

# **BASIS-WISKUNDE**

GERARD VAN DER GEER

# Basis- Wiskunde

Gerard van der Geer

Versie 0.3, 2009



## 1. INLEIDING

Net zoals we onze moedertaal niet leren door te beginnen met het leren van expliciete grammaticale regels, maar eerst later bij nadere beschouwing deze regels expliciet maken, begint het verwerven van elementaire wiskunde meestal met het al doende leren van de regels. Pas later komt een nadere reflectie op de gebruikte regels en de fundamenteen waarop onze kennis is gebouwd. Zo zullen we het ook doen in deze inleiding in de wiskunde. We beginnen direct met echte wiskunde en leren al doende de regels van het spel. Een strenge axiomatische opbouw van bijv. verzamelingenleer en de reële getallen wordt gereserveerd voor later. Dan zijn ook de voorbeelden voorhanden waarmee deze strenge en abstracte opbouw geïllustreerd kan worden.

Een van de aantrekkelijke aspecten van de wiskunde is dat er niet veel hulpmiddelen bij nodig zijn. Pen en papier zijn vaak voldoende, al is toegang tot een computer wel handig. Zelf actief wiskunde bedrijven kan een bron van veel plezier zijn. Het begint vaak met een eigen variant op een gegeven bewijs dat eleganter of korter is dan het origineel of een generalisatie van een gegeven bewering. We hopen dat de voorbeelden aanzetten tot eigen creativiteit en het actief uitproberen van eigen gedachten.

Echte wiskunde begint bijna altijd met eenvoudige voorbeelden aan de hand waarvan algemene feiten kunnen worden afgeleid of geraden.

De hierboven gedane bewering over benodigde hulpmiddelen heeft wel enige nuancering. Een goede wiskundebibliotheek is vaak een onmisbaar hulpmiddel. Maak daarom gebruik van de geboden mogelijkheden op dit gebied. Er vallen veel interessante en verrassende dingen te ontdekken. Aarzel niet de docenten om suggesties voor geschikte literatuur te vragen; naarmate je bekender wordt met de wiskundige terminologie en grondbegrippen komt er meer literatuur in aanmerking voor een verkenningstocht.

## 2. EEN EERSTE BEGIN

*Het Getal beheerst de Kosmos*  
Pythagoras<sup>1</sup>

De vraag ‘Wat is wiskunde’ is even lastig te beantwoorden als de analoge vraag ‘Wat is muziek’. Maar net zoals bij muziek is het niet lastig wiskunde te herkennen als we wiskunde tegenkomen. Duidelijk is dat wiskunde zich bezighoudt met getallen, meetkundige figuren en meer algemeen structuren en patronen.

De eerste wiskundige activiteit van mensen (en meer algemeen waarschijnlijk van de mensheid) is het tellen en optellen van natuurlijke getallen. De natuurlijke getallen

$$\mathbb{N} := \{1, 2, 3, 4, \dots\}$$

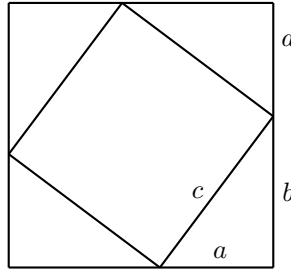
behoren tot het oudste culturele erfgoed van de mensheid. De eerste ons bekende tekenen van wiskundige activiteit dateren uit de Aurignac-periode (30.000-20.000 jaar geleden) en bestaan uit inkepingen van botten. Maar onze archeologische kennis is zeer fragmentarisch, en tel-activiteit trad wellicht al veel eerder op in de geschiedenis van de mensheid. Het abstraheren van het getalbegrip, waarbij bijvoorbeeld het getal 2 de abstractie was van alle verzamelingen die uit twee objecten bestaan (een paar ogen, een paar schoenen, een paar stenen) is een reusachtige stap in de culturele en intellectuele ontwikkeling geweest, waarvan wij alleen nog met grote moeite de moeilijkheidsgraad kunnen inschatten. Opvallend is dat in veel talen het woord voor 3 etymologisch verwant is met ‘veel’.

Bij telactiviteit komen in eerste instantie alleen de natuurlijke getallen voor. In onze definitie beginnen de natuurlijke getallen met 1. Maar vele wiskundigen nemen in hun definitie van natuurlijke getallen de nul erbij. Het is een kwestie van smaak. Maar historisch gezien is de nul bepaald niet zo natuurlijk. De nul kwam in de klassieke Griekse wiskunde nog niet voor en treedt pas op in de laat-Babylonische wiskunde (3de eeuw voor het begin van de jaartelling) en bij de Indische wiskunde in de 3de tot de 5de eeuw.

Een volgende grote stap in de geschiedenis is de ontdekking dat getallen naast tellen ook gebruikt konden worden voor meten van lengte, oppervlakte en inhoud waarbij een eenheid van lengte, oppervlakte en inhoud gekozen werd. Een eerste hoogtepunt in deze nieuwe ontwikkeling van de wiskunde was de Stelling van Pythagoras. Zowel in oude wiskundige teksten van Griekenland als die van het verre oosten (India en China) vinden we bewijzen voor deze stelling. Bij de Grieken vinden we het korte bewijs “Kijk” met de volgende figuur erbij.

---

<sup>1</sup>Pythagoras, Grieks wiskundige en filosoof, circa 569-475; wordt wel gezien als de eerste zuivere wiskundige.



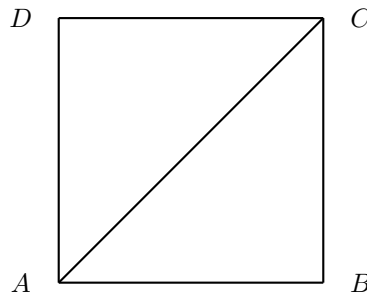
En inderdaad, als je kijkt zie je dat de oppervlakte van het vierkant gelijk is aan  $(a+b)^2$ , want de zijden hebben lengte  $a+b$ . Maar anderzijds is de oppervlakte ook gelijk aan de oppervlakte  $c^2$  van het centrale vierkant en de oppervlakte  $4 \times ab/2 = 2ab$  van de vier driehoeken. Dus

$$a^2 + 2ab + b^2 = c^2 + 2ab,$$

en dit geeft  $a^2 + b^2 = c^2$ , de stelling van Pythagoras voor de rechthoekige driehoek met zijden  $a$ ,  $b$  en  $c$ . Einde bewijs.

Het werken met lengtematen leidde op een natuurlijke manier tot het begrip 'breuk' of 'rationaal getal' wanneer de gemeten lengte niet een geheel veelvoud was van de eenheid van lengte. Bij de klassieke Griekse wiskundigen leidt dit gebruik van getallen tot een fundamentele wiskundige ontdekking, de ontdekking van niet-rationale getallen.

Laat gegeven zijn een standaardvierkant  $ABCD$  met zijden van lengte 1. Volgens de Stelling van Pythagoras is de lengte van de diagonaal  $AC$  dan gelijk aan  $\sqrt{2}$ .



**Stelling 2.1.** *De lengte van de diagonaal in een vierkant is niet een rationaal veelvoud van de lengte van een zijde.*

De stelling betekent dat er niet twee natuurlijke getallen  $n$  en  $m$  zijn zodat

$$m \cdot \text{lengte}(AB) = n \cdot \text{lengte}(AC).$$

Voor de klassieke Griekse wiskundigen was dit een onthutsende ontdekking.

Het bewijs dat de Grieken hiervoor gaven stamt uit de school van de Pythagoreërs en heeft nog niets van zijn charme en elegantie verloren. Hier is het, in een modern jasje natuurlijk:

*Bewijs.* We moeten bewijzen dat  $\sqrt{2}$  niet geschreven kan worden als breuk. Stel dit kan wel, zeg

$$\sqrt{2} = \frac{m}{n}, \tag{1}$$

waarbij  $m$  en  $n$  twee natuurlijke getallen zijn. Als  $m$  en  $n$  beide een veelvoud van een natuurlijk getal  $d > 1$  zijn (een gemeenschappelijke deler  $d > 1$  hebben) dan delen we  $m$  en  $n$  door  $d$  en we mogen daarom dan aannemen dat in de presentatie (1) de getallen  $m$  en  $n$  geen gemeenschappelijke deler hebben anders dan 1. Door kwadrateren krijgen we  $2 = m^2/n^2$ , en door beide kanten met  $n^2$  te vermenigvuldigen wordt dit

$$2n^2 = m^2. \quad (2)$$

Duidelijk is dat de linkerkant even is, dus de rechterkant moet dit ook zijn. Maar als  $m$  oneven is, zeg  $m = 2k + 1$ , dan is ook  $m^2 = 4k^2 + 4k + 1$  ook oneven, dus  $m$  moet wel even zijn, zeg  $m = 2m_1$ . We delen dan beide kanten van de vergelijking (2) door 2 en krijgen

$$n^2 = 2m_1^2 \quad (3)$$

Met eenzelfde argument volgt nu dat  $n$  ook even is. Maar dan zijn zowel  $m$  als  $n$  even, in tegenspraak met onze aanname dat geen natuurlijk getal  $d > 1$  zowel  $m$  als  $n$  deelt. Dus onze aanname dat  $\sqrt{2}$  te schrijven was als breuk is niet houdbaar. Einde bewijs.

Deze ontdekking van de irrationale verhoudingen ('onderling onmeetbare grootheden') wordt toegeschreven aan Hippasos van Metapontos, een lid van de Pythagoreïsche school in de vijfde eeuw voor het begin van onze jaartelling en kwam als een enorme schok voor de school van Pythagoras waar men er van uitging dat alle dingen in (verhoudingen van) natuurlijke getallen uitgedrukt konden worden.

Het ligt voor de hand hierop te variëren. Zo heeft de diagonaal in een kubus met zijden van lengte 1 een lengte  $\sqrt{3}$ . Probeer zelf nu te bewijzen dat  $\sqrt{3}$  geen rationaal getal is. Net zoals bij muziek kunnen we genieten van de scheppingen van anderen, maar we kunnen ook zelf aan de slag en dat geeft vaak minstens zoveel plezier. Er is niet veel meer nodig dan een gezond stel hersens en pen en papier. Een beetje doorzettingsvermogen kan ook geen kwaad.

Van Theodorus van Cyrene stamt het bewijs van de irrationaliteit van

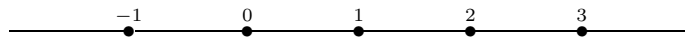
$$\sqrt{3}, \sqrt{5}, \dots, \sqrt{17}.$$

Het bewijs dat algemeen voor een natuurlijk getal  $n$  dat geen kwadraat van een natuurlijk getal is, de kwadraatwortel  $\sqrt{n}$  geen rationaal getal is wordt toegeschreven aan Theaetetus<sup>2</sup> (zie Plato's Dialoog 'Theaetetus') rond 400 voor het begin van onze jaartelling.

Het idee van een onweerlegbaar bewijs komt ook van de Grieken en wordt in de school van Plato een hoeksteen van de wiskunde. Onder een bewijs verstaan we een glasheldere redenering die de waarheid van een bewering (Stelling, Propositie, Lemma,...) afleidt uit aannamen en eerder aanvaarde stellingen.

De natuurlijke getallen passen in het grotere geheel van de gehele getallen. De uitbreiding van  $\mathbb{N}$  tot de verzameling  $\mathbb{Z}$  van de gehele getallen

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\},$$



<sup>2</sup>Theaetetus van Athene, Grieks wiskundige, 417–369, geldt als een groot wiskundige. Aan hem wordt de constructie van het regelmatige achthoekvlak (octaëder) en het regelmatige twintigvlak (icosaëder) toegeschreven.



maar het heeft tot het begin van de 19de eeuw geduurd voor complexe getallen geheel geaccepteerd waren.

Voor ons bestaat de verzameling van de complexe getallen  $\mathbb{C}$  uit de uitdrukkingen  $a + b\sqrt{-1}$ , ofwel

$$\{a + bi : a \in \mathbb{R}, b \in \mathbb{R}\}$$

waarbij we  $i$  voor  $\sqrt{-1}$  schrijven. Door met  $a + bi$  het paar  $(a, b)$  te laten corresponderen kunnen we deze verzameling net zo goed identificeren met de verzameling van paren

$$\mathbb{C} := \{(a, b) : a \in \mathbb{R}, b \in \mathbb{R}\}$$

zodat we geen verwijzing naar een nog niet gedefinieerd element  $i$  nodig hebben. (De notatie  $A := B$  betekent dat  $A$  gedefinieerd wordt gelijk te zijn aan  $B$ .) We kunnen dan de schrijfwijze  $a + bi$  opvatten als een handige notatie voor een paar  $(a, b)$ . We noemen  $a$  het reële deel van  $z = a + bi$  en  $b$  het imaginaire deel. (Notatie:  $\operatorname{Re}(z)$  en  $\operatorname{Im}(z)$ .)

We definiëren nu een optelling op  $\mathbb{C}$  via

$$(a, b) + (c, d) := (a + c, b + d)$$

ofwel in de andere notatie

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

en een vermenigvuldiging via

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc).$$

ofwel in de meer aansprekende notatie

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i.$$

Merk op dat geldt  $(a, 0) + (c, 0) = (a + c, 0)$  en  $(a, 0) \cdot (c, 0) = (ac, 0)$  hetgeen betekent dat, als we de reële getallen zien als complexe getallen  $a + bi$  met  $b = 0$ , de optelling en de vermenigvuldiging niets anders zijn dan de gebruikelijke optelling en vermenigvuldiging op de reële getallen. Verder geldt dat

$$(0, 1) \cdot (0, 1) = (-1, 0),$$

ofwel  $i \cdot i = -1$ . Dus het element  $(0, 1)$  kan nu opgevat worden als een kwadraatwortel uit  $-1$ . We kunnen nu nagaan dat de gebruikelijke rekenregels die we ook gebruiken bij het rekenen met rationale of reële getallen ook gelden voor complexe getallen. Zo kunnen we delen door een complex getal ongelijk aan 0. De nul wordt hier opgevat als  $0 + 0i$ . Er geldt namelijk

$$(a + bi)(a - bi) = a^2 + b^2$$

Dus het complexe getal

$$\frac{a - bi}{a^2 + b^2} \quad \text{met} \quad a^2 + b^2 \neq 0$$

fungeert als de inverse (omgekeerde)  $1/(a + bi)$  van  $a + bi$ . Immers:

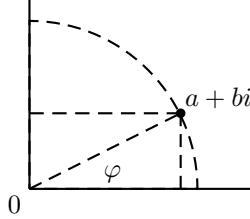
$$(a + bi) \cdot \frac{a - bi}{a^2 + b^2} = \frac{(a + bi)(a - bi)}{a^2 + b^2} = 1.$$

In de praktijk laten we de punt die het product moet aangeven gewoon weg.

Het getal  $\bar{z} = a - bi$  heet de complex geconjugeerde van  $z = a + bi$ .

Met een paar  $(a, b)$  kunnen we een punt in het vlak  $\mathbb{R}^2$  laten corresponderen. Dan heeft het complexe getal  $z = a + bi$  de afstand  $r = \sqrt{a^2 + b^2}$  tot de oorsprong

$(0, 0)$  en het lijnstuk dat  $a + bi$  met  $(0, 0)$  verbindt maakt een (positieve) hoek  $\varphi$  met de  $x$ -as. Hierbij nemen we  $\varphi$  tussen 0 en 360 graden of we drukken de hoek  $\varphi$  uit in de lengte van de cirkelboog tussen  $(r, 0)$  en  $(a, b)$ . Een complex getal  $\neq 0$  wordt dus bepaald door een paar  $(r, \varphi)$  met  $r$  een positief getal en een hoek  $\varphi$  waarbij we deze hoek begrenzen tussen 0 en  $2\pi$ :  $0 \leq \varphi < 2\pi$ . (Deze normalisatie is niet nodig, maar soms wel handig.)



De hoek  $\varphi$  heet het *argument* van  $z$  en  $r$  heet de *absolute waarde* van  $z$ . We schrijven  $|z|$  voor  $r$ . (Voor  $z = 0$  is geen argument gedefinieerd.) We kunnen nu dus schrijven

$$z = r(\cos \varphi + i \sin \varphi).$$

In deze meetkundige interpretatie van complexe getallen  $\mathbb{C}$  wordt vermenigvuldiging met  $z = a + bi$  een  $\mathbb{R}$ -lineaire afbeelding op  $\mathbb{R} \times \mathbb{R}$  gegeven door een matrix

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} r \cos \varphi & -r \sin \varphi \\ r \sin \varphi & r \cos \varphi \end{pmatrix}$$

(Een lineaire afbeelding  $\lambda : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$  is een afbeelding met  $\lambda(az_1 + bz_2) = a\lambda(z_1) + b\lambda(z_2)$  voor alle  $a$  en  $b$  in  $\mathbb{R}$  en alle  $z_1$  en  $z_2$  in  $\mathbb{C}$ . Dan ligt  $\lambda$  volledig vast door  $\lambda(1)$  en  $\lambda(i)$ . Ga na.) Dus de meetkundige interpretatie van vermenigvuldiging met het complexe getal  $z = a + bi$  is een draaiing over een hoek  $\varphi$  gevolgd door een vergroting met een factor  $r$ .

