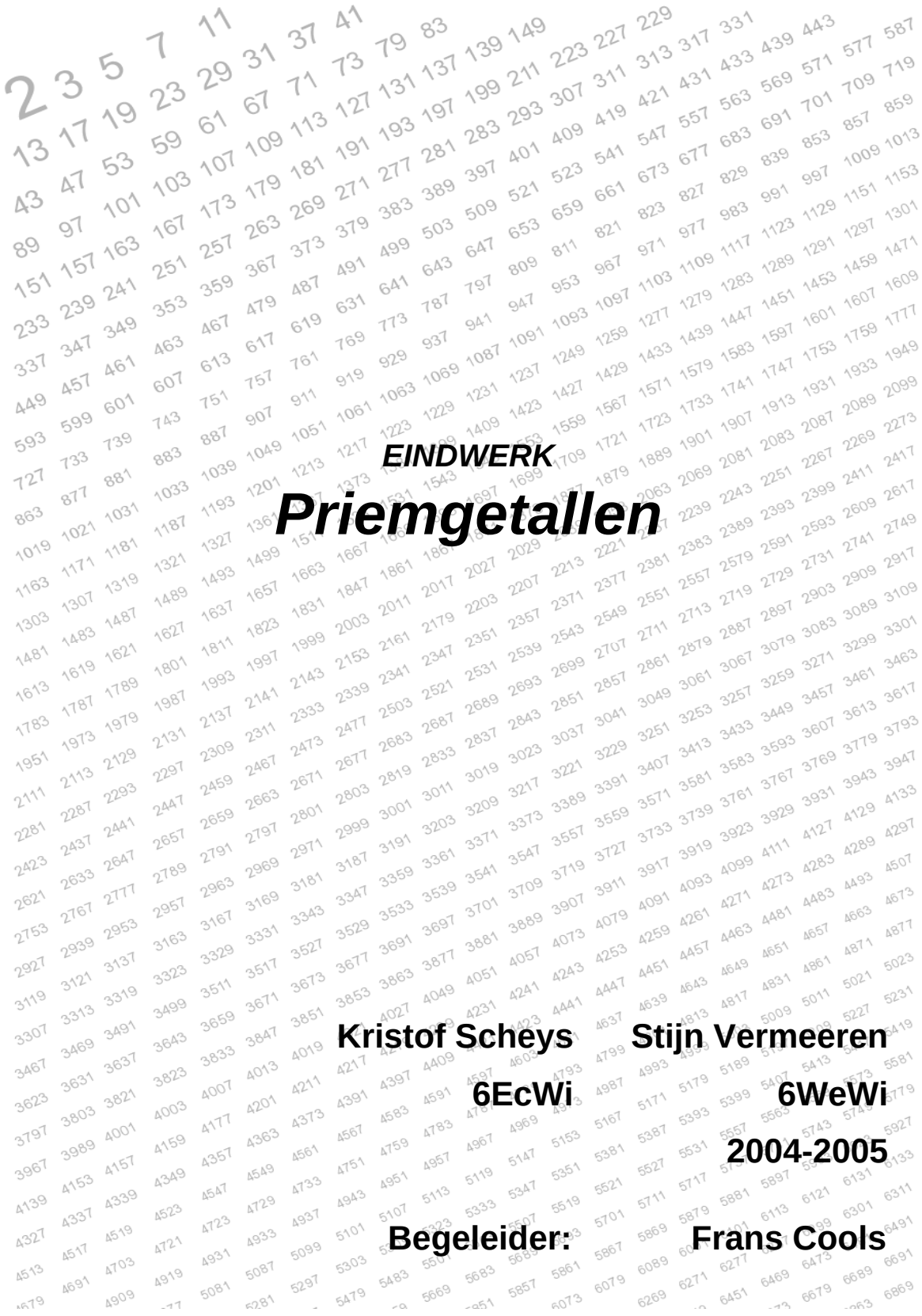
SINT-JOZEFSCOLLEGE
AARSCHOT



EINDWERK

Priemgetallen

Kristof Scheys **6EcWi**

Stijn Vermeeren **6WeWi**

2004-2005

Begeleider: **Frans Cools**

VOORWOORD

"Priemgetallen? Wat kan je daar nu over schrijven?" Deze reactie kregen we veel te horen als we het onderwerp van ons eindwerk vermeldden.

Maar een dergelijke reactie kan enkel steunen op het vooroordeel dat zuivere wiskunde niet interessant kán zijn. Wie echter, net als ons, op ontdekkingstocht gaat door priem-land, zal zijn mening moeten bijsturen. Priemgetallen hebben een zeer boeiende geschiedenis, van Euclides, over Fermat naar Woltman. Er bestaan honderden verrassende eigenschappen over priemgetallen, waarvan er ook nog vele niet bewezen zijn. Priemgetallen spelen tegenwoordig een hoofdrol in de cryptografie... Priemgetallen blijken zelfs in de natuur voor te komen bij de levenscyclus van cicaden.

In het begin van dit schooljaar kwamen wij, Kristof Scheys en Stijn Vermeeren, onafhankelijk van elkaar op de keuze 'priemgetallen' als onderwerp voor ons eindwerk. Als goede vrienden was het aanbod van onze begeleider, Frans Cools, om samen één eindwerk te maken, snel aanvaard. Tijdens de afgelopen maanden hebben we echter ontdekt dat met twee personen één verhandeling maken, meer inhoudt dan elk maar de helft van het werk doen. Je moet zorgen voor afspraken, coördinatie, organisatie en werkverdeling. Je moet zelfstandig informatie zoeken en verwerken, maar je moet ook regelmatig samenkomen om tot een goed eindproduct te komen. En je moet voortdurend de ander achter zijn veren zitten, want het is maar al te verleidelijk om te denken, 'och, hij zal dat wel doen'.

Maar we hebben samen dit eindwerk tot een goed einde gebracht. We hebben een waardevolle ervaring voor de toekomst op zak. En bovenal: moesten we er alleen voor gestaan hebben, dan zou ons eindwerk nooit even boeiend geweest zijn.

In het *eerste hoofdstuk* van dit eindwerk bekijken we de geschiedenis van de priemgetallen. Euclides vertelt ons wat priemgetallen zijn en hoeveel er zijn. Eratosthenes geeft ons een handige methode om ze te vinden. Fermat onthult ons een speciale soort priemgetallen, net als Mersenne. En dan nemen we nog eens kijkje bij de GIMPS, de organisatie die zoekt naar steeds grotere priemgetallen, een zoektocht waaraan je ook zélf kunt deelnemen.

In het *tweede hoofdstuk* bekijken we de iets lichtere kant van de priemgetallen: verbazingwekkende eigenschappen, speciale priemgetallen... Zo is er het vermoeden van Goldbach, één van de meeste beruchte problemen uit de wiskunde. Het vermoeden van Goldbach is een zeer eenvoudige stelling, maar men zoekt al meer dan 250 jaar vruchteloos naar een bewijs. Verder maken we kennis met illegale priemgetallen, sexy priemtweelingen, en de zeer spectaculaire palpriem-piramide!

Dat priemgetallen niet alleen een plezier zijn voor getaltheoretici, maar ook toepassingen hebben, zien we in *hoofdstuk drie*. Meer bepaald ontdekken we hoe bepaalde soorten cicaden (insecten) voordeel hebben bij een cyclus van een priem aantal jaar. En we ontdekken hoe we dankzij priemgetallen veilig aankopen kunnen doen op het internet.

"Priemgetallen vormen de bouwstenen van de rekenkunde. Als je een huis wilt bouwen, moet je weten welke stenen je ter beschikking hebt. Zo moet iedereen die zich bezighoudt met wiskunde, de priemgetallen goed kennen,"[(1)] zo mailde de Amerikaanse professor Chris Caldwell ons. En hoewel elke bouwsteen op zich saai lijkt, vormen alle bouwstenen samen een harmonieus geheel. Je kan er de meest verbazingwekkende huizen mee bouwen!

Wij hopen dat dit eindwerk voor iedere geïnteresseerde een boeiende ontdekkingstocht door het land van de priemgetallen is.

Kristof Scheys en **Stijn Vermeeren** - 25 februari 2005

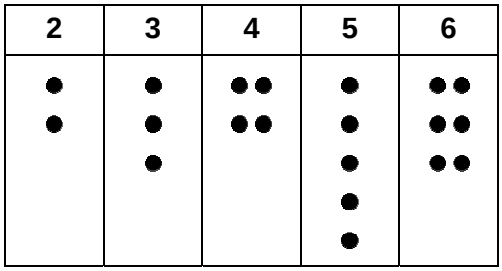
INHOUD

Hoofdstuk 1: ONEINDIG VEEL PRIEMGETALLEN

§1 – Het ontstaan van priemgetallen

De oude Griek Pythagoras is bij scholieren over heel de wereld berucht voor zijn stelling over rechthoekige driehoeken. Maar Pythagoras heeft in zijn leven nog veel meer gedaan. Rond 530 v.C. stichtte hij in Crotona (Zuid-Italië) een gemeenschap, die zich bezighield met religie, wijsbegeerte, wiskunde en politiek. De Pythagoreërs hadden een bijzondere interesse in natuurlijke getallen en hun eigenschappen. Ze geloofden dat de natuurlijke getallen en hun verhoudingen de basis waren van alle leven en van het heelal. (2)

Dankzij hun grote interesse in de natuurlijke getallen, ontdekten de Pythagoreërs al voor 400 v.C. iets bijzonders over bepaalde getallen. Stel je een getal voor door een overeenkomstig aantal steentjes, dan kunnen sommige getallen gerangschikt worden als een rechthoek. Zo kan zes gerangschikt worden als een rechthoek van twee op drie steentjes. Andere getallen kunnen echter niet gerangschikt worden als een rechthoek. Hoe je ook probeert, vijf steentjes kan je niet in een rechthoek leggen, enkel op een rechte lijn van vijf steentjes.



Figuur 1: Rechtlijnige en rechthoekige getallen

De Pythagoreërs maakten zo een onderscheid tussen rechthoekige getallen (zoals 4, 6, 8, 9, 10…) en rechtlijnige getallen (zoals 2, 3, 5, 7…). Het is waarschijnlijk geen verrassing dat de rechtlijnige getallen overeenkomen met wat wij nu priemgetallen noemen.

Een meer rekenkundig idee van priemgetallen werd ontwikkeld door de Griek Euclides. Euclides was een leraar die leefde van ca. 300 v.C. tot ca. 250 v.C. Over zijn leven is weinig bekend, maar hij was wel een van de belangrijkste wiskundigen uit de Oudheid. Zijn dertiendelig werk *De Elementen* was eeuwenlang het standaardwerk voor de meetkunde en Euclides schreef belangrijke boeken over bijna elk onderdeel van de wiskunde. (3)

Euclides introduceerde het begrip deelbaarheid in de rekenkunde. Een natuurlijk getal *d* is een deler van een natuurlijk getal a, als en slechts als $\frac{a}{d}$ een natuurlijk getal is. '*d* Is een deler van *a*' wordt in symbolisch geschreven als *d*|*a*. (4)

In symbolen:

$\forall a, d \in \mathbb{N} : d \,|\, a \Leftrightarrow (\exists q \in \mathbb{N} : d \cdot q = a)$

Tabel 1: ...is deelbaar door...

***a* =**	***d* =**	***d*|*a* =**	***d*|*a*…**
15	3	5	3|15
15	5	3	5|15
15	4	3,75	4|15 is fout
16	4	4	4|16
17	4	4.25	4|17 is fout

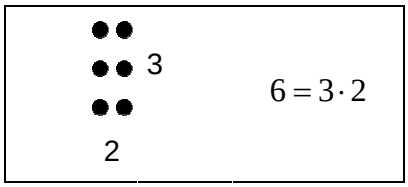
1 is een deler van elk natuurlijk getal *a*, want $1 \cdot a = a$. Elk strikt natuurlijk getal a is ook een deler van zichzelf, want $a \cdot 1 = a$.

