Algebra en Getaltheorie@Work: van cryptosysteem tot digitale handtekening

Dr. Fabien Decruyenaere, St. Amandscollege, 8500 Kortrijk
fabien.decruyenaere@skynet.be

Prof. Dr. Paul Igodt, K.U.Leuven Campus Kortrijk, 8500 Kortrijk
Paul.Igodt@kulak.be

Eekhoutcentrum, 27 oktober 2004

Woord vooraf

In onze maatschappij, die steeds méér en ingrijpender gebruik maakt van Wiskundige technieken en inzichten, is een blijvende zorg en inzet voor degelijk Wiskunde-onderwijs een grote noodzaak. Sinds langere tijd reeds wordt er beleidsmatig geknabbeld aan het beschikbare lessenpakket voor deze opdracht. Het de facto op vele plaatsen beëindigen van de zogenaamde "8-uurs" en het invoeren van nieuwe begrippen als de "vrije ruimte" zijn hier recente indicatoren voor. Laat ons echter ons enthousiasme niet verliezen, en laat ons evenmin bij de pakken blijven zitten! Kwalitatief Wiskunde-onderwijs kan verbazingwekkend interdisciplinair zijn, en is daarom een uitstekend aanbod voor de invulling van die vrije ruimte.

Deze tekst, in een eerste indruk allicht ietwat (te?) lang, is niet bedoeld als een ononderbroken "cursus" die een gedreven leraar aan zijn leerlingen in de vrije ruimte kan aanbieden. De tekst brengt veeleer een aantal zaken samen, die ofwel in iets langer verleden nog courant aan bod kwamen of die we willen suggereren als bijzonder geschikt voor enkele enthousiasmerende Wiskundelessen. Elk van deze 'mini-thema's' (relaties, orde, groepen, ...) is overigens erg beperkt gehouden en zou zonder moeite (en aanbevelens waard) kunnen aangevuld worden (b.v. kardinaalgetallen, infimum en supremum, ...). Uit deze tekst kan in elk geval her en der lesmateriaal en lesinhoud "geplukt" worden. We hopen dat dit zal gebeuren.

De meermaals verbazingwekkende kracht en schoonheid van de Wiskunde heeft als eerder dure prijs dat het nogal eens een lange leertijd duurt vooraleer die schoonheid zich ontplooit en manifesteert. Onze onderwijsbeleid wekt op zijn minst de indruk haar leerlingen die tijd niet meer te gunnen, en verkiest klaarblijkelijk frequent allerlei "vaardigheden" boven "capaciteit en vorming om vaardigheden snel te verwerven".

De inhoud van deze tekst is - zo hopen we - voldoende Wiskundig streng om vormend te zijn, voldoende Wiskundig fris om prikkelend te zijn en voldoende toepassingsgericht-actueel om enthousiasmerend te zijn, dit zowel voor de leerkracht als de leerling. Op een aantal plaatsen werd er een zgn. ICT-onderwijstoepassing ingelast, uit te voeren met een hedendaags grafisch rekenmachine. Het kan leerkracht en leerling helpen om een aantal aangebrachte problemen meer experimenteel te verkennen of met beter realiteitsgehalte te simuleren.

Als er dan toch een woordje uit het hoger onderwijs mag aan toegevoegd worden, laat het dan dit wezen: het is natuurlijk beter en vooral eenvoudiger (voor het hoger onderwijs, om af te stemmen) indien de basis Wiskundige vorming van elke nieuwe student berust op een grote gemeenschappelijke inhoud en methode. Dit lijkt minder dan in het verdere verleden het geval geworden. Veeleer meer diversiteit dan meer uniformiteit dient zich aan, mogelijks meer dan ooit ook met een schoolgebonden component in de achtergrond. Belangrijk blijft echter dat, op zijn minst, bij wat men leert, een voldoende groot gedeelte ervan een voldoende grote diepgang heeft. Zit het vormende immers ook niet in die capaciteit tot diepte?

Wij hopen u - als leerkracht, met een grote verantwoordelijkheid - , uw onderwijs en uw leerlingen met deze bijdrage tot steun te zijn. Blijf enthousiast! Blijf aanmoedigen! Hou contact!

Kortrijk 27 oktober 2004

Inhoudsopgave

Hoofdstuk 1

Algebra en getaltheorie: bouwstenen

1.1 Relaties: terug van weg

Definitie 1.1.1 Als A en B verzamelingen zijn, dan is

$$A \times B = \{(a, b) \parallel a \in A, b \in B\}$$

de productverzameling van A met B (in het bijzondere geval dat $A = B$, wordt de notatie A^2 gebruikt). Elke deelverzameling $\mathcal{R}$ van $A \times B$ wordt een relatie van A naar B genoemd. Als $A = B$, spreken we van een relatie in A.

Bijvoorbeeld, als $A = \{a, b, c\}$ en $B = \{1, 2, 3, 4\}$, dan is $\mathcal{R} = \{(a, 2), (a, 3), (b, 4), (c, 3)\}$ een relatie van A naar B.

Notatie 1.1.2 In plaats van $(a, b) \in \mathcal{R}$, noteert men meestal $a\mathcal{R}b$.

We geven enkele voorbeelden waarvan sommige heel belangrijk zijn in het kader van deze tekst en andere aan bod kunnen komen in andere gebieden van de Wiskunde (analyse, lineaire algebra, meetkunde,...) :

Voorbeelden 1.1.3

1. $\{(x, y) \in \mathbb{Z}^2 \parallel \ x < y\}$ is een relatie in $\mathbb{Z}$;
2. $\{(x, y) \in \mathbb{Z}^2 \parallel x \leq y\}$ is een relatie in $\mathbb{Z}$;
3. $\{(x, y) \in \mathbb{N}^2 \parallel x \mid y\}$ is een relatie in $\mathbb{N}$;
4. $\{(x, y) \in \mathbb{Z}^2 \parallel x \mid y\}$ is een relatie in $\mathbb{Z}$;
5. als $A = \{0, 1, 2, 3, 4, 5, 6\}$, dan is $\{(x, y) \in A^2 \parallel x \mid y\}$ een relatie in A; (voor een exacte definitie van "$\ldots \mid \ldots$", zie deel 3)
6. "$\equiv \bmod 4$" $= \{(x, y) \in \mathbb{Z}^2 \parallel 4 \mid x - y\}$ is een relatie in $\mathbb{Z}$;
7. de relatie $\mathcal{R}_1$ in $\mathbb{Z} \times \mathbb{Z}_0$ gedefinieerd door: $(a, b)\mathcal{R}_1(c, d) \Longleftrightarrow a \cdot d = b \cdot c$;
8. $\mathcal{R}_2 = \{(x, y) \in \mathbb{R}^2 \parallel y = x^3\}$ is een relatie in $\mathbb{R}$;
9. $\mathcal{R}_3 = \{(x, y) \in \mathbb{R}^2 \parallel x^2 + y^2 = 1\}$ is een relatie in $\mathbb{R}$;
10. $\mathcal{R}_4 = \{(x, y) \in \mathbb{R}^2 \parallel E(x) = E(y)\}$ is een relatie in $\mathbb{R}$, waarbij $E(x)$ het grootste geheel getal is dat kleiner is dan of gelijk aan x (E wordt de Entier-functie van Legendre genoemd);

11. de relatie $\mathcal{R}_5$ in de verzameling van alle rechten in het vlak, gedefinieerd door:

$$a\mathcal{R}_5 b \iff a \parallel b$$

12. de relatie $\mathcal{R}_6$ in de verzameling van alle $m \times n$-matrices, gedefinieerd door:
$A\mathcal{R}_6 B \iff$ er bestaat een eindig aantal elementaire rijbewerkingen die A omzetten in B.

13. de relatie $\mathcal{R}_7$ in de verzameling van alle rationale functies, gedefinieerd door:
$f\mathcal{R}_7 g \iff$ de rationale vormen $f(x)$ en $g(x)$ zijn gelijk.

14. de relatie $\mathcal{R}_8$ in de verzameling van alle veeltermfuncties, gedefinieerd door:
$f\mathcal{R}_8 g \iff Df = Dg$.

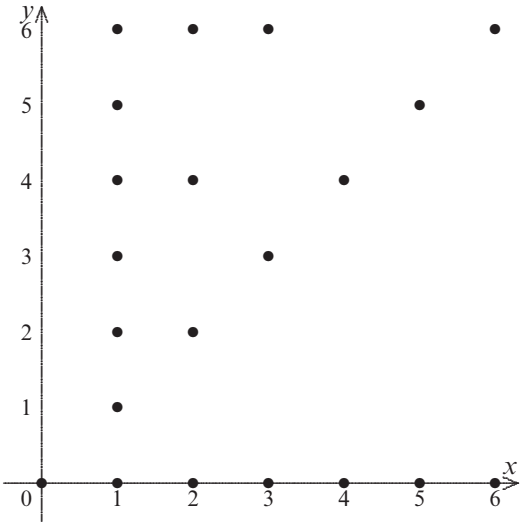
15. de relatie $\mathcal{R}_9$ in een verzameling van proposities, gedefinieerd door:
$p\mathcal{R}_9 q \iff (p \to q)$.

Grafische voorstelling 1.1.4

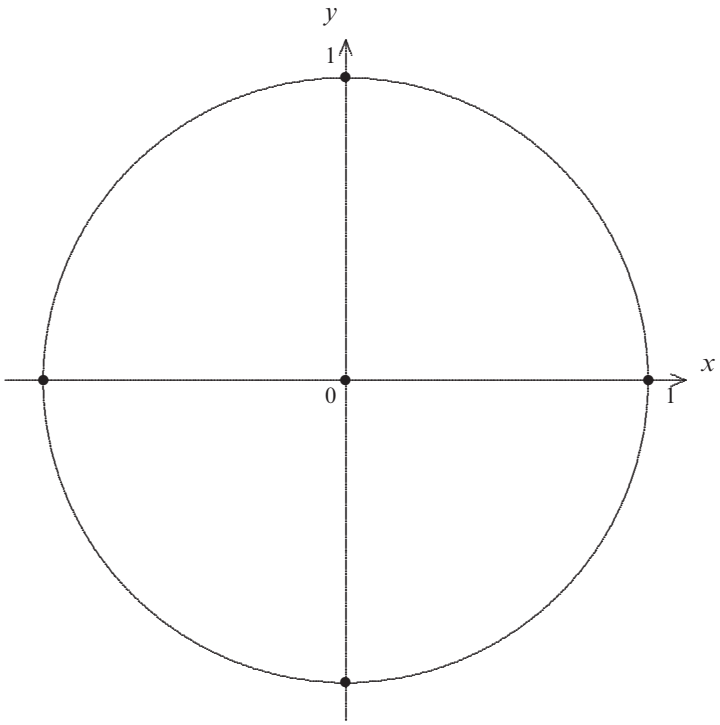
We geven een kort overzicht van de verschillende manieren om een relatie visueel voor te stellen :

- een roosterdiagram (of grafiek) : dit is de meest gekende voorstellingswijze omdat een functie meestal op deze manier grafisch wordt voorgesteld (merk op dat een functie f van A naar B een relatie is van A naar B zodat voor elk element a van A hoogstens één element b van B bestaat waarvoor $(a, b) \in f$).

  Bij deze voorstellingswijze worden de elementen van A en B resp. op de X-as en de Y-as voorgesteld : het roosterdiagram bestaat dan uit alle punten van het (X, Y)-vlak waarvan de coördinaat behoort tot de relatie. De grafiek van voorbeeld 5 hierboven is een verzameling van punten die er als volgt uitziet :



  De grafiek van voorbeeld 9 daarentegen is een kromme (t.o.v. een orthonormaal assenstelsel een cirkel) :



- een gerichte graaf (als A en B eindige verzamelingen zijn): hierbij worden de elementen van A en B voorgesteld door stippen en telkens als $a\mathcal{R}b$, wordt een pijl getekend van a naar b. Grafen vormen een interessant studie-onderwerp met vele toepassingen binnen en buiten de wiskunde (cf.[1, 4])

  Oefening. Teken de graaf van de relatie uit voorbeeld 5.

- een binaire matrix (als A en B eindige verzamelingen zijn en hun elementen geordend worden): als $A = \{a_1, a_2, \ldots, a_n\}$ en $B = \{b_1, b_2, \ldots, b_m\}$, dan is de binaire matrix $M = (m_{i,j})$ van een relatie $\mathcal{R}$ van A naar B een $n \times m$-matrix, waarbij

$$\begin{cases} m_{i,j} = 1, & \text{als } (a_i, b_j) \in \mathcal{R} \ ; \\ m_{i,j} = 0, & \text{als } (a_i, b_j) \notin \mathcal{R} \ ; \end{cases}$$

  In voorbeeld 5 is

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Definitie 1.1.5 Als $\mathcal{R}$ een relatie is van A naar B, dan is de omgekeerde relatie $\mathcal{R}^{-1}$ een relatie van B naar A zodat $(a, b) \in \mathcal{R} \Longleftrightarrow (b, a) \in \mathcal{R}^{-1}$.

Oefeningen.

1. Hoe verkrijg je de graaf van $\mathcal{R}^{-1}$ uit de graf van $\mathcal{R}$? Wat gebeurt er met de binaire matrix?

2. Hoe ontstaat het voorschrift van $\mathcal{R}^{-1}$ uit dat van $\mathcal{R}$? Illustreer dit op de voorbeelden 1,2,3,4,7,8,9 en 11.

3. Teken de grafiek van de relatie $\mathcal{R}_2$ t.o.v. een orthonormaal assenstelsel; teken vervolgens de grafiek van $\mathcal{R}_2^{-1}$ t.o.v. datzelfde assenstelsel. Wat constateer je? Controleer dit ook voor $\mathcal{R}_3$. Formuleer je vermoeden als een eigenschap.

Eigenschappen 1.1.6 Zij $\mathcal{R}$ een relatie in A

1. $\mathcal{R}$ is reflexief als en slechts als $\forall a \in A : a\mathcal{R}a$;
2. $\mathcal{R}$ is symmetrisch als en slechts als $\forall a, b \in A : a\mathcal{R}b \Longrightarrow b\mathcal{R}a$;
3. $\mathcal{R}$ is anti–symmetrisch als en slechts als $\forall a, b \in A : a\mathcal{R}b$ en $b\mathcal{R}a \Longrightarrow a = b$;
4. $\mathcal{R}$ is transitief als en slechts als $\forall a, b, c \in A : a\mathcal{R}b$ en $b\mathcal{R}c \Longrightarrow a\mathcal{R}c$.

Oefeningen.

1. Wat is kenmerkend voor de graaf van een relatie die
   (a) reflexief is?
   (b) symmetrisch is?
2. Wat is kenmerkend voor de binaire matrix van een relatie die
   (a) reflexief is?
   (b) symmetrisch is?
   (c) anti-symmetrisch is?
3. Een relatie in een verzameling van 4 elementen heeft volgende binaire matrix:

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

   Welke van de eigenschappen uit 1.1.6 zijn voldaan?
4. Ga na welke van de eigenschappen uit 1.1.6 voldaan zijn voor de voorbeelden uit 1.1.3.
5. Vind de fout in het volgende bewijs:

   > Onderstel dat $\mathcal{R}$ een symmetrische en transitieve relatie is in een verzameling A. Zij a een willekeurig element van A. Door de symmetrie van $\mathcal{R}$ volgt uit $a\mathcal{R}b$ dat $b\mathcal{R}a$. Maar uit $a\mathcal{R}b$ en $b\mathcal{R}a$ volgt, door de transitiviteit van $\mathcal{R}$, dat $a\mathcal{R}a$. Daar a een willekeurig element van A voorstelt, is $\mathcal{R}$ reflexief. Elke symmetrische transitieve relatie is dus ook reflexief.

   Geef ook een voorbeeld van een symmetrische transitieve relatie die niet reflexief is.

We maken nu kennis met een heel belangrijke klasse van relaties:

Definitie 1.1.7 Een relatie $\mathcal{R}$ in A is een equivalentierelatie als en slechts als $\mathcal{R}$ reflexief, symmetrisch en transitief is.

Oefening. Welke van de voorbeelden uit 1.1.3 zijn equivalentierelaties?

Definitie 1.1.8 Als $\mathcal{R}$ een equivalentierelatie is en als $a \in A$, dan noemen we

$$\bar{a} = \{b \in A \mid a\mathcal{R}b\}$$

de (equivalentie)klasse van a.

Lemma 1.1.9 Als $\mathcal{R}$ een equivalentierelatie is in A en als $a, b \in A$, dan $b \in \bar{a} \Longrightarrow \bar{a} = \bar{b}$

Bewijs: Onderstel dat $b \in \bar{a}$. Dan $a\mathcal{R}b$.
Als nu $x \in \bar{b}$, dan $b\mathcal{R}x$. Daar $\mathcal{R}$ transitief is, volgt dan dat $a\mathcal{R}x$ en dus $x \in \bar{a}$.
Bijgevolg $\bar{b} \subseteq \bar{a}$.
Als nu $y \in \bar{a}$, dan $a\mathcal{R}y$. Daar $a\mathcal{R}b$ volgt uit de symmetrie van $\mathcal{R}$ dat $b\mathcal{R}a$. Daar $\mathcal{R}$ transitief is, volgt dan dat $b\mathcal{R}y$ en dus $y \in \bar{b}$.
Bijgevolg $\bar{a} \subseteq \bar{b}$.
Dit bewijst dat $\bar{a} = \bar{b}$.

Q.E.D.

De volgende eigenschap illustreert het belang van equivalentierelaties :

Eigenschap 1.1.10 De verzameling van alle klassen van een equivalentierelatie $\mathcal{R}$ in een verzameling A is een partitie van A, d.w.z.

1. geen enkele klasse is leeg;
2. elke twee verschillende klassen zijn disjunct (hebben lege doorsnede);
3. de unie van alle klassen is A.

Bewijs:

1. is voldaan omdat elk element a van A behoort tot zijn eigen klasse $\bar{a}$ (want $\mathcal{R}$ is reflexief).
2. Onderstel dat $x \in \bar{a} \cap \bar{b}$ met $\bar{a} \neq \bar{b}$. Dan $a\mathcal{R}x$ en $b\mathcal{R}x$. Door de symmetrie van $\mathcal{R}$ volgt dan dat $x\mathcal{R}b$. Daar $\mathcal{R}$ transitief is, volgt dan uit $a\mathcal{R}x$ en $x\mathcal{R}b$ dat $a\mathcal{R}b$ of $b \in \bar{a}$. Lemma 1.1.9 impliceert dan dat $\bar{a} = \bar{b}$, een contradictie. Dus $\bar{a} \cap \bar{b} = \emptyset$.
3. Zij $a \in A$. Dan behoort a tot zijn eigen klasse (omdat $\mathcal{R}$ reflexief is) en bijgevolg tot de unie van alle klassen.

Q.E.D.

Oefening. Ga na, in de voorbeelden uit 1.1.3 die equivalentierelaties zijn, hoe de equivalentieklassen kunnen omschreven worden.

Vele verzamelingen zijn op natuurlijke wijze geordend. Het meest voor de hand liggende voorbeeld is de verzameling van de reële getallen die geordend zijn door hun "grootte": uitdrukkingen als $3 \leq \pi$, $-4 < 3$, $2 < \sqrt{8} < 3$ zijn welbekend. Analoog is elke verzameling van verzamelingen geordend door de "inclusie": als $A \subseteq B$, dan kunnen we A als "kleiner" dan B beschouwen. Dit soort relaties zouden we orderelaties kunnen noemen. Maar, in tegenstelling met equivalentierelaties, zijn er verschillende soorten orderelaties. Beschouw b.v. de relaties in $\mathbb{R}$, resp. gedefinieerd door $x \leq y$ en $x < y$; deze relaties hebben verschillende eigenschappen. B.v. de eerste relatie is reflexief en de tweede niet. Vrij algemeen hanteert men de volgende

Definitie 1.1.11 Een partiële orde(relatie) $\mathcal{R}$ in een verzameling A is een relatie die reflexief, anti–symmetrisch en transitief is. We noemen $(A, \mathcal{R})$ een partieel geordende verzameling.

Voorbeelden 1.1.12

1. $\{(x, y) \in \mathbb{R}^2 \parallel x \leq y\}$ is een partiële orde in $\mathbb{R}$;
2. Als $\mathcal{F}$ een verzameling van verzamelingen is, dan is $\mathcal{R}$, gedefinieerd door $\forall A, B \in \mathcal{F} : A\mathcal{R}B \Longleftrightarrow A \subseteq B$, een partiële orde in $\mathcal{F}$;
3. $\{(x, y) \in \mathbb{N}^2 \parallel x \mid y\}$ is een partiële orde in $\mathbb{N}$;

   Daarentegen $\{(x, y) \in \mathbb{Z}^2 \parallel x \mid y\}$ is geen partiële orde in $\mathbb{Z}$ (verklaar!);
4. Als $\mathcal{W}$ de verzameling van alle woorden uit "het groene boekje" is, dan is $\mathcal{R}$, gedefinieerd door

   $$\forall w_1, w_2 \in \mathcal{W} : w_1\mathcal{R}w_2 \Longleftrightarrow w_1 = w_2 \text{ of } w_1 \text{ komt voor } w_2 \text{ in het groene boekje,}$$

   een partiële orderelatie in $\mathcal{W}$: dit is de gewone alfabetische (of lexicografische) ordening van woorden;
5. de relatie $\mathcal{R}$ in $\mathbb{R}^2$, gedefinieerd door

   $$(x_1, y_1)\mathcal{R}(x_2, y_2) \Longleftrightarrow (x_1 < x_2) \text{ of } (x_1 = x_2 \text{ en } y_1 \leq y_2)$$

   is een partiële orde in $\mathbb{R}^2$: deze orde is analoog aan de alfabetische orde van woorden (vorig voorbeeld);
6. de relatie $\mathcal{R}$ in $\mathbb{R}^2$, gedefinieerd door

   $$(x_1, y_1)\mathcal{R}(x_2, y_2) \Longleftrightarrow x_1 \leq x_2 \text{ en } y_1 \leq y_2$$

   is een partiële orde in $\mathbb{R}^2$.

Oefening. Ga na dat de hierboven vermelde voorbeelden wel degelijk partiële orderelaties zijn.

Een partieel geordende verzameling $(A, \mathcal{R})$ kan een grootste element hebben, maar dat hoeft niet, en analoog voor een kleinste element. B.v. $(\mathbb{Z}, \leq)$ heeft geen grootste en geen kleinste element, terwijl $(\mathbb{N}, \leq)$ wel een kleinste element heeft, nl. 0, maar geen grootste element heeft.
Uiteraard heeft elke eindige deelverzameling van $(\mathbb{R}, \leq)$ een grootste en een kleinste element.
Dit betekent niet dat elke eindige partieel geordende verzameling een grootste en kleinste element heeft: beschouw de verzameling van alle echte deelverzamelingen van $\{a, b, c\}$, geordend door $\subseteq$ (hoeveel elementen telt deze verzameling?). Het kleinste element is $\emptyset$, maar er is geen grootste element aangezien er drie deelverzamelingen van $\{a, b, c\}$ zijn die twee elementen bevatten.
Een oneindige deelverzameling van $\mathbb{R}$ hoeft ook geen grootste of kleinste element te hebben: b.v. $]0, 1[= \{x \in \mathbb{R} \mid 0 < x < 1\}$ heeft geen grootste en geen kleinste element, maar $[0, 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$ wel, nl. resp. 1 en 0.
Deze voorbeelden tonen aan dat we enige precisie aan de dag moeten leggen bij het exact definiëren van de volgende begrippen :

Definitie 1.1.13 Zij $(A, \mathcal{R})$ een partieel geordende verzameling.
Een grootste element (maximum) van A (indien het bestaat) is een element M van A zodat $\forall a \in A : a\mathcal{R}M$.
Een kleinste element (minimum) van A (indien het bestaat) is een element m van A zodat $\forall a \in A : m\mathcal{R}a$.

Merk op dat, indien m en M bestaan, ze uniek zijn. In dat geval kunnen we dus spreken van "het" kleinste en "het" grootste element van A. Onderstel b.v. dat er nog een maximum M' zou zijn: dan zou volgens de definitie $M'\mathcal{R}M$ (want M is maximum) en ook $M\mathcal{R}M'$ (want M' is maximum); uit de anti–symmetrie van $\mathcal{R}$ volgt dan dat $M = M'$.
Terugkomend op het voorbeeld van de echte deelverzamelingen van $\{a, b, c\}$ kunnen we gemakkelijk bewijzen dat er geen maximum is volgens deze definitie. Echter, elk van de drie deelverzamelingen bestaande uit 2 elementen kan beschouwd worden als een "grootst mogelijke", in de betekenis dat er geen grotere zijn dan deze. We formaliseren dit idee in de volgende

Definitie 1.1.14 Zij $(A, \mathcal{R})$ een partieel geordende verzameling. Een element x van A is maximaal als en slechts als $\forall a \in A : x\mathcal{R}a \Longrightarrow x = a$. Een element y van A is minimaal als en slechts als $\forall a \in A : a\mathcal{R}y \Longrightarrow y = a$.

Oefening.Bepaal het (eventuele) maximum, minimum en alle maximale en minimale elementen in

1. de voorbeelden uit 1.1.12;
2. $(\{2, 4, 8, 16, 32\}, |)$;
3. de verzameling van de echte natuurlijke delers van 210, voorzien van de orderelatie |.

Het verband tussen kleinste en minimale en tussen grootste en maximale elementen wordt verduidelijkt in volgende

Stelling 1.1.15 Zij $(A, \mathcal{R})$ een partieel geordende verzameling. Als A een grootste element M heeft, dan is M het enige maximale element. Analoog, als A een kleinste element m heeft, dan is M het enige minimale element.

Bewijs : Zij M het grootste element van A.
Onderstel dat $M\mathcal{R}a$ met $a \in A$: daar M het grootste element is van A, weten we dat $a\mathcal{R}M$; bijgevolg, door de anti–symmetrie van $\mathcal{R}$, $a = M$ en M is dus een maximaal element van A.
Onderstel nu dat x een maximaal element van A is, dan $x\mathcal{R}M$ (want M is het grootste element). Maar aangezien x maximaal is, volgt dat $x = M$. Dus M is het enige maximale element van A.
Het bewijs voor het kleinste element is volledig analoog. Q.E.D.

Definitie 1.1.16 Een totale orde (of lineaire orde) in A is een partiële orde in A die voldoet aan de volgende (dichotomie)eigenschap:

$$\forall a, b \in A : a\mathcal{R}b \text{ of } b\mathcal{R}a.$$

Oefening.

1. Ga na welke voorbeelden uit 1.1.12 totale ordes zijn.
2. Een verzameling A voorzien van een totale orde $\mathcal{R}$ wordt welgeordend genoemd als elke niet-lege deelverzameling van A een kleinste element heeft voor $\mathcal{R}$.
   (a) Toon aan dat elke eindige verzameling, voorzien van een totale orde, welgeordend is ;
   (b) toon aan dat noch $\mathbb{Z}$, noch $\mathbb{R}^+$, voorzien van de orde $\leq$, welgeordend zijn;
   (c) geef een voorbeeld van een oneindige welgeordende verzameling.

1.2 Functies: enkele elementaire begrippen

Definitie 1.2.1 Een functie f van A naar B is een relatie van A naar B waarbij voor elk element x van A hoogstens één element y van B bestaat zodat $(x, y) \in f$.

Notatie 1.2.2 We noteren $y = f(x)$ en noemen y het beeld van x onder f. We schrijven $f : A \to B : x \mapsto f(x) = y$.

Definitie 1.2.3 De verzameling van alle elementen van A die een beeld hebben onder f noemen we het domein van f en noteren we met $\text{dom}(f)$.
De verzameling van alle elementen van B die beeld zijn van één of meerdere elementen van A onder f noemen we de beeldenverzameling van f of kortweg het beeld van f en noteren we met $\text{Im}(f)$.