Laat nu twee complexe getallen  $z_1$  en  $z_2$  gegeven zijn:

$$z_1 = r_1(\cos \varphi_1 + i \sin \varphi_1), \quad z_2 = r_2(\cos \varphi_2 + i \sin \varphi_2).$$

Als  $z_1$  en  $z_2$  niet gelijk zijn aan 0 dan volgt uit bovenstaande meetkundige interpretatie dat onder vermenigvuldiging de hoeken van  $z_1$  en  $z_2$  bij elkaar worden opgeteld en dat de absolute waarden met elkaar worden vermenigvuldigd:

$$z_1 \cdot z_2 = r_1 r_2 (\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)). \quad (4)$$

Anderzijds krijgen we uit direct vermenigvuldigen

$$\begin{aligned} z_1 \cdot z_2 &= r_1 r_2 (\cos \varphi_1 + i \sin \varphi_1) \cdot (\cos \varphi_2 + i \sin \varphi_2) \\ &= r_1 r_2 ((\cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2) + i (\cos \varphi_1 \sin \varphi_2 + \sin \varphi_1 \cos \varphi_2)). \end{aligned}$$

Vergelijken van dit laatste met (4) geeft ons de additiefomules voor de sinus en de cosinus:

**Propositie 2.1.** *Voor alle  $\varphi_1, \varphi_2 \in \mathbb{R}$  geldt:*

$$\sin(\varphi_1 + \varphi_2) = \cos \varphi_1 \sin \varphi_2 + \sin \varphi_1 \cos \varphi_2.$$

en

$$\cos(\varphi_1 + \varphi_2) = \cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2.$$

Voor  $\cos \varphi + i \sin \varphi$  wordt wel  $e^{i\varphi}$  geschreven. Dit kan beargumenteerd worden door naar de Taylorontwikkeling van de functies  $\cos \varphi$  en  $\sin \varphi$  te kijken. Dit komt bij Analyse uitgebreid aan de orde. Er geldt dan  $e^{i\pi} = -1$ .

We hebben gezien dat we de reële getallen nodig hebben om zinvol met getallen als  $\sqrt{2}$  te kunnen omgaan. Verder was de uitbreiding van de reële getallen naar de complexe getallen nodig om met getallen als  $\sqrt{-1}$  te kunnen omgaan. Gaat dit zo verder? Met andere woorden hebben we steeds grotere getalsystemen nodig om de wortels van algebraïsche vergelijkingen (zoals  $X^2 = 2$  en  $X^2 + 1 = 0$ ) onder te kunnen brengen? Het verrassende antwoord is nee. Een bekende stelling die we hier niet bewijzen (komt aan de orde bij de Algebra) zegt dat iedere polynoomvergelijking

$$a_0x^n + a_1x^{n-1} + \dots + a_n = 0$$

met  $n \geq 1$  en de  $a_i$  complexe getallen met  $a_0 \neq 0$  een oplossing  $x$  in de complexe getallen heeft. Dit verklaart de bijzondere positie van de complexe getallen.

Maar er bestaan ook geheel andere getalsystemen ('lichamen' in het jargon) en die zullen we later bij de algebra tegenkomen. In tegenstelling tot bijv. de reële getallen of de complexe getallen laten sommige van deze systemen zich heel eenvoudig definiëren. Neem bijvoorbeeld een verzameling  $\mathbb{F}_2$  met twee elementen, die we voor het gemak met  $\bar{0}$  en  $\bar{1}$  aangeven. Dus zeg

$$\mathbb{F}_2 := \{\bar{0}, \bar{1}\}.$$

We definiëren nu een optelling via:

$$\bar{0} + \bar{0} = \bar{0}, \quad \bar{0} + \bar{1} = \bar{1}, \quad \bar{1} + \bar{0} = \bar{1}, \quad \bar{1} + \bar{1} = \bar{0}.$$

Zo ook definiëren we een vermenigvuldiging, hier even genoteerd met  $*$ :

$$\bar{0} * \bar{0} = \bar{0}, \quad \bar{0} * \bar{1} = \bar{0}, \quad \bar{1} * \bar{0} = \bar{0}, \quad \bar{1} * \bar{1} = \bar{1}.$$

We kunnen nu ook delen door  $\bar{1}$  (ga zelf na) en aan alle gebruikelijke rekenregels is voldaan. We zijn het niet gewend, maar het zou wellicht natuurlijker zijn met zulke systemen te beginnen dan met zulke grote en ingewikkelde systemen als  $\mathbb{R}$  en  $\mathbb{C}$ .

De constructie van  $\mathbb{R}$  uitgaande van  $\mathbb{Q}$  (door Dedekind sneden of als limieten van rijtjes rationale getallen) wordt later bij de Analyse gedaan.

### Opgaven

- 1) Bewijs dat  $\sqrt{3}$  niet rationaal is.
- 2) Bewijs dat  $\sqrt[3]{2}$  niet rationaal is.
- 3) Bewijs dat  $\sqrt{2} + \sqrt{3}$  niet rationaal is.
- 4) Laat het reële getal  $r \in \mathbb{R}$  gegeven zijn. Bewijs: voor elke  $\epsilon \in \mathbb{R}_{>0}$  is er een rationaal getal  $q \in \mathbb{Q}$  zodat  $q < r < q + \epsilon$ .
- 5) Laat zien dat voor  $n \in \mathbb{N}$  met  $n \geq 2$  de  $n$  complexe getallen  $\cos(2k\pi/n) + i \sin(2k\pi/n)$  met  $k = 0, \dots, n-1$  de hoekpunten van een regelmatige  $n$ -hoek definiëren.
- 6) Druk  $\cos 3\varphi$  uit als polynoom in  $\cos \varphi$  en  $\sin \varphi$ . Zelfde vraag voor  $\sin 5\varphi$ .
- 7) Laat zien dat

$$\zeta = \frac{\sqrt{5}-1}{4} + \frac{i}{4}\sqrt{10+2\sqrt{5}}$$

een vijfde-machts eenheidswortel is:  $\zeta^5 = 1$ .

8) Laat  $z = a + bi$  en  $w = c + di$  complexe getallen zijn. Laat zien dat  $|zw| = |z||w|$ . Concludeer: het product van twee sommen van twee kwadraten is een som van twee kwadraten.

9) Laat  $\text{Mat}(2, \mathbb{R})$  de verzameling van  $2 \times 2$ -matrices met reële coëfficiënten zijn. Laat  $\mu : \mathbb{C} \rightarrow \text{Mat}(2, \mathbb{R})$  de afbeelding zijn gegeven door

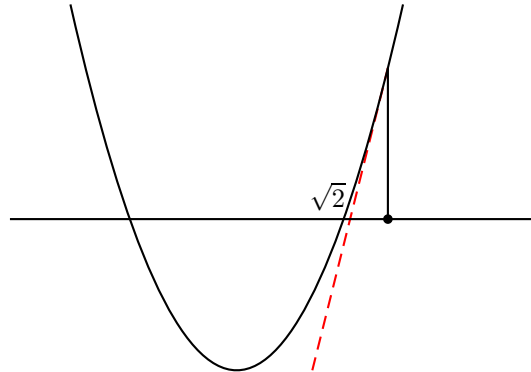
$$a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Ga na dat  $\mu((a + bi)(c + di)) = \mu(a + bi) * \mu(c + di)$ , waarbij  $*$  het matrix-product aangeeft.

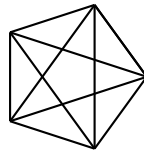
10) Teken de parabool gegeven door  $y = x^2 - 2$ . Bepaal de raaklijn  $L$  aan de parabool in het punt  $(2, 2)$ . Waar snijdt  $L$  de  $x$ -as? Laat zien dat het volgende algoritme een benadering van  $\sqrt{2}$  geeft: laat  $x_0 = 2$  (onze startwaarde). Definiëer voor  $k = 1, 2, \dots$

$$x_k = x_{k-1}/2 + 1/x_{k-1}.$$

Ga na hoe snel dit gaat. Programmeer het op de computer. Geef een benadering van  $\sqrt{3}$ . En een van  $\sqrt[3]{2}$ .



11) Laat  $ABCDE$  een regelmatige vijfhoek zijn. Stel de lengte van een zijde is 1. Bereken de lengte van een diagonaal (bijv.  $AC$ ) en laat zien dat deze lengte niet door een rationaal getal wordt gegeven. (Naar alle waarschijnlijkheid heeft Hippasos van Metapontos zijn vondst van irrationale verhoudingen gedaan bij een regelmatige vijfhoek. De snijpunten van de diagonalen binnen de vijfhoek geven weer een nieuwe vijfhoek, een van de emblemen van de Pythagoreïsche school.)



## 3. VERZAMELINGEN EN AFBEELDINGEN

*Succeeding generations embellish and polish the first  
primitive steps so that future students will come to  
see the work as ‘almost obvious’.*  
Atiyah<sup>6</sup>

## VERZAMELINGEN

De taal van de hedendaagse wiskunde is gebaseerd op de verzamelingenleer. De introductie van deze taal dateert van rond de eeuwwisseling van de 19de naar de 20ste eeuw. Daarvoor werd wiskunde vaak beschreven met vergelijkingen en coördinaten.

Het is niet goed mogelijk van het begrip verzameling een bevredigende definitie te geven, net zoals de maker van het woordenboek ook niet alle woorden kan omschrijven zonder in een cirkelredenering te vervallen. We zullen daarom uitgaan van een intuïtieve bekendheid met het begrip verzameling. Van Georg Cantor<sup>7</sup> stamt de volgende omschrijving: een *verzameling* is het bijeenemen tot één geheel van zekere wel-onderscheiden objecten van ons denken. Die objecten zijn dan de *elementen* van de verzameling. Om aan te geven dat een object  $x$  behoort tot een verzameling  $X$  gebruiken we de notatie

$$x \in X.$$

Als  $x$  geen element is van  $X$  kunnen we dit uitdrukken met de schrijfwijze  $x \notin X$ . Logici bestuderen de verzamelingenleer en hebben axioma's voor de verzamelingenleer aangegeven. Ieder axioma beschrijft een eigenschap van verzamelingen die wiskundigen bij het redeneren algemeen accepteren en tezamen geven ze de regels die we gebruiken bij het hanteren van verzamelingen. Wij zullen een pragmatisch standpunt innemen en uitgaan van een zekere bekendheid hiermee, of deze bekendheid gaandeweg verwerven. Maar een onzorgvuldig gebruik van verzamelingen, in het bijzonder van oneindige verzamelingen, kan gemakkelijk tot tegenspraken leiden.

Als een verzameling  $X$  uit eindig veel elementen  $x_1, \dots, x_n$  bestaat gebruiken we wel de notatie

$$\{x_1, x_2, \dots, x_n\}.$$

Dus  $X = \{x_1, \dots, x_n\}$ . Het aantal elementen van deze eindige verzameling  $X$  wordt wel aangegeven met  $\#X$  of ook wel met  $|X|$ . Een goed voorbeeld is de verzameling van de eerste  $n$  natuurlijke getallen:

$$\{1, 2, 3, \dots, n\}$$

of ons alfabet

$$\{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}.$$

Verzamelingen worden meestal met een hoofdletter aangegeven. We hebben al een aantal van de belangrijkste verzamelingen in de wiskunde ontmoet; bijvoorbeeld de

---

<sup>6</sup>Sir Michael Atiyah, 1929-, Brits wiskundige. Speelde een belangrijke rol in de wiskunde van de tweede helft van de 20ste eeuw.

<sup>7</sup>Georg Cantor, Duits wiskundige, 1845-1918, grondlegger van de axiomatische verzamelingenleer.

verzameling  $\mathbb{N}$  van de natuurlijke getallen

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

Dit is niet een eindige verzameling. Ook de verzamelingen  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  en  $\mathbb{C}$  zijn oneindige verzamelingen. Een ander voorbeeld van een eindige verzameling is de *lege verzameling*. Deze verzameling bevat geen elementen en wordt genoteerd met  $\emptyset$ :

$$\emptyset := \{ \}.$$

Als  $x$  en  $y$  twee elementen uit een verzameling  $X$  zijn dan betekent  $x = y$  dat  $x$  en  $y$  hetzelfde object uit  $X$  voorstellen. Als  $x$  en  $y$  verschillende objecten van  $X$  zijn dan kunnen we dit aangeven met  $x \neq y$ .

Als  $X$  en  $Y$  twee verzamelingen zijn dan schrijven we  $X \subset Y$  (of ook  $X \subseteq Y$ ) als ieder element van  $X$  ook een element van  $Y$  is. Zo geldt bijvoorbeeld

$$\mathbb{N} \subset \mathbb{Z}.$$

We zeggen dat  $X$  een *deelverzameling* van  $Y$  is. We zeggen ook wel dat  $Y$  de verzameling  $X$  omvat. Voor iedere verzameling  $X$  geldt dus  $X \subseteq X$ . Gelijkheid van twee verzamelingen  $X$  en  $Y$  betekent precies dat  $X \subset Y$  en  $Y \subset X$ . Als  $X$  een deelverzameling van  $Y$  is, maar  $X$  en  $Y$  zijn verschillend dan schrijven we

$$X \subsetneq Y \quad \text{of} \quad X \subsetneq Y.$$

Dit betekent dus dat  $Y$  een element  $y$  bezit dat niet een element van  $X$  is. De relatie  $\subset$  wordt wel inclusie en  $\subsetneq$  wordt wel echte inclusie genoemd. Als  $X \subsetneq Y$  dan zeggen we dat  $X$  een echte deelverzameling van  $Y$  is (of echt bevat is in  $Y$ ).

Eindige verzamelingen kunnen we omschrijven door een lijst van alle elementen te geven, alhoewel dit voor grote verzamelingen niet echt doenlijk is. De gebruikelijke manier om een verzameling te geven is als deelverzameling van een al bekende verzameling. Dit wordt gedaan door aan te geven dat onze verzameling bestaat uit alle elementen van die bekende verzameling die een bepaalde eigenschap bezitten; zo kunnen we bijvoorbeeld de verzamelingen

$$E := \{n \in \mathbb{Z} : n \text{ is even}\}$$

en

$$P := \{n \in \mathbb{N} : n \text{ is een priemgetal}\}$$

omschrijven. De haakjes in de notatie zijn een afkorting voor ‘de verzameling van alle elementen’ en de dubbele punt (of ook wel het teken  $|$ , dus  $E := \{n \in \mathbb{Z} \mid n \text{ is even}\}$ ) betekent ‘met de eigenschap dat’.

Uit verzamelingen kunnen we op verschillende manieren nieuwe verzamelingen maken. Als  $X$  en  $Y$  twee verzamelingen zijn dan is de *vereniging* van  $X$  en  $Y$  de verzameling van alle elementen van  $X$  en alle elementen van  $Y$ . We schrijven dit als

$$X \cup Y = \{x : x \in X \text{ of } x \in Y\}.$$

Hierbij is enige voorzichtigheid op zijn plaats. Het woordje ‘of’ hier sluit niet uit dat  $x$  zowel element is van  $X$  als van  $Y$ . Ons gebruik van het woord ‘of’ is dus dat van ‘of’ in de ruime zin des woords. Dus niet het zgn. exclusieve *òf ...òf*. Dus

$$\{1, 2, 3, 4, 5, 6\} \cup \{2, 4, 6, 8, 10\} = \{1, 2, 3, 4, 5, 6, 8, 10\}.$$

Er geldt voor elke verzameling  $X$  dat

$$X \cup \emptyset = X.$$

Ook geldt  $X \cup Y = Y \cup X$ .

Een tweede manier om een nieuwe verzameling uit gegeven verzamelingen te maken is de *doorsnede*. De doorsnede van  $X$  en  $Y$  is de verzameling die bestaat uit alle elementen  $x$  die zowel element zijn van  $X$  als van  $Y$ . In notatie:

$$X \cap Y := \{x : x \in X \text{ en } x \in Y\}.$$

Dit is symmetrisch in  $X$  en  $Y$ :  $X \cap Y = Y \cap X$ . Natuurlijk kan het gebeuren dat deze doorsnede leeg is: de verzamelingen

$$\mathbb{R}_+ := \{x \in \mathbb{R} : x > 0\} \quad \text{en} \quad \mathbb{R}_- := \{x \in \mathbb{R} : x < 0\}$$

hebben een lege doorsnede:  $\mathbb{R}_+ \cap \mathbb{R}_- = \emptyset$ . Als  $X \cap Y = \emptyset$  zeggen we dat  $X$  en  $Y$  *disjunct* zijn. Voor elke verzameling  $X$  geldt

$$X \cap \emptyset = \emptyset.$$

Een gevolg hiervan is dat voor elke verzameling  $X$  de inclusie  $\emptyset \subset X$  geldt.

Gegeven twee verzamelingen  $X$  en  $Y$  met  $Y \subset X$  kunnen we het *complement* van  $Y$  in  $X$  nemen:

$$X - Y := \{x : x \in X, x \notin Y\}.$$

Dit is een deelverzameling van  $X$ . (Ook de notatie  $X \setminus Y$  wordt wel gebruikt.) Ga zelf na dat als  $Y$  en  $Z$  deelverzamelingen van  $X$  zijn geldt

$$X - (Y \cup Z) = (X - Y) \cap (X - Z).$$

Een andere belangrijke manier om bij twee gegeven verzamelingen  $X$  en  $Y$  een nieuwe verzameling te maken is het *Cartesisch product*, genoemd naar Descartes<sup>8</sup>. Het Cartesisch product  $X \times Y$  wordt gedefinieerd als de verzameling van geordende paren  $(x, y)$  met  $x \in X$  en  $y \in Y$ :

$$X \times Y := \{(x, y) : x \in X, y \in Y\}.$$

Zo is het Cartesisch product  $\mathbb{R} \times \mathbb{R}$  niets anders dan het platte vlak.

[Voor diegenen die een definitie van een geordend paar in verzamelingtheoretische termen willen, geven we die hier: een geordend paar  $(x, y)$  is een verzameling  $\{\{x\}, \{x, y\}\}$  bestaande uit twee verzamelingen. We garanderen niet dat dit veel verheldert.]

We kunnen deze constructie ook voor eindig veel verzamelingen doen: als verzamelingen  $X_1, \dots, X_n$  gegeven zijn, dan is het Cartesisch product  $X_1 \times \dots \times X_n$  de verzameling van geordende  $n$ -tallen:

$$X_1 \times \dots \times X_n := \{(x_1, \dots, x_n) : x_1 \in X_1, \dots, x_n \in X_n\}.$$

Merk op dat we hier spreken van *geordende* twee- of meertallen; zo is in  $X \times X$  het element  $(x, y)$  verschillend van  $(y, x)$  als  $x \neq y$ .