De meeste natuurlijke getallen hebben buiten 1 en zichzelf nog andere delers. Zo heeft 15 ook de delers 3 en 5. Sommige getallen hebben echter slechts twee delers: 1 en zichzelf. Voorbeelden zijn 2, 3, 5… Deze getallen noemde Euclides de priemgetallen. Andere getallen noemde hij samengestelde getallen. Deze samengestelde getallen zijn immers het product van verschillende priemgetallen.

Maar heel belangrijk is dus de definitie van priemgetallen: *een priemgetal is een natuurlijk getal met juist twee delers (1 en zichzelf).*

§2 – Ontbinden in priemfactoren

Wat is het juiste verband tussen priemgetallen en samengestelde getallen? Daarvoor keren we eerst nog even terug naar de rechtlijnige en rechthoekige getallen. Euclides zag in dat rechtlijnige getallen de basis vormen voor de rechthoekige getallen. Elk rechthoekig getal is het product van twee andere getallen, namelijk de twee getallen die staan voor de lengtes van zijn zijden. Deze twee factoren zijn op zich weer rechthoekig, en kunnen verder gesplitst worden, of zijn rechtlijnig.



Figuur 2: Ontbinden in priemfactoren
Het rechthoekig getal 6 is het product van twee rechtlijnige getallen, namelijk de lengtes van de zijden: 2 en 3.

Zo kan je na enige tijd elk rechthoekig getal ontbinden in rechtlijnige getallen. Of anders: je kan elk samengesteld getal ontbinden in priemfactoren.

Elk rechthoekig getal is dus opgebouwd uit het product van rechtlijnige getallen. Elk natuurlijk getal is het product van priemgetallen. De priemgetallen zijn als het ware de atomen waaruit elk natuurlijk getal is opbebouwd. Daarvan komt ook de benaming ‘priemgetal’: primus komt uit het Latijn en betekent ‘eerste, belangrijkste’.

Tabel 2: Ontbinding in priemfactoren

4	$= 2^2$
6	$= 2 \cdot 3$
8	$= 2^3$
9	$= 3^2$
10	$= 2 \cdot 5$
12	$= 2^2 \cdot 3$
14	$= 2 \cdot 7$
15	$= 3 \cdot 5$
16	$= 2^4$

Maar is het nu echt voor elk natuurlijk getal mogelijk om het te ontbinden in priemfactoren? En is die ontbinding uniek? Bestaan er misschien voor eenzelfde getal meerdere mogelijke ontbindingen in priemfactoren?

Euclides bewees in zijn boek *De Elementen* dat **elk** natuurlijk op **juist één** manier kan ontbonden worden in priemfactoren, als we niet kijken naar de volgorde toch. Dit is zo essentieel dat de stelling de *hoofdstelling van de rekenkunde* genoemd wordt.

Enkele voorbeeldje:

$$\begin{aligned} 42 &= 2 \cdot 3 \cdot 7 \\ &= 3 \cdot 2 \cdot 7 \\ &= 7 \cdot 3 \cdot 2 \\ &\ldots \end{aligned}$$

Je kan de volgorde van de factoren veranderen, maar je kan 42 niet op een andere manier schrijven als het product van priemgetallen.

De hoofdstelling van de rekenkunde geeft nog extra kracht aan het beeld van priemgetallen als de atomen die alle natuurlijke getallen kunnen vormen.

§3 – Welke getallen zijn priem?

Welke getallen zijn priem? Je kan alle getallen stuk voor stuk uitproberen, door hun deelbaarheid te testen met alle getallen tussen 1 en het onderzochte getal. 2 is zeker een priemgetal. 3 is er ook een, want 3 is niet deelbaar door 2. 4 is geen priemgetal, want 4 is deelbaar door 2 ($4 = 2 \cdot 2$). 4 is dus het eerste samengestelde getal. 5 is weer een priemgetal, want 5 is niet deelbaar door 2, 3 of 4. Enzovoort. Als je nog een tijdje verdergaat, ontdek je dat 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 alle priemgetallen kleiner dan 100 zijn.

Waarom is 1 geen priemgetal? Per definitie natuurlijk: 1 heeft slechts één deler (zichzelf), en geen twee. Maar waarom is de definitie niet gewoon: ‘Een priemgetal is een natuurlijk getal dat enkel 1 en zichzelf als delers heeft’? Dit geldt wel voor 1. De belangrijkste reden om 1 toch niet als priemgetal te beschouwen, is dat de hoofdstelling van de rekenkunde niet meer zou gelden met 1 als priemgetal. Door naar believen 1’tjes toe te voegen, kan een natuurlijk getal immers op oneindig veel manieren geschreven worden als het product van priemgetallen.

$$\begin{aligned} 42 &= 2 \cdot 3 \cdot 7 \\ &= 1 \cdot 2 \cdot 3 \cdot 7 \\ &= 1^2 \cdot 2 \cdot 3 \cdot 7 \\ &\ldots \end{aligned}$$

De hoofdstelling van de rekenkunde is echter veel te belangrijk om te laten vallen. (5)

Alle getallen uittesten op hun deelbaarheid om priemgetallen te vinden is 'vrij omslachtig'. Daarom zou het interessant zijn om te weten of er een patroon in de lijst van priemgetallen te herkennen is. Kunnen we een formule opstellen die alle priemgetallen geeft? Of is er een formule die ons snel veel priemgetallen oplevert? De 18de-eeuwse wiskundige Leonard Euler vond de formule f(x) = $x^2 + x + 41$. Voor $x \in (0,1,2,...,39)$ zijn alle f(x) priem. Maar f(41) is geen priemgetal, want

$$\begin{aligned} f(41) &= 41^2 + 41 + 41 \\ &= 41 \cdot (41 + 1 + 1) \\ &= 41 \cdot 43 \end{aligned}$$

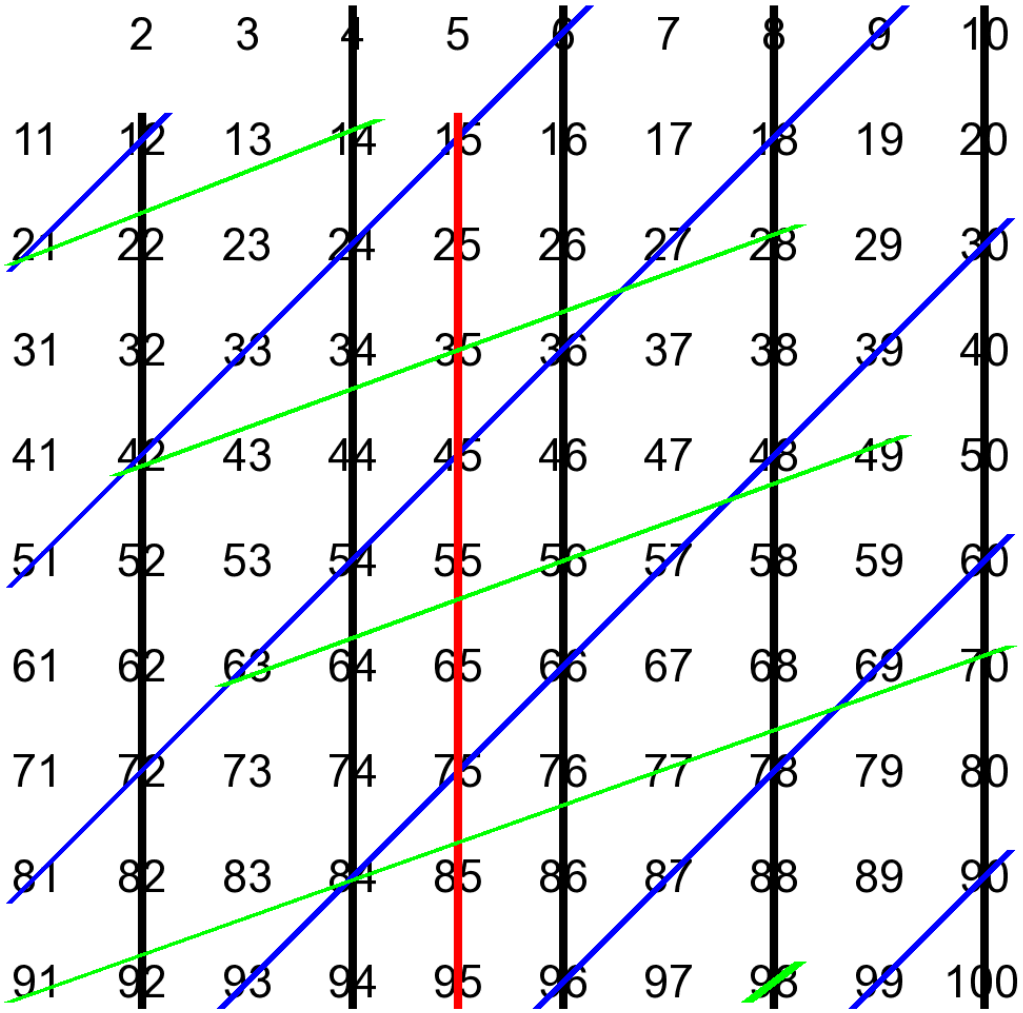
f(41) is dus samengesteld. Ook f(40) is geen priemgetal, want

$$\begin{aligned} f(40) &= 40^2 + 40 + 41 \\ &= 40 \cdot (40 + 1) + 41 \\ &= 40 \cdot 41 + 41 \\ &= 41 \cdot (40 + 1) \\ &= 41^2 \end{aligned}$$

Tot op heden is er geen enkele goede formule voor priemgetallen gevonden.

Dat priemgetallen zo onregelmatig verdeeld zijn, maakt hen moeilijker, maar ook interessanter. Want hoe kan je nu snel veel priemgetallen vinden? De Griek Eratosthenes vond al rond 200 v.C. een handige methode hiervoor.

- Willen we alle priemgetallen tot en met 100 kennen, schrijven we eerst alle getallen van 2 tot en met 100 neer.
- Dan nemen we het eerste getal, 2, en doorstrepen we alle veelvouden van dit getal, groter dan het getal zelf. We doorstrepen dus 4, 6, 8… Dit zijn allemaal samengestelde getallen.
- We nemen nu het volgende, nog niet doorstreepte getal, 3, en doorstrepen alle veelvouden van 3.
- 4 is reeds doorstreept, dus vier kunnen we overslagen.
- Nu doorstrepen we alle veelvouden van 5, dan alle veelvouden van 7 en dan…



Figuur 3: Zeef van Eratosthenes

En dan mogen we stoppen! Het mooie aan deze methode, de *zeef van Eratosthenes*, is dat je om alle priemgetallen tot en met *n* te kennen, niet tot en met *n* moet doorstrepen, maar slechts tot en met $\sqrt{n}$!

We bewijzen dit uit het ongerijmde. [6] Stel dat er toch een samengesteld getal $x \leq 100$ nog niet doorstreept is. Omdat *x* samengesteld is, geldt $x = a \cdot b$, met $a \leq \sqrt{100}$ of $b \leq \sqrt{100}$. (Als *a* en *b* beide groter zijn dan $\sqrt{100}$, is $a \cdot b = x$ immers groter $\left(\sqrt{100}\right)^2 = 100$.) *x* is dus een veelvoud van een getal kleiner dan $\sqrt{100}$, maar al deze veelvouden hebben we doorstreept! Elk niet doorstreept getal kleiner dan 100 kan dus niet samengesteld zijn, en moet een priemgetal zijn!

§4 – Hoeveel priemgetallen zijn er?

