Vakantiecursus 2008

# Wiskunde en profil

## Het gezicht van de wiskunde

22 en 23 augustus in Eindhoven
29 en 30 augustus in Amsterdam

Centrum Wiskunde & Informatica

CWI SYLLABUS 58

De Vakantiecursus Wiskunde voor leraren in de exacte vakken in VWO, HAVO en HBO en andere belangstellenden is een initiatief van de Nederlandse Vereniging van Wiskundeleraren. De cursus wordt sinds 1946 jaarlijks gegeven op het Centrum Wiskunde & Informatica en aan de Technische Universiteit Eindhoven.

Deze cursus is mede mogelijk gemaakt door een subsidie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek.

Omslag: Tobias Baanders

ISBN veranderen ISBN 90 6196 548 9
NUGI-code: 811


Printed by Grafisch bedrijf Ponsen & Looijen bv, Wageningen.

# Inhoud

# Docenten

Prof.dr. J.M. Aarts
Technische Universiteit Delft, Faculteit EWI
Postbus 5031, 2600 GA Delft, tel. 015-2126448
Van Kinschotstraat 13, 2614 XJ Delft
johannesaarts@gmail.com

Prof.dr. J.H. Geuvers
Mathematisch Instituut, Radboud Universiteit
Postbus 9010, 6500 GL Nijmegen
herman@cs.ru.nl

Dr. P.D. Grünwald
Centrum Wiskunde & Informatica, Quantum Computing and Advanced Systems Research
Postbus 94079, 1090 GB Amsterdam, tel. 020-5924115
Peter.Grunwald@cwi.nl

Drs. A.J. Goddijn
Freudenthal Institute for science and mathematics education, Universiteit Utrecht
tel. 030-26335542, A.Goddijn@fi.uu.nl

Prof.dr. E. Postma
Postbus 616, 6200 MD Maastricht
postma@micc.unimaas.nl

Dr. M.D.G. Swaen
Hogeschool van Amsterdam
Postbus 1025, 1000 BA Amsterdam
mdgswaen@xs4all.nl

Dr. L. Taelman
Mathematisch Instituut, Universiteit Leiden
Postbus 9512, 2300 RA Leiden
lenny.taelman@gmail.com

Prof.dr.ir. C. Vuik
Delft Institute of Applied Mathematics
Mekelweg 4, 2628 CD Delft
c.vuik@tudelft.nl

Dr. F. Wiedijk
Mathematisch Instituut, Radboud Universiteit
Postbus 9010, 6500 GL Nijmegen
freek@cs.ru.nl

Drs. B. Zevenhek
Mathematisch Instituut, Universiteit Leiden
Postbus 9512, 2300 RA Leiden
bartzevenhek@gmail.com

## Contacten Centrum Wiskunde & Informatica

Mevrouw W. van Ojik
Centrum Wiskunde & Informatica, Kruislaan 413, Postbus 94079,
1090 GB Amsterdam, 020 - 592 4009, Wilmy.van.Ojik@cwi.nl

# Ten geleide

Jan Aarts
Technische Universiteit Delft
johannesaart@gmail.com

*Wiskunde anders*: zo zou ik de vakantiecursus 2008 kort willen kenschetsen. Werd in de afgelopen jaren een specifiek onderdeel van de wiskunde of een toepassingsgebied belicht, in de komende cursus proberen we eens op een heel andere manier naar de wiskunde te kijken: niet en face maar en profil, met meer aandacht voor de contouren van de wiskunde. Vandaar de titel:

## Wiskunde en profil
## Het gezicht van de wiskunde

In een interessante mix van voordrachten wordt een beeld geschetst van het profiel van de wiskunde. De enthousiaste wiskunde docent zal vele ideeën kunnen opdoen voor mogelijke (profiel) werkstukken. Waarover gaan de voordrachten?

De wiskunde is heden ten dage heel anders dan vroeger; door de computer kunnen we sneller rekenen en beter boekhouden (ook binnen de wiskunde). Fraaie voorbeelden hiervan vindt men in de numerieke wiskunde. Hoe oplossingen van niet-lineaire vergelijkingen numeriek benaderd kunnen worden met behulp van discretisatie wordt door **prof.dr.ir. C. Vuik** uitgelegd in de lezing *Iteratieve Methoden voor niet-lineaire Vergelijkingen*.

Ook voor de moderne geavanceerde coderingstechnieken zijn computers onontbeerlijk. **Dr. L. Taelman** zal in de voordracht *RSA* een uiteenzetting geven van het geheimschrift *RSA*.

Echt of vals in de kunst is een boeiend thema. **Prof.dr. E. Postma** laat in de voordracht *De Zaak Zonnebloemen* zien hoe modern authenticiteitsonderzoek plaatsvindt.

**Drs. B. Zevenhek** werkt in het kader van het NWO-programma Leraar in Onderzoek aan de rij van Fibonacci. In de lezing *Fibonacci aan de uni-*

*versiteit* behandelt hij onder andere deelbaarheidseigenschappen van de rij van Fibonacci.

In de schone letteren van rond 1800 duikt soms plotseling de wiskunde of de natuurwetenschap op. Het beeld dat gegeven wordt is bepaald niet onverdeeld positief. **Drs. A. Goddijn** zal dit thema behandelen in de lezing *De verbeelding verhongert.*

De beroemdste Nederlandse wiskundige, L.E.J. Brouwer, had heel oorspronkelijke ideeën over de beoefening van de wiskunde. **Dr. M.D.G. Swaen** zal daarover iets onthullen in de lezing *Brouwers ware wiskunde.*

Bewijzen spelen een grote rol in de wiskunde. Vroeger moesten ook leerlingen 'alles' kunnen bewijzen. Net zoals de computer ons kan helpen bij het maken van berekeningen, zo kan de computer ons ook helpen bij het uitvoeren van bewijzen; daarover zal **dr. F. Wiedijk** ons vertellen in *De Kunst van het bewijzen.*

Maar is een wiskundig bewijs ook geldig buiten de wiskunde? Precieser, zegt een bewijs ook iets over gebeurtenissen in het dagelijks leven? De vraag is in het bijzonder relevant bij toepassingen van de statistiek en waarschijnlijkheidsrekening. Een originele visie op dit probleem wordt gegeven door **dr. P. Grünwald** in de (actuele) voordracht *Kansloos: van Willem Ruis tot Lucia de B.*

# Niet-lineaire vergelijkingen

Prof.dr.ir. C. Vuik
Delft Institute of Applied Mathematics

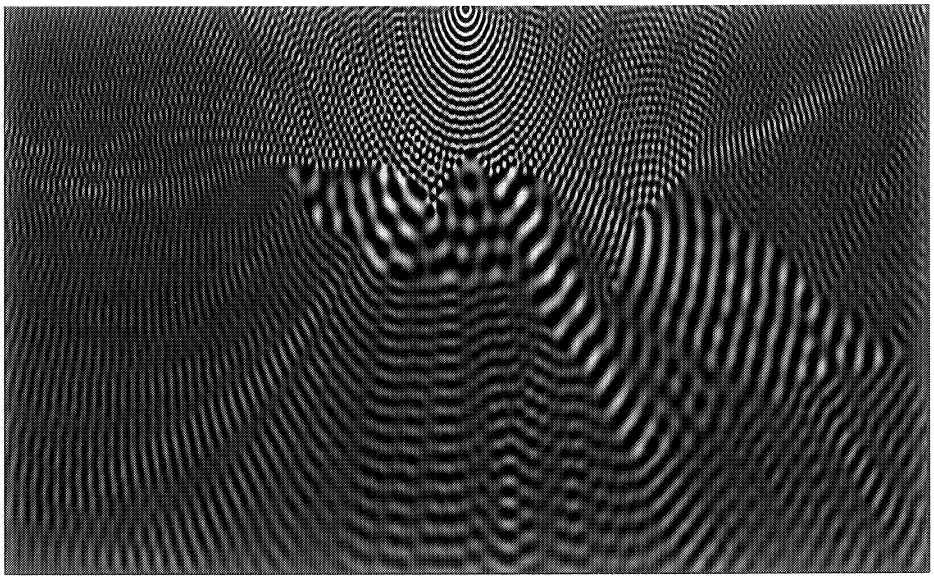
## 1 Inleiding

Bij het modelleren van praktische toepassingen worden vaak partiële differentiaalvergelijkingen gebruikt. Soms zijn dit lineaire vergelijkingen maar meestal levert dit een stelsel niet-lineaire partiële differentiaalvergelijkingen op. Deze niet-lineaire stelsels zijn vaak niet exact op te lossen. De oplossing wordt dan benaderd door een discretisatie van het gegeven stelsel. Dit leidt tot een zeer groot stelsel gewone niet-lineaire vergelijkingen.

In dit hoofdstuk starten we met één niet-lineaire vergelijking. Het is wel bekend dat slechts voor een zeer beperkte klasse van vergelijkingen de oplossing exact bepaald kan worden. Voor andere vergelijkingen kan de oplossing alleen benaderd worden met behulp van een iteratieve methode. Kennis over het bestaan van een oplossing, het aantal oplossingen en de globale ligging van de oplossingen is van groot belang voor het ontwikkelen en gebruiken van succesvolle iteratieve methoden.

Voor dat een iteratieve methode gebruikt kan worden moet er een startoplossing gegeven worden. Deze oplossing wordt ingevuld in de vergelijking. Als dit een exacte oplossing is, dan stopt de methode. Anders wordt er een algoritme (recept) gebruikt om een betere benadering te vinden. Dit proces wordt herhaald net zo lang totdat de vergelijking "min of meer"geldig is.

We zullen starten met de bisectie methode en de Picard methode. Daarna gaan we over op de Newton-Raphson methode. Het zal



Figuur 1: De oplossing van een seismisch probleem die berekend is met een nieuwe in Delft ontwikkelde iteratieve methode

blijken dat de methode lokaal zeer snel convergeert echter globaal kan de methode divergent zijn. Als laatste zal de methode uitgeschreven worden voor een stelsel niet-lineaire vergelijkingen. Dit betekent dat er per iteratie een groot stelsel lineaire vergelijkingen opgelost moet worden. Dit kan gedaan worden met Gauss eliminatie (vegen) of opnieuw met een iteratieve methode.

# 2 Een toepassing

Als voorbeeld nemen we de drukval in een stromende vloeistof. Bij lage stroomsnelheden is de stroming laminair terwijl bij hoge snelheden de stroming turbulent genoemd wordt. Het Reynoldsgetal kan gebruikt worden om te zien of een stroming turbulent is. Voor een stroming in een ronde pijp met diameter $D(m)$ wordt het Rey-

noldsgetal gegeven door

$$Re = \frac{Dv}{\nu} ,$$

waarbij $v$ $(m/s)$ de gemiddelde vloeistofsnelheid is en $\nu$ $(m^2/s)$ de viscositeit is van de vloeistof. Als het Reynoldsgetal kleiner is dan 2100 dan is de stroming laminair, terwijl als $Re \geq 3000$ dan is er een turbulente stroming.

Voor een turbulente stroming wordt het drukverschil tussen de uit- en inlaat gegeven door

$$P_{\text{uit}} - P_{\text{in}} = \frac{\rho w L v^2}{2gD} ,$$

hierbij is $w$ de wrijvingsfactor, $\rho$ $(kg/m^3)$ is de soortelijke dichtheid, $L$ $(m)$ is de lengte en $g$ $(m/s^2)$ is de valversnelling. Als de vloeistof deeltjes bevat (zand, papiervezels) dan voldoet de wrijvingsfaktor $w$ aan de vergelijking:

$$\frac{1}{\sqrt{w}} = \frac{\ln(Re\sqrt{w}) + 14 - \frac{5.6}{k}}{k} ,$$

waarbij $k$ een parameter is, die bekend is uit experimenten.

In dit hoofdstuk zullen methoden behandeld worden om $w$ te bepalen uit deze vergelijking, als de waarden van $Re$ en $k$ gegeven zijn.

# 3 Een eenvoudige nulpuntsmethode

### Bisectie

De eerste methode, de Bisectie-methode, is gebaseerd op de tussenwaarde stelling ??. Stel $f$ is een continue functie gedefinieerd op een interval $[a, b]$ waarbij $f(a)$ en $f(b)$ een tegengesteld teken hebben. Volgens de tussenwaarde stelling bestaat er een getal $p$ in $(a, b)$ waar $f(p) = 0$. We nemen aan dat er slechts één zo'n $p$ is. In de methode wordt het interval steeds gehalveerd waarbij in elke

stap het interval gekozen wordt waar $p$ in ligt.

We starten de methode met $a_1 = a$ en $b_1 = b$ en nemen voor $p_1$ het gemiddelde van $a_1$ en $b_1$:

$$p_1 = \frac{1}{2}(a_1 + b_1) \ .$$

Als $f(p_1) = 0$ dan zijn we klaar, anders heeft $f(p_1)$ hetzelfde teken als $f(a_1)$ of $f(b_1)$. Als $f(p_1)f(a_1) > 0$ dan nemen we $a_2 = p_1$ en $b_2 = b_1$ anders $a_2 = a_1$ en $b_2 = p_1$. Daarna herhalen we de procedure met het interval $[a_2, b_2]$.

**Stopcriterium**
De Bisectie methode is een iteratieve methode. Dat betekent dat een gebruiker op moet geven wanneer de methode moet stoppen. De volgende stopcriteria kunnen gebruikt worden

$$\frac{|p_n - p_{n-1}|}{|p_n|} \leq \varepsilon \ , \text{ als } p \neq 0,$$

of

$$|f(p_n)| < \varepsilon \ .$$

**Convergentie**
De Bisectie-methode kan traag convergeren. Het kan ook gebeuren dat $|p_{i-1} - p| \ll |p_i - p|$. Een groot voordeel is dat de methode altijd convergeert naar een oplossing. De Bisectie-methode wordt vaak gebruikt om een goede startoplossing te genereren voor efficiëntere methoden, die later in dit hoofdstuk behandeld zullen worden.

**Stelling 3.1** *Stel $f \in C[a, b]$ en $f(a) \cdot f(b) < 0$, dan genereert de Bisectie-methode een rij $\{p_n\}$ die convergeert naar een nulpunt $p$ van $f$ waarbij*

$$|p_n - p| \leq \frac{b - a}{2^n} \ , \quad n \geq 1 \ .$$

**Bewijs:**
Voor elke $n \geq 1$ hebben we $b_n - a_n = \frac{1}{2^{n-1}}(b - a)$ en $p \in (a_n, b_n)$. Omdat $p_n = \frac{1}{2}(a_n + b_n)$ volgt

$$|p_n - p| \leq \frac{1}{2}(b_n - a_n) = \frac{b - a}{2^n} \ .$$

$\boxtimes$

**Afrondfouten**
Als van een functie $f$ de berekende waarden $\hat{f}$ een afrondfout $\bar{\varepsilon}$ hebben dan kan men niet het echte nulpunt $p$ bepalen, immers elk punt van de verzameling

$$I = \{x \in [a, b] \mid |f(x)| < \bar{\varepsilon}\}$$

zou het (of een) nulpunt van $f$ kunnen zijn. Een dergelijk interval noemt men een onbetrouwbaarheidsinterval. Het heeft bijvoorbeeld geen zin om als stopcriterium

$$|f(p_n)| < \varepsilon$$

te nemen als $\varepsilon < \bar{\varepsilon}$ gekozen is. Er is dan een grote kans dat het algoritme dan altijd blijft itereren. Met behulp van linearisatie blijkt dat als $p$ een enkelvoudig nulpunt is van $f$ en $f'(p) \neq 0$ dan is $I$ ongeveer gelijk aan

$$I \approx [p - \frac{\bar{\varepsilon}}{|f'(p)|},\ p + \frac{\bar{\varepsilon}}{|f'(p)|}] \ .$$

Merk op dat als $|f'(p)|$ dicht bij 0 ligt, het bepalen van $p$ een slecht gesteld probleem is.

# 4 Vaste punt iteratie

Een vast punt van een gegeven functie $g$ is een getal $p$ zodanig dat $g(p) = p$. In deze paragraaf beschouwen we het vinden van oplossing voor een vast punt probleem en het verband tussen deze problemen en het vinden van nulpunten.

Het vinden van een nulpunt en vast punt problemen zijn als volgt gerelateerd: als we het nulpunt $p$ zoeken zodat $f(p) = 0$, dan kunnen we een niet unieke functie $g$ definiëren als $g(x) = x - f(x)$ of $g(x) = x + \sqrt{f(x)}$. Aan de andere kant als $g$ een vast punt heeft in $p$, dan heeft de functie gedefinieerd door $f(x) = x - g(x)$ een nulpunt in $p$.

In de volgende stelling geven we voldoende voorwaarden voor de existentie en eenduidigheid van een vast punt.

