukken voor de tweede, acht voor de derde en twintig voor de vierde, mogelijk met bovenstaande configuraties. Verrassend genoeg, over hoeveel soldaten je ook beschikt, is het onmogelijk om verder te geraken dan de vierde lijn!

Simon Tatham en Gareth Taylor konden bewijzen dat de vijfde rij wél toegankelijk is met een oneindige reeks zetten (zie daarvoor <http://www.chiark.greenend.org.uk/~sgtatham/solarmy>). Ook wanneer diagonale zetten toegestaan zijn, kunnen de soldaten verder geraken: tot aan de achtste rij.

## 312 Russisch vermenigvuldigen

Dit praktische algoritme om vermenigvuldigingen uit te rekenen, was de oude Egyptenaren al bekend, en werd tot in moderne tijden nog gebruikt door Russische boeren die geen opleiding genoten hadden, vandaar de naam. Het algoritme vereist geen kennis van de tafels, alleen van optellen, verdubbelen en halveren.

1. Schrijf de twee te vermenigvuldigen getallen naast elkaar, bovenaan twee kolommen.
2. Halveer het getal in de eerste kolom en rond af naar beneden (negeer halve getallen), en verdubbel het getal in de tweede kolom.
3. Herhaal stap 2 totdat het getal in de eerste kolom 1 wordt.
4. Tel nu alle getallen uit de rechterkolom samen waar zijn buur in de linkerkolom oneven is; de som hiervan is het product van de twee originele getallen.

Beschouw als voorbeeld het product  $38 \times 31$ :

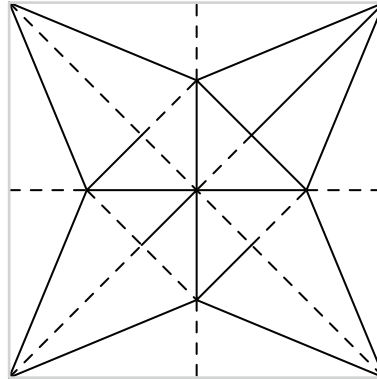
38	×	31	
38		<del>31</del>	
19		62	62
9		124	+124
4		<del>248</del>	
2		<del>496</del>	
1		992	+992
			= 1178

## 313 Origamistellingen

Zoals de axioma's van Huzita-Justin bewijzen (zie 318, blz. 309), valt er heel wat wiskunde te beleven met geplooid papier. Enkele volwaardige stellingen vormen zelfs het hart van de vlakke origami.

### 313.1 Stelling van Maekawa

Beschouw een vouwpatroon van een reglementair gevouwen vlak origamiwerk. Een eerste bekende resultaat, vernoemd naar Jun Maekawa, is dat het aantal bergvouwen en het aantal dalvouwen rondom een bepaald snijpunt steeds 2 verschillen. Dit geldt niet altijd voor origami in 3D: bepaalde technieken om papier driedimensionaal te maken, kunnen uitzonderingen vormen.



### 313.2 Stelling van Kawasaki

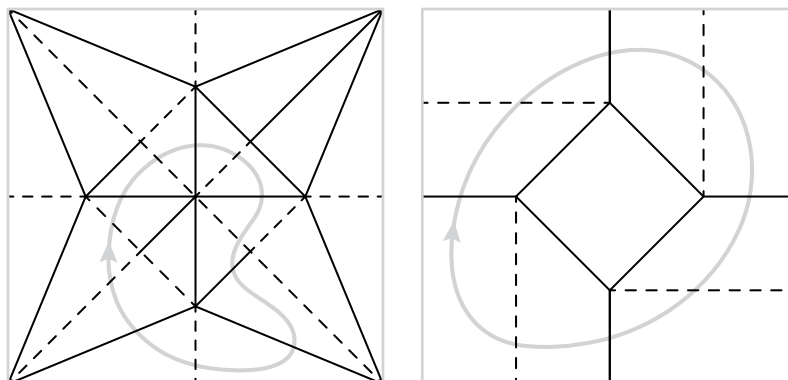
De stelling van Toshikazu Kawasaki geeft een criterium voor vlakke origami met betrekking tot hoeken. Rondom elk punt moeten de gevouwen hoeken in aantal even zijn ( $\alpha_1, \alpha_2 \dots \alpha_{2n}$ ) en om en om optellen tot  $180^\circ$ :

$$\alpha_1 + \alpha_3 + \dots + \alpha_{2n-1} = \alpha_2 + \alpha_4 + \dots + \alpha_{2n} = 180^\circ$$

Omdat de stelling in twee richtingen geldt, kan deze dienen als lokale test voor vlakheid bij een gegeven vouwpatroon. Echter, een *globale* test voor “platvouwbaarheid” is een NP-compleet probleem (zie 322, blz. 313) en dus heel wat moeilijker!

### 313.3 Stelling van Justin

Jacques Justin, die de zeven origami-axioma's beschreef, ontdekte tevens een complexere maar algemenere versie van bovenstaande stellingen. Teken een gesloten kromme op een vlak vouwpatroon, snijpunten tussen vouwen ontwijkend, zoals hieronder.



Hier zal de curve een even aantal vouwen snijden, maar de stelling van Maekawa is niet rechtstreeks toepasbaar. Ook kunnen de hoeken  $\alpha_1, \alpha_2, \dots, \alpha_{2n}$  bepaald worden als de hoeken tussen twee elkaar opvolgende vouwen op de curve, positief als het hoekpunt aan de binnenzijde van de curve ligt en negatief als die erbuiten ligt. Voor het linkerdiagram worden de hoeken bijvoorbeeld, vanaf de pijl:

$$90^\circ, -45^\circ, 45^\circ, 45^\circ, 45^\circ, 45^\circ, 45^\circ, -90^\circ, 67,5^\circ, 67,5^\circ, 67,5^\circ, -22,5^\circ$$

In het rechterdiagram zijn de hoeken afwisselend  $0^\circ$  en  $90^\circ$ . Kawasaki's stelling houdt hier dus evenmin stand! De uiteindelijke stelling van Justin is echter wél voor elke curve in elk diagram voor vlakke origami geldig:

$$\alpha_1 + \alpha_3 + \dots + \alpha_{2n-1} = \alpha_2 + \alpha_4 + \dots + \alpha_{2n} = \pi \cdot \frac{M - V}{2} \pmod{2\pi}$$

### 314 Eulers 36 officieren

Leonhard Euler deed onderzoek naar een uitbreiding op Latijnse vierkanten\* toen hij het concept der Grieks-Latijnse vierkanten (ook wel Eulervierkanten) bedacht: roosters die koppels getallen of symbolen bevatten, zodanig dat elk symbool uniek voorkomt in elke rij en kolom en geen twee koppels dezelfde zijn. Bijvoorbeeld voor een  $3 \times 3$ -Grieks-Latijns vierkant:

$A\alpha$	$B\gamma$	$C\beta$
$B\beta$	$C\alpha$	$A\gamma$
$C\gamma$	$A\beta$	$B\alpha$

Euler zag in dat zo'n configuratie onmogelijk is voor een  $2 \times 2$ -rooster, en slaagde er ook niet in een  $6 \times 6$ -rooster te vullen. Vandaar dus het volgende probleem uit 1782, dat neerkomt op de constructie van een  $6 \times 6$ -Grieks-Latijns vierkant:

KAN EEN DELEGATIE VAN 36 OFFICIEREN (ZES REGIMENTEN MET ELK EEN KOLONEL, EEN LUITENANT-KOLONEL, EEN MAJOR, EEN KAPITEIN, EEN LUITENANT EN EEN ONDERLUITENANT) ZODANIG IN EEN VIERKANTE OPSTELLING GEPLAATST WORDEN DAT IN GEEN ENKELE RIJ OF KOLOM EENZELFDE GRAAD OF REGIMENT MEERDERE KEREN VOORKOMT?

Euler vermoedde dat het probleem onoplosbaar is. Hij ging nog verder door te beweren dat er geen Grieks-Latijnse vierkanten van orde 2, 6, 10, 14, ... bestaan, maar dit bleef algemeen onbewezen. Gaston Tarry bewees pas in 1901 door uitputting van alle mogelijke combinaties (met de hand!) dat Grieks-Latijnse vierkanten van orde 6 niet bestaan zijn en loste daarmee het officierenprobleem op.

In tegenstelling tot wat Euler echter vermoedde, bestaan vierkanten van orde 10 en hoger wél: in 1959 construeerden Sharadchandra Shrikhande en Raj Bose een tegenvoorbeeld van orde 22, waarna Ernest Parker deze hieronder vond van orde 10 via computerberekeningen. In april 1959 publiceerden Parker, Bose en Shrikhande een paper waarin ze Eulers vermoeden als vals bewezen voor  $n \geq 10$ . Dus samengevat, bestaan er Grieks-Latijnse vierkanten van willekeurige orde  $n \geq 3$ , behalve voor  $n = 6$ .

---

\*Latijnse vierkanten zijn getallenroosters waarin geen twee dezelfde getallen voorkomen in één rij of kolom.

A $\alpha$	B $\iota$	G $\gamma$	I $\kappa$	D $\epsilon$	E $\zeta$	C $\theta$	F $\beta$	J $\eta$	H $\delta$
C $\kappa$	G $\eta$	H $\iota$	D $\gamma$	I $\alpha$	F $\epsilon$	E $\beta$	B $\theta$	A $\delta$	J $\zeta$
E $\theta$	C $\alpha$	D $\delta$	J $\iota$	F $\gamma$	I $\eta$	B $\epsilon$	H $\kappa$	G $\zeta$	A $\beta$
H $\epsilon$	E $\kappa$	C $\eta$	F $\zeta$	A $\iota$	B $\gamma$	I $\delta$	J $\alpha$	D $\beta$	G $\theta$
I $\zeta$	J $\epsilon$	E $\alpha$	C $\delta$	B $\beta$	G $\iota$	H $\gamma$	A $\eta$	F $\theta$	D $\kappa$
J $\gamma$	I $\beta$	A $\epsilon$	E $\eta$	C $\zeta$	H $\theta$	D $\iota$	G $\delta$	B $\kappa$	F $\alpha$
F $\iota$	A $\gamma$	I $\theta$	G $\epsilon$	E $\delta$	C $\beta$	J $\kappa$	D $\zeta$	H $\alpha$	B $\eta$
G $\beta$	D $\theta$	F $\kappa$	B $\alpha$	H $\eta$	J $\delta$	A $\zeta$	I $\iota$	C $\gamma$	E $\epsilon$
D $\eta$	F $\delta$	B $\zeta$	H $\beta$	J $\theta$	A $\kappa$	G $\alpha$	C $\epsilon$	E $\iota$	I $\gamma$
B $\delta$	H $\zeta$	J $\beta$	A $\theta$	G $\kappa$	D $\alpha$	F $\eta$	E $\gamma$	I $\epsilon$	C $\iota$

In 1725 beschreef Jacques Ozanam al een Grieks-Latijns  $4 \times 4$ -vierkant als een puzzel met speelkaarten.

## 315 Kiessystemen

Kenneth Arrow was een Amerikaans econoom en won op 51-jarige leeftijd (tot op heden de jongste leeftijd) de Nobel Memorial Prize in Economics. Hij publiceerde een verrassend resultaat met betrekking tot kiessystemen. Deze systemen zijn op zich al bijzonder, omdat verschillende methoden ook verschillende resultaten kunnen geven bij gelijke stemmen. Ze worden hieronder besproken en toegepast op deze fictieve verkiezing:

#	A	B	C	D	E
18	5	1	2	4	3
12	1	5	3	4	2
10	2	5	4	1	3
9	4	5	1	2	3
4	2	5	3	4	1
2	4	5	3	2	1

De getallen aan de linkerkolom staan voor het aantal personen die deze volgorde van voorkeur opgeven. Zo zijn er tien personen die kandidaat D prefereren, en zes die een voorkeur hebben voor kandidaat E.

### 315.1 Meerderheid

Het meest rechttoe rechtaan is de rangschikking door meerderheid: de kandidaat met de meeste stemmen op de eerste plaats, wint. Bij gelijke stemmen wordt verder gekeken naar de tweede plaats, etc.

In het voorbeeld zou kandidaat B dus gewonnen zijn; die kreeg het hoogste resultaat van 18 stemmen.

### 315.2 Meerderheid met run off

Bij een run off stemming worden eerst de twee kandidaten met de meeste voorkeuren bepaald. Daarna wordt gekeken hoeveel stemmers de eerste kandidaat boven de tweede verkozen en vice versa. Wie van de twee zo het grootste aantal stemmers achter zich heeft, wint.

In het voorbeeld heeft kandidaat B 18 voorkeursstemmen behaald en kandidaat A 12. In het algemeen echter wordt A boven B verkozen door 37 personen, en B boven A slechts door 18 personen; de winnaar wordt dus A.



### 315.3 Opeenvolgende run off

Deze methode werkt de omgekeerde richting. Eerst wordt de kandidaat met de minste voorkeursstemmen geëlimineerd uit de ranking, en worden de andere stemmen hernummerd. Dit proces wordt herhaald tot er nog maar twee kandidaten over zijn, en de winnaar is die met de meeste (telkens hernummerde) voorkeursstemmen.

Kandidaat E heeft in het voorbeeld slechts zes voorkeursstemmen en wordt daarom uitgeschakeld. De stemmen hernummeren geeft de volgende tabel:

#	A	B	C	D
18	4	1	2	3
12	1	4	2	3
10	2	4	3	1
9	3	4	1	2
4	1	4	2	3
2	3	4	2	1

Nu verliest C met negen stemmen en wordt de volgende stap:

#	A	B	D
18	3	1	2
12	1	3	2
10	2	3	1
9	2	3	1
4	1	3	2
2	2	3	1

Kandidaat A verliest met zestien stemmen, en enkel B en D schieten nog over.

#	B	D
18	1	2
12	2	1
10	2	1
9	2	1
4	2	1
2	2	1

Nu is het duidelijk dat D de uiteindelijke winnaar in dit kiessysteem wordt.

### 315.4 Bordatelling

Deze methode, vernoemd naar Frans wiskunde en politicoloog Jean-Charles de Borda, bestaat erin punten toe te kennen aan de plaatsen in elke voorkeursvolgorde. Een eerste plaats is 5 punten waard, een tweede plaats 4, een derde plaats 3, een vierde plaats levert 2 punten op en een vijfde plaats in de ranglijst slechts 1 punt. Volgens de Bordatelling wint diegene dan met de meeste punten.

We werken de Bordatelling uit voor kandidaat A in het voorbeeld.

plaats	punten	# stemmen	# punten
1	5	12	60
2	4	14	56
3	3	0	0
4	2	11	22
5	1	18	18
totaal aantal punten:			156

Analoog vinden we 127 punten voor B, 191 punten voor C, 162 voor D en 189 voor E, zodat C hier als winnaar uit de bus komt.

### 315.5 Condorcetmethode

De Condorcetmethode is een alternatief kiessysteem dat niet altijd een winnaar oplevert. De Condorcetwinnaar is diegene die wint bij vergelijking met alle andere kandidaten in een één-tegen-éénconfrontatie. Wanneer de Condorcetmethode geen winnaar oplevert, moet een ander kiessysteem aangewend worden.

Beschouw als voorbeeld kandidaat D, vergeleken met de andere kandidaten:

kandidaat	voorkeur	vergeleken met D	winnaar
A	16	←→ 39	D
B	18	←→ 37	D
C	43	←→ 12	C
E	36	←→ 19	E

D wint bij vergelijking met de anderen in twee van de vier gevallen, en is dus geen Condorcetwinnaar. Kandidaat E echter wordt hier wél overal verkozen boven alle anderen in één-tegen-éénconfrontaties!

kandidaat	voorkeur	vergeleken met E	winnaar
A	22	←→ 33	E
B	18	←→ 37	E
C	27	←→ 28	E
D	19	←→ 36	E

### 315.6 Arrows onmogelijkheidsstelling

Er bestaat een heel wiskundig framework rond kiessystemen: *social choice theory*. Door middel van *social welfare functions* wil men uit individuele voorkeuren of waarden een collectieve beslissing maken. De monografie *Social Choice and Individual Values* van Kenneth Arrow uit 1951 legde de basis voor deze theorie.

Wat vooral opvalt aan de kiessystemen hierboven is dat elk van de vijf systemen tot een andere winnaar leidt. Een redelijke vraag zou dus zijn, welk van deze systemen het meest “eerlijk” is (en dus in praktijk aangewezen zou zijn). Een ideaal kiesstelsel zou moeten voldoen aan de volgende eisen:

- **Individuele soevereiniteit:** elke kiezer moet kunnen stemmen voor de kandidaat naar zijn keuze.
- **Unanimititeit:** een kandidaat wint sowieso als hij alle stemmen krijgt.
- **Geen dictatuur:** het verkiezingsresultaat mag niet bepaald worden door de stem van één kiezer.
- **Onafhankelijkheid van irrelevante alternatieven:** als één mogelijke kandidaat uit de opties verwijderd wordt, mag de ranking van de anderen niet veranderen.
- **Pareto-efficiëntie\*:** als iedere kiezer een bepaalde kandidaat  $A$  verkiest boven een andere,  $B$ , dan moet  $A$  ook in de uiteindelijke ranking boven  $B$  eindigen.

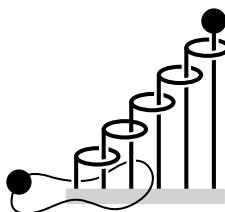
Arrow bewees echter (op wiskundige wijze) dat het onmogelijk is zo'n kiesstelsel te definiëren! Gelijk welk systeem er ook aangewend wordt, deze zal altijd minstens een van deze criteria schenden wanneer er minstens drie keuzeopties en minstens twee kiezers zijn. De Bordatelling bijvoorbeeld voldoet niet aan de onafhankelijkheid van irrelevante alternatieven.

\*Pareto-efficiëntie is een begrip afkomstig uit de economie en houdt in dat niemand zijn/haar positie kan verbeteren zonder dat dit ten koste gaat van anderen.