Dat er veel priemgetallen zijn is wel duidelijk, maar hoeveel juist? Je kan ze proberen allemaal te tellen, door elk getal te controleren op zijn deelbaarheid of door de zeef van Eratosthenes te gebruiken. Maar dan ben je wel een tijdje bezig. Er zijn oneindig veel natuurlijke getallen, dus om elk getal te controleren ben je ook oneindig lang bezig. Je kan priemgetallen wel tellen, maar je kan er nooit zeker van zijn dat een bepaald priemgetal het laatste is. Daarvoor moet je alle (oneindig veel) getallen die groter zijn dan dat priemgetal controleren…

Er is dus een andere, algemenere methode nodig om het aantal priemgetallen te bepalen. Dit werd voor het eerst gedaan door Euclides, weeral in zijn boek *De Elementen*. Maar Euclides gaf tot ieders verbazing echter niet het aantal priemgetallen. Euclides bewees dat er geen grootste priemgetal bestaat, met andere woorden dat er oneindig veel priemgetallen bestaan! Euclides' bewijs hiervoor is een pareltje van de elegantie van de wiskunde, en is vandaag nog steeds een van de meest beroemde bewijzen.

Euclides maakt gebruik van een bewijs uit het ongerijmde. Hij stelt eerst dat er wél een eindig aantal priemgetallen is. We maken eerst een lijst van al die priemgetallen: 2, 3, 5, …, *p*. Vermenigvuldig dan al deze priemgetallen. Het product $N = 2 \cdot 3 \cdot 5 \cdot ... \cdot p$ is een eindig getal dat deelbaar is door elk priemgetal in de lijst. Beschouw dan nu het getal *N*+1.

- *N*+1 is niet deelbaar door 2, want *N* is deelbaar door 2. Als je *N*+1 deelt door 2 heb je sowieso een rest van 1.
- *N*+1 is ook niet deelbaar door 3, ook hier heb je weer een rest van 1.
- *N*+1 is ook niet deelbaar door 5, 7, …, *p*, telkens om dezelfde reden.

N+1 is dus een getal dat ofwel zelf priem is, ofwel deelbaar is door een priemgetal dat niet in onze lijst 2, 3, 5, …, *p* zit. Oei: onze lijst van alle priemgetallen blijkt toch niet alle priemgetallen te bevatten. We hebben dus een tegenstrijdigheid ontdekt. Hoe groot je je lijst van priemgetallen ook maakt, ze is nooit volledig. Er is dus geen grootste priemgetal… het aantal priemgetallen is oneindig!

Het moet wel gezegd worden dat Euclides zijn bewijs niet op deze manier gaf. Ten eerste hadden de oude Grieken nog niet ons abstract idee van getallen, maar beschouwden getallen als de lengte van lijnstukken. Euclides beschouwde in zijn bewijs dus niet getallen op zich, maar werkte met lijnstukken van een bepaalde lengte. Ten tweede had men toen ook nog niet ons huidig begrip van oneindigheid. In plaats van te stellen dat er oneindig veel priemgetallen bestaan, schreef Euclides dus dat er meer priemgetallen waren dan eender welk aantal dat men kon beschouwen. Ten derde werkte Euclides eigenlijk met een voorbeeld, in plaats van het algemeen geval te beschouwen. Een voorbeeld levert natuurlijk niet het wiskundig bewijs, maar het is wel duidelijk dat Euclides ook de achterliggende algemene gedachte volledig begreep. [(7)]

Dat er een oneindig aantal priemgetallen bestaat, maakt de priemgetallen een moeilijker, maar ook veel interessanter begrip. Moest er slechts een eindig aantal priemgetallen bestaan, zouden we ze allemaal kunnen opschrijven, al hun eigenschappen onderzoeken, en dat was het dan. Maar er bestaan oneindig veel priemgetallen! Dit betekent dat we steeds grotere priemgetallen en steeds nieuwe interessante eigenschappen kunnen ontdekken, zonder dat er ooit een eind aan komt! Over de zoektocht naar steeds grotere priemgetallen zullen we het in de volgende paragrafen hebben. Over de vele leuke, verrassende en interessante eigenschappen van priemgetallen gaat hoofstuk twee.

§5 – Fermat-getallen, Pepins test

Pierre de Fermat was de 17de-eeuwse zoon van een lederwarenverkoper. Hij was advocaat en magistraat, en had beroepshalve weinig te maken met wiskunde. In zijn vrije tijd maakte hij echter veel belangrijke wiskundige ontdekkingen, daarom wordt hij vaak de 'Prince of Amateurs' genoemd. Hij publiceerde slechts één belangrijk manuscript in zijn leven, en dan nog niet onder zijn echte naam. Maar hij correspondeerde veel met wiskundigen. Fermat was één van de stichters van de analytische meetkunde, hij kwam samen met Pascal tot de theorie van kansberekening, en hij hielp de fundamenten voor het rekenen leggen. Maar zijn echte liefde ging uit naar de getaltheorie. (8)

Fermat stelde dat elk getal van de vorm $F_n = 2^{2^n} + 1$ een priemgetal is. De eerste vijf Fermat-getallen zijn inderdaad allemaal Fermat-*priem*getallen:

$F_0 = 3$
$F_1 = 5$
$F_2 = 17$
$F_3 = 257$
$F_4 = 65537$

In 1732 ontdekte Euler echter dat F_5 kan gedeeld worden door 641. Je hebt slechts twee proefdelingen nodig om deze factor te vinden omdat Euler aantoonde dat elke deler van een Fermat-getal F_n met $n > 2$ de vorm $2^{n+2} \cdot k + 1$ heeft. In het geval van F_5 is dit $128 \cdot k + 1$, zodat we 257 en 641 zouden proberen (want 129, 385 en 513 zijn niet priem).

Nu weten we dat alle Fermat-getallen samengesteld zijn voor $n \in [5,30]$. Waarschijnlijk zijn de eerste vijf Fermat-getallen ook de enige Fermat-*priem*getallen, maar dat is nog niet bewezen.

De snelste manier om om aan te tonen of een Fermat-getal al dan niet priem is, als proefdelen niet lukt om een kleine factor te vinden, is gebruik te maken van Pepin's test. Deze methode werd in 1877 bewezen door Pepin.

Pepin' s test: F_n is priem als en slechts als de rest van de deling van $3^{\frac{Fn-1}{2}}$ door F_n gelijk is aan F_n-1**.** [9][10]

Als F_n priem is, kan door Pepin's test worden aangetoond dat F_n priem is, maar wanneer F_n een samengesteld getal is vertelt Pepin's test ons niet wat de factoren zullen zijn. Dan vertelt de test ons alleen dat het geen priemgetal is. Een voorbeeldje: Selfridge en Hurwitz toonden in 1963 aan dat F_{14} geen priemgetal is, maar we kennen nog steeds geen van de delers van dat getal.

Kunnen we met deze test nu van alle Fermat-getallen, hoe groot ook, testen of het priemgetallen zijn? Helaas niet, er is namelijk een praktisch probleem. Het getal $3^{\frac{Fn-1}{2}}$ dat gebruikt wordt in de test, wordt al snel enorm groot. Voor $F_3 = 257$ bestaat $3^{\frac{Fn-1}{2}}$ al uit 61 cijfers! Zelf de modernste computers moeten het opgeven als de getallen nog groter worden.

§6 – Mersenne-getallen, de Lucas-Lehmer-test

Marin Mersenne, die leefde van 1588 tot 1648, ging naar school in het College de Mans. Daarna, vanaf 1604, spendeerde hij vijf jaar in het Jezuietencollege in La Fleche. Van 1609 tot 1611 studeerde hij theologie in Sorbonne. Mersenne sloot zich aan bij de godsdienstige orde van de Minims in 1611. De naam van de orde is ontstaan omdat dat de Minims zichzelf beschouwden als de minsten van alle religies. Zij wijdden zich enkel aan gebed en studie. In 1612 werd hij priester op de Place Royale in Parijs. Hij onderwees filosofie aan het Minim klooster in Nevers van 1614 tot 1618. In 1619 keerde hij terug naar de Minims in Parijs. Zijn afdeling daar werd een vergaderplaats voor Fermat, Pascal, Gassendi, Roberval, Beaugrand en anderen die later de kern van de Franse Academie van Wetenschappen werden. Mersenne correspondeerde met andere belangrijke wiskundigen en hij speelde een belangrijke rol in het overbrengen van wiskundige kennis in heel Europa. Toen waren er immers nog geen wetenschappelijke tijdschriften. [11]

Mersenne onderzocht priemgetallen en hij probeerde een formule te vinden waaruit men alle priemgetallen kon vinden. Hij is hier niet in geslaagd, maar hij heeft wel belangrijk werk verricht aangaande priemgetallen van een bepaalde vorm. Deze getallen noemt met tegenwoordig Mersenne-getallen. Ze hebben allemaal de volgende vorm:

$M_p = 2^p - 1$ (p is priem)

Enkele kleine voorbeelden:

$M_2 = 3$
$M_3 = 7$
$M_5 = 31$
$M_7 = 127$
…

Tot nu toe heeft men 41 Mersenne-getallen gevonden die priem zijn. Het 41ste is $2^{24,036,583}$-1. Dit getal bestaat uit maar liefst 7.235.733 cijfers! Over dergelijke 'priemreuzen' zullen we het in de volgende paragraaf nog uitgebreid hebben.

Maar hoe weet je of een Mersenne-getal priem is? Hiervoor gebruikt men de Lucas-Lehmer test.

Lucas-Lehmer test: Als p een priemgetal (groter dan 2) is, is het Mersenne-getal 2^p-1 priem als en slechts als S(p-1) deelbaar is door 2^p-1, waarbij S(n+1) = S(n)^2-2 en S(1) = 4. (12)

De theorie voor de test is uitgevonden door Lucas rond 1870. Lehmer heeft de test vereenvoudigd, tot de hierboven vermelde test, rond 1930.

Om de test te verduidelijken, geven we een voorbeeldje voor een heel klein Mersenne-getal. Als we willen weten of $M_3 = 7$ priem is, dan zoeken we dus eerst S(2).

S(2) = S(1)²-2
= 4²-2
= 16-2
= 14

Dan controleren we of 14 deelbaar is door 2^p-1 = 7, en dat is natuurlijk waar. Dus $M_3 = 7$ is inderdaad priem!

Voor heel grote Mersenne-getallen geldt bij de Lucas-Lehmer test opnieuw hetzelfde probleem als bij Pepins test: zelfs moderne computer kunnen niet goed overweg met zulke grote getallen. Daarom blijft het een uitdaging om steeds grotere priemgetallen proberen te vinden. En daarover gaat dan ook de volgende paragraaf.

§7 – Zoeken naar steeds grotere priemgetallen

Al sinds Euclides het begrip priemgetallen definieerde, lijkt het wel een wedstrijd om steeds grotere priemgetallen te ontdekken. In 1588 stond het record op 2^{19}-1, een 6-cijferig priemgetal dat met gewone, primitieve proefdelingen ontdekt was door Cataldi. Met meer geavanceerde wiskundige stellingen kon Lucas (een van de ontdekkers van de eerder vernoemde Lucas-Lehmer-test) in 1876 bewijzen dat 2^{127}-1, een getal van 39 cijfers, priem was. Sinds de intrede van computers in de tweede helft van de vorige eeuw, gaat het vinden van priemgetallen veel sneller. Het grootst bekende priemgetal (op 25 februari 2004) bestaat uit meer dan 7 miljoen cijfers!

Dat het zoeken naar grote priemgetallen al lange tijd belangrijk is, daarvan getuigt deze speciale poststempel. Het wiskunde-departement van de Universiteit van Illinois was zo trots op de ontdekking van het nieuwe Mersenne-priemgetal 2^{11213}-1 in 1963, dat ze deze speciale stempel lieten maken! (13)

Wil je zelf zoeken naar hele grote priemgetallen, is het handig om met Mersenne-getallen te werken. Van getallen in de vorm $M_p = 2^p - 1$ (p is priem) is namelijk bekend dat er vele grote priemgetallen tussen zitten. Verder is het handig om gebruik te maken van Fermats kleine stelling. Zoals we dadelijk zullen zien, kan je dan snel vele getallen elimineren die zeker samengesteld zijn.