Als  $X$  een verzameling is dan krijgen we ook een nieuwe verzameling door alle deelverzamelingen van  $X$  te bekijken. De *machtsverzameling* van  $X$  is de verzameling

$$\mathcal{P}(X) := \{Y : Y \subset X\}.$$

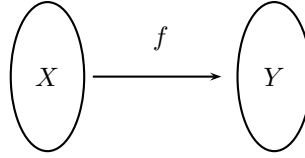
#### AFBEELDINGEN

Minstens zo belangrijk als verzamelingen zelf zijn relaties tussen verzamelingen. Cruciaal hierbij is het begrip *afbeelding*.

<sup>8</sup>R n  Descartes, 1596-1650, Frans wiskundige en filosoof, die meer dan twintig jaar in Amsterdam heeft gewoond.

**Definitie 3.1.** Laat  $X$  en  $Y$  verzamelingen zijn. Een afbeelding is een voorschrift  $f$  dat aan ieder element  $x \in X$  een element  $f(x)$  van  $Y$  toevoegt.

Notatie:  $f : X \rightarrow Y$ ,  $x \mapsto f(x)$ . Schematisch ziet dat er zo uit:



Vaak wordt ook de term ‘functie’ gebruikt, in het bijzonder als  $X$  de verzameling van de reële getallen of een deel daarvan is.

*Voorbeeld 3.2.* Laat  $X = Y = \mathbb{N}$  en  $f$  het voorschrift dat aan  $n \in \mathbb{N}$  zijn kwadraat  $n^2$  toevoegt:  $f : \mathbb{N} \rightarrow \mathbb{N}$ ,  $n \mapsto f(n) = n^2$ . Of neem de reële functie sinus:  $\mathbb{R} \rightarrow \mathbb{R}$ ,  $x \mapsto \sin x$ .

Een flauw maar vaak gebruikt voorbeeld is de identieke afbeelding. Als  $X$  een willekeurige verzameling is definiëren we de afbeelding  $\text{id}_X$ , soms ook wel  $1_X$  geschreven, door

$$\text{id}_X : X \rightarrow X, \quad x \mapsto x.$$

Voor een afbeelding  $f : X \rightarrow Y$  noemen we  $X$  de definitieverzameling of het *domein* van  $f$ . Verder noemen we  $f(x)$  het beeld van  $x$  onder  $f$ . Merk op dat

$$f(X) := \{f(x) : x \in X\}$$

een deelverzameling is van  $Y$ . Deze deelverzameling heet het *beeld* van  $f$ . Dus in ons voorbeeld is  $f(\mathbb{N})$  de verzameling van de kwadraten in  $\mathbb{N}$ .

Als  $f : X \rightarrow Y$  een afbeelding is en  $y \in Y$  is een element van  $X$  dan is

$$\{x : x \in X, f(x) = y\}$$

een deelverzameling van  $X$ . Deze deelverzameling heet het (*volledig*) *origineel* van  $y$ . Notatie:  $f^{-1}(y)$ . Voor een deelverzameling  $Z$  van  $Y$  definiëren we analoog

$$f^{-1}(Z) := \{x \in X : f(x) \in Z\}.$$

[ Om consistent te zijn zouden we eigenlijk  $f^{-1}(\{y\})$  moeten schrijven voor het origineel van een element  $y \in Y$ .]

[In plaats van te spreken van een ‘voorschrift’ kunnen we een afbeelding ook geheel in verzamelingstheoretische termen definiëren. Namelijk een voorschrift  $f$  bepaalt een deelverzameling

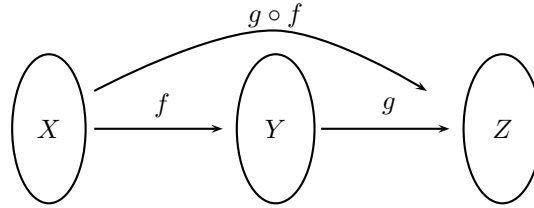
$$\Gamma(f) := \{(x, y) \in X \times Y : y = f(x)\},$$

de graaf of grafiek van  $f$ . (Vgl. de grafiek van een functie.) Iedere deelverzameling  $Z \subset X \times Y$  met de eigenschap dat voor elke  $x \in X$  de doorsnede  $Z \cap \{x\} \times Y$  uit precies één element bestaat definieert een  $f$  door aan  $x$  het element  $Z \cap \{x\} \times Y$  toe te voegen.]

Als gegeven zijn een afbeelding  $f : X \rightarrow Y$  en een afbeelding  $g : Y \rightarrow Z$  dan kunnen we de *samenstelling* van  $f$  en  $g$  definiëren:

$$g \circ f : X \rightarrow Z, \quad x \mapsto g(f(x)).$$

Merk op dat dit een welgedefinieerde afbeelding is:  $f(x)$  is een element van  $Y$  en daar kunnen we  $g$  op toepassen. De samenstelling  $g \circ f$  is dus niets anders dan ‘eerst  $f$  uitvoeren en daarna  $g$  uitvoeren’



Als we nu drie afbeeldingen hebben

$$f : X \rightarrow Y, \quad g : Y \rightarrow Z, \quad \text{en} \quad h : Z \rightarrow W,$$

dan hebben we a priori twee samenstellingen:

$$h \circ (g \circ f) : X \xrightarrow{g \circ f} Z \xrightarrow{h} W$$

en

$$(h \circ g) \circ f : X \xrightarrow{f} Y \xrightarrow{h \circ g} W$$

Maar als we naar de definitie kijken zien we dat dit hetzelfde levert:  $x \mapsto h(g(f(x)))$ . We mogen de haakjes dus gerust weglaten.

Ga zelf na dat voor een afbeelding  $f : X \rightarrow Y$  geldt  $\text{id}_Y \circ f = f$  en  $f \circ \text{id}_X = f$ .

**Definitie 3.3.** Een afbeelding  $f : X \rightarrow Y$  heet *injectief* als verschillende elementen van  $X$  ook verschillende beelden in  $Y$  hebben. Meer formeel: als  $x_1, x_2 \in X$  en  $x_1 \neq x_2$  dan volgt  $f(x_1) \neq f(x_2)$ .

Een andere manier om de conditie uit te drukken is: als  $f(x_1) = f(x_2)$  dan volgt  $x_1 = x_2$ .

*Voorbeeld 3.4.* De afbeelding  $f : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $x \mapsto -x$  is injectief. De afbeelding  $f : \mathbb{N} \rightarrow \mathbb{N}$ ,  $x \mapsto x^2$  is injectief. De afbeelding  $f : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $x \mapsto x^2$  is niet injectief, want bijv. 2 en  $-2$  hebben hetzelfde beeld 4.

Ga zelf na dat als  $X$  een eindige verzameling is en  $f : X \rightarrow Y$  een injectieve afbeelding, dan geldt  $\#f(X) = \#X$ .

Voor een injectieve afbeelding geldt

$$f^{-1}(y) \text{ bestaat uit één of nul punten.}$$

Soms wordt wel de notatie  $f : X \hookrightarrow Y$  gebruikt voor een injectieve afbeelding.

**Definitie 3.5.** Een afbeelding  $f : X \rightarrow Y$  heet *surjectief* als ieder element van  $Y$  optreedt als beeld, m.a.w.,  $f(X) = Y$ .

*Voorbeeld 3.6.* De afbeelding  $f : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $x \mapsto -x$  is surjectief. De afbeelding  $f : \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}$ ,  $x \mapsto x^2$  is surjectief. De inclusieafbeelding  $\mathbb{Q} \rightarrow \mathbb{R}$ ,  $x \mapsto x$  is niet surjectief.

Soms wordt wel de notatie  $f : X \twoheadrightarrow Y$  gebruikt om aan te geven dat een afbeelding surjectief is.

**Definitie 3.7.** Een afbeelding  $f : X \rightarrow Y$  heet *bijjectief* als  $f$  zowel injectief als surjectief is.

Soms, maar niet zo vaak, wordt wel de notatie  $f : X \longleftrightarrow Y$  of ook wel  $f : X \xrightarrow{1-1} Y$  gebruikt om aan te geven dat een afbeelding bijectief is.

Een bijectieve afbeelding geeft een één-één correspondentie tussen de punten van  $X$  en de punten van  $Y$ . Als  $f : X \rightarrow Y$  een bijectie is tussen eindige verzamelingen  $X$  en  $Y$  dan hebben  $X$  en  $Y$  evenveel elementen.

Als  $f : X \rightarrow Y$  een bijectie is kunnen we ook een afbeelding ‘terug’ definiëren door te stellen

$$f^{-1} : Y \rightarrow X, \quad y \mapsto f^{-1}(y).$$

Merk op dat  $f^{-1}$  een wel-gedefinieerde afbeelding is. Immers, voor elke  $y \in Y$  is er een  $x \in X$  die onder  $f$  op  $y$  wordt afgebeeld, dus  $f^{-1}(y)$  is niet leeg; omdat  $f$  injectief is bestaat het inverse beeld  $f^{-1}(y)$  uit niet meer dan één punt en dus is  $f^{-1}(y)$  een welgedefinieerd element van  $X$ .

Deze afbeelding  $f^{-1}$  heet de inverse afbeelding. Als  $f$  bijectief is dan zal er geen verwarring zijn met het al eerder gedefinieerde inverse beeld  $f^{-1}(y)$ . Voor een bijectieve afbeelding  $f : X \rightarrow Y$  geldt

$$f \circ f^{-1} = \text{id}_Y \quad f^{-1} \circ f = \text{id}_X.$$

We geven nu een criterium om te testen of een afbeelding bijectief is.

**Propositie 3.8.** *Als  $f : X \rightarrow Y$  en  $g : Y \rightarrow X$  afbeeldingen zijn zodat de samenstelling  $f \circ g : Y \rightarrow Y$  gelijk is aan  $\text{id}_Y$  en de samenstelling  $g \circ f : X \rightarrow X$  gelijk is aan  $\text{id}_X$  dan is zowel  $f$  als  $g$  een bijectie.*

*Bewijs.* We moeten bewijzen dat  $f$  zowel injectief als surjectief is, en idem dito voor  $g$ . We beginnen met  $f$ . Stel  $f$  is niet injectief. Dan zijn er twee elementen  $x_1 \neq x_2$  in  $X$  met  $f(x_1) = f(x_2)$ . Toepassen van  $g$  levert  $g(f(x_1)) = g(f(x_2))$ , dus  $x_1 = x_2$ , een tegenspraak. Dus  $f$  is injectief. Verder is het beeld  $f(g(Y))$  gelijk aan het beeld van  $\text{id}_Y$ , dat is,  $Y$ . Maar het beeld  $f(g(Y))$  is bevat in  $f(X)$  want  $g(Y) \subset X$ , dus  $Y \subset f(X)$ , en omdat  $f(X) \subset Y$  volgt  $Y = f(X)$ .

Het bewijs van de injectiviteit en de surjectiviteit van  $g$  gaat net zo (gebruik de symmetrie van de propositie). Einde bewijs.

Nu we het begrip afbeelding tot onze beschikking hebben kunnen we bij twee verzamelingen  $X$  en  $Y$  nog een nieuwe verzameling maken:

$$Y^X := \{f : f \text{ is een afbeelding van } X \text{ naar } Y\}.$$

De notatie mag op het eerste gezicht wat vreemd lijken. Maar als  $X$  en  $Y$  eindige verzamelingen zijn geldt

$$\#(Y^X) = (\#Y)^{\#X}.$$

Immers, een afbeelding  $f : X \rightarrow Y$  wordt bepaald door voor iedere  $x \in X$  te zeggen wat het beeld is. Voor een gegeven  $x \in X$  hebben we  $\#Y$  mogelijkheden voor het beeld  $f(x)$ , en dat geeft in totaal

$$(\#Y)^{\#X}$$

mogelijkheden.

**Lemma 3.9.** *Er is een bijectie  $\mathcal{P}(X) \longleftrightarrow \{0, 1\}^X$  van de machtsverzameling van  $X$  naar de verzameling van afbeeldingen van  $X$  naar  $\{0, 1\}$ .*

*Bewijs.* Een deelverzameling  $Y \subset X$  is volledig bepaald door voor ieder element  $x$  van  $X$  te zeggen of het element van  $Y$  is of niet. Definieer daarom voor  $Y \subset X$  een afbeelding  $f_Y : X \rightarrow \{0, 1\}$  door  $f_Y(x) = 0$  als  $x \in Y$  en  $f_Y(x) = 1$  als  $x \notin Y$ . Dit geeft een afbeelding  $\phi : \mathcal{P}(X) \rightarrow \{0, 1\}^X$  met  $\phi(Y) = f_Y$ .

Omgekeerd, bij gegeven afbeelding  $f : X \rightarrow \{0, 1\}$  definiëren we een deelverzameling  $Y_f$  via

$$Y_f := f^{-1}(0).$$

Dit geeft een afbeelding  $\psi : \{0, 1\}^X \rightarrow \mathcal{P}(X)$  met  $\psi(f) = Y_f$ . Er geldt nu

$$\phi \circ \psi = \text{id}_{\{0,1\}^X},$$

en

$$\psi \circ \phi = \text{id}_{\mathcal{P}(X)}.$$

Dit bewijst dat  $\phi$  en  $\psi$  bijecties zijn.

**Definitie 3.10.** Twee verzamelingen  $X$  en  $Y$  heten *gelijkmachtig* als er een bijectie  $f : X \rightarrow Y$  bestaat. We zeggen ook wel:  $X$  en  $Y$  hebben dezelfde cardinaliteit.

Verzamelingen  $X$  die gelijkmachtig zijn met  $\{1, 2, \dots, n\}$  voor een  $n \in \mathbb{N}$  heten *eindig*. Verzamelingen die niet eindig zijn heten *oneindig*.

Als  $A$  de indexverzameling van een niet-lege collectie van verzamelingen  $X_\alpha$  is ( $A$  hoeft hierbij niet eindig te zijn) kunnen we de vereniging definiëren als

$$\cup_{\alpha \in A} X_\alpha := \{x : x \in X_\alpha \text{ voor tenminste één } \alpha \in A\}$$

en de doorsnede als

$$\cap_{\alpha \in A} X_\alpha := \{x : x \in X_\alpha \text{ voor elke } \alpha \in A\}.$$

De volgende generalisatie van het Cartesisch product wordt ook regelmatig gebruikt. Met een *oneindige rij* elementen uit een gegeven verzameling  $X$  bedoelen we een afbeelding

$$f : \mathbb{N} \rightarrow X.$$

Dus voor ieder natuurlijk getal  $n$  is een element  $x_n \in X$  gedefinieerd. We schrijven dit vaak als

$$(x_1, x_2, x_3, \dots) \quad \text{of als} \quad (x_n)_{n=1}^\infty.$$

Onder het Cartesisch product

$$\prod_{i=1}^\infty X$$

verstaan we de verzameling oneindige rijen van elementen uit  $X$ , dus  $X^\mathbb{N}$ . Meer algemeen voor een collectie  $A$  van verzamelingen  $X_\alpha$  is het Cartesisch product gedefinieerd als

$$\prod_{\alpha \in A} X_\alpha := \{f : A \rightarrow \cup_{\alpha \in A} X_\alpha : f(\alpha) \in X_\alpha\}.$$

## POLYNOMEN

Polynomen of veeltermen spelen een belangrijke rol in de wiskunde. We bekijken eerst polynomen met reële coëfficiënten. De verzameling van polynomen in  $X$  met reële coëfficiënten  $\mathbb{R}[X]$  bestaat per definitie uit de uitdrukkingen

$$a_0 + a_1X + a_2X^2 + \dots + a_nX^n \tag{1}$$

waarbij  $n \in \mathbb{Z}_{\geq 0}$  en  $a_0, a_1, \dots, a_n \in \mathbb{R}$ . We schrijven ook wel

$$\sum_{i=0}^n a_i X^i$$

of ook wel

$$\sum_{i=0}^{\infty} a_i X^i,$$

waarbij alle  $a_i \in \mathbb{R}$  en slechts eindig veel  $a_i$  ongelijk 0 zijn. Zulke uitdrukkingen heten veeltermen of polynomen. Het teken  $\sum$  is het sommatieteken, ‘neem de som over ...’. We definiëren nu een optelling  $+$  via

$$\sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i = \sum_{i=0}^{\infty} (a_i + b_i) X^i$$

en een vermenigvuldiging  $\cdot$  via

$$\left( \sum_{i=0}^{\infty} a_i X^i \right) \cdot \left( \sum_{i=0}^{\infty} b_i X^i \right) = \sum_{i=0}^{\infty} c_i X^i$$

met  $c_i$  bepaald door

$$c_i = \sum_{j,k:j+k=i} a_j b_k \quad (2)$$

Hierbij worden de optelling en vermenigvuldiging in  $\mathbb{R}$  gebruikt. Het nulpolynoom is de veelterm  $0 = \sum_{i=0}^{\infty} 0 X^i$ . Deze bewerkingen voldoende aan de gebruikelijke regels voor optellen en vermenigvuldigen. Dit komt later bij de algebra uitgebreid aan de orde. De regel voor de vermenigvuldiging volgt uit de distributiviteit  $f \cdot (g + h) = f \cdot g + f \cdot h$  en  $(f + g) \cdot h = f \cdot h + g \cdot h$  en de regel

$$(a_i X^i) \cdot (b_j X^j) = a_i \cdot b_j X^{i+j}.$$

Als voorbeeld geldt de identiteit

$$X^n - 1 = (-1 + X)(1 + X + X^2 + \dots + X^{n-1}).$$

Wellicht is de definitie van polynoom niet geheel bevredigend omdat we niet zeggen wat  $X$  is. Daarom geven we hier een definitie in verzamelingstheoretische termen. Een polynoom van graad  $\leq n$  met reële coëfficiënten  $f$  is een geordend rijtje

$$(a_0, a_1, a_2, \dots, a_n) \quad \text{met } a_i \in \mathbb{R}.$$

Kortom, de verzameling van polynomen van graad  $\leq n$  met reële coëfficiënten is niets anders dan de verzameling  $\mathbb{R}^{n+1}$ . We kunnen dan (1) opvatten als een handige schrijfwijze van zulke rijtjes. Als we de graad niet specificeren dan moeten we oneindige rijtjes

$$(a_0, a_1, a_2, \dots)$$

van reële getallen bekijken met de eigenschap dat slechts eindig veel  $a_i$  ongelijk nul zijn. Dus de verzameling van polynomen met reële coëfficiënten is de verzameling

$$\{(a_0, a_1, a_2, \dots) : \text{slechts eindig veel } a_i \text{ ongelijk } 0\} \subset \mathbb{R}^{\mathbb{Z}_{\geq 0}}.$$

De optelling en vermenigvuldiging kunnen dan voor deze rijtjes gegeven worden

$$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$$

en

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots)$$

waarbij

$$c_k = \sum_{i=0}^k a_i b_{k-i}.$$

De graad van een polynoom  $(a_0, a_1, a_2, \dots)$  dat niet het nulpolynoom is, is de grootste  $n$  met  $a_n \neq 0$ . (De graad van het nulpolynoom is 0.) Een reëel polynoom  $f \in \mathbb{R}[X]$  definieert een afbeelding:  $\mathbb{R} \rightarrow \mathbb{R}$  via  $x \mapsto f(x)$ , waarbij we  $x$  in het polynoom invullen. We zeggen dan dat  $x$  een *nulpunt* is van  $f$  als  $f(x) = 0$ .