## 316 Baguenaudier

Naar verluid werd deze puzzel bedacht door de Chinese generaal Hung Ming, rond het jaar 200, als verpozing voor zijn vrouw terwijl hij weg was op oorlogspad. De benaming *baguenaudier* echter is Frans; de puzzel zou door Franse boeren gebruikt geweest zijn om koffers af te sluiten. Letterlijk betekent baguenaudier zoveel als “tijdverprutser”. In Italië staat de puzzel dan weer bekend als *Anelli di Cardano*, Cardano’s ringen.

De baguenaudier bestaat uit een aantal ringen, trapvormig in elkaar gezet, met rond de eerste pijler een koord in een lus; zie het diagram hieronder. Het doel van de puzzel ligt voor de hand: de lus scheiden van de ringen.



Édouard Lucas, bekend als uitvinder van de torens van Hanoi (zie ??, blz. ??), gaf een elegante oplossing gebruik makende van binaire getallen en Graycodes (zie ??, blz. ??). Voor de puzzel met  $n$  ringen is het minimale aantal stappen  $S(n)$  vereist voor de oplossing, eenvoudig uit te drukken:

$$S(n) = \left\lceil \frac{2}{3} \cdot 2^n - 1 \right\rceil$$

Recursief worden ze gegeven door:

$$S(1) = 1, \quad S(2) = 2, \quad S(n) = S(n-1) + 2S(n-2) + 1$$

0, 1, 2, 5, 10, 21, 42, 85, 170, 341, 682, 1365, 2730, 5461, 10922, 21845, 43690, 87381 . . . (OEIS A000975)

## 317 Conways pijlenketen

Een handige manier op om te springen met extreem grote getallen, nog veel groter dan Knuths pijlomhoognotatie (zie 305, blz. 298) zou aankunnen, zijn de pijlenkettingen van John Conway. Deze bestaan uit een eindige rij natuurlijke getallen, gescheiden door een “ $\rightarrow$ ”. Zo’n keten wordt als volgt recursief gedefinieerd; schrijf  $p$  en  $q$  voor natuurlijke getallen en  $S$  voor een subketen.

- De keten  $p$  stelt gewoon het getal  $p$  voor.
- De keten  $p \rightarrow q$  representeert  $p^q$ .
- $S \rightarrow p \rightarrow 1$  is equivalent met  $S \rightarrow p$ .
- $S \rightarrow 1 \rightarrow p$  is equivalent met  $S$ .
- $S \rightarrow (p+1) \rightarrow (q+1)$  kan worden herleid naar  $S \rightarrow (S \rightarrow p \rightarrow (q+1)) \rightarrow q$

Merk op dat pijlenketens altijd als een geheel moeten beschouwd worden! Deze beschrijven geen herhaalde-toepassing van een binaire operator en kunnen niet in fragmenten berekend worden. De ketens zijn niet associatief. Zo geldt dat  $2 \rightarrow 3 \rightarrow 2 = 16$ , maar  $2 \rightarrow (3 \rightarrow 2) = 512$  en  $(2 \rightarrow 3) \rightarrow 2 = 64$ .

Deze definitie geeft al gauw onhandelbaar grote getallen. Een keten van lengte drie,  $p \rightarrow q \rightarrow r$ , correspondeert met de pijlomhoognotatie van Knuth,  $p \uparrow^r q$ . Voor langere ketens wordt ook Knuths notatie al gauw onbruikbaar. Het gigantische getal van Graham (zie 245, blz. 203) ligt tussen  $3 \rightarrow 3 \rightarrow 64 \rightarrow 2$  en  $3 \rightarrow 3 \rightarrow 65 \rightarrow 2$ . Een exacte representatie ervan is mogelijk via  $f(n) = 3 \rightarrow 3 \rightarrow n$ ; dan geldt dat Grahams getal gelijk is aan  $f^{64}(4)$ . En het kan nog veel groter:  $3 \rightarrow 3 \rightarrow 3 \rightarrow 3$  is alweer onvoorstelbaar veel groter dan het getal van Graham. . .

### 318 Axioma's van Huzita-Justin

Origami is een alternatieve manier om aan meetkunde te doen. In 1989 presenteerden Humiaki Huzita en Benedetto Scimemi op de eerste *International Meeting of Origami Science and Technology* zes onafhankelijke methoden om vouwen te maken, uitgaande van bepaalde configuraties punten en lijnen, die zouden bekend geraken als de axioma's van Huzita. In 2001 echter ontdekte Koshiro Hatori een zevende axioma, en onderzoek van origami-expert Robert Lang wees uit dat er geen origami-axioma's meer mogelijk zijn.

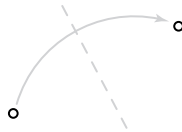
Hatori was niet de eerste die het laatste axioma vond: Jacques Justin publiceerde in 1989, vóór de eerste *IMOST*, een paper *Résolution par le pliage de l'équation du troisième degré et applications géométriques* waarin hij zeven mogelijke combinaties van uitlijningen beschreef. Deze komen overeen met de zes axioma's van Huzita en het zevende van Hatori. Daarom wordt het stelsel vandaag meestal aangeduid als de axioma's van Huzita-Justin.

Dit zijn de zes originele axioma's van Huzita.

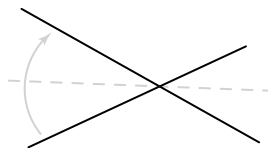
- Gegeven twee punten  $P_1$  en  $P_2$ , dan kan er een vouw gemaakt worden die  $P_1$  met  $P_2$  verbindt.



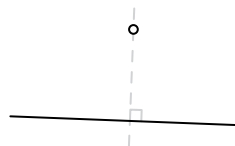
- Gegeven twee punten  $P_1$  en  $P_2$ , dan kan  $P_1$  op  $P_2$  gevouwen worden.



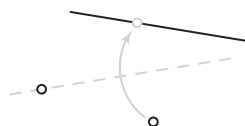
- Gegeven twee lijnen  $\ell_1$  en  $\ell_2$ , dan kan  $\ell_1$  op  $\ell_2$  gevouwen worden.



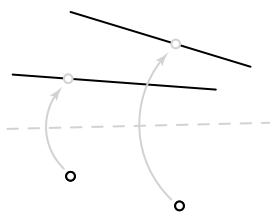
- Gegeven een punt  $P$  en een lijn  $\ell$ , dan kan er een vouw gemaakt worden die door  $P$  gaat en loodrecht staat op  $\ell$ .



- Gegeven twee punten  $P_1$  en  $P_2$  en een lijn  $\ell$ , dan kan er een vouw gemaakt worden die door  $P_1$  gaat en  $P_2$  op  $\ell$  plaatst.

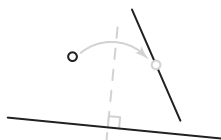


- Gegeven twee punten  $P_1$  en  $P_2$  en twee lijnen  $\ell_1$  en  $\ell_2$ , dan kan er een vouw gemaakt worden die  $P_1$  op  $\ell_1$  plaatst en  $P_2$  op  $\ell_2$ .



Deze configuratie is onafhankelijk van de zes vorige en vormt het zevende axioma van Hatori.

- Gegeven een punt  $P$  en twee lijnen  $\ell_1$  en  $\ell_2$ , dan kan een vouw gemaakt worden die loodrecht staat op  $\ell_2$  en  $P$  op  $\ell_1$  plaatst.

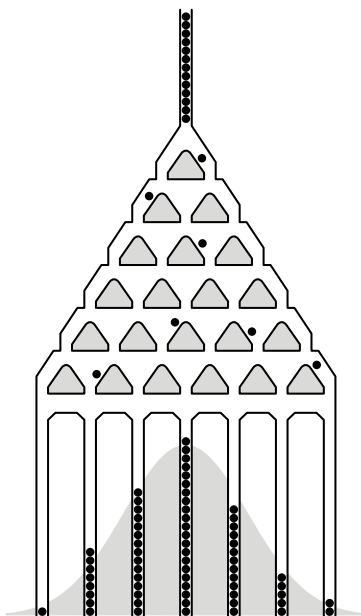


Met deze origamimeetkunde zijn verrassende dingen mogelijk. In tegenstelling tot passer-en-liniaal-meetkunde zijn de trisectie van een hoek en de verdubbeling van een kubus wél realiseerbaar via origami. Ook nulpunten van veeltermen tot en met de vierde graad met rationale coëfficiënten kunnen worden gevouwen, net als een regelmatige  $N$ -hoek waarbij  $N = 2^a \cdot 3^b \cdot (2^c \cdot 3^d + 1)$  zolang  $2^c \cdot 3^d + 1$  priem is\*.

Met origami kunnen ook volwaardige wiskundige stellingen geponeerd worden; zie bijvoorbeeld 313, blz. 302.

## 319 Bord van Galton

Het bord van Galton (ook bekend als de quincunx of de *bean machine*) is een ontwerp van Francis Galton en is een ideale illustratie voor de centrale limietstelling. In het bijzonder toont het experiment aan dat de binomiaalverdeling een normaalverdeling benadert. Het bord bestaat uit een aantal spijkers in een driehoek gerangschikt, waarop balletjes gedropt worden. Elke keer als een balletje op een spijker stuit, kan hij links of rechts vallen naar het niveau eronder. Uiteindelijk worden de balletjes verzameld in gleuven onderaan.



\*Een priemgetal van deze vorm,  $2^c \cdot 3^d + 1$ , wordt een Pierpontpriemgetal genoemd.

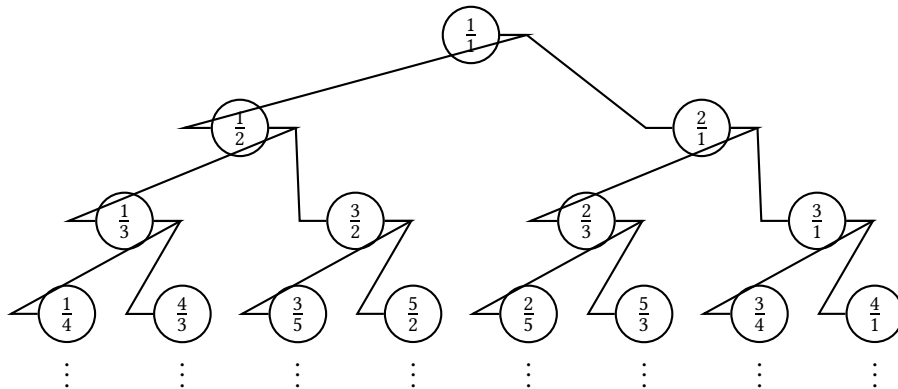
Noem  $n$  het aantal niveaus in het bord van Galton. Het aantal paden dat landt in de  $k^{\text{de}}$  sleuf wordt dan gegeven door de binomiaalcoëfficiënt  $\binom{n}{k}$  (zie ook Pascals driehoek: 246, blz. 204). Noem dan  $p$  de kans dat een balletje op een spijker naar links valt (normaliter  $\frac{1}{2}$ , zonder bias), dan is de kans dat een balletje in de  $k^{\text{de}}$  gleuf terecht komt:

$$P(\text{bereikte gleuf} = k^{\text{de}} \text{ gleuf}) = \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k}$$

Dit is juist de kansfunctie van de binomiaalverdeling. Volgens de centrale limietstelling benadert deze een normaalverdeling, nauwkeuriger naarmate er meerdere balletjes en meerdere niveaus in het bord zijn, wat duidelijk experimenteel te zien is aan de hoogte van de balletjes in de gleuven.

### 320 Boom van Calkin-Wilf

In 2000 introduceerden Neil Calkin en Herbert Wilf deze boomstructuur, waarin elk positief rationaal getal éénmalig voorkomt, direct herleid naar zijn eenvoudigste vorm. De boom is geworteld in het getal 1. Elk knooppunt, met breuk  $\frac{a}{b}$ , vertakt zich naar  $\frac{a}{a+b}$  en  $\frac{a+b}{b}$ .



Vanuit deze boom kan de rij van Calkin-Wilf worden opgesteld. Lees de afzonderlijke rijen na elkaar:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{2}, \frac{2}{3}, \frac{3}{1}, \frac{1}{4}, \frac{4}{3}, \frac{3}{5}, \frac{5}{2}, \frac{2}{5}, \frac{5}{3}, \frac{3}{4}, \frac{4}{1}, \frac{1}{5}, \frac{5}{4}, \frac{4}{7}, \frac{7}{3}, \frac{3}{8}, \frac{8}{5}, \frac{5}{7}, \frac{7}{2}, \frac{2}{7}, \frac{7}{5}, \frac{5}{8}, \frac{8}{3}, \frac{3}{7}, \frac{7}{4}, \frac{4}{5}, \frac{5}{1}, \frac{1}{6}, \frac{6}{5}, \frac{5}{9}, \frac{9}{4}, \frac{4}{11}, \frac{11}{7}, \dots$$

Natuurlijk bevat dan ook deze rij alle positieve rationale getallen, juist één keer, naar hun eenvoudigste vorm herleid. Er bestaat ook een recursief voorschrift dat dezelfde rij genereert:

$$u_0 = 1, \quad u_{n+1} = \frac{1}{2[u_n] - u_n + 1}$$

Er geldt ook een rechtstreeks verband met de fusc-functie (zie 77, blz. 58):

$$u_n = \frac{\text{fusc}(n)}{\text{fusc}(n+1)}$$

### 321 RSA

Het RSA-algoritme wordt vandaag veelvuldig gebruikt om bijvoorbeeld online transacties te beveiligen. In 1977 werd het systeem ontwikkeld door Ron Rivest, Adi Shamir en Leonard Adleman aan de Massachusetts Institute of Technology. Het algoritme wordt naar hun initialen vernoemd, ook al ontwikkelde Clifford Cocks vier jaar eerder aan de Britse inlichtingendienst Government Communications Headquarters (GCHQ) dezelfde encryptiemethode, dat tot 1997 als topgeheim geclassificeerd werd en daardoor onopgemerkt bleef.

Het fundamentele idee achter RSA is dat er geen efficiënte methode bekend is om grote getallen te factoriseren

in priemfactoren. Wanneer een getal  $n = p \cdot q$  gegeven wordt, is het met huidig bekende technieken ondoenlijk om  $p$  of  $q$  te achterhalen uit  $n$  binnen redelijke tijd wanneer  $p$  en  $q$  gigantisch grote priemgetallen zijn.

De benodigdheden voor het RSA-algoritme zijn de volgende getallen:

- Twee grote priemgetallen  $p$  en  $q$
- Hun product  $n = p \cdot q$
- De totiënt  $\varphi(n)$ , gelijk aan  $(p - 1) \cdot (q - 1)$  (zie 12, blz. 10)
- Een geheel getal  $e$  waarvoor  $1 < e < \varphi(n)$  en onderling ondeelbaar met  $\varphi(n)$
- De multiplicatieve inverse  $d$  van  $e$  modulo  $\varphi(n)$

De publieke sleutel bestaat dan uit de modulus  $n$  en de encryptie-exponent  $e$  en mag algemeen bekend gemaakt worden. De private sleutel dient echter geheim gehouden te worden en bestaat uit de modulus  $n$  en de decryptie-exponent  $d$ . De overige getallen hebben geen verder nut meer, maar mogen niet worden publiek gemaakt omdat de waarde van  $d$  eenvoudig uit deze getallen te berekenen is.

Om een boodschap te versleutelen, moet die eerst worden omgezet in een getal  $m$  kleiner dan  $n$ , via een afgesproken *padding scheme*. Dit kan bijvoorbeeld door  $a$  te versleutelen als 01,  $b$  als 02 etc. Mocht  $m$  groter zijn dan  $n$ , dan moet de boodschap in meerdere stukken worden opgesplitst. Daarna wordt  $m$  versleuteld met behulp van de publieke sleutel  $(n, e)$  van de ontvanger:

$$c = m^e \pmod{n}$$

Er zijn efficiënte methodes gekend om zo'n modulaire machtsverheffing uit te voeren, dus deze stap neemt weinig tijd in beslag. De ontvanger vindt de originele boodschap  $m$  uit de versleutelde  $c$  dan terug via zijn geheime  $d$ :

$$m = c^d \pmod{n}$$

Zolang een potentiële hacker de waarde van  $d$  niet kent (wat om een boodschap te versleutelen niet nodig is), is het zeer tijdrovend om een eenmaal versleutelde boodschap te decoderen. Beschouw als voorbeeld de waarden  $p = 62.987$  en  $q = 35.401$ . Dan is  $n = 2.229.802.787$  en  $\varphi(n) = 2.229.704.400$ . Kiezen we dan  $e = 17$ , dan is  $d = 1.836.227.153$ . Een boodschap  $m = 1234$  wordt dan versleuteld tot  $c = m^e \pmod{n} = 890.560.568$ . Willen we nu  $m$  terugvinden uit  $c$ , berekenen we  $m = c^d \pmod{n} = 1234$ . In praktische toepassingen worden de priemgetallen natuurlijk veel groter gekozen.

Weliswaar zijn enkele beveiligingslekken mogelijk voor specifieke gevallen, zoals bijvoorbeeld wanneer  $p$  en  $q$  te dicht bij elkaar liggen,  $p - 1$  of  $q - 1$  voornamelijk kleine priemfactoren heeft, of  $d$  te klein is.

Martin Gardner beschreef het RSA-systeem in zijn column *Mathematical Games* in augustus 1977. Daarbij presenteerde hij een boodschap gecodeerd door de ontwerpers van RSA, met de uitdaging die te kraken.

$$\begin{aligned} n &= 114.381.625.757.888.867.669.235.779.976.146.612.010.218.296.721.242.362.562.561.842.935. \\ &\quad 706.935.245.733.897.830.597.123.563.958.705.058.989.075.147.599.290.026.879.543.541 \\ e &= 9007 \\ c &= 96.869.613.754.622.061.477.140.922.254.355.882.905.759.991.124.674.319.874.695.120.930. \\ &\quad 816.298.225.145.708.356.931.476.622.883.989.628.013.391.990.551.829.945.157.815.154 \end{aligned}$$

Pas in 1994 vonden Derek Atkins, Michael Graff, Arjen Lenstra en Paul Leyland via een gemeenschappelijk computerproject, waarin 600 vrijwilligers rekenkracht van 1600 computers bundelden, na zes maanden de oorspronkelijke woorden:

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

## 322 P vs. NP

Dit onderwerp staat bekend als een van de belangrijkste open kwesties van dit ogenblik, waarvan de oplossing de toekomstige loop van wiskunde en informatica drastisch zou kunnen bepalen. P vs. NP behoort tot de zeven Millenniumproblemen, waarvoor een prijs van een miljoen dollar wordt uitgereikt aan diegene die er een kan oplossen. Nogal filosofisch gesteld, komt het neer op de vraag: kan intelligentie geluk vervangen?