**Stelling 4.1** *1. Als $g \in C[a,b]$ en $g(x) \in [a,b]$ voor alle $x \in [a,b]$ dan heeft $g$ een vast punt in $[a,b]$.*

*2. Als bovendien $g'(x)$ bestaat voor $x \in [a,b]$ en er is een positieve constante $k < 1$ zodanig dat*

$$|g'(x)| \leq k \quad \textit{voor alle} \quad x \in [a,b] \ ,$$

*dan is het vaste punt in $[a,b]$ uniek.*

**Bewijs:**

1. Als $g(a) = a$ of $g(b) = b$ dan heeft $g$ een vast punt in een eindpunt. Anders geldt $g(a) > a$ en $g(b) < b$. De functie $h(x) = g(x) - x$ is continu op $[a,b]$ en $h(a) > 0$ en $h(b) < 0$. Uit de tussenwaarde stelling ?? volgt er is een $p$ zodat $h(p) = 0$, dus $p$ is een vast punt van $g$.

2. Stel $|g'(x)| \leq k < 1$ en er zijn twee vaste punten $p$ en $q$ waarbij $p < q$. Uit de middelwaardestelling volgt er is een $\xi \in [p,q]$ zodat
$$\frac{g(p) - g(q)}{p - q} = g'(\xi) \ .$$
Dan volgt
$$|p - q| = |g(p) - g(q)| = |g'(\xi)||p - q| < |p - q| \ ,$$
dit is een tegenspraak, dus $p = q$ en het vaste punt is uniek. ⊠

**Opmerkingen**

- Bovenstaande stelling wordt op veel plaatsen gebruikt en is bekend onder de volgende namen: Vaste-punt stelling (van Banach), Dekpunt stelling (van Brouwer) en Contractie-stelling.

- De convergentiefactor wordt gegeven door $|g'(p)|$. Als $|g'(p)|$ klein is, dan is er snelle convergentie, als $|g'(p)| \geq 1$ dan is er geen convergentie en als $|g'(p)|$ iets kleiner dan 1 is, dan is er trage convergentie.

Om een vast punt van een functie $g$ te benaderen, kiezen we een startwaarde $p_0$ en bepalen $p_n$ door middel van $p_n = g(p_{n-1})$ voor $n \geq 1$. Als de rij convergeert naar $p$ en $g$ is een continue functie dan geldt

$$p = \lim_{n\to\infty} p_n = \lim_{n\to\infty} g(p_{n-1}) = g(\lim_{n\to\infty} p_{n-1}) = g(p) \ ,$$

zodat $p$ een vast punt is van $g$. Dit noemen we de vaste-punt (of Picard-) iteratie.

**Voorbeeld 4.1**

Voor het bepalen van het nulpunt van de functie $f(x) = x^3+3x-4$, gebruiken we de hulpfunctie:

$$g(x) = \frac{4}{x^2+3}$$

in onze vaste punt methode. Deze functie is bepaald via de volgende stappen:

$$f(x) = 0, \quad x^3 + 3x - 4 = 0$$

$$x^3 + 3x = 4 \rightarrow x(x^2+3) = 4 \rightarrow x = \frac{4}{x^2+3}$$

In Figuur 2 staat het iteratieproces getekend, waarbij gestart is met $x_0 = 0$.

Convergentie van de methode volgt uit de Vaste Punt Stelling.

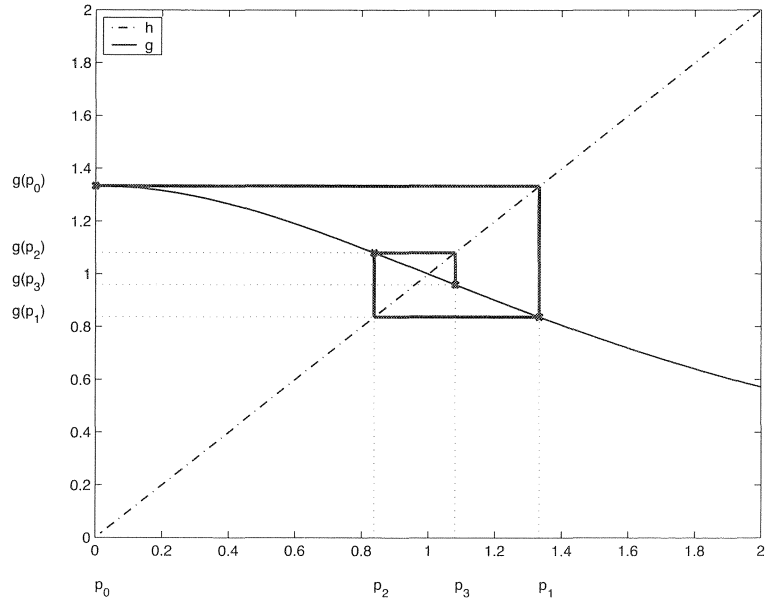
**Stelling 4.2** *Stel $g \in C[a,b]$, $g(x) \in [a,b]$, als $x \in [a,b]$ en $|g'(x)| \leq k < 1$ voor $x \in [a,b]$. Dan geldt dat de vaste punt iteratie convergeert naar $p$ voor elke waarde $p_0 \in [a,b]$.*

**Bewijs:**
Onder de gegeven voorwaarden heeft $g$ een uniek vast punt $p$. Uit de middelwaardestelling volgt:

$$|p_n - p| = |g(p_{n-1}) - g(p)| = |g'(\xi)||p_{n-1} - p| \leq k|p_{n-1} - p| \ .$$

Met inductie volgt

$$\lim_{n\to\infty} |p_n - p| \leq \lim_{n\to\infty} k^n |p_0 - p| = 0 \ ,$$




Figuur 2: Grafische voorstelling van de vaste punt methode.

dus $p_n$ convergeert naar $p$. ⊠

De bovenstaande stelling kan ook gebruik worden om een goed stopcriterium te geven.
Merk op dat voor $m > n \geq 1$ geldt

$$\begin{aligned} |p_m - p_n| &= |p_m - p_{m-1} + p_{m-1} + ... + p_{n+1} - p_n| \\ &\leq |p_m - p_{m-1}| + |p_{m-1} - p_{m-2}| + ... + |p_{n+1} - p_n| \\ &\leq k^{m-n}|p_n - p_{n-1}| + ... + k|p_n - p_{n-1}| \\ &= (k + ... + k^{m-n})|p_n - p_{n-1}| \ . \end{aligned}$$

Omdat $\lim_{m\to\infty} p_m = p$ geldt

$$|p - p_n| = \lim_{m\to\infty} |p_m - p_n| \leq k \sum_{i=0}^{\infty} k^i |p_n - p_{n-1}| = \frac{k}{1-k}|p_n - p_{n-1}| \ .$$

Dit betekend dat als we stoppen wanneer

$$|p_n - p_{n-1}| \leq \frac{1-k}{k}\varepsilon \ ,$$

dan geldt $|p - p_n| \leq \varepsilon$.

# 5 De Newton-Raphson methode

De Newton-Raphson methode is één van de krachtigste en bekendste numerieke methoden voor het oplossen van een niet-lineaire vergelijking $f(x) = 0$. We zullen de methode uitleggen aan de hand van een Taylorpolynoom.

Veronderstel $f \in C^2[a, b]$. Laat $\bar{x} \in [a, b]$ een benadering zijn van de oplossing $p$ zodanig dat $f'(\bar{x}) \neq 0$ en veronderstel dat $|\bar{x} - p|$ klein is. Beschouw het eerste graads Taylorpolynoom:

$$f(x) = f(\bar{x}) + (x - \bar{x})f'(\bar{x}) + \frac{(x - \bar{x})^2}{2} f''(\xi(x)) \ ,$$

waarbij $\xi(x) \in (x, \bar{x})$. Omdat $f(p) = 0$ geldt

$$0 = f(\bar{x}) + (p - \bar{x})f'(\bar{x}) + \frac{(p - \bar{x})^2}{2} f''(\xi(x)) \ .$$

Omdat we aangenomen hebben dat $|p - \bar{x}|$ klein is geldt:

$$0 \approx f(\bar{x}) + (p - \bar{x})f'(\bar{x}) \ .$$

Als we hieruit $p$ oplossen krijgen we

$$p \approx \bar{x} - \frac{f(\bar{x})}{f'(\bar{x})} \ .$$

Dit motiveert de Newton-Raphson methode, die start met een beginbenadering $p_0$ en een rij $\{p_n\}$ genereert volgens

$$p_n = p_{n-1} - \frac{f(p_{n-1})}{f'(p_{n-1})} \ , \quad \text{voor} \quad n \geq 1 \ .$$

**Voorbeeld 5.1**

Stel we willen het positieve nulpunt bepalen van de functie $f(x) = x^2 - 2$. Het exacte antwoord is $p = \sqrt{2} = 1.41421$. We nemen als startpunt $p_0 = 1$. De vergelijking van de raaklijn is nu

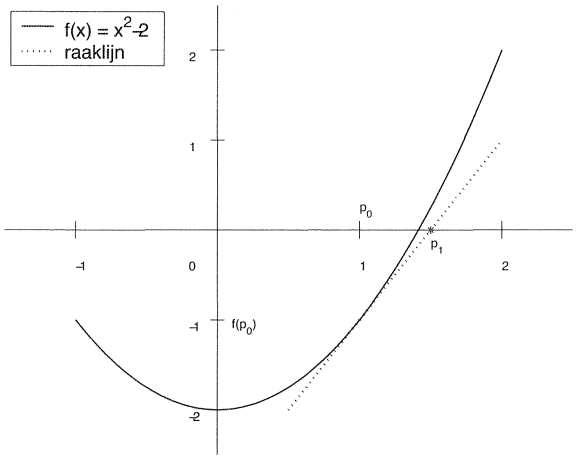
$$h(x) = -1 + 2(x - 1).$$

De nieuwe benadering van het nulpunt $p_1$ is nu:

$$p_1 = 1 - \frac{-1}{2} = 1.5.$$

Zo doorgaande vinden we:
$p_1 = 1.50000$
$p_2 = 1.41666$
$p_3 = 1.41421$

Hieruit blijkt dat de oplossing al na 3 stappen gevonden is. De procedure voor de eerste iteratie staat uitgelegd in Figuur 3.




Figuur 3: De Newton-Raphson methode.

We kunnen dezelfde stopcriteria gebruiken als bij de bisectie methode:

$$\frac{|p_n - p_{n-1}|}{|p_n|} < \varepsilon \quad \text{of} \quad |f(p_n)| < \varepsilon \,.$$

In de stelling hierna geven we het verband tussen de Newton-Raphson iteratie en een vaste-punt methode.

**Stelling 5.1** *Laat $f \in C^2[a,b]$. Als $p \in [a,b]$ zodat $f(p) = 0$ en $f'(p) \neq 0$ dan is er een $\delta > 0$ zodanig dat Newton's methode een rij $\{p_n\}$ genereert, die naar $p$ convergeert voor elke $p_0 \in [p-\delta,\ p+\delta]$.*

**Bewijs:**
Beschouw Newton's methode als de vaste punt iteratie $p_n = g(p_{n-1})$ met

$$g(x) = x - \frac{f(x)}{f'(x)} .$$

We proberen eerst een interval $[p-\delta,\ p+\delta]$ te vinden zodat $|g'(x)| \leq k < 1$ voor $(p-\delta,\ p+\delta)$.
Omdat $f'(p) \neq 0$ en $f'$ continu is bestaat er een $\delta_1 > 0$ zodat $f'(x) \neq 0$ voor $x \in [p-\delta_1,\ p+\delta_1]$. Dus $g$ is gedefinieerd en continu op $[p-\delta_1,\ p+\delta_1]$. Bovendien geldt

$$g'(x) = 1 - \frac{(f'(x))^2 - f(x)f''(x)}{(f'(x))^2} = \frac{f(x)f''(x)}{(f'(x))^2} .$$

Omdat $f \in C^2[a,b]$ is $g(x) \in C^1[p-\delta_1,\ p+\delta_1]$. Merk op dat $g'(p) = 0$ omdat $f(p) = 0$. Daar $g'$ continu is, bestaat er een $\delta < \delta_1$ zodat

$$|g'(x)| \leq k < 1 \quad \text{voor alle} \quad x \in [p-\delta,\ p+\delta] .$$

Als laatste moeten we laten zien dat $g : [p-\delta,\ p+\delta] \to [p-\delta,\ p+\delta]$. Uit de middelwaardestelling volgt

$$|g(x) - g(p)| = |g'(\xi)||x-p| \quad \text{voor } \xi \text{ tussen } x \text{ en } p .$$

Omdat $x \in [p-\delta,\ p+\delta]$ geldt $|x-p| < \delta$ en dus

$$|g(x) - g(p)| = |g(x) - p| < |x-p| < \delta .$$

Hiermee is de stelling bewezen. ⊠

Om een goede vergelijking van convergentie mogelijk te maken voeren we de volgende definitie in.

**Definitie**
Stel $\{p_n\}_{n=0}^{\infty}$ is een rij die convergeert naar $p$, met $p_n \neq p$ voor alle $n$.

Als er positieve constantes $\lambda$ en $\alpha$ bestaan met

$$\lim_{n\to\infty} \frac{|p_{n+1} - p|}{|p_n - p|^{\alpha}} = \lambda , \tag{1}$$

dan convergeert $\{p_n\}$ naar $p$ met orde $\alpha$ en asymptotische constante $\lambda$.

In het algemeen convergeert een hogere orde methode sneller dan een lagere orde methode. De waarde van de asymptotische constante is minder belangrijk. Twee gevallen zijn belangrijk

- als $\alpha = 1$ dan noemen we het proces lineair convergent,
- als $\alpha = 2$ dan noemen we het proces kwadratisch convergent.

Het is eenvoudig om in te zien dat elke convergerende vaste-punt methode tenminste lineair convergent is.

Voor Newton-Raphson merken we op

$$0 = f(p) = f(p_n) + (p - p_n)f'(p_n) + \frac{(p - p_n)^2}{2} f''(\xi_n) \ , \xi_n \in (p_n, p) \ .$$

Volgens de definitie geldt

$$0 = f(p_n) + (p_{n+1} - p_n)f'(p_n) \ .$$

Aftrekken geeft

$$p_{n+1} - p = (p_n - p)^2 \frac{f''(\xi)}{2f'(p_n)} \ .$$

Dit is inderdaad van de gedaante (1) met $\alpha = 2$ en $\lambda = \left| \frac{f''(p)}{2f'(p)} \right|$, zodat Newton-Raphson kwadratisch convergent is.

Er zijn allerlei varianten op de Newton-Raphson methode bekend. We zullen deze alleen noemen.

**Secant methode** (Koorden-Newton)
Vervang $f'(p_{n-1})$ door $\frac{f(p_{n-1}) - f(p_{n-2})}{p_{n-1} - p_{n-2}}$. Voordeel hiervan is dat $f'$ niet bepaald behoeft te worden.
**Regula Falsi methode**
Stel er zijn twee benaderingen gegeven $p_0$ en $p_1$ zodanig dat $f(p_0) \cdot f(p_1) < 0$. Het schema om $p$ te benaderen is nu:

stap 1 $q_0 = f(p_0)$
$q_1 = f(p_1)$
$n = 2$
stap 2 doe zolang $n \leq N_0$
stap 3 $p = p_1 - q_1(p_1 - p_0)/(q_1 - q_0)$
$q = f(p)$
$n = n + 1$
stap 4 als $q \cdot q_1 < 0$ dan $p_0 = p$; $q_0 = q$
anders $p_1 = p$ $q_1 = q$

# 6 Stelsels niet-lineaire vergelijkingen

Een stelsel van niet-lineaire vergelijkingen heeft de vorm

$$\begin{aligned} f_1(x_1, ..., x_n) &= 0 , \\ &\vdots \\ f_n(x_1, ..., x_n) &= 0 . \end{aligned}$$

We noteren dit ook als

$$\boldsymbol{F}(\boldsymbol{x}) = \boldsymbol{0} . \tag{2}$$

De Newton-Raphson methode voor (2) wordt gegeven door

$$\boldsymbol{x}^{(p)} = \boldsymbol{x}^{(p-1)} - J(\boldsymbol{x}^{(p-1)})^{-1} F(\boldsymbol{x}^{(p-1)}) .$$

Hierbij wordt $J(\boldsymbol{x})$ de Jacobiaan matrix genoemd, die gedefinieerd is als:

$$J(\boldsymbol{x}) = \begin{pmatrix} \frac{\partial f_1(\boldsymbol{x})}{\partial x_1} & \cdots & \frac{\partial f_1(\boldsymbol{x})}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_n(\boldsymbol{x})}{\partial x_1} & \cdots & \frac{\partial f_n(\boldsymbol{x})}{\partial x_n} \end{pmatrix} .$$

Als het exact uitrekenen van $\frac{\partial f_j}{\partial x_k}(\boldsymbol{x})$ onmogelijk is, dan kunnen we de partiële afgeleiden vervangen door eindige differentiebenaderingen. Bijvoorbeeld

$$\frac{\partial f_j}{\partial x_k}(\boldsymbol{x}) \approx \frac{f_j(\boldsymbol{x} + \boldsymbol{e}_k h) - f_j(\boldsymbol{x})}{h} ,$$

waarbij $\boldsymbol{e}_k$ de $k^e$ eenheidsvector is. Dit noemen we een quasi-Newton methode.