Fermats kleine stelling: Als het priemgetal *p* geen deler is van *a*, dan heeft $\frac{a^{p-1}}{p}$ een rest van 1. (14)(15)

Stel nu dat je een bepaald getal *a* hebt. Als je dan een priemgetal *p* kunt vinden waarvoor $\frac{a^{p-1}}{p}$ *niet* rest 1 levert, dan is *a* deelbaar door *p* en dus samengesteld! Deze test is heel snel uit te voeren met moderne computers, ook voor grote getallen. Van de meeste getallen kunnen we door Fermats kleine stelling toe te passen, heel snel zeggen dat ze samengesteld zijn. Helaas werkt de test niet in de andere richting. Stel dat Fermats kleine stelling telkens een rest van 1 oplevert voor *a*, dan kunnen we nog niet zeggen dat *a* priem is. We moeten nog eerst *a* volledig controleren op zijn deelbaarheid, een proces dat wel een tijdje duurt.

Maar door Fermats kleine stelling kunnen we al meteen een hele hoop getallen elimineren, getallen die zeker samengesteld zijn. De andere getallen, 'kandidaat-priemgetallen', moeten nog volledig op hun deelbaarheid gecontroleerd worden.

De GIMPS, de Great Internet Mersenne Prime Search, werkt op die manier. Van Mersenne-getallen wordt eerst onderzocht of het 'kandidaat-priemgetallen' zijn, zo ja wordt er uitgebreid gecontroleerd of het getal ook echt priem is.

Het leuke aan de GIMPS is dat je er zelf aan kunt deelnemen. De berekeningen voor het zoeken naar nieuwe priemgetallen worden namelijk niet op één centrale computer uitgevoerd, maar men gebruikt de rekenkracht van duizenden computers van liefhebbers over de hele wereld. Je kan zelf deelnemen, door van de site van de GIMPS (*http://www.mersenne.org*) een programma te downloaden dat op jouw computer mee zoekt achter een nieuw Mersenne-priemgetal. Als je héél veel geluk hebt, en je vindt een nieuw priemgetal, dan wordt de server verwittigd. Dan krijg je ook een geluid te horen, zodat je weet dat je het volgende grote priemgetal ontdekt hebt! En dan kan je beginnen met een groot feestje te bouwen.

Sinds zijn onstaan in 1995 heeft de GIMPS zeven nieuwe Mersenne-priemgetallen ontdekt. De vier grootst gekende priemgetallen van het moment zijn allemaal door de GIMPS ontdekt. Het grootste, $2^{24,036,583}-1$, een getal van meer dan 7 miljoen cijfers en het 41^{ste} gekende Mersenne-priemgetal, werd in maart 2004 ontdekt.

Waarom zoekt men eigenlijk naar zo'n grote priemgetallen? Er zijn er toch oneindig veel, de zoektocht houdt nooit op.

Maar er zijn natuurlijk heel wat redenen om toch op zoek te gaan naar grote priemgetallen:

1. Traditie
2. Roem
3. De hardware van een pc testen
4. Men verzamelt graag mooie en zeldzame dingen
5. Meer leren over priemgetallen

...

George Woltman, de oprichter van de GIMPS, verwoordde het als volgt: "Het is zoals de Mount Everest beklimmen. Je doet het voor het plezier en de uitdaging!" (16)

Hoofdstuk 2: VERRASSENDE EIGENSCHAPPEN

§1 – Het vermoeden van Goldbach

Er zijn heel wat stellingen over priemgetallen, zowel eenvoudige stellingen als stellingen die alleen beroepswiskundigen kunnen begrijpen. Ook zijn sommige van deze stellingen nog steeds niet bewezen, we spreken dan van een ‘vermoeden’. Om het boeiend te houden, zullen we in dit eindwerk de meeste stellingen over priemgetallen links laten liggen. Maar het vermoeden van Goldbach, de meest beruchte van alle stellingen, verdient wel een eigen paragraaf.

De Duitse wiskundige Christian Goldbach leefde van 1690 tot 1764. Hij werd geboren in Königsberg in het toenmalige Pruisen[17]. Hij studeerde aanvankelijk Rechten, maar was vooral geboeid door de getaltheorie. Goldbach was zo sterk dat hij werd aangesteld als persoonlijke leraar van de aanstaande tsaar Peter II in Moskou. Dit gaf hem de mogelijkheid om veel te reizen, waardoor hij in contact kwam met de verschillende belangrijke wiskundigen uit zijn tijd. Zo hield hij uitgebreide briefwisselingen met onder andere Leibniz, Daniel Bernoulli en Leonard Euler. [18]

In de marge van een van zijn brieven aan Euler, pende Goldbach op 7 juni 1742 het volgende zinnetje neer: “Het lijkt erop dat elk getal groter dan twee kan geschreven worden als de som van drie priemgetallen.” [19] *(Een ingescande versie van de brief vind je in bijlage 1.)* Goldbach beschouwde 1 overigens als een priemgetal.

Euler verwoordde de stelling in een iets vereenvoudigde, maar evenwaardige vorm, die later bekend zou worden als het vermoeden van Goldbach.

Vermoeden van Goldbach: Elk even getal groter dan twee is de som van twee priemgetallen.

Enkele kleine voorbeelden:

4 = 2 + 2
6 = 3 + 3
8 = 3 + 5
10 = 3 + 7 = 5 + 5
12 = 5 + 7
14 = 3 + 11 = 7 + 7
...

Hierbij valt het op het dat sommige getallen ook op verschillende manieren kunnen geschreven worden als de som van twee priemgetallen. Meer nog: voor de meeste getallen geldt: hoe groter het getal, hoe groter het aantal correcte paren priemgetallen. Zo kan 10.000 al op 127 manieren geschreven worden als de som van twee priemgetallen!

Maar dat volstaat natuurlijk nog niet als bewijs. Euler antwoordde aan Goldbach hij de stelling als waar beschouwde, hoewel hij niet in staat was om het te bewijzen. En daarvoor moet Euler zich niet schamen. Zelfs meer dan 250 jaar nadat Goldbach zijn brief schreef, blijft deze vraag nog steeds onopgelost! Het vermoeden van Goldbach is een verbazingwekkend eenvoudig probleem, maar niemand heeft ooit een bewijs of tegenbewijs gevonden.

Omdat het probleem zo eenvoudig is, maar toch zo ondoordringbaar, oefent het vermoeden van Goldbach een grote aantrekkingskracht uit op iedereen die graag bezig is met getaltheorie. Zo schreef de Griek Apostolos Doxiados in 2000 een leuk, fictief boek over een man die zijn hele leven tevergeefs zocht naar een bewijs voor het vermoeden, getiteld *Oom Petros en het vermoeden van Goldbach*. Om publiciteit te maken voor het boek, beloofde de Britse uitgever Tony Faber een beloning van een miljoen dollar aan wie het vermoeden voor april 2002 kon bewijzen. De prijs werd natuurlijk nooit opgeëisd.

Dat het vermoeden van Goldbach nog niet bewezen werd, betekent niet dat er geen belangrijke ontdekkingen zijn gedaan. In 1939 bewees Schnirelmann dat elk even getal, groter dan 2, geschreven kan worden als de som van ten hoogste 300.000 priemgetallen. Het is dus niet mogelijk dat als je steeds grotere even getallen neemt, er steeds meer priemgetallen nodig zijn om ze weer te geven. Een som van 300.000 priemgetallen of minder volstaat steeds. Sindsdien is dit resultaat een aantal keer verbeterd. Het beste resultaat staat op naam van Olivier Ramaré. Hij bewees in 1995 dat een som van maximum zeven priemgetallen steeds voldoende is. Maar een echt bewijs is nog niet in zicht.

Een bekende variatie op het vermoeden van Goldbach is het zogenaamde *oneven* vermoeden van Goldbach.

Oneven vermoeden van Goldbach: Elk oneven getal groter dan 5 is de som van drie priemgetallen.

Het *oneven* vermoeden van Goldbach volgt uit het gewone vermoeden van Goldbach. Als het vermoeden van Goldbach waar is, kunnen we met een som van twee priemgetallen elk even getal (>2) bekomen. Door aan die som nog eens het (priem)getal 3 toe te voegen kunnen we dus ook elk oneven getal (>5) bekomen. Het omgekeerde is echter niet geldig: het oorspronkelijke vermoeden van Goldbach volgt *niet* uit het *oneven* vermoeden van Goldbach.

Het *oneven* vermoeden van Goldbach is dus in feite een zwakkere versie van het vermoeden van Goldbach. Het *oneven* vermoeden is ook nog steeds onbewezen, maar staat wel al een pak dichter bij een bewijs. Zo bewees Ivan Vinogradov in 1937 dat elk voldoende groot getal kan geschreven worden als de som van drie priemgetallen, hoewel hij niet in staat was te zeggen wat 'voldoende groot' juist was. Zijn student Borodzin slaagde daar wel in: hij bewees dat elk getal groter dan $3^{3^{15}}$ 'voldoende groot' was. Deze grens is sindsdien meerdere keren verlaagd, en staat sinds 1989 op 10^{43000}. Er moet dus nog maar een eindig aantal getallen gecontroleerd worden om het *oneven* vermoeden van Goldbach te bewijzen, maar dit aantal is nog steeds veel te groot voor de modernste computers.

§2 – Illegale priemgetallen

Een DVD kan veel meer informatie opslagen dan een CD. Daarom slaat men op een DVD ook vaak films op. Om te voorkomen dat DVD's afgespeeld worden op een machine die er niet voor gemaakt is, worden DVD's gecodeerd, zodat alleen DVD-spelers de DVD kunnen afspelen.

Maar al snel verscheen er code op het internet om DVD's te decoderen (ontcijferen). De beroemdste hiervan is DeCSS. Deze code werd op 6 oktober 1999 anoniem gepubliceerd. Natuurlijk waren de filmproducenten hier niet mee akkoord. Ze spanden een rechtszaak aan om de verspreiding van de DeCSS-code te verbieden. Dit heeft onder meer betrekking op een bedrijf dat T-shirts produceerde waarop de code gedrukt was.

Men stelde zich de vraag of een verbod op het verspreiden van de code niet in strijd was met het recht op vrije meningsuiting. Maar de rechter die de rechtszaak leidde vond van niet en verbood de verdere verspreiding van de code. En dat terwijl in twee andere zaken die hier niets mee te maken hadden, de rechters beslisten dat de code van een bepaald programma wel nog mocht verspreid worden omdat het anders een belemmering was voor de vrije meningsuiting. Hieruit kun je dus afleiden dat er nog veel onenigheid over is.

Als het verboden is de code te verspreiden, maar het is nog steeds toegestaan een tekstuele beschrijving van de code te verspreiden, waar moet men dan de grens trekken?

Uit het protest tegen het vonnis, doken er op het internet al snel vele versies van de code op, zij het in verborgen vorm. Deze kunst om een geheime boodschap te verstoppen, noemt men steganografie. Dit zullen we nu illustreren met twee ingenieuze voorbeelden [(20)].