Algoritmes worden onderverdeeld in enkele complexiteitsklassen. Programma's met invoer van grootteorde  $n$  worden normaliter uitgevoerd in een tijdsduur afhankelijk van  $n$ , zoals  $n^2$ ,  $n \log n$ ,  $2^n$ ,  $\sqrt{n}$ ,  $n! \dots$

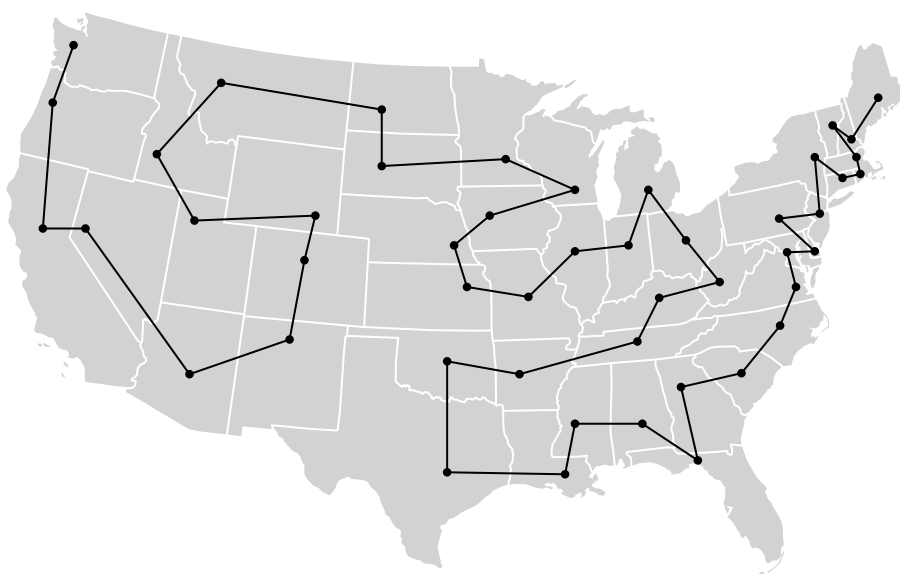
Een algoritme dat nagaat of een gegeven lijst een welbepaald getal bevat, heeft in een worstcasescenario dubbel zo veel tijd nodig voor een dubbel zo lange lijst. Dit programma verloopt lineair met de lengte  $n$  van de lijst, wat men noteert als  $\mathcal{O}(n)$ . Voor een algoritme echter dat controleert of twee getallen uit de lijst copriem zijn, zal het tijdsverloop niet langer lineair zijn t.o.v. de lengte van de lijst maar kwadratisch,  $\mathcal{O}(n^2)$ .

Algemeen worden algoritmes uit te voeren in polynomiale tijd,  $\mathcal{O}(n^p)$  voor een zekere constante  $p$ , opgenomen in de complexiteitsklasse P. Grofweg gesproken zijn deze problemen "eenvoudig": hun benodigde looptijd blijft handelbaar als hun invoer groter wordt.

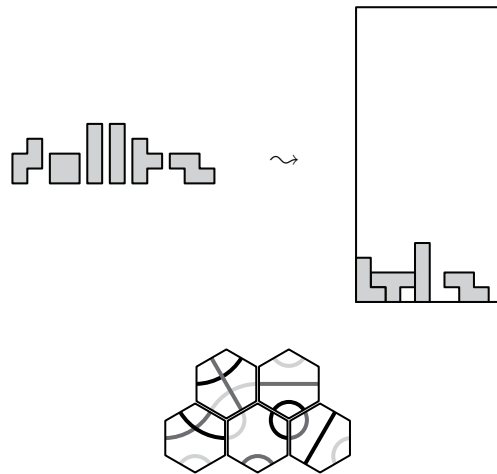
Er bestaan ook lastigere problemen, zoals nagaan of een gegeven lijst een deelverzameling gehele getallen bevat die sommeren tot nul. Tot nog toe bekend zit er niks anders op dan domweg alle mogelijke deelverzamelingen te verifiëren, maar dit verloopt bijlange niet in polynomiale tijd maar in  $\mathcal{O}(2^n)$ , zodat bij langere lijsten de benodigde rekestijd exponentieel toeneemt en het probleem al gauw onhandelbaar wordt. Tenzij we geluk hebben! Een oplossing *verifiëren* is namelijk zeer eenvoudig en lukt wel in polynomiale tijd, i.t.t. een oplossing *vinden*.

Algemeen worden algoritmes die een oplossing kunnen verifiëren in polynomiale tijd, opgenomen in de complexiteitsklasse NP, wat staat voor "niet-deterministisch polynomiaal". Grofweg gesproken betekent dit dat het algoritme mag gokken naar een oplossing en dan snel kan controleren of het al dan niet klopt.

Het is duidelijk dat  $P \subseteq NP$  en lijkt aannemelijk dat  $NP \not\subseteq P$ .







### 323 Fractran

John Conway beschreef deze bizarre programmeertaal FRACTRAN. Zijn elegante systeem is Turing-compleet (zie ??, blz. ??), wat inhoudt dat elke mogelijke programmeerbare berekening of gegevensbewerking in theorie ook in FRACTRAN geprogrammeerd kan worden (zij het nogal omslachtig). Een programma in FRACTRAN bestaat uit een lijst positieve breuken  $f_i$ , met een initiële, gehele input  $n$ .

$$n \mapsto (f_1, f_2 \dots f_k) \mapsto ?$$

Een FRACTRAN-programma wordt uitgevoerd als volgt. Vervang  $n$  door  $n \cdot f$ , waarin  $f$  de eerste breuk in de lijst is zodat  $n \cdot f$  opnieuw geheel is, en herhaal deze stap totdat geen enkele breuk nog een geheel getal oplevert. Een eerste, eenvoudig voorbeeld, dat de optelling implementeert: de invoerwaarde  $n = 2^a 3^b$  in dit programma geeft na  $b$  stappen het geheel getal  $2^{a+b}$  terug.

$$2^a 3^b \mapsto \left(\frac{2}{3}\right) \mapsto 2^{a+b}$$

De volgende programma's produceren  $\min(a, b)$  en  $\max(a, b)$  vanuit dezelfde input.

$$2^a 3^b \mapsto \left(\frac{5}{6}, \frac{1}{2}, \frac{1}{3}\right) \mapsto 5^{\min(a,b)}$$

$$2^a 3^b \mapsto \left(\frac{5}{6}, \frac{5}{2}, \frac{5}{3}\right) \mapsto 5^{\max(a,b)}$$

Vermenigvuldiging wordt al ingewikkelder:

$$2^a 3^b \mapsto \left(\frac{455}{33}, \frac{11}{13}, \frac{1}{11}, \frac{3}{7}, \frac{11}{2}, \frac{1}{3}\right) \mapsto 5^{ab}$$

Het volgende programma geeft  $H(a)$ , het aantal 1'en in de binaire schrijfwijze van  $a$ , als uitvoer.

$$2^a \mapsto \left(\frac{33}{20}, \frac{5}{11}, \frac{13}{10}, \frac{1}{5}, \frac{2}{3}, \frac{10}{7}, \frac{7}{2}\right) \mapsto 13^{H(a)}$$

Conway gaf zelf een verbazingwekkende toepassing van FRACTRAN, genaamd PRIMEGAME: vertrekkende bij 2 genereert het programma een oneindige lijst gehele getallen, waarbij de enige geproduceerde machten van 2 juist een priemgetal als exponent hebben! Zo genereert PRIMEGAME alle priemgetallen, elk juist éénmaal en in opklimmende volgorde.

$$2 \mapsto \left(\frac{17}{91}, \frac{78}{85}, \frac{19}{51}, \frac{23}{38}, \frac{29}{33}, \frac{77}{29}, \frac{95}{23}, \frac{77}{19}, \frac{1}{17}, \frac{11}{13}, \frac{13}{11}, \frac{15}{2}, \frac{1}{7}, \frac{55}{1}\right) \mapsto \dots, 2^2, \dots, 2^3, \dots, 2^5, \dots$$

Misschien nog spectaculairder is PiGAME: een programma met invoerwaarde  $2^n$ , dat  $2^{\pi(n)}$  produceert als eerstvolgende macht van 2, waarbij  $\pi(n)$  de  $n^{\text{de}}$  decimaal na de komma is van het getal  $\pi$ !

$$2^n \mapsto \left( \begin{array}{cccccccccccc} \frac{365}{46}, \frac{29}{161}, \frac{79}{575}, \frac{679}{451}, \frac{3159}{413}, \frac{83}{407}, \frac{473}{371}, \frac{638}{355}, \frac{434}{335}, \frac{89}{235}, \frac{17}{209}, \frac{79}{122}, \\ \frac{31}{183}, \frac{41}{115}, \frac{517}{89}, \frac{111}{83}, \frac{305}{79}, \frac{23}{73}, \frac{73}{71}, \frac{61}{67}, \frac{37}{61}, \frac{19}{59}, \frac{89}{57}, \frac{41}{53}, \frac{833}{47}, \frac{53}{43}, \\ \frac{86}{41}, \frac{13}{38}, \frac{23}{37}, \frac{67}{31}, \frac{71}{29}, \frac{83}{19}, \frac{475}{17}, \frac{59}{13}, \frac{41}{291}, \frac{1}{7}, \frac{1}{11}, \frac{1}{1024}, \frac{1}{97}, \frac{89}{1} \end{array} \right) \mapsto \dots 2^{\pi(n)} \dots$$

## 324 Paradox van Sierpiński-Mazurkiewicz

De paradox van Banach-Tarski (zie ??, blz. ??) stelt dat een bol kan worden verdeeld in vijf stukken die opnieuw in elkaar kunnen worden gezet tot twee identieke bollen, maar steunt op het controversiële keuzeaxioma. Het is echter ook mogelijk om paradoxale decomposities te bekomen zonder het keuzeaxioma te betrekken, zoals Waclaw Sierpiński en Stefan Mazurkiewicz zich realiseerden. Zij definieerden een deelverzameling  $S$  van het vlak en een partitie ervan in  $A$  en  $B$ , zodanig dat wanneer  $A$  over één radiaal groteerd wordt, of  $B$  over één eenheid getransleerd, het resultaat geheel  $S$  is. De verzameling  $S$  is te bewerken tot twee kopieën van zichzelf!

Beschouw het complexe, transcendente getal  $e^i$ , dat geen wortel is van een veelterm met gehele coëfficiënten. Laat  $S$  nu de verzameling zijn van alle veeltermen in  $x$  met positieve gehele coëfficiënten, geëvalueerd in  $x = e^i$ . Dan stelt  $S$  een verzameling punten in het complexe vlak voor, en door de transcendente aard van  $e^i$  komt elke veelterm juist met één punt in het vlak overeen.

Noem nu  $A$  de deelverzameling van  $S$  van alle veeltermen met constante term gelijk aan nul, en  $B$  die van alle veeltermen met constante term verschillend van nul.  $A$  en  $B$  vormen dan duidelijk een partitie van  $S$ .

Roteer daarna alle punten uit  $A$  over één radiaal met de klok mee. Dit komt overeen met vermenigvuldigen van de veeltermen uit  $A$  met  $e^{-i}$ , zijnde  $x^{-1}$ , oftewel delen door  $x$ . De veeltermen met constante term nul worden zo afgebeeld op alle mogelijke veeltermen, zijnde volledig  $S$ !

Hetzelfde geldt voor  $B$  door een verschuiving naar links over één eenheid. Deze translatie komt namelijk overeen met 1 aftrekken van elke veelterm uit  $B$ , zodat deze veeltermen (met positieve, constante term verschillend van nul) worden afgebeeld op alle veeltermen uit  $S$ .

## 325 Surreële getallen

Surreële getallen vormen een uitbreiding van de reële getallen, maar zijn ook in staat allerlei infinitesimalen uit te drukken. John Conway legde het systeem bloot tijdens onderzoek naar wiskundige spellen (i.h.b. Hackenbush; zie ??, blz. ??), maar de benaming “surreële getallen” werd ingeblikt door Donald Knuth, die ze introduceerde in een fictienovelle genaamd *Surreal Numbers: how two ex-students turned on to pure mathematics and found total happiness*.

Surreële getallen worden vrij eigenaardig gedefinieerd als een tweetal verzamelingen van surreële getallen. Deze twee verzamelingen worden de linker- en rechterverzameling  $L$  en  $R$  genoemd en het nieuwe getal wordt genoteerd als  $\{L|R\}$ . Als bijkomende eis in deze recursieve definitie mag geen enkel element uit  $R$  kleiner dan of gelijk aan een element uit  $L$  zijn.

Maar ook “kleiner dan of gelijk aan” wordt bij surreële getallen recursief herinterpreteerd: een getal  $x$  is kleiner

dan of gelijk aan een getal  $y$  als en slechts als  $y$  kleiner dan of gelijk aan geen enkel element van de linkerverzameling van  $x$  is, en geen enkel element van de rechterverzameling van  $y$  kleiner dan of gelijk aan  $x$  is. Uit deze relatie  $\leq$  worden de andere relaties  $\not\leq$ ,  $\geq$ ,  $\not\geq$ ,  $=$  en  $\neq$  gebaseerd zoals gewoonlijk.

Op dit moment kennen we nog geen surreële getallen, dus zijn we genoodzaakt er één te construeren waarvoor  $L$  en  $R$  de ledige verzameling zijn. Deze  $\{\phi|\phi\}$  voldoet triviaal aan de extra eis in de definitie, en we noemen dit getal  $0$ . Met dit eerste surreële getal kunnen we nieuwe getallen construeren, zoals  $\{\{0\}|\phi\}$ . Om de notatie licht te houden, worden  $\phi$ 's en extra accolades weggelaten, dus schrijven we simpelweg  $\{0|\}$ . Er blijkt dat dit nieuwe getal goed gedefinieerd is, en daarenboven  $\{0|\} \leq \{|\}$ , terwijl  $\{|\} \not\leq \{0|\}$ . We hebben dus wel degelijk een verschillend getal gevonden, dat we noteren als  $-1$ . Analoog vinden we  $\{0|\}$  oftewel  $1$ . Het getal  $\{0|0\}$  schendt echter de voorwaarde in de definitie en is dus geen deugdelijk surreëel getal, maar wordt een pseudogetal genoemd. Aldus wordt het systeem steeds verder uitgebreid met nieuwe surreële getallen, hoewel niet elke nieuwe samenstelling een nieuwe waarde geeft. Er geldt bijvoorbeeld dat  $\{-2, -1|\} = \{-1|\} = 0 = \{|\}$ : om een waarde te bepalen, volstaat het om het grootste element in  $L$  en het kleinste in  $R$  te kennen.

Het is duidelijk dat surreële getallen in generaties geconstrueerd worden:  $S_0$  bevat enkel  $0$ , en de volgende generaties  $S_n$  (met  $n$  eender welk ordinaalgetal; zie 295, blz. 274) alle surreële getallen gegenereerd via de constructieregel uit eerdere generaties.

- $S_0 = \{0\}$
- $S_1 = \{-1 < 0 < 1\}$
- $S_2 = \{-2 < 1 < -\frac{1}{2} < 0 < \frac{1}{2} < 1 < 2\}$
- $S_3 = \{-3 < -2 < -\frac{3}{2} < -1 < -\frac{3}{4} < -\frac{1}{2} < -\frac{1}{4} < 0 < \frac{1}{4} < \frac{1}{2} < \frac{3}{4} < 1 < \frac{3}{2} < 2 < 3\}$
- $S_4 = \{-4 < \dots < -\frac{1}{8} < 0 < \frac{1}{8} < \frac{1}{4} < \frac{3}{8} < \frac{1}{2} < \frac{5}{8} < \frac{3}{4} < \frac{7}{8} < 1 < \frac{5}{4} < \frac{3}{2} < \frac{7}{4} < 2 < \frac{5}{2} < 3 < 4\}$
- ...

Uiteraard willen we ook kunnen rekenen in dit systeem. Het tegengestelde van een surreële  $x = \{L_x|R_x\}$  ziet er als volgt uit:

$$-x = -\{L_x|R_x\} = \{-R_x|-L_x\}$$

Men kan nagaan dat de volgende optelling, alweer recursief, overeenkomt met vertrouwde optelling.

$$x + y = \{L_x|R_x\} + \{L_y|R_y\} = \{L_x + y, L_y + x|R_x + y, R_y + x\}$$

Vermenigvuldiging is lastiger:

$$x \cdot y = \{L_x \cdot y + L_y \cdot x - L_x \cdot L_y, R_x \cdot y + R_y \cdot x - R_x \cdot R_y | L_x \cdot y + R_y \cdot x - L_x \cdot R_y, L_y \cdot x + R_x \cdot y - R_x \cdot L_y\}$$

In bovenstaande definities dienen de bewerkingen toegepast op een verzameling beschouwd te worden als de verzameling met de bewerkingen toegepast op alle elementen ervan. Al deze definities leveren een goed gedefinieerd, consistent stelsel met een veldstructuur op.