In de Analyse komen functies van $\mathbb{R}$ naar $\mathbb{R}$ (reële functies) overvloedig aan bod en worden verschillende klassen van functies zoals veeltermfuncties, rationale functies, irrationale functies, goniometrische en cyclometrische functies, exponentiële en logaritmische functies e.d. bestudeerd. We geven enkele voorbeelden :

Voorbeelden 1.2.4

1. $f_1 : \mathbb{R} \to \mathbb{R} : x \mapsto x^2 = y$;
2. $f_2 : \mathbb{R} \to \mathbb{R} : x \mapsto x^3 = y$;
3. $f_3 : \mathbb{R} \to \mathbb{R} : x \mapsto \sqrt{x} = y$;
4. $f_4 : \mathbb{R} \to \mathbb{R} : x \mapsto \sqrt[3]{x} = y$;
5. $f_5 : \mathbb{R} \to \mathbb{R} : x \mapsto \frac{1}{x} = y$;
6. $f_6 : \mathbb{R} \to \mathbb{R} : x \mapsto \sin x = y$;
7. $f_7 : \mathbb{R} \to \mathbb{R} : x \mapsto 2^x = y$.

Oefening. Zoek van elk van deze reële functies domein en beeld.

Wij zullen in de toepassingen werken met functies in een eindige verzameling en zijn vooral geïnteresseerd in volgende kenmerken van functies:

Definitie 1.2.5 Een functie f van A naar B is een afbeelding van A in B als en slechts als elk element van A een beeld heeft onder f in B, of, equivalent, als $\mathrm{dom}(f) = A$; indien $A = B$, dan spreken we van een transformatie van A.
Een functie f van A naar B is injectief van A in B als en slechts als elke twee elementen van A verschillende beelden hebben onder f in B, of equivalent als voor elk element b van B hoogstens één element a van A bestaat zodat het beeld van a onder f gelijk is aan b;
Een functie f van A naar B is surjectief van A op B als en slechts als voor elk element b van B minstens één element a van A bestaat zodat het beeld van a onder f gelijk is aan b, of, equivalent, als $\mathrm{Im}(f) = B$;
Een functie f van A naar B is een bijectie van A op B als en slechts als f is een injectieve en surjectieve afbeelding van A in B; indien $A = B$, dan spreken we van een permutatie van A.

Oefeningen.

1. Formuleer bovenstaande definities in symbolen.
2. Ga na welke van deze kenmerken voldaan zijn voor de voorbeelden uit de vorige paragraaf ($A = B = \mathbb{R}$). Indien een functie niet injectief is, vind dan een maximale injectieve beperking ervan, d.w.z. beperk het domein tot een zo groot mogelijke deelverzameling zodat de functie wel injectief wordt.
3. Teken de graaf van een bijectie van A op B waarbij A en B eindige verzamelingen zijn; wat kun je hieruit besluiten? Formuleer je besluit als een eigenschap.
4. Vind een bijectie van $\mathbb{N}$ op $\mathbb{Z}$.

Het belang van bijecties, inzonder injectieve functies, blijkt uit het volgende : aangezien een functie f van A naar B in de eerste plaats een relatie is van A naar B en voor elke relatie een omgekeerde relatie bestaat, is volgende vraag heel logisch :

Wanneer is de omgekeerde relatie f^{-1} opnieuw een functie (van B naar A)?

Opdracht. Teken de graaf van een functie waarvan de omgekeerde relatie niet opnieuw een functie is. Wat kun je hieruit besluiten?

We verkrijgen aldus

Eigenschap 1.2.6 Zij f een functie van A naar B. Dan is f^{-1} een functie van B naar A als en slechts als f injectief is van A in B. In dit geval noemen we f^{-1} de inverse functie van f.

In symbolen:

$$f^{-1} : B \to A : y \mapsto f^{-1}(y) = x \Longleftrightarrow f(x) = y.$$

Oefeningen.

1. Zoek voor alle injectieve functies of maximale injectieve beperkingen uit 1.2.4 het voorschrift van de inverse functie en teken van beide de grafiek t.o.v. een orthonormaal assenstelsel in het vlak.
2. Bewijs: f is een injectieve afbeelding van A in $B \Longleftrightarrow$ er bestaat een functie g van B naar A zodat $g \circ f$ gelijk is aan Id_A, de identieke afbeelding van A;

   als ook $A = B$ een eindige verzameling is, dan is f een permutatie van A en dan is g de inverse functie van f.
3. Ga na op een graaf: als f een bijectie is van A op B, dan geldt: $f \circ f^{-1} = \mathrm{Id}_B$ en $f^{-1} \circ f = \mathrm{Id}_A$.

1.3 Deelbaarheid in $\mathbb{Z}$

Definitie 1.3.1 Gegeven twee gehele getallen, m en n, dan zeggen we dat m een deler is van n als en slechts als er een geheel getal q bestaat zo dat $q.m = n$.
In symbolen:

$$\forall m, n \in \mathbb{Z} : m \mid n \Leftrightarrow \exists q \in \mathbb{Z} : m.q = n.$$

Voorbeeld 1.3.2

- Elk geheel getal n heeft zichzelf en $-n$ als delers.

  $$\forall n \in \mathbb{Z} : n \mid n \text{ en } -n \mid n \text{ (want } 1.n = n \text{ en } -1.-n = n).$$

- De getallen 1 en -1 zijn deler van elk geheel getal n.

  $$\forall n \in \mathbb{Z} : 1 \mid n \text{ en } -1 \mid n \text{ (want } n.1 = n \text{ en } -n.-1 = n).$$

- Als d een deler is van het geheel getal n, dan is ook $-d$ een deler van n; d en $-d$ worden geassocieerde delers genoemd.
- Elk geheel getal n is deler van 0.

  $$\forall n \in \mathbb{Z} : n \mid 0 \text{ (want } 0.n = 0).$$

- We noteren del(n) voor de verzameling van de delers van n. 0 is het enige geheel getal met een oneindige verzameling delers; in het bijzonder geldt del(0)$= \mathbb{Z}$.
- Voor elk geheel getal n, noemen we 1, -1, n en $-n$ de onechte delers van n. n kan op triviale wijze geschreven worden als product $n = 1.n = n.1 = -1.-n = -n.-1$. Een geheel getal n verschillend van 1 en -1 heeft dus minstens 4 delers.

Verifieer nu zelf de volgende

Eigenschap 1.3.3 Stel $a, b, d \in \mathbb{Z}$. Als d een deler is van a en van b, dan is d ook een deler van $k \cdot a + l \cdot b$ $(k, l \in \mathbb{Z})$ en van $a \cdot b$.

Definitie 1.3.4 Een priemgetal is een natuurlijk getal p dat precies twee delers in $\mathbb{N}$ heeft (nl. 1 en p).

Voorbeeld 1.3.5

- 2, 3, 5, 7, 11, 13, ... zijn priemgetallen. 2 is het enige even priemgetal.
- 0 en 1 zijn geen priemgetallen (verklaar!).
- De Franse Wiskundige Pierre de Fermat (1601-1665) dacht dat al de zogenaamde Fermatgetallen $F_i = 2^{2^i} + 1$ ($i \in \mathbb{N}$) priemgetallen waren. Nu blijkt inderdaad dat $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ en $F_4 = 65537$ priemgetallen zijn. In 1732 ontdekte Leonhard Euler evenwel dat $F_5 = 641 \cdot 6700417$ geen priemgetal is (beide factoren in deze ontbinding zijn wel priem). Ook F_6, F_7, F_8 en F_9 zijn geen priemgetallen. De ontbinding van F_6 werd in 1880 ontdekt door Landry en Le Lasseur, die van F_7 in 1970 door Brillhart en Morrison, die van F_8 in 1980 door Brent en Pollard en F_9 werd pas in 1990 ontbonden door Lenstra, Lenstra, Manasse en Pollard. Dit illustreert de moeilijkheid van het ontbinden in factoren. Anderzijds zien we ook een snelle vooruitgang: het duurde tot 1970 vooraleer F_7 (bestaande uit 39 decimalen!) ontbonden werd, maar F_7 (bestaande uit 155 decimalen!!) werd slechts 20 jaar later ontbonden. Meer informatie over priemgetallen vind je b.v. in [2].

Oefeningen.

1. Hoeveel priemgetallen zijn er, kleiner dan 10000, waarvan de som van de cijfers 2 is?

   (V.W.O. 95-96, 1e ronde, vraag 27)

2. Hoeveel van de volgende vier uitspraken over natuurlijke getallen zijn waar?
   (1) Van drie opeenvolgende oneven natuurlijke getallen zijn er precies twee priem.
   (2) Van drie opeenvolgende oneven natuurlijke getallen zijn er minstens twee priem.
   (3) Van drie opeenvolgende oneven natuurlijke getallen is er minstens één priem.
   (4) Van drie opeenvolgende oneven natuurlijke getallen is er minstens één niet priem.

   (V.W.O. 96-97, 1e ronde, vraag 7)

3. Als p een oneven priemgetal is, welk is dan ook een priemgetal?
   (A) $2p + 1$ (B) $p^2 + 1$ (C) $3p + 2$ (D) $p^3 + 2$ (E) geen van de vorige

   (V.W.O. 85-86, 1e ronde, vraag 18)

4. Bewijs dat elk priemgetal groter dan 3 een 6-voud ± 1 is. Is een 6-voud ± 1 altijd een priemgetal?

5. Vind voorbeelden van priemgetallen die slechts twee van elkaar verschillen. Zulke getallen noemen we tweelingspriemgetallen. De vraag of er oneindig veel tweelingspriemgetallen zijn, is tot op heden onbeantwoord gebleven.

6. Bewijs : voor elke $n \in \mathbb{N} \setminus \{0, 1\}$ bestaan er n opeenvolgende natuurlijke getallen die geen priemgetallen zijn.

   Hint : de 999 opeenvolgende natuurlijke getallen $1000! + 2, 1000! + 3, \ldots, 1000! + 1000$ zijn deelbare getallen.

7. Getallen van de vorm $M_p = 2^p - 1$ waarbij p een priemgetal is, worden Mersenne getallen genoemd (naar de Franse priester Mersenne (1588-1648)). Stel vast dat M_p een priemgetal is voor $p \in \{2, 3, 5, 7, 13\}$ en dat M_{11} geen priemgetal is. $M_{24036583}$ is het 41e Mersenne priemgetal en tegelijk het grootste op dit ogenblik (juli 2004) gekende priemgetal (ontdekt op 15 mei 2004) : het telt 7235733 cijfers en werd ontdekt via het GIMPS-project.

8. We definiëren een "priemdrieling" als een drietal priemgetallen (a, b, c) met $c-b = b-a = 2$. Hoeveel dergelijke priemdrielingen zijn er?

(V.W.O. 99-00, 2de ronde, vraag 15)

9. Als x een priemgetal is en $x^2 + y^2 = z^2$ met $x, y, z \in \mathbb{N}_0$, dan is y gelijk aan
(A) $\frac{x^2-1}{2}$ (B) $\frac{x^2+1}{2}$ (C) x (D) $x^2 - 1$ (E) $x^2 + 1$

(V.W.O. 00-01, 1e ronde, vraag 29)

Een bijzonder belangrijk resultaat uit de rekenkunde van $\mathbb{Z}$ is de

Stelling 1.3.6 (Stelling van de Euclidische deling) Onderstel dat m en n gehele getallen zijn, zo dat $n \neq 0$. Dan bestaan er unieke gehele getallen q ("het quotiënt") en r ("de rest"), zó dat $0 \leq r < |n|$ en zó dat $m = q.n + r$.

Bewijs : Beschouw de verzameling

$$A = \{m - \lambda.n \mid\mid \lambda \in \mathbb{Z}\}.$$

Het is duidelijk dat $A \cap \mathbb{N} \neq \emptyset$. Bijgevolg heeft A een (uniek) kleinste element. Noem dit element r. Stel dat $r = m - q.n$, voor een unieke $q \in \mathbb{Z}$. Dan geldt dat $r < |n|$, want indien dit niet voldaan was, zou $r - |n| = r \pm n = m - (q \pm 1)n$ nog tot $A \cap \mathbb{N}$ behoren. Q.E.D.

Dit resultaat is door de meeste leerlingen gekend (zeker voor de natuurlijke getallen): bij deling van een natuurlijk getal m door een van nul verschillend natuurlijk getal n, verkrijgen we een quotiënt q ($\in \mathbb{N}$) en een positieve rest r die hoogstens gelijk is aan $n - 1$. Het uitvoeren van de deling wordt in het basisonderwijs reeds aangeleerd.

Voorbeeld 1.3.7

- Neem $m = 48$ en $n = 14$. Dan geldt $48 = 3.14 + 6$; bij deling van 48 door 14 vinden we quotiënt 3 en rest 6.
- Neem $m = -34$ en $n = 5$. We vinden nu $-34 = -7.5 + 1$; quotiënt -7, rest $+1$.
- Neem $m = 27$ en $n = -8$. Nu geldt: $27 = -3. - 8 + 3$; quotiënt -3, rest $+3$.
- Neem $m = -64$ en $n = -8$. We vinden $-64 = -8. - 8 + 0$; de rest is 0 en bijgevolg is -64 deelbaar door -8.

Oefening. Zij $a, b, c \in \mathbb{N}_0$. Als bij deling van a door b het quotiënt q is en de rest r is, en bij deling van q door c het quotiënt q' is en de rest r' is, waaraan is dan de rest bij deling van a door bc gelijk?

(V.W.O. 96-97, 2de ronde, vraag 15)

Definitie 1.3.8 Een grootste gemene deler van een eindige, niet lege verzameling A van gehele getallen is een gemeenschappelijke deler d van elk element uit A, zó dat elke gemeenschappelijke deler van de elementen van A ook deler is van d.
Notatie : $d = \text{ggd}(A)$. I.h.b. als $A = \{m, n\}$, $d = \text{ggd}(m, n)$.
Twee getallen m en n worden relatief priem (of onderling ondeelbaar) genoemd als en slechts $\text{ggd}(m, n) = 1$.
Een kleinste gemeen veelvoud van een eindige, niet lege verzameling A van gehele getallen is een gemeenschappelijk veelvoud k van de elementen van A, zó dat k een deler is van elk gemeenschappelijk veelvoud van de elementen van A.
Notatie : $k = \text{kgv}(A)$. I.h.b. als $A = \{m, n\}$, $k = \text{kgv}(m, n)$.

Opmerking 1.3.9 De definitie heeft het inderdaad over "een" grootste gemene deler (resp. kleinste gemeen veelvoud). In $\mathbb{Z}$ is een ggd of een kgv niet uniek, want geassocieerde getallen (d.w.z. gehele getallen die enkel op het teken na verschillen) zijn tegelijk ggd of kgv. Meestal gaat men echter op zoek naar ggd en kgv in de verzameling van de natuurlijke getallen. Hier zijn grootste gemene delers (resp. kleinste gemene veelvouden) uniek. Vandaar volgende alternatieve

Definitie 1.3.10 Zij A een eindige, niet lege verzameling van gehele getallen. Als $\mathcal{D}$ de verzameling van alle gemeenschappelijke delers in $\mathbb{N}$ van elk element van A is, dan is $\text{ggd}(A)$ het maximum van de partieel geordende verzameling $(\mathcal{D}, |)$. Als $\mathcal{V}$ de verzameling van alle gemeenschappelijke veelvouden in $\mathbb{N}$ van elk element van A is, dan is $\text{kgv}(A)$ het minimum van de partieel geordende verzameling $(\mathcal{V}, |)$.

Voorbeeld 1.3.11

1. We zoeken de grootste gemene deler (in $\mathbb{N}$) van 36 en 48. Daartoe bekijken we de verzameling van de delers van beide getallen. Enerzijds

   $$\text{del}(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

   en anderzijds

   $$\text{del}(48) = \{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}.$$

   De gemeenschappelijke delers zijn dan elementen van

   $$\mathcal{D} = \text{del}(36) \cap \text{del}(48) = \{1, 2, 3, 4, 6, 12\}.$$

   Het maximum van $(\mathcal{D}, |)$ is 12 en daarom geldt $12 = \text{ggd}(36, 48)$.

2. Voor elk geheel getal n geldt: $\text{ggd}(0, n) = n$ en $\text{kgv}(0, n) = 0$. Opnieuw kijken we naar de gemeenschappelijke delers van 0 en n. Daar elk geheel getal deler is van 0, zijn alle delers van n meteen ook gemeenschappelijke deler. n heeft al deze delers als deler en is daarom grootste gemene deler van 0 en n. Alleen 0 is een gemeenschappelijk veelvoud van 0 en n; 0 is dus ook kleinste gemeen veelvoud.

3. Voor elk geheel getal n geldt: $\text{ggd}(1, n) = 1$ en $\text{kgv}(1, n) = n$. Alleen 1 (en -1) zijn gemeenschappelijke delers van 1 en n. Alle veelvouden van n zijn gemeenschappelijk veelvoud van n en 1; n is deler van al deze veelvouden en bijgevolg kleinste gemeen veelvoud.

Toepassing 1.3.12 De stelling van de Euclidische deling kent een uitermate belangrijke algoritmische toepassing voor het opzoeken van grootste gemene delers. Vandaar trouwens, dat men vaak van het algoritme van Euclides spreekt. We blijven hier even bij stilstaan.

Het algoritme van Euclides.		
Beschrijving		Merk op:
Gegeven: gehele getallen m en n (verschillend van 0). Onderstel dat $\|n\| < \|m\|$. Anders wisselen we de rollen om.		
Deel m door n. Je vindt zo een uniek quotiënt q_1 en een unieke positieve rest r_1 $(0 \leq r_1 < \|n\|)$ zo dat	$m = q_1.n + r_1$	$r_1 = m - q_1.n$
Deel vervolgens n door r_1. Je vindt een unieke q_2 en r_2, met $0 \leq r_2 < r_1$ waarvoor	$n = q_2.r_1 + r_2$	$r_2 = n - q_2.r_1$ $= n - q_2.(m - q_1.n)$ $= n(1 + q_2.q_1) - q_2 m$
Herhaal deze werkwijze door steeds opnieuw de deling uit te voeren met de twee laatst gevonden resten (r_1 door r_2, r_2 door r_3, enz...).	$r_1 = q_3.r_2 + r_3$ $r_2 = q_4.r_3 + r_4$	
Omdat de resten positief zijn en steeds kleiner worden, zal er een ogenblik komen waarbij voor het eerst een deling opgaat en dus rest gelijk aan nul oplevert. Onderstel dat dit zich voordoet bij de deling van r_{n-1} door r_n, m.a.w.:	$r_{n-2} = q_n r_{n-1} + r_n$ $r_{n-1} = q_{n+1} r_n$.	$r_n = a.n + b.m$ (voor een $a, b \in \mathbb{Z}$)
STOP!		

Nu geldt r_n =ggd(m,n). Immers, r_n is een deler van r_{n-1} en dus (bekijk de voorlaatste deling!) van r_{n-2}, en dus van r_{n-3}, enz...en dus ook van n en m. M.a.w. r_n is een gemeenschappelijke deler van m en n.
Als d op zijn beurt een gemeenschappelijke deler is van m en n, dan moet d ook een deler zijn van r_1 (bekijk de eerste deling), en bijgevolg van r_2 enz..., en tenslotte ook van r_n.

In de kolom rechts hierboven tonen we dat de gevonden grootste gemene deler r_n uiteindelijk, door het bijhouden van de opeenvolgende quotiënten, geschreven zal kunnen worden in de vorm $a.n + b.m$, voor zekere gehele getallen a en b.

Voorbeeld 1.3.13 We bepalen ggd$(98, 34)$. In de meest rechtse kolom herschrijven we de laatst gevonden rest steeds als lineaire combinatie van de oorspronkelijke deler en deeltal.

Stap 1.	$98 = 2.34 + 30$	$30 = 98 - 2.34$
Stap 2.	$34 = 1.30 + 4$	$\begin{aligned} 4 &= 34 - 1.30 \\ &= 34 - (98 - 2.34) \\ &= 3.34 - 98 \end{aligned}$
Stap 3.	$30 = 7.4 + 2$	$\begin{aligned} 2 &= 30 - 7.4 \\ &= 98 - 2.34 - 7.(3.34 - 98) \\ &= 8.98 - 23.34 \end{aligned}$
Stap 4.	$4 = 2.2 + 0$	

BESLUIT

$\text{ggd}(98, 34) = 2$

$2 = 8.98 - 23.34$

Oefeningen.

1. Welk is de grootst mogelijke grootste gemene deler van 6 verschillende natuurlijke getallen van 2 cijfers?

   (V.W.O. 00-01, 2de ronde, vraag 19)

2. Bewijs dat $\forall n \in \mathbb{N}: \text{ggd}(35n + 57, 45n + 76) = 1$ of 19.

3. Bewijs dat voor elke $n \in \mathbb{Z}$ de getallen $5n + 3$ en $7n + 4$ onderling ondeelbaar zijn.

4. Bewijs dat, als $\text{ggd}(a, b) = 1$, dan $\text{ggd}(a + b, a - b) = 1$ of 2.

5. Bewijs dat, als $\text{ggd}(a, b) = 1$, dan $\text{ggd}(a + b, a^2 - ab + b^2) = 1$ of 3.

6. Hoeveel koppels gehele getallen (n, k) bestaan er met de eigenschap dat $1 = 3n + 5k$?

   (V.W.O. 95-96, 2de ronde,vraag 16)

7. Beschouw de vergelijking $6x - 9y = k$ met $k \in \mathbb{N}$. Voor hoeveel waarden van k $(k < 90)$ heeft deze vergelijking oplossingen die behoren tot $\mathbb{Z}$?

   (V.W.O. 01-02, 1e ronde, vraag 26)

8. Het natuurlijk getal n is het kleinste dat bij deling door 2 rest 1, bij deling door 3 rest 2, bij deling door 4 rest 3, bij deling door 5 rest 4 en bij deling door 6 rest 5 oplevert. Waaraan is de rest bij deling van n door 7 gelijk?

   (V.W.O. 03-04, 2de ronde, vraag 14)

Priemgetallen zijn natuurlijke getallen die men niet "echt" kan ontbinden in factoren. Dat bleek reeds in de definitie. Dit blijkt nogmaals uit de volgende eigenschap van deze getallen:

Stelling 1.3.14 Zij p een priemgetal en $a, b \in \mathbb{N}$. Dan geldt

$$p \mid a.b \Rightarrow p \mid a \text{ of } p \mid b$$

Bewijs: Stel dat p geen deler is van a. Dan geldt $\text{ggd}(p,a) = 1$. Dus volgt uit 1.3.12 dat, voor zekere gehele getallen x en y

$$1 = xp + ya.$$

Hieruit volgt dan

$$b = 1.b = (xp + ya).b = xpb + yab.$$

Nu is p deler van beide termen in het rechterlid en dus ook van b.
Analoog bewijst men dat, als p geen deler is van b, dan p een deler is van a.

Q.E.D.

Priemgetallen vormen de "bouwstenen" voor alle natuurlijke getallen, zoals blijkt uit de volgende belangrijke

Stelling 1.3.15 (De Hoofdstelling van de Getaltheorie.)
Elk natuurlijk getal, verschillend van 0 en 1, kan geschreven worden als product van priemgetallen. Op de volgorde van de priemfactoren na, is deze ontbinding uniek.

Bewijs: We bewijzen eerst het bestaan van een priemfactorontbinding. Hiervoor gebruiken we een redenering door volledige inductie. Het kleinste natuurlijk getal strikt groter dan 1 is 2. 2 is een priemgetal en dit bewijst de factorisatie voor 2. Onderstel dat a een willekeurig natuurlijk getal is, strikt groter dan 1; onderstel tevens dat een priemfactorisatie bestaat voor alle natuurlijke getallen vanaf 2 tot en met $a-1$. Onderzoek de delers van a en kies een echte deler, b.v. d, van a. Als dit niet mogelijk is, is a priem en is er niets aan te tonen. Zowel voor d als voor $\frac{a}{d}$ bestaat, dank zij de inductiehypothese, een priemfactorisatie. Dus kan a ook ontbonden worden in priemfactoren.
Ook de uniciteit (op de volgorde na) van deze priemfactorisaties kan aangetoond worden door inductie, nu op het aantal priemfactoren. Als a een priemgetal is, is de factorisatie duidelijk uniek. Stel dat a geen priemgetal is en stel dat alle priemfactorisaties bestaande uit minder dan n priemgetallen op de volgorde na uniek zijn. Onderstel dat we twee priemfactorisaties hebben voor a; b.v.

$$a = p_1.p_2.\ldots.p_n = q_1.q_2.\ldots.q_t.$$

p_1 deelt het product $q_1.q_2.\ldots.q_t$, en dus één van de factoren van dat product; b.v. $p_1 \mid q_i$. Dit impliceert dat $p_1 = q_i$ en dus dat $p_2.p_3.\ldots.p_n = q_1.q_2.\ldots.q_{i-1}.q_{i+1}.\ldots.q_t$. Door het toepassen van de inductiehypothese volgt dat $n = t$ en dat de priemfactorisaties dezelfde zijn op de volgorde van de priemgetallen na.

Q.E.D.

Gevolg 1.3.16 Er zijn oneindig veel priemgetallen.

Bewijs: Onderstel dat er slechts eindig veel priemgetallen zijn, en dat we die dus kunnen opsommen als $p_1, p_2, \ldots, p_k$. Vorm nu het getal $n = p_1.p_2.p_3.\ldots.p_k + 1$. De stelling leert dat n geschreven moet kunnen worden als product van priemfactoren (m.a.w. als een product van getallen uit $\{p_1, p_2, p_3, \ldots, p_k\}$). Het is duidelijk dat dit tot een contradictie leidt, vermits 1 door geen enkele van die priemfactoren gedeeld wordt.

Q.E.D.

Door het daadwerkelijk opstellen van de priemfactorontbinding van verschillende natuurlijke getallen wordt de betekenis van deze stelling geoefend. Deze stelling opent ook nieuwe mogelijkheden: b.v.

- voor het bepalen van grootste gemene delers en kleinste gemene veelvouden.
- voor het bepalen van het totaal aantal delers van een gegeven getal.

- voor het gebruik in het kader van (zeer elementaire) deelbaarheidstesten; eventueel voor het opstellen van deelbaarheidstesten.

Voorbeeld 1.3.17

- $\text{ggd}(180, 72) = 36$.
  Immers, $180 = 2.2.3.3.5$ en $72 = 2.2.2.3.3$; bijgevolg is hun grootste gemene deler gelijk aan $2.2.3.3 = 36$.
- $\text{kgv}(224, 42) = 672$
  Omdat $224 = 2.2.2.2.2.7$ en $42 = 2.3.7$ vinden we het kleinste gemeen veelvoud als $2.2.2.2.2.3.7 = 672$.
- Hoeveel delers heeft 180 (in $\mathbb{N}$)? De priemfactorontbinding van 180 is gegeven als

  $$180 = 2^2.3^2.5.$$

  Elke deler d van 180 moet bijgevolg van de vorm

  $$d = 2^\alpha.3^\beta.5^\gamma$$

  zijn, waarin $\alpha, \beta \in \{0, 1, 2\}$ en $\gamma \in \{0, 1\}$. Er zijn bijgevolg $3.3.2 = 18$ mogelijkheden. Elk van deze mogelijkheden levert (omwille van de uniciteit van een priemfactorontbinding) een verschillende deler van 180 op.

Oefeningen.

1. Schrijf 37800 als een product van priemgetallen.
2. Bepaal via ontbinding in priemfactoren $\text{ggd}(235, 124)$.
3. Bepaal het aantal delers in $\mathbb{N}$ van 2^n $(n \in \mathbb{N})$.
4. Bepaal het aantal delers in $\mathbb{N}$ van het natuurlijk getal n waarvan de priemfactorontbinding gegeven is door
   $$n = p_1^{a_1}.p_2^{a_2}.\ldots.p_k^{a_k}?$$
5. Als a en b deler zijn van c en als $\text{ggd}(a, b) = 1$, toon dan aan dat $a.b$ ook een deler is van c.
6. Bewijs volgende eigenschap : $\forall a, b, c \in \mathbb{N}_0 : \text{ggd}(ab, ac) = a \cdot \text{ggd}(b.c)$
7. Waaraan is de grootste gemene deler van 878787878787 en 787878787878 gelijk?