Voorbeeld 1:

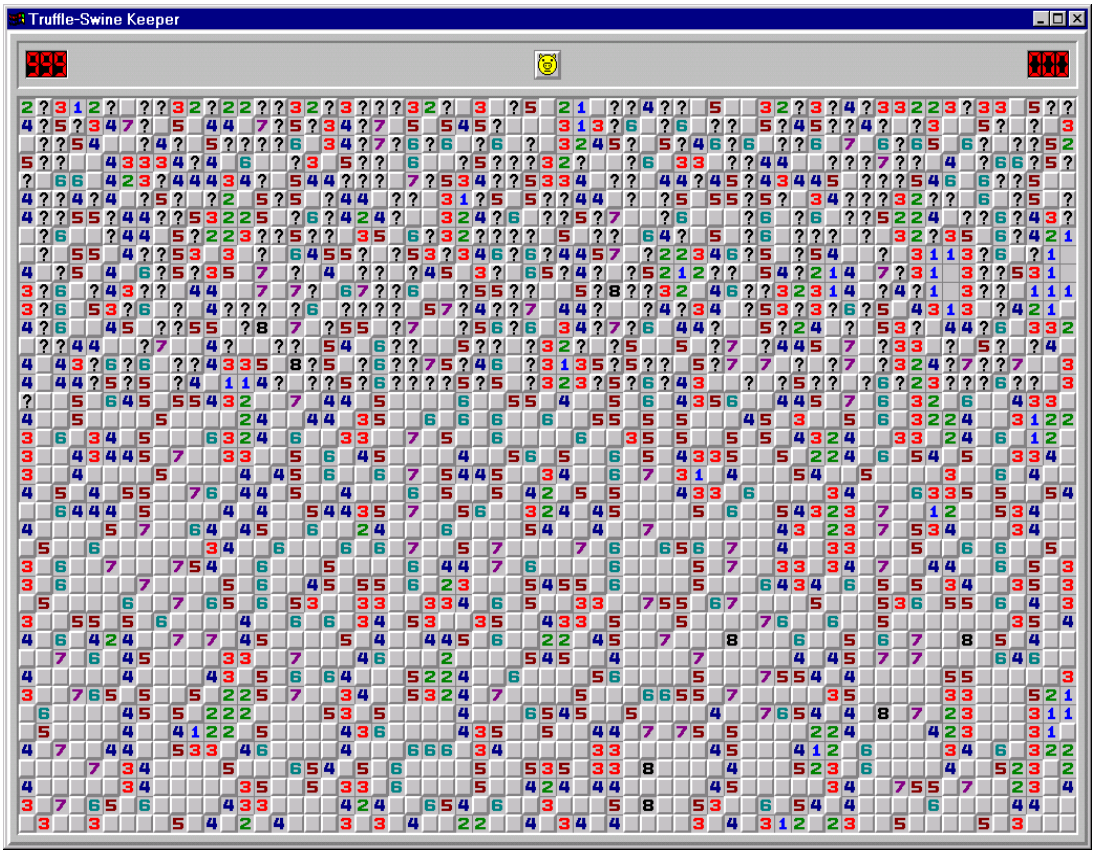
Joerg Dietrich kreeg het idee dat de code misschien wel in ons DNA verstopt kan zijn. DNA bestaat uit een lange reeks bases die voorgesteld worden met de letters A, C, G en T. Zo'n tekenreeks kan je omzetten in een computer-code. Hier een stuk DNA-structuur die een deel van de DeCSS-code bevat:

```
AGTT AGGG AGAA AAGG AGAA AGGG AGAA AGAA CGAT CTAT CTAT CCTT CGCA CGCC CTAT
CGAT CTAG CGAC CGTC CGAG CGTA CGCC AGTG CGAT AAGG AGAA AGGG AAGG AGAA AGGG
AGAA AGAA CCAG CGCC CGTA CGCC CGAC CTAT CGCC CGCA AGAA CTCC CGTG CGCA CGCC
CTAG AGAA CTCA CGGA CGCC AGAA CTCG CGCC CTAG CTAT CGGC CGTT CGTG AGAA ATAG
AGAA CGTT CGCG AGAA CTCA CGGA CGCC AGAA CACT CCAA CATA AGTG AAGG AGAA AGGG
AAGG AGAA AGGG AGAA AGAA CAAT CGTT CTAA CTGC CTAG CGGC CGCT CGGA CTCA AGAA
ATAC ATGC ATGC ATGC AGAA CACA CGCC CTAG CGCC CGGT AGAA CACG CGAC CTCT CGAT
CTCC CTAT AAGG AGAA AGGG AAGG AGAA AGGG AGAA AGAA CCCA CGGA CGGC CTAT AGAA
CGCG CGGC CGTA CGCC AGAA CGAT CGTT CGTG ...
```

Joerg Dietrich maakte hierbij de volgende bedenking: "Stel dat iemand erin slaagt om deze volgorde te vinden in het DNA van de mens. Dan zouden er meer dan zes miljard mensen op de aarde zijn die de wet breken!" (21)

Voorbeeld 2:

Iedereen kent wel het computerspelletje mijnenveger. Iemand die zichzelf “Blat Froop” noemt, ontwierp wel een erg bijzonder mijnenveld. Het spelbord is 63 op 40 vakjes groot. Je moet de plaatsen van alle mijnen zoeken. De vakjes waar de mijnen liggen stellen 1’en van de computercode voor, en de vakjes die reeds onthuld zijn de 0’en. De rest van de code wordt gevormd door de vraagtekens.



Heel ingenieus! Een simpel spelletje mijnenveger kan toch niet illegaal zijn?

Wat heeft dit nu te maken met priemgetallen? Op het eerste zicht niets. Maar alles wat op een computer wordt opgeslagen, wordt binair opgeslagen. De DeCSS-code is dus gewoon een getal.

Dan kwam Phil Carmody opdagen. Hij besloot om van de DeCSS-code een versie te maken die een priemgetal was. Hierbij vertrok hij van de originele anonieme code die hij omvormde tot een kortere code. In maart 2001 werd zo het eerste illegale priemgetal ontdekt door Carmody. [(22)]

Dit was het bewuste getal:

```
                                                4 8565078965 7397829309
8418946942 8613770744 2087351357 9240196520 7366869851 3401047237
4469687974 3992611751 0973777701 0274475280 4905883138 4037549709
9879096539 5522701171 2157025974 6669932402 2683459661 9606034851
7424977358 4685188556 7457025712 5474999648 2194184655 7100841190
8625971694 7970799152 0048667099 7592359606 1320725973 7979936188
6063169144 7358830024 5336972781 8139147979 5551339994 9394882899
8469178361 0018259789 0103160196 1835034344 8956870538 4520853804
5842415654 8248893338 0474758711 2833959896 8522325446 0840897111
9771276941 2079586244 0547161321 0050064598 2017696177 1809478113
6220027234 4827224932 3259547234 6880029277 7649790614 8129840428
3457201463 4896854716 9082354737 8356619721 8622496943 1622716663
9390554302 4156473292 4855248991 2257394665 4862714048 2117138124
3882177176 0298412552 4464744505 5834628144 8833563190 2725319590
4392838737 6407391689 1257924055 0156208897 8716337599 9107887084
9081590975 4801928576 8451988596 3053238234 9055809203 2999603234
4711407760 1984716353 1161713078 5760848622 3637028357 0104961259
5681846785 9653331007 7017991614 6744725492 7283348691 6000647585
9174627812 1269007351 8309241530 1063028932 9566584366 2000800476
7789679843 8209079761 9859493646 3093805863 3672146969 5975027968
7712057249 9666698056 1453382074 1203159337 7030994915 2746918356
5937621022 2006812679 8273445760 9380203044 7912277498 0917955938
3871210005 8876668925 8448700470 7725524970 6044465212 7130404321
1826101035 9118647666 2963858495 0874484973 7347686142 0880529443
```

Oeps... Nu dat we dit getal vermeld hebben, hebben we dan een rechterlijk vonnis genegeerd? Is ons eindwerk nu illegaal? We vermelden toch gewoon een priemgetal in ons eindwerk, dat nota bene over priemgetallen gaat...

§3 – Priemtweelingen

Priemtweelingen zijn paren van priemgetallen van de vorm (p, p+2).

De eerste priemtweelingen: (3,5), (5,7), (11,13), (17,19)…

Men vermoed dat er oneindig veel priemtweelingen bestaan, maar dit heeft men ondanks vele pogingen nog steeds niet kunnen bewijzen.

Zoals men bij gewone priemgetallen steeds op zoek is naar nieuwe en grotere priemgetallen, is men ook steeds op zoek naar nieuwe en grotere priemtweelingen. De grootst gekende priemtweeling is $33218925 \cdot 2^{169690} \pm 1$. Dit getal bestaat uit 51090 cijfers en werd in 2002 ontdekt door Daniel Papp.

Naast priemtweelingen spreekt men ook van *neef-priemgetallen* (p, p+4) en *sexy priemgetallen* (p, p+6).

Neef-priemgetallen: (3,7), (7,11), (13,17), (19, 23)*...*
Sexy priemgetallen: (5,11), (7,13), (11,17), (13,19)…

Er bestaan geen priem*drie*lingen (p, p+2, p+4) of *neef-priemdrietallen* (p, p+4, p+8), behalve (3, 5, 7) en (3, 7, 11). Dit komt omdat telkens minstens een van de getallen deelbaar door drie is. Maar er bestaan wel *sexy priemdrietallen* (p, p+6, p+12) en zelfs *sexy priemviertallen* (p, p+6, p+12, p+18).

Sexy priemdrietallen: (7, 13, 19), (17, 23, 29), (31, 37, 43), (47, 53, 59)...
Sexy priemviertallen: (11, 17, 23, 29), (41, 47, 53, 59), (61, 67, 73, 79)...

Er bestaan echter geen *sexy priemvijftallen* (p, p+6, p+12, p+18, p+24), want minstens een van deze getallen is deelbaar door vijf. Daarom beginnen ook alle *sexy priemviertallen* met een getal dat eindigt met het cijfer 1. Enkel zo zal pas het vijfde getal in de rij eindigen op een 5.

§4 – Priemgetallen met een speciale vorm

Priemgetallen hebben altijd al een bijzondere aantrekkingkracht gehad op wiskundigen. En ook als je niet slim genoeg bent om de stelling van Goldbach of een ander belangrijk probleem aan te pakken, kan je je nog steeds verdiepen in de ontelbare verrasende eigenschappen die sommige priemgetallen hebben. Hier volgen enkele bijzondere soorten priemgetallen. [23]

A: Palindroom-priemgetallen

Een palindroom-priemgetal (of palpriem) blijft exact hetzelfde als we de cijfers van rechts naar links lezen. Zo zijn 313 en 12721 palindroom-priemgetallen.

Er zijn heel veel palindroom-priemgetallen, waaronder een aantal leuke speciale gevallen:

1234567890987654321234567890987654321234567890987654321234567890987654321234567890987654321

Een palpriem dat vijf keer de cijfersreeks op en af gaat.

92303290000000000000000000000000000000066600000000000000000000000000000000009230329

Dit is een wel heel mooie palpriem. Het bestaan uit 666, geflankeerd door 32 0'en en 9230329. Bovendien…

- 9230329 is exact het 666ste palindroom-priemgetal
- $666 \cdot 32$ = 21312 (een mooi palindroom)
- $666 \cdot 64$ = 42624 (nog een mooi palindroom)

3141592653589793238462643383346264832397985356295141 3

De decimale ontwikkeling van π in een palpriem, de correcte decimalen zijn onderstreept.

De cijferreeks 944449 komt voor in de decimale ontwikkeling van π vanaf het 75557'ste decimaal. Beide getallen zijn palpriem, en bovendien hebben beide de zogenaamde depressie-vorm.

Nog meer palindroom-priemgetallen in π: de cijferreeks 9136319 komt voor in de decimale ontwikkeling van π vanaf het 9128219'ste decimaal. Deze twee getallen zijn twee opeenvolgende palpriemen. Door de '91' te laten vallen komen nog twee nieuwe priemgetallen tevoorschijn: 38319 en 28219. En ook 91 363 282 19 is een priemgetal!

32323232323...32323232323

Een zeer regelmatig palindroom-priemgetal van wel 6959 cijfers lang!

1000… 116010611 …0001

Het grootst gekende palindroom-priemgetal, bestaande uit 130037 cijfers!

74295029087**00000**78092059247
74295029087**10101**78092059247
74295029087**20202**78092059247
74295029087**30303**78092059247
74295029087**40404**78092059247
74295029087**50505**78092059247
74295029087**60606**78092059247
74295029087**70707**78092059247
74295029087**80808**78092059247
74295029087**90909**78092059247

Een erg opvallende reeks bestaande uit allemaal palpriemetallen!

Wat dacht je van deze palpriem-piramide? Elke ‘laag’ is een palindroom-priemgetal, waarbij het middendeel op de koop toe hetzelfde blijft!