De unie van alle klassen  $S_n$  met eindige  $n$  wordt genoteerd als  $S_*$ . Merk op dat  $S_*$  enkel dyadische rationale getallen bevat, d.w.z. breuken met een macht van twee als noemer; andere rationale getallen en irrationale getallen treden pas op in  $S_\omega$  na transfinitie inductie. Bijvoorbeeld  $\frac{1}{3}$ :

$$\frac{1}{3} = \{\alpha \in S_* : 3\alpha < 1 | \beta \in S_* : 3\beta > 1\}$$

In  $S_\omega$  zitten echter nog andere, niet-reële getallen verdoken. Het grootste getal ervan,  $\omega$ , is uniek bepaald en groter dan eender welk ander reëel getal:

$$\omega = \{1, 2, 3, 4, \dots\}$$

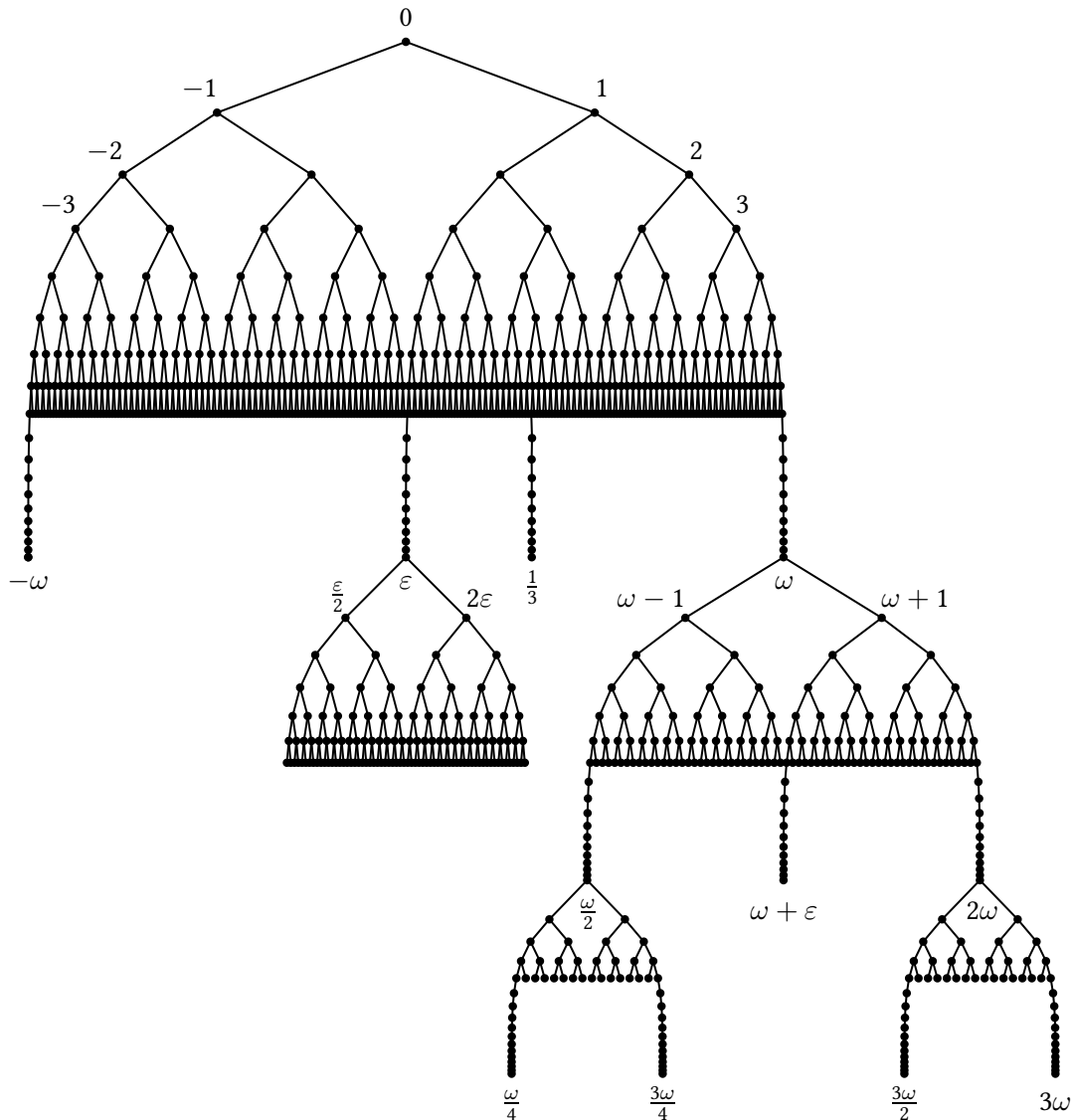
Naast  $\omega$  en  $-\omega$  vind je ook infinitesimale niet-reële getallen  $\varepsilon$  en  $-\varepsilon$ :

$$\varepsilon = \left\{ 0 \mid 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8} \dots \right\}$$

De transfinitie inductie verderzetten na  $S_\omega$  produceert nog meer surreële getallen, zoals  $\omega - 1$ :

$$\omega - 1 = \{ 1, 2, 3, 4 \dots \mid \omega \}$$

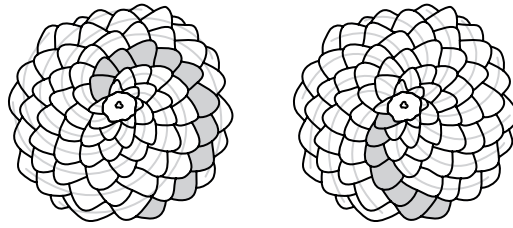
Merk op dat  $\omega - 1$  in feite geen ordinaalgetal is, zodat surreële getallen wel degelijk “rijker” zijn. Je kan natuurlijk nog veel exotischere surreële getallen construeren, zoals  $\sqrt{\omega + \pi \cdot \varepsilon^\varepsilon} + \omega^{2+\varepsilon} - 1$  of ingewikkelder.



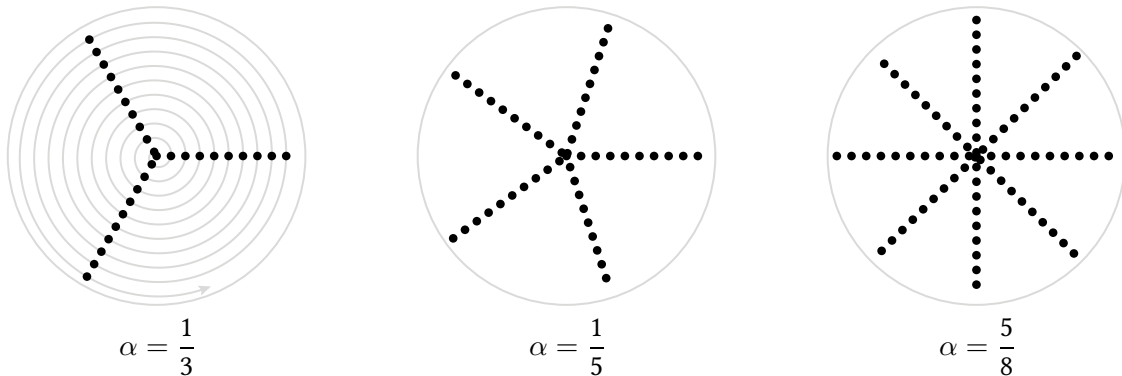
## 326 Gulden snede in fyllotaxis

Het is een hardnekkige mythe dat Fibonaccigetallen (zie 91, blz. 65) en verhoudingen volgens de gulden snede overall in de natuur voorkomen. Bekende (maar onterechte en op toeval berustende) voorbeelden zijn verhoudingen in vingerkootjes of de positie van de navel in het menselijk lichaam. Er zijn echter wel degelijk verklaarbare patronen te vinden, zoals in de fyllotaxis (de rangschikking van bladeren langs een stengel).

In artisjokken, zonnebloemen, ananassen, romanesco's, aloëplanten en talloze andere bloemen blijkt het aantal bladeren of spiralen in de zaden juist een Fibonaccigetel te zijn. Hieronder wordt een denappel van onderaf bekeken: men telt juist acht spiralen met de klok mee, of dertien tegen de klok in. Tel maar na op echte denappels!

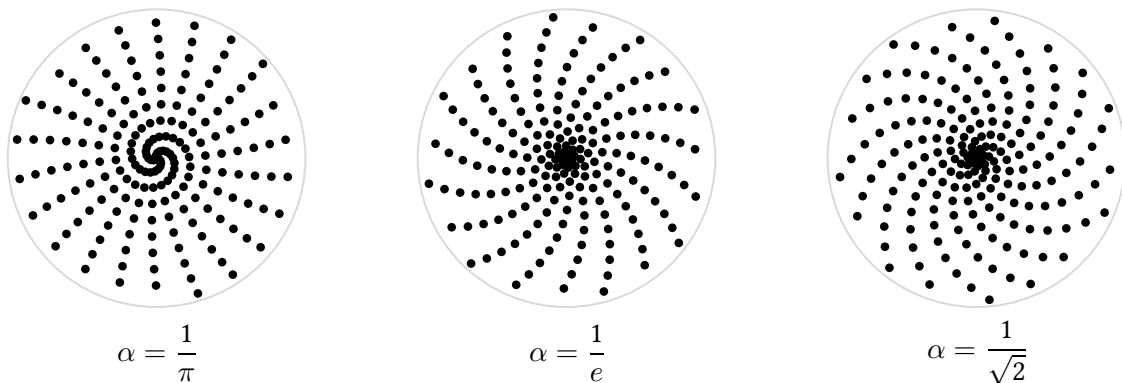


Een wiskundig model kan dit fenomeen verklaren. We definiëren een “bloem” vertrekkende vanuit een centraal draaiende, groeiende punt, die na elke  $\alpha$  draaiingen ( $\alpha$  zijnde een vaste reële parameter) een nieuw blaadje of zaadje achterlaat en steeds verder naar buiten groeit. Wanneer we voor  $\alpha$  een eenvoudig rationaal getal kiezen, zoals hieronder, verkrijgen we deze patronen:



Dit levert een aantal radiale spaken op, net zoveel als de noemer in de onvereenvoudigbare vorm van  $\alpha$ . Vanuit het standpunt van de bloem is dit bijzonder oninteressant, omdat de bladeren dan allemaal op elkaar zitten en er veel ruimte verspild wordt. Een plant wil juist zodanig groeien dat zijn blootstelling aan zonlicht, dauw of koolstofdioxide gemaximaliseerd wordt.

Het wordt interessanter wanneer we voor  $\alpha$  een irrationale parameter kiezen:

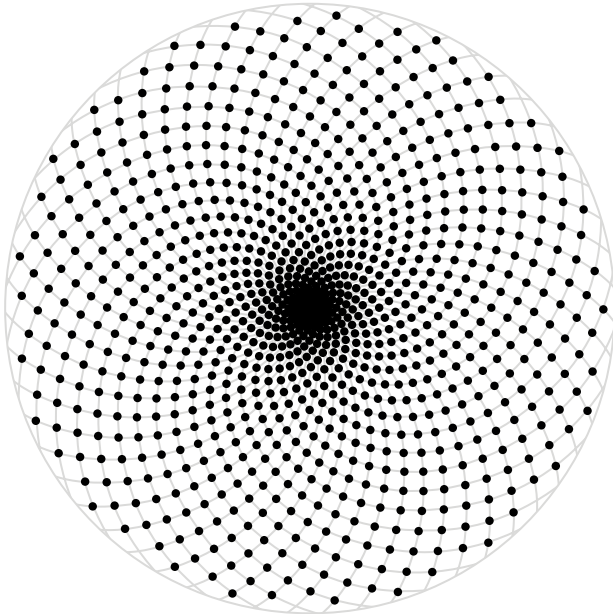


De patronen voor  $\alpha = \frac{1}{\pi}$  of  $\alpha = \frac{1}{e}$  stagneren na een tijdje in spiralen die wat gelijkjes op de patronen van daarnet. Deze corresponderen precies met de best benaderende rationale getallen voor  $\alpha$ . Centraal in de linkerbloem zijn er duidelijk drie spiraalarmen te zien, wat overeenkomt met de benadering  $\pi \approx 3$ . Daarna breekt deze benadering uiteen tot 22 spiraalarmen, die telkens per 7 verspringen:  $\pi \approx \frac{22}{7}$ . Men kan aantonen dat de “best benaderende breuken” of convergenten van een irrationaal getal juist de rationale getallen zijn verkregen door diens kettingbreuk (zie 22, blz. 14) af te kappen na een eindig aantal termen.

Een bloem die zijn zaden of bladeren optimaal wil verdelen, moet dus een  $\alpha$  kiezen die “lastig te benaderen” is met rationale getallen. De gulden verhouding  $\varphi$  is nu net een van de lastigste omdat zijn kettingbreuk uitsluitend uit 1'en bestaat. Inderdaad, als we het model laten lopen met  $\alpha = \frac{1}{\varphi}$ , verkrijgen we een mooi regelmatig verdeeld

patroon, dat geen zo'n duidelijk te onderscheiden spiralen bevat:

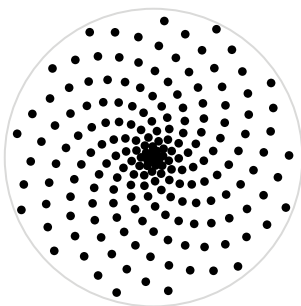
$$\varphi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \ddots}}}}$$



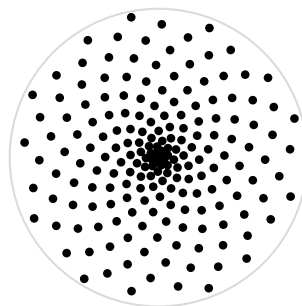
Het resultaat valt prachtig te vergelijken met bijvoorbeeld de stempelschijf van een zonnehoed, hierboven rechts.

De convergenten van de gulden snede zijn  $1, 2, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}, \frac{55}{34} \dots$ . Teller en noemer zijn telkens Fibonacci-getallen, wat meteen een verklaring geeft voor het aantal spiralen of bloemblaadjes. Het patroon hierboven telt 34 spiraalarmen tegen de klok in en 55 met de klok mee.

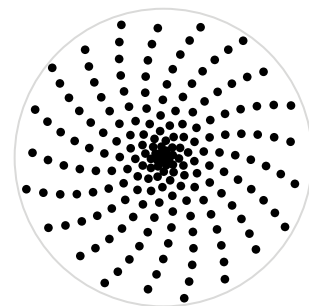
De parameter  $\alpha$  blijkt nogal gevoelig: een kleine afwijking in de hoek waarover telkens geroteerd wordt alvorens een nieuw zaadje of blaadje te plaatsen, verknoeit al gauw het delicate evenwicht bereikt door de gulden snede.



$222,4^\circ$



$\alpha = \frac{360^\circ}{\varphi} (\approx 222,5^\circ)$

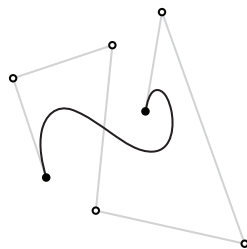


$222,6^\circ$

## 327 Bézierkrommen

Bézierkrommen zijn parameterkrommen die een cruciale rol spelen in veel vectorgrafische software zoals Adobe Illustrator. Hun verdienste is dat slechts enkele punten nodig zijn (standaard vier) om een volledig gladde curve te beschrijven, die daarenboven zeer intuïtief te bewerken is. De uiterste controlepunten geven het begin- en

eindpunt van de kromme weer, de andere punten schetsen het verloop ertussen. Bézierkrommen werden ontwikkeld door Pierre Bézier en Paul de Casteljou, ingenieurs bij respectievelijk Renault en Citroën, die ze gebruikten in autodesign en daarmee de basis voor de moderne CAD legden.



Noem de controlepunten  $\mathbf{P}_0$  t.e.m.  $\mathbf{P}_n$ , waarin  $n$  de orde van de Bézierkromme heet. Een kromme met orde  $n = 1$  is niets meer dan een lijnstuk tussen twee controlepunten en heeft als parameterrepresentatie:

$$\mathbf{B}_1(t) = (1 - t) \cdot \mathbf{P}_0 + t \cdot \mathbf{P}_1 \quad \text{met } t \in [0, 1]$$

Drie punten  $\mathbf{P}_0$ ,  $\mathbf{P}_1$  en  $\mathbf{P}_2$  leggen een kwadratische Bézierkromme vast, verkregen door corresponderende punten op de lineaire Bézierkrommen van  $\mathbf{P}_0$  naar  $\mathbf{P}_1$  en van  $\mathbf{P}_1$  naar  $\mathbf{P}_2$ , lineair te interpoleren:

$$\begin{aligned} \mathbf{B}_2(t) &= (1 - t) \cdot \left( (1 - t) \cdot \mathbf{P}_0 + t \cdot \mathbf{P}_1 \right) + t \cdot \left( (1 - t) \cdot \mathbf{P}_1 + t \cdot \mathbf{P}_2 \right) \\ &= (1 - t)^2 \cdot \mathbf{P}_0 + 2(1 - t)t \cdot \mathbf{P}_1 + t^2 \cdot \mathbf{P}_2 \end{aligned}$$

Analoog definieert men kubieke Bézierkrommen als lineaire combinatie van twee kwadratische:

$$\begin{aligned} \mathbf{B}_3(t) &= (1 - t) \cdot \left( (1 - t)^2 \cdot \mathbf{P}_0 + 2(1 - t)t \cdot \mathbf{P}_1 + t^2 \cdot \mathbf{P}_2 \right) + t \cdot \left( (1 - t)^2 \cdot \mathbf{P}_1 + 2(1 - t)t \cdot \mathbf{P}_2 + t^2 \cdot \mathbf{P}_3 \right) \\ &= (1 - t)^3 \cdot \mathbf{P}_0 + 3(1 - t)^2 t \cdot \mathbf{P}_1 + 3(1 - t)t^2 \cdot \mathbf{P}_2 + t^3 \cdot \mathbf{P}_3 \end{aligned}$$

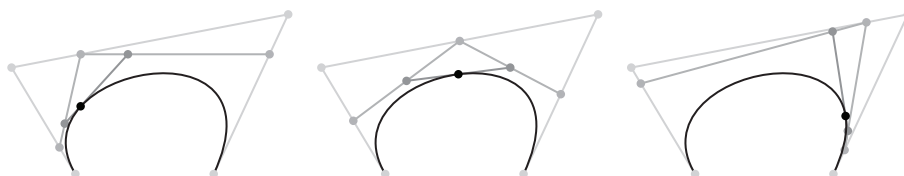
Voor bepaalde keuzes van controlepunten kunnen zulke krommen zichzelf snijden of keerpunten bevatten. De uitbreiding naar meerdere punten verloopt rechttoe rechtaan, en algemeen is de formule als volgt. Bézierkrommen met  $n > 4$  worden in de praktijk maar zelden gebruikt. Meestal verbindt men eenvoudige krommen van lagere orde ter constructie van ingewikkeldere vormen, wat zogeheten splines oplevert.

$$\mathbf{B}_n(t) = \sum_{i=0}^n \binom{n}{i} (1 - t)^{n-i} t^i \cdot \mathbf{P}_i \quad \text{met } t \in [0, 1]$$

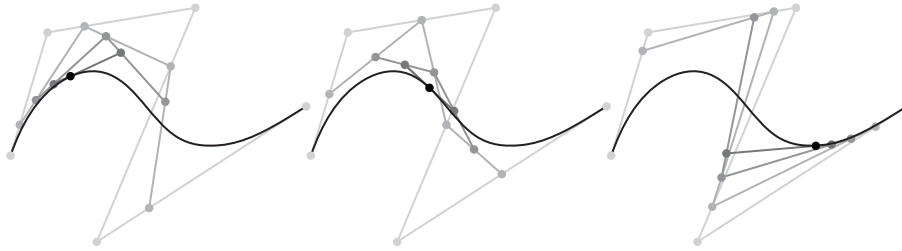
De coëfficiënten van de vectoren  $\mathbf{P}_i$  (die functie van  $t$  zijn) heten Bernsteinveeltermen en waren al bekend in 1912, maar het duurde tot 1959 eer de Casteljou hun grafische mogelijkheden blootlegde, waarna Bézier ze grootschalige bekendheid bracht in 1962. De Casteljou gaf tevens een algoritme dat lineaire combinaties van Bernsteinveeltermen evalueert, met een interessante meetkundige interpretatie:

- Verbind de opeenvolgende controlepunten  $\mathbf{P}_0$  tot en met  $\mathbf{P}_n$  tot een gebroken lijn.
- Verdeel elk lijnstuk in verhouding  $t : (1 - t)$  en verbind de verkregen punten. Dit geeft een nieuwe gebroken lijn met één segment minder.
- Herhaal de vorige stap met dezelfde  $t$ -waarde, tot er nog één enkel punt overblijft: dit is het punt op de Bézierkromme horende bij parameter  $t$ .