We kunnen dit ook doen voor andere getsystemen zoals  $\mathbb{Z}$ ,  $\mathbb{Q}$  en  $\mathbb{C}$ . De bijbehorende verzamelingen van polynomen worden gedefiniëerd als  $\mathbb{Z}[X]$ ,  $\mathbb{Q}[X]$  en  $\mathbb{C}[X]$ . Zo geldt in  $\mathbb{C}[X]$  de identiteit  $1 + X^2 = -(i + X)(i - X)$ . Verder kunnen we ook polynomen in meer variabelen bekijken. Bijv. elementen van  $\mathbb{R}[X, Y]$ . We vatten die hier op als polynomen in  $Y$  met coëfficiënten uit  $\mathbb{R}[X]$ . Bij de Algebra komt dit later uitgebreid aan de orde.

### Opgaven

1) Laat  $X, Y$  en  $Z$  verzamelingen zijn. Bewijs de distributieve wetten:

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$

en

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

2) Bewijs de volgende regels voor het complement

$$X - (Y \cup Z) = (X - Y) \cap (X - Z)$$

en

$$X - (Y \cap Z) = (X - Y) \cup (X - Z).$$

3) Ga na of algemeen de volgende uitspraken voor verzamelingen  $X, Y, Z$  en  $W$  gelden:

- i)  $X \subset Y, Z \subset W \implies X \times Z \subset Y \times W$ .
- ii)  $X \times Z \subset Y \times W \implies X \subset Y$  en  $Z \subset W$ .
- iii)  $(X \times Y) - (Z \times W) = (X - Z) \times (Y - W)$ .

4) Laat  $X, Y$  en  $Z$  deelverzamelingen van een eindige verzameling  $U$  zijn. Ga na dat geldt

$$\#(X \cup Y \cup Z) = \#X + \#Y + \#Z - \#(X \cap Y) - \#(X \cap Z) - \#(Y \cap Z) + \#(X \cap Y \cap Z).$$

Dit is een manifestatie van het zgn. inclusie-exclusie principe.

5) Laat  $f : \mathbb{R} \rightarrow \mathbb{R}$  de afbeelding zijn gegeven door  $x \mapsto x^3 + 2x$ . Bewijs dat  $f$  surjectief is. Is  $f$  ook injectief?

6) Als  $f : X \rightarrow Y$  een afbeelding is dan gelden de inclusies:

$$A \subset f^{-1}(f(A)) \quad \text{voor alle } A \subset X$$

en

$$f(f^{-1}(B)) \supset B \quad \text{voor alle } B \subset f(X).$$

Bewijs dit.

7) Laat  $f : \mathbb{R} \rightarrow \mathbb{R}$  de afbeelding (of functie) zijn gegeven door  $x \mapsto f(x) = 2x^2 + 3$ . Bepaal  $f(\mathbb{R})$ ,  $f^{-1}(\mathbb{R})$ ,  $f^{-1}(f(\mathbb{R}))$  en ook  $f(f^{-1}(\mathbb{R}))$ .

8) Laat  $f : \mathbb{R} \rightarrow \mathbb{R}$  gegeven zijn door  $f(x) = 3x^2 + 5$  en  $g : \mathbb{R} \rightarrow \mathbb{R}$  door  $g(x) = 7x^2 + 1$ . Bereken de samenstelling  $g \circ f$ .

9) Laat  $f : X \rightarrow Y$  en  $g : Y \rightarrow Z$  afbeeldingen zijn. Laat zien dat voor een deelverzameling  $W \subset Z$  geldt

$$(g \circ f)^{-1}(W) = f^{-1}(g^{-1}(W)).$$

10) Laat  $f : X \rightarrow Y$  en  $g : Y \rightarrow Z$  afbeeldingen zijn. Laat zien dat  $g \circ f$  injectief is als  $f$  en  $g$  dat zijn. Als  $g \circ f$  injectief is zijn  $g$  en  $f$  dan injectief? (Bewijs of geef een tegenvoorbeeld.) Als  $g \circ f$  surjectief is zijn  $g$  en  $f$  dan surjectief?

11) Laat  $X$  een eindige verzameling zijn en  $f : X \rightarrow X$  een afbeelding. Bewijs:  $f$  is surjectief dan en slechts dan als  $f$  injectief is.

12) Laat  $X$  een eindige verzameling zijn met  $n$  elementen. Bereken het aantal elementen van de machtsverzameling  $\mathcal{P}(X)$ .

## 4. GEHELE GETALLEN EN PRIEMGETALLEN

*Die ganzen Zahlen hat der liebe Gott gemacht,  
alles andere ist Menschenwerk.*

L. Kronecker<sup>9</sup>

## GEHELE GETALLEN

De *natuurlijke getallen*  $1, 2, 3, \dots$  zijn wellicht de meest fundamentele wiskundige objecten. Zoals we al zagen, noteren de verzameling van de natuurlijke getallen met  $\mathbb{N}$ . Dus

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

De natuurlijke getallen vormen een verzameling waarin een element  $1 \in \mathbb{N}$  aangegeven is en die een afbeelding  $S : \mathbb{N} \rightarrow \mathbb{N}$  (opvolgerfunctie) bezit met de volgende eigenschappen:

- i)  $S$  is injectief;
- ii)  $1 \notin S(\mathbb{N})$ ;
- iii) Als een deelverzameling  $M \subseteq \mathbb{N}$  het element 1 bevat en voldoet aan  $S(M) \subseteq M$  dan  $M = \mathbb{N}$ .

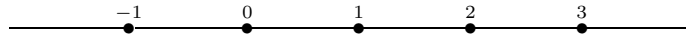
Deze drie axioma's corresponderen met ons welbekende eigenschappen van tellen: ieder natuurlijk getal heeft een opvolger ( $S(1) = 2$ ,  $S(2) = 3, \dots$ ). Het eerste axioma zegt ons dat we daarbij een gegeven natuurlijk getal niet meer dan een keer tegenkomen. Het derde is equivalent met twee andere 'principes', het welorderingsprincipe en het principe van volledige inductie, dat we in dit hoofdstuk al gebruiken, maar in het volgende hoofdstuk meer uitgebreid behandelen. Het eerste, dat we vaak zullen hanteren, luidt (voor  $\mathbb{N} \cup \{0\}$ ) als volgt.

**Principe 4.1.** *Iedere niet-lege verzameling van niet-negatieve gehele getallen bevat een kleinste element.*

Zie het volgende hoofdstuk voor een afleiding van dit principe uit iii).

De uitbreiding van  $\mathbb{N}$  tot de verzameling  $\mathbb{Z}$  van de gehele getallen

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\},$$



die men krijgt door 0 en de negatieve getallen toe te voegen, mag voor ons heel vanzelfsprekend zijn, maar dateert ook pas van later zoals we al zagen. Dit illustreert de 'psychologische' hordes die in de wiskunde genomen moeten worden, maar die achteraf nauwelijks meer een probleem lijken te zijn. De gehele getallen spelen een fundamentele rol in de gehele wiskunde, en dus ook in de algebra. In dit hoofdstuk bespreken we een paar fundamentele eigenschappen van gehele getallen, in het bijzonder deelbaarheid.

Eerst leiden we nu de mogelijkheid van 'deling met rest' af.

**Stelling 4.1.** (Deling met Rest.) *Laat  $a$  en  $b$  gehele getallen zijn met  $b > 0$ . Dan bestaan er twee eenduidig bepaalde gehele getallen  $q$  en  $r$  zodat*

$$a = qb + r \quad \text{met} \quad 0 \leq r < b.$$

---

<sup>9</sup>L. Kronecker, Duits wiskundige, 1823–1891, speelde een rol van betekenis in de getaltheorie.

*Bewijs.* Het idee van het bewijs is simpel: trek  $b$  net zolang van  $a$  af totdat er een rest over is die kleiner is dan  $b$ . Meer precies gaat dat zo. Beschouw de verzameling

$$V = \{\dots, a - 2b, a - b, a, a + b, a + 2b, \dots\} = \{a - xb : x \in \mathbb{Z}\}.$$

Deze verzameling bevat niet-negatieve elementen: bijv. als  $a \geq 0$  nemen we  $x = 0$  en  $x = a$  als  $a < 0$ . Volgens bovenstaand principe is er dan een kleinste niet-negatief getal, zeg  $r = a - qb$ , in  $V \cap \{0, 1, 2, \dots\}$  voor zekere  $q$ . Dan kunnen we schrijven

$$a = qb + r \quad \text{met} \quad r \geq 0.$$

Wanneer  $r \geq b$ , dan is  $r - b$  weer een element van  $V \cap \{0, 1, 2, \dots\}$ , want  $r - b \geq 0$  en  $r - b = a - (q + 1)b$ . Wegens  $r - b < r$  weerspreekt dit de minimaliteit van  $r$ . Dus concluderen we  $0 \leq r < b$ .

Nu we een  $q$  en een  $r$  met de gevraagde eigenschappen gevonden hebben moeten we nog laten zien dat  $q$  en  $r$  eenduidig bepaald zijn. Als  $q', r'$  een ander paar is, dan geldt

$$a = qb + r,$$

$$a = q'b + r'$$

met  $0 \leq r, r' < b$ . Stel nu dat  $q \neq q'$ . Na eventueel verwisselen van  $q$  en  $q'$  mogen we veronderstellen dat  $q > q'$ . Aftrekken van bovenstaande vergelijkingen en gebruikmaken van  $q - q' \geq 1$ , dus  $(q - q')b \geq b$ , levert

$$b \leq (q - q')b = r' - r \leq r' < b.$$

Deze tegenspraak leert ons dat  $q = q'$ , dus dat  $r = a - qb = a - q'b = r'$ . Dit bewijst de eenduidigheid en daarmee de gehele uitspraak. Het getal  $q$  in de stelling heet het *quotiënt* en  $r$  heet de *rest* van  $a$  na deling door  $b$ . Bijvoorbeeld voor  $a = -27$  en  $b = 6$  vinden we  $-27 = -5 \cdot 6 + 3$ , d.w.z.  $q = -5$ ,  $r = 3$ .

**Definitie 4.2.** Laat  $a, b$  gehele getallen zijn. We zeggen:  $a$  *deelt*  $b$  als er een geheel getal  $c$  bestaat met

$$b = ac.$$

Dus bijvoorbeeld 7 deelt 35 omdat  $35 = 7 \cdot 5$ . Als  $a$  het getal  $b$  deelt zeggen we ook dat  $a$  een *deler* is van  $b$  of dat  $b$  *deelbaar* is door  $a$ . De notatie hiervoor is:

$$a \mid b.$$

Merk op dat ieder getal een deler is van 0, terwijl 1 ieder getal deelt. Verder geldt dat wanneer  $a$  zowel  $b$  als  $b'$  deelt, dan deelt  $a$  ook  $b \pm b'$  en ook iedere gehele lineaire combinatie  $xb + yb'$  met  $x, y \in \mathbb{Z}$ .

**Definitie 4.3.** Laat  $a$  en  $b$  gehele getallen zijn, niet beide gelijk aan 0. De *grootste gemene deler* van  $a$  en  $b$ , geschreven  $\text{ggd}(a, b)$ , is het grootste gehele getal dat zowel  $a$  als  $b$  deelt. Verder definiëren we  $\text{ggd}(0, 0) = 0$ . We zeggen dat  $a$  en  $b$  *onderling ondeelbaar* zijn als  $\text{ggd}(a, b) = 1$ .

Als  $d$  een deler is van  $x$  en  $x \neq 0$  dan  $|d| \leq |x|$ . Daarom gaat het hier om het grootste element van een eindige verzameling gehele getallen en heeft bovenstaande definitie zin.

**Lemma 4.4.** *Laat  $a$  en  $b$  gehele getallen zijn. Dan geldt:*

- i)  $\text{ggd}(a, b) = \text{ggd}(b, a)$ ;
- ii)  $\text{ggd}(a, b) = \text{ggd}(-a, b)$ ;
- iii)  $\text{ggd}(a, b + xa) = \text{ggd}(a, b)$  voor alle  $x \in \mathbb{Z}$ .

*Bewijs.* We laten het bewijs van i) en ii) aan de lezer over. Voor iii) merken we op dat iedere deler  $d$  van  $a$  en  $b$  ook de lineaire combinatie  $b + xa$  deelt. Omgekeerd, iedere deler van  $a$  en  $b + xa$  deelt ook de lineaire combinatie  $b = (b + xa) - xa$ . Dus de verzameling van gemeenschappelijke delers van  $a$  en  $b$  is gelijk aan de verzameling van gemeenschappelijke delers van  $a$  en  $b + xa$ . Dit bewijst iii).

**Stelling 4.2.** *Laat  $a$  en  $b$  gehele getallen zijn, niet beide gelijk aan 0. Dan is de grootste gemene deler van  $a$  en  $b$  gelijk aan het kleinste positieve element van de verzameling*

$$L = \{ax + by : x, y \in \mathbb{Z}\}.$$

*Bewijs.* De verzameling  $L$  bevat  $a$ ,  $-a$ ,  $b$  en  $-b$  zoals men ziet door  $x = \pm 1, y = 0$  of  $x = 0, y = \pm 1$  te nemen. Dus  $L$  bevat positieve elementen.

Laat  $d = ax_0 + by_0$  het kleinste positieve element van  $L$  zijn. Omdat alle elementen van  $L$  sommen van veelvouden van  $a$  en  $b$  zijn, zijn ze allemaal door  $\text{ggd}(a, b)$  deelbaar, in het bijzonder is ook  $d$  deelbaar door  $\text{ggd}(a, b)$ . We vinden

$$\text{ggd}(a, b) \leq d. \tag{1}$$

Van de andere kant, als  $c = ax_1 + by_1$  een element van  $L$  is, dan levert deling door  $d$  met rest:  $c = md + r$  met  $0 \leq r < d$ . Maar  $r$  is een lineaire combinatie van  $a$  en  $b$  want

$$r = c - md = a(x_1 - mx_0) + b(y_1 - my_0),$$

dus  $r \in L$ . Omdat  $d$  het kleinste positieve getal in  $L$  is moet  $r$  nul zijn. Dus concluderen we dat  $d$  ieder getal  $c$  in  $L$  deelt. Dus  $d$  deelt in het bijzonder  $a$  en  $b$ , dus

$$d \leq \text{ggd}(a, b). \tag{2}$$

De twee ongelijkheden (1) en (2) tezamen impliceren  $d = \text{ggd}(a, b)$ , zoals te bewijzen was.

**Gevolg 4.5.** *De grootste gemene deler van twee gehele getallen  $a, b$  kan geschreven worden als een lineaire combinatie van  $a$  en  $b$ , d.w.z. er bestaan  $x, y \in \mathbb{Z}$  zodat*

$$\text{ggd}(a, b) = ax + by.$$

*Bewijs.* Dit is duidelijk uit de voorgaande stelling voor  $a, b$  niet beide nul. Wanneer  $a = b = 0$  dan is het ook direct duidelijk.

**Gevolg 4.6.** *Als  $d$  een deler van  $a$  en  $b$  is, dan ook van  $\text{ggd}(a, b)$ .*

**Propositie 4.7.** *Laat  $a, b, c \in \mathbb{Z}$ . Stel  $\text{ggd}(a, b) = 1$  en  $a|bc$ . Dan geldt  $a|c$ .*

*Bewijs.* Het gegeven  $\text{ggd}(a, b) = 1$  impliceert dat er  $x$  en  $y$  zijn met

$$1 = ax + by.$$

Na vermenigvuldiging met  $c$  geeft dit  $c = cax + cby$ . Omdat  $a$  het product  $bc$  deelt is er een  $z \in \mathbb{Z}$  met  $bc = za$ , en dus vinden we  $c = cax + cby = a(cx + zy)$ , d.w.z.  $a$  deelt  $c$ .

## PRIEMGETALLEN EN ONTBINDING

**Definitie 4.8.** Een geheel getal  $p$  heet een *priemgetal* (of simpelweg *priem*) als  $p > 1$  en als de enige positieve delers van  $p$  de getallen 1 en  $p$  zijn. Een geheel getal  $n > 1$  dat niet priem is heet *samengesteld*.

Voorbeelden van priemgetallen zijn:

$$\begin{aligned} 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \dots, \\ 101, 103, 107, 109, 113, 127, 131, 137, 139, \dots, \\ 1009, 1013, 1019, 1021, 1031, \dots, \\ 10007, 10009, 10037, 10039, \dots, \\ 100003, 100019, 100049, \dots, \\ 10000019, 10000079, \dots, \end{aligned}$$

maar ook bijvoorbeeld

$$2^{127} - 1 = 170141183460469231731687303715884105727.$$

We noteren de verzameling van priemgetallen met  $\mathcal{P}$ . De priemgetallen zijn de ‘atomen’ van de wiskunde.