   (V.W.O. 00-01, 2de ronde, vraag 9)

8. Waaraan is de rest bij deling van 1991! door 1992 gelijk?

   (V.W.O.91-92,1e ronde,vraag 3)

9. Als k het kleinste natuurlijk getal verschillend van nul is zodat $k!$ deelbaar is door 1000, waaraan is dan de som van de cijfers van k gelijk?

   (V.W.O. 93-94, 1e ronde, vraag 26)

10. Hoeveel verschillende uitkomsten kunnen we verkrijgen door twee willekeurige (verschillende) getallen van de verzameling $\{4, 8, 9, 16, 27, 32, 64, 81, 243\}$ te vermenigvuldigen?

    (V.W.O. 94-95, 1e ronde, vraag 14)

11. Voor hoeveel verzamelingen (met 3 elementen) $\{a,b,c\} \subset \mathbb{N}_0$ is het waar dat $a \cdot b \cdot c = 2310$?

(V.W.O. 94-95, 2de ronde, vraag 26)

12. Noem n het kleinste element van $\mathbb{N}_0$ waarvoor het product $1260 \cdot n$ de derdemacht is van een natuurlijk getal, dan is
(A) $n < 100$ (B) $100 < n < 500$ (C) $500 < n < 1000$ (D) $1000 < n < 5000$ (E) $5000 < n$.

(V.W.O. 95-96, 1e ronde, vraag 4)

13. Hoeveel natuurlijke getallen n bestaan er $(0 \leq n \leq 1996)$ zodat $\sqrt[3]{96n}$ een natuurlijk getal is?

(V.W.O. 95-96, 2de ronde, vraag 10)

14. Het kleinste natuurlijk getal met juist 15 delers behoort tot het interval
(A) $]0,50]$ (B) $]50,100]$ (C) $]100,150]$ (D) $]150,200]$ (E) $]200,250]$

(V.W.O. 99-00, 2de ronde, vraag 14)

15. Op hoeveel nullen eindigt het product van $15^6, 28^5$ en 55^7?

(V.W.O. 01-02, 1e ronde, vraag 4)

16. Bepaal de kleinste waarde van n waarvoor $n!$ deelbaar is door 2002

(V.W.O. 01-02, 2de ronde, vraag 2)

17. Over het getal $N = 2^{10} \cdot 10^2$ worden volgende uitspraken gedaan :
I. N is deelbaar door 5.
II. N is niet deelbaar door 25.
III. N is deelbaar door 40.
IV. N is niet deelbaar door 50.
Hoeveel van deze uitspraken zijn juist?

(V.W.O. 02-03, 1e ronde, vraag 14)

18. Door welk getal is het product $26 \cdot 38 \cdot 51 \cdot 55 \cdot 56 \cdot 107$ niet deelbaar?
(A) 9 (B) 17 (C) 32 (D) 66 (E) 190

(J.W.O. 03-04, 1e ronde, vraag 20)

In deze contekst komen ook een aantal deelbaarheidscriteria aan bod: aan de hand van de priemfactorontbinding van een getal kunnen die criteria dan gecombineerd worden tot eventuele nieuwe testen.

Voorbeeld 1.3.18

- Een geheel getal is deelbaar door 2 (is even) als en slechts als het eindigt op 0, 2, 4, 6 of 8 (of, equivalent, als en slechts als het laatste cijfer van het getal deelbaar is door 2).

- Een geheel getal is deelbaar door 4 als en slechts als het getal gevormd door de laatste twee cijfers deelbaar is door 4.
- Een geheel getal is deelbaar door 3 als en slechts als de som van de cijfers van dat getal deelbaar is door 3.
- Een geheel getal is deelbaar door 5 als en slechts als het eindigt op 0 of 5.
- Een geheel getal is deelbaar door 9 als en slechts als de som van de cijfers van dat getal deelbaar is door 9.
- Een geheel getal is deelbaar door 6 als en slechts als het deelbaar is door 2 en deelbaar is door 3.

Oefening. Bewijs de correctheid van deze testen.

1.4 Modulorekenen.

De introductie van restklassen modulo n en vooral van bewerkingen met deze restklassen is een cruciale stap in de algebra. Voor onze toepassingen en voorbeelden in de contekst van codeerproblemen is dit van vrij groot belang.
Kiezen we nu even een vast natuurlijk getal $n \neq 0$ en veralgemenen we één van de voorbeelden uit 1.1.3 :

$$\mathcal{R} = \{(a,b) \in \mathbb{Z}^2 \parallel n \mid a-b\} \ (n \in \mathbb{N}_0)$$

We gaan na dat deze relatie een equivalentierelatie is :

1. $\mathcal{R}$ is reflexief : $\forall a \in \mathbb{Z} : a\mathcal{R}a$ want $n \mid a-a=0$.
2. $\mathcal{R}$ is symmetrisch : als $a\mathcal{R}b$, dan $n \mid a-b$, maar dan ook $n \mid b-a$ en derhalve $b\mathcal{R}a$.
3. $\mathcal{R}$ is transitief :

   Gegeven : $a,b,c \in \mathbb{Z}$; $a\mathcal{R}b$; $b\mathcal{R}c$.

   Te bewijzen : $a\mathcal{R}c$

   Bewijs : Uit het gegeven volgt dat $n \mid a-b$ en $n \mid b-c$. Maar dan volgt uit eigenschap 1.3.3 dat $n \mid (a-b)+(b-c)$ of dat $n \mid a-c$. Bijgevolg $a\mathcal{R}c$.

Definitie 1.4.1 Twee gehele getallen a en b noemen we congruent modulo n als en slechts als $(a,b) \in \mathcal{R}$, m.a.w. als $n \mid a-b$ (in woorden: als en slechts als $a-b$ een n-voud is).

Notatie 1.4.2 $a \equiv b \bmod n$

Deze equivalentierelatie geeft dus, zoals gezien in eigenschap 1.1.10, aanleiding tot een partitie van $\mathbb{Z}$: de equivalentieklassen worden restklassen modulo n genoemd: immers,

Eigenschap 1.4.3 Twee gehele getallen a en b behoren tot dezelfde equivalentieklasse als en slechts als a en b dezelfde rest hebben bij Euclidische deling door n.

Bewijs: Enerzijds, als a en b dezelfde rest hebben bij Euclidische deling door n, dan geldt

$$a = q_1.n + r \text{ en } b = q_2.n + r \text{ met } 0 \leq r < n.$$

Bijgevolg $a-b = (q_1-q_2)\cdot n$ en dus $n \mid a-b$ of $a \equiv b \bmod n$. Derhalve behoren a en b tot dezelfde equivalentieklasse.
Anderzijds, onderstel dat a en b tot dezelfde equivalentieklasse behoren, m.a.w. dat $a \equiv b \bmod n$ of equivalent dat $n \mid a-b$. Deel nu a en b door n; dit leidt tot

$$a = q_1.n + r_1 \text{ en } b = q_2.n + r_2 \text{ met } 0 \leq r_1, r_2 < n.$$

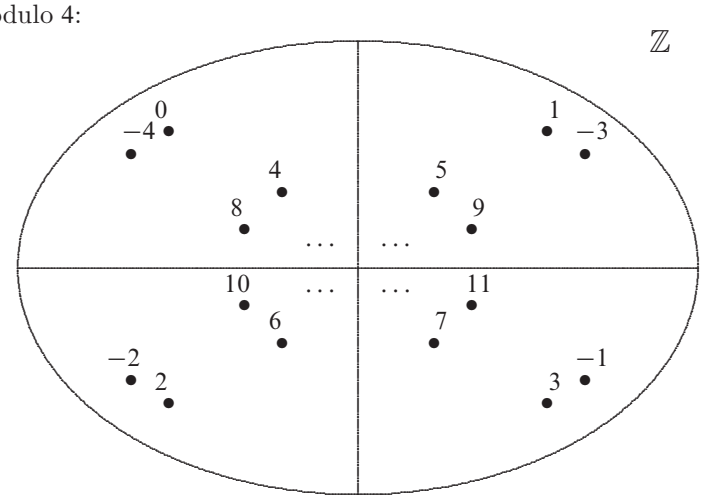
Dan volgt dat $a-b=(q_1-q_2).n+(r_1-r_2)$. Uit de onderstelling en eigenschap 1.3.3 volgt nu dat $n \mid r_1-r_2$. Omdat r_1 en r_2 allebei positief en strikt kleiner dan n zijn, kan dit enkel als $r_1-r_2=0$ of als $r_1=r_2$.

Q.E.D.

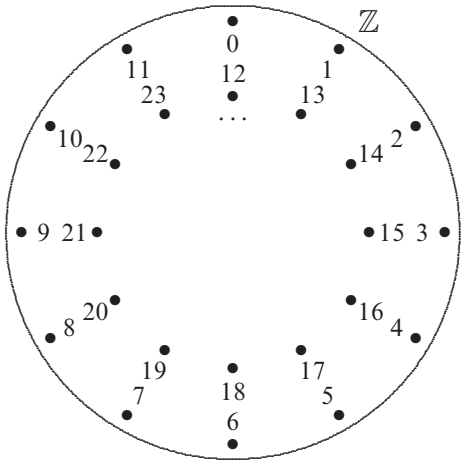
We stellen de restklassen modulo n voor, als $n=4,12,9,0$:

Voorbeeld 1.4.4

De restklassen modulo 4:



De restklassen modulo 12:



Vraag : Vanwaar ken je eigenlijk al restklassen modulo 12?

Restklassen modulo 9: Ga na dat, om te bepalen tot welke restklasse modulo 9 een gegeven natuurlijk getal n behoort, volgende eigenschap geldt : de restklasse modulo 9 van een natuurlijk getal n is gelijk aan de restklasse modulo 9 van het getal dat verkregen wordt door de cijfers (van de tiendelige voorstelling) van n op te tellen. B.v. de restklasse van 2365023 is gelijk aan de restklasse van $2+3+6+5+0+2+3$ en is dus gelijk aan de restklasse van 3 modulo 9.

De restklasse van 0: Voor elk natuurlijk getal n is de restklasse van 0 modulo n precies de deelverzameling van alle n-vouden in $\mathbb{Z}$, m.a.w. $n\mathbb{Z}$. Controleren of een gegeven geheel getal deelbaar is door n (deelbaarheidstest!) komt dus neer op het nagaan of dat getal behoort tot de restklasse van 0 modulo n.

Definitie 1.4.5 Voor elk natuurlijk getal $n \neq 0$, noteren we voortaan $\mathbb{Z}_n$ voor de verzameling van de restklassen modulo n. De restklasse waartoe een gegeven getal $a \in \mathbb{Z}$ behoort, noteren we met $\bar{a}$: we noemen a een representant van die restklasse.

Merk op dat om het even element b van deze restklasse $\bar{a}$ evengoed als representant van $\bar{a}$ kan gekozen worden : immers, uit Lemma 1.1.9 volgt dat, als $b \in \bar{a}$, dan $\bar{a} = \bar{b}$.
Samengevat : $\bar{a} = \bar{b} \Longleftrightarrow a \equiv b \bmod n \Longleftrightarrow n \mid a - b$.

Voorbeeld 1.4.6

1. $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$
2. $\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}\}$
3. $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\} = \{$“de even getallen”, “de oneven getallen”$\}$
4. $\mathbb{Z}_1 = \{\mathbb{Z}\}$
5. Voor elk strikt positief natuurlijk getal n geldt dat $\mathbb{Z}_n$ precies n elementen telt. De getallen 0, 1, ...,$n-1$ zijn als het ware de “standaard”-representanten van de (n) verschillende restklassen modulo n.

Vooraleer we beginnen te rekenen met restklassen, volgt eerst een inleiding op algebraïsche structuren, i.h.b. groepen.

1.5 Groepen

Definitie 1.5.1 Zij X een verzameling. Een afbeelding $\star : X \times X \to X : (x_1, x_2) \mapsto x_1 \star x_2$ noemen we een bewerking op X.

Opmerking : De definitie impliceert dat $\forall x_1, x_2 \in X : x_1 \star x_2 \in X$, m.a.w. dat de bewerking $\star$ inwendig overal bepaald is (I.O.B.) in X.

Oefening: beschouw de gekende getallenverzamelingen $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. Ga na of de optelling, de aftrekking, de vermenigvuldiging en de deling bewerkingen zijn op elk van deze verzamelingen.

Definitie 1.5.2 Een bewerking $\star$ op een verzameling X is associatief als en slechts als

$$\forall a, b, c \in X : a \star (b \star c) = (a \star b) \star c.$$

Een bewerking $\star$ op een verzameling X is commutatief als en slechts als

$$\forall a, b \in X : a \star b = b \star a.$$

Als $\star$ een associatieve bewerking is op X, dan noemen we $(X, \star)$ een halfgroep; als deze bewerking ook commutatief is, dan noemen we $(X, \star)$ een commutatieve of Abelse halfgroep (genoemd naar de Noor Niels Henrik Abel: zie Historische Noot achteraan).

Oefeningen.

1. Welke van de in de vorige oefeningen gevonden bewerkingen leveren samen met de bijhorende verzameling een halfgroep op? Welke halfgroepen zijn ook commutatief?

2. Beschouw de verzameling van alle $n \times n$-matrices met de optelling en met de vermenigvuldiging : zijn dit halfgroepen? Zijn de bewerkingen commutatief?

3. Beschouw de verzameling van alle transformaties van een verzameling X met de samenstelling $\circ$: is dit een halfgroep? Is de bewerking commutatief?

4. We noteren in een halfgroep $(S, \star)$

$$\underbrace{a \star a \star a \star \ldots \star a}_{\text{n keren}} = a^n$$

We merken op dat dit de zgn. multiplicatieve notatie is (als de bewerking b.v. de vermenigvuldiging of de samenstelling is). In de zgn. additieve notatie (als de bewerking de optelling is) krijgen we

$$\underbrace{a + a + a + \ldots + a}_{\text{n keren}} = n \cdot a$$

Onder welke voorwaarde(n) geldt in een (multiplicatieve) halfgroep $(H, \star)$ dat

$$\forall a, b \in H : (a \star b)^n = a^n \star b^n \quad (n \in \mathbb{N} \setminus \{0, 1\})?$$

(Ga na op de vorige voorbeelden) Hoe ziet deze formule er uit in de additieve notatie?

Definitie 1.5.3 Een neutraal element van een halfgroep $(S, \star)$ is een element e van S zodat

$$\forall a \in S : a \star e = e \star a = a$$

Een halfgroep die een neutraal element bevat, wordt een monoïde genoemd.

Eigenschap 1.5.4 Een neutraal element in een monoïde is uniek.

Bewijs : Onderstel dat e en e' neutrale elementen zijn in de monoïde $(S, \star)$; uit vorige definitie met neutraal element e en $a = e'$, volgt dat $e' \star e = e'$. Maar uit dezelfde definitie met e' als neutraal element en $a = e$, volgt dat $e' \star e = e$. Bijgevolg $e = e'$.

Q.E.D.

Oefening. Geef in alle vorige voorbeelden van halfgroepen aan welke monoïden zijn en duid telkens het neutraal element aan.

Definitie 1.5.5 Als $(S, \star)$ een monoïde is met neutraal element e, dan noemen we een element $a \in S$ inverteerbaar als en slechts als

$$\exists b \in S : a \star b = e = b \star a.$$

We noemen b een invers element van a in $(S, \star)$.

Eigenschap 1.5.6 Indien a een invers element heeft in de monoïde $(S, \star)$, dan is dat invers element uniek.

Bewijs : Zij e het neutraal element. Onderstel dat b en b' beide inverse elementen zijn van a, dan

$$\begin{cases} a \star b = e = b \star a & (1) \\ a \star b' = e = b' \star a & (2) \end{cases}$$

Uit (1) volgt dan dat $(b \star a) \star b' = e \star b' = b'$. Uit (2) volgt dat $b \star (a \star b') = b \star e = b$. De associativiteit van $\star$ impliceert dan dat $b = b'$.

Q.E.D.

Notatie 1.5.7 Het invers element van a wordt genoteerd met a^{-1}.

Oefeningen.

1. Duid in alle vorige voorbeelden van monoïden de inverteerbare elementen aan en geef hun invers element.
2. Bewijs : als a inverteerbaar is, dan is a^{-1} dat ook en $(a^{-1})^{-1} = a$.
3. Bewijs : als a en b inverteerbaar zijn , dan is $a \star b$ dat ook en $(a \star b)^{-1} = b^{-1} \star a^{-1}$.
   Let op de volgorde van de factoren in deze uitdrukking. Zoals we 's morgens eerst onze kousen en dan pas onze schoenen aandoen, zo doen we 's avonds eerst onze schoenen en dan pas onze kousen uit.

Definitie 1.5.8 Een groep is een monoïde waarin elk element inverteerbaar is. Als de commutativiteit ook geldt, spreken we van een commutatieve of Abelse groep.

Samengevat: Een groep $(G, \star)$ wordt volledig bepaald door de vier volgende voorwaarden:

1) IOB: $\forall a, b \in G : a \star b \in G$;

2) A: $\forall a, b, c \in G : a \star (b \star c) = (a \star b) \star c$;

3) NE: $\exists e \in G : \forall a \in G : a \star e = e \star a = a$;

4) IE: $\forall a \in G : \exists b \in G : a \star b = e = b \star a$.

Het is opmerkelijk dat heel de groepentheorie, die veel belangrijke resultaten omvat en die nog lang niet volledig geëxploreerd is, uiteindelijk slechts op deze vier axioma's steunt.

Oefeningen.

1. Duid in alle vorige voorbeelden van monoïden aan welke groepen zijn.
2. Geef twee deelverzamelingen van $\mathbb{R}$ die met het product een groep vormen.
3. Als X een verzameling is en $\mathcal{S}(X)$ is de verzameling van alle permutaties van X, bewijs dan dat $(\mathcal{S}(X), \circ)$ een groep is. In het geval dat X een eindige verzameling is met $\sharp X = n$, wordt deze groep genoteerd met $(\mathcal{S}_n, \circ)$: hoeveel elementen telt deze groep dan?
4. Stel elk element van $(\mathcal{S}_3, \circ)$ voor d.m.v. een graaf en noem deze elementen Id,a,b,c,d,e (de volgorde heeft geen belang). Vul nu volgende tabel verder aan :

$\circ$	Id	a	b	c	d	e
Id						
a						
b						
c						
d						
e						

   Het element b.v. in de derde rij en de vierde kolom stelt $a \circ b$ voor. We noemen dergelijke tabel een Cayley-tabel (genoemd naar de Brit Arthur Cayley: zie Historische Noot achteraan).
5. Bewijs dat $(\{f_{ab} : \mathbb{R} \to \mathbb{R} : x \mapsto ax + b \mid a, b \in \mathbb{R}, a \neq 0\}, \circ)$ een groep is (de 1-dimensionale affiene groep). Leid formules af voor de samengestelde van twee dergelijke functies en voor het invers element van zo'n functie.
6. Bewijs dat de verzameling van alle reguliere $n \times n$-matrices, $\mathrm{GL}(n, \mathbb{R})$, met het product een groep vormt (the general linear group of order n).

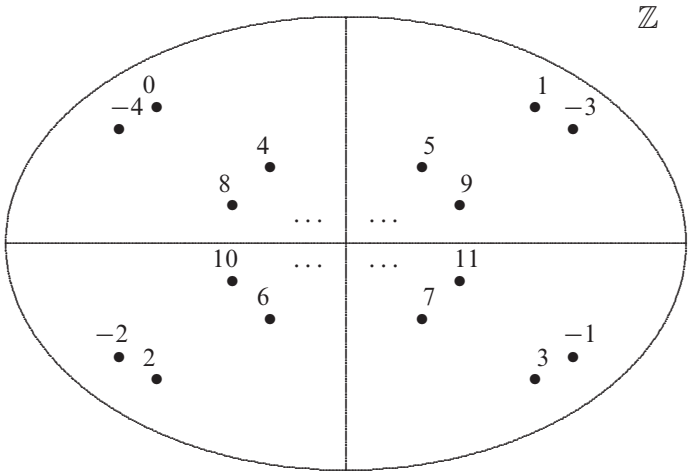
Alle groepen, behalve de symmetriegroep uit voorbeeld 4 hiervoor, hebben oneindig veel elementen; in het volgende deel maken we kennis met heel belangrijke eindige groepen.

1.6 Rekenen met restklassen

Na de "ontdekking" van de restklassen is de constructie van de verzameling van de restklassen modulo n een eerste moeilijke stap; inderdaad, de overstap waarbij "restklassen modulo n" als elementen van een nieuwe verzameling $\mathbb{Z}_n$ genomen worden, vergt enige gewenning en is een niet alledaagse abstrahering.
Dit wordt wellicht nog iets meer geaccentueerd wanneer men voorstelt om met de elementen van die nieuwe verzameling $\mathbb{Z}_n$ te gaan "rekenen".
Wie rekenen zegt, denkt aan bewerkingen. De voor de hand liggende (en gekende) bewerkingen met gehele getallen zijn de optelling (+) en het product (.).
Het idee om deze bewerkingen als "uitvalsbasis" te nemen om er bewerkingen op $\mathbb{Z}_n$ mee te maken lijkt aanvaardbaar en het proberen waard.

1.6.1 Optellen van restklassen modulo n.

Laat ons de optelling in $\mathbb{Z}$ als uitgangspunt nemen voor een nieuwe bewerking in $\mathbb{Z}_n$. We nemen als voorbeeld $\mathbb{Z}_4$.



Willen we twee restklassen modulo 4 "optellen", dan moeten we onvermijdelijk terugvallen op de elementen van die restklassen en op de optelling, in $\mathbb{Z}$, van die elementen.
Zoals opgemerkt na definitie 1.4.5, kan elk element van zo een restklasse als representant van de gehele klasse optreden.
Opdracht : Neem een willekeurige representant van de restklasse waartoe 2 behoort en een willekeurige representant van de restklasse waartoe 3 behoort. Tel beide op (in $\mathbb{Z}$). Tot welke restklasse behoort de som?
Probleem : als je andere representanten voor dezelfde restklasse neemt, zullen de berekende sommen (in $\mathbb{Z}$) dan wel een unieke restklasse bepalen?
Als dat niet zo is, dan ontstaat er een groot probleem. We worden hier geconfronteerd met het probleem van de "onafhankelijkheid van de representanten" voor de definitie van een optelling in $\mathbb{Z}_n$.
We tonen aan

Eigenschap 1.6.1 Als $\bar{a} = \bar{a'}$ en $\bar{b} = \bar{b'}$, dan $\overline{a+b} = \overline{a'+b'}$
of, equivalent,
als $a \equiv a' \bmod n$ en $b \equiv b' \bmod n$, dan $(a+b) \equiv (a'+b') \bmod n$.

Bewijs:

$$\left.\begin{array}{l} a \equiv a' \bmod n \Leftrightarrow n \mid (a'-a) \\ b \equiv b' \bmod n \Leftrightarrow n \mid (b'-b) \end{array}\right\} \overset{1.3.3}{\Rightarrow} \quad n \mid (a'+b'-(a+b))$$

$$\Rightarrow \quad (a'+b') \equiv (a+b) \bmod n.$$

Q.E.D.

Pas nu kunnen we –terecht– besluiten met een goed geformuleerde

Definitie 1.6.2 In $\mathbb{Z}_n$ wordt een optelling + gedefinieerd als volgt: voor elke twee elementen $\bar{a}$, $\bar{b} \in \mathbb{Z}_n$,

$$\bar{a} + \bar{b} = \overline{a+b}.$$

Nu we zeker zijn dat de nieuwe bewerking + goed gedefinieerd is, is het makkelijk na te gaan dat

Stelling 1.6.3 $(\mathbb{Z}_n, +)$ is een commutatieve groep.

Voorbeelden 1.6.4 We maken een Cayley-tabel voor $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_5$ met de optelling :

$\mathbb{Z}_2, +$

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\mathbb{Z}_4, +$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\mathbb{Z}_5, +$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Oefening. Maak de Cayley-tabellen voor + in $\mathbb{Z}_{12}$ en voor $\mathbb{Z}_{24}$. Herken je in de resultaten de "uur"-bewerkingen?

1.6.2 Vermenigvuldigen van restklassen modulo n.

In een volgende stap onderzoeken we of een analoge redenering mogelijk is om een "product" in te voeren in $\mathbb{Z}_n$.
We verifiëren

Eigenschap 1.6.5 Als $\bar{a} = \bar{a'}$ en $\bar{b} = \bar{b'}$, dan $\overline{a.b} = \overline{a'.b'}$
of, equivalent,
als $a \equiv a' \bmod n$ en $b \equiv b' \bmod n$, dan $a.b \equiv a'.b' \bmod n$.

Bewijs:

$$\left.\begin{array}{l} a \equiv a' \bmod n \Leftrightarrow n \mid (a'-a) \\ b \equiv b' \bmod n \Leftrightarrow n \mid (b'-b) \end{array}\right\} \overset{1.3.3}{\Rightarrow} n \mid (a'-a).(b'-b)$$

Nu geldt

$$(a'-a).(b'-b) = a'.b' - a.b - b(a'-a) - a(b'-b),$$

en dus geldt, door gebruik te maken van eigenschap 1.3.3, dat

$$n \mid a'.b' - a.b,$$

of m.a.w.

$$a'.b' \equiv a.b \bmod n.$$

Q.E.D.

We kunnen andermaal besluiten met een goed geformuleerde

Definitie 1.6.6 In $\mathbb{Z}_n$ wordt een product $\cdot$ gedefinieerd als volgt: voor elke twee elementen $\bar{a}$, $\bar{b} \in \mathbb{Z}_n$,

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

Oefening. Vul volgende Cayley-tabellen aan :

$\mathbb{Z}_2, \cdot$

.	$\bar{0}$	$\bar{1}$
$\bar{0}$		
$\bar{1}$		

$\mathbb{Z}_4, \cdot$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$				
$\bar{1}$				
$\bar{2}$				
$\bar{3}$				

$\mathbb{Z}_5, \cdot$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$					
$\bar{2}$					
$\bar{3}$					
$\bar{4}$					

(1.1)

Eenmaal wat ervaring opgedaan is en het vertrouwen in de eigen vaardigheid groeit, "vergeet" men de restklasse-notaties en gaat men kortweg a noteren voor $\bar{a} \in \mathbb{Z}_n$. In plaats van te spreken van rekenen met restklassen, spreekt men nu van "rekenen modulo" of "rekenen met congruenties (modulo)".
De "onafhankelijkheid van de representanten" voor de optelling en de vermenigvuldiging modulo n laat zien dat we niet langer met grote getallen in $\mathbb{Z}$ moeten blijven werken, doch veeleer onze toevlucht kunnen zoeken tot kleine representanten van de restklassen. Dit opent onvermoede perspectieven. De eerste toepassingen, vaak reeds heel handig, vindt men in de contekst van deelbaarheidstesten. We illustreren met een paar problemen, die de mogelijkheden van de nieuwe bewerkingen mooi laten blijken.

Voorbeeld 1.6.7

1. Bepaal de rest bij deling door 7 van 73.52? Anders gesteld: tot welke restklasse behoort 73.52? We zoeken dus de kleinste positieve representant van die restklasse.
   Het antwoord is nu vrij snel te vinden (en zonder dit grote product te moeten berekenen in $\mathbb{Z}$), gebruik makend van eigenschap 1.6.5; inderdaad, $73 \equiv 3 \bmod 7$ en $52 \equiv 3 \bmod 7$, zodat $73.52 \equiv 3.3 \equiv 9 \equiv 2 \bmod 7$. Het gevraagde antwoord is dus 2.