2
70207
357020753
9635702075369
33963570207536933
7233963570207536932721
127233963570207536933272179
97127233963570207536933272179
11971272339635702075369332721791109
9011971272339635702075369332721791109
339011971272339635702075369332721791109333
94339011971272339635702075369332721791109334983
3894339011971272339635702075369332721791109334983
193894339011971272339635702075369332721791109334983391
15193894339011971272339635702075369332721791109334983915157
751519389433901197127233963570207536933272179110933498391515747
7475151938943390119712723396357020753693327217911093349839151574721
127475151938943390119712723396357020753693327217911093349839151574721
30127475151938943390119712723396357020753693327217911093349839151574721033
7330127475151938943390119712723396357020753693327217911093349839151574721033337
337330127475151938943390119712723396357020753693327217911093349839151574721033733
99337330127475151938943390119712723396357020753693327217911093349839151574721033733999
729933733012747515193894339011971272339635702075369332721791109334983915157472103373399927
92729933733012747515193894339011971272339635702075369332721791109334983915157472103373399272729
1892729933733012747515193894339011971272339635702075369332721791109334983915157472103373399272981
131892729933733012747515193894339011971272339635702075369332721791109334983915157472103373399272981311

Is het je overigens opgevallen dat alle palindroom-priemgetallen (behalve 11) een oneven aantal cijfers bevatten? Dit is geen toeval. Het is bewezen dat elk palindroom-getal met een even aantal cijfers deelbaar is door 11.

B: Tetraëdische priemgetallen

Tetraëdische priemgetallen zijn palindroom-priemgetallen die niet alleen van links naar rechts hetzelfde zijn, maar ook ondersteboven en gespiegeld. Deze getallen mogen dus enkel de cijfers 0, 1 en 8 bevatten. Enkele voorbeelden zijn 181, 188818881, 188888881 en 1888081808881. De absolute recordhouder is 1000...10111100100111101...0001 (78943 cijfers).

C: Repunit priemgetallen

Repunit priemgetallen zijn ook speciale palindroom-priemgetallen. Repunit komt van het Engelse ‘repeat unit’, wat ‘herhaling van de eenheid’ betekent. Een repunit getal R_n is dan ook het getal dat uit een opeenvolging van n 1’en bestaat. R_2 = 11 is een repunit priemgetal, maar er zijn er meer. Zo zijn R_{19} = 1111111111111111111 en R_{23} = 11111111111111111111111 ook priem, net als R_{317} en R_{1031}.

R_{1031} is momenteel het grootst bekende repunit priemgetal, maar men heeft sterke vermoedens (op basis van veelvuldig toepassen van Fermat’s kleine stelling) dat ook R_{49081} priem is. Opvallend is dat repunit priemgetallen steeds uit een priem aantal 1’en bestaan. Dit komt omdat $R_{a \cdot b}$ steeds deelbaar is door R_a en R_b.

Zijn er nog andere priemgetallen (>10) die slechts één cijfer bevatten? Neen, want zo’n getal is steeds deelbaar door het cijfer in kwestie.

D: Circulaire priemgetallen

Circulaire priemgetallen zijn priemgetallen die steeds priem blijven als je het laatste cijfer ‘wegkapt’ en het er vooraan terug ‘aanplakt’. Een voorbeeld om dit te verduidelijken: 197 is een circulair priemgetal, want zowel 197, 719 en 971 zijn priem. Het is meteen duidelijk dat alle repunit priemgetallen ook circulaire priemgetallen zijn. Maar andere circulaire priemgetallen zijn zeldzaam (en daarom des te meer bijzonder).

Hier volgt een lijst van alle gekende circulaire priemgetallen, waarbij telkens alleen de kleinste vertegenwoordiger wordt vermeld: 2, 3, 5, 7, 11, 13, 17, 37, 79, 113, 197, 199, 337, 1193, 3779, 11939, 19937, 193939, 199933, R_{19}, R_{23}, R_{317} en R_{1031}.

E: Permutabele priemgetallen

Een speciale vorm van circulaire priemgetallen zijn permutabele priemgetallen. Bij permutabele priemgetallen moeten *alle* permutaties (herschikkingen) van de cijfers priem zijn, en bovendien moeten er minstens twee verschillende cijfers zijn, waardoor de repunit priemgetallen uitgesloten worden.

113 is wel een voorbeeld van een permutabel priemgetal, want zowel 113, 131 als 311 zijn priem. 197 is echter geen permutabel priemgetal, want 791 en 917 zijn *geen* priem. Het aantal permutabele priemgetallen is zeer klein. Men vermoedt dat 13, 17, 37, 79, 113, 199, 337 en hun permutaties de enige permutabele priemgetallen zijn.

F: Beschrijvende priemgetallen

In een reeks van beschrijvende getallen beschijft elk getal het vorige letterlijk. Op 113 volgt 2113 omdat 113 bestaat uit “twee 1’en gevolgd door één 3”. Soms bestaat zo’n reeks uit verschillende priemgetallen, bijvoorbeeld:

233
1223
112213
21221113
1211223113
11122122132113

Het volgende getal in de reeks is echter samengesteld.

De langst gekende reeks van beschrijvende priemgetallen bestaat uit zeven priemgetallen:

19972667609
112917122617161019
211219111711221611171116111011119
122112111931172122111631173116311031119
1122211231191321171211223116132117132116132110132119
213221121321191113122117111221221321161113122117111312211611131221101113122119
121113222112111312211931131122211731221122111312211631131122211731131122211631131122211031131122119

G: Besluit

Wie heeft er baat bij al deze curiositeiten? Praktisch nut hebben ze waarschijnlijk nauwelijks. Bovendien spelen we hier met de cijfers van een getal, maar deze cijfers veranderen als we van het decimaal talstelsel overstappen op een ander talstelsel. Rekenen we in een ander talstelsel, moeten we *al* onze curiositeiten herzien. De tetraëdische priemgetallen hebben zelfs betrekking op de *vorm* van de cijfers, niet eens op het patroon. Het wiskundige belang van deze speciale soorten priemgetallen is dus nihil.

Maar er zijn honderden mensen ter wereld die verzot zijn op dit soort weetjes in verband met priemgetallen. Op internet vind je dan ook een absurde hoeveelheid aan priem-curiositeiten. Wist je bijvoorbeeld dat 285646799 een priemgetal is, gelijk aan $(2 \cdot 19 \cdot 23 \cdot 317 \cdot 1031) + 1$, waarbij de vijf factoren tevens de lengte van de vijf gekende repunit priemgetallen voorstellen? De website *http://primes.utm.edu/curios/* vertelt het je. Deze website stelt zich overigens tot doel alle weetjes over priemgetallen te verzamelen. “Er staan momenteel 6560 curiositeiten over 3423 verschillende getallen in onze database, waardoor er nog een oneindig aantal curiositeiten overblijven die jij kan ontdekken,” [24] vertelt men ons. Succes!

Hoofdstuk 3: INTERESSANTE TOEPASSINGEN

§1 – De cyclus van cicaden

Cicaden zijn een familie van insecten die leven van plantensappen. Cicaden brengen het grootste deel van hun leven onder de grond door, waar ze hun voedsel halen uit de wortels van planten. Maar na enkele jaren komen deze cicaden bovengronds om zich voor te planten.

In Noord-Amerika zijn er echter enkele soorten, periodieke cicaden genoemd, die een heel speciale cyclus hebben. Alle cicaden van deze soort hebben hun cyclus op elkaar afgestemd. Je komt deze periodieke cicaden dus jarenlang niet tegen, maar opeens komen ze met miljoenen tegelijk bovengronds om te paren. En even plots als ze gekomen zijn, verdwijnen ze dan weer collectief onder de grond.

Deze methode heeft een aantal voordelen. Zo is er heel veel voortplanting mogelijk, omdat alle cicaden van een soort tegelijkertijd boven de grond komen om te paren. En omdat ze plots met miljoenen tegelijk bovengronds komen, is er ook geen verdediging tegen predatoren (dieren die cicaden eten) nodig. Immers: hoe gulzig de predatoren ook zijn, ze kunnen nooit een groot deel van alle cicaden opeten.

Maar er is nog een veel interessanter aspect aan deze periodieke cicaden. De lengte van hun cyclus, hun *periode*, is behoorlijk groot, meer bepaald steeds 13 of 17 jaar. Twee priemgetallen! Zou daar een bepaalde reden voor zijn?

Men neemt aan dat er vroeger cicaden-predatoren waren die ook volgens een cyclus leefden. Om de hoeveel jaar komen cicade en predator elkaar tegen? Dit is het kleinste gemene veelvoud van de twee periodes. Cicaden met een cyclus van 6 jaar en predatoren met een cyclus van 4 jaar bijvoorbeeld, komen elkaar elke 12 jaar tegen.

Het kleinste gemene veelvoud van twee getallen kan je bereken door de twee getallen te ontbinden in priemfactoren, de gemeenschappelijke factoren in één van de getallen te schrappen, en alle resterende factoren van de twee getallen te vermenigvuldigen.

Hier een voorbeeld voor het kleinste gemene veelvoud van 12 en 15.

$30 = 2 \cdot 3 \cdot 5$

$12 = 2^{\not 2} \cdot \not 3$ $\quad kgv = 2^2 \cdot 3 \cdot 5 = 60$

Hoe kunnen we dit toepassen om onze cicaden grote overlevingskansen te geven? De cicaden die vaak predatoren tegenkwamen, werden allemaal opgegeten. Maar de cicaden die slechts heel zelden predatoren tegenkwamen als ze bovengronds kwamen, overleefden. We moeten dus zorgen dat het kleinste gemene veelvoud van de twee periodes zo groot mogelijk is. Het kleinste gemene veelvoud is maximaal als er geen gemeenschappelijke factoren geschrapt kunnen worden. En een priemgetal heeft als enige priemfactor zichzelf! Is de periode van de cicaden een priem aantal jaar, dan zullen we geen factoren kunnen schrappen (tenzij de periode van de predator een veelvoud hiervan is). Deze cicaden zullen slechts zelden predatoren tegenkomen.

En zo heeft de evolutie ervoor gezorgd dat cicaden die een niet-prieme periode hadden, opgegeten werden. Maar de cicaden met een cyclus die een priem aantal jaren duurt, kwamen slechts zelden predatoren tegen. De predatoren kwamen om van hongersnood. En de cicaden met de cycli van 13 jaar en 17 jaar overleefden!

Sommige biologen beweren dat de hypothese van de predatoren niet klopt. Zij komen met een gelijkaardige, alternatieve uitleg. Met een prieme periode komen de cicaden niet alleen zelden predatoren tegen, maar ook zelden andere periodieke cicaden-soorten. Zo worden kruisingen tussen twee soorten cicaden met een verschillende periode vermeden. Kruisingen zijn te vermijden, want ze verstoren de mooie regelmatige periodes van de hele soort, wat fataal kan zijn voor het voortbestaan van de soort. Een periode die een priem aantal jaar duurt, is daarom ideaal, niet zozeer om predatoren te mijden, maar juist om andere cicadensoorten te mijden.

Het is nog niet duidelijk welke van de twee verklaringen de juiste is. Ook weet men niet zeker waarom juist de priemgetallen 13 en 17 door de natuur ‘uitgekozen’ werden. Wel komen periodes van 17 jaar vooral voor in meer noordelijk gelegen regionen. Waarschijnlijk zorgt het koudere klimaat er daar voor dat de ondergrondse groeiperiode langer moet duren dan in de warmere streken, waar cicaden toekomen met een 13-jarige periode. [(25)]

§2 – Priemgetallen in de cryptografie

A: Een korte cryptografiegeschiedenis

Kristof wil aan Stijn een geheime boodschap versturen, maar boze Frans probeert die boodschap te onderscheppen. Om te voorkomen dat Frans de boodschap onderschept en gewoon kan aflezen, stuurt Kristof de boodschap door in een verborgen vorm. In de paragraaf over illegale priemgetallen zijn we al enkele voorbeelden tegengekomen van steganografie: de tekst wordt gecodeerd in een afbeelding. Kristof legt aan Stijn uit hoe hij de boodschap uit de afbeelding kan halen. Maar als Frans de afbeelding in handen krijgt, zal hij er de boodschap waarschijnlijk niet in vinden.