# 7 Samenvatting

In dit hoofdstuk zijn de volgende begrippen behandeld:

- Bisectie-methode
- stopcriteria
- convergentie
- vaste punt iteratie (Picard)
- Newton-Raphson
- Secant-methode, Regula Falsi methode
- stelsels niet-lineaire vergelijkingen

# 8 Opgaven

1. Stel $f(x) = 3(x+1)(x-\frac{1}{2})(x-1)$. Gebruik de Bisectie methode op de volgende intervallen om $p_3$ te bepalen: [-2 1.5] en [-1.25 2.5].

2. We beschouwen de vaste punt methoden: $p_n = \frac{20p_{n-1}+21/p_{n-1}^2}{21}$ en $p_n = p_{n-1} - \frac{p_{n-1}^3-21}{3p_{n-1}^2}$. Beantwoord voor beide methoden de volgende vragen. Laat zien dat het vaste punt $(21)^{\frac{1}{3}}$ is. Geef een schatting van de convergentie snelheid. Bepaal $p_3$ met $p_0 = 1$.

3. We gaan een methode afleiden voor het bepalen van een nulpunt van $f$ gebaseerd op interpolatie.

   (a) Stel er zijn twee startwaarden gegeven $p_0$ en $p_1$. Bepaal het lineaire interpolatiepolynoom van de functie $f$.

   (b) Neem voor $p_2$ het punt waar het interpolatiepolynoom de x-as snijdt. We kunnen dit herhalen met $p_1$ en $p_2$ om $p_3$ te bepalen etc. Deze methode staat bekend als de Koorden Newton methode.

   (c) Doe 2 iteraties met de deze methode voor de functie $f(x) = x^2 - 2$ met $p_0 = 1$ en $p_1 = 2$.

4. Gegeven de functie $f(x) = x - \cos x, x \in [0, \frac{\pi}{2}]$. Bepaal met behulp van de Newton-Raphson methode een benadering van het nulpunt met een fout kleiner dan $10^{-4}$.

5. Doe twee iteraties met de Newton-Raphson methode met startvector $(1, 1)$ om het volgende niet-lineaire stelsel op te lossen: $x_1^2 - x_2 - 3 = 0$ en $-x_1 + x_2^2 + 1 = 0$ . Vergelijk de benadering met de exacte oplossing $(2, 1)$.

# De verbeelding verhongert

## *Vroeg romantische dichters over wiskunde*[1]

**Aad Goddijn (FIsme)**

*In de schone letteren van rond 1800 duikt soms plotseling de wiskunde of de natuurwetenschap op. Het beeld dat gegeven wordt is bepaald niet onverdeeld positief. De kenmerken ervan horen bij het verzet tegen de Verlichting dat bij sommige strijdbare Romantici behoorlijk sterk was.*
*De 'argumenten' zijn nú - begin 21e eeuw - ook nog hoorbaar. Terecht?*

***De steen en de schelp***

'The Prelude' is de autobiografie in verzen van William Wordsworth (1770-1850). De eerste vier delen vertellen vooral hoe zijn band met de eeuwige 'Nature' langzaam aan mystiek en onverbreekbaar wordt. Deel vijf heeft de ondertitel 'Books' en spreekt over de schitterende maar vergankelijke werken van de mens:

> Thou also, man! hast wrought,
> For commerce of thy nature with herself,
> Things that aspire to unconquerable life;
> And yet we feel–we cannot choose but feel–
> That they must perish[2]

Kort hierna vertelt Wordsworth wat Borges later 'de vervolmaking van de nachtmerrie' heeft genoemd[3]. De dichter ligt in een grot aan zee, naast hem het boek waarin hij heeft gelezen. Mijmerend over:

> poetry and geometric truth,
> And their high privilege of lasting life.

---

[1] Een kortere versie van dit artikel verscheen in Euclides, jrg. 79, 4 (2004) onder de titel *Het romantisch ongenoegen met de rede.* Deze versie werd geschreven voorjaar 2003, al lijkt het staartje toegevoegd als onderdeel van de discussies van 2007 en 2008 over wiskundeonderwijs. Dat is echter niet zo; de tekst is nauwelijks aangepast, slechts enkele toevoegingen zijn van juni 2008.

[2] William Wordsworth: The Prelude. Fragmenten uit het begin van boek V. Versie van 1850. In deze versie is de dromer Wordsworth zelf; in de versie uit 1805 is het een vriend.

[3] Jorge Luis Borges: Zeven Avonden. Tweede avond: De Nachtmerrie. Bezige Bij, 1984.

De droom die hem dan overrompelt, laat een Arabier zien op een kameel. Onder de ene arm houdt deze een steen, onder de andere een schelp. De dromer hoopt een gids in de woestijn te hebben gevonden, maar het is anders:

> the Arab told me that the stone
> (To give it in the language of the dream)
> Was "Euclid's Elements," and "This," said he,
> "Is something of more worth;" and at the word
> Stretched forth the shell, so beautiful in shape,
> In colour so resplendent, with command
>
> That I should hold it to my ear. I did so,
> And heard that instant in an unknown tongue,
> Which yet I understood, articulate sounds,
> A loud prophetic blast of harmony;
> An Ode, in passion uttered, which foretold
> Destruction to the children of the earth
> By deluge, now at hand.

Steen en schelp blijken de twee boeken te zijn die als enige bewaard moeten blijven na de op handen zijnde wereldramp:

> The one that held acquaintance with the stars,
> And wedded soul to soul in purest bond
> Of reason, undisturbed by space or time;
> The other that was a god, yea many gods,
> Had voices more than all the winds, with power
> To exhilarate the spirit, and to soothe,
> Through every clime, the heart of human kind.

De Arabier vertelt dat inderdaad zondvloed en totale ondergang nabij zijn. De dromer ziet in hem op dat moment ook nog Don Quichote, uit de roman van Cervantes, en wil niets liever dan meegaan, maar dat kan niet. Dit is de nachtmerrie zelf:

> He left me: I called after him aloud;
> He heeded not; but, with his twofold charge
> Still in his grasp, before me, full in view,
> Went hurrying o'er the illimitable waste,
> With the fleet waters of a drowning world
> In chase of him; whereat I waked in terror,
> And saw the sea before me, and the book,
> In which I had been reading, at my side.

Wakker! Misschien door het water dat de grot aan zee inspoelde; en dat boek, ja, dat wás de Don Quichote. Wat een tegenstellingen! Enerzijds kennis die reikt naar de sterren, verkregen door de ongestoorde pure rede. Anderzijds de stem uit de schelp die de ondergang aankondigt én bode is van goddelijke troost, die geest, hart en ziel streelt. Harde steen of kwetsbare schelp, Euclides of Cervantes, meetkunde of poezie.

***Fabel, Eros en de 'Schreiber'***

Novalis (1772-1801) schrijft zijn (Bildungs)roman Heinrich von Ofterdingen in de laatste jaren van de 18e eeuw. Daarin trekt een middeleeuwse jongeling door de wereld, op zoek naar het paradijs van zijn dromen. Novalis drukt er zijn belangrijkste ideeën in uit, eigenlijk net zo als Wordsworth in zijn 'Prelude' doet, want de 'Heinrich' bevat ook autobiografische elementen. Maar kleur en toon van de roman zijn heel anders. Hoofdstuk IX is één lang sprookje, het sprookje van Klingsohr, vol allegorische figuren en alchemistische verwijzingen. In het volgende fragment wordt voor de eerste keer zonder enige inleiding of toelichting de figuur van de 'Schreiber' opgevoerd. Het duurt nog even voor de ware bezigheden van de Schreiber tevoorschijn komen, maar ze staan van meet af aan in kwaad daglicht:

> Zu der Zeit lag der schöne Knabe Eros in seiner Wiege und schlummerte sanft, während Ginnistan
> seine Amme die Wiege schaukelte und seiner Milchschwester Fabel die Brust reichte. Ihr buntes Halstuch hatte sie über die Wiege ausgebreitet, daß die hellbrennende Lampe, die der Schreiber vor sich stehen hatte, das Kind mit ihrem Scheine nicht beunruhigen möchte. Der Schreiber schrieb unverdrossen, sah sich nur zuweilen mürrisch nach den Kindern um, und schnitt der Amme finstere Gesichter, die ihn gutmütig anlächelte und schwieg.[4]

Een vrolijk samenspel van de kindertjes Eros en Fabel met de Schreiber is bij voorbaat uitgesloten, want wat een naarling is die man. Zijn schrijfwerk kan een eenvoudige toets al niet doorstaan:

[4] Novalis (pseudoniem voor Friedrich von Hardenberg): Heinrich von Ofterdingen, Ein Roman. Erster Teil, Die Erwartung. Berlijn 1802. Fragmenten uit Hoofdstuk 9.

> Der Vater der Kinder ging immer ein und aus, indem er jedesmal die Kinder betrachtete und Ginnistan freundlich begrüßte. Er hatte unaufhörlich dem Schreiber etwas zu sagen. Dieser vernahm ihn genau, und wenn er es aufgezeichnet hatte, reichte er die Blätter einer edlen, göttergleichen Frau hin, die sich an einen Altar lehnte, auf welchem eine dunkle Schale mit klarem Wasser stand, in welches sie mit heiterm Lächeln blickte. Sie tauchte die Blätter jedesmal hinein, und wenn sie beim Herausziehn gewahr wurde, daß einige Schrift stehen geblieben und glänzend geworden war, so gab sie das Blatt dem Schreiber zurück, der es in ein großes Buch heftete, und oft verdrießlich zu sein schien, wenn seine Mühe vergeblich gewesen und alles ausgelöscht war.

Het klare water in de schaal wijst onverbiddelijk uit wat blijvende waarde heeft en wat niet. Het laat ook zien wat de Schreiber dan wél bezielt:

> Die Frau wandte sich zuzeiten gegen Ginnistan und die Kinder, tauchte den Finger in die Schale, und sprützte einige Tropfen auf sie hin, die, sobald sie die Amme, das Kind, oder die Wiege berührten, in einen blauen Dunst zerronnen, der tausend seltsame Bilder zeigte, und beständig um sie herzog und sich veränderte. Traf einer davon zufällig auf den Schreiber, so fielen eine Menge Zahlen und geometrische Figuren nieder, die er mit vieler Emsigkeit auf einen Faden zog, und sich zum Zierat um den magern Hals hing.

Wat een tegenstellingen weer! Enerzijds Eros en Fabel, de levende blauwe5 damp waarin won-dere beelden opbloeien. Anderzijds de Schreiber, die met mierachtige ijver (Emsigkeit) neerge-vallen getallen en meetkundige figuren aan een draad rijgt.
Novalis heeft het tweede deel van de roman niet kunnen voltooien. Een kort gedicht is bewaard, dat volgens Novalis' vriend Ludwig Tieck de kern van dat deel moest zijn. De 'Zahlen und Fi-guren' zijn er weer, maar ook de verhalen van de kleine Fabel:

> Wenn nicht mehr Zahlen und Figuren
> Sind Schlüssel aller Kreaturen
> Wenn die so singen, oder küssen,
> Mehr als die Tiefgelehrten wissen.
> Wenn sich die Welt ins freie Leben
> Und in die Welt wird zurückbegeben,

[5] De kleur blauw en vooral 'Die Blaue Blume' heeft een bijzonder betekenis bij Novalis en in navolging van hem bij andere Duitse Romantici: eindeloos Verlangen, Liefde en streven naar het Oneindige.

Wenn dann sich wieder Licht und Schatten
Zu echter Klarheit werden gatten.
Und man in Märchen und Gedichten
Erkennt die wahren Weltgeschichten,
Dann fliegt vor Einem geheimen Wort
Das ganze verkehrte Wesen fort.[6]

***Verschillen in tegenstellingen***

In de aantekeningen van Novalis voor deel I staan bij het 'sprookje' de woorden:

> Vernunft – Phantasie. Verstand. Gedächtnis. Herz. (Der Verstand ist feind-selig – er wird verwandelt.)[7]

Novalis was intiem bevriend met Friedrich Schlegel, die in zekere zin de 'theoreticus' van de vroege Duitse Romantiek is. Volgens Schlegel moet poezie 'Universalpoesie' zijn, tegelijk filosofisch, mythologisch, ironisch en religieus. Aan Schlegel legt Novalis de bedoeling van zijn sprookje in een brief uit:

> Die Antipathie gegen Licht und Schatten, die Sehnsucht nach klaren, heissen, durch-dringenden Ather, das Unbekanntheilige, die Vesta in Sophien, die Vermischung des Romantischen aller Zeiten, der petrifizierende und petrifizierte Verstand, Arctur, der Zufall, der Geist des Lebens, einzelne Züge bloss, als Arabesken – so betrachte nun mein Märchen8

Nee, we misinterpreteren niet, als we onder de beeldschone en verleidelijke oppervlakte van Novalis' sprookje een aanval op de 'moderne' rationaliteit en ook de wiskunde zien. De aanval wordt zelfs met een romantische theorie onderbouwd. Natuurlijk is dat niet Novalis' hoofdbedoeling, dat is uit de hier gegeven fragmenten ook duidelijk; maar blijkbaar is het afzetten tegen 'Zahlen und Figuren' voor hem noodzakelijk in zijn allegorisch-mythologisch-filosofisch betoog.

Novalis wist zeker wel wat wiskunde was. Ook in zijn 'Aphorismen' treedt de wiskunde naar voren; niet in negatieve zin, maar wel Schlegeliaans ingekleurd. Novalis studeerde in Leipzig rond 1792 onder andere recht, wiskunde en filosofie. In 1794 ontmoet hij de dan

---

[6] Novalis: Heinrich von Ofterdingen. Uit Tiecks Bericht über die Fortsetzung. Het gedicht is immens populair in provincie .de van het www. De popgroep Novalis gebruikte de tekst in het album Bran-dung in 1977

[7] Novalis: Paralipmena zum 'Heinrich von Ofterdingen'

[8] Novalis, brief aan Friedrich Schlegel in Jena, 18 juni 1800.

12-jarige Sophie Kühn. Novalis zegt in een brief aan zijn broer dat er toen in een kwartier over zijn leven beslist werd. Sophie sterft in 1797. Novalis had haar willen *nachsterben*, maar schrijft toch nog zijn Heinrich von Ofterdingen. Dat Sophie daarin doorleeft, is duidelijk. 'Sophie' is de naam van de göttergleichen Frau bij de waterschaal; ze wordt door Eros zo genoemd, als deze uit de wieg stapt, plotseling groot is en uit de waterschaal wenst te drinken.
Ook Wordsworth kunnen we niet verwijten dat hij uit onkunde axioma's en proposities in de gedaante van de koele steen stelt tegenover de troost die uit de schelp ruist. In het museum in Wordsworth's huis in Grasmere (in het Lake District in Noord West Engeland) ligt de lijst van boeken die zijn vader bezat, in William's handschrift. Cervantes en Euclides staan erop; Euclides' Elementen waarschijnlijk in de vertaling van Simson, die met 26 drukken tussen 1756 en 1844 vast een fors marktaandeel bezat. Opmerkelijk is de aanwezigheid van 'Système de la nature', van Holbach, uit de Verlichte school van Diderot en D'Alembert. William werd naar de Grammar School in Hawkshead gestuurd, een 'boarding school'. Het curriculum omvatte klassieke talen, Engelse literatuur en behoorlijk wat wiskunde. De Elementen, boek I tot en met VI, en algebra tot en met het oplossen van tweede graadsvergelijkingen. Hawkshead was beroemd om de kwaliteit van het wiskundeonderwijs aldaar en Wordsworth in hnet bijzonder moet het goed gedaan hebben, al is hij daar nederig over in The Prelude:

> Yet may we not entirely overlook
> The pleasure gathered from the rudiments
> Of geometric science. Though advanced
> In these enquiries, with regret I speak,
> No farther than the threshold, there I found
> Both elevation and composed delight.[9]

Jongens van Hawkshead die in Cambridge gingen studeren, scoorden daar hoog op de beruchte Mathematical Tripos, die door Newton was ingesteld. De voor iedereen verplichte Mathematical Tripos waren echter rond 1790 al ontaard in een soort 'toelatingsdrempel'. Het was competitiegerichte wiskunde, die Gilbert Wakefield in zijn memoirs van 1804 'odious beyond conception' noemde, en de docenten met 'ignorant, heedless, insipid' beschreef. Onderwijs kon toen bar slecht zijn, zelfs zonder de gigantische corruptie en omkopingen die de uitgifte van de diploma's aan de beter gesitueerde studenten ken-

[9] Wordsworth, The Prelude, boek VI, 115 e.v.

merkte. Daarom van nu uit hulde voor de headmaster van Wordsworth in Hawkshead, die in een lokaal van 7 bij 12 meter 100 jongens van zes leeftijdsklassen voor zich had en ze opleidde van de eenvoudigste Latijnse declinaties naar Horatius en van het ondeelbare punt in definitie I naar propositie 33 van Elementen VI. Wordsworth schatte de wiskunde hoog, maar niet zo hoog als de poezie. Dat bleek al uit de beelden in de droom, maar ook uit een passage, verderop in The Prelude. Wordsworth beschrijft daar een periode van morele twijfel, na zijn bezoek aan Frankrijk, waar hij kort na de bestorming van de Bastille de bloedige terreur meemaakte waarmee die vooruitgang gepaard ging. Van twijfel naar wanhoop; morele zekerheid op het niveau van 'formeel bewijs' was er niet meer zijn:

> till, demanding formal 'proof',
> And seeking it in every thing, I lost
> All feeling of conviction, and, in fine,
> Sick, wearied out with contrarieties,
> Yielded up moral questions in despair.[10]

En daarom een vlucht:

> ... turned to abstract science, and there sought
> Work for the reasoning faculty...