2. Is $(2^{15})(14^{40})+1$ deelbaar door 11? Anders gesteld: is het waar dat $(2^{15})(14^{40})+1 \equiv 0 \bmod 11$?
   Opnieuw moeten we niet langer rekenen met "grote" getallen, maar kunnen we zo snel mogelijk reduceren modulo 11. Hier geldt: $2^5 = 32$ en $32 \equiv -1 \bmod 11$. Dus is $2^{15} = (2^5)^3 \equiv (-1)^3 \equiv -1 \bmod 11$. Voor 14^{40} vinden we $14^{40} \equiv 3^{40} \bmod 11$; en verder, $3^{40} = (3^2)^{20} \equiv (-2)^{20} \equiv 2^{20} \equiv 1 \bmod 11$. Bijgevolg vinden we dat
   $$(2^{15})(14^{40}) + 1 \equiv (-1).1 + 1 \equiv 0 \bmod 11.$$

3. Bewijs dat $F_5 = 2^{2^5} + 1$ deelbaar is door 641 (zie 1.3.5).
   Vooreerst, $641 = 640 + 1 = 5 \cdot 2^7 + 1$. Bijgevolg,
   $$5 \cdot 2^7 \equiv -1 \bmod 641.$$
   Uit eigenschap 1.6.5 volgt dan dat
   $$5^4 \cdot 2^{28} \equiv 1 \bmod 641. \quad (1)$$
   Anderzijds, $641 = 625 + 16 = 5^4 + 2^4$. Bijgevolg
   $$5^4 \equiv -2^4 \bmod 641. \quad (2)$$
   Uit (1) en (2) volgt dan dat
   $$-2^{32} \equiv 1 \bmod 641,$$
   of dat
   $$2^{32} + 1 \equiv 0 \bmod 641.$$

4. Een andere toepassing van rekenen met restklassen vinden we in het maken van b.v. "de negen-proef" om een gegeven som of product een extra controle te gunnen. Deze negen-proef combineert de "onafhankelijkheid van de representanten" met het feit dat restklassen modulo 9 heel gemakkelijk kunnen bepaald worden:

   Als $n + m = s$ (in $\mathbb{Z}$), dan geldt ook $n + m \equiv s \bmod 9$.
   Als $n.m = p$ (in $\mathbb{Z}$), dan geldt ook $n.m \equiv p \bmod 9$.

   De negen-proef kan bijgevolg enkel gebruikt worden als ontdekker van fouten, en niet als bewijs voor de correctheid van de gemaakte berekening. Een sluitende negen-proef is enkel een bevestigende indicatie voor de oorspronkelijke bewerking.

Oefeningen.

1. Toon aan dat $4^{2n+1} + 3^{n+2}$ voor alle $n \in \mathbb{N}$ een veelvoud van 13 is. ([11, Oef.I.4, p.3])
2. Als a,b en c positieve gehele getallen zijn en a en b oneven zijn, dan is $3^a + (b-1)^2 c$
   (A) oneven voor alle waarden van c;
   (B) even voor alle waarden van c;
   (C) oneven als c even is; even als c oneven is;
   (D) oneven als c oneven is; even als c even is;
   (E) oneven als c geen drievoud is; even als c een drievoud is.

   (V.W.O. 91-92, 1e ronde, vraag 5)
3. Schrijf alle gehele getallen van 19 tot 92 achtereen en vorm zo een groot geheel getal

   $$N = 19202122 \ldots 909192.$$

   Als 3^k de grootste macht van 3 is die N deelt, waaraan is k dan gelijk?

   (V.W.O. 91-92, 1e ronde, vraag 17)
4. Hoeveel van de volgende zes getallen (met 10 cijfers) zijn deelbaar door 6?

   1515151515 1994001994 2222222224 2333333334 3888888888 9999999999

   (V.W.O. 94-95, 1e ronde, vraag 4)
5. Wat is het laatste cijfer van de volgende som?

   $$S = 1! + 2! + 3! + \ldots + 1995! + 1996!$$

   (V.W.O. 95-96, 2de ronde, vraag 6)
6. Een getal n bestaat uit 7 verschillende cijfers en is deelbaar door elk van zijn cijfers. Welke cijfers kunnen onmogelijk in n voorkomen?

   (V.W.O. 99-00, finale, vraag1)
7. Wat is het laatste cijfer van het product $1 \cdot 3 \cdot 5 \cdot 7 \ldots 2001 \cdot 2003$?

   (V.W.O. 02-03, 2de ronde, vraag 18)
8. Waaraan is de rest van de deling van $(1! + 2! + 3! + 4! + 5! + 6! + 7! + 8! + 9!)^2$ door 5 gelijk?

   (V.W.O. 02-03, 2de ronde, vraag 20)
9. Hoeveel van de volgende getallen zijn deelbaar door 6?

   888 888 8 888 888 88 888 888 888 888 888 8 888 888 888

   (J.W.O. 03-04, 2de ronde, vraag 3)

1.7 Rekenen met restklassen modulo een priemgetal.

Eenmaal enkele Cayley-tabellen voor het product voorhanden, zijn we geneigd na te gaan of we hiermee, analoog aan de situatie voor de som, ook een groepsstructuur aantreffen.
Een aandachtige observator zal heel snel het probleem van "de nul" ontdekken: vermenigvuldigen met nul levert steeds nul op. T.o.v. het product werkt de nul als een "opslorper". Zolang we werken in $\mathbb{Z}_n$ is er voor het product dus geen neutraal element.
Het idee om nul niet te beschouwen en ons te beperken tot $\mathbb{Z}_n \setminus \{\bar{0}\}$ is vrij natuurlijk. Echter, kunnen we ons zo maar beperken tot $\mathbb{Z}_n \setminus \{\bar{0}\}$?
Opnieuw leren voorbeelden ons dat we voorzichtig moeten zijn; immers, kijken we b.v. naar de Cayley-tabel voor $\mathbb{Z}_4, \cdot$ en denken we daarin even de nul weg, dan is het product niet langer een bewerking op $\mathbb{Z}_4 \setminus \{0\}$ ($2.2 \equiv 0 \bmod 4$!). Dit fenomeen – niet-nul elementen met product nul in $\mathbb{Z}_n$ – doet zich frequent voor: zoek enkele andere waarden voor n waarbij dit fenomeen optreedt. Dergelijke elementen noemen we nuldelers. Het fenomeen van de nuldelers doet zich b.v. ook voor bij het vermenigvuldigen van matrices (kun je een voorbeeld hiervan geven?)
In $\mathbb{Z}_2$, $\mathbb{Z}_5$ en $\mathbb{Z}_7$ vinden we geen producten van niet-nul elementen die nul zijn (ga dit na!). Deze voorbeelden laten uiteraard enkel vermoeden dat dit fenomeen afhangt van eigenschappen van n. Inderdaad, we hebben de volgende

Stelling 1.7.1 Als n geen priemgetal is, dan bevat $\mathbb{Z}_n$ nuldelers.
Als n een priemgetal p is, dan is $\mathbb{Z}_p \setminus \{0\}, \cdot$ een commutatieve groep.

Bewijs: Als n geen priemgetal is, dan kan n geschreven worden als product $n = a.b$, met getallen a en b die voldoen aan $1 < a, b < n$. Dit betekent dat a en b beiden niet congruent zijn met nul modulo n, terwijl hun product dat wel is. In $\mathbb{Z}_n$ is het product van a en b dus gelijk aan 0, terwijl a noch b nul zijn (modulo n). Bijgevolg zijn a en b nuldelers in $\mathbb{Z}_n$.

Als n wel een priemgetal is, b.v. $n = p$, dan kiezen we een willekeurig geheel getal a met $1 \leq a < p$. D.w.z. dat a niet congruent is met nul modulo p.
Vorm nu de deelverzameling

$$\{1 \cdot a, 2 \cdot a, 3 \cdot a, 4 \cdot a, \ldots, (p-1) \cdot a\} \subset \mathbb{Z}_p$$

Enerzijds is door stelling 1.3.14 geen enkel element in deze deelverzameling nul modulo p, want p deelt a niet en p deelt evenmin één van de factoren 1, 2, 3, $\ldots$, $p-1$. Dit toont aan dat de vermenigvuldiging inwendig overal bepaald is in $\mathbb{Z}_p \setminus \{0\}$.
Het is duidelijk dat de vermenigvuldiging associatief is en dat $\bar{1}$ het neutraal element is.
Anderzijds zijn alle elementen van die deelverzameling onderling verschillend; immers, stel dat $i.a \equiv j.a \bmod p$. Dan moet $i.a - j.a = (i-j).a \equiv 0 \bmod p$. Dus $p \mid (i-j)a$ en door stelling 1.3.14, $p \mid i-j$ of $p \mid a$. Maar omdat p geen deler is van a, moet p dan wel $i-j$ delen. Zowel i als j zijn positief en strikt kleiner dan p ; $i-j$ kan dus enkel deelbaar zijn door p als $i = j$.
Uit voorgaande volgt dus dat de gegeven verzameling $p-1$ van nul verschillende elementen van $\mathbb{Z}_p$ bevat; dit betekent dat

$$\{1 \cdot a, 2 \cdot a, 3 \cdot a, 4 \cdot a, \ldots, (p-1) \cdot a\} = \{1, 2, 3, 4, \ldots, p-1\} \subset \mathbb{Z}_p.$$

We concluderen dat juist één van de elementen $i.a$ ($1 \leq i \leq p-1$) congruent moet zijn met 1 (modulo p). Elk willekeurig element $a \in \mathbb{Z}_p \setminus \{0\}$ heeft dus een invers voor het product in $\mathbb{Z}_p \setminus \{0\}$.

Q.E.D.

Werken we met congruenties modulo een priemgetal, dan hebben zowel + als . (elk apart) bijzonder mooie eigenschappen waarmee een groepsstructuur verkregen wordt; voegen we hier nog de eenvoudig na te gaan distributiviteit van . t.o.v. + aan toe, dan hebben we alles voorhanden om van het veld $(\mathbb{Z}_p, +, .)$ te spreken.
Is n geen priemgetal, dan is er enkel sprake van de ring $(\mathbb{Z}_n, +, .)$

Opmerking 1.7.2 Stel dat p een priemgetal is en a niet congruent met 0 modulo p. Dan weten we dat $\text{ggd}(a, p) = 1$ (a en p zijn relatief priem). Als toepassing van het algoritme van Euclides (zie 1.3.12) kunnen we dus schrijven:

$$1 = x.a + y.p \quad \text{voor zekere } x \text{ en } y \text{ in } \mathbb{Z}.$$

Hieruit volgt dat

$$x.a = 1 - y.p \quad \text{en dus } x.a \equiv 1 \bmod p.$$

We besluiten dat het algoritme van Euclides ons in staat stelt om de inversen voor het product te berekenen in $\mathbb{Z}_p$.

Enigszins in de ban van het product in $\mathbb{Z}_p$, kan uitgaande van de Cayley-tabellen hierboven, het volgende spelletje gespeeld worden: bepaal voor elke $a \in \mathbb{Z}_p$ de opeenvolgende machten van a.
Oefening. Vul de volgende tabellen in $\mathbb{Z}_5$ en $\mathbb{Z}_7$ aan :

	waarden voor a^r mod 5, per r			
$a \backslash r$	1	2	3	4
0				
1				
2				
3				
4				

	waarden voor a^r mod 7, per r					
$a \backslash r$	1	2	3	4	5	6
0						
1						
2						
3						
4						
5						
6						

Besluit : na verloop van tijd komt voor elk element verschillend van 0, door opeenvolgende machten te nemen, de waarde 1 voor. Alhoewel dit niet voor alle elementen gelijktijdig gebeurt, observeren we in het algemeen dat de $(p-1)$-de macht van een niet nul element congruent met 1 is modulo p.
Het resultaat dat we in de voorbeelden vaststellen blijkt geen toeval te zijn. We eindigen deze paragraaf met een stelling, die dit resultaat algemener bevestigt, en waarvan het belang voor de getaltheorie vandaag nog steeds moeilijk te overschatten is[1].

Stelling 1.7.3 (Kleine stelling van Fermat) Als p een priemgetal is, dan geldt voor elk element $a \in \mathbb{Z}_p \setminus \{0\}$, dat $a^{p-1} \equiv 1 \bmod p$.

Bewijs: als a van nul verschilt in $\mathbb{Z}_p$, dan hebben we reeds vastgesteld dat

$$\{1 \cdot a, 2 \cdot a, 3 \cdot a, 4 \cdot a, \ldots, (p-1) \cdot a\} = \{1, 2, 3, 4, \ldots, p-1\}.$$

Vormen we in beide verzamelingen het product van alle elementen, dan moeten beide resultaten gelijk zijn mod p; d.w.z.

$$(p-1)!.a^{p-1} \equiv (p-1)!$$

Hieruit volgt dat

$$(p-1)!.(a^{p-1} - 1) \equiv 0 \bmod p$$

en bijgevolg, omdat $(p-1)!$ niet congruent is met nul modulo p en omdat er geen nuldelers zijn in $\mathbb{Z}_p$, geldt

$$a^{p-1} \equiv 1 \bmod p.$$

Opmerking: hieruit volgt dat voor alle elementen a die niet nul zijn modulo p, $a^p \equiv a \bmod p$; deze bewering is natuurlijk ook geldig voor $a \equiv 0 \bmod p$ en bijgevolg tref je de kleine stelling van Fermat vaak aan in de vorm

$$\forall a \in \mathbb{Z}_p : a^p \equiv a \bmod p.$$

[1] We verwijzen hier graag naar de voordracht van Prof. H.W.Lenstra jr. n.a.v. de proclamatie van de tiende Vlaamse Wiskunde Olympiade, mei 1995; de voordracht van Prof. Lenstra is verschenen in Wiskunde en Onderwijs.

Toepassing 1.7.4 De kleine stelling van Fermat is nog steeds een gewaardeerde, alhoewel elementaire, priemgetaltest. Dank zij dit resultaat kan echter enkel met zekerheid vastgesteld worden dat een bepaald getal, b.v. n, geen priemgetal is.
Onderstel dat we het getal n willen testen op het priem zijn. Als n priem is, dan moet de stelling van Fermat voldaan is. Als we door het testen van verschillende getallen a, kunnen vaststellen dat dit voor ook maar één a niet het geval is, dan is n geen priemgetal.
Weliswaar bestaan er oneindig veel deelbare getallen n, de zogenaamde Carmichael-getallen (ontdekt in 1912), zodat voor elke a die geen nuldeler is in $\mathbb{Z}_n$, $a^{n-1} \equiv 1 \bmod n$ (uiteraard kan een nuldeler a geen invers hebben in $\mathbb{Z}_n$ - ga dit na - en dus kan ook voor geen enkel natuurlijk getal n, $a^{n-1} \equiv 1 \bmod n$). Het kleinste Carmichael-getal is $561 = 3 \cdot 11 \cdot 17$ en de volgende (tot aan 10000) zijn 1105, 1729, 2465, 2821, 6601 en 8911.

1.8 ICT-toepassingen

1.8.1 Het algoritme van Euclides

Een zeer korte PASCAL-implementatie van dit algoritme (zie p.14) kan als volgt gebeuren:

```
procedure euclides (a,b:integer; var x,y,d:integer);
  begin
    if b=0 then
      begin
           d:=a;
           x:=1;
           y:=0
      end
    else
      begin
           euclides(b, a-b*(a div b),y,x,d);
           y:=y-x*(a div b)
      end
  end;
```

In een PASCAL-programma zorgt de aanroep

```
euclides(a,b,x,y,d)
```

dan ervoor dat van de gehele getallen a en b een grootste gemene deler d berekend wordt, die meteen geschreven kan worden als $d = x.a + y.b$.
Opdracht: ontleed deze implementatie en overtuig je ervan dat dit in elk geval een correct resultaat zal opleveren.

Een implementatie voor het grafisch rekentoestel TI83 of TI84 (eenvoudig aanpasbaar voor andere programmeerbare rekentoestellen) kan er als volgt uitzien:

```
program:euclides
  Prompt A : A → F :  Prompt B : B → G
  If B = 0
  Then
    1 → X : 0 → Y
    Disp "GGD(F,G)=",F
  End
  1 → Q : 0 → P : 0 → U : 1 → T
  While B ≠ 0
    A-iPart(A/B)*B→R
```

```
    Q-iPart(A/B)*P→X
    U-iPart(A/B)*T→Y
    B→A : R→B : P→Q : X→P : T→ U : Y→T
  End
  Q→X : U→ Y
  Disp "DE GGD IS ",A
  Disp "X=",X
  Disp " Y=",Y
```

Indien het programma uitgevoerd wordt, wordt gevraagd een waarde voor A en B in te voeren. Het programma geeft de ggd$(A, B) = d$ en geeft ook X en Y zodat $d = X \cdot A + Y \cdot B$.

Voorbeeld 1.8.1
We illustreren de werking van het vorige algoritme bij een input $A = 4864$ en $B = 3458$: ggd$(4864, 3458) = 38$ en $38 = 4864 \cdot 32 + 3458 \cdot (-45)$. Volgende tabel toont de opeenvolgende stappen van het algoritme :

iPart(A/B)	A-iPart(A/B)	X	Y	A	B	Q	P	U	T
-	-	-	-	4864	3458	1	0	0	1
1	1406	1	-1	3458	1406	0	1	1	-1
2	646	-2	3	1406	646	1	-2	-1	3
2	114	5	-7	646	114	-2	5	3	-7
5	76	-27	38	114	76	5	-27	-7	38
1	38	32	-45	76	38	-27	32	38	-45
2	0	-91	128	38	0	32	-91	-45	128

1.8.2 Modulorekenen

Dit eenvoudig programma, genaamd MODULO, laat toe m.b.v. het grafisch rekentoestel TI83 of TI84 een getal K modulo een getal N te berekenen ($K \in \mathbb{N}, N \in \mathbb{N}_0$).

```
PROGRAM:MODULO
  Prompt K
  Prompt N
  K-N*iPart(K/N)→L
  Disp K, "MODULO",N, "IS",L
```

Oefeningen.

1. Neem $K = 341$ en $N = 5$ en maak een tabel waarin je de opeenvolgende waarden plaatst die het programma berekent voor K, L en N.
2. Neem het getal gevormd door de eerste 10 cijfers van je bankrekeningnummer en bereken dit getal modulo 97. Wat constateer je?
3. Neem $N = 2^{143}$ en achtereenvolgens $K = 5$ en $K = 7$? Wat constateer je? Kan dit? Dit probleem wordt verholpen met het volgende programma dat (grote) machten modulo N kan berekenen.

1.8.3 Machten modulo n

We lassen hier een programma in dat toelaat om m.b.v. het grafisch rekentoestel TI83 of TI84 machten a^k modulo een willekeurig natuurlijk getal n te berekenen.
De meest voor de hand liggende manier om dit te doen is: eerst $a \cdot a$ berekenen, dan $a \cdot a \cdot a$, enz. tot je aan a^k komt; vervolgens deel je a^k door n om de rest te verkrijgen. Dit is in tweevoudig opzicht een slecht idee: eerst en vooral moet je n vermenigvuldigingen uitvoeren, wat veel computertijd

en -geheugen vergt; anderzijds leidt het, zeker bij een grafisch rekentoestel, vlug tot overflow. B.v. $2^{1110} \bmod n$ kan op deze manier niet meer berekend worden.
Een veel efficiëntere manier is gebaseerd op volgende afleiding, gebruik makende van de binaire schrijfwijze van de exponent k:
onderstel dat

$$k = \sum_{i=0}^{t} k_i 2^i, \text{ met } k_i \in \{0, 1\}$$

dan

$$a^k = \prod_{i=0}^{t} a^{k_i 2^i} = (a^{2^0})^{k_0} (a^{2^1})^{k_1} \dots (a^{2^t})^{k_t}.$$

Het programma BINEXP leidt de binaire schrijfwijze van een getal K af :

```
PROGRAM:BINEXP
  Prompt K
  1 → dim(⌊BINR )
  1 → dim(⌊BIN )
  If K = 0
  Then
    Disp "DE BIN.EXP.IS{0}"
  Else
    1 → I
    While iPart(K/2) ≠ 0
      K-2*iPart(K/2)→ ⌊BINR(I)
      iPart(K/2)→K
      I+1→I
    End
    1 → ⌊BINR(I)
    dim(⌊BINR ) → D
    For(J, 0, D − 1)
    ⌊BINR(D − J) → ⌊BIN(J + 1)
  End
  Disp"DE BIN.EXP.IS",⌊BIN
```

Het eindresultaat van dit programma is dat de lijst BIN de binaire expansie van K weergeeft (de lijst BINR, die we in het hiernavolgende programma zullen nodig hebben, geeft ook deze expansie weer, maar in omgekeerde volgorde).

Het programma MACHTMOD berekent nu $A^K \bmod N$:

```
PROGRAM:MACHTMOD
  Prompt A
  prgmBINEXP
  Prompt N
  1 → B
  If K = 0
  Then
    Disp B
  Else
    A → P
    If ⌊BINR(1) = 1
    Then
      A → B
    End
```

```
  For(I,2,dim(⌊BIN))
    P^2 − N ∗ iPart(P^2/N) → P
    If ⌊BINR(I) = 1
    Then
      P ∗ B − N ∗ iPart(P ∗ B/N) → B
    End
  End
Disp B
```

Volgende tabel illustreert de werking van het programma bij de berekening van

$$5^{596} \bmod 1234 = 1013.$$

I	1	2	3	4	5	6	7	8	9	10
$\lfloor$BINR(I)	0	0	1	0	1	0	1	0	0	1
P	5	25	625	681	1011	369	421	779	947	925
B	1	1	625	625	67	67	1059	1059	1059	1013

Oefeningen.

1. Bereken $2^{11111110} \bmod 11111111$.
2. Kun je via de kleine stelling van Fermat en m.b.v. het programma MACHTMOD nagaan of volgende getallen priemgetallen zijn?
   (a) 220987 $(= 191 \cdot 89 \cdot 13)$
   (b) 1473407 $(= 13 \cdot 113 \cdot 59 \cdot 117)$
   (c) 65537
3. Ga m.b.v hetzelfde programma de bewering uit toepassing 1.7.4 na i.v.m. de Carmichael-getallen voor enkele van deze getallen.

1.9 Historische noten

1.9.1 Niels Henrik Abel

In de eerste helft van de negentiende eeuw maakte de Wiskunde een grote ontwikkeling door. Die tijd heeft dan ook veel grote wiskundigen opgeleverd zoals Gauss, Poisson, Cauchy, Jacobi, Dirichlet, Hamilton, Liouville en Galois. Ook de Noorse wiskundige Niels Henrik Abel leefde in die tijd. In zijn korte leven heeft hij veel belangrijke wiskundige ontdekkingen gedaan en dat hadden er nog veel meer kunnen zijn als niet bijna alles in zijn leven hem zo tegenzat. Zo leefde hij in Noorwegen, een land dat niet bepaald het Walhalla van de Wiskunde was en moest hij Duits en Frans leren voordat hij met de grote Wiskundigen uit zijn tijd kon corresponderen. Verder is Abel altijd zeer arm geweest en daarnaast was hij ook nogal schuchter, wat niet in positieve zin aan zijn Wiskundige productiviteit heeft bijgedragen.
Niels Henrik Abel werd geboren op 5 augustus 1802 op Finnoy, een eilandje vlakbij Stavanger. Hij was het derde kind van dominee SØren Georg Abel en diens vrouw Anne Marie, die daarna nog vier kinderen zouden krijgen. Het gezin was erg arm, hoewel SØren redelijk veel invloed binnen Noorwegen had. Zo werkte hij in 1814 mee aan het schrijven van een nieuwe Noorse grondwet. Echter, SØren dronk nogal veel, terwijl zijn vrouw een 'lage moraal' gehad schijnt te hebben. Desondanks slaagden ze erin een gezin van zeven kinderen te onderhouden.
Inmiddels verhuisd naar Gjerstad, genoot Abel de eerste jaren van zijn leven thuisonderwijs, totdat hij op 13-jarige leeftijd werd toegelaten tot de Cathedral School in Kristiania, het tegenwoordige Oslo. Deze school had juist daarvoor veel leraren verloren aan de pas opgerichte universiteit van Oslo. Onder deze omstandigheden presteerde Abel de eerste jaren niet bijster veel. Hier kwam verandering in nadat zijn Wiskunde-docent was ontslagen, na een leerling zodanig te hebben gestraft, dat deze aan de gevolgen daarvan overleed.
Zijn vervanger was de nog jonge Brent Michael Holmboe, een assistent van Christopher Hansteen aan de universiteit. Beide mannen werden al snel goede vrienden van Abel en zouden een belangrijke invloed op zijn leven heben. Holmboe zag Abels wiskundige talenten al snel in en daagde hem uit door nieuwe problemen en boeken aan te dragen, zoals Gauss' boek 'Disquitiones', waarin hij enkele hiaten in bewijzen van stellingen wist op te vullen. Al gauw waren de rollen omgedraaid en was het Abel die Holmboe onderwees. In 1817, vlak na zijn aantreden schreef Holmboe over Abel : "hij is een wiskundig genie", een jaar later werd dat al : "nog tijdens zijn leven zal hij een groot Wiskundige worden". Deze laatste woorden waren doorgestreept, waarschijnlijk heeft daar iets als "de allergrootste Wiskundige" gestaan.
In 1820 werd de situatie voor Abel nog slechter, omdat zijn vader overleed. Abel kreeg nu de zware taak op zijn schouders om zijn moeder, broers en zussen te onderhouden. Dat was geen gemakkelijke zaak, want de dranklust van zijn vader had de familie geruïneerd. Er was geen geld meer voor Abel om zijn school af te maken, laat staan om naar de universiteit te gaan. Holmboe hielp Abel echter aan een beurs om op school te blijven en in 1821 kon hij naar de universiteit gaan. Daar kreeg hij les van Hansteen, die eigenlijk professor in de astronomie was. Hansteen steunde Abel ook financieel en zijn vrouw begon voor Abel te zorgen, alsof het haar eigen kind was.
Terwijl hij nog op de middelbare school zat deed Abel een belangrijke ontdekking. Al eeuwen waren wiskundigen op zoek naar een algemene formule om oplossingen van de vijfdegraadsvergelijking ( ) te vinden. Die voor de tweedegraadsvergelijking (de bekende discriminant-formule) was al sinds mensenheugenis bekend en die voor de derde- en vierdegraadsvergelijking waren in de 16e eeuw gevonden door Tartaglia en Del Ferro en door Ferrari. Nu dacht Abel een manier gevonden te hebben om de vijfdegraadsvergelijking op te lossen. Holmboe, die inzag dat er niemand in Noorwegen was, die Abels methode kon begrijpen, adviseerde hem zijn methode op te sturen naar de Deense wiskundige Ferdinand Degen.
In Degens antwoord vroeg deze Abel een numeriek voorbeeld te geven, om zijn methode te demonstreren. Toen Abel dat probeerde, ontdekte hij een fout in zijn methode, later zou hij bewijzen dat het niet mogelijk is een algemene oplossing van de vijfdegraadsvergelijking te geven. Nog belangrijker echter, was het advies dat Degen aan Abel gaf om zich met elliptische integralen bezig