Bij cryptografie wordt de originele tekst omgezet in een andere tekst (de *code*), Kristof zet de tekst niet om in een afbeelding, maar in een ander stuk tekst. Om de originele tekst in de code om te zetten en omgekeerd, gebruiken Stijn en Kristof een bepaalde sleutel. Frans kent deze sleutel echter niet, en zal grote moeite hebben om de code te ontcijferen. Kristof en Stijn kunnen hun boodschappen dus uitwisselen zonder dat Frans de inhoud van de boodschap kent.

Het gebruik van cryptografie kwam al voor bij de oude Grieken, de Perzen, de Arabieren en de Romeinen.

Bekend is het eenvoudig geheimschrift van de romein Julius Caesar, die geëncrypteerde boodschappen gebruikte om zijn leger te informeren. Caesar schoof elke letter drie plaatsen op in het alfabet. ‘Veni, vidi, vici’ bijvoorbeeld, werd YHQL, YLGL, YLFL. Omdat hij het systeem zo vaak gebruikte heeft men het naar hem genoemd, en noemt men het ‘het Caesar-cijfer’. Een tekst die met dit systeem geëncrypteerd (versleuteld) is, is echter zeer snel te kraken en dus niet erg veilig.

Kan je deze geheime boodschap ontcijferen?
HON HYHQ JHWDO, JURWHU GDQ WZHH, NDQ JHVFKUHYHQ ZRUGHQ DOV GH VRP YDQ WZHH SULHPJHWDOOHQ.

Geheimschriften werden in de geschiedenis vooral gebruikt in het diplomatieke verkeer en in oorlogen om het vijandelijke staten en legers moeilijk te maken geheime berichten te ontcijferen. Zo is het breken van de Duitse Enigma-code in de Tweede Wereldoorlog door de Engelsen waarschijnlijk van doorslaggevende betekenis geweest om de oorlog te eindigen. Het resultaat ervan was dat de geheime routes van Duitse U-boten bij de geallieerden bekend werden.

Door de opkomst van de computers kan men bijna onbreekbare vercijferingmethodes maken. Zo vond men in de jaren ’70 de DES (Data Encryption Standard) uit. In 1998 maakten twee Belgen, Joan Daemen en Vincent Rijmen, nog een veel sterkere code: de Advanced Encryption Standard, ook gekend als Rijndael. Rijndael is zelfs voor de modernste computers een vrijwel onbreekbare code.

B: Het probleem van de sleutelverdeling

Maar zelfs de sterkste codes hebben een belangrijk zwak punt: hoe kan de sleutel op een veilige manier worden uitgewisseld? Om een versleutelde boodschap naar Stijn te sturen, moet Kristof eerst zorgen dat Stijn de juiste sleutel kent. Maar die sleutel zelf kan Kristof natuurlijk niet versleuteld doorsturen, want dan zou Stijn de sleutel niet begrijpen. Frans heeft dus de kans om de sleutel te onderscheppen, waardoor zelfs de sterkste codering terug waardeloos wordt.

Zo moest het Duitse opperbevel tijdens Wereldoorlog Twee elke maand een boek met alle sleutels voor die maand over het hele Duitse leger, inclusief U-boten, verspreiden. Dit vormde een enorm logistiek probleem, en als er één sleutelboek onderschept werd door de Britten, konden de Britten een maand lang alle Duitse berichten zonder enig probleem ontcijferen.

In de jaren ’70 vonden Whitfield Diffie, Martin Hellman en Ralph Merkle een oplossing voor het probleem. Ze vonden het concept van de asymmetrische cryptografie uit. Bij asymmetrische cryptografie is er niet één sleutel, maar zijn er twee sleutels: een geheime sleutel en een publieke sleutel. Iedereen heeft een eigen geheime sleutel, die hij aan niemand laat zien, en een eigen publieke sleutel, die openbaar gemaakt wordt. De publieke sleutel kan gebruikt worden om berichten te coderen, maar enkel met de geheime sleutel kan het bericht ontcijferd worden.

Om een bericht te sturen aan Stijn, zoekt Kristof eerst Stijns publieke sleutel. Daarmee vercijfert Kristof het bericht. Ook Frans kent Stijns publieke sleutel, maar Frans kan de geheime code hiermee niet ontcijferen. Enkel Stijn kan met zijn geheime sleutel de boodschap ontcijferen.

Je zou het concept van de asymmetrische cryptografie kunnen vergelijken met een hangslot. Iedereen kan een hangslot dichtklikken, maar je hebt een sleutel nodig om het hangslot terug te openen. Kristof steekt zijn boodschap in een koffertje, en klikt een hangslot van Stijn dicht om het koffertje te sluiten. Enkel Stijn kan met zijn geheime sleutel het hangslot terug openen.

C: Priemgetallen in de cryptografie

Door asymmetrische cryptografie moeten er geen geheime sleutels meer uitgewisseld worden. Maar de vraag rest nog hoe dit concept in de praktijk moet omgezet worden. Er is een functie nodig die in de de ene richting door iedereen kan uitgevoerd worden (het dichtklikken van het hangslot), maar die in de andere richting slechts kan uitgevoerd worden als je over extra informatie beschikt (het sleuteltje).

RSA, dat in 1977 ontdekt werd, bracht de oplossing. De letters van RSA staan voor de namen van de drie ontdekkers: Ron Rivest, Adi Shamir en Len Adleman. RSA is een asymmetrisch cryptografiesysteem, en om sterke sleutels te maken, gebruikt RSA... priemgetallen!

Het systeem gebruikt priemgetallen omdat het heel gemakkelijk is om twee priemgetallen met elkaar te vermenigvuldigen. De functie in de andere richting uitvoeren is echter een groot probleem. Het product van twee priemgetallen, vooral dan bij grote priemgetallen, kan heel moeilijk ontbonden worden in de twee priemfactoren.

Een voorbeeld: we nemen twee priemgetallen, bijvoorbeeld 9419 en 1933. Met een rekenmachine hebben we deze twee priemgetallen snel vermenigvuldigd, het product is 18.206.927. Maar dit getal ontbinden in zijn twee priemfactoren, 9419 en 1933, dat duurt wel een tijdje. Er zijn immers geen efficiënte methodes bekend om getallen te ontbinden in priemfactoren. Je moet eigenlijk gewoon voor elk priemgetal testen of het een deler is van het product (18.206.927). Voor dit voorbeeld valt dat nog mee, maar als je zeer grote priemgetallen vermenigvuldigt (priemfactoren van ongeveer 10^{200}), moeten zelfs de modernste computers passen voor de factorisatie van het product.

Bij RSA vormen de twee priemfactoren de private sleutel, en het product de publieke sleutel. Om een geheime boodschap aan Stijn te sturen, zoekt Kristof Stijns publieke sleutel, het product van de twee priemfactoren dus. Hij versleutelt zijn bericht en stuurt het naar Stijn. De code kan echter enkel ontcijferd worden met de twee priemfactoren. Stijn heeft zelf deze twee priemfactoren, en kan het bericht snel ontcijferen. Maar als Frans de geheime boodschap wil kennen, moet hij ook beschikken over de priemfactoren. Frans kent echter alleen het product (de publieke sleutel) en moet dit product dus eerst ontbinden in priemfactoren. Als Stijn een voldoende grote sleutel heeft, staat Frans voor een hopeloze taak. De geheime boodschap is helemaal veilig!

In 1997 werd overigens bekend dat Rivest, Shamir en Adleman in feite niet de eersten waren die de RSA-encryptie uitvonden. In 1975, twee jaar eerder, werd deze techniek al uitgevonden door een groep cryptografen, waarbij het belangrijkste aandeel was voor James Ellis, Clifford Cocks en Malcolm Williamson. Zij werkten echter voor de GCHQ (Government Communication Headquarters), een Britse *top secret*-organisatie, en moesten hun ontdekkingen geheimhouden. Pas in 1997 werd bekend dat zij de eersten waren die de encyptiemethode uitvonden, die twee jaar later opnieuw zou ontdekt worden door Rivest, Shamir en Adleman. Maar deze laatsten moesten hun ontdekking niet geheimhouden, waardoor iedereen nu spreekt van RSA-encryptie.

D: Het belang van goede encryptie

Tegenwoordig wordt cryptografie niet alleen gebruikt voor oorlogsvoering, maar ook door banken om geldtransacties te versleutelen, zodat ze niet door 'digitale bankrovers' onderschept kunnen worden. Door de opkomst van internet-winkelen heeft ook de gewone internet-gebruiker veel belang bij een goede versleuteling van zijn kredietkaart-gegevens. En zelfs gewoon e-mailverkeer wordt tegenwoordig steeds meer versleuteld om de privacy van zender en ontvanger te beschermen.

Diverse geheime diensten en veiligheidsorganisaties, zoals de Amerikaanse NSA (National Security Agency) verzetten zich echter hevig tegen te sterke codes. De sterke encryptie kan immers ook gebruikt worden voor illegale doeleinden zoals terrorisme, drugshandel en belastingontduiking. De Verenigde Staten besteden miljarden dollars aan het ‘aftappen’ van onder andere telefoon- en e-mailverkeer, om zo bijvoorbeeld terroristische aanslagen te verhinderen. Maar als terroristen hun e-mails gaan versleutelen, hebben de terroristen vrij spel voor hun communicatie.

Vooral in de VS heeft men zich daarom sterk verzet tegen sterke codes als de RSA-encryptie. Zo ontwierp de programmeur Phil Zimmerman in 1991 een computerprogramma dat volgens de manier van de RSA-encryptie werkt. Het programma, PGP (Pretty Good Privacy) genaamd, kwam wereldwijd gratis beschikbaar. Sterke cryptografie wordt in de VS echter tot ‘ammunitie’ gerekend. De FBI opende een onderzoek tegen Zimmermann, en hij werd zelfs aangeklaagd wegens overtreding van de wet op de export van strategische wapens en ammunitie.

Maar vooral dankzij de spectaculaire ontwikkeling van het internet, is het nu voor iedereen ter wereld mogelijk om zijn communicatie veilig te versleutelen, zodat deze zelfs voor geheime diensten onleesbaar blijft. Dankzij priemgetallen kunnen we met een gerust hart boeken kopen op Amazon, of andere internet-aankopen doen. En de geheime diensten, tja... die hebben nog een hele resem andere spionagemethodes om terroristen op te sporen.

BESLUIT

“Priemgetallen? Wat kan je daar nu over schrijven?” Deze vraag hebben we nu hopelijk goed beantwoord. We hopen dat iedereen die dit gelezen heeft verbaasd is over de verrassende wereld van de priemgetallen en er nog meer in geïnteresseerd raakt.

Maar men is nog steeds niet uitgepraat over priemgetallen, en men zal er nooit over uitgepraat raken. Er zijn immers oneindig veel priemgetallen. Elke dag wordt naar nieuwe, almaar grotere priemgetallen gezocht en probeert men nieuwe eigenschappen en curiositeiten te vinden. Zo nemen er steeds meer mensen deel aan de GIMPS, waardoor er steeds sneller nieuwe priemgetallen zullen gevonden worden.

Misschien zal iemand het vermoeden van Goldbach bewijzen, waarvan er nu, na meer dan 250 jaar, nog steeds geen bewijs gevonden is. Dat zou dan waarschijnlijk het moment van het eeuw worden.