Hoe verder we op de getallenrechte komen, des te minder priemgetallen treffen we aan; alle veelvouden van eerdere priemgetallen vervallen als mogelijke kandidaat. Blijft er op den duur nog iets over? Het antwoord is van Euclides<sup>10</sup> (Prop. 20 uit Boek IX van de Elementen):

**Stelling 4.3.** (Euclides) *Er zijn oneindig veel priemgetallen.*

*Bewijs.* Stel dat  $\mathcal{P}$  eindig is, zeg  $\mathcal{P} = \{p_1, \dots, p_r\}$ . Beschouw dan

$$N = p_1 p_2 \cdots p_r + 1.$$

Laat  $p$  de kleinste deler  $> 1$  van  $N$  zijn. Omdat een deler van  $p$  tenslotte ook een deler van  $N$  is moet  $p$  een priemgetal zijn. Dus geldt  $p = p_i$  voor zekere  $i$ . Maar dan deelt  $p$  zowel  $p_1 p_2 \cdots p_r$  als  $N$ , dus ook het verschil  $N - p_1 p_2 \cdots p_r = 1$ . Deze tegenspraak bewijst dat  $\mathcal{P}$  niet eindig is.

Dit bewijs heeft sinds Euclides nog niets van zijn charme verloren!

**Lemma 4.9.** *Lemma van Euclides. Laat  $a$  en  $b$  gehele getallen zijn en  $p$  een priemgetal. Als  $p$  het product  $ab$  deelt, dan deelt  $p$  ofwel  $a$  ofwel  $b$  (of beide).*

*Bewijs.* Omdat  $p$  priem is geldt  $\text{ggd}(p, a) = 1$  of  $\text{ggd}(p, a) = p$ . Als  $p$  geen deler is van  $a$ , dan  $\text{ggd}(p, a) = 1$ . Uit propositie (4.7) volgt dan dat  $p|b$ .

**Stelling 4.4.** Hoofdstelling van de Rekenkunde. *Ieder geheel getal  $n > 1$  kan geschreven worden als product van priemgetallen: er bestaan priemgetallen  $p_1, \dots, p_r$  zodat*

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_r. \quad (3)$$

*Deze schrijfwijze is eenduidig op de volgorde na.*

<sup>10</sup>Euclides, wiskundige uit Alexandrië die rond 330 v. C. leefde en daar een wiskundige school stichtte tijdens de regering van Ptolemeus I.

*Bewijs.* We bewijzen eerst het bestaan van een schrijfwijze (3). We doen dit met inductie naar  $n$ . Als  $n = 2$  hebben we zo een schrijfwijze met  $r = 1$  en  $p_1 = 2$ . Stel dat het bestaan van zo een schrijfwijze bewezen is voor alle getallen  $x$  met  $1 < x < n$ . Nu is  $n$  òf priem, òf samengesteld. Als  $n$  priem is hebben we de gezochte schrijfwijze  $n = p$ . Stel nu dat  $n$  samengesteld is, zeg  $n = ab$  met  $1 < a, b < n$ . Volgens de inductieveronderstelling kunnen zowel  $a$  als  $b$  als product van priemgetallen geschreven worden:

$$a = p_1 \cdot \dots \cdot p_s \quad \text{en} \quad b = q_1 \cdot \dots \cdot q_t.$$

Dan is  $n = p_1 \cdot \dots \cdot p_s \cdot q_1 \cdot \dots \cdot q_t$  de verlangde schrijfwijze.

Om de eenduidigheid te bewijzen nemen we aan dat er geen uniciteit geldt en beschouwen we het kleinste gehele getal  $n > 1$  dat twee zulke schrijfwijzen heeft:

$$n = p_1 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot q_s. \quad (4)$$

Het priemgetal  $p_1$  deelt dan het product  $q_1 \cdot \dots \cdot q_s$ . Met herhaald toepassen van het Lemma van Euclides volgt dat  $p_1$  een priemgetal  $q_i$  deelt voor een  $1 \leq i \leq s$ . Omdat zowel  $p_1$  als  $q_i$  priem zijn volgt  $p_1 = q_i$ . Deling door  $p_1 = q_i$  levert

$$n/p_1 = p_2 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot q_{i-1} \cdot q_{i+1} \cdot \dots \cdot q_s. \quad (5)$$

Omdat  $n/p_1$  kleiner is dan  $n$  is de schrijfwijze (5) eenduidig op volgorde na. Maar daaruit volgt direct dat ook de schrijfwijze (4) eenduidig is op volgorde na. Dit weerspreekt onze aanname en bewijst de stelling.

We kunnen de stelling ook geldig maken voor  $n = 1$  door het lege product gelijk te stellen aan 1. Voor negatieve gehele getallen  $n$  levert toepassing van de stelling op  $-n$  een schrijfwijze

$$n = -p_1 \cdot \dots \cdot p_r$$

op, wederom eenduidig op volgorde na.

In het bewijs is gebruik gemaakt van het Principe van Volledige Inductie.

**Principe 4.10.** Principe van Volledige Inductie. *Laat  $V$  een verzameling gehele getallen zijn met  $1 \in V$ . Stel dat  $V$  de eigenschap heeft dat wanneer  $n \in V$  ook  $n + 1 \in V$ . Dan is ieder positief geheel getal in  $V$  bevat.*

Dit principe is equivalent met het principe (4.1). In het bewijs van de hoofdstelling van de rekenkunde bestaat  $V$  uit alle getallen die eenduidig te factorizeren zijn. We komen hierop nader terug in het volgende hoofdstuk.

Priemgetallen vormen een fascinerend onderwerp in de wiskunde en sinds kort vinden priemgetallen ook toepassingen in de cryptografie. Eratosthenes<sup>11</sup> gaf een methode aan om alle priemgetallen kleiner dan een gegeven natuurlijk getal te vinden. Beschouw de verzameling  $\{2, 3, 4, 5, \dots, n\}$ . We weten dat 2 een priemgetal is, dus alle tweevouden  $> 2$  zijn niet priem. Streep die door. Het kleinste getal na 2 dat blijft staan (dat is 3) moet dan priem zijn. Maar dan vervallen alle drievouden  $> 3$  als mogelijke priemen, streep die dus door. Ga zo door totdat er niets meer valt door te strepen of het eerstvolgende niet-doorgestreepte getal  $> \sqrt{n}$  is. De getallen die zijn blijven staan zijn de priemgetallen  $\leq n$ . Ga na dat dit een goed algoritme is, dwz een eenduidig recept dat het gevraagde antwoord levert. (Vgl. Opgave 5.) Dit algoritme heet de ‘Zeef van Eratosthenes’. Omdat we steeds meer getallen

<sup>11</sup>Eratosthenes van Cyrene, Grieks wiskundige, 276–194, werkzaam in Alexandrië.

doorstrepen verwachten we hoe verder we op de getallenrechte komen steeds minder vaak een priemgetal tegen te komen. Meer precies, definiëer de functie  $\pi(x)$  op  $\mathbb{N}$  door

$$\pi(x) := \#\{p : p \in \mathbb{N}, p \leq x, p \text{ is priem}\}.$$

Dan kan men bewijzen dat voor elk positief reëel getal  $\epsilon > 0$  er een  $N \in \mathbb{N}$  is zodat

$$\pi(x)/x < \epsilon$$

als  $x > N$ . Dus de spoeling wordt willekeurig dun als we maar ver genoeg gaan. Een precieze analyse van de zeef van Eratosthenes leidt tot deze afschatting.

Het lijkt verder onbegonnen werk veel over de statistiek van het aantal priemgetallen, dwz. het gedrag van de functie  $\pi(x)$  te zeggen. Het verrassende is dat het toch mogelijk is een precieze uitspraak over  $\pi(x)$  te doen. Namelijk dat voor grote  $x$  de functie  $\pi(x)$  zich gaat gedragen als  $x/\log x$ . Dit is de zgn. priemgetalstelling die thuishoort in de analytische getaltheorie en in 1896 door Hadamard<sup>12</sup> en de Vallée Poussin<sup>13</sup> onafhankelijk van elkaar werd bewezen.

### Opgaven

1) Laat  $a$  en  $b$  gehele getallen zijn met  $\text{ggd}(a, b) = d \neq 0$ . Bewijs dat  $a/d$  en  $b/d$  onderling ondeelbaar zijn.

2)

i) Laat  $c$  een positief geheel getal zijn. Bewijs dat  $\text{ggd}(ac, bc) = c \text{ggd}(a, b)$ .

ii) Laat  $a, b, c \in \mathbb{Z}$ . Bewijs dat  $\text{ggd}(a, \text{ggd}(b, c)) = \text{ggd}(\text{ggd}(a, b), c)$ .

3) Laat  $a$  en  $b$  natuurlijke getallen zijn. Laat zien dat het volgende algoritme de ggd van  $a$  en  $b$  levert: Stel  $r_0 = a$  en  $r_1 = b$ . Voor  $k = 2, \dots$  doe:

$$r_k = \text{rest van } r_{k-2} \text{ na deling door } r_{k-1}$$

Als  $r_k = 0$  dan  $\text{ggd}(a, b) = r_{k-1}$ . Als  $r_k \neq 0$ , ga naar volgende  $k$ . Dit algoritme heet het Euclidisch algoritme.

4)

i) Bepaal de grootste gemene deler  $d := \text{ggd}(666, 2003)$  en geef gehele getallen  $x$  en  $y$  aan met  $666 \cdot x + 2003 \cdot y = d$ .

ii) Bepaal alle oplossingen  $(x, y) \in \mathbb{Z}^2$  van de vergelijking  $666 \cdot x + 2003 \cdot y = d$ .

5) Voor ieder priemgetal  $p > 3$  is  $p^2 - 1$  deelbaar door 24. Bewijs dit.

6) Laat zien dat een geheel getal  $n > 1$  priem is dan en slechts dan als  $n$  geen positieve gehele delers  $d$  heeft met  $1 < d \leq \sqrt{n}$ .

7) Laat  $a, b, c \in \mathbb{Z}$ . Als  $x = r/s$  met  $r, s \in \mathbb{Z}$  en  $\text{ggd}(r, s) = 1$  een oplossing is van  $aX^2 + bX + c = 0$  dan is  $r$  een deler van  $c$  en is  $s$  een deler van  $a$ . Bewijs dit. Laat zien dat als  $X^2 + bX + c$  een oplossing  $x$  in de rationale getallen heeft dan  $x \in \mathbb{Z}$ .

8) Laat  $a \in \mathbb{Z}_{>0}$  en  $n \in \mathbb{Z}_{\geq 2}$ . Bewijs dat als  $a^n - 1$  priem is dat  $a = 2$  en  $n$  een priemgetal is. Geldt ook het omgekeerde? De getallen  $2^p - 1$  met  $p$  priem heten de *Mersenne*<sup>14</sup> *getallen*. Het is niet bekend of er oneindig veel Mersenne-priemen onder de Mersenne-getallen zijn. De grootste bekende Mersenne-priem op dit moment (sep. 2008) heeft  $p = 43112609$  en is een getal met 12978189 cijfers.

<sup>12</sup>Hadamard, Frans wiskundige, 1865–1963

<sup>13</sup>de la Vallée Poussin, Belgisch wiskundige, 1866–1962.

<sup>14</sup>Marin Mersenne, een Franse monnik, 1588–1648

**9)** Bepaal alle priemgetallen tussen 1000 en 1100; idem voor de twee intervallen [10 000, 10 100] en [100 000, 100 100].

**10)** Laat zien dat als  $m$  en  $n$  onderling ondeelbare gehele getallen zijn dat

$$\frac{1}{mn} = \frac{x}{m} + \frac{y}{n}$$

voor zekere gehele getallen  $x$  en  $y$ .

**11)** Het product van  $n$  opeenvolgende natuurlijke getallen is deelbaar door  $n!$ . Bewijs dit.

**12)** Laat  $n = p^m$  een macht van een priemgetal zijn ( $m \in \mathbb{N}$ ). Bewijs de volgende formule voor de som van de delers van  $n$ :

$$\sum_{d|n} d = \frac{p^{m+1} - 1}{p - 1}.$$

Wat is voor algemene  $n$  (niet noodzakelijk een priemmacht) de formule voor de som van de delers?

**13)** Bewijs dat voor alle  $n \in \mathbb{Z}_{\geq 2}$  de som  $1 + 1/2 + 1/3 + \dots + 1/n$  niet geheel is.

### Suggesties voor verdere literatuur

Het volgende artikel over priemgetallen kan zeer worden aanbevolen.

D. Zagier: The first 50 Million Prime Numbers. *Mathematical Intelligencer* **0** (1977), p. 7–19.

## 5. VOLLEDIGE INDUCTIE

‘Why,’ said the Dodo, ‘the best way to explain it is to do it.’  
uit: ‘Alice in Wonderland’ van Lewis Carroll<sup>15</sup>

## VOLLEDIGE INDUCTIE

Stel we willen de volgende wel-bekende formule voor de som van de natuurlijke getallen van 1 tot en met  $n$  (met  $n \geq 1$ )

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$$

bewijzen. We kunnen de formule eenvoudig controleren voor lage waarden van  $n$ , zoals  $n = 1$  en  $n = 2$ . Maar als we weten dat de formule waar is voor een gegeven waarde van  $n$  dan is de geldigheid voor de volgende waarde  $n + 1$  gemakkelijk af te leiden. Immers, aan de linkerkant komt er bij de overgang van  $n$  op  $n + 1$  precies  $n + 1$  bij terwijl er aan de rechterkant

$$\frac{(n+1)(n+2)}{2} - \frac{n(n+1)}{2} = 2 \frac{n+1}{2} = n+1,$$

d.w.z. ook  $n+1$ , bijkomt. Kortom, als de formule waar is voor  $n$ , dan ook voor  $n+1$ . Maar omdat de formule waar is voor  $n = 1$  zoals we eenvoudig konden controleren kunnen we stap voor stap de geldigheid voor willekeurige  $n$  afleiden. Deze methode om stap voor stap– *inductief*– de bewering af te leiden heet een *bewijs met volledige inductie* of ook wel bewijs met *natuurlijke inductie*. Dat dit kan volgt direct uit de axioma’s voor de natuurlijke getallen, zie het vorige hoofdstuk.

**Principe 5.1.** (Principe van Volledige Inductie.) *Als  $E$  een eigenschap van natuurlijke getallen is waarvoor geldt i)  $E(1)$  is waar, ii) voor alle  $n \in \mathbf{N}$  geldt: de waarheid van  $E(n)$  impliceert die van  $E(n+1)$ , dan geldt  $E(n)$  voor alle  $n$ .*

Laten we (nog) maar een voorbeeld doen.

**Propositie 5.2.** *Voor elk natuurlijk getal  $n$  geldt*

$$1 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

*Bewijs.* We controleren de formule voor  $n = 1$ . Zowel links als rechts van het gelijkheidsteken vinden we 1. Stel we weten dat de formule geldt voor een zekere  $n$ . Bij de overgang van  $n$  op  $n + 1$  komt er links  $(n + 1)^2 = n^2 + 2n + 1$  bij. Aan de rechterkant komt erbij

$$\frac{(n+1)(n+2)(2(n+1)+1)}{6} - \frac{n(n+1)(2n+1)}{6}$$

dat is

$$\frac{(2n^3 + 9n^2 + 13n + 6) - (2n^3 + 3n^2 + n)}{6} = \frac{6n^2 + 12n + 6}{6} = (n+1)^2.$$

Weer zien we dat er aan beide kanten hetzelfde bijkomt als we van  $n$  op  $n + 1$  overgaan. De formule blijft dus geldig bij deze overgang.

Meer formeel, als we de linkerkant schrijven als

$$L(n) := 1^2 + 2^2 + \dots + n^2$$

---

<sup>15</sup>Charles Lutwidge Dodgson, 1832–1898, Engels literator en wiskundige.

en de rechterkant als

$$R(n) := n(n+1)(2n+1)/6$$

dan zien we direct  $L(n+1) - L(n) = (n+1)^2$  en  $R(n+1) - R(n) = (n+1)^2$  met bovenstaande berekening. Dus als  $L(n) = R(n)$  dan volgt

$$L(n+1) = L(n) + \underbrace{L(n+1) - L(n)}_{=(n+1)^2} = L(n) + (n+1)^2$$

dus met de inductie-aanname

$$= R(n) + (n+1)^2 = R(n) + \underbrace{R(n+1) - R(n)}_{(n+1)^2} = R(n+1).$$

We bewijzen nu het Wel-orderingsprincipe (zie (4.1)) met volledige inductie.

**Principe 5.3.** *Ieder niet-lege deelverzameling van  $\mathbb{N}$  heeft een kleinste element.*

*Bewijs.* We bewijzen met inductie eerst de bewering:

voor elke  $n \in \mathbb{N}$  geldt: iedere niet-lege deelverzameling van  $\{1, 2, \dots, n\}$  heeft een kleinste element.

Bewijs hiervan: Dit is duidelijk juist voor  $n = 1$ , want 1 is dan het kleinste element. Laat  $A$  de verzameling zijn van natuurlijke getallen waarvoor deze bewering juist is. We weten dan dat  $1 \in A$ . We laten zien dat als  $n \in A$  dan ook  $n+1 \in A$ .

Namelijk, laat  $X$  een niet-lege deelverzameling zijn van  $\{1, 2, \dots, n+1\}$ . Als  $X = \{n+1\}$  dan is  $n+1$  het kleinste element. Als  $X \neq \{n+1\}$  dan bekijken we  $X \cap \{1, 2, \dots, n\}$ . Deze verzameling is dan niet leeg. Wegens onze inductieveronderstelling heeft  $X \cap \{1, 2, \dots, n\}$  een kleinste element, dus  $X$  ook. Dus  $n+1 \in A$  en we concluderen dat  $A = \mathbb{N}$ . Dus onze bewering geldt voor alle  $n$ .

Als  $Y$  nu een niet-lege deelverzameling van  $\mathbb{N}$  is, is er een  $n \in Y$  en we bekijken dan  $Y \cap \{1, 2, \dots, n\}$ . Dit heeft een kleinste element, dus  $Y$  ook. Einde bewijs.