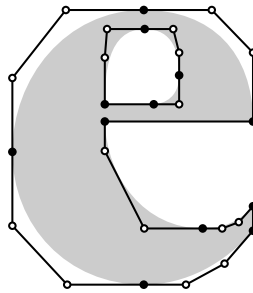
Beschouw dit proces toegepast op vier punten, voor parameters  $t = 0,25$ ,  $t = 0,5$  en  $t = 0,85$ :



Hetzelfde proces met vijf punten, voor dezelfde parameterwaarden:



Vandaag spelen Bézierkrommen ook nog een grote rol in typografie: TrueType lettertypen slaan lettertekens op als splines samengesteld uit lineaire en kwadratische krommen, OpenType benut ook kubieke krommen. Hieronder staat zo'n lettertekenspline, waarbij de zwarte punten uiteinden van aparte krommen voorstellen en de witte punten controlepunten ertussen.

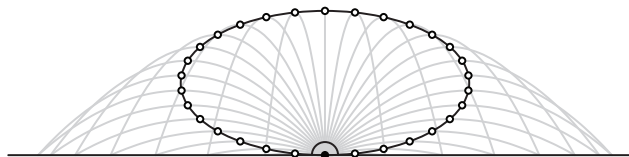


## 328 Ballistische ellips

Ballistiek is het onderzoeksdomein van de mechanica dat projectielbewegingen bestudeert. Dit probleem in het bijzonder heeft ook een mooie wiskundige betekenis. Wanneer een projectiel wordt afgeschoten vanuit de oorsprong van het  $xy$ -vlak met een beginsnelheid  $v_0$  en onder een hoek  $\alpha$  met de  $x$ -as, dan wordt de vergelijking van zijn baan gegeven door de volgende parametervoorstelling:

$$x(t) = v_0 t \cos \alpha, \quad y(t) = v_0 t \sin \alpha - \frac{g t^2}{2}$$

Lanceer nu een aantal projectielen vanuit de oorsprong, met gelijke beginsnelheid maar variërende hoeken. Een interessante vraag is dan: welke kromme is de meetkundige plaats van de maximale hoogtes van de parabolische banen? Verrassend genoeg blijkt dit een perfecte ellips te zijn:



$$\frac{x^2}{4a^2} + \frac{(y-a)^2}{a^2} = 1 \quad \text{met } a = \frac{v_0^2}{4g}$$

De vergelijking van de ballistische ellips kan zonder veel moeite worden opgesteld. De vorm van de ellips is onafhankelijk van de parameters van de bewegingen: de lange as is steeds dubbel zo lang als de korte, en dus heeft de ellips eccentriciteit  $\frac{\sqrt{3}}{2}$ .

## 329 Lexicodes

Lexicografische codes, of lexicodes zoals John Conway ze vaak afkorte, zijn eenvoudig te definiëren codes maar kennen toch een rijke structuur, die absoluut niet voor de hand ligt. Om een systeem van lexicodes vast te leggen,



volstaan een natuurlijk getal  $k$  en een welbepaald “alfabet”, waarvoor we hier  $\mathbb{N}$  gebruiken. De lexicographische codes zijn dan “woorden” over dit alfabet, in de volgende vorm te schrijven:

$$A = \dots a_n \dots a_2 a_1 a_0$$

Er zijn nog een aantal bijkomende restricties van kracht. Slechts een eindig aantal  $a_i$ 's (“cijfers” van  $A$ ) mag verschillen van 0, en voorloophnullen mogen worden weggelaten in de notatie. We definiëren ook een natuurlijke ordening op de codes:  $A > B$  als en slechts als  $a_N > b_N$  voor zekere  $N$ , met  $a_n = b_n$  voor alle  $n > N$ .

Nu kunnen we de lexicografische codes inductief definiëren. Veronderstel dat er al een verzameling codewoorden bekend is; het volgende woord is dan het kleinste woord dat verschilt van alle reeds bekende woorden in minstens  $k$  cijfers. De code begint telkens met een kleinste woord, zijnde het nulwoord  $\dots 000$ . Stel bijvoorbeeld  $k = 3$ , dan zijn de eerste woorden van de lexicode:

$$\begin{array}{c} \dots 000000 \\ \dots 000111 \\ \dots 000222 \\ \dots 000333 \\ \vdots \\ \dots 001012 \\ \dots 001103 \\ \dots 001230 \\ \dots 001321 \\ \dots 001456 \\ \vdots \\ \dots 002023 \\ \vdots \\ \dots 003031 \\ \vdots \\ \dots 004048 \\ \vdots \\ \dots 010013 \\ \vdots \end{array}$$

Onthou dat elk natuurlijk getal als cijfer kan dienen, dus ook bijv.  $\dots 00121212$  is een lexicodewoord, met drie cijfers. De centrale lexicodestelling (of zoals ze hier gepresenteerd wordt, eigenlijk -axioma) stelt nu dat de verzameling codes, uitgerust met coördinaatsgewijze optelling en scalaire vermenigvuldiging, de structuur van een vectorruimte heeft. De definities van deze bewerkingen zijn echter *niet* die zoals we ze kennen! Beschouw maar eens de codes  $(1012)$  en  $(111)$ . De naïeve som ervan, zijnde  $(1123)$ , is géén lexicode, evenmin als het naïeve scalair product van de eerste met 2, zijnde  $(2024)$ .

Feitelijk worden de nieuwe bewerkingen juist vastgelegd door het axioma. Merk op dat  $(\dots 00000) + (\dots 00000) = (\dots zzzzz)$  met  $0 + 0 = z$ , wat een nieuwe lexicode moet zijn en dus slechts een eindig aantal niet-nul cijfers mag hebben. Dit impliceert dat  $0 + 0$  nog steeds gelijk is aan 0.

Wat ook bewaard blijft, is dat  $x + 0 = x = 0 + x$  voor alle  $x$ . De som  $(111) + (1012)$ , die dan van de vorm  $(11xy)$  is, is ook een lexicode en kan dus enkel  $(1103)$  zijn. Dit betekent dat  $y = 1 + 2 = 3$ , maar  $x = 1 + 1 = 0$ ! Andere sommen kunnen analoog worden afgeleid en leveren de volgende opteltabel op:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

In feite kan men aantonen dat deze optelling niet volledig uit de lucht komt vallen. Wanneer  $N$  een macht van twee is, dan blijkt  $N + n$  gelijk aan de som zoals we die kennen, voor alle  $n < N$ . Ook is steeds  $N + N = 0$ . Deze eigenschap is voldoende om te besluiten dat de lexicodesom in feite overeenkomt met de toch iets bekendere nimsom (zie 339, blz. 332).

Vermenigvuldiging is moeilijker te herkennen. Deze is slechts op een constante factor na bepaald, zodat het mogelijk is een eenheid te kiezen; een acceptabele keuze is 1. Voor nul blijft gelden dat  $x \cdot 0 = 0 = 0 \cdot x$ , ongeacht  $x$ . Het product  $2 \cdot (1\ 1\ 0\ 2)$ , dat dan van de vorm  $(2\ 2\ 0\ x)$  is, impliceert nu dat  $2 \cdot 2 = 3$ , en zo kan men de volgende vermenigvuldigingstabel beginnen opbouwen:

·	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	3	1	8	10	11	9
3	0	3	1	2	12	15	13	14
4	0	4	8	12	6	2	14	10
5	0	5	10	15	2	7	8	13
6	0	6	11	13	14	8	5	3
7	0	7	9	14	10	13	3	4

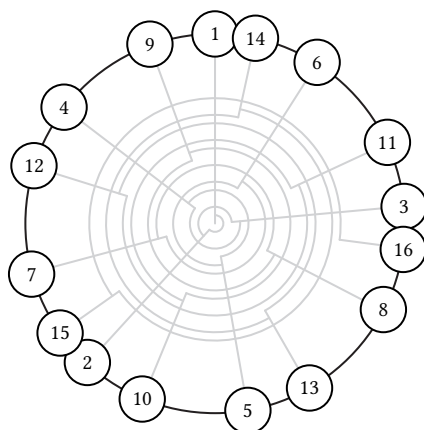
Wanneer  $N$  een Fermatgetal is, d.i. een getal van de vorm  $2^{2^k}$  (zie 47, blz. 36), dan is het product  $N \cdot n$  dat waarmee we vertrouwd zijn, voor alle  $n < N$ . Daarenboven is  $N \cdot N = \frac{3}{2}N$  zoals we dat kennen, en deze relaties volstaan om alle mogelijke producten uit te rekenen.

Tot slot is het ook opmerkelijk dat 1, 2 en 3 net de derdemachtswortels van de eenheid zijn, of 1, 8, 10, 13 en 14 de vijfdemachtswortels.

### 330 Gulden rondgang

Nog een bewijs dat Fibonaccigetallen (zie 91, blz. 65) onlosmakelijk verbonden zijn met de gulden verhouding. Teken een cirkel waarvan de omtrek gelijk is aan de gulden snede,  $\frac{1}{2}(1 + \sqrt{5})$ . Kies een startpunt op de cirkelrand

en geef deze label 1. Beweeg vervolgens langsheen de rand in een vaste richting, in stappen met booglengte één, en label de aangetroffen punten 2, 3 etc. Dit voorbeeld illustreert de eerste 16 punten (kloksgewijze geselecteerd).

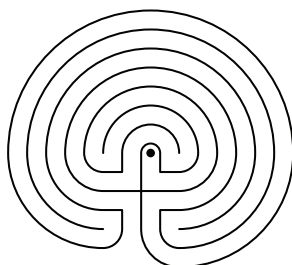


Na elke stap is het verschil tussen elk paar adjacente getallen op de cirkel dan een Fibonaccigetel!

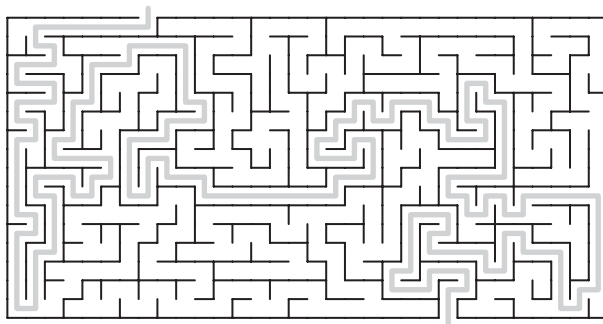
### 331 Doolhoven

Doolhoven vormen al millennialang een bron van cultuur en amusement. Denk maar aan de Griekse mythologie (de Minotaurus in het labyrint in Knossos), het bordspel *De betoverde doolhof*, hagenlabyrinten of spiegeltenten in hedendaagse amusementsparken, algemene populaire cultuur (boeken, films, videogames), kunst en religie...

De oudst bekende afbeeldingen van doolhoven zijn meer dan drie millennia oude, mediterrane rotstekeningen. In tegenstelling tot modernere doolhoven, die allerlei complexe vertakkingen vertonen, bestaan deze klassieke labyrinten maar uit één lange bochtige gang en volgt hun constructie vaak een vast patroon zoals hieronder. Ook veel Keltische patronen vertonen doolhofachtige structuren.



Dergelijke puzzels zijn ook wiskundig significant, aangezien ze kunnen worden gemodelleerd via grafentheorie of topologie en er interessante algoritmes bestaan om doolhoven te genereren of op te lossen. Een eenvoudige en snelle tactiek, die enkel bruikbaar is bij overzicht van de volledige doolhof ineens, is alle doodlopende eindes aanduiden en de doorgangen van daaruit vullen tot aan het eerste kruispunt (*dead end filling*). Op die manier wordt de unieke oplossing blootgelegd als die bestaat, of alle mogelijke oplossingen in een doolhof met lussen.



Voor enkelvoudig samenhangende doolhoven, waarin alle muren met elkaar verbonden zijn en er geen eilanden voorkomen, is *wall following* welbekend: houd één hand in contact met een muur en blijf deze volgen. Als men terugkomt op de startpositie heeft de doolhof geen uitweg of is deze niet enkelvoudig samenhangend.

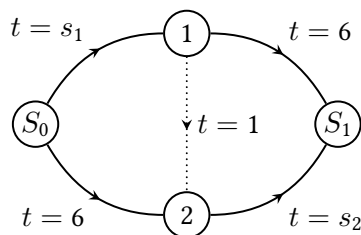
Een variant op wall following vindt gegarandeerd de uitgang vanuit eender welke startpositie in een willekeurige tweedimensionale doolhof (ook met lussen of eilanden) en wordt vernoemd naar John Pledge, die het algoritme als twaalfjarige student ontwierp. Het algoritme van Pledge probeert in essentie obstakels te vermijden. Vertrek in een willekeurig gekozen richting en ga rechtdoor, totdat een opstakel opduikt. Pas dan wall following toe en hou het aantal gemaakte bochten bij (tel bijvoorbeeld +1 voor een draai naar rechts en  $-1$  naar links). Wanneer men terug in de oorspronkelijke richting kijkt (te zien aan de bijgehouden som, die dan 0 is), wordt het obstakel achtergelaten en gaat men terug rechtdoor tot aan een nieuw obstakel, tot de uitgang wordt bereikt.

Charles Trémaux gaf een algoritme dat doolhoven in eender welke dimensie oplost. Markeer elke gevolgde gang met een lijn. Bij elke nog onbezochte kruising kies je een willekeurige nieuwe richting; anders keer je terug, markeer je de gang met een tweede lijn, en kies je een nieuwe gang bij de volgende kruising indien mogelijk.

### 332 Paradox van Braess

De paradox van Braess wordt toegekend aan de Duitse Dietric Braess en stelt dat extra capaciteit toevoegen aan een netwerk, waarbij eenheden zelfzuchtig hun eigen route kiezen, kan resulteren in een daling van de globale prestatie. Denk bijvoorbeeld aan verkeersnetwerken: de paradox beweert in deze context dat het aanleggen van extra wegen kan leiden tot een minder efficiënte verkeersstroom, in tegenstelling tot wat men zou verwachten.

Een voorbeeld:



Vier pendelaars wensen van vertrekpunt  $S_0$  naar eindpunt  $S_1$  te reizen. Vooraleer de gestippelde route wordt aangelegd, zijn er twee banen, elk met een tussenstop. De reistijd (in minuten) over de eerste helft van de eerste baan is gelijk aan het aantal reizigers  $s_1$  die deze weg gebruiken, en over de tweede helft steeds gelijk aan zes minuten (onafhankelijk van het aantal weggebruikers). Voor de tweede baan is de situatie analoog.

De reizigers zijn rationeel maar zelfzuchtig, en kiezen steeds de snelst mogelijke route. Evenwicht treedt hier op als  $s_1 = s_2 = 2$ : beide routes duren dan elk acht minuten en niemand heeft er baat bij om van route te veranderen.

Dit verandert wanneer de extra weg tussen beide tussenstops in gebruik wordt genomen. Veronderstel dat de tijd nodig voor deze weg slechts één minuut is. In deze situatie verkiest de rationale reiziger in eerste instantie route  $S_0-1$ , want deze neemt hoogstens vier minuten in beslag, terwijl route  $S_1-2$  gegarandeerd langer duurt. Eenmaal aan dit tussenstation is de route  $1-2$  te verkiezen, opnieuw omdat het vervolg van de rit dan met zekerheid de kortste is van beide mogelijkheden. Dit betekent dat de optimale reistijd nu verhoogd is tot negen minuten, terwijl niemand geneigd zou zijn de originele routes te gebruiken (die nu tien minuten kosten)!

Iedereen zou tijd besparen mocht men overeenkomen de nieuwe route niet te gebruiken, maar dan kan iedereen persoonlijk voordeel halen door deze weg te gebruiken; het globale optimale evenwicht is dus niet stabiel.