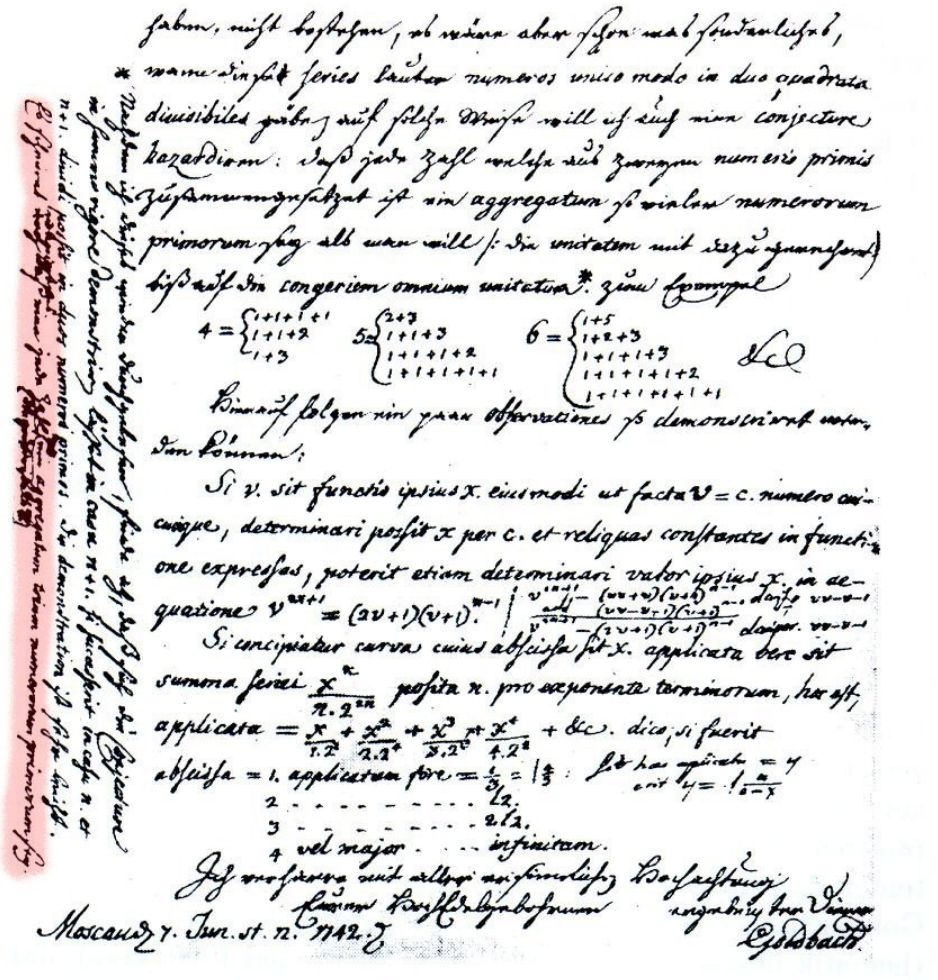
Voorlopig heeft men in de dierenwereld alleen een verband gevonden tussen cicaden en priemgetallen. Het is dus best mogelijk dat er iemand is die bij een andere diersoort nog zoiets ontdekt.

En hoe zit het met de toekomst van de cryptografie? Een snelle methode om getallen te ontbinden in priemfactoren zou het mogelijk maken om geheime communicatie zonder veel problemen te ontcijferen.

Kortom: de priemgetallen zijn de bouwstenen van de wiskunde. En er zijn nog oneindig veel bouwstenen ter beschikking, waarmee we nog een oneindig aantal constructies mee kunnen maken!

BIJLAGEN

Bijlage 1: Brief van Goldbach aan Euler



Dit is de brief die Christian Goldbach op 7 juni 1742 aan Leonard Euler schreef. In de marge staat zijn beroemd vermoeden, dat elk even getal (>2) kan geschreven worden als de som van twee priemgetallen. *"Es scheinet wenigstens, daß eine jede Zahl, die größer ist als 2, ein aggregatum trium numerorum primorum sey."* (26)

Wiskundigen schrijven overigens wel vaker hun beste werk in de marge neer. Pierre de Fermat, die we ook al in hoofdstuk 1 tegenkwamen, schreef in 1637 in de kantlijn van een boek: "$x^n + y^n = z^n$ heeft geen oplossingen voor $n > 2$ en $x, y, z, n \in \mathbb{N}$. Ik heb hier een spectaculair bewijs voor gevonden, maar deze kantlijn is te klein om het te bevatten." Tegenwoordig wordt echter betwijfeld of Fermat inderdaad een geldig bewijs had. In elk geval duurde het meer dan 350 jaar tot er iemand anders een bewijs vond. In 1993 presenteerde de Britse wiskunde Andrew Wiles zijn bewijs van het zgn. laatste raadsel van Fermat.

NOTEN

Voorwoord

(1) Origineel citaat: “Primes are the basic building blocks of arithmetic. Just like knowing what bricks you have available is important to a man going to build a house, the primes are important to anyone studying the integers.” Bron: eigen e-mailcommunicatie met Chris Caldwell

Hoofdstuk 1: Oneindig veel priemgetallen

(2) M. NACHTEGAEL en J. BUYSSE, *Wiskundig vademecum – Een synthese van de leerstof wiskunde*, Kapellen, 2001, p. 209

(3) M. NACHTEGAEL en J. BUYSSE, *idem*, p. 209

(4) Meestal heeft men het bij deelbaarheid (en bij $d|a$) over gehele getallen. Omdat dit werk over priemgetallen gaat, beschouwen we echter alleen de (strikt) natuurlijke getallen.

(5) http://primes.utm.edu/notes/faq/one.html

(6) Een bewijs uit het ongerijmde gaat als volgt. We willen een stelling A bewijzen. Eerst veronderstellen we het tegengestelde van het te bewijzen (niet-A). We rekenen hierop voort, totdat we op een duidelijke tegenspraak, een duidelijke fout uitkomen. Omdat we op een fout zijn uitgekomen, kan niet-A dus niet waar zijn, en moet A (het te bewijzen) waar zijn.

(7) http://www.utm.edu/research/primes/notes/proofs/infinite/euclids.html

(8) http://primes.utm.edu/glossary/page.php?sort=Fermat en http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Fermat.html (foto)

(9) Hier kan 3 door bepaalde andere getallen vervangen worden, waaronder 5 en 10.

(10) Of anders: F_n is priem als en slechts als $3^{(Fn-1)/2} = -1 \pmod{Fn}$

(11) http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Mersenne.html

(12) http://www.utm.edu/research/primes/mersenne/index.html#test

(13) http://www.utm.edu/research/primes/prove/prove2_2.html

(14) Of anders: Als p geen deler is van a, dan heeft $a^{p-1} = 1 \pmod{p}$

(15) http://primes.utm.edu/mersenne/index.html

(16) Origineel citaat: “It like climbing Mount Everest. You do it for the fun and challenge.” Bron: eigen e-mailcommunicatie met George Woltman.

Hoofdstuk 2: Verrassende priemgetallen

(17) Deze stad heet vandaag Kaliningrad en ligt in Rusland

(18) http://www.wiskundeweb.nl/Wiskundegeschiedenis/Wiskundigen/Goldbach.html

(19) Origineel citaat: "Es scheinet wenigstens, daß eine jede Zahl, die größer ist als 2, ein aggregatum trium numerorum primorum sey."

(20) http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/Stego/index.html

(21) Origineel citaat: “Maybe somebody with a local copy of the Human Genome Project database on his personal supercomputer can find this sequence in our genetical information. This would mean nearly 6 billion lawbreakers on this planet." Bron: http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/Stego/index.html

(22) http://asdf.org/~fatphil/maths/illegal2.html

(23) Alle records in deze paragraaf (bijvoorbeeld de grootste priemtweeling) zijn de records van 5 januari 2005. Het is mogelijk dat deze record ondertussen reeds gebroken zijn.

(24) Origineel citaat: “There are currently 6560 curios corresponding to 3423 different numbers in our database, that leaves an infinite number for you to discover!” Bron: http://primes.utm.edu/curios/ (25 februari 2005).

Hoofdstuk 3: Verrassende priemgetallen

(25) http://www.bio.davidson.edu/people/midorcas/animalphysiology/websites/2004/Hindsley/Evolution.htm

Bijlagen

(26) http://www.informatik.uni-giessen.de/staff/richstein/ca/Goldbach.html

BRONNEN

- M. NACHTEGAEL en J. BUYSSE: *Wiskundig vademecum – Een synthese van de leerstof wiskunde*, Uitgeverij Pelckmans, Kapellen, 2001, 216 p.
- S. SINGH: *Code – De wedloop tussen makers en brekers van geheime codes en geheimschrift*, Uitgeverij De Arbeiderspers, Amsterdam, Antwerpen, 1999, 481 p.
- http://primes.utm.edu
- http://www-groups.dcs.st-and.ac.uk
- http://www.mersenne.org/prime.htm (http://www.mersenneforum.org/showthread.php?s=&postid=15142 #post15142)
- http://mathforum.org/library/drmath/view/56057.html
- http://nl.wikipedia.org/ en http://en.wikipedia.org/
- http://www.worldofnumbers.com/
- http://www.geocities.com/CapeCanaveral/Launchpad/4057/palindromes.htm
- http://www.wschnei.de/digit-related-numbers/descriptive-primes.html
- http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/
- http://www.vanegten.net/scriptie/scriptie-2.2.html
- http://www.mpi-dortmund.mpg.de/departments/swo/markus/save/nature_cicada_2.html
- http://www.bio.davidson.edu/people/midorcas/animalphysiology/websites/2004/Hindsley/Evolution.htm
- http://msnbc.msn.com/id/4893167/

Nawoord

Op 1 maart 2005 leverden Kristof en ik dit eindwerk in. Enkele dagen later ontdekte Kristof dat de tekst reeds achterhaald was: de GIMPS had twee weken eerder, op 18 februari, een nieuw grootste Mersenne-priemgetal ontdekt. Ons eindwerk verhaalt nog uitgebreid over het oude record...

Dat stond niet in de weg dat dit eindwerk goed beoordeeld werd. Ook nu, twee jaar later, is er nog steeds interesse in de tekst, en wordt hij regelmatig geraadpleegd via internet. Daarom neem ik nu de moeite om een klein nawoord te schrijven om enkele zaken te verduidelijken.

Het eindwerk is niet door mij alleen geschreven. Kristof Scheys heeft een evenwaardige bijdrage aan het resultaat geleverd. Helaas wordt er nogal vaak gerefereerd naar deze tekst als *het eindwerk van Stijn*, wat te verklaren is door mijn *bekendheid* als wiskundige en door het feit dat het eindwerk via mijn website te downloaden is. Maar dat zou geen reden mogen zijn om de waardevolle bijdrage van Kristof te negeren.

Een aantal leerlingen heeft dit eindwerk reeds gebruikt als bron om zelf een tekst over priemgetallen te schrijven, iets waar wij natuurlijk trots op zijn. Ik wil echter leerlingen aanmoedigen om zich niet teveel te spiegelen aan deze tekst. Wij hebben er bewust voor gekozen om een heel toegankelijk eindwerk te maken, waarbij wiskundige afleidingen de goede leesbaarheid niet mochten schaden. Daardoor bleven een aantal bewijzen achterwege, en werden meer gevorderde onderwerpen als de priemgetallenstelling en het vermoeden van Riemann niet vermeld. Dat wil geenszins zeggen dat die onderwerpen niet boeiend zijn. (Dit hebben wij bovenaan pagina 17 eigenlijk zelf verkeerdelijk gesteld.) Een verhandeling over priemgetallen die een andere keuze maakt in onderwerpen of stijl, kan zeker net zo interessant zijn als het onze. Ga dus zeker op ontdekking bij andere bronnen, en maak zelf je keuze tussen de overvloed aan boeiende plekjes in het land van de priemgetallen.

Ik ga met niet bezighouden om alle kleine spellingsfoutjes en onnauwkeurigheden uit de tekst te filteren. En ook niet met het up to date houden van de verschillende records die vermeld worden. Wie de actuele records wil kennen, kan die gemakkelijk vinden op internet, bijvoorbeeld op *primes.utm.edu*. En wie vragen heeft over priemgetallen of over dit eindwerk, mag mij steeds contacteren.

Stijn Vermeeren
Juni 2007