te houden.
In 1823 kreeg Abel een kleine beurs om naar Kopenhagen te gaan, om Degen en andere Wiskundigen te ontmoeten. Behalve Wiskundigen ontmoette hij daar ook Christine Kemp, die al snel zijn verloofde zou worden. Nadat hij weer teruggekeerd was in Kristiania, probeerde hij een beurs te krijgen voor een reis naar Frankrijk en Duitsland, om de grote Wiskundigen uit die tijd te bezoeken. Abel sprak echter geen Frans of Duits, dus hij besloot nog twee jaar in Kristiania te blijven, deels om beide talen onder de knie te krijgen, deels ook om geld uit te sparen.
In deze tijd vond Abel ook het bewijs dat er geen algemene methode is om een vijfdegraadsvergelijking op te lossen. Een dergelijk bewijs was al in 1799 gegeven door de Italiaan Paolo Ruffini (1762-1822), maar dat was door de Wiskundigen nooit aanvaard. Het bewijs van Abel zou dat, hoewel pas later, wel worden. Abel moet het resultaat van Ruffini overigens wel gekend hebben: toen hij nog op school zat, had hij Cauchy's werk uit 1815 bestudeerd, waarin een verwijzig stond naar de resultaten van Ruffini. Hij stuurde zijn resultaten naar verscheidene Wiskundigen, waaronder Gauss, die hij van plan was te bezoeken.
In augustus 1825 kreeg Abel geld van de Noorse regering om door Europa te trekken en een maand later ging hij samen met vier vrienden op reis, allereerst naar Wiskundigen in Noorwegen en Denemarken. In Denemarken kreeg hij te horen dat Degen inmiddels overleden was en hij veranderde zijn plannen om meteen naar Parijs te gaan, zoals Hansteen hem geadviseerd had, en besloot met zijn vrienden mee naar Berlijn te gaan. Abel was nogal schuchter en reisde liever samen. Wanneer hij alleen was, voelde hij zich erg ongelukkig en kon hij zich slecht op de Wiskunde concentreren.
In Berlijn ontmoette hij August Leopold Crelle (1780-1855), een invloedrijke en vermogende constructie-adviseur. Crelle zag al snel de talenten van Abel in en moedigde hem aan een verduidelijkende versie van zijn werk over de vijfdegraadsvergelijking te schrijven. Deze versie verscheen in de eerste editie van Crelle's Journal, samen met nog vier andere verhandelingen van Abel over elliptische functies.
Terwijl hij in Berlijn was, hoorde Abel dat Holmboe benoemd was tot Wiskunde-professor aan de universiteit van Kristiania. Dit was de enige dergelijke functie in Noorwegen en Abel begon zich zorgen over zijn eigen toekomst te maken. Eigenlijk wilde Abel met Crelle naar Berlijn gaan en onderweg Gauss in Göttingen bezoeken. Hij kreeg echter te horen dat Gauss geen interesse had in zijn werk : vermoedelijk omdat hij geen belang hechtte aan het oplossen van algebraïsche vergelijkingen, hoewel hij Abels werk nooit heeft gelezen. In 1801 schreef Gauss echter dat "de oplossing van een algebraïsche vergelijking niet méér voorstelt dan een symbool definiëren voor de oplossing van de vergelijking en vervolgens zeggen dat de oplossing en het symbool gelijk aan elkaar zijn."
Crelle moest echter in Berlijn blijven en kon dus niet naar Parijs gaan. Abel besloot derhalve met zijn vrienden mee te reizen naar Italië alvorens naar Parijs te gaan. In Parijs bleek er weinig belangstelling voor zijn werk. Hij bleef een paar maanden in Parijs, werkte aan zijn resultaten uit Crelle's Journal en ontmoette Wiskundigen als Cauchy en Legendre, die hij verschillende artikelen van zijn hand gaf.
Vanwege zijn slechte gezondheid en zijn steeds groter wordende geldzorgen besloot hij terug naar Berlijn te gaan, waar hij wat geld leende om van te kunnen leven. Crelle probeerde Abel over te halen in Berlijn te blijven, tot hij een baan voor hem aan de universiteit van Berlijn had gevonden. Abel besloot echter terug naar Kristiania te gaan, waar hij in mei 1827 aankwam.
Hij leende hier wat geld van de universiteit, met de belofte dat het ingehouden zou worden van een eventueel later salaris. Daarnaast gaf Abel les aan schoolkinderen. Zijn verloofde Christine ging als gouvernante werken in Froland bij vrienden van de familie Abel. De situatie werd iets beter toen Hansteen naar Siberië vertrok om onderzoek te doen naar het magnetisch veld van de aarde en Abel zijn positie aan de universiteit kon innemen.
In 1828 kreeg Abel een artikel onder ogen van de Duitser Carl Gustav Jacobi (1804-1851) over transformaties van elliptische integralen. Abel zag overeenkomsten met zijn eigen werk en werkte verder aan Jacobi's resultaten. Daarnaast deed hij ook nog onderzoek naar de oplossingen van algebraïsche vergelijkingen, wat Wiskundigen nu Galoistheorie noemen.
De zomer van 1828 bracht Abel door bij Christine in Froland en ook met kerst van dat jaar ging

hij naar Froland. Op de reis daar naartoe (per slee!) werd Abel erg ziek en hoewel het met kerst iets beter ging, verslechterde zijn toestand daarna snel. Toen Crelle dat hoorde, deed hij extra hard zijn best om een positie voor Abel aan de Berlijnse universiteit te krijgen. En met succes : op 8 april 1829 schreef Crelle naar Abel dat hij een baan voor hem gevonden had. Het mocht echter niet baten : drie dagen daarvoor, in de morgen van 5 april, had Abel zijn laatste adem uitgeblazen.
Na Abels dood werd het artikel dat hij aan Cauchy gegeven had, gevonden. Het verscheen in druk in 1841 maar raakte weer zoek en werd pas in 1952 opnieuw gevonden. Na zijn dood vond men nog enig ongepubliceerd werk over het oplossen van algebraïsche vergelijkingen. Hierin stonden ook enkele resultaten die Galois enige jaren later, overigens onafhankelijk van Abel, bereikte.
Abels invloed op de Wiskunde is groot geweest, wat bijvoorbeeld al te zien is aan de Abelse groep, de naam die meestal aan een commutatieve groep gegeven wordt en die vaak zelfs zonder hoofdletter geschreven wordt. In de Analyse kent men de stelling van Abel over sommeerbare rijen van functies en – naar aanleiding daarvan – spreekt men over Abel-sommen van getalrijen. Ook spreekt men over de integraalvergelijking van Abel. Verder speelde Abel een grote rol in de ontwikkeling van de groepentheorie en in de theorie van algebraïsche vergelijkingen. Hoewel Abel en Galois elkaar nooit ontmoet hebben, hebben deze twee Wiskundigen, van wie de levens zo tragisch waren, een grote rol gespeeld in de ontwikkeling van de Wiskunde en zijn hun werken niet of nauwelijks los van elkaar te zien.
Noorwegen, erkentelijk voor de invloed van het wiskundig werk van Niels Henrik Abel, heeft in 2002 een fonds opgericht, waarmee o.a. vanaf 2003, jaarlijks de ABEL PRIJS wordt uitgereikt. Deze prijs, ter waarde van een Nobel prijs, werd voor het eerst toegekend in 2003, aan Jean Pierre Serre, Professor aan het Collège de France, in Parijs. In 2004 werd deze prestigieuse onderscheiding toegekend aan de Professoren Sir Michael Atiyah (University of Edinburgh) and Isadore Singer (Massachusetts Institute of Technology). Meer hierover, over Niels Henrik Abel en de Abel prijzen, kunt u lezen op http://www.abelprisen.no/ . Een niet te versmaden must!

1.9.2 Arthur Cayley

Wanneer iemand een lijst maakt van de 100 beste Wiskundigen van de negentiende eeuw – algemeen gezien als de eeuw van de Wiskunde –, zal het opvallen dat het grootste deel van de lijst uit Fransen en Duitsers bestaat. Het is vooral verrassend dat er zo weinig Engelsen op een dergelijke lijst staan, zeker wanneer je bedenkt dat in andere wetenschappen Engeland in die tijd wel een voorname rol speelde. Deze achterstand is een rechtstreekse erfenis van een ruzie tussen Newton en Leibniz in de zeventiende eeuw en werd versterkt door oorlogen tussen Engeland en landen van het Europese vasteland. Pas tegen het eind van de negentiende eeuw had de Wiskunde in Engeland eenzelfde niveau als in de rest van Europa bereikt. Eén van de weinige Engelse Wiskundigen die wel met zijn Europese collega's kon wedijveren was Arthur Cayley.
Arthur Cayley werd op 16 augustus 1821 geboren in Richmond, even ten zuidwesten van Londen in Engeland. Hij was de tweede zoon van Henry Cayley en Maria Antonia Doughty, beide afkomstig uit gegoede families. Henry Cayley was een koopman die met Rusland handelde en daarom bracht Arthur de eerste paar jaar van zijn leven grotendeels in Sint-Petersburg door. Toen Arthur acht jaar was, gaf zijn vader het koopmansbestaan op en de familie vestigde zich definitief in Engeland. Arthur ging hier naar een privé-school in Blackheath en later, toen hij veertien was, naar King's College School in Londen. Al vroeg uitte zijn wiskundig talent zich : net als de jonge Gauss was Cayley goed in het doen van lange numerieke berekeningen, die hij vaak ter ontspanning deed. Hij was met grote voorsprong de beste Wiskundige van de klas en zijn leraren zagen een grote toekomst binnen de Wiskunde voor hem weggelegd.
Aanvankelijk was Cayley's vader er erg op tegen dat zijn zoon Wiskunde zou gaan studeren. Het hoofd van de school wist hem echter te overtuigen van de talenten van zijn zoon en zo ging Arthur Cayley in 1838 naar Trinity College in Cambridge, destijds en nog altijd één van Engelands meest prestigieuze universiteiten.
Ook hier was Cayley veruit de beste student. Al tijdens zijn studie publiceerde hij drie artikelen in het kort daarvoor door Gregory opgerichte Cambridge Mathematical Journal. Ook won hij tegen

het eind van zijn studie de Smith's prize, wat hem een beurs opleverde zodat hij na zijn studies voor vier jaar als assistent in Cambridge mocht blijven werken.
Cayley's interesses reikten overigens verder dan louter Wiskunde. Zo hield hij veel van literatuur, met name van inmiddels klassieke schrijvers als Walter Scott en Jane Austin. Daarnaast kon hij ook erg genieten van toneelstukken van Shakespeare. Hij las ook literatuur in andere talen : Cayley sprak vloeiend Frans en ook behoorlijk Duits, Italiaans en Oudgrieks. Dit kwam hem goed van pas tijdens zijn vele reizen door het Europese continent, waar hij lange wandelingen maakte en diverse bergen beklom.
Om een inzicht te krijgen in de situatie waarin de Wiskunde in Engeland zich in de eerste helft van de negentiende eeuw bevond, moeten we terug naar het eind van de zeventiende eeuw. Toen ontstond er een felle discussie tussen Leibniz en Newton over wie de differentiaalrekening had uitgevonden. De Engelse Wiskundigen kozen haast zonder uitzondering partij voor Newton en werden daarom vaak 'fluxies' genoemd, naar Newtons fluxrekening. Zij zagen elke poging om 'continentale' Wiskunde te bedrijven als een soort heiligschennis tegenover Newton. Dit werd nog eens versterkt door de koloniale en Napoleontische oorlogen, toen ook nationalistische principes een rol gingen spelen.
Engelands isolationisme op wiskundig gebied werd in 1812 doorbroken, toen een aantal jonge Wiskundigen in Cambridge, met Babbage en Herschel als bekendsten, pogingen ondernamen om de ideeën van Leibniz ook in Engeland te verspreiden. Zij werden flink tegengewerkt door de oudere generatie Wiskundigen, maar kregen het voor elkaar dat een aantal belangrijke 'continentale' Wiskunde-boeken in het Engels werden vertaald, zodat Engelse Wiskundigen eenvoudiger toegang tot deze Wiskunde zouden krijgen. Toch zou Engeland haar achterstand op wiskundig gebied pas aan het eind van de negentiende eeuw hebben goedgemaakt.
Toen zijn vierjarige aanstelling in Cambridge was afgelopen, lukte het Cayley niet om een baan binnen de Wiskunde te krijgen. Omdat hij toch rond moest komen, besloot hij, zoals veel jonge wetenschappers in een vergelijkbare situatie, advocaat te worden. Zijn opleiding hiertoe rondde hij in 1849 af en hij werkte vervolgnes veertien jaar als advocaat. Hij schijnt hier vrij goed in te zijn geweest, maar heeft het zelf altijd beschouwd als niet méér dan een manier om in leven te blijven. Hij nam dan ook niet méér zaken aan dan nodig. In zijn vrije tijd deed hij veel wiskundig onderzoek : in de jaren waarin hij als advocaat werkte, publiceerde hij zo'n 250 artikelen, meer dan menig beroepswiskundige.
In de jaren waarin hij als advocaat werkte ontmoette Cayley ook James Joseph Sylvester, een andere Wiskundige die net als hijzelf zijn geld in de advocatuur verdiende en net als Cayley in de Lincoln's Inn rechtbank werkte. De in 1814 geboren Sylvester was een Jood en dat maakte het voor hem nog moeilijker een aanstelling te krijgen. Voor zijn afstuderen moest hij naar Dublin gaan, omdat hij in Cambridge een aantal artikelen moest onderschrijven waar volgens de Anglikaanse kerk ieder rationeel denkend mens – lees : iedere gelovige – het mee eens moest zijn. Na zijn afstuderen verbleef hij zelfs korte tijd aan de Universiteit van Virginia in de Verenigde Staten, destijds nog een unicum, maar na een ruzie keerde hij toch weer terug naar Engeland.
Cayley en Sylvester deden samen veel wiskundig onderzoek, met name in de algebraïsche invariantentheorie waarvan zij min of meer als de uitvinders gelden. Enkele voorbeelden van deze theorie, die algebraïsche vergelijkingen bestudeert die invariant blijven onder zeker transformaties, waren al bij Lagrange en Gauss bekend, maar het waren Cayley en Sylvester die ontdekten dat er een hele theorie achter schuilging.
In 1863 lukte het Cayley dan uiteindelijk om een aanstelling als Wiskundige te krijgen: hij werd Sadlerian Professor in de theoretische Wiskunde te Cambridge. Dat betekende weliswaar een flinke achteruitgang in inkomen, maar Cayley was maar wat blij om zich nu fulltime met Wiskunde bezig te houden. In het jaar van zijn aanstelling trouwde hij ook met Susan Moline. Hij was weliswaar al 42 bij zijn trouwen, maar schonk nog wel het leven aan een zoon en dochter.
Cayley's wiskundig onderzoek besloeg een groot deel van de Wiskunde en zelfs van de onderwerpen waar hij zelf niet aan werkte, was hij uitstekend op de hoogte. Veel dingen die in de hedendaagse Wiskunde volkomen ingeburgerd zijn, hebben we aan Cayley te danken. Zo is hij de ontdekker van de n-dimensionale meetkunde en deed hij veel onderzoek in de algebraïsche theorie van matrices : beide onderwerpen bleken van groot belang toen Heisenberg in 1925 de quantummechanica

ontdekte. Ook de formele definitie van 'groep' is van Cayley afkomstig. Groepen als zodanig, en dan met name permutatiegroepen, werden al door Lagrange bestudeerd, maar Cayley gaf als eerste de formele definitie, samen met vermenigvuldigingstabellen van enkele speciale groepen, die daarom ook vaak Cayley-tabellen worden genoemd.
Naast zijn onderzoek moest Cayley enig bestuurswerk binnen de universiteit doen. Hier kwam zijn ervaring als advocaat goed van pas: hij was vrij verlegen en sprak niet veel op vergaderingen, maar als hem iets op het hart lag, kon hij zijn mening vaak met overtuigende argumenten ondersteunen. Het belangrijkste resultaat van zijn bestuurswerk was het feit dat hij ervoor zorgde dat voortaan ook vrouwen in Cambridge mochten komen studeren.
In het voorjaar van 1882 gaf hij enkele colleges aan de John Hopkins University te Baltimore in de Verenigde Staten. Hij kwam hier op uitnodiging van zijn vriend Sylvester die zich, na herhaalde problemen met de Engelse bureaucratie, in 1876 in Baltimore had gevestigd. Maar toen er in 1883 een positie voor hoogleraar in Oxford vrijkwam en men Sylvester vroeg voor deze post, accepteerde hij hem toch. In december van 1885 hield hij – inmiddels 71 jaar oud! – zijn inaugurele rede.
Met Cayley ging het inmiddels steeds slechter. Al op 60-jarige leeftijd werd hij door anderen omschreven als een vriendelijke oude man, die er erg slecht uitzag en zelfs vrij moeilijk sprak. Uiteindelijk zou hij, na een lang ziekbed, op 26 januari 1895 overlijden, 73 jaar oud, twee jaar eerder dan zijn zeven jaar oudere vriend Sylvester.
Cayley's naam leeft tegenwoordig voort in enkele begrippen uit de Algebra en de Discrete Wiskunde, zoals de Stelling van Cayley-Hamilton, die zegt dat een matrix nulpunt is van zijn karakteristieke veelterm. Maar de invloed van Cayley, die sinds 1852 lid was van de Royal Society en van 1868 tot 1870 zelfs voorzitter van de London Mathematics Society, op de Wiskunde is groter dan deze begrippen doen vermoeden. Niet alleen introduceerde hij belangrijke begrippen als n-dimensionale meetkunde en groepen, hij zette de Engelse wiskunde definitief op de plaats die ze nog immer inneemt.

Hoofdstuk 2

@work: van cryptosysteem tot digitale handtekening

2.1 Coderen van informatie.

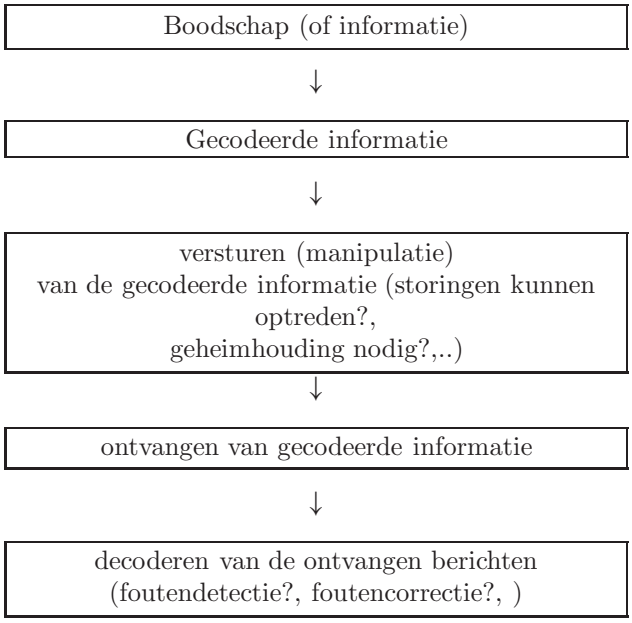
Informatie doorgeven is een op en top menselijke activiteit. Daarvoor moeten we helemaal niet aan heel gesofisticeerde acties denken. Onze moedertaal is een informatiedrager die we van op bijzonder jonge leeftijd aanleren. De woorden en de syntax die we door de jaren heen aanleerden, helpen ons onze bedoelingen of wensen, kortweg onze informatie, kenbaar te maken voor anderen. We coderen deze informatie in een taal die door anderen begrepen wordt; hierdoor wordt ze transporteerbaar. Voor dit overzetten van de informatie – hetzij al sprekende, hetzij al schrijvende, hetzij met een of ander modern medium – is het vaak van groot belang dat dit foutenloos gebeurt.
Bovendien willen we soms al eens iets doorgeven met een eerder vertrouwelijk karakter.
Meteen komen twee aspecten ter sprake die we vandaag willen illustreren, niet zozeer voor wat betreft onze gewone taal, maar veeleer in de contekst van de "informatiemaatschappij" waarin we leven. Een enorm aantal activiteiten heeft te maken met het verhandelen van informatie. We kunnen inderdaad vrijwel niets meer doen in onze samenleving of we ontmoeten één of andere vorm van codering voor die informatie. Denken we maar aan

- een telefoongesprek of de radio beluisteren: de informatie wordt omgezet in signalen of golven die over een zekere afstand getransporteerd worden. Deze signalen kunnen gestoord worden en bijgevolg moeilijk verstaanbare informatie voor de ontvanger opleveren.
- bankverrichtingen gebeuren met behulp van rekeningnummers en persoonlijke codes en via allerlei verbindingen; de minste fout veroorzaakt ongewenste resultaten (foute of onmogelijke transacties). Vele transacties hebben een persoonlijk (vertrouwelijk) karakter.
- bij onze dagelijkse aankopen worden produkten verhandeld die voorzien zijn van een typering in een of andere vorm (streepjescode, produktnummer).

  Dit maakt identificatie en herkomstinformatie (b.v. met het oog op kwaliteitscontrole) mogelijk.
- wanneer we werken met een PC of een CD met muziek beluisteren, wordt de informatie getransporteerd doorheen verschillende media in ons toestel, alvorens wij ermee kunnen werken of ervan kunnen genieten (bestanden worden op een harde schijf gestockeerd, muziek vanop de CD gelezen, ...)

De meeste codeersystemen die tegenwoordig aangewend worden, doen een beroep op technieken uit de rekenkunde, de algebra of gevorderde wiskunde; ze variëren van heel eenvoudig tot bijzonder gesofisticeerd. Vaak wordt gebruik gemaakt van sterk conceptuele resultaten (soms van de

afwezigheid van bepaalde kennis) om het geconstrueerde codeersysteem bepaalde – op voorhand gewenste en goed getypeerde – eigenschappen te geven.
Ten einde meer concreet en in detail kennis te kunnen maken met voorbeelden, vatten we, kort en schematisch, nog even de werking van de meeste codeersystemen samen:



De begrippen codetheorie en cryptografie worden nogal dooreen gebruikt : codetheorie zorgt ervoor dat boodschappen leesbaar blijven, zelfs indien storing optreedt, terwijl cryptografie ervoor zorgt dat boodschappen onleesbaar worden, tenzij voor de ontvanger voor wie de boodschap bestemd is. Deze complementaire technieken blijken op Wiskundig vlak veel gemeen te hebben. Codeertechnieken zijn anderzijds ook in gebruik om informatie te comprimeren, zoals bij foto- of filmmateriaal.

2.2 Modulorekenen : eenvoudige toepassingen

De meeste codeersystemen zijn zo ontworpen dat ze een ingebouwde beveiliging bevatten tegen een aantal courant optredende (manipulatie)fouten. We illustreren.

2.2.1 Bankrekeningnummers

De rekeningnummers van Belgische bankrekeningen worden steeds weergegeven als een getal van 12 cijfers, voorgesteld als

$$x_1x_2x_3/x_4x_5x_6x_7x_8x_9x_{10}/x_{11}x_{12}.$$

In feite bevatten de eerste 10 cijfers alle nodige informatie. De laatste 2 vormen een zogeheten controlegetal. Dit moet ervoor zorgen dat niet elk willekeurig opgeschreven getal van 12 cijfers een geldig bankrekeningnummer weergeeft en het helpt foutjes te ontdekken die bij snelle manipulaties van deze nummers wel eens meer voorkomen.
Het controlegetal $c = x_{11}x_{12}$ van een Belgisch bankrekeningnummer voldoet steeds aan

$$x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10} \equiv c \mod 97.$$

Opdracht 2.2.1

1. Verifieer zelf of de je bekende rekeningnummers voldoen aan dit elementaire beveiligingssysteem.

2. Bij het copiëren van een rekeningnummer was nogal grote haast geboden. Het nummer ziet er als volgt uit : $284 - 73604 \bullet \bullet - 47$.

   Kun je het getal van 2 cijfers bepalen dat op de plaats van de stippen moet worden ingevuld?

(V.W.O. 1989, 1e ronde, vraag 28)

2.2.2 Kredietkaarten

Ook de nummers van kredietkaarten (VISA, Eurocard, American Express, ...) zijn niet zomaar willekeurige getallen. Uiteraard bevatten ze een belangrijk informatiegedeelte, maar opnieuw is er een controlefunctie ingebouwd, ter beveiliging tegen fouten bij het doorgeven van die nummers. Dit systeem staat bekend als het CODABAR systeem.
Het laatste cijfer van het kredietkaartnummer is het controlegetal.
Onderstel dat een volledig nummer er als volgt uitziet :

$$x_1x_2x_3x_4/x_5x_6x_7x_8/x_9x_{10}x_{11}x_{12}/x_{13}x_{14}x_{15}x_{16}.$$

Het laatste cijfer, x_{16} wordt dan bepaald zo dat voldaan is aan

$$2.(x_1 + x_3 + x_5 + \cdots + x_{13} + x_{15}) + n_o + (x_2 + x_4 + \cdots + x_{14}) + x_{16} \equiv 0 \bmod 10.$$

Hierin staat n_o voor het aantal cijfers op een oneven plaats dat groter is dan 4. Het is zonder meer duidelijk dat dit CODABAR systeem ook kan toegepast worden op getallen bestaande uit meer (of minder) dan 16 cijfers.

Voorbeeld 2.2.2
Onderstel dat een bank beslist dat het informatiegedeelte van het kredietkaartnummer voor een klant gegeven wordt door

$$1302/6251/0047/239\bullet .$$

Het nummer moet nu volledig gemaakt worden door het correcte controlecijfer op de plaats van $\bullet$ te bepalen. Daartoe

$$2(x_1 + x_3 + \cdots + x_{15}) = 2.(1 + 0 + 6 + 5 + 0 + 4 + 2 + 9) = 2.27 = 54$$

$$n_o = 3 \text{ alleen } x_5 = 6,\ x_7 = 5 \text{ en } x_{15} = 9 \text{ zijn groter dan } 4$$

$$x_2 + x_4 + \cdots x_{14} = 3 + 2 + 2 + 1 + 0 + 7 + 3 = 18$$

Nu moet x_{16} voldoen aan

$$54 + 3 + 18 + x_{16} \equiv 0 \bmod 10$$

en bijgevolg vinden we

$$x_{16} = 5.$$

Opdracht 2.2.3 Heb je een kredietkaart, verifieer dan of de codering van het nummer ervan met dit systeem overeenkomt.

2.2.3 European Article Numbering - code (EAN)

In de USA ontstond al vrij snel de zogenaamde UPC-code (Universal Product Code), een streepjescodeersysteem waarbij vrijwel alle producten die verhandeld worden, worden geïdentificeerd. Enige tijd later werd een Europese variant in het leven geroepen, bekend als de EAN-code. De administratieve zetel van het EAN-systeem bevindt zich overigens te Brussel (zie http://www.ean-int.org/).
De zogenaamde EAN-13 (er is ook een EAN-8) code identificeert elk product door er een 13-cijferig nummer aan toe te kennen. Een code ziet er uit als volgt:

$$x_1\ x_2x_3x_4x_5x_6x_7\ x_8x_9x_{10}x_{11}x_{12}x_{13}.$$

Hierin is het laatste cijfer een controlecijfer. Het is zo bedacht dat

$$x_1 + 3x_2 + x_3 + 3x_4 + \cdots + x_1 1 + 3x_1 2 + x_1 3 \equiv 0 \text{ mod} 10.$$

Op de website van de EAN administratie, kan een javascript-programmaatje geraadpleegd worden dat het controlecijfer bepaalt/verifieert voor om het even welk product. Zie http://www.ean-int.org/cdcalcul.html.

2.2.4 Boeken en hun ISBN-nummer.

Boeken behoren tot de dagelijkse ervaringswereld van alle leerlingen. Ten gevolge van een internationale afspraak worden alle (voldoende recente) boeken geïdentificeerd aan de hand van hun "International Standard Book Number", kortweg het ISBN-nummer genoemd. Wil je een nieuw boek bestellen, dan volstaat het dit nummer aan je boekhandelaar te geven opdat hij het boek ondubbelzinnig zou kunnen bepalen.
Elk ISBN-nummer bestaat uit 10 tekens, waarvan de eerste negen steeds cijfers zijn. Het tiende teken hangt evenwel af van de vorige 9 op de volgende manier: als het ISBN-nummer de vorm

$$x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9 x_{10}$$

heeft, dan wordt het laatste teken (x_{10}) zó bepaald dat voldaan is aan de voorwaarde

$$x_1 + 2.x_2 + 3.x_3 + \cdots + 8.x_8 + 9.x_9 + 10.x_{10} \equiv 0 \text{ mod } 11$$

We kunnen deze voorwaarde herschrijven als

$$10.x_{10} \equiv -(x_1 + 2.x_2 + \cdots + 9.x_9) \text{ mod } 11$$

of, in rekening brengend dat $10 \equiv -1 \text{ mod } 11$, ook als

$$x_{10} \equiv x_1 + 2.x_2 + \cdots + 9.x_9 \text{ mod } 11$$

Dit betekent dat $x_{10} \in \mathbb{Z}_{11}$; omdat deze verzameling 11 elementen telt en er maar 10 beschikbare cijfers zijn, wordt overeengekomen de congruentieklasse van 10 met X te noteren. Het tiende teken van een ISBN-nummer is dus een cijfer of het teken X.