De ommekeer wordt teweeg gebracht door Wordsworth's zuster Dorothy:

> She, in the midst of all, preserved me still
> A Poet, made me seek beneath that name,
> And that alone, my office upon earth.

Wordsworth maakt voor zichzelf een doorleefde keuze, grof afzetten science zelf is er niet bij. De Franse Revolutie en de Meetkunde, het lijken jeugdige dwalingen uit de dagen dat William zijn hoge roeping tot Dichter nog niet geheel begreep. Wordsworth raakte later zeer bevriend met Hamilton, astronoom en uitvinder van de algebra der quaternionen. Hamilton literatuurde ook, hij stuurde pakken poezie ter beoordeling naar Words-worth. Deze vond dat Hamilton zich beter tot wetenschap kon beperken en prees de poezie van Hamilton's zuster Eliza. Hamilton op zijn buurt was zeker gecharmeerd door William's zuster Dorothy. Hij bezocht Dorothy's graf in Grasmere een jaar na

[10] idem, boek X1, 301 e.v.

haar dood in 1855 en kuste de steen; bij maanlicht, zoals hij in een brief aan een vriend vermeldde.

### *Het verzet tegen de Verlichting*

De milde Wordsworth en de wat overbegeesterde Novalis tonen typische voorbeelden van het romantisch verzet tegen de Verlichting, de 17e en 18e eeuwse beweging die de rede als enig leidsnoer kiest om de wereld te begrijpen en de menselijke conditie te verbeteren. De Verlichting heeft diepgaande invloed gehad op kunsten, wetenschaps-beoefening en religieuze inzichten. Tot nu aan toe. De Verlichte wetenschapper omarmde de wiskunde als onderzoeksmiddel bij uitstek en modelleerde zijn exposé bovendien nog graag naar het voorbeeld van Euclides: uitgaan van grondwaarheden en daaruit propositie na propositie afleiden. Spinoza schrijft zo zijn 'Ethica' ordine geometrico demonstrata, op de wijze van de meetkunde dus. Dit gold niet de vorm alleen: slechts wat door de Rede uit enkele grondbeginselen kon worden afgeleid, kon waar zijn. Newton's bewegingswetten zijn feitelijk evenzo axioma's waaruit de ellips vorm van de planeetbanen wordt afgeleid. De Romantici zetten forse vraagtekens bij deze werkwijze als geheel; in dit verzet is de wiskunde niet het enige doelwit, de 'traditionele' natuurwetenschap krijgt er in het algemeen even fors van langs in de voorbeelden die nu ter illustratie volgen. [11]

### *De 'Verbeelding' verhongert*

Samuel Coleridge (1772-1834), tijdgenoot en lange tijd vriend en zielsverwant van Words-worth, herschrijft in 1791 het bewijs van de eerste propositie van de Elementen in versvorm. De bewerking begint zo:

> This is now--this was erst,
> Proposition the first--and Problem the first.
>
> I

[11] We zullen zo dadelijk zien dat Newton bij de Romantici enorm verzet riep. Spinoza (1632-1677) deed dat niet, waarschijnlijk omdat de Romantici Spinoza's onafhankelijk waardeerden, maar ook om zijn gelijkstellen van de natuur met God. Zowel Goethe als Coleridge prezen hem om zijn dogmaloze stellingname. Zowel Idealisten als Marxisten 'lazen' hun eigen ideeen in Spinoza's werk. Spinoza wist door zijn belangrijkste werken niet, of slechts zeer omzichtig in eigen kring te publiceren, een ernstig lot te vermijden. Het verzet tegen zijn gedachten was in de periode na zijn dood ongelooflijk hard. Zie het boek van J. Israel in de literatuurlijst.

On a given finite Line
Which must no way incline;
To describe an equi-
--lateral Tri-
--A, N, G, L, E.
Now let A. B. Be the given line
Which must no way incline;
The great Mathematician
Makes this Requisition,
That we describe an Equi--
--lateral Tri--
--angle on it:
Aid us, Reason--aid us, Wit!

Verdere lezing wordt hier ontraden, omdat het hele bewijs vier van dergelijke strophen vergt. De motivering van Coleridge, in een brief aan zijn broer, is belangrijker:[12]

> Dear Brother,
> I have often been surprized, that Mathematics, the quintessence of Truth, should have found admirers so few and so languid.--Frequent consideration and minute scrutiny have at length unravelled the cause--viz.--that though Reason is feasted, Imagination is starved; whilst Reason is luxuriating in it's proper Paradise, Imagination is wearily travelling on a dreary desart. To assist Reason by the stimulus of Imagination is the design of the following production.

William Blake (1757-1827), zeer origineel graficus, dichter en ontwerper van een volkomen eigen mythologie, gaat als een oudtestamentisch profeet veel heftiger te keer tegen het scheiden van Rede en Verbeelding:

> The Spectre is the Reasoning Power in Man; & when separated
> From Imagination, and closing itself as in steel, in a Ratio
> Of the Things of Memory, It thence frames Laws & Moralities
> To destroy Imagination! the Divine Body, by Martyrdoms & Wars.[13]

[12] Vers en bijhorende brief staan op internet.
[13] William Blake: Jerusalem (1802-1806). Blake's tekst is altijd onderdeel van een met de hand ingekleurde ets. Plate 74: The Four Zoa's.

Of duidelijker nog, als hij spreekt over 'Albion's Sons'

> Fixing their Systems, permanent: by mathematic power
> Giving a body to Falshood that it may be cast off for ever.
> With Demonstrative Science piercing Apollyon with his own bow![14]

Coleridge lijkt slechts een didactisch doel te hebben, Blake zou graag de *Demonstrative Science* met wortel en tak uitroeien!

### *Zien met hart en ziel*

Vele, vele regels van Wordsworth vertellen in vele vormen dit verhaal:

> To me the meanest flower that blows can give
> Thoughts that do lie too deep for tears.[15]

Wordsworth had alleen bezwaar tegen 'wetenschappelijke observatie' als die ontaardde in louter verzamelen van namen, in dorre classificatie. Daarin heeft hij in Goethe een zielsverwant. Goethe wil bijvoorbeeld het eigen gebaar van individuele plant ten diepste geschouwd hebben, voor er 'wetenschappelijk' tot 'soort' geclassificeerd wordt. Goethe wil de plant de kans geven zich te tonen, de experimenterende natuurwetenschapper dwingt de plant een bekentenis af. Bedenk wel dat de biologie als wetenschap begin 19e eeuw nog bijna alleen klassificeren wàs.

### *De wereld is geen klok*

Het ideaal van de Verlichting was een heelal - of een natuur - waarvan de bewegingen voorspelbaar zijn op grond van wiskundige regels, een heelal dat zich als het ware gedroeg als een mechanische klok. Dit waseen gruwel voor de Romantici. De persoonlijke vrijheid, de fantasie, alles wat 'Spiritual' was of 'Seele' had, kon daar geen plaats in hebben. Newton en Locke (en elders ook Bacon) werden als hoofdschuldige gezien,[16] ontwerpers van een helse wereld van tirannieke tandwielen. Volgens William Blake:

> I turn my eyes to the Schools & Universities of Europe
> And there behold the Loom of Locke whose Woof rages dire

---

[14] Idem, Plate 12.
[15] Wordsworth: Ode, Intimitations of Immortality. 1802-1804. Slotregels.
[16] Er is later onderzocht hoe dit gewraakte materialistische en mechanistische wereldbeeld (een danige misvorming van wat Newton werkelijk dacht) tot stand kwam bij de Romantici. Zie Thomas & Ober in de literatuurlijst.

Washd by the Water-wheels of Newton. black the cloth
In heavy wreathes folds over every Nation; cruel Works
Of many Wheels I view, wheel without wheel, with cogs tyrannic
Moving by compulsion each other: not as those in Eden: which
Wheel within Wheel in freedom revolve in harmony.[17]

Opmerkelijk genoeg heeft Blake waarschijnlijk de wiskundeliteratuur het meest geciteerde poeziefragment geleverd. Speciaal in meetkundeboeken, als het over symmetrie gaat treffen we vaak de eerste regels van The Tiger:

Tyger Tyger, burning bright,
In the forests of the night;
What immortal hand or eye,
Could frame thy fearful symmetry? [18]

Fearful symmetry, verderop gevolgd door beschouwingen over waar het vuur waar de tijger in gesmeed is:

What the hammer? what the chain,
In what furnace was thy brain?
What the anvil? what dread grasp,
Dare its deadly terrors clasp!

Na het citaat uit Jerusalem kunnen we het antwoord wel weten: *not in Eden.*

***Unweaving the Rainbow***

Een fraai diner bij de schilder Benjamin Haydon (1786-1846) thuis, op 28 december 1817. John Keats (1795-1821) is er, Wordsworth ook en Charles Lamb (1775-1834), deze laatste in de memoirs van de gastheer beschreven als na enige tijd 'delightfully merry'. Lamb haalt vrolijk uit tegen Newton, 'who believed nothing unless it was as clear as the three sides of a triangle'. Keats beschuldigde bij dit gelag Newton ervan de poezie van de regenboog te hebben vernield, door deze te reduceren tot de losse kleuren waarin een prisma licht zou splitsen. Er werd getoast op 'Newton's health, and confusion to mathematics'. Wordsworth lachte ogenschijnlijk mee.
Iets later: krachtige taal in Keats' *Lamia*, uitgegeven in 1818:

---

[17] William Blake: Jerusalem. Plate 15: The Four-fold men. Het beeld van het heelal als uurwerk is overigens al oud. Het komt al voor in Dante's Divina Commedia (Paradiso, XXIV, 13-18, rond 1316), daar geheel zonder negatieve connotaties.
[18] William Blake: Songs of Innocence and Experience (1794).

Philosophy will clip an Angel's wings,
Conquer all mysteries by rule and line,
Empty the haunted air, and gnomed mine -
Unweave a rainbow, as it erewhile made
The tender-person'd Lamia melt into a shade. [19]

'Phylosophy' staat hier duidelijk voor natuurfilosofie, de exacte wetenschappen.
De 'gnomed mine', de door levende wezens bevolkte binnensten der aarde, zijn het opmerken waard. Geologie en mysterieuze mineralen al helemaal, ze werden door Romantici hoog gewaardeerd. Novalis zal zijn Heinrich de blauwe bloem, top-Romantisch symbool van inzicht in de eigen Ziel Zelf, in een diepe mijngang laten vinden.
Lamia is tegelijk slang en beeldschone mensenvrouw. De 'philosopher' die haar ten overstaan van haar minnaar Lucius ontmaskert, heet betekenisvol Apollonius. Keats gebruikte de regenboog in het begin van het gedicht trouwens om Lamia te beschrijven:

She was a gordian shape of dazzling hue,
Vermilion-spotted, golden, green, and blue;
Striped like a zebra, freckled like a pard,
Eyed like a peacock, and all crimson barr'd;
And full of silver moons, that, as she breathed,
Dissolv'd, or brighter shone, or interwreathed
Their lustres with the gloomier tapestries—
So rainbow-sided, touch'd with miseries,
She seem'd, at once, some penanced lady elf,
Some demon's mistress, or the demon's self.

Goethe fulmineert in zijn Zur Farbenlehre rechtstreeks honderden bladzijden lang tegen Newton's zeer geometrische Optica en probeert met eigen experimenten Newton te weerleggen. Goethe's 'verklaring' van de kleuren aan een zijde van het prisma mag in mathematische of wetenschappelijke zin onbeholpen zijn, de beschrijving van kleurverschijnselen in de Farbenlehre is steeds meeslepend. Twee heel verschillende citaten:

Ich sah die Erscheinungen der Natur in offner Welt, und brauchte nicht erst einen zwirnsfädigen Sonnenstrahl in die finsterste Kammer zu lassen, um zu erfahren, dass hell und dunkel Farben erzeuge.

[19] John Keats: Lamia (1818), Part II, 234-239.

Als aber die Sonne sich endlich ihrem Niedergang näherte und ihr durch die stärkeren Dünste höchst gemässigter Strahl die ganze mich umgebende Welt mit der schönsten Purpurfarbe überzog, da verwandelte sich die Schattenfarbe in ein Grün, das nach seiner Klarheit einem Meergrün, nach seiner Schönheit einem Smaragdgrün verglichen werden konnte .[20]

Het eerst polemische citaat bevat de kern van Goethes verklaring van de kleuren achter het pris-ma: ze ontstaan waar donker en licht op elkaar stuiten. Het tweede citaat haalt het moderne natuurkundeboek niet omdat de natuurkundige van nu de 'Farbenlehre' waarschijnlijk al tweehonderd bladzijden eerder definitief heeft gesloten.
Het belangrijkst in deze romantische stellingname is natuurlijk niet het verdedigen van de regenboog, die is in het Lake District vaak genoeg te zien, maar de diepe aversie tegen het tot op het bod klein snijden van de verschijnselen, tegen het reductionisme als de enige weg naar kennis.
Wordsworth had overigens wél grote bewondering voor Newton, al in zijn schooljaren in Hawkshead. Zijn beschrijving van het standbeeld van Newton in Cambridge mag hier dan ook niet ontbreken:

> And from my pillow, looking forth by light
> Of moon or favouring stars, I could behold
> The antechapel where the statue stood
> Of Newton with his prism and silent face,
> The marble index of a mind for ever
> Voyaging through strange seas of Thought, alone.[21]

Schitterend én huiveringwekkend: silent, marble, strange, alone.
De eerste regels van dit citaat zijn uit 1805, de laatste twee zijn toegevoegd in 1838; een mogelijke aanwijzing dat Wordsworth houding in dezen veranderde, mogelijk sterker werd in de weerstand tegen de te eenzijdige exacte wetenschap.

### *Die hoogmoedigen*

Keats zei het al: ze komen overal aan met hun regels en rechte lijnen. Dit verwijt werd door velen gemaakt, het verwijt dat wetenschappers meenden dat ze alles konden begrijpen door het op hún manier aan te pakken. Goethe nogmaals, nu over de wiskundigen in het bijzonder:

---

[20] J. W. Goethe: Die Frabenlehre. Gesamtausgabe Stuttgart, 1885, X.
[21] Wordsworth, The Prelude, boek III, 58-63.

> Die Mathematiker sind wunderliche Leute: durch das Großes, was sie leisteten, haben sie sich zur Universalgilde aufgeworben und wollen nichts anerkennen, als was in ihren Kreis paßt, was ihr Organ behandeln kann.[22]

Het is een overduidelijk verzet tegen de mathematische arrogantie. Keats'

> Philosophy will clip an Angel's wings,
> Conquer all mysteries by rule and line,
> ....

zegt nog iets méér en is verwant aan Novalis' prachtige term uit de brief aan Schlegel 'das Unbekanntheilige'. Voor de Romanticus zijn begrippen 'verte', 'het onbekende', 'Wandern' van levensbelang, luister maar naar de teksten van de liederen van Schubert en Schumann. Ze hebben een symboolwaarde die dieper gaat dan de zoete heimwee naar de onbereikbare verte zelf. Het gaat om het heilig-mysterieuze dat zich ontrekt aan de mechanischmen van het wiskundig verklaarbare.

***En nú?***

Het romantisch ongenoegen met de rede leeft na de korte periode rond 1800 waar we even in vertoefden, nog volop voort en de bezwaren die de romantische dichters aanvoerden, zijn dagelijks in allerlei vormen hoorbaar.

Wie zegt: 'O, dus jij denkt dat je alles kunt berekenen' toont dezelfde ergernis als Keats, zij het wat schameler geformuleerd.

En wij exacten doen het zelf ook. We spreken nog steeds graag van harde objectieve feiten en van koel redeneren. De steen van Wordsworth is dan niet ver, en Blake's 'Spectre of Reason' glijdt als een rilling over de ruggen.

Het 'Universalgilde' van Goethe dat zich nu in krantencolumns over van alles uitspreekt in de media is niet meer alleen bevolkt door wiskundigen, ook door mathematische economen, sterrenkundigen en biochemici, die hun door de Rede geslepen pijlen vuren op de warboel van politiek bedrijf, emotie-cultuur en onderwijs.[23]

---

[22] J. W. Goethe: Ueber die Naturwissenschaft, einzelne Betrachtungen und Aphorismen. Gesamtausgabe Stuttgart, 1885, I

[23] *Onderwijs*: toevoeging juni 2008. Goethe's kritiek op het Universalgilde schiet nog steeds raak wanneer denken over onderwijs verengd wordt tot kiezen van een eindterm algebra meer (en niet minder) en het systematisch verwerpen van alles wat naar didactiek zweemt.