Het paradoxale effect van Braess treedt wel degelijk ook op in realistische situaties: zo werd in Seoul een vlottere verkeersstroom rond de stad opgemerkt toen een snelweg werd afgesloten voor restauratiewerken, in Stuttgart verbeterde de verkeerssituatie niet (ondanks investeringen in het wegennet in 1969) totdat een deel van de nieuw aangelegde weg opnieuw werd gesloten, en de verkeersopstopping in New York City nam af in 1990 door het sluiten van een straat. Ook in het design van datanetwerken kan de paradox zich manifesteren.





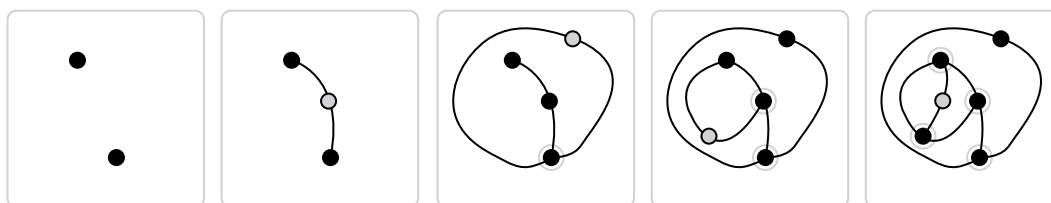
## 333 Sprouts

Sprouts werd uitgevonden door John Conway en Michael Paterson op de Cambridge University begin jaren 60 en werd aandachtig geanalyseerd en gepopulariseerd door Conway. Het is nog steeds een van de populairste wiskundige spellen met pen en papier; er bestaan zelfs heuse Sproutstoernooien.

Het spel begint met een aantal punten op een vel papier. Elke speler tekent op zijn beurt een nieuwe lijn tussen twee bestaande punten en tekent daarop een nieuw punt, volgens deze regels:

- De nieuwe lijn mag geen andere bestaande lijn raken of kruisen.
- Het nieuwe punt op de lijn mag niet samenvallen met een eindpunt van de lijn.
- Uit geen enkel punt mogen meer dan drie lijnen vertrekken.

Lussen zijn toegestaan. De speler die geen geldige lijn meer kan trekken, verliest.



Ondanks dat na elke beurt er een nieuw punt bijkomt, kan het spel niet eeuwig doorgaan. Een beginopstelling met  $n$  punten geeft een spel met minimum  $2n$  beurten en maximum  $3n - 1$ . Aangezien in Sprouts ook duidelijk geen gelijkspel mogelijk is, bestaat er een winnende strategie voor ofwel de eerste, ofwel de tweede speler. Voor een klein aantal beginpunten is de analyse eenvoudig, maar het spel wordt snel complex bij meerdere beginpunten. Denis Mollison bewees dat Sprouts met zes punten een winnende methode voor de tweede speler bevat, in een handgemaakte, 47 pagina's tellende analyse. Met behulp van de beste hardware van dat moment konden David Applegate, Guy Jacobson en Daniel Sleator in 1990 grotere spellen onderzoeken, tot en met elf punten. Ze bekwamen de volgende gegevens en vermoedden dat het patroon zich voortzet:

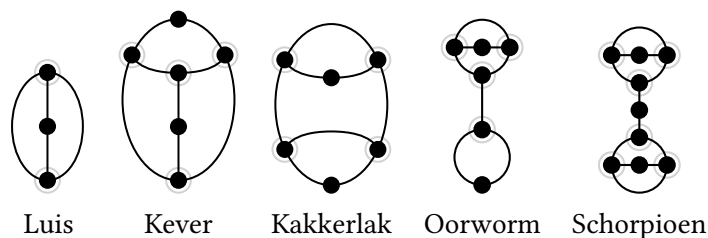
Beginpunten:	1	2	3	4	5	6	7	8	9	10	11
Winnende speler:	2	2	1	1	1	2	2	2	1	1	1

Dus, de eerste speler zou moeten kunnen winnen wanneer het aantal beginpunten congruent is met drie, vier of vijf, modulo zes. In 2006 bereikte Josh Jordan een verdere analyse tot en met 14. Julien Lemoine en Simon Viennot bedachten een efficiënt algoritme om de berekeningen drastisch te versnellen, en breidden de analyse verder uit tot 44 punten in 2011. Tot zover blijken alle resultaten consistent met het vermoeden van Applegate, Jacobson en Sleator.

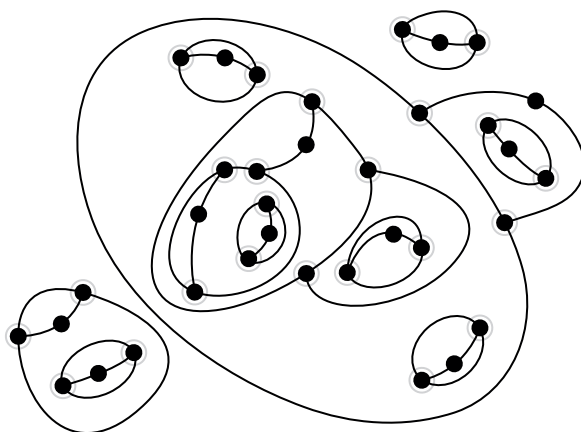
Het is eenvoudig in te zien waarom een partijtje Sprouts na ten hoogste  $3n - 1$  stappen beëindigd is. Noem het "leven" van een punt het aantal lijnen dat er nog aan kan toegevoegd worden; dus een spel met  $n$  punten begint met  $3n$  levens. Elke beurt verliezen er twee punten een leven, en wordt er een punt met slechts één leven toegevoegd, zodat het totaal met één leven gereduceerd wordt. Het allerlaatste punt van het spel is echter nog steeds in leven, dus het totaal aantal beurten kan maximaal  $3n - 1$  bedragen.



De zonderlinge FROZOM-stelling van Mollison en Conway (Fundamental Theorem of Zeroth Order Moribundity) houdt in dat wanneer een spel juist  $2n$  beurten duurt, de eindconfiguratie dan bestaat uit de volgende “insecten”, eventueel binnenstebuiten gedraaid:

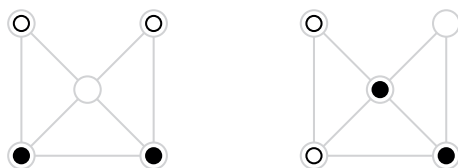


Meer bepaald bevat het eindspel juist één van deze insecten, geïnfecteerd met een onbepaald aantal luizen. Het voorbeeld hieronder bevat een binnenstebuiten gekeerde schorpioen midden in een heuse luizenplaag.



### 334 Pong Hau K'i

Pong Hau K'i is een traditioneel Chinees bordspelletje en staat in Korea bekend als Ou-moul-ko-no. Het spelbord bestaat uit vijf velden, verbonden door zeven lijnen; beide spelers krijgen elk twee stenen (zie de beginopstelling links) en verplaatsen elk om beurt één van hun stenen naar een aanliggend veld. Winnaar is degene die zijn tegenstander weet te blokkeren, zodat die geen geldige zet meer kan doen, zoals voor wit het geval is op het rechterbord.

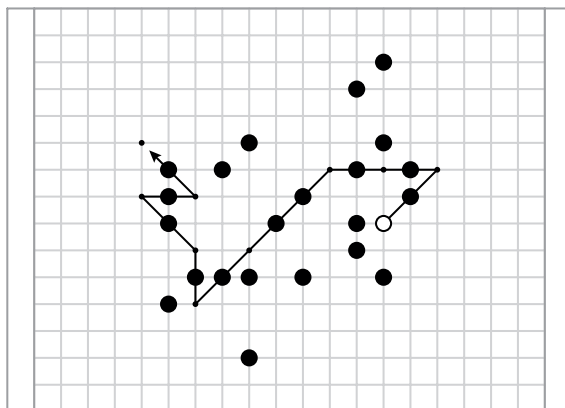


### 335 Phutball

In hun befaamde wiskundige spellenboek *Winning Ways for your Mathematical Plays* beschreven Richard Guy, John Conway en Elwyn Berlekamp dit complexe strategiespel Phutball, ondertussen ook wel gekend als Philosopher's Football. Het spel wordt gespeeld op een  $15 \times 19$ -rooster met één witte steen, de voetbal, en zoveel zwarte stenen als nodig, de voetballers. De ruimte achter de uiterste kolommen van het bord dient als goal.

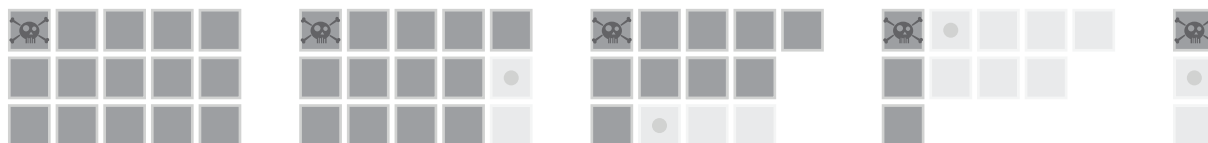
De match begint met de voetbal op de centrale kruising. Elk om beurt zetten de spelers een nieuwe voetballer op een lege kruising op het veld, of verplaatsen ze de bal. De laatste optie bestaat uit een aantal opeenvolgende sprongen over reeds geplaatste voetballers, willekeurig hoeveel, maar een voetballer wordt van het veld gehaald

als de bal hem gepasseerd is. De reeks sprongen mag zo lang doorgaan als gewenst zolang er voetballers beschikbaar zijn. Een doelpunt wordt gescoord, en zo de winnaar bepaald, wanneer de bal op de laatste kolommen van het veld (de doellijnen) terecht komt, of in de ruimte erachter.



### 336 Chomp

Chomp is een eenvoudig doch intrigerend spelletje, geformuleerd door Frederik Schuh in een equivalente vorm met delers van een vastgelegd getal, en later in deze vorm door David Gale. Het spelbord is een chocoladereep, van overeengekomen grootte, waarvan het blokje linksboven vergiftigd is. Elk om beurt kiezen de spelers een blokje uit en eten ze het op, samen met alle blokjes die zich rechts en onder dat blokje bevinden. Wie gedwongen wordt het giftige blokje op te eten, verliest.



Er bestaat een winnende strategie voor de eerste speler, ongeacht de grootte van de chocoladereep, maar het bewijs daarvoor is niet constructief en er is in feite geen strategie gekend voor het algemene bord. Veronderstel dat speler  $B$  een winnende strategie heeft tegen elke mogelijke openingszet van speler  $A$ . Wanneer  $A$  dus het chocoladeblokje helemaal rechtsonder kiest, zou  $B$  een reactie kunnen geven die hem naar de overwinning leidt. Maar als zo'n winnende zet bestaat, kon  $A$  deze direct in zijn eerste beurt kiezen en aldus zelf winst afdwingen. Als  $B$  wint, moet  $A$  dus ergens een fout gemaakt hebben.

Ondanks dit eenvoudige argument kunnen partijtjes Chomp verrassend complex zijn, zeker met grotere repen. Er zijn wel vorderingen gemaakt op specifieke borden, zoals  $2 \times n$ .

Chomp wordt eenvoudig uitgebreid naar drie- of hogerdimensionale varianten. Ook borden die zich oneindig ver uitstrekken zijn interessante generalisaties. De originele versie van Schuh vertrekt vanuit de strikte delers van willekeurig geheel getal i.p.v. chocolade, en laat de spelers om beurt een overblijvende deler aanduiden en alle veelvouden ervan schrappen. Een getal met  $n$  priemdelers modelleert zo een  $n$ -dimensionaal Chompspel, met als afmetingen de exponenten van de priemdelers.

### 337 Lineair schaken

Martin Gardner introduceerde in 1980 via zijn column in de *Scientific American* de volgende schaakvariant. In deze versie bewegen de koning en de toren zoals gebruikelijk, maar beweegt het paard juist twee hokjes, eventueel door over een ander stuk te springen. Wit kan hier gelijkspel afdwingen in zijn openingszet door

de toren van zwart te slaan. Gardner vraagt zijn lezers of de witte speler ook een winnende strategie heeft, en inderdaad, wit kan schaakmat afdwingen in zes zetten, door met z'n paard over de toren te springen.



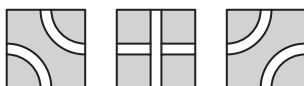
De volgende variant is afkomstig van Sid Sackson. De stukken bewegen zoals in Gardners versie, maar één keer per spel mag elke speler zijn koning omwisselen met zijn toren op het uiterste eind van het bord, als een soort rokeren. Alleen mag deze rokade ook wanneer de koning en toren al verzet zijn, de koning in schaak staat, etc. Wanneer rokeren zijn enige mogelijke optie is, kan een speler ook gelijkspel door patstelling claimen. Dit om te voorkomen dat wit al in de eerste beurt de toren van de tegenstander slaat en direct tot een rokade dwingt.



Dam Glimnes variant is nog wat groter en wordt gespeeld op een bord met 18 vakjes. De koning beweegt één of twee vakjes, zonder te springen. Een toren gaat zoals normaal. Lopers mogen hier enkel over vakjes van hun kleur gaan, maar kunnen over stukken springen als deze op een vakje van het andere kleur staan. De dame heeft de bewegingsvrijheid van zowel de loper als de toren. Het paard beweegt twee of drie vakjes, en springt over andere stukken. De pionnen ten slotte kunnen enkel één vakje vooruit gaan, of twee in hun eerste zet, en slaan zoals ze bewegen. Ook rokeren is toegestaan, onder de gebruikelijke voorwaarden van het klassieke schaakspel.



### 338 **Black Path Game**



### 339 **Nim**





- Wiskunde is de koninging der wetenschappen en getaltheorie is de koningin der wiskunde.  
*Carl Friedrich Gauss*
- Wie niet gelooft dat wiskunde simpel is, realiseert zich niet hoe gecompliceerd het leven is.  
*John von Neumann*
- Een wiskundige is een apparaat dat koffie omzet in stellingen.  
*Alfréd Rényi*
- Sommige dingen lijken ongelooflijk voor diegenen die geen wiskunde gestudeerd hebben.  
*Archimedes*
- Wiskunde is de deur én de sleutel tot de wetenschappen.  
*Roger Bacon*
- God schiep het gehele getal, al de rest is mensenwerk.  
*Leopold Kronecker*
- Bij mij verandert alles in wiskunde.  
*René Descartes*
- Een wiskundige die niet iets heeft van een dichter, zal nooit een complete wiskundige zijn.  
*Karl Weierstrass*
- Waarom zijn getallen mooi? Dat is zoals vragen waarom Beethovens Negende Symfonie mooi is: als je niet ziet waarom, kan niemand het uitleggen. Ik weet dat getallen mooi zijn. Als zij al niet mooi zijn, is niks het.  
*Paul Erdős*
- Wiskunde is als zuurstof. Als het er is, merk je het niet. Als het er niet zou zijn, merk je dat je niet zonder kunt.  
*Lex Schrijver*
- Getaltheoretici zijn zoals lotuseters: eenmaal dit voedsel geproefd, kunnen ze het nooit opgeven.  
*Leopold Kronecker*
- De essentie van de wiskunde ligt in haar vrijheid.  
*Georg Cantor*
- Filosofie is een spel met doelen, maar zonder regels. Wiskunde is een spel met regels, maar zonder doelen.  
*Ian Ellis*
- Wiskunde is als de liefde: een simpel idee, maar het kan gecompliceerd worden.  
*onbekend*
- Wij horen vaak dat wiskunde hoofdzakelijk bestaat uit “stellingen bewijzen”. Is de taak van een schrijver hoofdzakelijk “zinnen schrijven”?  
*Gian-Carlo Rota*

- In de wiskunde zijn wij eerder dienaars dan meesters.  
*Charles Hermite*
- Wiskunde bevat niet alleen waarheid, maar ook opperste schoonheid.  
*Bertrand Russell*
- Net zoals de Nijl begint de studie van wiskunde in nietigheid en eindigt ze in grootsheid.  
*Charles Caleb Colton*
- Hoewel hij niet altijd zijn gebondenheid herkent, leeft de moderne mens onder een getallentirannie.  
*Nicholas Eberstadt*
- De logica is onoverwinnelijk, want om logica aan te vallen is het noodzakelijk logica te gebruiken.  
*Pierre Boutroux*
- Het boek der natuur is geschreven in de taal der wiskunde.  
*Galileo Galilei*
- Als God bestaat, is hij een groots wiskundige.  
*Paul Dirac*
- Waar het getal is, is er schoonheid.  
*Proclus*
- Wiskundige zijn is onmogelijk zonder poëet te zijn in ziel.  
*Sofia Kovalevskaya*
- Het getal beheerst het universum.  
*Pythagoras*
- Als ik ongelukkig ben, doe ik wiskunde om gelukkig te worden. Als ik gelukkig ben, doe ik wiskunde om gelukkig te blijven.  
*Alfréd Rényi*
- Enkel in wiskunde komen waarheid en schoonheid op hetzelfde neer.  
*Danica McKellar*
- De wiskundige bestudeert geen zuivere wiskunde omdat ze praktisch is, hij bestudeert ze omdat hij zich erin verheugt en hij verheugt zich erin omdat ze mooi is.  
*Henri Poincaré*
- Als ik na duizend jaar slapen zou ontwaken, zou mijn eerste vraag zijn: “Is de Riemannhypothese al bewezen?”  
*David Hilbert*
- Wiskunde bestaat erin het meest evidente te bewijzen om de minst evidente manier.  
*George Pólya*
- Het leven is slechts goed voor twee zaken: wiskunde ontdekken en wiskunde onderrichten.  
*Siméon Poisson*
- De wetten der natuur zijn slechts de wiskundige gedachten van God.  
*Euclides*
- Logica is de hygiëne van de wiskundige om zijn ideeën gezond en sterk te houden.  
*Hermann Weyl*