Wat is hiervan de bedoeling? Wel, zoals de meeste andere identificatiesystemen, wordt het ISBN-nummer heel frequent gehanteerd en doorgegeven. Het is best mogelijk dat bij die veelvuldige manipulaties foutjes ontstaan. Dit "codeersysteem" kan een aantal vaak voorkomende fouten "ontdekken". Ook zorgt het er mede voor dat het niet gemakkelijk is zomaar snel een "geldig" fictief ISBN nummer te bedenken.

Eigenschap 2.2.4 Het ISBN-codeersysteem ontdekt alle enkelvoudige fouten, d.w.z. fouten waarbij één enkel cijfer of teken verkeerd wordt doorgegeven :

Bewijs : onderstel dat $x = x_1 x_2 \ldots x_{10}$ een correct ISBN-nummer is en dat bij een manipulatie van dit nummer de ontvanger het nummer $y = y_1 y_2 \ldots y_{10}$ in handen krijgt, waarbij $x_i = y_i$ voor alle $i \in \{1, 2, \ldots, 10\}$, behalve voor één index $j \in \{1, 2, \ldots, 10\}$; zij b.v. $y_j = x_j + a$ $(a \neq 0)$, dan geldt :

$$y_1 + 2.y_2 + \cdots + 10.y_{10} = x_1 + 2.x_2 + \cdots + 10.x_{10} + j.a$$

en, omdat x een geldig ISBN-nummer was, vinden we dus

$$y_1 + 2.y_2 + \cdots + 10.y_{10} \equiv j.a \text{ mod } 11.$$

Maar $j.a$ is zeker niet congruent met 0 modulo 11, want $1 \leq j \leq 10$ en $1 \leq |a| < 10$. Het ontvangen nummer wordt dus als fout geregistreerd. Q.E.D.

Eigenschap 2.2.5 Het ISBN-codeersysteem ontdekt alle fouten waarbij twee verschillende tekens worden omgewisseld.

Bewijs : onderstel dat het ontvangen nummer y gelijk is aan x waarbij twee verschillende tekens, zeg x_j en x_k, van plaats zijn omgewisseld ; dan geldt dat $y_j = x_k$, $y_k = x_j$ en $y_i = x_i$ voor alle i met $i \neq j$ en $i \neq k$. Bijgevolg

$$\begin{aligned} \sum_{i=1}^{10} i.y_i &= \sum_{i=1}^{10} i.x_i + (k-j)x_j + (j-k)x_k \\ &\equiv (k-j)(x_j - x_k) \end{aligned}$$

en dit is niet congruent met 0 modulo 11, omdat zowel $|k-j|$ als $|x_j - x_k|$ getallen zijn tussen 1 en 10.

Q.E.D.

Voorbeeld 2.2.6
We nemen als voorbeelden de ISBN-nummers van enkele boeken uit de bibliografie bij deze tekst, en we gaan telkens hun correctheid na.

Boek van R.Hill ([6]) : Het ISBN-nummer is $0-19-853804-9$. Controleer

$$0+2+27+32+25+18+56+36+90 \equiv 2+5+10+3+7+1+3+2 \equiv 0 \bmod 11.$$

Boek van A.Weil ([11]): Het ISBN-nummer is $0-387-90381-X$. Controleer

$$0+6+24+28+45+0+21+64+9+100 \equiv 6+2+6+1+10+9+9+1 \equiv 0 \bmod 11.$$

Opdracht 2.2.7

1. Een vriend gaf me op een blaadje het ISBN-nummer van het boek [3]. Het luidde: $0-669-29496-4$. Ten einde het boek te bestellen trok ik met deze gegevens naar de boekhandel. De handelaar verzekerde me echter dat dit geen correct nummer was. Ga dit zelf even na. Kun je beslissen waar de fout zich heeft voorgedaan?

2. Op een fotocopie van slechte kwaliteit waren de volgende ISBN-nummers onvolledig herkenbaar. Kun je de ontbrekende cijfers aanvullen?

   (a) $0-13-1\bullet 9139-9$

   (b) $0-02-32\bullet\bullet 80-0$

2.3 Het RSA-codeersysteem

2.3.1 De ingrediënten

De voorbeelden hierboven illustreren hoe het toekennen van codes enigszins beveiligd kan worden (beveiligd tegen fouten bij het veelvuldig manipuleren!) door het toevoegen van controle-getallen. Elementair rekenen met congruenties volstond voorlopig.
In deze paragraaf ligt de klemtoon op een ander soort beveiligen: nu hebben we het over afschermen van informatie voor strikt gebruik tussen verzender en ontvanger. We maken kennis met een "publieke sleutel" codeersysteem, dat gebaseerd is op het grondiger begrijpen van het rekenen met congruenties. "Publieke sleutel" codeersystemen zullen in nabije toekomst hun toepassingen sterk zien uitbreiden, b.v. dank zij de groei van en de toenemende belangstelling van het INTERNET (de digitale handtekening). RSA is in dit opzicht één van de bekende en populaire systemen.

Bij elke codeer/decodeer operatie is het natuurlijk de bedoeling dat het resultaat van het decoderen identiek gelijk is aan de oorspronkelijk gecodeerde boodschap.
In wiskundetaal vertaald, kunnen we het "coderen" daarom best voorstellen als een bijectie f van een verzameling A (de verzameling van de boodschappen) naar een verzameling B (de verzameling van de gecodeerde boodschappen). We onderstellen hierbij steeds dat we werken met eindige verzamelingen. Een codeersysteem (bepaald door een bijectie f) wordt moeilijk te breken wanneer de inverse afbeelding (bijectie) voor f moeilijk te vinden of te construeren is. Wanneer daarenboven de informatie, die nodig is om f te kennen en uit te voeren, eenvoudig is en deze informatie tegelijk niet volstaat om snel de inverse afbeelding van f te construeren, is alles voorhanden voor een zogenaamd "publieke sleutel codeersysteem".
We zullen dit principe toepassen op de verzameling $\mathbb{Z}_n$, waarbij n gelijk is aan $p.q$, het product van twee verschillende priemgetallen (p en q) is.
Afbeeldingen f_r van de vorm

$$f_r : \mathbb{Z}_{pq} \to \mathbb{Z}_{pq} : a \mapsto f(a) = a^r \text{ met } r \in \mathbb{N}$$

zijn zeer eenvoudig concreet uit te voeren. Het berekenen van de functiewaarden onder f_r stelt geen bijzondere moeilijkheden voor de hedendaagse technologie (ook niet als r en/of n zeer groot zijn): uiteraard kan het programma `MACHTMOD` hierbij helpen (zie (1.8.3)).

Probleem 2.3.1 (Research-Project!) We vragen ons nu af:

1. of er afbeeldingen $f_r : \mathbb{Z}_n \to \mathbb{Z}_n$ zijn die bijectief zijn (d.w.z. die geschikt zijn om er een codeersysteem mee te bouwen), én,

2. indien ja, of we kunnen beschrijven voor welke waarden van r deze bijecties optreden en wat dan hun inversen zijn.

Voorbeeld 2.3.2
We werken in $\mathbb{Z}_{14}$ ($p = 2, q = 7$): meer bepaald gaan we na voor welke waarden van r uit $\{1, 2, \ldots, 14\}$ de afbeelding f_r een permutatie is van $\mathbb{Z}_{14}$. Het programma `MACHTMOD` kan hierbij uiteraard gebruikt worden. De resultaten vatten we samen in de volgende tabel:

	per waarde van r, a^r mod 14													
$a \backslash r$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	2	4	8	2	4	8	2	4	8	2	4
3	3	9	13	11	5	1	3	9	13	11	5	1	3	9
4	4	2	8	4	2	8	4	2	8	4	2	8	4	2
5	5	11	13	9	3	1	5	11	13	9	3	1	5	11
6	6	8	6	8	6	8	6	8	6	8	6	8	6	8
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
9	9	11	1	9	11	1	9	11	1	9	11	1	9	11
10	10	2	6	4	12	8	10	2	6	4	12	8	10	2
11	11	9	1	11	9	1	11	9	1	11	9	1	11	9
12	12	4	6	2	10	8	12	4	6	2	10	8	12	4
13	13	1	13	1	13	1	13	1	13	1	13	1	13	1
	de kolommen die een bijectie tonen													
	↑				↑		↑				↑		↑	
	1				5		7				11		13	

Wat valt hierbij op?

1. De waarden voor r die een permutatie f_r bepalen zijn resp. 1, 5, 7, 11 en 13 (zie de met $\uparrow$ aangeduide kolommen in de tabel). Kunnen we hierin een patroon herkennen? Ongetwijfeld kunnen hier verschillende hypotheses uit voortkomen. B.v. hier zou de hypothese kunnen zijn dat r gelijk is aan 1 of een oneven priemgetal groter dan 3.

2. Dat r niet gelijk mag zijn aan 2 (en dus evenmin even mag zijn), is trouwens snel in te zien als je beseft dat steeds $(-1)^2 = 1^2 = 1$.

3. De tabel illustreert ook dat er geen analoog is voor de kleine stelling van Fermat (cf. Deel I, toepassing 7.4) als we niet modulo een priemgetal werken ; uit de tabel lezen we b.v. af dat alle machten van 7 (resp. 8) modulo 14 gelijk zijn aan 7 (resp. 8)

Een extra voorbeeld (eventueel meerdere) kan (kunnen) de hypothese(s) ontkrachten of verfijnen, of, wie weet, zelfs alle duidelijkheid ontnemen en daardoor de moeilijkheidsgraad van het probleem onderlijnen. We kijken daarom nog even naar de situatie voor $\mathbb{Z}_{10}$ $(10 = 2.5)$.

	per waarde van r, a^r mod 10									
$a\backslash r$	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	6	2	4	8	6	2	4
3	3	9	7	1	3	9	7	1	3	9
4	4	6	4	6	4	6	4	6	4	6
5	5	5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6	6	6
7	7	9	3	1	7	9	3	1	7	9
8	8	4	2	6	8	4	2	6	8	4
9	9	1	9	1	9	1	9	1	9	1
	$\uparrow$		$\uparrow$		$\uparrow$		$\uparrow$		$\uparrow$	
	1		3		5		7		9	

Meteen blijkt uit dit voorbeeld dat de hierboven geformuleerde hypothese niet correct is; de "goede" waarden van r zijn niet telkens priem; bovendien is $r = 3$ hier wel een goede waarde. Het vergt dus een beter onderzoek om een nieuwe hypothese te formuleren.

Opdracht 2.3.3 Maak zelf de tabel voor $\mathbb{Z}_{21}$ $(21 = 7 \cdot 3)$ en $\mathbb{Z}_{35}$ $(35 = 7 \cdot 5)$.

Geduldig speurwerk, aan de hand van alle vorige voorbeelden, leidt uiteindelijk tot het volgende resultaat, dat we als stelling formuleren:

Stelling 2.3.4 Als $n = p.q$, waarbij p en q verschillende priemgetallen zijn,
en als $\text{ggd}(r, (p-1)(q-1)) = 1$, dan is $f_r : \mathbb{Z}_n \to \mathbb{Z}_n : a \mapsto f(a) = a^r$ een permutatie van $\mathbb{Z}_n$.

Bewijs:
Onderstel dat $\text{ggd}(r, (p-1)(q-1)) = 1$. Het algoritme van Euclides leert ons dat we de grootste gemene deler van twee getallen als gehele lineaire combinatie van beide getallen kunnen schrijven; dus bestaan er gehele getallen s en t zodat

$$1 = r.s - (p-1)(q-1).t \quad \text{of } r.s = 1 + t.(p-1)(q-1)$$

Onderstel dat a niet congruent is met 0 modulo p; dan volgt dat

$$a^{r.s} = a.(a^{(p-1)})^{t.(q-1)}$$

We maken gebruik van de kleine stelling van Fermat en besluiten dat

$$a^{r.s} \equiv a.1 \equiv a \bmod p$$

Uiteraard geldt dit laatste ook als $a \equiv 0 \bmod p$.
We kunnen dezelfde redenering herhalen, maar nu werken modulo q (het tweede priemgetal). Dan vinden we dus, voor alle a,

$$a^{r.s} \equiv a.1 \equiv a \bmod q$$

We besluiten nu met, $\forall a$:

$$\left.\begin{array}{l} p \mid a^{r.s} - a \\ q \mid a^{r.s} - a \end{array}\right\} \overset{p \neq q}{\Rightarrow} p.q \mid a^{r.s} - a. \text{ (zie Deel I, 3.17, oef.5)}$$

Dit betekent dus, $\forall a$:

$$(a^r)^s \equiv a \bmod p.q$$

of, anders geschreven,

$$f_s(f_r(a)) = a.$$

Uit eigenschap (1.2.6), oefening 2 volgt dat f_r injectief is in $\mathbb{Z}_n$ en bijgevolg (daar $\mathbb{Z}_n$ een eindige verzameling is) een permutatie van $\mathbb{Z}_n$ is. Tegelijk volgt dat f_s de inverse permutatie is van f_r.

Q.E.D.

Opmerking 2.3.5

1. Het algoritme van Euclides laat toe deze s te construeren, op voorwaarde althans dat we p en q kennen!
2. Ook het omgekeerde resultaat van deze stelling geldt; m.a.w. als f_r een permutatie is van $\mathbb{Z}_{pq}$ (p en q verschillende priemgetallen), dan zijn r en $(p-1)(q-1)$ relatief priem. Een bewijs gebruik makend van enkel deelbaarheidseigenschappen is echter niet zo eenvoudig te geven.

2.3.2 RSA als publieke sleutel cryptosysteem: stapsgewijs.

Alle elementen zijn nu voorhanden om tot de constructie van een ingenieus "publieke sleutel" codeersysteem over te gaan. Het systeem dat we hier beschrijven staat in de literatuur bekend als het RSA-systeem, genoemd naar R. Rivest, A. Shamir en L. Adleman die het omstreeks 1975 voorstelden : het was het eerste publieke sleutel codeersysteem en het is nog steeds één van de belangrijkste.
Dit systeem maakt handig gebruik van de volgende gegevens :

- er bestaan vrij goede algoritmes om na te gaan of een gegeven (denk "groot") getal priem of niet priem is. Anders gezegd: primaliteit van een getal testen is relatief eenvoudig.
- er bestaan zeer goede algoritmes om snel te rekenen modulo een gegeven getal n (zowel $+$ als .)
- het is (jammer genoeg) nog steeds niet mogelijk om een willekeurig gegeven zeer groot getal, waarvan men weet dat het geen priemgetal is, snel te ontbinden in priemfactoren. Ook vandaag kan de computertijd nodig om b.v. een getal van 100 cijfers te ontbinden in priemfactoren snel oplopen tot de grootte-orde van jaren en decennia. Het RSA-systeem is dus gebaseerd op de afwezigheid van een voldoende snel algoritme voor priemfactorisatie. Het dient dus opgemerkt dat een stap voorwaarts in de Wiskunde op dit vlak een potentiële bedreiging voor dit codeersysteem is.

Werking van het RSA-systeem.
Laat ons stapsgewijs deze werking overlopen.
Een uitgangspunt van dit systeem is dat de codeersleutel (f_r hierboven) bekend is voor ieder die dat wenst ("de zenders"). De decodeersleutel (f_s hierboven) is enkel bekend door diegene waarvoor de gecodeerde boodschappen bedoeld zijn ("de ontvanger").

Het coderen (resp. decoderen) gebeurt door het rekenen met congruenties modulo een vooraf door de ontvanger bepaald getal n. Dit getal n is het product van twee verschillende priemgetallen p en q.
De te versturen boodschappen moeten dus vooraf omgezet worden in "getallentaal". Hiervoor kan een systeem overeengekomen worden. Om het eenvoudig te houden, komen we overeen de volgende omzetting te hanteren: A= 01, B= 02, ..., Z= 26, spatie= 00. Hiermee kunnen alle geschreven boodschappen in cijfers omgezet worden. Eenmaal dat gebeurd is, wordt de lange rij cijfers in blokjes van gelijke lengte verdeeld. Deze lengte is zo bepaald dat het grootste getal in zo een blokje niet groter kan worden dan het getal n.
De ontvanger kiest een getal r dat relatief priem is tot $(p-1)(q-1)$. Hij berekent meteen een (positief) getal s zodat

$$r.s \equiv 1 \bmod (p-1)(q-1).$$

De ontvanger maakt hierna aan alle potentiële zenders de codeersleutel bekend : een getal a $(< n)$ moet gecodeerd worden als $a^r \bmod n$. Dit betekent dus niets anders dan

$$a \in \mathbb{Z}_n \text{ wordt afgebeeld op } f_r(a) \in \mathbb{Z}_n.$$

(Noteer goed: enkel n en r worden bekend gemaakt.)
Iedereen die dat wenst kan zijn boodschap nu coderen en doorsturen naar de ontvanger. Om te decoderen moet de ontvanger de inverse permutatie van f_r toepassen, d.w.z. f_s. Hij kent deze, want hij heeft r en s kunnen berekenen, gebruik makend van de priemfactorontbinding van n. Iemand die de decodeersleutel wil kennen, moet dus de priemfactorontbinding van n kunnen bepalen. Als n voldoende groot gekozen wordt, is dit een nagenoeg onmogelijke opdracht.

Voorbeelden 2.3.6

1. We illustreren het RSA-systeem met een heel eenvoudig (en voor wat betreft de uiteindelijke bedoeling onbruikbaar) voorbeeld. We kiezen 2 priemgetallen: $p = 11$ en $q = 89$, zodat $n = p.q = 979$. Nu moeten we een r bepalen die relatief priem tot $(p-1)(q-1) = 10.88 = 880$. $(880 = 2.2.2.2.5.11)$ Kies r gelijk aan 57. Als publieke sleutel maken we dus bekend: $n = 979$, $r = 57$ en coderen gaat via de permutatie

   $$f_{57} : \mathbb{Z}_{979} \to \mathbb{Z}_{979} : a \mapsto a^{57}.$$

   Willen we nu b.v. de boodschap "MORGEN OM ACHT UUR" coderen, dan wordt deze eerst omgezet in getal-vorm. We krijgen dan

   $$1315180705140015130001030820002121 18.$$

   Nu verdelen we dit grote getal in blokjes van gelijke lengte. De resulterende getallen mogen daardoor echter niet groter worden dan $n = 979$. We kunnen dus blokjes nemen van lengte hoogstens 3. De te coderen informatie is dus

   $$131 \;\; 518 \;\; 070 \;\; 514 \;\; 001 \;\; 513 \;\; 000 \;\; 103 \;\; 082 \;\; 000 \;\; 212 \;\; 118.$$

   Op elk van deze getallen passen f_{57} toe; we verkrijgen dan

   $$791 \;\; 100 \;\; 060 \;\; 695 \;\; 001 \;\; 314 \;\; 000 \;\; 313 \;\; 300 \;\; 000 \;\; 746 \;\; 321$$

   Voer nu zelf de decodering uit.

2. De ontvanger in een RSA-codeersysteem heeft als publieke sleutel bekend gemaakt: $n = 2813$ en $r = 283$. De boodschappen moeten in een groot getal omgezet worden, dat daarna in blokjes van lengte 4 verdeeld wordt.

   Een gecodeerde boodschap wordt onderschept. Deze luidt:

2014 1107 0880 0328 0880 1373 1277 0004

0417 2238 0666 2416 2408 0849

Wat was de boodschap?[1]

2.3.3 Een digitale handtekening met behulp van het RSA systeem

Hierboven legden we uit hoe het RSA systeem als cryptosysteem functioneert. Daarbij is het de bedoeling informatie "geheim" te houden. Een andere bedoeling van een cryptosysteem kan er in bestaan de authenticiteit van een document of de ondertekenaar ervan aan te tonen. Dit is het aspect dat populair bekend is als "een digitale handtekening afleveren".
Veronderstel dat in dit geval de zender een brief stuurt naar de ontvanger, en dat het hierbij erg belangrijk is dat de ontvanger de authenticiteit van de zender kan verifiëren. De zender moet dus een stuk informatie toevoegen op een manier waartoe enkel hijzelf in staat is, maar zodat de ontvanger dat ook kan nagaan. Daarom zal de zender de brief zgn. ondertekenen met een clausule die hij encrypteerde met zijn private sleutel uit het RSA systeem. Als de ontvanger deze informatie krijgt, is hij in staat met de publieke sleutel van de zender, effectief na te gaan dat de clausule (handtekening) effectief een leesbare boodschap bevat.
Typisch wil de zender er natuurlijk ook voor zorgen dat de inhoud van de brief zelf niet zomaar ter beschikking komt en beschermd blijft. Hij zal daarom het geheel van de brief en de ondertekeningsclausule encrypteren met de publieke sleutel van de ontvanger, zodat enkel de ontvanger, door gebruik te maken van zijn private sleutel, de briefinhoud kan ontcijferen, er de nog steeds geëncrypteerde ondertekening aantreffen, en ook die vervolgens kan verifiëren.

2.4 Het Diffie-Hellman systeem van sleuteluitwisseling

We beschrijven hier het protocol van Diffie en Hellman dat toelaat geheime sleutels uit te wisselen via onveilige kanalen; dit protocol is zelf geen publieke sleutel codeersysteem, maar is wel de basis voor het ElGamal publieke sleutel codeersysteem, dat we hierna bestuderen.
Beschouwen we de volgende situatie: 2 personen willen een symmetrisch codeersysteem gebruiken om hun boodschappen, verstuurd via een onveilig kanaal, geheim te houden: bij een symmetrisch codeersysteem is het zo dat de codeer- en de decodeersleutel equivalent zijn, d.w.z. dat de ene makkelijk uit de andere kan afgeleid worden (vaak zijn beide sleutels zelfs gelijk, men spreekt dan van een 1-sleutel codeersysteem).
Een eenvoudig voorbeeld hiervan vinden we in de zogenaamde Caesarcodering (voor het eerst gebruikt door de Romeinse veldheer Julius Caesar), waarbij de codering bestaat uit de permutatie p van het alfabet, die elke letter 3 plaatsen naar rechts verschuift :

$$\begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & A & B & C \end{pmatrix}$$

De decodering bestaat dan uit het toepassen van de inverse permutatie p^{-1}.
Een belangrijk probleem bij een symmetrisch codeersysteem is een efficiënte methode te vinden om deze sleutel af te spreken en uit te wisselen: het Diffie-Hellman systeem van sleuteluitwisseling laat toe om daarvoor een onveilig kanaal te gebruiken. Iedereen kan de sleuteluitwisseling afluisteren, maar de informatie die op die manier verkregen wordt, kan niet gebruikt worden om de geheime sleutel te weten te komen! Daarom is het protocol van Diffie-Hellman een mijlpaal in codetheorie.
In tegenstelling tot RSA-codering is bij Diffie-Hellman sleuteluitwisseling de veiligheid niet gebaseerd op de moeilijkheid om een (groot) getal te ontbinden in priemfactoren, maar wel op het discrete-logaritme-probleem (DLP), dat we hierna toelichten. Eerst moeten we echter iets meer weten over discrete logaritmen.

[1] Was je nog tijdig klaar?

We weten reeds dat voor elk priemgetal p $\mathbb{Z}_p \setminus \{0\}, \cdot$ een commutatieve groep is. In een eindige groep hebben we de volgende

Definitie 2.4.1 Als $(G, \star)$ een eindige groep is met neutraal element e, dan is de orde van een element g van G het kleinste niet-nul natuurlijk getal n zodat

$$\begin{cases} g^n = e & \text{(multiplicatieve notatie)} \\ n \cdot g = e & \text{(additieve notatie)} \end{cases}$$

We beperken ons vanaf nu tot de multiplicatieve groepen $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ (p wordt steeds priem verondersteld); door de kleine stelling van Fermat weten we reeds dat de orde van elk element hoogstens gelijk is aan $p-1$, zoals zal blijken in de volgende

Voorbeelden 2.4.2

1. In $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is de orde van het element 2 gelijk aan 4,
   want $2^2 = 4$, $2^3 = 3$, $2^4 = 1$. De volledige tabel ziet er als volgt uit :

g	1	2	3	4
orde van g	1	4	4	2

2. In $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$

g	1	2	3	4	5	6
orde van g	1	3	6	3	6	2

Oefening.
Stel een dergelijke tabel op voor $(\mathbb{Z}_{13} \setminus \{0\}, \cdot)$.

We stellen in alle vorige voorbeelden twee zaken vast: ten eerste zien we dat de orde van elke element een deler is van het aantal elementen van de groep. Inderdaad

Stelling 2.4.3 In een eindige groep $(G, \star)$ is de orde van elke element g een deler van het aantal elementen van de groep.

Bewijs in het geval dat $(G, \star) = (\mathbb{Z}_p \setminus \{0\}, \cdot)$:
Onderstel dat er een element $g \in \mathbb{Z}_p \setminus \{0\}$ bestaat zodat de orde van g gelijk is aan k en k geen deler van $p-1$ is ; dan is $g^k = 1$ en $p - 1 = k \cdot q + r$ met $0 < r < k$. Bijgevolg

$$g^{p-1} = (g^k)^q \cdot g^r = g^r. \tag{2.1}$$

Maar anderzijds volgt uit de kleine stelling van Fermat dat

$$g^{p-1} = 1. \tag{2.2}$$

Uit (2.1) en (2.2) volgt dan dat $g^r = 1$, maar dit is in tegenspraak met de onderstelling dat de orde van g gelijk is aan k en het feit dat $0 < r < k$.

Q.E.D.

Een tweede zaak die we constateren in de vorige voorbeelden betreft de aanwezigheid van een element waarvan de orde precies gelijk is aan $p-1$, het aantal elementen van de groep; b.v. in $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ is 2 een dergelijk element (naast 3); dit impliceert dat $\{2^0, 2^1, 2^2, 2^3\} = \mathbb{Z}_5 \setminus \{0\}$ (merk op dat $2^4 = 2^0 = 1$). We noemen 2 (en ook 3) een primitieve wortel modulo 5. Ook in $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$ zien we elementen met orde 6, nl. 3 en 5; ook hier geldt b.v. $\{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} = \mathbb{Z}_7 \setminus \{0\}$ (en $3^6 = 3^0 = 1$). We noemen 3 (en ook 5) een primitieve wortel modulo 7. We hebben de volgende

Definitie 2.4.4 Een getal $g \in \{1, 2, \ldots, p-1\}$ is een primitieve wortel modulo p als en slechts als de orde van g in $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ gelijk is aan $p-1$.

Volgende eigenschap aanvaarden we zonder bewijs

Eigenschap 2.4.5 Voor elk priemgetal p bestaat er een primitieve wortel modulo p, of, anders gezegd, voor elk priemgetal p bestaat er een getal $g \in \{1, 2, \ldots, p-1\}$ zodat $\mathbb{Z}_p \setminus \{0\} = \{1, g, g^2, \ldots, g^{p-2}\}$; we zeggen dan dat $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ een cyclische groep is die voortgebracht wordt door g.

Hieruit volgt dat elke element van $\mathbb{Z}_p \setminus \{0\}$ op een unieke manier kan geschreven worden als een macht van g, waarbij de exponenten behoren tot $\{0, 1, \ldots, p-2\}$. Nu we dit weten, kunnen we overgaan tot de definitie van een cruciaal begrip in het Diffie-Hellman systeem:

Definitie 2.4.6 Zij g een primitieve wortel modulo p; de discrete logaritme van een willekeurig getal $a \in \{1, 2, \ldots, p-1\}$ is het unieke getal $e \in \{0, 1, \ldots, p-2\}$ zodat $a = g^e$ in $\mathbb{Z}_p$, of, equivalent, $a \equiv g^e \bmod p$.

We noteren deze logaritme met $\mathrm{dlog}_g\, a$.

Voorbeelden 2.4.7

- 2 is een primitieve wortel modulo 5; we verkrijgen dan in $\mathbb{Z}_5 \setminus \{0\}$ volgende tabel:

a	1	2	3	4
$d\log_2 a$	0	1	3	2

- 3 is een primitieve wortel modulo 7; we verkrijgen dan in $\mathbb{Z}_7 \setminus \{0\}$ volgende tabel:

a	1	2	3	4	5	6
$d\log_3 a$	0	2	1	5	6	4

- 5 is ook een primitieve wortel modulo 7; we verkrijgen dan in $\mathbb{Z}_7 \setminus \{0\}$ volgende tabel:

a	1	2	3	4	5	6
$d\log_5 a$	0	4	5	2	1	3

Oefening. Maak zelf zo'n tabel voor $(\mathbb{Z}_{13} \setminus \{0\}, \cdot)$ met primitieve wortel 2.