#### BINOMIAALCOËFFICIËNTEN

Laat  $n$  en  $k$  natuurlijke getallen zijn met  $n > k$ . We definiëren de binomiaalcoëfficiënt  $\binom{n}{k}$  via

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}$$

waarbij voor een natuurlijk getal  $m$  de uitdrukking  $m!$  (spreek uit:  $m$  faculteit) recursief gedefiniëerd is door

$$1! := 1, \quad m! := (m-1)! \cdot m.$$

We definiëren verder  $0! = 1$  en

$$\binom{n}{n} = \binom{n}{0} = 1 \quad \text{voor alle } n \geq 0$$

en

$$\binom{0}{k} = 0 \quad \text{voor alle } k > 0.$$

We noemen  $\binom{n}{k}$  ‘ $n$  boven  $k$ ’ of ook wel ‘ $n$  kies  $k$ ’ in verband met het volgende lemma.



Binomiaalcoëfficiënten duiken overal op, bijv. in de statistiek en kansrekening. De naam komt van het zgn. binomium van Newton<sup>18</sup>

**Propositie 5.5.** (Binomium van Newton) *Er geldt voor  $n \in \mathbb{Z}_{\geq 0}$*

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}.$$

*Bewijs.* We bewijzen dit met inductie naar  $n$ . De bewering is duidelijk voor  $n = 0$  en  $n = 1$ . Stel we weten dat

$$(x + y)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-1-k}.$$

Dan volgt

$$(x + y)^n = (x + y)^{n-1}(x + y) = \sum_{k=0}^{n-1} \binom{n-1}{k} x^{k+1} y^{n-1-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k}.$$

De coëfficiënt van  $x^k y^{n-k}$  aan de rechterkant is dan  $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$ . Einde bewijs.

We kunnen deze identiteit interpreteren als een identiteit van polynomen in  $x$  en  $y$  met geheeltallige coëfficiënten.

Deze bewijzen laten zien hoe handig natuurlijke inductie soms is.

#### EEN ONGELIJKHEID

We presenteren hier een voorbeeld van een bewijs met volledige inductie waar de inductie met een omweg gaat. Dit prachtige bewijs komt van Cauchy<sup>19</sup> en bewijst een fundamentele ongelijkheid. We moeten even echt werken, maar dat wordt beloond met een fraai resultaat.

We gebruiken in het bewijs de volgende twee eigenschappen van positieve reële getallen  $a, b$  en  $c$ :

$$a < b \iff a^n < b^n \quad \text{voor een } n \in \mathbb{N}$$

en

$$ac < bc \iff a < b.$$

**Stelling 5.1.** *Laat  $r_1, r_2, \dots, r_n$  positieve reële getallen zijn. Dan gelden de ongelijkheden*

$$\frac{n}{\frac{1}{r_1} + \dots + \frac{1}{r_n}} \leq \sqrt[n]{r_1 r_2 \cdots r_n} \leq \frac{r_1 + r_2 + \dots + r_n}{n}.$$

*Verder geldt gelijkheid aan beide kanten precies dan als  $r_1 = r_2 = \dots = r_n$ .*

*Bewijs.* Laat  $E(n)$  de eigenschap zijn dat voor alle  $n$ -tallen van positieve reële getallen  $r_1, \dots, r_n$  geldt

$$r_1 r_2 \cdots r_n \leq \left( \frac{r_1 + r_2 + \dots + r_n}{n} \right)^n.$$

<sup>18</sup>Sir Isaac Newton, 1643–1727, Engels wis- en natuurkundige, een van de belangrijkste wiskundigen, uitvinder van de differentiaal- en integraalrekening.

<sup>19</sup>A. Cauchy, 1789–1857, Frans wiskundige, een van de belangrijkste wiskundigen van zijn tijd.

Uit  $E(n)$  volgt de tweede ongelijkheid in de stelling door de  $n$ -de machts wortel te nemen. Deze ongelijkheid  $E(n)$  geldt voor  $n = 1$  (triviaal, ofwel ‘flauw’) en  $n = 2$ , waar de bewering zegt

$$r_1 r_2 \leq \left( \frac{r_1 + r_2}{2} \right)^2$$

en dit is gelijkwaardig met (breng alles naar een kant)

$$\left( \frac{r_1 + r_2}{2} \right)^2 - r_1 r_2 = \left( \frac{r_1 - r_2}{2} \right)^2 \geq 0$$

en dit laatste is juist want een kwadraat is altijd niet-negatief.

We laten nu de volgende twee implicaties zien:

- i)  $E(n)$  impliceert  $E(n - 1)$  voor  $n \geq 2$ ;
- ii)  $E(n)$  en  $E(2)$  impliceren  $E(2n)$  voor  $n \geq 1$ .

Tezamen impliceren i) en ii) dat uit  $E(n)$  de ongelijkheden  $E(2n)$ ,  $E(2n - 1)$ ,  $E(2n - 2), \dots, E(n + 1)$ , volgen, en dus dat  $E(n + 1)$  geldt. Daarmee kunnen we de volledige inductie voeren.

We bewijzen nu eerst i). We moeten laten zien dat  $E(n - 1)$  geldt onder aanname van  $E(n)$ . Nu is  $E(n - 1)$  een uitspraak over  $n - 1$ -tallen positieve reële getallen. Laat dus  $r_1, \dots, r_{n-1}$  willekeurige positieve getallen zijn. We definiëren nu een  $n$ -de positief reëel getal hierbij door te stellen

$$R = \frac{1}{n-1} \sum_{k=1}^{n-1} r_k.$$

De inductie-hypothese  $E(n)$  toegepast op de  $n$  reële getallen  $r_1, \dots, r_{n-1}, R$  zegt

$$\left( \prod_{k=1}^{n-1} r_k \right) R \leq \left( \frac{\sum_{k=1}^{n-1} r_k + R}{n} \right)^n$$

en de rechterkant kunnen we schrijven als

$$\left( \frac{(n-1)R + R}{n} \right)^n = R^n.$$

Daarom zien we dat

$$\left( \prod_{k=1}^{n-1} r_k \right) R \leq R^n$$

dus na delen door  $R$

$$\prod_{k=1}^{n-1} r_k \leq R^{n-1} = \left( \frac{\sum_{k=1}^{n-1} r_k}{n-1} \right)^{n-1},$$

en dit is precies de ongelijkheid  $E(n - 1)$ , zoals verlangd in i).

Voor de bewering ii) delen we de verzameling  $\{r_1, r_2, \dots, r_{2n}\}$  op in twee verzamelingen van  $n$  reële getallen  $\{r_1, \dots, r_n\}$  en  $\{r_{n+1}, \dots, r_{2n}\}$  en passen op beide verzamelingen  $E(n)$  toe:

$$\prod_{k=1}^{2n} r_k = \left( \prod_{k=1}^n r_k \right) \left( \prod_{k=n+1}^{2n} r_k \right) \leq \left( \sum_{k=1}^n \frac{r_k}{n} \right)^n \left( \sum_{k=n+1}^{2n} \frac{r_k}{n} \right)^n \quad (1)$$

en op de twee factoren aan de rechterkant passen we nu  $E(2)$  toe:

$$\left(\sum_{k=1}^n \frac{r_k}{n}\right) \cdot \left(\sum_{k=n+1}^{2n} \frac{r_k}{n}\right) \leq \left(\frac{\sum_{k=1}^n \frac{r_k}{n} + \sum_{k=n+1}^{2n} \frac{r_k}{n}}{2}\right)^2$$

en dat zegt dat de rechterkant van (1) kleiner gelijk is aan

$$\left(\frac{\sum_{k=1}^{2n} \frac{r_k}{n}}{2}\right)^{2n},$$

dus

$$\prod_{k=1}^{2n} r_k \leq \left(\frac{\sum_{k=1}^{2n} r_k}{2n}\right)^{2n},$$

en dit is juist de ongelijkheid  $E(2n)$ . Daarmee is de bewering in de stelling over de ongelijkheid

$$\sqrt[n]{r_1 r_2 \cdots r_n} \leq \frac{r_1 + \cdots + r_n}{n} \quad (2)$$

bewezen. De andere ongelijkheid

$$\frac{n}{\frac{1}{r_1} + \cdots + \frac{1}{r_n}} \leq \sqrt[n]{r_1 r_2 \cdots r_n}$$

volgt uit (2) door die toe te passen op de positieve reële getallen  $1/r_1, \dots, 1/r_n$ . Immers dit geeft

$$\frac{1}{\sqrt[n]{r_1 r_2 \cdots r_n}} \leq \frac{\frac{1}{r_1} + \cdots + \frac{1}{r_n}}{n}.$$

Maar als geldt  $a/b < c/d$  dan geldt  $b/a > d/c$ , dus we krijgen

$$\sqrt[n]{r_1 r_2 \cdots r_n} \geq \frac{n}{\frac{1}{r_1} + \cdots + \frac{1}{r_n}},$$

zoals verlangd.

Wat nog rest is de uitspraak over het optreden van gelijkheid te bewijzen. Als  $r_1 = r_2 = \dots = r_n$  dan zijn de drie termen in de stelling allemaal gelijk aan  $r_1$ , dus dan geldt gelijkheid. Dat was niet moeilijk.

Stel nu omgekeerd dat  $r_1, \dots, r_n$  positieve reële getallen zijn zodat

$$\sqrt[n]{r_1 r_2 \cdots r_n} = \frac{r_1 + \cdots + r_n}{n}$$

We gaan nu met inductie naar  $n$  bewijzen dat  $r_1 = \dots = r_n$ . Het bewijs is eigenlijk geheel analoog aan de gang van het bewijs van de ongelijkheden en kan als een niet zo makkelijke maar wel verhelderende oefening aan de lezer worden overgelaten. Zo niet, dan volgen hier wat aanwijzingen:

Laat  $G(n)$  de bewering zijn dat voor alle  $n$ -tallen positieve reële getallen  $r_1, \dots, r_n$  geldt: als

$$r_1 r_2 \cdots r_n = \left(\frac{r_1 + \cdots + r_n}{n}\right)^n$$

dan volgt  $r_1 = \dots = r_n$ . Het is niet moeilijk in te zien dat  $G(1)$  juist is en  $G(2)$  ook. Dan is het voldoende te bewijzen:

- i)  $G(n)$  impliceert  $G(n-1)$  voor alle  $n \geq 2$ ;
- ii)  $G(2)$  en  $G(n)$  impliceren  $G(2n)$  voor alle  $n \geq 1$ .

We schetsen een bewijs van i) en laten ii) aan de lezer over. Laat  $r_1, \dots, r_{n-1}$  willekeurige positieve gehele getallen zijn. Neem aan dat geldt

$$r_1 r_2 \cdots r_{n-1} = \left( \frac{r_1 + \dots + r_{n-1}}{n-1} \right)^{n-1}. \quad (3)$$

Definiëer nu  $R = \sum_{i=1}^{n-1} r_i / (n-1)$ . Dan hebben we weer  $n$  positieve reële getallen  $r_1, \dots, r_{n-1}, R$  en gaan hier  $G(n)$  op toepassen. Uit (3) volgt nu

$$r_1 r_2 \cdots r_{n-1} \cdot R = \left( \frac{r_1 + \dots + r_{n-1}}{n-1} \right)^{n-1} \cdot R$$

en de rechterkant is hier gelijk aan

$$R^{n-1} R = R^n.$$

De gelijkheid impliceert wegens de aanname  $G(n)$  dat  $r_1 = r_2 = \dots = R$ . Dus we vinden  $r_1 = \dots = r_{n-1}$ , dwz.  $G(n-1)$  geldt. Ga vooral zelf nu ii) na. Einde bewijs.

Dit is een zeer listig bewijs! Het laat de kracht van natuurlijke inductie zien. De drie termen die in deze stelling optreden hebben een naam:

$$\sqrt[n]{r_1 r_2 \cdots r_n}$$

heet het meetkundig gemiddelde van de getallen  $r_1, \dots, r_n$ . De rechterkant

$$\sum_{k=1}^n r_k / n$$

heet het rekenkundig gemiddelde. De uitdrukking  $n(1/r_1 + \dots + 1/r_n)$  heet het harmonisch gemiddelde.

### Opgaven.

1. Geef een bewijs zonder volledige inductie van de formule  $1 + 2 + \dots + n = n(n+1)/2$ .
- 2) Geef een formule voor de som  $1 + 3 + 5 + \dots + 2n - 1$  van de eerste  $n$  oneven natuurlijke getallen. Bewijs deze formule met volledige inductie.
- 3) Geef een formule voor de som  $1^3 + 2^3 + \dots + n^3$  en bewijs deze formule.
- 4) Bewijs of weerleg: voor  $x = 1, 2, \dots$  is  $x^2 + x + 41$  een priemgetal. (Dit polynoom stamt van Euler<sup>20</sup>.)
- 5) Bewijs:  $\sum_{k=0}^n \binom{n}{k} = 2^n$  voor  $n \in \mathbb{Z}_{\geq 0}$ .
- 6) Laat  $r_1$  en  $s_1$  twee positieve reële getallen zijn. Definiëer voor  $k \geq 2$  getallen  $r_k$  en  $s_k$  door

$$r_k := (r_{k-1} + s_{k-1})/2, \quad s_k := \sqrt{r_{k-1} s_{k-1}}.$$

Ga met de computer na wat er gebeurt met  $(r_k, s_k)$  als  $k$  groot wordt.

- 7) Bewijs dat voor alle  $m$  en  $n$  in  $\mathbb{N}$  geldt:  $(m+1)^n > mn$ .
- 8) Bewijs de identiteit:  $\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$  voor  $n \in \mathbb{N}$ .

---

<sup>20</sup>Leonard Euler, 1707–1783, wiskundige geboren in Basel; een van de belangrijkste wiskundigen van de 18de eeuw.

## 6. EQUIVALENTIERELATIES

*Twee figuren zijn gelijkvormig of equivalent als ze op zich beschouwd niet onderscheiden kunnen worden omdat ze iedere denkbare eigenschap of objectieve betekenis gemeen hebben.*

G.W. Leibniz<sup>21</sup>

## EQUIVALENTIERELATIES

Het komt vaak voor in de wiskunde dat we bepaalde dingen als gelijk willen zien terwijl ze het niet zijn. Bijvoorbeeld beschouwen we  $3 - 4$  en  $-1$  als gelijk. Ook gelijkvormige driehoeken worden soms als gelijk beschouwd. Om verschillende objecten toch als gelijk te kunnen beschouwen voeren we het begrip *equivalentierelatie* in. Dit berust op de observatie dat het gelijkteken  $=$  de volgende eigenschappen heeft:

- i)  $a = a$ ;
- ii) als  $a = b$  dan ook  $b = a$ ;
- iii) als  $a = b$  en  $b = c$  dan  $a = c$ .

**Definitie 6.1.** Een equivalentierelatie op een verzameling  $V$  is een deelverzameling  $R$  van  $V \times V$  zodat voor alle  $a, b, c \in V$  geldt

- i)  $(a, a) \in R$ ;
- ii) als  $(a, b) \in R$  dan ook  $(b, a) \in R$ ;
- iii) als  $(a, b) \in R$  en  $(b, c) \in R$  dan  $(a, c) \in R$ .

De drie eigenschappen heten (in deze volgorde) *reflexiviteit*, *symmetrie* en *transitiviteit*. We schrijven in plaats van  $(a, b) \in R$  vaak eenvoudig  $a \sim b$  en we zeggen:  $a$  is equivalent met  $b$  als  $(a, b) \in R$ . Ook andere symbolen worden soms gebruikt, bijvoorbeeld  $\equiv$  en  $\cong$ , zoals we later zullen zien.

**Definitie 6.2.** Als  $\sim$  een equivalentierelatie is op een verzameling  $V$  en  $v \in V$  een element, dan heet de deelverzameling

$$\{w \in V : w \sim v\}$$

de *equivalentieklasse* van  $v$ .

De equivalentieklasse van  $v$  wordt vaak genoteerd met  $[v]$  of  $\bar{v}$ . We geven nu een aantal voorbeelden.

*Voorbeeld 6.3.* Beschouw het complexe vlak  $\mathbb{C}$ . Elementen hiervan, de complexe getallen, hebben een schrijfwijze  $a+bi$  met  $a, b \in \mathbb{R}$ . Hierbij geldt  $i^2 = -1$ . De norm of absolute waarde  $|z| \in \mathbb{R}_{\geq 0}$  van een complex getal  $z = a + bi$  wordt gedefinieerd door

$$|z|^2 = a^2 + b^2.$$

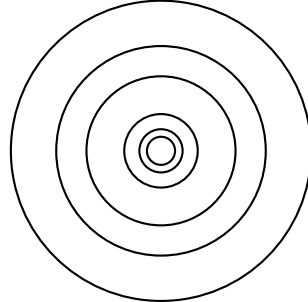
We definiëren nu een equivalentierelatie op  $\mathbb{C}$  door

$$z \sim w \quad \text{dan en slechts dan als} \quad |z| = |w|.$$

---

<sup>21</sup>G.W. Leibniz, Duits wiskundige, 1646–1716, uitvinder van de algebra van de differentiaal- en integraalrekening.

Meetkundig zegt dit: de afstand van  $z$  en  $w$  tot de oorsprong is gelijk. Omdat  $=$  reflexief, symmetrisch en transitief is volgt dit nu ook voor onze  $\sim$ . De equivalentieklasse van  $z \in \mathbb{C}$  is de cirkel met straal  $|z|$  en met de oorsprong als middelpunt.



*Voorbeeld 6.4.* We nemen als verzameling  $\mathbb{Z}$ , de gehele getallen en als relatie

$$a \sim b \quad \text{dan en slechts dan als} \quad 2|(a - b).$$

Dit is een equivalentierelatie: i)  $2|(a - a)$ ; ii) als  $2|(a - b)$  dan ook  $2|(b - a)$ ; iii) als  $2|(a - b)$  en  $2|(b - c)$  dan  $2|(a - b) + (b - c)$ , dus  $2|(a - c)$  zoals gewenst.