- Een wiskundige is een goochelaar die zijn geheimen verklapt.  
*John Conway*
- Het verschil tussen een dichter en een wiskundige is dat de dichter probeert zijn gedachten in de hemel te krijgen, terwijl de wiskundige juist de hemel in zijn gedachten wil.  
*Gilbert Chesterton*
- Zuivere wiskunde is het beste spel ter wereld. Het is meeslepender dan schaken, een grotere gok dan poker, en gaat langer mee dan Monopoly. Het is gratis. En het kan overal gespeeld worden: Archimedes deed het in een badkuip.  
*Richard Trudeau*
- “Ingebeelde” universa zijn zo veel mooier dan dit dom gebouwde “reële” universum, en de meeste van de fijnste producten geschapen uit de verbeelding van een wiskundige worden, zodra ze zijn gemaakt, afgewezen, door de brutale maar voldoende reden dat ze de feiten niet passen.  
*Godfrey Harold Hardy*
- Alle wiskundigen delen een gevoel van verbazing over de oneindige diepte, de mysterieuze schoonheid en de bruikbaarheid van de wiskunde.  
*Martin Gardner*
- Ik hou van wiskunde omdat ze niet menselijk is en niks bijzonders te doen heeft met deze planeet of met het gehele toevallige universum, want zoals Spinoza’s God zal ze niet op haar beurt van ons houden.  
*Bertrand Russell*
- Zuivere wiskunde is, op haar manier, de poëzie der logische gedachten.  
*Albert Einstein*
- Ga diep genoeg in eender wat en je zal wiskunde ontdekken.  
*Dean Schlicter*
- Het is niet de taak van de wiskundige om correcte rekenkundige bewerkingen uit te voeren, dat is de taak van de boekhouder.  
*Samuil Shchatunovski*







## Boeken

- AIGNER, M., ZIEGLER, G., *Proofs from THE BOOK*.  
Berlijn, Springer-Verlag, 2010, 274 p.
- BELLOS, A., *Getallen ontraadseld*.  
Utrecht/Antwerpen, Kosmos Uitgevers B.V., 2010, 432 p.
- CONWAY, J., CURTIS, R., NORTON, S., PARKER, R., WILSON, R., *ATLAS of Finite Groups*.  
New York, Oxford University Press, 1985, 294 p.
- CONWAY, J., GUY, R., *The Book of Numbers*.  
New York, Springer-Verlag, 1996, 310 p.
- CRILLY, T., *50 inzichten wiskunde*.  
Diemen, Veen Magazines, 2009, 208 p.
- DELAHAYE, J.-P., *Complexiteit: waar wiskunde en informatica tegen grenzen aanlopen*.  
Diemen, Veen Magazines, 2008, 234 p.
- DE SMIT, B., TOP, J., *Speeltuin van de wiskunde*.  
Diemen, Veen Magazines, 2003, 139 p.
- DU SAUTOY, M., *Het symmetriemonster*.  
Amsterdam, Uitgeverij Nieuwezijds, 2009, 360 p.
- ELWES, R., *Hoe bouw je een brein: 35 echt interessante toepassingen van wiskunde*.  
Houten, Uitgeverij Unieboek | het Spectrum, 2012, 224 p.
- GLAESER, G., POLTHIER, K., *Wiskunde in beeld*.  
Diemen, Veen Magazines, 2012, 340 p.
- HOFFMAN, P., *De man die van getallen hield*.  
Amsterdam, Uitgeverij Bert Bakker, 1999, 249 p.
- HOFSTADTER, D., *Gödel, Escher, Bach: een eeuwige gouden band*.  
Amsterdam, Uitgeverij Contact, 1985, 899 p.
- GARNER, M., *The Colossal Book of Mathematics*.  
New York City, W. W. Norton & Company, 2001, 724 p.
- KLOUWEN, J., *Denkwaar: spelen met getallen, woorden en vormen*.  
Diemen, Veen Magazines, 2010, 192 p.
- KRANTZ, S., *Techniques of Problem Solving*.  
U.S., American Mathematical Society, 1997, 465 p.
- MOSCOVICH, I., *Het grote breinbreker boek*.  
Tielt, Uitgeverij Lannoo, 2011, 432 p.
- PETCOVIĆ, M., *Famous Puzzles of Great Mathematicians*.  
U.S., American Mathematical Society, 2009, 325 p.
- PICKOVER, C., *Het wiskundeboek*.  
Kerkdriel, Librero b.v., 2010, 528 p.
- PICKOVER, C., *Wonders of Numbers*.  
Oxford, Oxford University Press, 2000, 396 p.
- POLSTER, B., *The Shoelace Book: a mathematical guide to the best (and worst) ways to lace your shoes*. U.S., American Mathematical Society, 2006, 126 p.

- POOK, L., *Flexagons inside out*.  
U.K., Cambridge University Press, 2003, 170 p.
- RICHESON, D., *Euler's Gem*.  
New Jersey, Princeton University Press, 2012, 317 p.
- STEWART, I., *17 equations that changed the world*.  
Londen, Profile Books, 2012, 342 p.
- STEWART, I., *Schatkamer vol wiskundige uitdagingen*.  
Hilversum, Uitgeverij Lias, 2012, 334 p.
- STEWART, I., *Verzameling van wiskundige raadsels*.  
Roeselare, Roularta Books, 2011, 307 p.
- TANTON, J., *Mathematics Galore!*  
U.S., Mathematical Association of America, 2012, 272 p.
- VAN DEN BRANDHOF, A., GUICHELAAR, J., JASPERS, A., *De Pythagoras code*.  
Amsterdam, Uitgeverij Bert Bakker, 2011, 271 p.
- VAN DEN BRANDHOF, A., VAN DER VEEN, R., VAN DE CRAATS, J., KOREN, B.,  
*De zeven grootste raadsels van de wiskunde*. Amsterdam, Uitgeverij Bert Bakker,  
2012, 186 p.
- VAN DEN ESSEN, A., *Magische vierkanten*.  
Diemen, Veen Magazines, 2006, 238 p.
- VAN DER NOORT, V., *Getallen zijn je beste vrienden: ontboezemingen van een nerd*.  
Amsterdam, Uitgeverij Athenaeum, 2011, 309 p.
- VAN DER VEEN, R., VAN DE CRAATS, J., *De Riemann-hypothese*.  
Utrecht, Epsilon Uitgaven, 2011, 102 p.
- WATKINS, J., *Wiskunde op een schaakbord*.  
Diemen, Veen Magazines, 2008, 271 p.
- WELLS, D., *Mysterieuze en fascinerende raadsels*.  
Amsterdam, Uitgeverij Bert Bakker, 1997, 389 p.
- WELLS, D., *Woordenboek van eigenaardige en merkwaardige getallen*.  
Amsterdam, Uitgeverij Bert Bakker, 1987, 267 p.
- WELLS, D., *Woordenboek van merkwaardige en interessante meetkunde*.  
Amsterdam, Uitgeverij Bert Bakker, 1993, 333 p.
- WINKLER, P., *Mathematical Puzzles: a connoisseur's collection*.  
Canada, A K Peters, 2004, 163 p.
- WOLFRAM, S., *A New Kind of Science*.  
U.S., Wolfram Media Inc., 2002, 1280 p.

## Algemene websites

- <http://www.artofproblemsolving.com>
- <http://www.cut-the-knot.org>
- <http://www.futilitycloset.com>
- <http://www.oeis.org>
- <http://www.math.hmc.edu/funfacts>
- <http://www.mathpages.com>
- <http://math.stackexchange.com>
- <http://mathworld.wolfram.com>
- <http://www.openproblemgarden.org>
- <http://www.theoremoftheday.org>

- <http://www.wikipedia.be>
- <http://www.wiskundemeisjes.nl>

## Specifieke websites

- [http://www.argentum.freemove.co.uk/lex\\_home.htm](http://www.argentum.freemove.co.uk/lex_home.htm)
- <http://www.astrolog.org/labyrnth/algrithm.htm>
- <http://www.chaos-math.org/>
- <http://www.chessvariants.org>
- <http://www.cim.mcgill.ca/~pdimit/cs507/webpage>
- <http://www.conwaylife.com/wiki>
- <http://www.cube20.org>
- [http://euler.slu.edu/escher/index.php/Wallpaper\\_Patterns](http://euler.slu.edu/escher/index.php/Wallpaper_Patterns)
- <http://faculty.evansville.edu/ck6/integer/fractals.html>
- <http://www.gomboc.eu>
- <http://helm.lu/cube/MarshallPhilipp>
- [http://www-history.mcs.st-and.ac.uk/HistTopics/Perfect\\_numbers.html](http://www-history.mcs.st-and.ac.uk/HistTopics/Perfect_numbers.html)
- [http://googology.wikia.com/wiki/TREE\\_sequence](http://googology.wikia.com/wiki/TREE_sequence)
- <http://www.geomagicsquares.com>
- <http://home.hccnet.nl/s.f.boukes/fractals/fracmath.htm>
- <http://www.ibiblio.org/lifepatterns>
- <http://www.ics.uci.edu/~eppstein/recmath.html>
- <http://www.ieeta.pt/~tos/goldbach.html>
- <http://jwilson.coe.uga.edu/MATH7200/TaxiCab/TaxiCab.html>
- <http://karlscherer.com/Wireworld.html>
- <http://www.langorigami.com/science/math/hja/hja.php>
- <http://www.madras.fife.sch.uk/departments/maths/games/index.html>
- <http://magicdragon.com/EmeraldCity/Nonfiction/four9s.html>
- <http://math.berkeley.edu/~robin/Pascal/theorem.html>
- <http://www.math.cornell.edu/~mec/2006-2007/Games/hypergame.html>
- <http://www.maths.surrey.ac.uk/hosted-sites/R.Knott/Fibonacci/cfINTRO.html>
- <http://www.minortriad.com/szilassi.html>
- <http://www.nahee.com/spanky/www/fractint/lsys/spacefilling.html>
- <http://numbers.computation.free.fr/Constants/E/e.html>
- <http://www.pandd.demon.nl>
- <http://www.origamiusa.org/node/2574>
- <http://www.petrospec-technologies.com/Herkommer/goldbach.htm>
- <http://www.pi314.net>
- <http://primes.utm.edu>
- <http://www.progonos.com/furuti/MapProj>
- <http://www.quinapalus.com/wi-index.html>
- <http://www.radicaleye.com/lifepage/patterns/sbm/sbm.html>
- <http://www.relisoft.com/science/hats.html>
- <http://www.retas.de/thomas/arbels/biola>
- <http://rendell-attic.org/gol/utm/index.htm>
- <http://www.robertdickau.com>
- <http://taxicabgeometry.net>
- [http://www-user.uni-bremen.de/~schmuhl/fractals/fractal\\_curves.html](http://www-user.uni-bremen.de/~schmuhl/fractals/fractal_curves.html)

- [http://web.math.princeton.edu/math\\_alive/Voting](http://web.math.princeton.edu/math_alive/Voting)
- [http://xahlee.info/Wallpaper\\_dir/c5\\_17WallpaperGroups.html](http://xahlee.info/Wallpaper_dir/c5_17WallpaperGroups.html)

## Quotes

- <http://www.math.okstate.edu/~wli/teach/fmq.html>
- <http://www.quotegarden.com/math.html>

## Blogs, YouTubechannels

- B\_HIDE, R., <http://ravi-bhide.blogspot.be>
- COOK, J., <http://www.johndcook.com/blog>
- HART, V., <http://www.youtube.com/user/vihart> of <http://www.vihart.com>.
- JOHNSTON, N., <http://www.youtube.com/user/NathanielJohnst> of <http://www.njohnston.ca>.
- KHOVANOVA, T., <http://blog.tanyakhovanova.com>.
- NUMBERPHILE, <http://www.youtube.com/user/numberphile> of <http://www.numberphile.com>.
- TAO, T., <http://terrytao.wordpress.com>.
- VAN WOUDENBERG, A., <http://www.aswinvanwoudenberg.com>

## Artikels, papers, cursussen, presentaties

- AGRAWAL, M., KAYAL N., SAXENA, N., *PRIMES is in P.*  
Department of Computer Science & Engineering (Indian Institute of Technology Kanpur),  
06/08/2002
- ALKAUSKAS, G., *Semi-regular continued fractions and an exact formula for the moments  
of the Minkowski question mark function.* 06/12/2009
- APPEGATE, D., POL, O., SLOANE, N., *The Toothpick Sequence and Other Sequences  
from Cellular Automata.* AT&T Shannon Lab, 13/02/2010 (<http://www.research.att.com>)
- ATKINS, D., GRAFF, M., LENSTRA, A., LEYLAND, P., *The magic words are squeamish  
ossifrage.* Proceedings of the 4<sup>th</sup> International Conference on the Theory  
and Applications of Cryptology: Advances in Cryptology, 1995
- BANDERIER, C., *Fortunate and unfortunate primes: nearest primes from a prime factorial.*  
Laboratoire d'Informatique de Paris-Nord, Université de Paris, september 1999
- BEUKERS, F., *The ABC-conjecture.*  
Leiden, 09/09/2005
- CONWAY, J., *Integral Lexicographic Codes.*  
Discrete Mathematics, volume 83, 1990, p. 219
- DE BEULE, J., *Relaties en Structuren.*  
Universiteit Gent, 2012-2013
- DE CRUYENAERE, F., IGODT, P., REBRY, S., *Van priemgetal tot digitale handtekening.*  
Katholieke Universiteit Leuven (Campus Kortrijk), 2010-2011
- DELÉGLISE, M., *Bounds for the Density of Abundant Integers.*  
Experimental Mathematics, nr. 2, volume 7, 11/11/1998, p. 137  
(<http://www.emis.de/journals/EM>)
- DEMAINE, E., DEMAINE, M., MINKSY, Y., MITCHELL, J., RIVEST, R., PĂTRASCU, M.,  
*Picture-Hanging Puzzles.* 16/03/2012
- DE MEUTER, W., JONCKERS, V., *Inleiding tot de computerwetenschappen.*  
Vrije Universiteit Brussel (Software Languages Lab), 16/02/2012

- FURTNER, M., *The Kakeya Problem*.  
Ludwig-Maximiliansuniversiteit München, 02/07/2008
- GAJARDO, A., MOREIRA, A., GOLES, E., *Complexity of Langton's ant*.  
Discrete Applied Mathematics, volume 117, 2002, p. 41-50
- GHYS, E., *Un carré dans une courbe*.  
Images des Maths (CNRS), 20/03/2012 (<http://images.math.cnrs.fr>)
- HENDRIKS, D., *Fractran (guest lecture Models of Computation)*  
Vrije Universiteit Amsterdam, 31/05/2011
- HO, K., *Fibonacci numbers in nature*.  
New York University, cSplash 2011
- IANNUCCI, D, MOUJIE, D., COHEN, G., *On Perfect Totient Numbers*.  
Journal of Integer Sequences, volume 6, 2003 (<http://www.cs.uwaterloo.ca/journals/JIS>)
- IONASCU, E., WILSON, A., *On the Erdős-Straus Conjecture*.  
07/01/2010 (<http://www.arxiv.org>)
- KEENAN, D., *To Dissect a Mockingbird: A Graphical Notation for the Lambda Calculus with Animated Reduction*. 27/08/1996, <http://dkeenan.com/Lambda>
- KUSNER, R., SULLIVAN, J., *Covering the Weaire-Phelan equal volume foam to Kelvin's foam*.  
24/07/1996
- MCMULLEN, L., *How I Found the Golden Ratio on my CAS*.  
The North Carolina Association Of Advanced Placement Mathematics Teachers Newsletter, nr. 1, volume 13, 2005
- PARVARDI, A., *Lifting The Exponent Lemma (LTE)*  
The Art of Problem-Solving, 07/04/2012, <http://www.artofproblemsolving.com/Resources/articles.php>
- PEGG, ED., *Paterson's Worms revisited*.  
Mathematical Association of America, 27/10/2003 (<http://www.maa.org>)
- RABINOWITZ, S., *A Polynomial Curve of Constant Width*.  
Missouri Journal of Mathematical Sciences, nr. 1, volume 9, 1997, p. 23-27
- REITER, C., SAWYER, G., *Perfect parallelepipeds exist*.  
15/12/2009 (<http://www.arxiv.org>)
- SANDIFER, E., *A forgotten Fermat problem*.  
How Euler did it, december 2008 (<http://www.maa.org/news/howeulerdidit.html>)
- SCHNEIDER, R., *A Golden Pair of Identities in the Theory of Numbers*.  
Cornell University Library, 14/09/2011
- SEGHERS, B., *De Tijd van Hilbert*.  
Universiteit Gent, 2009-2010
- SKERRITT, M., *An Introduction to Knot Theory*.  
27/06/2003
- SLOANE, N., *Seven Staggering Sequences*.  
AT&T Shannon Lab, 03/04/2006 (<http://www.research.att.com>)
- STEVENS, G., *A Connell-Like Sequence*.  
Journal of Integer Sequences, volume 1, 1998 (<http://www.cs.uwaterloo.ca/journals/JIS>).
- THANGADURAI, R., *On the Coefficients of Cyclotomic Polynomials*.  
Institute of Mathematical Sciences, 1999
- VAN DE BULT, F., *A Slow-Growing Sequence Defined by an Unusual Recurrence*.  
Journal of Integer Sequences, volume 10, 2007 (<http://www.cs.uwaterloo.ca/journals/JIS>)
- VAN DEN BRANDHOF, A., *P = NP? Dat is de vraag*.  
Kennislink, 11/08/2009 (<http://www.kennislink.nl/publicaties>)

## Films, documentaires

- GHYS, E., LEYS, J., ALVAREZ, A., *Chaos*.
- GHYS, E., LEYS, J., ALVAREZ, A., *Dimensions*.