Werking van het Diffie-Hellman protocol voor sleuteluitwisseling.
Onderstel dat Ricky en Ulrike een gemeenschappelijke geheime sleutel willen afspreken en dat ze enkel kunnen communiceren langs een onveilig kanaal. Om te beginnen, spreken ze een (groot) priemgetal p en een primitieve wortel g modulo p af, met $2 \leq g \leq p-2$. Het priemgetal p en de primitieve wortel g mogen publiek gemaakt geworden.
Nu kiest Ricky een willekeurig geheel getal $a \in \{0, 1, \ldots, p-2\}$ en hij berekent

$$A = g^a \bmod p$$

Hij zendt het resultaat A naar Ulrike, maar houdt de exponent a geheim.
Ulrike kiest ook een willekeurig geheel getal $b \in \{0, 1, \ldots, p-2\}$, berekent

$$B = g^b \bmod p$$

en zendt het resultaat B naar Ricky. Ulrike houdt ook de exponent b geheim.
Om de gemeenschappelijke geheime sleutel te verkrijgen, berekent Ricky

$$B^a \bmod p = g^{ab} \bmod p$$

en berekent Ulrike

$$A^b \bmod p = g^{ab} \bmod p.$$

De gemeenschappelijke geheime sleutel is dus

$$K = g^{ab} \bmod p.$$

We illustreren ook deze methode met een eenvoudig en in de praktijk dus onbruikbaar

Voorbeeld 2.4.8
Zijn $p = 17$ en $g = 3$. Ricky kiest $a = 7$, berekent $g^a \bmod p = 11$ en zendt het resultaat $A = 11$ naar Ulrike. Ulrike kiest $b = 4$, berekent $g^b \bmod p = 13$ en zendt het resultaat $B = 13$ naar Ricky. Hij berekent $B^a \bmod p = 4$ en zij berekent $A^b \bmod p = 4$. De gemeenschappelijke sleutel is dus 4.

Hoe veilig is het systeem van Diffie-Hellman? Waar het RSA-codeersysteem gebaseerd is op de onmogelijkheid om, binnen een redelijke termijn, een groot getal te ontbinden in priemfactoren, zo steunt het systeem van Diffie-Hellman op het (voorlopig) ontbreken van een efficiënt algoritme om discrete logaritmen te berekenen bij zeer grote priemgetallen.
Bekijken we de zaak eens vanuit het standpunt van een aanvaller van het systeem : de aanvaller wil dus de geheime sleutel K kunnen afleiden uit p, g, A en B. Dit wordt het Diffie-Hellman probleem genoemd (verder DHP genoteerd). Indien de aanvaller discrete logaritmen modulo p kan berekenen, kan hij DHP oplossen. Dit is de enige totnogtoe gekende manier om het Diffie-Hellman protocol te kraken. Merk wel op dat het nog niet bewezen is dat, als iemand DHP kan oplossen, hij dan ook efficiënt discrete logaritmen modulo p kan berekenen. Het is een belangrijk open probleem in publieke-sleutel cryptografie een bewijs hiervan te vinden.
Zolang DHP niet op te lossen is, kan geen enkele aanvaller de geheime sleutel afleiden uit de publiek gemaakte informatie. Maar er is ook nog een andere aanval mogelijk op het Diffie-Hellman systeem, nl. de "man in het midden" aanval: hierbij buit de aanvaller uit dat Ricky niet kan weten dat de gegevens die hij ontvangt, werkelijk van Ulrike komen, en omgekeerd. De aanvaller onderschept alle boodschappen tussen Ulrike en Ricky. Hij speelt de rol van Ulrike en wisselt een sleutel uit met Ricky. Hij speelt ook de rol van Ricky en wisselt een sleutel uit met Ulrike. Dus, als Ricky een boodschap zendt die voor Ulrike bestemd is, onderschept de aanvaller deze boodschap en om ze te decoderen, gebruikt hij de sleutel die hij met Ricky heeft uitgewisseld. Dan kan hij de boodschap veranderen en doorsturen naar Ulrike.
Om een dergelijke aanval te verhinderen, kan gebruik gemaakt worden van een digitale handtekening.

We gaan nu over naar een rechtstreekse toepassing van het systeem van Diffie-Hellman.

2.5 Het ElGamal codeersysteem.

2.5.1 De Codering

Net zoals bij RSA moet de boodschap eerst worden omgezet in getallentaal. We kiezen daartoe een (in de praktijk) groot priemgetal p en verdelen de tekst in blokjes zodat elk getal hoogstens gelijk is aan $p - 1$.
We noemen het drietal (p, g, A) de publieke sleutel van Ricky en a zijn privé geheime sleutel. Het getal A is zijn sleuteldeel van het Diffie-Hellman protocol. Voor Ulrike zijn dit resp. (p, g, B), b en B.
Om een boodschap m te coderen, bepaalt Ulrike

$$c = A^b \cdot m \bmod p.$$

M.a.w. Ulrike codeert de boodschap m door deze te vermenigvuldigen modulo p met de Diffie-Hellman gemeenschappelijke geheime sleutel. De volledige ElGamal sleuteltekst is dan het paar (B, c).
We illustreren dit met een voorbeeld: laat ons aannemen dat beiden $p = 29$ en $g = 3$ hebben afgesproken (ga na dat 3 inderdaad een primitieve wortel modulo 29 is) en dat Ulrike van Ricky $A = 20$ ontvangt; Ulrike kiest zelf $b = 13$. Onderstellen we dat ze volgende boodschap wil coderen:

HET IS BIJNA TIJD

Als we elke letter vervangen door zijn plaats in het alfabet dan krijgen we volgende rij van getallen

08052009190209101401200910 04

Dit grote getal verdelen we in blokjes van lengte 2 en elk getal uit die rij (dit komt hier natuurlijk overeen met het "letter per letter" coderen, wat sowieso niet zeer verstandig of realistisch is, maar hier als voorbeeld functioneert) wordt nu vermenigvuldigd met $A^b = 20^{13} \bmod 29 = 16$ en dit geeft de volgende rij :

$$12220128140328152116012815 06$$

Aangezien $B = 3^{13} \bmod 29 = 19$, is de volledig sleuteltekst dan

$$19122201281403281521160128150 6$$

2.5.2 De Decodering

Ricky heeft de sleuteltekst (B, c) ontvangen. Hij kent uiteraard zijn privé geheime sleutel a. Om de oorspronkelijke boodschap m te reconstrueren, deelt hij c door de Diffie-Hellman sleutel $B^a \bmod p$. Om daarbij te vermijden dat hij inverse elementen modulo p moet berekenen, bepaalt hij de exponent $x = p - 1 - a$ en berekent hij $B^x \cdot c \bmod p$. Dit levert hem de oorspronkelijke boodschap op, want:

$$\begin{aligned} B^x \cdot c &\equiv B^{p-1-a} \cdot c \mod p \\ &\equiv g^{b(p-1-a)} \cdot A^b \cdot m \mod p \\ &\equiv \left(g^{p-1}\right)^b \cdot (g^a)^{-b} \cdot A^b \cdot m \mod p \\ &\equiv 1 \cdot A^{-b} \cdot A^b \cdot m \mod p \quad \text{(door de kleine stelling van Fermat)} \\ &\equiv m \mod p. \end{aligned}$$

Toegepast op ons voorbeeld: uit de getallenrij die Ricky ontvangt, leidt hij af dat $B = 19$ (de eerste twee cijfers van de tekst). Zijn privé geheime sleutel is $a = 16$ (ga zelf na dat inderdaad $g^a \equiv A = 20 \bmod 29$). Hij vermenigvuldigt nu modulo 29 elk getal van de sleuteltekst met $B^{p-1-a} = 19^{29-1-16} = 19^{12} = 10^{12} = 100^6 = 13^6 = 169^3 = (-5)^3 = 20$.
Ga na dat hij op die manier inderdaad de oorspronkelijke tekst ontvangt.

Oefening.
Stel dat Joke $p = 23$, $g = 7$ en $a = 6$ kiest. Chris kiest $b = 3$ en codeert de boodschap $m = 7$ en verstuurt die m.b.v. zijn sleutel naar Joke. Leg uit hoe hij dit doet en hoe Joke de ontvangen boodschap decodeert.

2.5.3 Keuze van de parameters

Het ElGamal codeersysteem is dus gebaseerd op het ontbreken van efficiënte algoritmes om discrete logaritmen te berekenen bij grote priemgetallen: in de praktijk moet het priemgetal p minstens binaire lengte 768 hebben!
Voor elke nieuwe ElGamal codering moet een nieuwe exponent b gekozen worden : als dezelfde exponent b gekozen wordt voor de codering van twee verschillende boodschappen m en m', dan verkrijgt men:

$$c = A^b \cdot m \mod p \text{ en } c' = A^b \cdot m' \mod p.$$

Bijgevolg

$$c' \cdot c^{-1} = m' \cdot m^{-1} \mod p.$$

Een aanvaller die één van de twee boodschappen m kent, kan dus de andere boodschap m' afleiden, via

$$m' = c' \cdot c^{-1} \cdot m \mod p.$$

Efficiëntie in vergelijking met RSA.
ElGamal decodering, net als RSA decodering, vereist modulaire machtsverheffingen. ElGamal codering daarentegen vereist twee modulaire machtsverheffingen (nl. de berekening van $A^b \bmod p$

en $B = g^b \bmod p$), terwijl RSA codering slechts één dergelijke bewerking vereist. Maar de machtsverheffingen bij ElGamal codering zijn onafhankelijk van de te coderen tekst en kunnen dus op voorhand uitgevoerd worden. De eigenlijke codering vereist slechts één modulaire vermenigvuldiging en is bijgevolg veel efficiënter dan RSA codering. Maar deze vooraf berekende waarden moeten wel veilig opgeslagen worden!

2.6 Een codeersysteem dat fouten corrigeert.

In de vorige paragrafen maakten we kennis met twee aspecten van het coderen van informatie, nl. het inbouwen van fouten-herkenning en het coderen om informatie te beveiligen voor ongewenst gebruik of om de authenticiteit van iets of iemand aan te tonen. Foutenherkenning laat heel vaak nog niet toe foutencorrectie toe te passen (het codeersysteem van het ISBN-nummer illustreert dit heel duidelijk).
In deze paragraaf maken we kennis met een systeem dat bedacht werd om fouten die ontstaan bij het doorsturen van informatie te kunnen herstellen. Laat ons beginnen met enkele voorbeelden.

Voorbeeld 2.6.1 Onderstel even dat een satelliet gelanceerd werd naar de planeet Mars en dat deze satelliet Mars aan het naderen is. Aan de hand van de foto's die deze satelliet zal nemen van het landingsgebied, zal het controlecentrum beslissen tot landing (signaal 1) of tot het overgaan in een baan rond Mars (signaal 0). De zeer grote afstand die dit signaal moet afleggen, maakt het optreden van een fout evenwel waarschijnlijk. Het is duidelijk dat een fout vrij erge gevolgen kan hebben voor het project. De vluchtleiding besluit daarom om in de plaats van het signaal 0 voor het overgaan in een baan rond Mars, een signaal bestaande uit 11 opeenvolgende nullen te sturen; analoog zal men in de plaats van het signaal 1 voor landing, 11 opeenvolgende tekens 1 sturen. De boordcomputer van de satelliet wordt meteen zo geprogrammeerd dat hij signalen zal ontvangen in blokken van lengte 11 en dat hij zo'n ontvangen blok zal interpreteren als een 0 (resp. een 1) als de meerderheid van de tekens in dat blok een 0 (resp. een 1 is). Het feit dat de blokken lengte 11 hebben, verzekert ons dat er steeds zo een meerderheid zal optreden.
Dit eenvoudige systeem vereist dat er minstens 6 fouten moeten optreden opdat de computer van de satelliet een foute beslissing zou nemen. Als we aannemen dat de fouten onafhankelijk van elkaar voorkomen, dan is het optreden van 6 fouten veel minder waarschijnlijk dan het optreden van één enkele fout.

Voorbeeld 2.6.2 Onderstel dat in een andere situatie de te versturen boodschap bestaat uit een opeenvolging van 500 nullen en/of enen. Onderstel ook dat de kans dat er een fout optreedt bij het versturen van één teken gelijk is aan 0.01 (1 honderdste). Als we deze boodschap zomaar doorsturen, zonder enige ingreep, dan is de kans dat hij correct ontvangen wordt gelijk aan

$$(0.99)^{500} \approx 0.0066$$

en dus heel klein.
Een relatief eenvoudige ingreep zou er in kunnen bestaan elk teken drie keer na een te sturen en de ontvangen blokjes van lengte 3 te decoderen volgens het meerderheidsprincipe (zie vorig voorbeeld). B.v. als de boodschap gelijk is aan 011001101 dan wordt het volgende verstuurd

$$000/111/111/000/000/111/111/000/111.$$

Als het ontvangen bericht gelijk is aan

$$001/110/001/000/010/011/111/001/011,$$

dan wordt dit geïnterpreteerd als

$$010001101.$$

Om de kans te bepalen dat het ontvangen bericht correct gedecodeerd wordt, moeten we bedenken dat als b.v. een 1 verzonden werd, het als een 0 zal gedecodeerd worden enkel en alleen als een blokje 001, 010, 100 of 000 ontvangen wordt. De kans dat dit gebeurt is

$$3.(0.01)(0.01)(0.99) + (0.01)^3 = 0.000298 < 0.0003$$

De kans dat elk verzonden teken correct gedecodeerd wordt is dus groter dan 0.9997; de kans dat de gehele boodschap correct gedecodeerd wordt is nu groter dan

$$0.9997^{500} \approx 0.86;$$

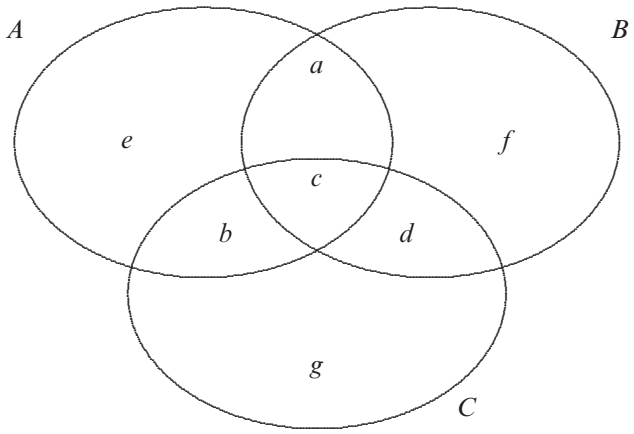
dit is een wel erg drastische verbetering t.o.v. de originele 0.0066 kans op correcte decodering.

Het volgend voorbeeld kan a.h.w. "live" gespeeld worden in de klas.

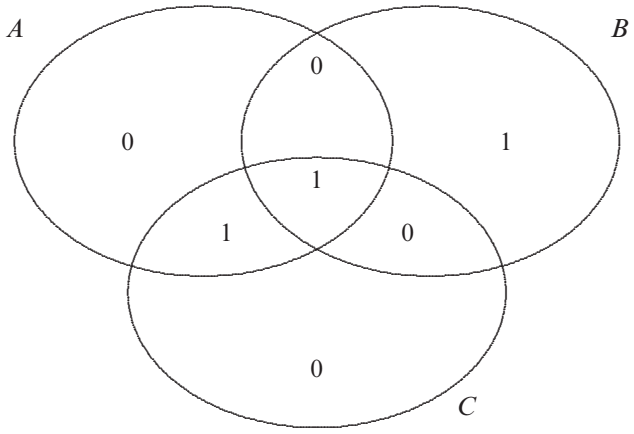
Voorbeeld 2.6.3 Onderstellen we dat de beschikbare informatie opgeslagen wordt onder de vorm van "woorden" van lengte 4 in de twee tekens 0 en 1 (of eventueel combinaties van dergelijke woorden). Er zijn 16 woorden van lengte 4 die gebouwd kunnen worden m.b.v. twee tekens. We sommen even op

De te versturen boodschappen.							
0000	0001	0010	0011	0100	0101	0110	0111
1000	1001	1010	1011	1100	1101	1110	1111

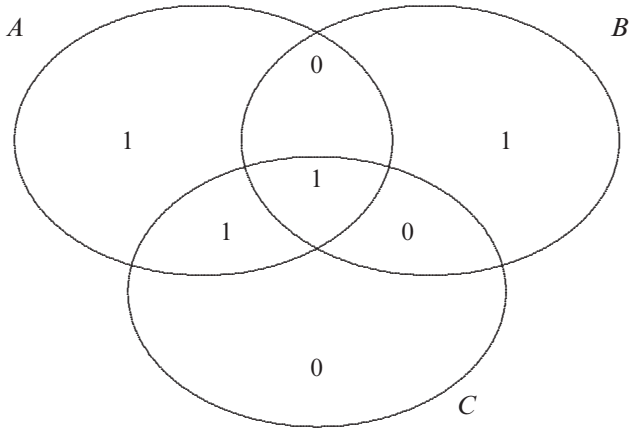
Met behulp van deze woorden kunnen boodschappen samengesteld worden; deze boodschappen wensen we te versturen. Onderweg kunnen allerlei invloeden evenwel het ontstaan van kleine, af en toe voorkomende, foutjes veroorzaken. In een poging om de informatie beter te beschermen tegen deze ongewenste fouten, gaan we als volgt te werk.
In plaats van woorden van lengte 4 te versturen, zullen we elk woord wat langer maken ("coderen") en deze langere woorden versturen. Deze werkwijze kan gevisualiseerd worden aan de hand van het volgende Venn-diagram.



In dit Venn-diagram zijn er 7 gebieden te onderscheiden, die genummerd zijn met een teken van a tot en met g. Welnu, voor we een woord versturen, plaatsen we het in dit Venn-diagram: het eerste teken van het woord in gebied a, het tweede teken in gebied b, het derde teken in gebied c en het vierde teken in gebied d. Daarna plaatsen we in de overblijvende drie gebieden (e, f en g) telkens één teken, een 0 of een 1, zó dat de som van alle tekens in de gebieden van één verzameling (A, B of C) telkens even wordt.
Deze werkwijze is hieronder uitgevoerd voor het woord 0110.



Het woord dat we wensen te versturen, 0110, zal daarom verstuurd worden als 0110010, een codewoord van 7 tekens. Hiervan bevatten enkel de eerste 4 tekens de informatie, de laatste 3 tekens werden door de codeerwijze hierboven toegevoegd.
Het is duidelijk dat deze werkwijze leidt tot een vertraging in de verzending van boodschappen. Alhoewel dit een nadeel lijkt, staat daar tegenover ook een belangrijk voordeel. We lichten dit toe. Onderstel dat het gecodeerde woord 0110010 verstuurd wordt, maar dat er onderweg door een of andere storing een foutje optreedt waarbij één teken veranderd wordt. De ontvanger registreert b.v. het codewoord 0110110. We onderzoeken dit ontvangen codewoord even aan de hand van ons Venn-diagram. Daartoe plaatsen we de tekens van dit woord in de gebieden a tot en met g van het Venn-diagram. Dan zien we



De som van de tekens in elke verzameling van dit Venn-diagram moet steeds even zijn. Voor de verzameling A noteren we als som $0+1+1+1$: oneven! In de verzameling B stellen we vast: $0+1+1+0$: even! In de verzameling C ten slotte is de som $1+1+0+0$: ook even! Enkel in de verzameling A loopt iets mis. Daarom is het teken in gebied e fout. De ontvangen boodschap is dus niet correct, en moet vervangen worden door 0110010, de oorspronkelijk verzonden boodschap!

Opdracht 2.6.4

1. Ga na hoe de andere woorden uit onze tabel hierboven gecodeerd worden.
2. Stel aan de hand van een drietal voorbeelden vast dat een foutje op 1 plaats steeds door dit systeem ontdekt èn gelocaliseerd (en dus hersteld) wordt.

We eindigen dit voorbeeld met de lijst van de gecodeerde boodschappen:

De gecodeerde boodschappen.			
0000000	0001011	0010111	0011100
0100101	0101110	0110010	0111001
1000110	1001101	1010001	1011010
1100011	1101000	1110100	1111111

Het voorbeeld illustreert op een heldere manier hoe we een boodschap ("de echte informatie") kunnen beschermen tegen optredende fouten, door die boodschap aan te vullen met extra gegevens die bepaalde informatie over de boodschap in zich dragen.

> Dit mag ons niet verwonderen. Ook in het gewone taalgebruik gebeurt dit; de extra gegevens zijn daar "de contekst" waarin onze informatie opgenomen wordt. Precies die contekst (vaak met strikt gezien overbodige zaken) laat toe kleine fouten als het ware spontaan te herkennen en te herstellen. Een telegramboodschap
>
> `Gisterenavond aangelomen. Iede reenveilig. Groefjes.`
>
> zal weinig verwarring stichten. In een document zorgt de contekst van een boodschap als het ware voor "overtallige" informatie. Het is deze zelfde techniek, gebaseerd op overtalligheid (in het Engels "redundancy") die aan de basis ligt van de foutenherstellende codeersystemen.

Voorbeeld 2.6.5 Het hierboven in het voorbeeld getoonde systeem kunnen we nu van uit een andere invalshoek opnieuw bekijken. De te versturen boodschappen waren woorden in de tekens 0 en 1. Werken met zo'n "binaire" woorden is veruit het meest frequent gehanteerde systeem wanneer informatie m.b.v. computers moet verwerkt of doorgegeven worden. We spreken daarom van binaire codes.
Deze twee tekens (getallen) doen ons meteen ook denken aan $\mathbb{Z}_2$ en aan rekenen modulo 2. Inderdaad, de informatie die verstuurd moest worden in het voorbeeld, kan nu opgevat worden als bestaande uit viertallen van elementen uit $\mathbb{Z}_2$. De beschikbare woorden vormen, zo gezien, precies de gehele verzameling $\mathbb{Z}_2^4 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Ook het coderen van de boodschappen, dat we aan de hand van het Venn-diagram uitvoerden, kan nu geïnterpreteerd worden; als $x_1x_2x_3x_4$ een woord was, werd dit in het voorbeeld gecodeerd als

$$x_1x_2x_3x_4 \overset{\text{coderen}}{\longrightarrow} x_1x_2x_3x_4x_5x_6x_7,$$

waarbij

$$x_5 = \begin{cases} 0 \text{ als } x_1 + x_2 + x_3 \text{ even is} \\ 1 \text{ als } x_1 + x_2 + x_3 \text{ oneven is} \end{cases}$$

en analoge voorwaarden voor x_6 en x_7. Gebruik makend van de optelling modulo 2 betekent dit niets anders dan dat

$$\begin{cases} x_5 \equiv x_1 + x_2 + x_3 \bmod 2 \\ x_6 \equiv x_1 + x_3 + x_4 \bmod 2 \\ x_7 \equiv x_2 + x_3 + x_4 \bmod 2 \end{cases}$$

of

$$\begin{cases} x_1 + x_2 + x_3 + x_5 \equiv 0 \bmod 2 \\ x_1 + x_3 + x_4 + x_6 \equiv 0 \bmod 2 \\ x_2 + x_3 + x_4 + x_7 \equiv 0 \bmod 2 \end{cases}$$

Deze vergelijkingen worden de pariteitscontrole-vergelijkingen genoemd. Ze kunnen samengevat weergegeven worden door middel van een matrix H, de pariteitscontrole-matrix, als volgt. Elke pariteitscontrole-vergelijking zorgt voor één rij van de matrix H. In die rij noteren we een 1 in

de kolommen van de variabelen die optreden in de betreffende vergelijking, en een 0 in de andere kolommen. De pariteits-controlematrix H wordt hier dus

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Het vergt nu geen grote inspanning meer om dit codeersysteem voor te stellen als een afbeelding

$$\begin{array}{rccl} c: & \mathbb{Z}_2^4 & \to & \mathbb{Z}_2^7 \\ & (x_1,x_2,x_3,x_4) & \mapsto & (x_1,x_2,x_3,x_4)\cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (x_1,x_2,x_3,x_4)\cdot G \end{array}$$

waarin we de matrix G de voortbrengende of genererende matrix van de code noemen. Deze matrix G staat hier in "standaard vorm", wat betekent dat de matrix - gelezen van links naar rechts - 'begint' met de (4×4)-eenheidsmatrix $\mathbb{1}_4$.

Deze vaststelling brengt ons weer volop in de algebra, ditmaal de algebra van de vectorruimten en de lineaire afbeeldingen. De "codeer"-afbeelding c is immers niets anders dan een (matrixvoorstelling van een) lineaire afbeelding van de vectorruimte $(\mathbb{Z}_2, \mathbb{Z}_2^4, +)$ naar de vectorruimte $(\mathbb{Z}_2, \mathbb{Z}_2^7, +)$. De bewerkingen + en . zijn natuurlijk die van in $\mathbb{Z}_2$!
Het hier getoonde codeersysteem wordt een $(7,4)-$lineaire (binaire) code genoemd, omdat de verzameling van de gecodeerde woorden precies een 4-dimensionale deelvectorruimte van $\mathbb{Z}_2^7$ vormt. Dit kunnen we zien we aan de rang van de matrixvoorstelling van c; deze rang is precies de dimensie van het beeld van de afbeelding c. Elk codewoord is dus te schrijven als lineaire combinatie van de rijen van deze matrix. B.v.

$$0111001 = 0100101 + 0010111 + 0001011.$$

Dit codeersysteem is een bijzonder geval van een grote familie lineaire codes, bedacht door Richard Hamming (1915 - 1998); deze familie staat bekend onder de naam van Hamming-codes. Het voorbeeld hier geeft een Hamming $(7,4)$-code.

Meer algemeen geldt

Definitie 2.6.6 Een binaire $(n,k)-$lineaire code is een k-dimensionale deelvectorruimte C van $\mathbb{Z}_2^n$. De elementen van C worden de codewoorden genoemd. De verhouding k/n is de informatieverhouding van de code.
I.p.v. de gewone $n-$tallen notatie voor de elementen van C, schrijven we de elementen van C vaak als woorden aaneengeschreven op. Het woord 0101110 staat dus voor $(0,1,0,1,1,1,0) \in \mathbb{Z}_2^7$.

Voorbeeld 2.6.7

1. De verzameling $\{00000, 11111\}$ is een 1-dimensionale deelvectorruimte van $\mathbb{Z}_2^5$ en is dus een $(5,1)$-lineaire code. De informatieverhouding is $1/5$.

2. De verzameling $\{0000, 0101, 1010, 1111\}$ is een $(4,2)$-lineaire code. Men ziet dit door vast te stellen dat $0101 + 1010 = 1111$.

3. Elke lineaire afbeelding

$$f_G : \mathbb{Z}_2^k \to \mathbb{Z}_2^n : (x_1, x_2, \ldots, x_k) \mapsto (x_1, x_2, \ldots, x_k)\cdot G$$

waarin G een $(k \times n)$-matrix is van rang k, bepaalt een binaire (n,k) lineaire code $C = \mathrm{Im}(f_G)$. G wordt de voortbrengende matrix genoemd. We zeggen dat de voortbrengende matrix in standaardvorm staat, als $G = (\mathbb{1}_k\ *)$.

Oefening Is de verzameling $\{0000000, 0010111, 0101011, 1001101, 1100110, 1011010, 0111100, 1110001\}$ een lineaire code? Leg uit waarom of waarom niet. Zo ja, bepaal haar parameters n en k.

Weten dat een bepaalde code een lineaire code is, heeft enkele opmerkelijke gevolgen. Dit zal blijken uit de volgende begrippen en toepassingen.

Definitie 2.6.8 De Hamming-afstand tussen twee codewoorden van een lineaire code is het aantal posities waar de tekens in die woorden verschillend zijn. Het Hamming-gewicht van een codewoord uit een lineaire code is het aantal niet-nul tekens in dat woord.
Als u en v codewoorden zijn van een lineaire code C, noteren we $d(u, v)$ voor hun Hamming-afstand en we noteren $w(u)$ voor het Hamming-gewicht van het woord u.