De equivalentieklasse van 0 bestaat uit alle *even* getallen; de equivalentieklasse van 1 bestaat uit alle *oneven* getallen. We schrijven

$$a \equiv b \pmod{2} \quad \text{voor} \quad a \sim b.$$

*Voorbeeld 6.5.* Beschouw weer de verzameling van gehele getallen  $\mathbb{Z}$ . Laat  $n$  een gegeven positief geheel getal zijn. Definieer op  $\mathbb{Z}$  een equivalentierelatie  $\sim$  door

$$a \sim b \quad \text{dan en slechts dan als} \quad n|(a - b).$$

Dit is ook weer een equivalentierelatie. (Ga dit na!) We schrijven nu om verwarring te voorkomen  $a \equiv b \pmod{n}$  in plaats van  $a \sim b$  en zeggen<sup>22</sup> *a is congruent met b modulo n*. De equivalentieklasse van  $a$  wordt genoteerd als  $a \pmod{n}$  of kortweg met  $\bar{a}$ .

De equivalentieklasse van een getal  $a$  is gelijk aan die van zijn rest  $r$  bij deling door  $n$ . Er geldt  $0 \leq r < n$ . We zien dus in dat er precies  $n$  equivalentieklassen zijn, namelijk

$$\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}.$$

Deze equivalentieklassen heten ook wel *restklassen* modulo  $n$ . De notatie voor deze verzameling equivalentieklassen is  $\mathbb{Z}/n\mathbb{Z}$ . Dus

$$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

met

$$\bar{0} = \{\dots, -10, -5, 0, 5, 10, \dots\}$$

$$\bar{1} = \{\dots, -9, -4, 1, 6, 11, \dots\}$$

etc.

---

<sup>22</sup>Deze notatie stamt van C.F. Gauss, Duits wiskundige, 1777–1855, een van de belangrijkste wiskundigen.

We zien in deze voorbeelden dat onze verzameling  $V$  opgedeeld wordt in disjuncte equivalentieklassen. Dat geldt algemeen:

**Definitie 6.6.** Een verdeling of partitie van een verzameling  $V$  is een collectie niet-lege disjuncte deelverzamelingen  $V_i : i \in I$  (met  $I$  een of andere indexverzameling) van  $V$  zodat hun vereniging gelijk is aan  $V$ .

**Propositie 6.7.** Laat  $V$  een verzameling zijn met een equivalentierelatie  $\sim$ . Dan geven de equivalentieklassen een verdeling van  $V$ .

*Bewijs.* Neem een element  $x \in V$ . Noteer de equivalentieklasse van  $x$  met  $\bar{x}$ . Wegens eigenschap i) geldt  $x \in \bar{x}$ . Dus een equivalentieklasse  $\bar{x}$  is niet leeg. Ook volgt hieruit dat de vereniging van de equivalentieklassen gelijk is aan  $V$ . Neem nu twee equivalentieklassen  $\bar{x}$  en  $\bar{y}$ . Stel dat hun doorsnede niet leeg is, zeg  $z \in \bar{x} \cap \bar{y}$ . Dan geldt  $x \sim z$  en  $y \sim z$  en wegens de symmetrie en transitiviteit geldt dus ook  $x \sim y$ . Dus als  $v \sim x$  geldt wegens transitiviteit  $v \sim y$ . Maar dat betekent  $\bar{x} = \bar{y}$ .

*Voorbeeld 6.8.* Beschouw het platte vlak  $\mathbb{R}^2$ . Kies een lijn  $L$  in  $\mathbb{R}^2$  door de oorsprong. Definieer een equivalentierelatie op  $\mathbb{R}^2$  via

$$v_1 \sim v_2 \quad \text{dan en slechts dan als} \quad v_1 - v_2 \in L.$$

Omdat  $0 \in L$  en met  $w \in L$  ook  $-w \in L$  volgen de reflexiviteit en de symmetrie. (Ga zelf na!) Verder geldt dat als  $v_1 - v_2 \in L$  en  $v_2 - v_3 \in L$  dat ook  $(v_1 - v_2) + (v_2 - v_3) \in L$ , waaruit de transitiviteit volgt. De equivalentieklasse van een element  $x \in \mathbb{R}^2$  bestaat uit alle vectoren van de vorm  $x + v$  met  $v \in L$ :

$$\bar{x} = \{x + v : v \in L\} = x + L.$$

Dus de equivalentieklasse is een lijn die evenwijdig is met  $L$ . Door ieder punt  $x \in \mathbb{R}^2$  gaat precies één lijn evenwijdig met  $L$ . De verdeling of partitie van  $\mathbb{R}^2$  wordt verkregen door  $\mathbb{R}^2$  te schrijven als disjuncte vereniging van alle lijnen evenwijdig met  $L$ .

We kunnen een equivalentierelatie vaak gebruiken om nieuwe wiskundige objecten te definiëren. We geven een paar voorbeelden.

**Constructie 6.9.** We gaan uit van de verzameling  $\mathbb{N} = \{1, 2, 3, \dots\}$  van natuurlijke getallen en gaan nu de verzameling  $\mathbb{Z}$  van de gehele getallen daaruit construeren. Beschouw de verzameling  $V = \mathbb{N} \times \mathbb{N}$  van geordende paren natuurlijke getallen. We definiëren een equivalentie  $\sim$  op  $V$  door:

$$(a, b) \sim (c, d) \quad \text{dan en slechts dan als} \quad a + d = c + b.$$

Het is niet moeilijk na te gaan dat dit een equivalentierelatie is. In het bijzonder is  $(a, b)$  equivalent met  $(a + x, b + x)$  voor iedere  $x \in \mathbb{N}$ . Denk gewoon aan de klasse van  $(a, b)$  als het verschil  $a - b$ . We noteren het paar  $(a, b)$  ook wel met  $a - b$ . We noteren de verzameling van equivalentieklassen voor het moment even met  $\Gamma$ . We kennen  $\Gamma$  al: het zijn de gehele getallen.

We kunnen nu een afbeelding maken  $\mathbb{N} \rightarrow \Gamma$  via  $n \mapsto \overline{(n + 1, 1)}$ . We kunnen dit uitbreiden tot een bijectie  $\mathbb{Z} \rightarrow \Gamma$  via  $n \mapsto \overline{(n + x, x)}$  waarbij  $x = x_n > 0$  zo gekozen is dat  $n + x > 0$ .

**Constructie 6.10.** In het tweede voorbeeld construeren we de rationale getallen ('breuken') uit de gehele getallen. Beschouw de verzameling  $V = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : b \neq 0\}$  van paren gehele getallen met  $b \neq 0$ . We definiëren een equivalentie  $\sim$  op  $V$  door:

$$(a, b) \sim (c, d) \quad \text{dan en slechts dan als} \quad ad = bc.$$

Het is niet moeilijk na te gaan dat dit een equivalentierelatie is. We controleren de transitiviteit. Als  $(a, b) \sim (c, d)$  en  $(c, d) \sim (e, f)$  dan geldt  $ad = bc$  en  $cf = de$ . Dit betekent dat  $adc f = bcde$ . Als  $c = 0$ , dan volgt  $a = 0$  en  $e = 0$  en geldt  $af = be$ . Als  $cd = dc \neq 0$  volgt ook  $af = be$  dus  $(a, b) \sim (e, f)$ .

In het bijzonder is  $(a, b)$  equivalent met  $(ax, bx)$  voor iedere  $x \in \mathbb{Z}$ ,  $x \neq 0$ . Denk gewoon aan de klasse van  $(a, b)$  als het quotiënt  $a/b$ . We noteren de equivalentieklasse van  $(a, b)$  ook als  $a/b$ . Er geldt dus

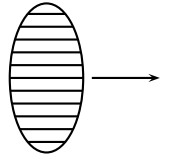
$$a/b = c/d \iff ad = bc.$$

De verzameling equivalentieklassen kan geïdentificeerd worden met de verzameling  $\mathbb{Q}$  van breuken. Iedere equivalentieklasse van een paar  $(a, b)$  met  $a \neq 0$  bevat precies één paar  $(a', b')$  waarbij  $\text{ggd}(a', b') = 1$  en  $b' > 0$ .

Een ander voorbeeld van een equivalentierelatie komt van een afbeelding  $f : X \rightarrow Y$ . Laat  $X, Y$  twee verzamelingen zijn en laat  $f : X \rightarrow Y$  een afbeelding zijn. We definiëren een equivalentierelatie op  $X$  via

$$x \sim y \quad \text{dan en slechts dan als} \quad f(x) = f(y).$$

Dit is een equivalentierelatie. Een equivalentieklasse heet een *vezel* van de afbeelding  $f$ .



*Voorbeeld 6.11.* i) Laat  $f : \mathbb{C} \rightarrow \mathbb{C}$  de afbeelding  $f(z) = z^n$  zijn. De vezels van  $f$  zijn van de vorm  $\{x, \zeta x, \zeta^2 x, \dots, \zeta^{n-1} x\}$  met  $\zeta = e^{2\pi i/n} = \cos(2\pi/n) + i \sin(2\pi/n)$  een zgn.  $n$ -de machts eenheidswortel. ii) Laat  $f : \mathbb{C} \rightarrow \mathbb{R}_{\geq 0}$  de afbeelding zijn met  $f(z) = |z|$ . De vezels zijn de cirkels met middelpunt  $0 \in \mathbb{C}$ , vgl. voorbeeld (6.3).

Vaak is het handig om uit iedere equivalentieklasse één element te kiezen waarmee we dan werken. Welk element dit is, doet dan meestal niet terzake. Bijvoorbeeld zouden we uit de verzameling equivalentieklassen  $\mathbb{Z}/5\mathbb{Z}$  van de relatie  $a \equiv b \pmod{5}$  de elementen  $0, 1, 2, 3, 4$  kunnen kiezen.

**Definitie 6.12.** Laat  $R$  een equivalentierelatie op de verzameling  $V$  zijn. Een *volledig representanten-systeem* voor  $R$  (ook wel volledig stelsel van representanten) is een deelverzameling  $W$  van  $V$  die uit iedere equivalentieklasse precies één element bevat.

**(6.13) Voorbeelden.** De verzameling  $\{0, 1, 2, 3, 4\}$  is een volledig representantensysteem voor de equivalentierelatie  $a \equiv b \pmod{5}$  op de gehele getallen  $\mathbb{Z}$ . De verzameling  $\{15, 26, -8, 18, 104\}$  is dat ook. Een lijn die niet evenwijdig is aan  $L$  in Voorbeeld (6.8) snijdt iedere lijn evenwijdig aan  $L$  in één punt en vormt dus zo een volledig representantensysteem voor de equivalentierelatie in (6.8). Geef zelf een volledig representantensysteem voor het voorbeeld van (6.3).

### Opgaven

1) Een *relatie* op een verzameling  $V$  is een deelverzameling van de verzameling  $V \times V$ . Geef een voorbeeld van een relatie die reflexief en symmetrisch is, maar niet transitief. Geef een voorbeeld van een relatie die symmetrisch en transitief is, maar niet reflexief.

2) Is de volgende relatie op de reële getallen  $\mathbb{R}$  een equivalentierelatie?  $x \sim y \iff xy \geq 0$

3) Bewijs dat een partitie van  $V$  aanleiding geeft tot een equivalentierelatie. Concludeer dat equivalentierelaties en partities gelijkwaardige begrippen zijn.

Definieer een relatie op het platte vlak  $\mathbb{R} \times \mathbb{R}$  door  $P \sim Q$  dan en slechts dan als  $P$  en  $Q$  dezelfde  $x$ -coördinaat hebben. Is dit een equivalentierelatie? Zo ja, beschrijf de equivalentieklassen.

5) Geef een volledig representantensysteem voor de equivalentierelatie van voorbeeld (6.11).

6) Bewijs de volgende beweringen over getallen  $n \in \mathbb{N}$  in het tientallig stelsel. i)  $n$  is deelbaar door 3 dan en slechts dan als de som van de cijfers van  $n$  deelbaar is door 3; ii)  $n$  is deelbaar door 9 dan en slechts dan als de som van de cijfers van  $n$  deelbaar is door 9; iii)  $n$  is deelbaar door 11 dan en slechts dan als de alternerende som van de cijfers deelbaar is door 11.

7) Bewijs dat  $a \sim b \iff a - b \in \mathbb{Z}$  een equivalentierelatie op de verzameling van reële getallen  $\mathbb{R}$  definieert. Geef een volledig stelsel representanten aan.

8) Geldt het Principe (4.1) ook voor de verzameling  $\mathbb{Q}$  van de rationale getallen?

9) Laat zien dat voor  $a, b \in \mathbb{Z}$  geldt  $(a+b)^p \equiv a^p + b^p \pmod{p}$  voor ieder priemgetal  $p$ .

10) Laat  $n, x \in \mathbb{N}$  met  $1 < x < n$ . Bewijs dat  $n$  geschreven kan worden als

$$n = a_0 + a_1x + a_2x^2 + \dots + a_kx^k$$

voor een zekere  $k$  en gehele getallen  $a_i$  met  $0 \leq a_i < x$  en dat  $k$  en de  $a_i$  éénduidig door  $n$  en  $x$  bepaald zijn.

11) Laat zien dat als  $a, b \in \mathbb{Z}$  dan  $(a-b)|(a^n - b^n)$ . Laat verder zien dat  $a+b$  het getal  $a^n + b^n$  deelt als  $n$  oneven is.

12) Voor welke gehele getallen  $x$  dat  $x^2 \equiv 1 \pmod{8}$ ?

13) Laat zien dat gelijkmatigheid een equivalentierelatie op een collectie verzamelingen is. De equivalentieklasse van  $X$  heet de *cardinaliteit* van  $X$ .

## 7. ONEINDIGE VERZAMELINGEN

*je le vois, mais je ne le crois pas*  
Cantor aan Dedekind<sup>23</sup>

We noemen een verzameling  $X$  eindig als  $X$  leeg is of er een natuurlijk getal  $n \in \mathbb{N}$  bestaat en een bijectie  $X \longleftrightarrow \{1, 2, \dots, n\} = \mathbb{N}_{\leq n}$ . Een verzameling  $X$  heet oneindig als  $X$  niet eindig is. Het standaardvoorbeeld van een oneindige verzameling is de verzameling  $\mathbb{N}$  van natuurlijke getallen. (Bewijs zelf met inductie dat  $\mathbb{N}$  niet eindig is.) We zullen zien dat dit in zekere zin ook de ‘kleinste’ oneindige verzameling is. Andere oneindige verzamelingen zijn  $\mathbb{Q}$ , de rationale getallen en  $\mathbb{R}$ , de reële getallen. Op het eerste gezicht lijkt  $\mathbb{Q}$  ‘groter’ dan  $\mathbb{N}$  en  $\mathbb{R}$  weer ‘groter’ dan  $\mathbb{Q}$ . Dit leidt tot de vraag:

*zijn  $\mathbb{N}$  en  $\mathbb{Q}$  gelijkmachtig?*

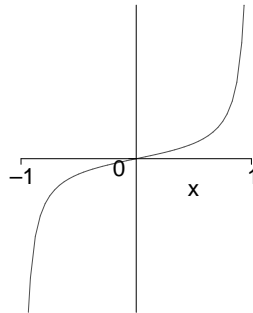
en ook

*zijn  $\mathbb{N}$  en  $\mathbb{R}$  gelijkmachtig?*

Met andere woorden, kunnen we een bijectie  $\mathbb{N} \longleftrightarrow \mathbb{Q}$  of  $\mathbb{N} \longleftrightarrow \mathbb{R}$  construeren? Dat onze eerste intuïtie misleidend kan zijn mag blijken uit het feit dat de functie

$$f : (-1, 1) = \{x \in \mathbb{R} : -1 < x < 1\} \rightarrow \mathbb{R}, x \mapsto \tan(\pi x/2)$$

een bijectie levert tussen een interval en de hele reële rechte. De functie  $x \mapsto x/(1-x^2)$  op  $(-1, 1)$  doet dit ook. Kortom, voorzichtigheid is geboden.



**Opgave** Ga na dat de intervallen  $(-1, 1)$  en  $(0, 1)$  gelijkmachtig zijn. Meer algemeen, bewijs dat een interval  $(a, b) \subset \mathbb{R}$  met  $a < b$  gelijkmachtig is met  $(0, 1)$ .

**Definitie 7.1.** Een verzameling  $X$  heet *aftelbaar* als  $X$  eindig is of gelijkmachtig met  $\mathbb{N}$ . In het laatste geval heet  $X$  *aftelbaar oneindig*. Een verzameling die niet aftelbaar is heet *overaftelbaar*.

Stel we voegen aan  $\mathbb{N}$  een element toe, zeg het getal 0; de resulterende verzameling

$$\mathbb{Z}_{\geq 0}$$

is gelijkmachtig met  $\mathbb{N}$  via de bijectieve afbeelding die aan  $x$  het getal  $x+1$  toevoegt. We kunnen dit herhalen. Dus het toevoegen van een eindige verzameling aan  $\mathbb{N}$  verandert niets aan de cardinaliteit, het is water naar de zee dragen: de resulterende verzameling is gelijkmachtig met  $\mathbb{N}$ .

<sup>23</sup>R. Dedekind, 1831-1916, Duits wiskundige, speelde een belangrijke rol in de getaltheorie.

Vaak wordt dit opmerkelijke feit geïllustreerd met de notie van ‘Het Hotel van Hilbert<sup>24</sup>’, waar de kamers genummerd zijn met de natuurlijke getallen. Ook al is het hotel volgeboekt, is er altijd nog plaats voor een extra gast. Men vraagt de al aanwezige gasten om een kamer op te schuiven, waardoor kamer 1 beschikbaar komt voor de nieuwe gast.

De verzameling  $\mathbb{Z}$  van gehele getallen is ook aftelbaar; we kunnen de elementen van  $\mathbb{Z}$  opsommen als

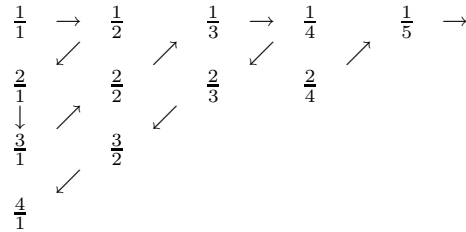
$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}.$$

(Meer formeel, de afbeelding  $\mathbb{N} \rightarrow \mathbb{Z}$  gegeven door  $x \mapsto (-1)^x \lfloor x/2 \rfloor$ , met  $\lfloor a \rfloor$  het grootste gehele getal  $\leq a$ , geeft de bijectie.)