Het wil op het moment niet zo best lukken met de aantrekkelijkheid van het vak wiskunde en de zusjes natuurwetenschap en techniek. Dat is bekend en er zijn vele redenen voor aangevoerd. Maar zou het misschien (ook een beetje) komen omdat er weinig echt geluisterd is naar de bezwaren van Wordsworth, Keats, Blake, Novalis en Goethe? Terwijl de bezwaren van de Romantici ons al twee eeuwen om de oren zingen. Terwijl toch duidelijk is dat op keuzemomenten in het leven (eind VWO bijvoorbeeld) persoonlijke, subjectieve ervaringen heel bepalend zijn.
Toch hameren we in de recente discussies over de teloorgang van wiskunde(onderwijs) en techniek en bij de staatsondermijning van het N&T-profiel nogal zwaar en eenzijdig op het nut-nutnut van wiskunde, natuurwetenschap en techniek. Zonder N&T geen kenniseconomie en spoedig breken de dijken door, als er geen Hansje meer is die nog zonder twee duimen op de rekenmachine kan staartdelen! Ik chargeer, zeker. Maar geen leerling van nu kiest wiskunde als levensdoel/studierichting/roeping (inclusief de impliciete gelofte van zelfaanvaarde armoede) omdat het algemeen Nederlands belang dat nodig heeft. Het publieke beeld van wiskunde klopt nodeloos goed met de romantische bezwaren. Het wordt door de media in samenwerking met de beroepsgroep mede instand gehouden. Een voorbeeld. Als het ons werkelijk menens is met het belangrijke (en schone) van de wiskunde, dan staat boven een klacht in de krant liever niet zulke wervende doomdenkerij als:

> Eens stond de Nederlandse wiskunde aan de internationale top. Maar die tijd is voorbij. Haakjes wegwerken, breuken onder één noemer brengen: vwo-scholieren kunnen het niet meer, klagen deskundigen.
> En het aantal wiskundestudenten daalde van vijfhonderd naar honderd.[24]

Dat zal de redacteur wel weer gedaan hebben, zo'n triviale inleiding zetten boven de pagina. Maar het geschapen beeld is weer erg bevestigd: wiskundigen zijn van die typen die alles tot formules reduceren en tot hun pensioen haakjes verdrijven of iets in factoren ontbinden. Geen gezond mens met nog een laatste spoortje 'Verbeelding' trapt daar in.

[24] Het Parool van 15/3/2003

*Tot slot*

Je kunt als enigszins geschoold wiskundige of gewoon wetenschapsliefhebber heel makkelijk al die romantische bezwaren van tafel vegen. Ongeveer zo: die kleurenleer van Goethe is totaal achterhaald en klopt aantoonbaar niet, wiskundigen zijn heel gepassioneerd over hun nieuwste stelling van Fermat, wiskunde is niet alleen reductie tot trivialiteiten maar ook synthese en opbouw, wiskunde is ook heel mooi, kijk maar in de kunstspecial van Euclides, en we knippen heus die engel de vleugels niet af.

Enzovoort, enzovoort. Maar weerleggen is niet zo'n interessante vorm van gesprek met een partner die heel onverlicht het hart laat spreken. Dat werkt niet. Je versterkt het beeld alleen maar. Nee, laat dan liever genieten van puur a-wetenschappelijke regels als:

The Rainbow

My heart leaps up when I behold
    A Rainbow in the sky:
So was it when my life began;
So be it when I shall grow old,
    Or let me die!
The Child is father of the man;
And I wish my days to be
Bound each to each by natural piety.[25]

The Child is father of the man, dat is de regel die nu in het klaslokaal van William Wordsworth, nu museum, in Hawkshead op de muur is gezet. Misschien is het wel Wordsworth's beroemdste regel. De jonge William liep in Hawkshead bijna dagelijks voor zes uur 's ochtends (als de school begon) steeds dezelfde vijf mijl rond het schitterende Esthwaite Water van zijn hospita naar school. Vandaar zijn band met Nature, hij zegt het zelf.

Mag iemand duizend keer de regenboog zien, zonder die met prisma's, bolvomige druppels en gedifferentieerde arcsinussen te willen begrijpen? Ik vind van wel, zeker als het zonder nodeloos verzet tegen de rede gaat, zoals bij Wordsworth.

Anders gezegd: waardering dezerzijds van de Romantische Beleving, zonder mee gaan in de excessen ervan (er zijn er vele, helaas!) schept misschien meer ruimte voor anderzijdse erkenning van de waarden van de Verlichte Rede dan honderd afgedwongen reisjes over 'strange seas of Thought, alone'.

---

[25] Wordsworth, ( 1802).

## *Bronnen*


De poetische werken van Wordsworth staan geheel op internet:

1. http://www.bartleby.com/145/.

Maar twee Penguinpockets zijn handiger, en veruit de beste gids voor wandelen in het Lake District. Alle geciteerde teksten van Wordsworth staan in de volgende twee bronnen:

2. **William Wordsworth**. *Selected Poems*. Penguin Classics, 1994.
3. **William Wordsworth**. *The Prelude, The four texts (1798, 1799, 1805, 1850)*. Penguin Classics, 1995.

Een recente biografie over William Wordsworth en een iets oudere:

4. **Juliet Baker**. *Wordsworth, A Life*. Viking Press, 2000.
5. **Hunter Davies**. *William Wordsworth.* Butler and Tanner, 1980.

Speciaal over *The Prelude*:

6. **John F. Danby**: *Wordsworth, The prelude and other poems*. Edward Arnold, publishers, 1970.

Buiten de directe bronnen (dwz. van de poezie zelf) weten we veel van de ideeën van Words-worth door zijn briefwisseling met Hamilton over wetenschap en poezie. Boeiend wat dit betreft is een biografie over Hamilton:

7. **Thomas L. Hankins**. *Sir William Rowan Hamilton*. John Hokins University Press, 1980.

Over de relatie Newton-Wordsworth:

8. **W. K. Thomas and Warren U. Ober.** *A Mind for ever voyaging*, Wordsworth at work, portraying Newton and science. University of Alberta Press, 1989.

Keats staat ook in de Penguinkast; er is een Nederlandse vertaling van diverse gedichten van Keats. Lamia staat daar gedeeltelijk in, maar 'Unweaving the rainbow' net niet.

9. **John Keats**. *Selected Poems*. Penguin Books, 1988.
10. **John Keats**. *Gedichten*. Ambo tweetalige editie, samengesteld door Léon Stapper. Ambo, 1991.

Novalis' Heinrich von Ofterdingen staat op internet én op papier en op MP3:

11. **Novalis**. *Heinrich von Ofterdingen.* http://gutenberg.spiegel.de/novalis/ofterdng/ofterdng.htm.
12. **Novalis**: *Heinrich von Ofterdingen*. Reclam, Stuttgart, 1978. (een schooluitgave)
13. **Novalis** (de Popgroep). *Brandung*. Track 2 is het nummer *Wenn nicht mehr Zahlen und Figuren.* Duur: 3.03. Free download via *http://www.progarchives.com/*

14. **Novalis.** *De blauwe Bloem.* Vertaling van de *Heinrich von Ofterdingen* door Ria van Hengel. Athenaeum – Polak & Van Gennep (2006) (Toevoeging juni 2008)

William Blake staat volledig in de Penguin Classics, maar zonder gekleurde platen is het wel mager en doorbijten door de overspannen teksten. Het boek van Roszak is uit de periode van de Flower Power en neemt Goethe, Wordsworth en Blake als voorbeelden voor 'nu'. Misschien wat gedateerd, maar toch noch informatief en inspirerend.

15. **William Blake.** *The Complete Poems.* Penguin Classics, 1977.
16. **William Blake.** *The Complete Illuminated Books.* Thames & Hudson, 2001.
17. **Theodore Roszak.** *Het einde van niemandsland, Politiek en transcendentie in de postindustriële samenleving.* Meulenhoff, 1972.

Goethe is in allerlei vormen uitgegeven. Bij zoeken met Google op 'Goethe Mathematik' komen evenveel vereerders als verwerpers van Goethe's inzichten boven. Goethe is bij een grote groep mensen vooral bekend gebleven via de ideeën van Rudolf Steiner, grondlegger van de Anthroposofie. Goethe schreef veel, heel veel. Tien banden van elk 900 bladzijden, met zeer kleine Gothische letters. Iets om in gotische letters te erven en af en toe te zien:

18. **J.W. Goethe.** *Sammtliche Werke, Vollständige Ausgabe in Zehn Bänden.* Stuttgart 1885.

De 'Farbenlehre' beslaat daarvan een vol deel. Ze staat nog steeds in de belangstelling, vooral in anthroposofische kringen. Er is een Nederlandse vertaling, maar die is niet volledig (het origineel omvat zo'n 600 bladzijden):

19. **J.W. Goethe.** *Kleurenleer.* Samengest. door Bob Siepman van den Berg; vertaling van Pim Lukkenaer. Zeist, Vrij Geestesleven, 1991.

Algemeen over literatuur en wetenschap in de 19e eeuw:

20. **J. A. V. Chapple.** *Science and literature in the nineteenth century.* Macmillan Education Limited, 1986.
21. **Jonathan Smith.** *Fact and Feeling, Baconian Science and nineteenth century literary imagination.* University of Wisconson Press, 1994.

Een belangrijk nieuw boek over de radicale voorlopers van de Verlichting, vooral Spinoza:

22. **Jonathan I. Israel.** Radical enlightenment: philosophy and the making of modernity, 16501750 . Oxford University Press, 2001.

Over de vroege romantiek in het algemeen:

23. **H. G. Schenk.** *The Mind of the European Romantics.* Oxford University Press, 1966.

24. **Hugh Honnour**. *Romanticism*. Harper and Row, 1979.
25. **Marilyn Butler**. *Romantics, Rebels and Reactionaries*. English Literature and its Background, 1760-1830. Oxford University Press, 1981.

Over de tweedeling literatuur-wetenschap gaat de beruchte Rede-lecture *The Two Cultures* van C.P. Snow uit 1959. Snow spreekt de literaten er op aan dat ze in natuurwetenschappelijk opzicht erger dan analfabeet zijn. Hier een bron met een uitvoerige weergave van het debat dat de lezing opriep:

26. **C.P. Snow**. *The Two Cultures*. Cambridge University Press, 1998.

# Emmaüsgangers zijn geen blindgangers

Igor Berezhnoy, Eric Postma, en Jaap van den Herik

Geschilderde kunst is een belangrijk onderdeel van ons culturele erfgoed. Computers worden tegenwoordig ingezet om schilderijen op ruime schaal te digitaliseren. De volgende stap is de automatische analyse van gedigitaliseerde schilderijen door de inzet van intelligente computerprogramma's. In deze bijdrage behandelen we de vraag: hoe kunnen computers een kunstkenner ondersteunen bij de beoordeling van schilderijen? Het gaat om kleur, compositie, herhaling van patronen, en penseelstreken. We beperken ons tot ons eigen onderzoek en geven een overzicht van het gebruik van complementaire kleuren en de penseelstreken in de werken van Vincent van Gogh. Voorts bespreken we de mate waarin onze technieken kunnen leiden tot een kunstmatig intelligente kunstkenner. Tenslotte trekken we een conclusie over de bijdrage van kunst en artificial intelligence aan het cultureel erfgoed.

## 1. Introductie

In de Nederlandse artificial intelligence (AI)-onderzoekswereld hebben twee vragen in de afgelopen 25 jaar veel aandacht gekregen. Het zijn: (1) kunnen computers schaken? (1975-1997) en (2) kunnen computers rechtspreken? (1991-heden). Omstreeks 1998 kwam daar een derde vraag bij: kunnen computers kunst herkennen? De vraag is even eenvoudig als doeltreffend. Het is een geweldig uitdagende onderzoeksvraag. Hij ligt dan ook in het verlengde van de eerste twee vragen. Niettemin is er duidelijk sprake van een *paradigm shift*. Bij schaken gaat het om cognitie (weten, kennen, leren kennen), bij rechtspreken gaat het om het beoordelen van casus die op schrift gesteld zijn (cognitie) en niet om het (mede-) beoordelen van antwoorden die een juridische partij geeft in de rechtszaal. Bij kunst gaat het om beelden, kleuren en composities, om percepties (herkennen, zien, waarnemen, begrijpen). Menselijke perceptie is het resultaat van een langdurig ontwikkel- en leerproces. Dat geldt ook voor kunstmatige perceptie. Het leren herkennen van visuele patronen speelt hierbij een belangrijke rol. In de AI wordt veel gebruik gemaakt van automatische leertechnieken, ook wel *machine-learning* technieken genoemd. Met behulp van deze technieken is het mogelijk om een computer aan de hand van voorbeelden een (visueel) patroon te laten herkennen.

Een computer is bepaald geen blindganger meer die bij toeval het goede antwoord geeft. In tegendeel, door een gedegen analyse en een zorgvuldige implementatie van diverse intelligente technieken hebben computers zich ontwikkeld tot ware experts. Enige jaren geleden onderzochten Postma en Van den Herik een manier om de visuele herkenningsprestaties van een automatische leertechniek te bepalen. Een tentoonstelling van neo-impressionisten bracht hen op het idee om een verzameling gedigitaliseerde schilderijen als uitgangspunt te gebruiken. Deze verzameling bestond uit werken van zes schilders (Claude Monet, Vincent van Gogh, Paul Cézanne, Alfred Sisley, Camille Pissarro, en George Seurat). Uit ieder schilderij werden door de computer specifieke kenmerken geëxtraheerd (kleur, compositie, herhaling van patronen, en penseelstreken). Uit neurowetenschappelijk en psychologisch onderzoek was ons bekend dat in het menselijk visueel systeem vooral kenmerken als kleur, vorm, en textuur, een belangrijke rol spelen in de visuele herkenning van objecten. Dat geldt ook voor schilderijen. In één van onze experimenten lieten we de computer daarom deze biologisch plausibele visuele kenmerken uit de gedigitaliseerde schilderijen halen. Vervolgens trachtten we aan de hand van de kenmerken automatisch de schilder bepalen. Tot onze verbazing bleek de computer in staat om in meer dan 90% van de gevallen de identiteit van de schilder te herkennen uit de textuureigenschappen alleen (dus uit de penseelstreek). Nadere analyse onthulde dat de computer had geleerd de verschillen in de manier waarop de verf op het doek was aangebracht te herkennen. Zo werd Van Gogh herkend door zijn specifieke wilde penseelstreek en Cézanne door zijn hoekige schilderstijl. Inmiddels is het schilderijenproject uitgegroeid tot een promotieonderzoek in het kader van het NWO-project *Authentic* [noot 1] waarin promovendus Igor Berezhnoy een systeem ontwikkelt dat kunstexperts ondersteunt bij hun analyse van schilderijen.

## 2. Het *Authentic*-project

In Maastricht concentreert het *Authentic*-project zich op de ontwikkeling van technieken voor de perfectionering van de automatische analyse. Een verzameling van 169 gedigitaliseerde schilderijen van Vincent van Gogh is onze bron van inspiratie en onderzoek. Tot op heden verrichten we vooral onderzoek met behulp van analyses van gebruikte kleuren en analyses van (lokale) textuur.