Voorbeeld 2.6.9

1. In de Hamming $(7, 4)$-code geldt:

$$d(0101110, 1011010) = 4 \text{ terwijl } w(0110010) = 3.$$

2. In de $(5, 1)$-lineaire code hierboven, geldt

$$d(00000, 11111) = 5 \text{ en } w(00000) = 0.$$

3.

De gewichten van de Hamming $(7,4)-$codewoorden.			
0000000 0	0001011 3	0010111 4	0011100 3
0100101 3	0101110 4	0110010 3	0111001 4
1000110 3	1001101 4	1010001 3	1011010 4
1100011 4	1101000 3	1110100 4	1111111 7

De volgende eigenschap is eenvoudig vast te stellen:

Eigenschap 2.6.10 Voor elke drie codewoorden u, v en w van een lineaire code geldt

1. $d(u, v) \geq 0$
2. $d(u, v) = d(v, u)$ (symmetrie)
3. $d(u, v) \leq d(u, w) + d(w, v)$ (driehoeksongelijkheid)
2. $d(u, v) = w(u - v)$.

De eerste drie eigenschappen zijn de kenmerkende eigenschappen voor een afstandsfunctie of metriek (ze worden vaak M1, M2 en M3 genoemd).

Tot hiertoe spraken we vooral over het coderen van een boodschap. Er is evenwel ook het aspect "decoderen". Een vaak gebruikt principe om ontvangen codewoorden te decoderen is "dichtste-buur-decodering". Deze methode gaat uit van de onderstelling dat van elk ontvangen codewoord v het oorspronkelijk gezonden codewoord u datgene was waarvoor $d(u, v)$ het kleinst is (in het geval dat er twee zo'n dichtste buren zijn, kan beslist worden niet te decoderen of kan men ook willekeurig één van beide kiezen).

De volgende stelling formuleert voor ons wat we allicht ook intuitief aanvoelen als capaciteit om fouten te detecteren of verbeteren.

Stelling 2.6.11 Als het Hamming-gewicht van elk niet-nul-codewoord in een lineaire code ten minste gelijk is aan $2t+1$, dan kan die code elk ontvangen woord waarin ten hoogste t fouten optraden, correct decoderen (de correctiecapaciteit van de code in dit geval dus t). Bovendien zal diezelfde code voor elk ontvangen woord waarin ten hoogste $2t$ fouten optraden, een fout detecteren (de detectiecapaciteit is dus $2t$).

Betekenis: Het minimum gewicht van een lineaire code bepaalt meteen hoeveel fouten die code maximaal correct kan corrigeren en hoeveel fouten ze kan detecteren. Als de code t codewoorden telt, volstaat het deze codewoorden alle één keer te overlopen om dit minimum gewicht te bepalen. Wil men het dichtste-buur-decoderingsprincipe toepassen op een niet-lineaire code met k codewoorden, dan moet voor elk ontvangen woord de dichtste buur bepaald worden; hiervoor moeten alle onderlinge afstanden tussen twee codewoorden berekend worden: dit zijn $k(k-1)/2$ vergelijkingen.

Bewijs: Onderstel dat een codewoord u verzonden wordt en dat dit ontvangen wordt met ten hoogste t fouten; we noemen het ontvangen woord v. Dus $d(v,u) \leq t$. Noteer x voor een willekeurig codewoord dat verschilt van u. Dan is $x-u$ een niet-nul codewoord (want de code is linear). Dus volgt uit eigenschap 2.6.10 dat

$$2t+1 \leq w(x-u) = d(x,u) \leq d(x,v) + d(v,u) \leq d(x,v) + t$$

en dus,

$$t+1 \leq d(x,v).$$

Elk codewoord x ligt dus op een grotere Hamming-afstand van het ontvangen woord v, dan het oorspronkelijk verstuurde woord u. Het dichtste-buur-decoderingsprincipe verzekert ons dus van een correcte decodering van het ontvangen woord v.
Onderstellen we nu dat het verzonden codewoord u als woord v ontvangen werd, en dat er tijdens de verzending minstens 1 en hoogstens $2t$ fouten optraden. Vermits het systeem er van uit gaat dat enkel codewoorden (d.w.z. elementen van C) verstuurd worden, wordt de fout ontdekt van zodra het ontvangen woord v geen codewoord is. Welnu, v kan geen codewoord zijn, want anders zou ook $v-u$ een niet-nul codewoord zijn ; maar dan zou $w(v-u) = d(v,u) \leq 2t < 2t+1$, terwijl $2t+1$ het minimum Hamming gewicht is van elk niet-nul codewoord uit de code : een contradictie.

Q.E.D.

Gevolg 2.6.12

1. De $(7,4)$-lineaire code heeft minimum Hamming-gewicht gelijk aan 3 (verifieer in de tabel hierboven). Daarom zal deze code alle enkelvoudige fouten correct kunnen corrigeren en zal ze alle dubbele fouten detecteren.

2. De $(5,1)$-lineaire code $C = \{00000, 11111\}$ heeft minimum Hamming-gewicht 5 en verbetert daarom tot 2 optredende fouten; ze detecteert tot 4 optredende fouten.

Stelling (2.6.11) mag niet foutief geïnterpreteerd worden. Een foutieve interpretatie zou zijn van te denken dat een lineaire code met Hamming-gewicht $2t+1$ t fouten kan corrigeren én $2t$ fouten kan detecteren. In werkelijkheid is het een of het ander, en de gebruikers van de code moeten vooraf duidelijk maken in welke rol ze de code zullen gebruiken. Om dit duidelijker te maken, de volgende overweging: beschouw de Hamming (7,4)-code (Hamming-gewicht 3), en veronderstel dat het woord 0001010 ontvangen werd. Het bedoelde (en verzonden) woord kan dan 0000000 zijn geweest (wat betekent dat er 2 foutjes werden gemaakt), maar het bedoelde woord kan ook 0001011 zijn geweest, waarbij er dan 1 foutje werd gemaakt. Zonder duidelijke afspraak vooraf, hoe de code zal worden aangewend, hebben we zo een situatie dit tot verwarring zal leiden.

Indien de (n,k)-lineaire code bepaald wordt via een voortbrengende matrix G in standaardvorm, m.a.w. een matrix G van de vorm

$$G = \begin{pmatrix} \mathbb{1}_k & A \end{pmatrix}$$

waarin A een $(k \times (n-k))$ matrix is, dan kun je een matrix H vormen

$$H = \begin{pmatrix} -A^t & \mathbb{1}_{n-k} \end{pmatrix}.$$

H noemt men de pariteitscontrole matrix, en heeft afmetingen $(n-k) \times n$. Deze pariteitscontrole matrix is erg behulpzaam bij het decodeerproces. Immers,

Stelling 2.6.13 Als C een binaire (n,k)-lineaire code is, bepaald door een voortbrengende matrix G in standaardvorm, en met pariteitscontrole matrix H, dan geldt:

$$\forall v \in \mathbb{Z}_2^n : v \cdot H^t = 0 \Leftrightarrow v \in C.$$

Bewijs: Noteer dat de matrix H^t een $(n \times (n-k)$ matrix is. We kunnen dus de afbeelding

$$f_{H^t} : \mathbb{Z}_2^n \to \mathbb{Z}_2^{n-k} : v = (x_1, \ldots, x_n) \mapsto v \cdot H^t$$

beschouwen.
Onderstel dat $v \in C$, d.w.z. $v = (x_1, \ldots, x_k) \cdot G$ voor een zekere $(x_1, \ldots, x_k) \in \mathbb{Z}_2^k$. Dan geldt

$$v \cdot H^t = (x_1, \ldots, x_k) \cdot \begin{pmatrix} \mathbb{1}_k & A \end{pmatrix} \cdot \begin{pmatrix} -A \\ \mathbb{1}_{n-k} \end{pmatrix} = 0$$

Omgekeerd, de verzameling van de vectoren $v \in \mathbb{Z}_2^n$ waarvoor $v \cdot H^t = 0$, is precies de nulruimte (of de kern) van de lineaire afbeelding f_{H^t}. Daar de matrix H^t rang $(n-k)$ heeft, is de dimensie van de kern van deze afbeelding gelijk aan k (dimensiestelling). Deze nulruimte bevat echter de code C, zelf een k-dimensionale deelruimte, en moet dus gelijk zijn aan C.

Q.E.D.

Dichtste buur decodering m.b.v. de pariteitscontrolematrix. Met behulp van deze pariteitscontrolematrix H, kan nu een meer praktische manier van werken voor het "dichtste buur" decoderen afgesproken worden. We veronderstellen een binaire (n,k)-lineaire code met standaard genererende matrix G en pariteitscontrolematrix H. Dit gaat als volgt:

Stap 1. bereken voor elk ontvangen woord w, $w \cdot H^t$;

Stap 2. als $w \cdot H^t = 0$, ga er dan van uit dat er geen fout gebeurde, en aanvaard w;

Stap 3. als $w \cdot H^t$ gelijk is aan de i-de rij van H^t, voor precies één i, ga er dan van uit dat er precies één fout gebeurde en wel op de i-de plaats van w. Als $w \cdot H^t$ gelijk is aan meer dan één rij in H^t, decodeer dan niet (en vraag b.v. om het woord opnieuw door te sturen);

Stap 4. in alle andere gevallen, ga er van uit dat er minstens 2 fouten gebeurden onderweg, en decodeer niet.

Over dit praktisch decodeer procédé hebben we volgend resultaat.

Stelling 2.6.14 Het decoderen m.b.v. de pariteitscontrolematrix H, zoals hierboven geschetst voor een binaire (n,k)-lineaire code met een genererende matrix G in standaardvorm, corrigeert elke enkelvoudige fout als en slechts als de kolommen van H onderling verschillend zijn en verschillen van 0.

Bewijs Veronderstel dat H onderling verschillende kolommen heeft, die niet 0 zijn. Veronderstel dat een codewoord v werd doorgestuurd en ontvangen als w en dat hierbij 1 fout optrad, meer bepaald in de i-de component van w. Laat ons $e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ noteren voor de vector die alleen op i-de positie een 1 heeft staan, en elders 0. Dan hebben we dus $w = v + e_i$. Bijgevolg

$$w \cdot H^t = (v + e_i) \cdot H^t = v \cdot H^t + e_i \cdot H^t = e_i \cdot H^t.$$

Dit is precies de i-de rij in H^t en dus de i-de kolom in H.
Veronderstel nu dat het decoderen m.b.v. H elke enkelvoudige fout corrigeert. Als b.v. de i-de kolom in H gelijk zou zijn aan 0, dan kan b.v. het codewoord $00\ldots0$ - in de veronderstelling van 1 fout - ontvangen zijn als e_i, en dan zouden we, vermits $e_i \cdot H^t = 0$ besluiten dat er geen fout opgetreden was. Veronderstel dat in H twee gelijke kolommen optreden, b.v. de i-de en de j-de kolom. Als een codewoord v ontvangen wordt als b.v. $v + e_i$ (met dus 1 foutje), dan vinden we

$$(v + e_i) \cdot H^t = e_i \cdot H^t = \text{ rij } i \text{ in } H^t = \text{ rij } j \text{ in } H^t$$

en volgens de afgesproken decodeerprocedure, decoderen we in dit geval niet. Er kunnen dus geen twee gelijke kolommen in H optreden.

Q.E.D.

Definitie 2.6.15 Een binaire Hamming code is een $(2^r - 1, 2^r - 1 - r)$-lineaire code met $r \in \mathbb{N} \setminus \{0, 1\}$.

Opmerking 2.6.16
De informatieverhouding neemt toe bij toenemende r, m.a.w. de rij

$$\left(\frac{2^r - 1 - r}{2^r - 1}\right)_{r \in \mathbb{N}\setminus\{0,1\}} = \frac{1}{3}, \frac{4}{7}, \frac{11}{15}, \frac{26}{31}, \ldots \text{ is een stijgende rij en}$$

$$\lim_{r \to +\infty} \frac{2^r - 1 - r}{2^r - 1} = 1.$$

Voorbeeld 2.6.17 De Hamming $(15, 11)$-binaire-code wordt verkregen met behulp van de pariteits-controlematrix H gegeven door

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Vertrekkend van een woord van lengte 11, wordt het bijhorende codewoord (van lengte 15) dus gevormd door er 4 tekens (resp. $x_{12}, x_{13}, x_{14}, x_{15}$) aan toe te voegen zó dat de rijen van de matrix H, geïnterpreteerd als pariteits-controle-vergelijkingen, vervuld zijn. Zo staat de derde rij van H b.v. voor de vergelijking:

$$x_3 + x_4 + x_5 + x_6 + x_8 + x_{10} + x_{11} + x_{14} \equiv 0 \bmod 2.$$

Opmerking 2.6.18
De pariteits-controlematrix H van de Hamming $(15, 11)$-binaire code, laat een bijzondere eigenschap zien. Elke rij in die matrix is een copie van de rij erboven, evenwel met een verschuiving van 1 positie naar rechts. Dit heeft voor gevolg dat voor elk codewoord $x_1x_2x_3\ldots x_{15}$ uit deze code het woord $x_{15}x_1x_2x_3\ldots x_{14}$ ook een codewoord zal zijn. Codewoorden blijven m.a.w. codewoorden wanneer we ze cyclisch doorschuiven (permuteren).
De $(15, 11)$-binaire Hamming code is daarom een cyclische code. Dit cyclisch karakter is van groot praktisch nut voor electronische toepassingen van de code ([9]).
Het nakijken van de codewoorden van $(7, 4)$-binaire Hamming code leert dat die code, zo voorgesteld, blijkbaar die cyclische eigenschap niet heeft. Men moet hier echter de vraag meer algemeen stellen, en afvragen of er geen equivalente binaire, lineaire $(7, 4)$-code bestaat die wel cyclisch is.
Meer diepgaand wiskundig onderzoek leert dat alle binaire Hamming-codes equivalent zijn met een cyclische code, en daarom kortweg cyclisch genoemd worden. Dit bewijzen kan echter niet zonder een grondiger studie van b.v. eindige velden. Hier wordt immers het resultaat gebruikt dat de multiplicatieve deelgroep van elk eindig veld (Galoisveld) cyclisch is.
Dit resultaat, gebaseerd op een abstract wiskundig onderzoek, is van groot praktisch nut (ingenieurtechnisch) is voor het gebruik van Hamming-codes in toepassingen.

Voorbeeld 2.6.19
De codewoorden van een cyclische voorstelling van de Hamming $(7,4)$-code zijn

Codewoorden in een cyclische Hamming $(7,4)$-code			
0000000	1010001	1110010	0100011
0110100	1100101	1000110	0010111
1101000	0111001	0011010	1001011
1011100	0001101	0101110	1111111

Een voortbrengende matrix (matrix van een lineaire afbeelding $c' : \mathbb{Z}_2^4 \to \mathbb{Z}_2^7$) voor deze codewoorden is

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Opmerking 2.6.20
De Hamming-codes hebben nog een bijzondere eigenschap, die hier het vermelden waard is.
Bekijken we daarvoor even opnieuw de Hamming $(7,4)$-code. Deze code telt 16 codewoorden en kan enkelvoudige fouten corrigeren (stelling 2.6.11). M.a.w. elk (binair) woord van lengte 7 dat slechts op ten hoogste 1 plaats van een codewoord verschilt zal als dát codewoord gedecodeerd worden. Voor elk van de 16 codewoorden (van de Hamming $(7,4)$-code) zijn er telkens precies 8 woorden (van lengte 7) die ten hoogste op 1 plaats van dat codewoord verschillen. Brengen we deze 8 codewoorden telkens samen in een deelverzameling, dan verkrijgen we op die wijze 16 disjuncte (!) verzamelingen. Samen tellen ze $16.8 = 128$ elementen en vormen ze dus een partitie van de gehele verzameling $\mathbb{Z}_2^7$ van alle binaire woorden van lengte 7. De Hamming $(7,4)$-code wordt daarom 1-perfect of kortweg "perfect" genoemd. Dit resultaat wordt visueel gemaakt in de tabel hierna.

Een analoge eigenschap geldt voor alle Hamming-codes. De Hamming-codes corrigeren enkelvoudige fouten. Het minimum-gewicht van de codewoorden is telkens 3. Voor elk codewoord u kan men de verzameling vormen van de woorden (van lengte n), die op Hamming-afstand kleiner of gelijk aan 1 van dat codewoord u liggen. Zo'n verzameling noemen we een bol met middelpunt u en straal 1. Welnu, deze bollen vormen een partitie van de verzameling van alle woorden van lengte n. Daarom noemt men Hamming-codes perfect, zoals we in de tabel hieronder laten zien in het geval van de $(7,4)$-code.

Alle elementen van $\mathbb{Z}_2^7$ in een "sphere packing" systeem - de codewoorden zijn onderlijnd (Hamming(7,4) is PERFECT)			
0000000	0000011	0000111	0001100
0000001	0001001	0010011	0010100
0000010	0001010	0010101	0011000
0000100	0001011	0010110	0011100
0001000	0001111	0010111	0011101
0010000	0011011	0011111	0011110
0100000	0101011	0110111	0111100
1000000	1001011	1010111	1011100
0000101	0001110	0010010	0011001
0100001	0100110	0100010	0101001
0100100	0101010	0110000	0110001
0100101	0101100	0110010	0111000
0100111	0101110	0110011	0111001
0101101	0101111	0110110	0111010
0110101	0111110	0111010	0111101
1100101	1101110	1110010	1111001
0000110	0001101	0010001	0011010
1000010	1000101	1000001	1001010
1000100	1001001	1010000	1010010
1000110	1001100	1010001	1011000
1000111	1001101	1010011	1011010
1001110	1001111	1010101	1011011
1010110	1011101	1011001	1011110
1100110	1101101	1110001	1111010
0100011	0101000	0110100	0111111
1000011	1001000	1010100	1011111
1100001	1100000	1100100	1101111
1100010	1101000	1110000	1110111
1100011	1101001	1110100	1111011
1100111	1101010	1110101	1111101
1101011	1101100	1110110	1111110
1110011	1111000	1111100	1111111

2.7 ICT-toepassing: orde van een element in $(Z_p \setminus \{0\}, \cdot)$.

Het volgende programma berekent de orde van een element G van de groep $Z_P \setminus \{0\}, \cdot$: het programma is eigenlijk een combinatie van de programma's BINEXP en MACHTMOD van het deel Algebra en Getaltheorie. We hebben expliciet het programma helemaal neergeschreven zodat het onafhankelijk van de beide andere programma's werkt. In essentie worden alle machten van G modulo P berekend, tot een macht gelijk is aan 1.

```
PROGRAM:ORDE
  Prompt P
  Prompt G
  2 → L
  While L ≠ P
    1 → dim(⌊BINR )
    1 → dim(⌊BIN )
    1 → I
```

```
L → K
While iPart(K/2) ≠ 0
  K-2*iPart(K/2)→ ⌊BINR(I)
  iPart(K/2)→K
  I+1→I
End
1 → ⌊BINR(I)
dim(⌊BINR ) → D
For(J, 0, D − 1)
  ⌊BINR(D − J) → ⌊BIN(J + 1)
End
1 → B
G → Q
If ⌊BINR(1) = 1
Then
  G → B
End
For(I, 2, dim(⌊BIN))
  Q² − P ∗ iPart(Q²/P) → Q
  If ⌊BINR(I) = 1
  Then
    Q ∗ B − P ∗ iPart(Q ∗ B/P) → B
  End
End
If B=1
Then
  Disp "DE ORDE VAN",G,"IS",L
  Stop
End
L + 1 → L
End
```

2.8 Historische noten

2.8.1 Ronald L. Rivest

Ronald R. Rivest werd geboren in 1947 in Schenectady, NY, USA. Hij werd Bachelor of Science in Wiskunde in 1969 aan Yale University en behaalde een doctoraat in computerwetenschappen in 1974 aan Stanford University. Hij is nu professor computerwetenschappen aan M.I.T. (Massachusetts Institute of Technology), waar hij voorzitter is van de "Cryptography and Information Security Group". Hij verricht onderzoek in cryptografie, netwerk- en computerbeveiliging en algoritmen. Hij ontwierp naast het RSA-algoritme, samen met Shamir en Adleman in 1977, ook de algoritmes voor symmetrische sleutel-encryptie RC2, RC4, RC5 en was co-uitvinder van RC6 (RC staat voor 'Rivest cypher' of 'Ron's code'). Hij is tevens lid van de National Academy of Engineering en van de National Academy of Sciences. Samen met Shamir en Adleman kreeg hij in 2000 de IEEE Koji Kobayashi Computers and Communications Award en in 2002 de ACM Turing Award (genaamd naar de beroemde Engelse Wiskundige Allan Turing, die er in de tweede wereldoorlog in slaagde de nazi-code Enigma te kraken).

2.8.2 Adi Shamir

Adi Shamir werd geboren in 1952 in Tel Aviv, Israel. Hij werd Bachelor of Science in Wiskunde aan de Tel-Aviv University in 1973. Hij werd Master of Science en doctor in de computerwetenschappen

in resp. 1975 en 1977 aan het Weizmann Institute in Rehovor, Israel, waar hij sedert 1984 professor Wiskunde is en computerwetenschappen doceert. Tussendoor verrichtte hij van 1977 tot 1980 onderzoek aan M.I.T. Naast RSA is hij ook bekend voor het breken van het Merkle-Hellman systeem en verrichtte hij onderzoek in visuele cryptografie. Hij ontdekte, samen met Eli Biham, de zogenaamde differentiaal-crypto-analyse (later bleek dat dit al ontdekt was maar geheim gehouden werd door zowel I.B.M. als N.S.A.). Hij is verweg de meest eminente specialist in crypto-analyse.

2.8.3 Leonard Adleman

Leonard (Len) Adleman werd geboren in 1945 in Tel Aviv, Israel. Hij werd Bachelor of Science en doctor in de Wiskunde aan de University of California, Berkeley in resp. 1968 en 1976. Naast RSA is hij ook gekend voor het berekenen van DNA en was hij actief in Grafentheorie: in zijn oplossing voor een onderdeel van het Hamiltoniaanse graaf probleem werd voor de eerste keer DNA gebruikt om een algoritme te berekenen. Het berekenen van DNA blijkt geschikt te zijn voor het oplossen van verschillende combinatorische problemen.
Hij zou ook de eerste geweest zijn om de term 'virus' te gebruiken (in de context van computervirussen).
Als leuke bijkomstigheid willen we nog vermelden dat hij de Wiskundige consulent was bij de film 'Sneakers' van Larry Lasker.

2.8.4 Richard Hamming

Richard Hamming werd geboren in 1915 in Chicago,IL,USA en overleed in 1998 in Monterey,CA,USA.
HIj werd Bachelor of Science aan de University of Chicago in 1937 en ging dan naar de University of Nebraska, waar hij in 1939 Master of Science werd; in 1942 behaalde hij zijn doctoraat aan de University of Illinois in Urbana-Champaign.
In 1945 ging hij bij het 'Manhattan Project', een project van de Amerikaanse regering om een atoombom aan te maken. In 1946, na het einde van de tweede wereldoorlog, ging hij werken bij Bell Laboratories; hij bleef er tot 1976, toen hij professor in de Computerwetenschappen werd aan de Naval Postgraduate School in Monterey in Californië.
Zijn hoofdartikel over Hamming-codes verscheen in 1950. In 1956 werkte hij mee aan één van de eerste computers, de IBM 650: zijn bijdrage daarin leidde tot de ontwikkeling van een programmeertaal, die geëvolueerd is tot de computertalen die gebruikt worden om de hedendaagse computers te besturen.
Tevens verrichtte hij onderzoek in Numerieke Analyse.
HIj ontving verschillende prijzen voor zijn werk, waaronder in 1968 de Turing-prijs vanwege The Association for Computing Machinery en in 1988 een medaille vanwege de IEEE voor "uitzonderlijke bijdragen tot informatie-wetenschappen en systemen"; de IEEE heeft deze medaille de Hamming medaille genoemd ter zijner ere.

2.8.5 Whitfield Diffie en Martin Hellman

Whitfield Diffie werd geboren in 1944. Hij werd Bachelor of Science in Wiskunde aan M.I.T. in 1965 en behaalde een doctoraat in de Technische Wetenschappen aan het 'Swiss Federal Institute of Technology' in 1992. Hij is vooral gekend voor zijn ontdekking in 1975 van het concept van publieke sleutel cryptografie: het hoofdartikel daarover "New Directions in Cryptography" verscheen in 1976 (samen met M. Hellman). In de jaren '90 werkte hij vooral op de publieke aspecten van cryptografie waarbij hij verscheidene keren als getuige optrad in de Senaat en de Kamer van Volksvertegenwoordigers. Zijn positie daaromtrent wordt weergegeven in het boek 'Crypto' door Steven Levy van Newsweek. Hij schreef ook in 1998 samen met Susan Landau het boek 'Privacy on the Line' over het aftappen van telefoons en over encryptie.
Hij kreeg verscheidene prijzen, o.a. van IEEE en NSA.

In de jaren '80 was hij Manager of Secure Systems Research voor Northern Telecom en in 1991 werd hij Chief Security Officer bij Sun Microsystems, een functie die hij nog steeds bekleedt. Hij is er tevens Vice President en Sun Fellow.

Martin Hellman werd geboren in 1945. HIj werd Bachelor of Science aan de New York University in 1966 en ging dan naar de Stanford University, waar hij een jaar later Master of Science werd en in 1969 een doctoraat behaalde, dit alles in ingenieurswetenschappen.
IN de jaren 1968-69 werkt hij bij IBM's Watson Research Center en van 1969 tot 1971 was hij assistent professor aan M.I.T. In 1971 keerde hij terug naar Stanford waar hij in 1996 Professor Emeritus werd.

2.8.6 Taher ElGamal

(http://en.wikipedia.org/wiki/Taher˙ElGamal)
Taher ElGamal werd Bachelor of Science aan de Universiteit van Cairo en behaalde dan zijn Master diploma en doctoraat aan de Stanford University. In 1985 publiceerde hij zijn artikel 'A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms': het cryptosysteem dat daarin beschreven wordt, is de basis voor het Digital Signature Algorithm (DSA), dat als standaard aanvaard wordt door het National Institute of Standards and Technology (NIST). Hij maakte ook deel uit van het 'SET' betalingsprotocol voor kredietkaarten.
HIj was van 1995 tot 1998 hoofdwetenschapper bij Netscape Communications. Hij was ook directeur bij RSA Security Inc., vooraleer hij in 1998 het bedrijf 'Securify' oprichtte en er CEO werd. Nadat het bedrijf enige tijd overgenomen werd, is het nu weer zelfstandig en bekleedt hij er de functie van Chief Technical Officer & Co-chair of the Board of Directors.
Vermelden we nog dat er 2 mogelijke schrijfwijzen zijn voor zijn naam : ElGamal of Elgamal.

Bibliografie

[1] V.K. Balakrishnan, Introductory Discrete Mathematics, Prentice Hall, New Jersey, 1991

[2] J-P. Delahaye, Merveilleux Nombres Premiers, Belin, Pour la Science, Paris, 2000

[3] J. A. Gallian, Contemporary Abstract Algebra, Houghton Mifflin Company, 2002 (Fifth edition)

[4] R. Garnier and J. Taylor, Discrete Mathematics for New Technology, Adam Hilger, Bristol, 1992

[5] S. Garfunkel, For all practical purposes. Introduction to contemporary mathematics, W.H. Freeman and Company, New York 1994

[6] Raymond Hill, A First Course in Coding Theory. Clarendon Press, Oxford, 1986

[7] Indexes of Biographies. http://www-history.mcs.st-andrews.ac.uk/BiogIndex.html

[8] A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of Applied Cryptography. CRC Press, Waterloo, 1996

[9] W. Wesley Peterson, Error-correcting codes. Scientific American, 206 (2), pp. 96–108 (1962)

[10] Vlaamse Wiskunde Olympiade http://www.vwo.be/

[11] André Weil, Number Theory for Beginners, Springer-Verlag, New York, 1979