De eerste verrassing komt met het volgende resultaat.

**Propositie 7.2.** *De verzameling  $\mathbb{Q}$  is aftelbaar.*

*Bewijs.* We kunnen de positieve rationale getallen  $\mathbb{Q}_{>0}$  als volgt opsommen

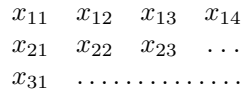


waarbij we breuken die we al gehad hebben overslaan. Dus  $\mathbb{Q}_{>0}$  is aftelbaar. Maar dan is ook  $\mathbb{Q}_{>0} \cup \mathbb{Q}_{<0}$  aftelbaar door na  $a/b$  eerst  $-a/b$  te noemen, en ook  $\mathbb{Q} = \mathbb{Q}_{>0} \cup \mathbb{Q}_{<0} \cup \{0\}$  is dan aftelbaar.

Hetzelfde argument als gebruikt om de aftelbaarheid van  $\mathbb{Q}$  te bewijzen voldoet voor het volgende Gevolg.

**Gevolg 7.3.** *De aftelbare vereniging van aftelbare verzamelingen is aftelbaar: Laat  $X_n$  voor  $n \in \mathbb{N}$  aftelbare verzamelingen zijn. Dan is de vereniging  $\cup_{n \in \mathbb{N}} X_n$  weer aftelbaar.*

Immers, als  $X_n = \{x_{n1}, x_{n2}, x_{n3}, \dots\}$  dan kunnen we de vereniging  $\cup_{n \in \mathbb{N}} X_n$  schrijven in een diagram



en dit diagram doorlopen als gedaan bij  $\mathbb{Q}_{>0}$ .

Na deze ervaringen is de natuurlijke vervolgvraag: is  $\mathbb{R}$  aftelbaar? De volgende stelling geeft het antwoord.

**Stelling 7.1.** (Cantor) *De verzameling  $\mathbb{R}$  van reële getallen is overaftelbaar.*

*Bewijs.* We gaan bewijzen dat het interval

$$I = (0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$$

---

<sup>24</sup>David Hilbert, 1862–1943, de belangrijkste Duitse wiskundige uit het begin van de 20ste eeuw

niet aftelbaar is. Dan is  $\mathbb{R}$  ook niet aftelbaar (omdat  $(0, 1) \subset \mathbb{R}$ ; ga na). Stel dat  $I$  aftelbaar is, dus

$$I = \{r_1, r_2, r_3, \dots\}.$$

We schrijven de reële getallen  $r_i$  in hun decimale ontwikkeling, en wel zo dat er niet oneindig veel nullen ‘aan het eind’ komen. Dus in plaats van  $r = 0,50000\dots$  schrijven we  $0,499999\dots$ . Dan is deze decimale schrijfwijze eenduidig. We schrijven de  $r_i$  nu in een diagram

$$\begin{array}{rcccc} r_1 & = & 0, & a_{11} & a_{12} & a_{13} & \dots \\ r_2 & = & 0, & a_{21} & a_{22} & a_{23} & \dots \\ r_3 & = & 0, & a_{31} & a_{32} & a_{33} & \dots \\ r_4 & = & 0, & a_{41} & a_{42} & a_{43} & \dots \\ & & & \dots & & & \end{array}$$

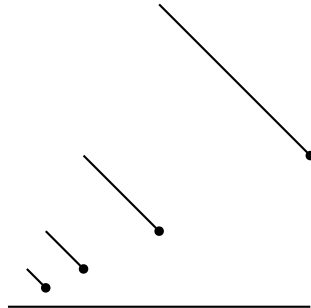
waarbij  $a_{ij}$  het  $j$ -de decimale cijfer achter de komma van  $r_i$  is. Het fantastische idee van Cantor is om de ‘diagonaal’ te nemen

$$0.a_{11}a_{22}a_{33}\dots$$

en in deze ontwikkeling iedere  $a_{ii}$  te veranderen, bijv. door er 1 bij op tellen (maar wel zo dat er aan het eind niet alleen nullen of negens staan). We krijgen zo een getal  $s \in (0, 1)$ . Dit getal  $s$  kan niet in onze lijst  $\{r_1, r_2, \dots\}$  voorkomen, want op de  $n$ -de plaats achter de komma staat een cijfer dat verschillend is van  $a_{nn}$ . Dit bewijst dat  $(0, 1)$  overaftelbaar is.

**Opgave.** Laat zien dat  $(0, 1] = \{x \in \mathbb{R} : 0 < x \leq 1\}$  en  $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$  gelijkmachtig zijn via de functie

$$x \mapsto \frac{3}{2^{n+1}} - x \quad \text{als} \quad 2^{-n-1} < x \leq 2^{-n} \quad n = 0, 1, 2, \dots$$



Ga verder ook na dat  $(0, 1)$  en  $[0, 1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$  gelijkmachtig zijn. Concludeer dat  $\mathbb{R}$  en  $(0, 1]$  gelijkmachtig zijn.

Deze resultaten laten zien hoe weinig onze intuïtie te vertrouwen is bij het hanteren van oneindige verzamelingen. Het kan nog erger:

**Stelling 7.2.** *Het vlak en de rechte zijn gelijkmachtig, d.w.z.  $\mathbb{R}$  en  $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$  zijn gelijkmachtig.*

*Bewijs* We bewijzen dat  $(0, 1]$  en  $(0, 1] \times (0, 1]$  gelijkmachtig zijn. We schrijven reële getallen weer met hun decimale ontwikkeling zonder oneindig veel nullen op het

eind. Laat nu  $(a, b) \in (0, 1]^2$  en schrijf de decimale ontwikkeling van  $a$  en  $b$  als in het volgende voorbeeld

$$\begin{array}{r} a = 0, \quad 5 \quad 001 \quad 7 \quad 4 \quad 7 \quad 005 \quad 03\dots \\ b = 0, \quad 006 \quad 2 \quad 08 \quad 9 \quad 0002 \quad 1 \quad 9\dots \end{array}$$

waarbij we de cijfers zo groeperen dat een groepje eindigt na het eerste cijfer ongelijk 0.

De afbeelding

$$\rho : (0, 1] \times (0, 1] \rightarrow (0, 1]$$

voegt nu aan  $(a, b)$  het getal  $c$  toe dat begint met 0, en dan het eerste groepje (na de komma) van  $a$ , dan het eerste groepje van  $b$ , daarna het tweede groepje van  $a$  en zo afwisselend de groepjes van  $a$  en  $b$ . Dus

$$\rho((a, b)) = 0, 50060012708\dots$$

Merk op dat  $c$  niet alleen nullen aan het eind heeft, dus de afbeelding is welgedefinieerd. Maar uit het beeld  $c$  kunnen we  $a$  en  $b$  direct terugvinden (door gewoon naar de nullen in de ontwikkeling van  $c$  te kijken). Dus de afbeelding is injectief en ook surjectief. Dit geeft de gevraagde bijectie.

*Vraag:* Waarom kunnen we niet gewoon afwisselend een cijfer van  $a$  en van  $b$  nemen?

Dit resultaat is bepaald contra-intuïtief te noemen; ook Cantor kon zijn eigen ogen niet geloven, zie het citaat hierboven. De afbeelding verknijpt het interval ook behoorlijk. Als we eisen dat de afbeelding continu is (zie Analyse voor de definitie van continu) lukt het niet meer zo een bijectie te maken. Dat is een beroemd resultaat van Brouwer<sup>25</sup> over het behoud van dimensie onder continue afbeeldingen. Deze stelling valt buiten dit bestek; de stelling komt aan de orde bij de algebraïsche topologie.

Zoals we al vermeldde is  $\mathbb{N}$  in zekere zin de ‘kleinste’ oneindige verzameling. Immers, als  $X$  niet eindig is, is  $X$  niet-leeg en kunnen we een element  $x_1$  uit  $X$  kiezen. Omdat  $X - \{x_1\}$  ook niet leeg is (want oneindig) kunnen we een element  $x_2$  kiezen. Met inductie vinden we een aftelbare deelverzameling

$$\{x_1, x_2, x_3, \dots\}$$

van  $X$ . Bij dit procédé gebruiken we het volgende axioma uit de verzamelingenleer. Sommige wiskundigen geven er de voorkeur aan dit axioma niet te gebruiken, maar kunnen dan minder bewijzen.

**Principe 7.4.** (Keuze-Axioma) *Gegeven zij een collectie van disjuncte niet-lege verzamelingen  $X_\alpha$  met  $\alpha \in A$ . Dan is er een verzameling  $X$  zodat  $X$  uit iedere  $X_\alpha$  precies één element bevat.*

De cardinaliteit van  $\mathbb{N}$  wordt wel genoteerd met  $\aleph_0$  (aleph nul). De vraag is ‘wat daarna komt’. Een eerste indicatie geeft de volgende stelling.

**Stelling 7.3.** *De verzameling  $\mathbb{R}$  van de reële getallen is gelijkmachting met de machtsverzameling van  $\mathbb{N}$ . Met andere woorden, er is een bijectie  $\mathbb{R} \leftrightarrow \mathcal{P}(\mathbb{N})$ .*

<sup>25</sup>L.E.J. Brouwer, 1881-1966, was hoogleraar aan deze universiteit en grondlegger van de algebraïsche topologie.

*Bewijs.* We schrijven in dit bewijs reële getallen in het binaire stelsel in plaats van in het tientallige stelsel. Dus bijv. wordt 691, dat is  $6 \times 10^2 + 9 \times 10 + 1$  geschreven als

$$1010110011$$

want  $691 = 2^9 + 2^7 + 2^5 + 2^4 + 2 + 1$ . Ieder reëel getal laat zich nu schrijven in een binaire ontwikkeling, waarbij we weer aannemen dat er ‘aan het eind’ niet alleen nullen staan. Dus  $0,011100000000\dots$  wordt geschreven als  $0,011011111111\dots$ . Met ieder reëel getal in  $(0, 1]$  correspondeert nu een rijtje nullen en enen (namelijk de getallen achter de komma). Aan de andere kant wordt een deelverzameling  $X$  van  $\mathbb{N}$  ook gegeven door een oneindige rij nullen en enen, namelijk het  $n$ -de cijfer zegt of  $n$  tot de deelverzameling  $X$  behoort ( $0 = \text{ja}$ ,  $1 = \text{nee}$ ). Als  $X$  niet het complement van een eindige deelverzameling van  $\mathbb{N}$  is levert dit een getal met niet alleen nullen aan het eind. Dus we krijgen op deze manier een bijectie tussen de reële getallen in  $(0, 1]$  en de deelverzamelingen van  $\mathbb{N}$  die niet van de vorm  $\mathbb{N}$  minus een eindige verzameling zijn. De verzameling van deelverzamelingen van de vorm  $\mathbb{N}$  minus een eindige verzameling is aftelbaar. (Ga na.) Nu is de disjuncte vereniging van een interval met een aftelbare verzameling gelijkmachtig met het interval. Dit bewijst de stelling.

De verwachting dat het eerste cardinaalgetal na  $\aleph_0$  gelijk is aan de cardinaliteit van  $\mathbb{R}$  werd de continuümhypothese genoemd. Met andere woorden, deze hypothese zegt dat er geen verzameling is met een cardinaliteit die ligt tussen de cardinaliteit van  $\mathbb{N}$  en die van  $\mathbb{R}$ . Cohen<sup>26</sup> heeft laten zien dat deze continuümhypothese onafhankelijk is van de gebruikelijke axioma’s van de verzamelingenleer. We kunnen de continuümhypothese dus als een extra axioma erbij nemen (of dat niet doen).

Het ‘diagonaalargument’ van Cantor laat zich generaliseren tot de volgende stelling.

**Stelling 7.4.** (Cantor) *Laat  $X$  een verzameling zijn. Dan zijn  $X$  en  $\mathcal{P}(X)$  niet gelijkmachtig.*

*Bewijs.* Er is altijd een injectieve afbeelding  $X \rightarrow \mathcal{P}(X)$  gegeven door  $x \mapsto \{x\}$ . We gaan laten zien dat er geen surjectie  $X \rightarrow \mathcal{P}(X)$  bestaat. Laat  $f : X \rightarrow \mathcal{P}(X)$  een willekeurige afbeelding zijn. We laten zien dat het beeld  $f(X)$  in  $\mathcal{P}(X)$  niet gelijk kan zijn aan  $\mathcal{P}(X)$ .

We bekijken hiervoor de verzameling

$$Z := \{x \in X : x \notin f(x)\}.$$

Dit is een deelverzameling van  $X$ , dus een element van  $\mathcal{P}(X)$ . Als  $Z$  in het beeld van  $f$  ligt dan is er een  $\xi \in X$  met

$$Z = f(\xi).$$

Nu geldt

$$\xi \in Z \iff \xi \notin f(\xi) \iff \xi \notin Z$$

waar de eerste  $\iff$  komt van de definitie van  $Z$  en de tweede  $\iff$  van de aanname dat  $Z = f(\xi)$ . Deze tegenspraak bewijst de stelling.

Met deze laatste stelling van Cantor kunnen we steeds grotere cardinaalgetallen maken. Dit is voer voor logici. Maar in de dagelijkse wiskundige praktijk kunnen we meestal toe met de cardinaliteiten van  $\mathbb{N}$  en  $\mathbb{R}$ .

<sup>26</sup>Paul J. Cohen, 1934-, Amerikaans wiskundige en logicus.

### Opgaven

- 1) Is de verzameling van afbeeldingen van  $\{0, 1\}$  naar  $\mathbb{N}$  aftelbaar? Is de verzameling van afbeeldingen  $f : \mathbb{N} \rightarrow \mathbb{N}$  aftelbaar?
- 2) Bewijs dat voor ieder natuurlijk getal  $n \in \mathbb{Z}_{>0}$  de verzamelingen  $\mathbb{R}$  en  $\mathbb{R}^n$  gelijkmachtig zijn.
- 3) Schrijf 666 in het tweetallig stelsel. Schrijf  $\pi$  in het tweetallig stelsel tot op twintig decimalen.
- 4) Laat  $Y$  een eindige deelverzameling van de oneindige verzameling  $X$  zijn. Bewijs:  $X$  is gelijkmachtig met  $X - Y$ .
- 5) Bewijs dat de cirkel  $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$  gelijkmachtig is met een interval  $[0, 1]$ .
- 6) Laat  $X$  een aftelbare verzameling zijn. Bewijs dat de verzameling van eindige deelverzamelingen van  $X$  aftelbaar is.
- 7) Bewijs dat de disjuncte vereniging  $Y$  van  $\mathbb{R}$  en een aftelbare verzameling gelijkmachtig is met  $\mathbb{R}$ .
- 8) Laat  $X$  en  $Y$  verzamelingen zijn met  $X \subset Y$  en laat een injectie  $f : Y \rightarrow X$  gegeven zijn. Definiëer verzamelingen  $X_n$  en  $Y_n$  voor  $n \in \mathbb{N}$  door  $X_1 = X$  en  $Y_1 = Y$  en

$$X_n := f(X_{n-1}) \quad Y_n := f(Y_{n-1}) \quad \text{voor } n \geq 2.$$

Laat zien dat geldt

$$Y_1 \supset X_1 \supset Y_2 \supset X_2 \supset \dots$$

Definiëer  $g : Y \rightarrow X$  via

$$g(y) := \begin{cases} f(y) & \text{als } y \in Y_n - X_n \text{ voor een } n; \\ y & \text{anders.} \end{cases}$$

Laat zien dat  $g$  een bijectie tussen  $X$  en  $Y$  geeft. Formuleer het resultaat als een stelling.

## Literatuur

Het is niet eenvoudig goede boeken te vinden die weinig bekend veronderstellen. Sommige vakken lenen zich daar ook beter voor dan andere. Elementaire getaltheorie leent zich er zeker toe. Een klassiek boek voor beginners is:

G.H. Hardy, E.M. Wright: An introduction to the theory of numbers. Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979. xvi+426 pp.

Voor beginners is ook het volgende boek:

F. Beukers: Getaltheorie voor beginners. Epsilon Uitgaven, Utrecht 1999.

Het volgende boek veronderstelt meer, maar bevat voor een beginner toch veel aantrekkelijks.

H.D. Ebbinghaus et al.: Numbers. (Vertaling van de Duitse versie: Zahlen.) Graduate Texts in Mathematics, 123. Readings in Mathematics. Springer-Verlag, New York, 1991.

Verder verwijzen we nogmaals naar het artikel van Zagier. Naast de al genoemde referentie is het ook te vinden in het boekje *Lebendige Zahlen*:

D. Zagier: Die ersten 50 Millionen Primzahlen. (German) [The first 50 000 000 prime numbers] Living numbers, pp. 39–73, Math. Miniaturen, 1, Birkhäuser, Basel-Boston, Mass., 1981.

Een meetkundeboek dat redelijk elementair begint en wellicht een verrassend onderwerp (knopen) behandelt is

Colin C. Adams: The knot book. An elementary introduction to the mathematical theory of knots. W. H. Freeman and Company, New York, 1994. xiv+306 pp.

Een aantrekkelijk boek voor beginners in de algebra is:

Igor R. Shafarevich: Discourses on algebra. Translated from the Russian by William B. Everett. Universitext. Springer-Verlag, Berlin, 2003. x+276 pp.

Een interessant boek, geschikt voor beginners, behandelt Koderingstheorie:

Thomas M. Thompson: From error-correcting codes through sphere packings to simple groups. Carus Mathematical Monographs, 21. Mathematical Association of America, Washington, DC, 1983. xiv+228 pp.

Bij de andere colleges worden ongetwijfeld ook suggesties gedaan voor verdere literatuur. Zo niet vraag er dan naar en maak er gebruik van. Veel plezier bij de ontdekkingstocht!

KORTEWEG-DE VRIES INSTITUUT, UNIVERSITEIT VAN AMSTERDAM, POSTBUS 94248, 1090 GE  
AMSTERDAM, THE NETHERLANDS  
*E-mail address:* `geer@science.uva.nl`