Voor de compositie en de herhaling van patronen gaat het om ruimtelijke zaken, ook wel de visuele contouren genoemd. Natuurlijk

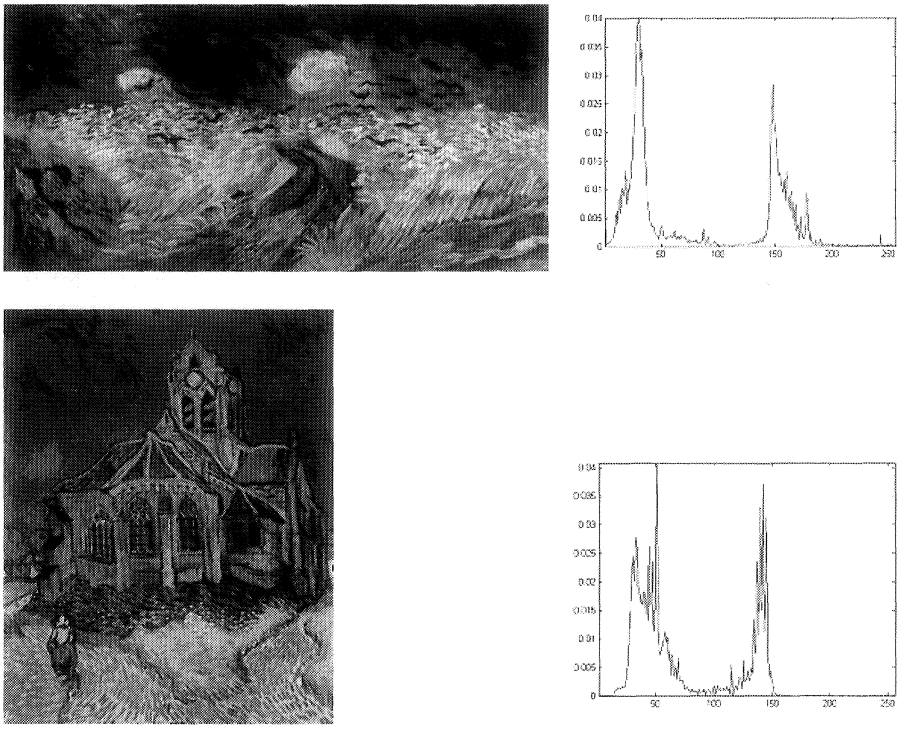
overlappen de contouren van objecten elkaar vaak of beïnvloeden ze elkaar met een schaduw. Om de schilderijen op een goede manier aan onze automatische leertechniek (een classifier) te kunnen aanbieden maken we gebruik van verschillende voorbereidingstechnieken die de dimensionaliteit van de afbeelding reduceren. Vijf voorbeelden van dergelijke voorbereidingstechnieken zijn: (1) *histogramming*, (2) wavelet transformatie, (3) statistische descriptoren, (4) principale componenten analyse, en (5) fractale dimensie analyse. Na de voorbereidingstechnieken gaat het eigenlijke herkenningswerk beginnen. Een automatisch lerende classifier is daar erg goed in, want eigenlijk is het een classificatietaak (Monet, Van Gogh, Cézanne, Sisley, Pissarro, en Seurat). Classificeren komt weer neer op tellen en daar is een computer nu juist heel goed in. Als je lokaal alles weet, dan kun globaal een heel goed oordeel geven. Om lokaal "alles" te weten doen we bijvoorbeeld een beroep op diverse statistische descriptoren die een deel van het schilderij beschrijven. In de kern zijn de descriptoren in staat om de "handtekening" van een schilder zeer nauwkeurig te beschrijven en de schilder derhalve te identificeren, zelfs op de tweedeling echt-onecht. Hieronder geven we enig inzicht over de aanpak bij kleur en penseelstreek.

## 3. Automatische analyse van kleur

Iedere pixel in een gedigitaliseerd schilderij bestaat uit een triplet van kleurintensiteiten behorende bij de basiskleuren *rood*, *groen*, en *blauw*. Door menging van de drie basiskleuren (ook wel *rgb*-kleuren genoemd) met verschillende intensiteiten ontstaat een spectrum van kleuren. De *rgb*-kleuren worden gebruikt voor de representatie en reproductie van kleuren. Voor onze doeleinden is met name de representatie van kleur belangrijk. Om een betrouwbare analyse te kunnen uitvoeren van de kleuren dienen we zo veel mogelijk rekening te houden met de perceptuele aspecten van kleur. (Hoe beleven mensen een kleur? En hoe "doet" een computer dat?) Uit neurowetenschappelijk onderzoek is gebleken dat kleurwaarneming veel complexer is dan het mengen van drie basiskleuren. Daarom wordt voor de representatie van de perceptuele aspecten van een kleur gebruik gemaakt van alternatieve kleurrepresentatiesystemen zoals *hsi* en *CIELab*. In het *hsi*-representatiesysteem worden kleuren gerepresenteerd door het triplet *Hue* (de tint), *Saturation* (de verzadiging), en *Intensity* (de intensiteit). Enkel op basis van de Hue-waarden kunnen al grove kleurovereenkomsten in een schilderij worden gedetecteerd. Ter illustratie toont figuur 1 twee schilderijen van Vincent van Gogh die een overeenkomstige globale kleurcompositie hebben. In beide

schilderijen wordt veel gebruik gemaakt van geel en blauw, hetgeen duidelijk zichtbaar is door een vergelijking van de bijbehorende *hue*-histogrammen. De pieken in beide histogrammen komen ruwweg overeen met de kleuren geel en blauw.

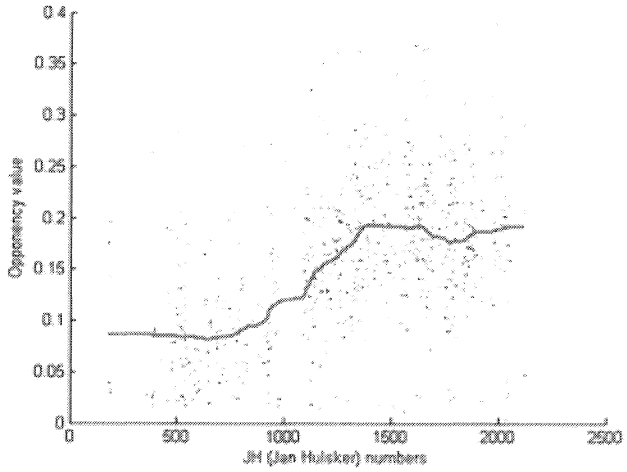
Vooral in zijn latere werk maakt Vincent van Gogh veelvuldig gebruik van complementaire kleuren om accenten aan te brengen in zijn schilderijen. De kleurparen rood-groen en geel-blauw zijn de belangrijkste complementaire kleuren. Uit neurowetenschappelijk onderzoek is gebleken dat deze kleurparen een belangrijke rol spelen in het neurale mechanisme dat aan kleurperceptie ten grondslag ligt. In dit zogenoemde *opponente-kleuren mechanisme* worden kleuren gerepresenteerd in termen van een balans tussen rood en groen, geel en blauw, en zwart en wit. Het *CIELab*-kleurrepresentatiesysteem is een adequate benadering van de opponente-kleuren representatie.



Figuur 1. Twee schilderijen van Vincent van Gogh met een overeenkomstige globale kleurcompositie. De histogrammen van de hue-component van het hsi-kleurrepresentatiesysteem vertonen pieken op vrijwel dezelfde hue-waarden (overeenkomend met de kleuren geel en blauw). Bron: het Webmuseum: http://www.ibiblio.org/wm. Met dank aan Nicolas Pioch.

## 3.1 JH-nummers

Iedere kunstenaar kent ontwikkelingen in zijn/haar werk. De meeste kunstenaars hebben een vroege periode en een late periode. Deze perioden hebben verschillende karakteristieken. In de tussenliggende periode zie je de ontwikkeling van de karakteristieken. De vraag is nu of dit pad volledig in kaart gebracht kan worden. Sterker nog, de eigenlijke vraag luidt: is het mogelijk om een collectie van schilderijen van een kunstenaar chronologisch te ordenen? Voor Van Gogh is dit min of meer gebeurd; dat wil zeggen, niet door een computer, maar door Jan Hulsker. Hij heeft een nummersysteem gedefinieerd dat de chronologische volgorde van de (vermeende) creaties van de schilderijen bij benadering goed vastlegt. De getallen worden JH-nummers genoemd. Een belangrijke vraag voor kunsthistorici is nu: kun je uit de JH-volgorde aflezen dat Van Gogh in zijn actieve periode (1881-1890) steeds meer gebruik ging maken van complementaire kleuren? Nauwkeurige analyse van opponente kleuren met behulp van het *CIELab*-representatiesysteem in de hoogwaardige digitale reproducties van schilderijen (gerangschikt volgens JH-nummers) toont aan dat dit vooral het geval is als Van Gogh in Parijs woont en later in Zuid Frankrijk. Figuur 2 geeft een weergave van de toename in het gebruik van complementaire kleuren (uitgedrukt in "opponency value", dat is de proportie rood-groen en geel-blauw overgangen in het schilderij) als een functie van de (bij benadering) chronologische JH-nummers. Een duidelijke overgang in het gebruik van complementaire kleuren is zichtbaar rondom de JH-nummers tussen 1000 en 1400. Deze nummers corresponderen met de tijd waarin Van Gogh verhuisde van Antwerpen naar Parijs en later Arles. Met onze analysetechniek is het tevens mogelijk om automatisch objecten te detecteren waarop Van Gogh de nadruk legde door rood-groen of geel-blauw overgangen. Figuur 3 toont een voorbeeld. De inzet rechtsonder is een silhouet van een persoon dat door Van Gogh is voorzien van geel-blauwe contouren. Zonder het te weten maakte Van Gogh gebruik van het neurale opponentie-mechanisme dat ten grondslag ligt aan de menselijke perceptie van kleuren.

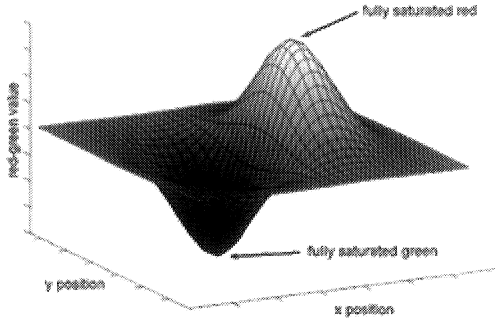



Figuur 2. De opponency value (proportie rood-groen en geel-blauw overgangen in een schilderij) als een functie van het Jan Hulsker nummer (een bij benadering chronologische ordening van de werken van Van Gogh). De curve geeft het gemiddelde aan.

Figuur 3. De automatische segmentatie van een silhouet van een persoon door de detectie van (in dit geval) geel-blauw overgang uit het schilderij "Landschap met bomen en vrouwelijke figuur" Saint-Rémy, 1889, (JH 1848). Bron: The Vincent van Gogh Gallery: http://www.vggallery.com. Met dank aan David Brooks

## 4. Automatische analyse van (lokale) textuur

Naast kleur is een van de belangrijkste kenmerken van een schilder zijn penseelstreek. Kunstexperts beweren zelfs dat een schilder direct te herkennen is aan de wijze waarop hij de penseelstreken aanbrengt. Door een specifieke verftechniek bepaalt de schilder de visuele textuur van het schilderij. Met behulp van geavanceerde visuele filtertechnieken (die wederom zijn geïnspireerd door neurowetenschappelijke inzichten) kan de gedigitaliseerde textuur worden gekwantificeerd. Een voorbeeld van een biologisch geïnspireerd filter tonen we in figuur 4. De x- en y-as vormen het beeldoppervlak van het schilderij, de z-as representeert de respons van het aangebrachte filter (een Gabor-filter). Gegeven de vorm en oriëntatie van het Gabor-filter, wordt een maximale respons verkregen wanneer er sprake is van een verticale rood-groen overgang. Dit filter is een voorbeeld van een model voor de gevoeligheid van neuronen in het visueel systeem. Bovendien heeft het wiskundig gezien aantrekkelijke eigenschappen, zoals een optimale combinatie van resolutie in spatiële frequentie en plaats. Voor het gebalanceerd kwantificeren van de lokale textuureigenschappen wordt doorgaans gebruik gemaakt van meerdere Gabor-filters op dezelfde positie, maar met verschillende oriëntaties en verschillende grootte.




Figuur 4. Illustratie van een Gabor-filter

Momenteel verrichten wij een diepgaande computationele analyse van de locale textuur zoals die is aangebracht op de diverse schilderijen met behulp van Gabor-filters en statistische leertechnieken. Het doel is om de statistische structuur van de penseelstreken van Van Gogh te inventariseren en vervolgens zodanig te karakteriseren dat de kunstexperts van het Van Gogh museum hun meetbare eigenschappen kunnen gebruiken voor hun oordeel (vals of echt).

## 5. Een intelligente kunstherkenner?

Om een schilderij te herkennen hebben we patroonherkennende vermogens nodig. Dat geldt zowel voor mensen als voor computers. De patroonherkennende vermogens van de door ons ontwikkelde technieken zijn groot. Tot op zekere hoogte zijn ze groter dan het patroonherkennend vermogen van een mens. Figuur 5 toont de beroemde Vermeer-vervalsing De *Emmaüsgangers* van meester-vervalser Han van Meegeren. Met onze technieken zou het schilderij ondubbelzinnig als een vervalsing worden geclassificeerd. Dat de vermaarde kunstexpert Abraham Bredius ondanks twijfels het schilderij als authentiek aanmerkte had meer te maken met zijn diepe wens om een echte Vermeer te ontdekken dan met een gebrekkig patroonherkennend vermogen. Zo beschouwd bieden onze technieken een objectieve bijdrage aan het werk van de kunstexpert. Ieder detail van het schilderij wordt door de computer moeiteloos en zonder emotie geanalyseerd en vertaald in een objectief oordeel. Bredius mag dan verblind zijn geweest door de twijfel die hem bevangen had, een computer zal dat niet (snel) overkomen. Computers zijn geen blindgangers meer als het relevante antwoorden betreft over de textuur van een schilderij.

Figuur 5. De Emmaüsgangers. (Vermeer vervalsing). Bron: http://www.museumbredius.nl/eerherstel.htm. Met dank aan het Museum Bredius en het Museum. [noot 2]

Is onze kunstmatige kunstkenner daarmee intelligent? Ja en nee. Enerzijds is onze kunstkenner intelligent, omdat het over een klein maar belangrijk stukje perceptuele intelligentie beschikt. Het is precies dat deel van de natuurlijke perceptuele intelligentie dat vooraf gaat aan de herkenning van objecten en dat mensen in staat stelt om snel te bepalen waar de blik op gericht dient te worden. Anderzijds is onze kunstkenner niet intelligent, omdat deze (nog) geen notie heeft van vorm of betekenis. Het huidig onderzoek aan de kunstmatige kunstkenner is daarop gericht. Misschien zijn we in de komende jaren in staat om de kunstkenner te leren objecten te herkennen (en op een juiste wijze te interpreteren). De kunstmatige bepaling van het "thema" van een schilderij vereist wereldkennis en die is voorlopig alleen nog maar beschikbaar in de hoofden van natuurlijke kunstkenners. Alleen zij kunnen zeggen of de Emmaüsgangers "blindgangers" waren. Eigenlijk moeten de kunstkenners voor een antwoord op deze vraag ook beschikken over een grote hoeveelheid theologische kennis.

### 5.1 Biologische geïnspireerd onderzoek

Het voorbeeld van de kunstmatige kunstkenner illustreert de kracht van biologisch geïnspireerd AI-onderzoek. Onze conclusie is dan ook dat de combinatie van biologisch plausibele kenmerken en leertechnieken, zoals neurale netwerken, in de toekomst een kunstmatig perceptueel intelligent systeem gaat opleveren dat kunstexperts kan ondersteunen bij hun analyse van schilderijen.

Een vraag van een geheel andere orde is tenslotte de eenvoudige vraag: vind je een schilderij mooi? Kan een computer daar ook iets zinnigs over zeggen? Laten we er dit van zeggen. Als een computer criteria heeft (geleerd) dan kan het deze criteria toepassen en is een waardering niet zo moeilijk te geven. Je zou in het slechtste geval kunnen zeggen dat de waardering idiosyncratisch is, maar als AI-onderzoeker willen we natuurlijk graag dat de waardering is verankerd in ons gevoel van esthetiek. Daarvoor zullen we nog een lange onderzoeksweg moeten afleggen.

## 6. Conclusie

Kunst en kunstmatige intelligentie hebben een gediversifieerde relatie met het cultureel erfgoed. Enkele gebieden zijn fundamenteel van aard (compositie en thema), andere hebben een meer praktisch karakter (kleuren en herhaling van patronen) en nog weer andere hebben een

duidelijk gericht toepassingsgebied (penseelstreek). Het cultureel erfgoed is een betrekkelijk nieuw toepassingsgebied, met name als dit vergeleken wordt met Recht en Informatica, als ook met Medische Informatica. Voor kunstmatige intelligentie en het cultureel erfgoed is in de samenleving evenwel een bijzondere positie weggelegd, immers dit erfgoed is ons spoor uit de historie dat ons de weg naar de toekomst wijst

## 7. Dankwoord

De auteurs bedanken het Van Gogh museum voor het beschikbaar stellen van hoogwaardige reproducties van schilderijen uit hun collectie. Het *Authentic*-onderzoek wordt gesubsidieerd door de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) in het kader van het Token-programma (subsidie 634.000.015).

## 8. Noten

1. Het *Authentic* project is een samenwerkingsverband met de Technische Universiteit Delft (prof.dr.ir. E. Backer, dr.ir. J.C.A. van der Lubbe, en A.I. Deac, M.Sc.)
2. Ondanks onderzoek hebben wij de rechthebbenden van het auteursrecht op 'De Emmausgangers' van Van Meegeren nog niet weten te traceren. Mocht u rechthebbende zijn, neemt u dan a.u.b. contact met ons op, op redactie@ziedaar.nl.

# Kansloos: van Willem Ruis tot Lucia de B.

Peter Grünwald

Centrum Wiskunde & Informatica

Postbus 94079, 1090 GB Amsterdam

homepages.cwi.nl/~pdg

### *1.1 Kansloze Situaties*

Uitspraken van de vorm "deze gebeurtenis heeft *X* procent kans" zijn in de praktijk vaak betekenisloos. In veel alledaagse situaties kan men eigenlijk niet spreken van "kansen", hoewel de meeste mensen (inclusief wiskundigen!) dit vaak wel doen. Deze voordracht gaat over dit soort "kansloze situaties," die ik bespreek aan de hand van drie voorbeelden:

-Het 3-Gevangenen Probleem. Een wiskundige puzzel die laat duidelijk laat zien dat een eenduidige "kans" soms niet bestaat (Sectie 2).