## Illustratieverantwoording

- Vermoeden van Andrica, blz. 23: © Krishnatej Vedala
- Collatzdiagram, blz. 29: © Jon McLoone
- Omschreven veelhoeken, blz. 85: © Brian Marks
- Cilinder, bol en kegel van Archimedes, blz. 110: © Cmglee (WikiMedia Commons)
- Schochcirkels, blz. 116: © Pbroks13 (WikiMedia Commons)
- Plant via Lindenmeyersysteem, blz. 160: © Sakurambo (WikiMedia Commons)
- Mandelbrotverzameling, blz. 164: © Adam Majewski
- Variaties op Barnsleys varen, blz. 169: © Kai Wang
- Kobondriehoeken met  $n = 17$ , blz. 199: © Johannes Bader
- Verdelingen bij de paradox van Bertrand, blz. 216: © Sakurambo (WikiMedia Commons)
- Projectie van de afgeknotte icosaeëder, blz. 231: © Guzman Tierno
- Geomagische vierkanten, blz. 243: © Lee Sallows
- Boomstructuur van surreële getallen, blz. 317: © Lukáš Lánský
- Rubik's Cube, blz. 289: © Christopher Martin
- Spaceships in RULE 110, blz. 254: © Matthew Cook
- *Primer* in de Game of Life, blz. 260: © Jason Summers
- *Sliding block memory* in de Game of Life, blz. 261: © Dean Hickerson
- *Turingmachine* in de Game of Life, blz. 262: © Paul Rendell
- *Primer* in WireWorld, blz. 267: © Mark Owen

## Dankbetuiging

- Ontwerp cover: Björn Waegebaert
- Kritische analyse: Bert Seghers
- Correcties: Stijn Cambie, Ben de Bondt, Tim Herpelinck, Bart Michels, Bert Seghers
- Inspiratie: Stijn Cambie, Ben de Bondt, Jeroen Meulewaeter, Bart Michels, Bert Seghers, An Vinckier, Johannes Weytjens, Robin Whittey, Bart Windels
- Wiskundevereniging PRIME (<http://prime.ugent.be>)

Gerendeerd met L<sup>A</sup>T<sub>E</sub>X.



$\epsilon_0$ .....	274
13-functie .....	79
15-puzzel .....	290
15-stelling .....	26
18-puntenprobleem .....	301
7 cirkels .....	146

## A

<i>abc</i> -vermoeden .....	25
Achilles (getal) .....	44
Agnesi (heks) .....	152
AKS-priemtest .....	33
Alexander	
gehoornde sfeer .....	178
veelterm .....	182
alternerende groep .....	290
alternerende permutaties .....	195
André (stelling) .....	195
Antoine (ketting) .....	185
arbelos .....	114
Archimedes	
arbelos .....	114
graf .....	109
tweelingcirkels .....	115
aritmetisch getal .....	23
Arrow (stelling) .....	307
astroïde .....	152

## B

baguenaudier .....	308
Balinski (stelling) .....	230
ballistiek .....	321
Bankoff (cirkel) .....	115
Barbier (stelling) .....	110
Barnsley (varen) .....	169
behangpatroongroepen .....	285
Beineke (stelling) .....	228
Bell (getallen) .....	194
Benford (wet) .....	217
Bernoulli (lemniscaat) .....	153
Bernstein (veeltermen) .....	319
Bertrand (paradox) .....	216
BEST (stelling) .....	234

Bézier (krommen) .....	319
Binet (formule) .....	65
Black (spel) .....	332
Blanc-mangerkromme .....	165
Blanche (dissectie) .....	99
Blaschke-Lebesgue (stelling) .....	110
Braess (paradox) .....	325
Brocard	
probleem .....	41
punten .....	106
Brouwer (stelling) .....	184
Brown (getallen) .....	41
Brun (stelling) .....	37
Buffon (naald) .....	213
Bunyakovsky (vermoeden) .....	49

## C

<i>C</i> -curve van Lévy .....	169
Calabi (driehoek) .....	124
Calkin-Wilf (boom) .....	311
Cantorstof .....	166
cardioïde .....	151
Carnot (stelling) .....	143
Cassini	
identiteit .....	65
ovalen .....	153
Catalan	
getallen .....	190
identiteit .....	65
vermoeden .....	12
Cayley	
formule .....	235
Cellérier (monster) .....	87
Cesàro (vierkant) .....	169
chaos game .....	160
Chinese ringen .....	308
Chomp .....	331
Church-Turing (hypothese) .....	276
cirkelkwadratuur .....	133
cissoïde van Diocles .....	154
Cohn (criterium) .....	49
Collatz (vermoeden) .....	29

combinatie	204	Dandelin (bollen)	120
common knowledge	271	de Bruijn	
Connell (rij)	62	stelling	207
constante		deelbaarheidsgraaf	231
Bloom-Schoenberg	137	dekpuntstelling	184
Brun	37	deltoïde	152
Conway	60	derangement	192
Euler	71	Desargues (stelling)	113
Gauss	77	Descartes	
Gelfond-Schneider	48	cirkelformule	142
Khinchin	42	folium	154
Landau-Ramanujan	14	tekenregel	47
Legendre	5	diatomische reeks	58
Liouville	50	Dilworth (stelling)	200
Mills	21	Diocles (cissoïde)	154
Niven	41	Dirac (touwtruc)	186
omgeschreven veelhoeken	84	Dirichlet	
papiergevouwen	68	principe	202
Rényi	76	dissectie	
tweelingpriemen	37	Blanche	99
Vardi	64	Duijvestijn	93
constante breedte	110	equidissectie	102
construeerbare getallen	118	Haberdasher	94
Conway		doolhof	324
\$10-000-rij	61	Douady (konijn)	165
13-functie	79	drakenkromme	162
15-stelling	26	driehoedenprobleem	213
cirkel	130	driehoek van Pascal	204
criterium	140	Duijvestijn (dissectie)	93
Fractran	314	duivenhokprincipe	202
Game of Life	255	<b>E</b>	
look-and-say	60	eenzame loper (vermoeden)	39
molentje	169	Efron (dobbelstenen)	212
monostatisch veelvlak	136	Egyptische breuken	20
pijlenketen	308	eindeloos typende apen	218
RATS	59	Eisenstein	
soldaten	301	criterium	48
surreële getallen	315	elementaire cellulaire automaat	246
tangles	175	elliptische krommen	81
veelterm	182	cryptografie	293
worm	262	groepenwet	293
Critters	264	epicycloïde	153
Cross (stelling)	147	Erdős	
Császár (veelvlak)	113	Erdős-Straus (vermoeden)	21
cycloïde	151	Erdős-Szekeres (vermoeden)	199
cyclotomische veelterm	52	zeef	12
<b>D</b>		Euclides	
Dürer (Melencolia)	241	formule	299

getal . . . . .	64
Euler	
36 officieren . . . . .	304
blok . . . . .	38
bruggen van Koningsbergen . . . . .	225
cirkel . . . . .	103
constante . . . . .	71
paardenrondgang . . . . .	241
paden en circuits . . . . .	225
rechte . . . . .	121
spiraal . . . . .	155
stelling . . . . .	24
totiëntfunctie . . . . .	10
Exeter (punt) . . . . .	121
<b>F</b>	
Fareysequenties . . . . .	13
Fermat	
halvecirkelprobleem . . . . .	101
Kerstmisstelling . . . . .	32
kleine stelling . . . . .	6
$n$ -hoeksgetalstelling . . . . .	17
priemgetallen . . . . .	36
Feuerbach (cirkel) . . . . .	103
Fibonacci	
rij . . . . .	65
folium van Descartes . . . . .	154
Ford (cirkels) . . . . .	27
Fortune (vermoeden) . . . . .	38
Fourierreeksen . . . . .	75
Freshman's dream . . . . .	8
Frieze (stelling) . . . . .	233
FTOZOM . . . . .	329
fusc-functie . . . . .	58
fyllotaxis . . . . .	317
<b>G</b>	
gömböc . . . . .	135
Gabriël (hoorn) . . . . .	78
Galton (bord) . . . . .	310
Game of Life . . . . .	255
gammafunctie . . . . .	73
Gauss	
17-hoek . . . . .	102
constante . . . . .	77
Gauss-Legende (algoritme) . . . . .	84
Gauss-Lucas (stelling) . . . . .	50
Gauss-Wantzel (stelling) . . . . .	102
lemma . . . . .	28

gebrekkige getallen . . . . .	18
Gelfond-Schneider (stelling) . . . . .	48
geluksgetal . . . . .	67
gemiddelden . . . . .	34
geomagisch vierkant . . . . .	243
Gerschgorin (theorema) . . . . .	53
Gijswijt (rij) . . . . .	60
Gods getal . . . . .	288
Goldbach (vermoeden) . . . . .	19
Golomb (rij) . . . . .	57
Goodstein (stelling) . . . . .	275
Gräffe (methode) . . . . .	50
Graham (getal) . . . . .	203
Grinberg (stelling) . . . . .	229
<b>H</b>	
Haberdasherpuzzel . . . . .	94
halting problem . . . . .	273
Hamilton (pad) . . . . .	229
happy ending problem . . . . .	199
Hardy-Littlewood (vermoeden) . . . . .	37
harmonische driehoek . . . . .	208
harmonische rij . . . . .	71
harmonisch getal van Ore . . . . .	43
Harshadgetallen . . . . .	24
Hasse (diagram) . . . . .	200
heks van Agnesi . . . . .	152
Hilbert	
axioma's . . . . .	127
hotel . . . . .	273
vlak . . . . .	127
Hippocrates (maantjes) . . . . .	119
Hofstadter	
\$10.000-rij . . . . .	61
$G$ -rij . . . . .	63
MU-puzzel . . . . .	270
Holditch (stelling) . . . . .	96
HOMFLY (veelterm) . . . . .	184
hoorn van Gabriël . . . . .	78
Hydra . . . . .	276
hyperbolische meetkunde . . . . .	128
hyperoperatie . . . . .	298
hypocycloïde . . . . .	153
<b>I</b>	
ideale driehoek . . . . .	128
intransitiviteit . . . . .	212
<b>J</b>	
Japanse cirkelstelling . . . . .	143

Jones (veelterm) . . . . .	183
Julia (verzameling) . . . . .	165
Jung (stelling) . . . . .	96
Juzuk (vierdemachten) . . . . .	12

## K

Takeya (verzameling) . . . . .	137
Kauffman (veelterm) . . . . .	183
Kelvin (vermoeden) . . . . .	139
kettingbreuk . . . . .	14
Khinchin (constante) . . . . .	42
kiessystemen . . . . .	305
Kimberling (rij) . . . . .	61
Kirchhoff (stelling) . . . . .	234
Klein	
vierdegraadskromme . . . . .	131
knopen . . . . .	179
Knuth (pijlomhoognotatie) . . . . .	298
Kobon (driehoeken) . . . . .	198
Koch (sneeuwvlak) . . . . .	162
Kolakoski (rij) . . . . .	63
Kolmogorov (0-1-wet) . . . . .	214
Kotzig (vermoeden) . . . . .	238
Kruskal (stelling) . . . . .	237
kusgetallen . . . . .	144
kwadraatvrije getallen . . . . .	6
kwadratische reciprociteit . . . . .	28
kwadratisch irrationale getallen . . . . .	82

## L

labyrint . . . . .	324
ladenprincipe . . . . .	202
Laisant (stelling) . . . . .	112
Lambdacalculus . . . . .	276
Langford (blokken) . . . . .	198
Langley (probleem) . . . . .	99
Langton (mier) . . . . .	254
Laplaciaanse matrix . . . . .	234
Legendre (symbool) . . . . .	28
Leibniz (harmonische driehoek) . . . . .	208
lemniscaat van Bernoulli . . . . .	153
Lévy ( <i>C</i> -curve) . . . . .	169
lexicode . . . . .	321
lexicografische code . . . . .	321
<i>Liber Abaci</i> . . . . .	65
lifting the exponent . . . . .	43
lijngraaf . . . . .	228
Lindenmayer	
algen . . . . .	158

L-systeem . . . . .	158
lineair schaken . . . . .	331
look-and-say . . . . .	60
Lorenz (attractor) . . . . .	85
Lucas (stelling) . . . . .	43
lucifers . . . . .	120

## M

de Méré (dobbelprobleem) . . . . .	215
magische zeshoek . . . . .	242
Main-Chowla (rij) . . . . .	62
Malfatti (probleem) . . . . .	107
Mandelbrot (verzameling) . . . . .	163
Mason-Stothers (stelling) . . . . .	47
max-flow . . . . .	236
McMullin (stelling) . . . . .	83
Melencolia . . . . .	241
Menger (spons) . . . . .	171
Midy (stelling) . . . . .	9
mier van Langton . . . . .	254
min-cut . . . . .	236
Minkowski	
metriek . . . . .	125
vraagtekenfunctie . . . . .	82
worst . . . . .	170
Mirsky (stelling) . . . . .	200
Möbius	
band . . . . .	174
inversieformule . . . . .	8
Moessner (stelling) . . . . .	36
Mohr-Mascheroni (stelling) . . . . .	118
Monge (stelling) . . . . .	127
mono-monostatisch . . . . .	135
monostatisch . . . . .	136
Monsky (stelling) . . . . .	102
Mordell-Weil (stelling) . . . . .	293
Morley (mirakel) . . . . .	101
Motzkin (getallen) . . . . .	196
N	
NAND-poorten . . . . .	272
Napoleon	
probleem . . . . .	118
stelling . . . . .	109
nefroïde . . . . .	152
negenpuntsirkel . . . . .	103
Newton	
getallen . . . . .	144
Nicomachus (stelling) . . . . .	8

Nim	332
Niven (constante)	41
Nivengetallen	24
<b>O</b>	
omschreven veelhoeken	84
onaanraakbare getallen	9
onverlichte kamer	145
ordinaalgetallen	274
Ore (harmonisch getal)	43
origami	
Huzita-Justin (axioma's)	309
Justin (stelling)	303
Kawasaki (stelling)	303
Maekawa (stelling)	303
overvloedige getallen	18
<b>P</b>	
$p$ -adische getallen	30
Pål (koppeling)	137
pannenkoekprobleem	199
papiergevouwen rij	68
Pappus	
keten	115
stelling	97
paradox	
blauwe ogen	271
Braess	325
driedeurenprobleem	212
Monty Hall	212
Parrondo	219
Sierpiński-Mazurkiewicz	315
Sint-Petersburg	217
parallellenpostulaat	128
Parrondo (paradox)	219
Pascal	
driehoek	204
slakkenlijn	154
stelling	100
passer-en-liniaalconstructies	118
Paterson (worm)	262
Peano	
kromme	166
Penrose	
onverlichte kamer	145
tegelpatroon	104
percolatie	214
perfecte getallen	18
permutatiegroepen	290

Perron (boom)	137
Phutball	330
$\pi$ -formule	
Al-Kashi	75
Gauss-Legendre	84
van Cusa	74
Wallis	78
zeef van Erdős	12
Pick (formule)	95
pizzastelling	141
Pledge (algoritme)	324
Polignac (vermoeden)	37
Pólya (vermoeden)	16
Poncelet	
Poncelet-Steiner (stelling)	118
Pong Hau K'i	330
poset	200
powerful	44
Power Tower	75
priemgetallen	
Andrica (vermoeden)	22
Bertrand (postulaat)	21
Cramér (vermoeden)	23
Fermat	36
Firoozbakht (vermoeden)	23
Gilbreath (vermoeden)	24
hiaten	21
Legendre (vermoeden)	22
Opperman (vermoeden)	23
priemgetalstelling	5
Ramanujan	22
tweelingen	37
priemknopen	181
primoriaal	38
<i>Principia Mathematica</i>	270
Proizvolov (eigenschap)	14
pronisch getal	208
Prouhet-Tarry-Escott (probleem)	11
Prüfer (sequenties)	235
Ptolemaeus (stelling)	111
P vs. NP	313
Pythagoras	
bomen	169
drietallen	299
<b>Q</b>	
quaternionen	287
quincunx	310

<b>R</b>	
random walk	220
RATS	59
Recamán (rij)	57
Reidemeister (bewegingen)	180
rekenkundige afgeleide	40
rep-tile	98
Reuleaux (driehoek)	110
Riemann	
reeksenstelling	88
Ringel (vermoeden)	238
RSA-codering	311
prins Rubert (probleem)	97
Rubik's Cube	288
Rule 110	246
Russell (paradox)	270
Russisch vermenigvuldigen	302
<b>S</b>	
sangaku	27
schaakbord	
damesdominantie	196
derangement	193
permutatie	193
Schiffler (punt)	121
schizofrene getallen	64
Schlegel (diagram)	230
Schoch (cirkels)	116
schoenveterformule	146
Schönhardt (veelvlak)	141
Schubert (stelling)	181
schuifpuzzel	290
Seifert (oppervlak)	184
Siamese methode	242
Sierpiński	
driehoek	160
tapijt	171
signatuurrij	62
slakkenlijn van Pascal	154
Soddy	
cirkelformule	142
Sophomore's dream	75
Sperner (lemma)	201
spinor	186
splines	319
Sprouts	329
Steinitz (stelling)	230
Stern (rij)	58
Stirling (formule)	7

strofoïde	153
Sturmketens	49
subfaculteit	192
surreële getallen	315
Sylvester	
rij	64
Sylvester-Gallai (stelling)	128
symmetrische groep	290
Szilassi (veelvlak)	113

<b>T</b>	
T-Square	169
Tait (vermoeden)	232
Takagi (kromme)	165
Tarski (probleem)	133
Terquem (cirkel)	103
Theodorus (spiraal)	123
Thistlethwaite (algoritme)	288
Thomae (functie)	74
Thue-Morse (rij)	58
Toeplitz (vermoeden)	122
topologische handboeien	174
tractrix	152
transpositie	290
Trémaux (algoritme)	324
Tucker (lemma)	202
Turtle Graphics	158
Tutte (graaf)	232
tweelingpriemgetallen	37

<b>U</b>	
universele koordstelling	89

<b>V</b>	
Van Aubel (stelling)	108
Van der Waerden (stelling)	201
Varignon (stelling)	134
vermoeden	
Erdős-Mollin-Walsh	44
Vicsek (sneeuwvlak)	168
vier-9's-puzzel	300
vierkleurenstelling	226
viertoppenstelling	136
Vieta (formules)	47
Vieta jumping	47
Viviani (stelling)	124
Vizing (stelling)	233
vlakvullende kromme	166
vlechtgroep	294

vlindereffect.....	85	Weierstrass (monster).....	87
vlinderstelling.....	97	wel-quasi-ordering.....	237
Voderberg (tegelpatroon).....	95	Wilson (stelling).....	7
vraagtekenfunctie.....	82	WireWorld.....	265
<b>W</b>		Wolfram (code).....	246
Wada (meer).....	186	Woo (cirkels).....	118
Wallace-Bolyai-Gerwien (stelling).....	133	<b>Z</b>	
wall following.....	324	Z-kromme.....	166
Weaire-Phelan (schuim).....	139	zigzagpermutaties.....	195