-Het 3-Deuren Probleem. Een, veel bekendere, wiskundige puzzel die laat zien dat onze intuitie hierover vaak verkeerd is (Sectie 3).

-Het 1-Gevangene Probleem. Dit is geen wiskundig maar een maatschappelijk probleem dat thans in Nederland speelt. Het laat zien dat onze pogingen om over "kansen" te praten als die er niet zijn, desastreuze gevolgen kunnen hebben! (Sectie 4)

Voordat ik begin, zal ik even uw geheugen opfrissen met betrekking tot kansrekening.

### *1.2 De Dobbelsteen – Conditionele Kansen*

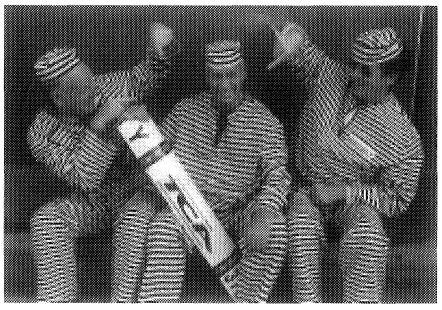
Stel ik gooi met een eerlijke dobbelsteen; ik zie de uitkomst (een getal tussen 1 en 6) maar u ziet de uitkomst niet. Ik vertel u ofwel "*de uitkomst is even*" ofwel "*de uitkomst is oneven*". Stel dat ik u vertel "de uitkomst is even." Wat is volgens u dan de kans dat er "4" is gegooid? U zegt: er zijn nog drie mogelijkheden over. Die hebben allemaal gelijke kans, dus: **de kans op**

**"4" is nu 1/3.**

Dat is een correcte redenering. Eerst was de kans 1/6. U past deze kans aan omdat u nieuwe informatie heeft; dit heet **conditioneren**. De kans is nu 1/3 geworden. We zeggen: "de *conditionele* kans op "X=4", *gegeven* dat "X is even", is 1/3". (in het Nederlands wordt meestal trouwens van 'voorwaardelijke kansen' in plaats van 'conditionele kansen' gesproken. Ik houd het bij 'conditioneel' omdat ik het woord 'conditioneren' veel ga gebruiken)

## 2. Het Drie Gevangenen Probleem (1959)

Dit probleem duikt voor het eerst op in de literatuur in 1959, in de column van Martin Gardner in de *Scientific American*. Het gaat als volgt. Er zijn drie gevangenen, **A**, **B** en **C**. Twee van hen worden willekeurig uitgekozen en zullen worden terechtgesteld. De gevangenen weten dit. Bijvoorbeeld, A wordt met kans 2/3 geëxecuteerd, dus hij overleeft met kans 1/3. Rita, de cipier, komt langs.



A vraagt haar of zij misschien kan zeggen of B of C wordt terechtgesteld. De cipier zegt: *B.* Wat is nu de nieuwe kans dat A wordt terechtgesteld?

We kunnen hier op twee manieren naar kijken. In eerste instantie lijkt het alsof de cipier geen nieuwe informatie geeft over A's overlevingskans geeft. A wist toch al dat B of C zou worden terechtgesteld. Dus volgens deze redenering blijft de kans dat A overleeft 1/3.

De tweede manier om ernaar te kijken is te gaan conditioneren. Het blijkt dat met conditioneren, de kans ineens omhoog springt naar 1/2! Er waren nl. eerst *drie mogelijkheden* met gelijke kans: A overleeft, B overleeft, C overleeft. Nadat de cipier zegt "B wordt terechtgesteld," zijn er nog *twee mogelijkheden* over: A overleeft, C overleeft. Dus de kans dat A overleeft is nu 1/2 !

Als ik lezingen over dit onderwerp geef, dan richt ik mij op dit moment altijd tot het publiek met de vraag of iedereen die denkt dat conditioneren (antwoord 1/2) hier correct is, zijn hand wil opsteken. Laatst stak zo'n 10% van de zaal zijn hand op. Helaas is conditioneren hier verkeerd! Om dit in te zien, hoeven we alleen maar te bedenken dat als de cipier C in plaats van B had geantwoord, we met conditioneren ook op 1/2 waren gekomen. Dus: A stelt een vraag, en *wat het antwoord op die vraag ook is*, nadat hij het antwoord heeft gehoord gaat de kans dat hij het overleeft omhoog. Dat kan niet goed zijn! Conditioneren geeft blijkbaar niet altijd het juiste antwoord.

Ik vraag vervolgens aan het publiek wie er denkt dat het eerste antwoord (kans blijft 1/3) correct is. Nu steekt soms wel zo'n 20% van het publiek zijn hand op. Bij nader inzien is dat ook niet helemaal goed, alhoewel het hier subtieler ligt.

Het juiste antwoord is: *je kunt niet meer zeggen wat de kans is*, tenzij je extra aannames doet over de psyche van de cipier. Om dit uit te leggen kan ik het beste eerst even teruggaan naar het dobbelsteenverhaal.

## *2.1 Dobbelstenen en Correcte Kansuitspraken*

Net als zojuist gooi ik met een eerlijke dobbelsteen die u niet ziet. Ik vertel u ofwel "de uitkomst lag *tussen 1 en 3*" ofwel "de uitkomst lag *tussen 4 en 6*". Ik vraag u wat de kans op '4' is. U bepaalt het antwoord door te conditioneren. Als ik zeg "tussen 1 en 3," dan zegt u: "de kans op '4' is 0". Als ik zeg "tussen 4 en 6," dan zegt u: "de kans op '4' is 1/3". Dit is geheel correct. Maar *waarom* is het eigenlijk correct? Wat voor uitspraak doet iemand eigenlijk over de wereld om hem heen als hij of zij zegt "de kans op 4 is 1/3"? Om dat te zien doen we een gedachtenexperiment: we gaan hetzelfde spelletje 6000 keer herhalen. Omdat we ervan uitgaan dat de munt eerlijk is, zal ik ongeveer 3000 keer zeggen "tussen 4 en 6". In ongeveer 1000 van die 3000 gevallen (1/3 dus) is de uitkomst '4'.

Dus, en dit is de clou van het het verhaal: de uitkomst is '4' *in ongeveer 1 op de 3 van de gevallen waarin u* **zegt** *"de kans op '4' is 1/3."* We kunnen dan zeggen dat uw kansuitspraak "correct" is: als we de situatie waarin u de uitspraak doet voldoende vaak herhalen, en de onderliggende aannames (eerlijke dobbelsteen) kloppen, dan zal de waargenomen

frequentie van een uitkomst ongeveer gelijk zijn aan de kans die u heeft vermeld.[1] In dit voorbeeld "werkt" conditioneren dus, omdat het tot correcte kansuitspraken leidt. Ik geef nu echter een soortgelijk voorbeeld waarin conditioneren *niet* werkt.

### *2.2 Dobbelstenen en Correcte Kansuitspraken – Vers 2*

Stel, we spellen het bovenstaande spel, maar ik vertel u nu ofwel "de uitkomst lag *tussen 1 en 4* " (in plaats van: tussen 1 en 3, zoals net) ofwel "de uitkomst lag tussen 4 en 6". Ik vraag u nu de kans op '4' te bepalen. U bepaalt deze kans wederom door te conditioneren. Dus als ik zeg "tussen 4 en 6" zegt u nog steeds: de kans op "4" is 1/3. Stel nu dat we deze variatie van het spel vaak herhalen. Het verschil met de vorige situatie is dat ik thans, steeds als de uitkomst 4 is, een ***keuze*** heb in wat ik u ga vertellen. Ik kan het bijvoorbeeld zo doen: als de uitkomst 4 is zeg ik altijd "tussen 1 en 4" en *nooit* "tussen 4 en 6." Als we het spelletje 6000 keer spelen, zal ik dan ongeveer 2000 keer "tussen 4 en 6" zeggen. Elk van die keren zult u zeggen: "de kans op 4 is 1/3", maar in werkelijkheid zal van al die keren de uitkomst geen enkele keer 4 zijn. Uw uitspraak "kans op 4 is 1/3" is dan dus *niet* correct; in dit geval had u moeten zeggen '0', dus conditioneren geeft het verkeerde antwoord. Maar het echte probleem ligt niet bij conditioneren. Er bestaat in feite geen enkele methode om uw kansen aan te passen die wel altijd het juiste antwoord geeft. Immers, ik zou zelf ook een eerlijk muntje kunnen gooien als de daadwerkelijke uitkomst 4 is. Bij kop zeg ik "tussen 1 en 4", en bij "munt" zeg ik "tussen 4 en 6." In dat geval zal ik ongeveer 2500 keer "tussen 1 en 4" zeggen, en ongeveer 500 van die keren zal de uitkomst "4" zijn. De "correcte" kans is dan dus 1/5. Ik kan ook met een valse munt gooien om te bepalen wat ik ga zeggen, en op deze manier kan ik iedere frequentie tussen 0 en 1/3 bereiken. Ik zou de keuze ook af kunnen laten hangen van de kleur van de eerstvolgende auto die ik buiten langs zie rijden, of wat dan ook. Het is duidelijk: als u niet weet op wat voor manier ik de keuze maak wat ik u ga vertellen telkens als de daadwerkelijke uitkomst 4 is, dan is het voor u onmogelijk om een correcte kans te bepalen, met wat voor methode dan ook. We zouden ook kunnen zeggen: een "correcte" kans bestaat nu niet meer,

---

[1] Er zijn veel toepassingen van kansrekening waarbij het subtieler ligt, maar daar zal ik hier verder niet op ingaan.

tenzij we bereid zijn extra aannames te doen. Een uitspraak als "de kans is X", voor wat voor X dan ook, is potentieel geheel verkeerd, of zelfs betekenisloos, tenzij X een interval in plaats van een getal is, of tenzij er bij verteld wordt wat voor aannames gedaan worden over de keuzes die ik maak.

### *2.3 Terug naar de Drie Gevangenen – Keuze en Overlap*

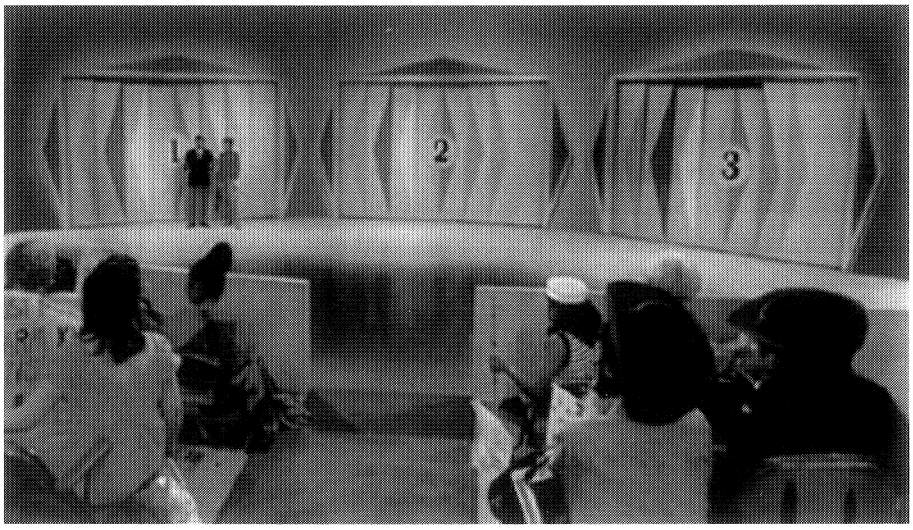
Ook het 3-gevangenen probleem wordt veroorzaakt doordat de cipier (soms) een **keuze** heeft in wat zij gaat vertellen. Als A overleeft (B en C worden geëxecuteerd), kan de cipier kiezen of zij B of C zegt. De echte kansen zijn wederom niet te bepalen als men niet weet wat voor strategie de cipier dan volgt. Als de cipier een eerlijk muntje gooit om te kiezen of zij B of C zegt, dan blijft A's overlevingskans 1/3, wat ze ook zegt. Vandaar dat sommigen wel iets voelen voor het antwoord 'de kans blijft 1/3': daarin zit de impliciete aanname dat de keuze van de cipier onafhankelijk is van de daadwerkelijke uitkomst. Toch is het niet goed om zomaar te zeggen '1/3'; wel goed is om te zeggen: '*als* ik ervan uitga dat de keuze van de cipier onafhankelijk is van de daadwerkelijke uitkomst, *dan* geeft zij A geen informatie en blijft de kans 1/3'.

Kort samengevat: u kunt uw kansen alleen aanpassen aan nieuwe informatie als er geen mogelijke *overlap* zit in de informatie die u kunt krijgen, zodat de persoon of machine van wie u de informatie krijgt, nooit een keuze kan maken. In dat geval dient u de kansen aan te passen door te conditioneren. Als er wel mogelijke overlap is, dan zijn de kansen in feite niet meer goed gedefinieerd, en bestaat er geen enkele correcte methode om uw kans aan te passen.

## 3. Het Drie Deuren (Quizmaster) Probleem (+/- 1970)

U doet mee aan een televisiequiz. In de studio zijn drie deuren. Achter één deur staat een auto, achter beide andere deuren een geit. Het spel gaat als volgt: U gaat voor een van de deuren staan. Monty Hall, de quizmaster, opent een van de twee

andere deuren, en laat zien dat er een geit achter zit. U mag nu blijven staan, of wisselen naar de de deur die nog dicht is. Vervolgens doet Monty de deur open waar u uiteindelijk voor bent gaan staan. Uw prijs is wat er achter die deur zit. U hoopt natuurlijk dat het de auto is. De vraag is nu: *is het verstandig om te wisselen nadat Monty Hall een deur met een geit erachter heeft opengemaakt?* We gaan er hierbij vanuit dat u zelf de eerste deur willekeurig hebt gekozen, en dat Monty (die weet waar de auto is) vervolgens hoe dan ook een deur met een geit zal openen.




Het blijkt dat veranderen van deur *zeer verstandig* is. Grofweg gezegd verhoogt u hiermee uw winstkansen van 1/3 tot 2/3. Vrijwel alle mensen, inclusief de meeste wiskundigen, denken echter in eerste instantie dat het niets uitmaakt of u van deur wisselt of niet! Voor beide dichte deuren geldt immers dat de kans dat de prijs erachter zit, gelijk is?

Een variant van het 3-deuren spel werd daadwerkelijk gespeeld in de quiz *Let's Make a Deal!* die in de jaren '60 en '70 heel populair was in de VS, en die, inderdaad, gepresenteerd werd door ene Monty Hall. Het schijnt dat hetzelfde spel ook op de Nederlandse televisie te zien was, in de Willem Ruis show, rond 1980. In 1990 beweerde Marilyn Vos Savant (volgens aanhoudende geruchten de "vrouw met het hoogste IQ ter wereld") in haar column in het tijdschrift *Parade* dat het veel beter was om van deur te verwisselen. Meer dan 10000 lezers reageerden op deze column met de opmerking dat Vos Savant

natuurlijk ongelijk had. Onder deze briefschrijvers waren meer dan honderd wiskundehoogleraren. Ook Paul Erdös, een van de grootste wiskundigen van de 20e eeuw, weigerde te geloven dat Vos Savant gelijk had. Er zijn hele boeken over het probleem geschreven (zie bijvoorbeeld G. von Randow, *Das Ziegenproblem,* Rowohlt 1992). Toch: hoewel er wel wat aan te merken valt op de analyse van Vos Savant, is haar conclusie volkomen correct: in dit spel is het beter om van deur te verwisselen.

Het grappige is dat, wiskundig gezien, het 3-gevangenen probleem en het 3-deuren probleem equivalent zijn. Net als bij het 3-gevangenen probleem zijn er in het 3-deuren probleem drie mogelijkheden: A, B en C. (A betekent hier dat de auto achter deur A zit; B betekent dat de auto achter deur B zit, en C dat de auto achter C zit). Stel u gaat voor deur A staan. Net als Rita geeft Monty u dan als informatie dat ofwel B niet het geval is, ofwel C niet het geval is ('B is niet het geval' betekende eerst 'B overleeft niet', en nu 'geen auto achter deur B'). Stel dat Monty B zegt. Wanneer u denkt dat het nu niets uitmaakt of u voor A blijft staan of naar C gaat, komt dat omdat u (misschien onbewust) conditioneert: er waren eerst drie mogelijkheden met gelijke kans, A, B en C. Daarvan zijn er twee over, A en C. Die hebben dus nog steeds gelijke kans. Die kans is dus 1/2, en het maakt dus niet uit. We hebben al gezien dat deze redenering verkeerd is. *Het gekke is dat vrijwel iedereen – wiskundige of niet – bij het 3-gevangenen probleem de juiste intuitie heeft (nl.: conditioneren werkt niet) terwijl bij het 3-deuren probleem vrijwel iedereen de verkeerde intuitie heeft (nl. conditioneren werkt wel).* Dit voorbeeld laat nog eens duidelijk zien hoezeer onze intuitie bepaald wordt door de manier waarop we een en hetzelfde wiskundige probleem "verpakken." Het probleem kan zodanig verpakt worden dat bijna iedereen de verkeerde intuitie heeft.

### *3.1. Een Complicatie*

*"Maar wacht nou eens even!"* zult u nu misschien zeggen: de les van het 3-gevangenen probleem was nou juist dat, nadat de cipier B of C heeft gezegd, de kans op A eigenlijk niet meer gedefinieerd is, of in ieder geval, niet bepaald kan worden. Waarom kan men dan wèl zo'n stellige kansuitspraak doen in het equivalente drie-deuren probleem? We zeiden immers:

"de kans om te winnen als men van deur verwisselt, is gelijk is aan 2/3." *(Uitspraak I)*

Dit lijkt hetzelfde als de uitspraak:

"de kans dat de auto achter C zit nadat de quizmaster deur B heeft geopend, is 2/3; de kans dat de auto achter A zit, is nu dus 1/3." *(Uitspraak II)*

Maar in het 3-gevangenen probleem hadden we juist gezegd dat, nadat Rita 'B' heeft gezegd, de uitspraak 'de kans op A blijft 1/3' *verkeerd* is, omdat de echte kans van Rita's keuzes afhangt, en dus niet meer te bepalen is. Hoe zit dat nou?

Het antwoord is subtiel: stel dat we *voordat* Monty Hall de eerste deur open doet, al bepalen dat we de volgende strategie gaan gebruiken: we kiezen eerst een willekeurige deur uit, zodat elke deur met kans 1/3 gekozen wordt. Vanaf dat moment noemen we de deur waar we voor staan deur A. Van de twee andere deuren moet er eentje verder naar links staan dan de andere. Die noemen we deur B; en de overgebleven deur noemen we deur C. Nu zal Monty dus of deur B of deur C openmaken en een geit laten zien. Welke deur Monty ook open maakt, wij gaan van deur veranderen en kiezen de overgebleven deur.

Het is eenvoudig in te zien dat, als we het spel 3000 keer herhalen, en we volgen steeds bovenstaande strategie, we ongeveer 2000 van de 3000 keer zullen winnen. Dus de kans dat we *winnen* is inderdaad 2/3: uitspraak I, het antwoord van Vos Savant is correct. Maar toch is uitspraak II *niet* correct. Deze uitspraak impliceert namelijk dat, wanneer we het spel

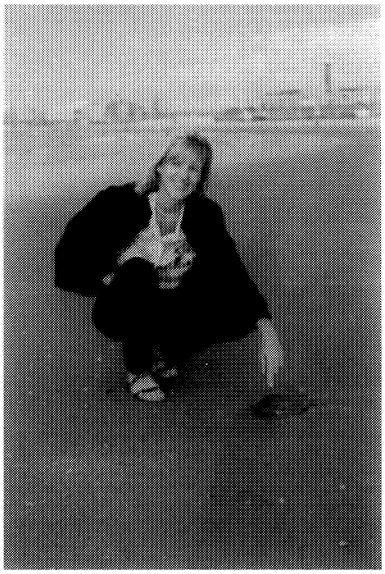
herhaaldelijk spelen, *ongeveer 2/3* **van de keren dat Monty deur B opendoet**, *de auto achter deur C zit.* En dit hoeft helemaal niet waar te zijn: Monty zou bijvoorbeeld altijd de meest rechts gelegen deur waarachter nog een geit zit open kunnen doen (dus als de auto achter A zit, en Monty dus kan kiezen tussen B en C, zal hij altijd deur C kiezen). In dat geval zal *iedere* keer dat Monty deur B opendoet, de auto achter deur C zitten. Het verschil tussen uitspraak I en uitspraak II is dat uitspraak I alleen iets zegt over het aantal keren dat we winnen op het *totaal* aantal keer dat we spelen; bij de strategie van altijd wisselen hangt de vraag of deze uitspraak correct is niet af van de door de quizmaster gemaakte keuze. Uitspraak II zegt ook iets over het aantal keren dat er iets gebeurt *in de gevallen waarin quizmaster deur B opent.* Dit hangt wel af van de door de quizmaster gemaakte keuze, en we kunnen er niet een bepaalde vaste kans aan toekennen.

*Terzijde I.* We hebben betoogd dat conditioneren in het drie deuren probleem niet werkt omdat de quizmaster (soms) een *keuze* heeft in wat hij ons vertelt. Een van de gangbare verklaringen waarom het antwoord 'de kans is 1/2' verkeerd is, is echter juist dat we in 2/3 van de gevallen in eerste instantie voor een geit staan en daarom de quizmaster *dwingen* om de enige andere deur met een geit erachter open te maken, en daarmee aan ons te signaleren dat de auto zich achter de overgebleven deur bevindt. Volgens deze redenering lijkt conditioneren juist niet te werken doordat de quizmaster in 2/3 van de gevallen *geen* keuze heeft. Dit lijkt in tegenspraak met de eerdere overweging. Bij nadere beschouwing verdwijnt de tegenspraak echter. Het is eenvoudig aan te tonen dat conditioneren altijd werkt (in de zin dat frequenties, bij veelvuldige herhaling van een experiment, ongeveer gelijk zijn aan de kansen) als degene die de informatie verstrekt *nooit* een keus heeft wat hij/zij gaat vertellen. Het is ook eenvoudig aan te tonen dat conditioneren altijd werkt als degene die de informatie verschaft *altijd* de keus heeft uit 2 berichten, en *altijd* met een eerlijke munt gooit om te bepalen wat hij gaat vertellen. In het 3-deuren probleem heeft Monty *soms* een keus tussen deur B en C (als de auto achter deur A staat), en *soms* geen keus (als de auto achter B of C staat). Deze situatie van soms wel, soms geen keuze is precies het geval waarin conditioneren niet werkt - zelfs als Monty "eerlijk" is en, als de auto achter A staat, met een eerlijke munt gooit om tussen B en C te kiezen.

*Terzijde II.* We hebben laten zien dat, als Rita of Monty ons vertellen dat B *niet* het geval is, de conclusie 'de kans op A blijft 1/3' inderdaad niet correct is. Toch suggereert bovenstaande analyse dat de uitspraak "de kans op A blijft 1/3" op de een of andere manier wel iets "beter" is dan de uitspraak "de kans op A wordt 1/2". Dit kan men volgens mij inderdaad hard maken, maar dit vereist een niet-standaard wiskundige definitie van het begrip 'kansverdeling'. De gebruikelijke definitie wordt dan een speciaal geval. Dit is een onderzoeksvraag waar ik thans aan werk. Een eerste aanzet in deze richting is gegeven in het paper *When Ignorance is Bliss (Proceedings UAI 2004)* dat ik samen met Joe Halpern (Cornell) heb geschreven. Het vervolgpaper belooft spannend en hoogst controversieel te worden!

# 4. Het ÉÉN Gevangene Probleem (2001-heden)

In 2004 werd verpleegkundige **Lucia de B.** in hoger beroep veroordeeld tot levenslang voor *7 moorden en 3 pogingen tot moord*. Zij heeft nooit schuld bekend.Ton Derksen, auteur van het *boek Lucia de B., Reconstructie van een gerechtelijke dwaling* heeft de zaak aangekaart bij de Commissie Post-humus-II (evaluatie afgesloten strafzaken). Deze commissie heeft drie wijze mannen aangesteld, die in oktober 2007 adviseerden dat de zaak inderdaad diende te worden her-opend. Vervolgens heeft de hoge raad zelf ook onderzoek laten doen. Op 2 april 2008 adviseerde de Procureur-Generaal van de Hoge Raad de zaak te heropenen, en werd Lucia de B. (na meer dan zes jaar gevangenis) voorlopig vrijgelaten. De uiteindelijke beslissing of de zaak wel of niet heropend wordt, wordt in zomer 2008 verwacht.



In deze zaak heeft statistiek een cruciale rol gespeeld.[2] Er zijn in de statistische analyse een aantal fouten gemaakt. Zoals we zullen zien is een van de belangrijkste fouten dat er van een 'kans' wordt gesproken in een situatie waarin dat eigenlijk niet kan – de kans is dus betekenisloos, net als in het 3-gevangenen probleem.

Lucia werkte op de Medium Care Unit van het Juliana Kinder-ziekenhuis (JKZ) in Den Haag. Er waren veel meer "incidenten" (plotselinge sterfgevallen en reanimaties) wanneer Lucia wel dienst had, dan wanneer Lucia geen dienst had. Op deze manier is de eerste verdenking gerezen: dat kon toch geen toeval zijn!?!?

Het hof vroeg een statisticus om de gegevens nader te analyseren. Deze statisticus berekende dat de kans dat een verpleegkundige bij toeval een dergelijk incidenten-patroon zou meemaken, kleiner is dan 1 op 342.000.000. Hij trok hieruit de conclusie dat het geen toeval kon zijn. Ik moet er meteen bijzeggen dat hij benadrukte dat dit *niet* betekent dat Lucia een moordenaar is. Ter illustratie geeft de statisticus een aantal mogelijke alternatieve verklaringen, zoals 'het zou bijvoorbeeld kunnen dat Lucia vaker nachtdiensten draait, en dat 's nachts meer patienten sterven'. Het hof schrijft echter in zijn arrest (11.13):

---

[2] *Officieel* heeft statistiek 'in de vorm van kansberekeningen' geen rol gespeeld in het hoger beroep. Maar wie het arrest en de getuigenverklaringen bekijkt ziet wel degelijk een aantal (foutieve) statistische redeneringen. Dat blijkt al uit het citaat uit het arrest op deze pagina. Het boek van Derksen bevat hier nog vele andere voorbeelden van. Ik geef er hier slechts een: bij een van de "vermoorde" patienten is aan zes medische experts gevraagd of het om een natuurlijke dood ging. Vijf van de zes dachten van wel. De *enige* expert die dacht dat het niet om een natuurlijke dood ging, is dezelfde arts die oorspronkelijk een natuurlijke dood-verklaring had afgegeven. Maar aan die niet-natuurlijke dood dacht hij pas vier jaar later, zoals hij zelf verklaart, nadat "in de media aandacht werd besteed aan onverklaarbare sterfgevallen in de diverse Haagse ziekenhuizen". Het hof volgt deze laatste expert, die zich duidelijk heeft laten leiden door de statistische redenering dat zoveel onverklaarbare sterfgevallen 'geen toeval kunnen zijn.'

*Er is geen enkele aannemelijke verklaring gevonden voor het feit dat de verdachte in die korte periode bij zoveel overlijdens gevallen en levensbedreigende incidenten betrokken was.*

Verderop in het arrest lezen we dat dit als belastend feit voor de verdachte wordt gezien. Dit speelt een belangrijke rol in de bewijsvoering. Het hof gebruikt dus wel degelijk statistiek – hoewel er geen getal genoemd wordt, wordt de statistische conclusie 'het kan geen toeval zijn' wel degelijk overgenomen (als het wel gewoon toeval kan zijn, is het niet vreemd dat er geen verklaring wordt gevonden voor de aanwezigheid van de verdachte bij al die incidenten, en kan de aanwezigheid op zich zeker niet als belastend worden gezien). Helaas blijft er bij nadere analyse niets over van de conclusie "het kan geen toeval zijn".

De statisticus deed een "nulhypothese toets" met significantie-niveau 1/10000. Dit is een standaard statistische methode. In grote lijnen werkt het als volgt: we formuleren eerst een zogenoemde 'nulhypothese' en een 'alternatieve' hypothese. In dit geval was de nulhypothese 'Lucia heeft dezelfde kans om een incident mee te maken als andere verpleegkundigen'. De alternatieve hypothese is 'Lucia heeft een hogere kans om een incident mee te maken als andere verpleegkundigen'. We kijken nu wat de kans[3] is op de daadwerkelijk geobserveerde gegevens als de nulhypothese waar zou zijn. Als die zgn. *overschrijdingskans* kleiner is dan het gekozen significantie-niveau (in dit geval, 1 op 10000), dan verwerpen we de nulhypothese. Stel bijv. dat er 10 incidenten waren in de tijd dat Lucia op de afdeling werkte, en dat Lucia bij 8 incidenten aanwezig was. Dan berekenen we de kans dat Lucia 8 *of meer* van die 10 incidenten meemaakt onder de aanname dat Lucia

---

[3] We moeten hierbij heel voorzichtig zijn. We mogen niet zomaar de kans op de gegevens berekenen, want *elke* verzameling gegevens heeft uiteindelijk een hele kleine kans. Als we 10 keer met een eerlijke dobbelsteen gooien, dan heeft de uiteindelijke reeks die we gooien een kans van (1/6) tot de macht 10, vele malen kleiner dan 1 op 10000. Dit geldt altijd, welke reeks we ook gooien. We mogen hieruit natuurlijk niet concluderen dat de dobbelsteen vals is! Bij een nulhypothese toets bepalen we daarom niet de kans op de gegevens zelf , maar een zgn. *overschrijdingskans*. Dit is de kans op een speciaal gekozen *eigenschap* van de gegevens, waarbij die eigenschap aan bepaalde voorwaarden moet voldoen. Bij de dobbelsteen kunnen we bijv. kijken naar het gemiddeld aantal ogen. Als we waarnemen dat dat 4.5 in plaats van de verwachte 3.5 is, en de kans op een aantal ogen van 4.5 *of hoger* is kleiner dan 1 op 10000, dan kunnen we wel degelijk concluderen dat de dobbelsteen vermoedelijk niet eerlijk is. In het geval Lucia kijken we naar de (overschrijdings-) kans op *evenveel of meer incidenten* dan Lucia heeft meegemaakt.

een evengrote kans heeft op een incident als andere verpleegkundigen. De statisticus vond dat de kans dat Lucia evenveel of meer incidenten meemaakte, dan zij daadwerkelijk meemaakte, kleiner was dan 1 op 342 miljoen. Dat is veel kleiner dan 1 op 10000. Daarom verwerpt hij de hypothese "Lucia heeft dezelfde kans op incidenten als andere verpleegkundigen," en hij concludeert hieruit "wat er gebeurd is, is geen toeval."

### *4.1 "De" kans bestaat niet*

Hoe werkt nulhypothese toetsen nou precies? De methode zit zo in elkaar, dat, als een statisticus hem herhaaldelijk (en correct) zou toepassen, dan zou gelden dat de statisticus gemiddeld maximaal 1 op 10000 keer *zegt* "dat kan geen toeval zijn" terwijl het wèl toeval is. Hij doet zo'n verkeerde uitspraak dus gemiddeld maximaal 1 op de 10000 keer dat hij de toets toepast. We kunnen bij een goed uitgevoerde hypothese toets trouwens *niet* zeggen (a) dat maximaal 1 op de 10000 keer dat er sprake is van toeval, er geconcludeerd wordt dat het geen toeval is; we kunnen alleen zeggen dat (b) maximaal 1 op de 10000 keer van alle keren dat de toets wordt toegepast, we in de situatie zitten dat het wel toeval is, maar dat we zeggen van niet. Het verschil tussen (a) en (b) is dat we, bij de definitie van "keer", in (a) kijken naar alleen die toetsen waarbij het in werkelijkheid toeval is, en bij (b), naar alle toetsen, of het nou in werkelijkheid wel of geen toeval is.

Helaas is de nulhypothese toets in het geval Lucia niet correct toegepast, en *kan* hij ook helemaal niet correct toegepast worden. Dat zien we meteen als we ons gaan afvragen *wat "herhaaldelijk toepassen" hier zou moeten betekenen.*

Herhalen we de berekening, en doen we de uitspraak 'wel/geen toeval'

1. ieder jaar, voor elke verpleegkundige *in het Juliana Kinderziekenhuis?*
2. ieder jaar, voor elke verpleegkundige *in Nederland/in Europa/op de wereld*?
3. elke keer als een verpleegkundige *in het Juliana Kinderziekenhuis* zoveel sterfgevallen meemaakt dat het nader onderzocht dient te worden?

4. elke keer als een verpleegkundige *ergens in Nederland/in Europa/op de wereld* zoveel sterfgevallen meemaakt dat het onderzocht dient te worden?
5. of telkens als er een *rechtzaak* is waarin het Openbaar Ministerie van een nulhypothese toets gebruik maakt?

Dit is volstrekt onduidelijk. En als we de berekening proberen aan te passen aan de drie gevallen hierboven, komen we in alle drie de gevallen op volledig verschillende getallen uit. Met andere woorden: zonder een precieze *context* aan te geven, is de uitspraak "het kan geen toeval zijn want de kans is 1 op 342 miljoen" simpelweg *betekenisloos*. Net als in het 3-gevangenen probleem is dit een 'kansloze situatie' waarin we niet, of in ieder geval niet zonder meer, van kansen kunnen spreken. In het hoger beroep is de rechter hierop expliciet geattendeerd door de hoogleraren M. Van Lambalgen (logica) en R. Meester (kansrekening), die optraden als deskundigen van de verdediging. Maar de rechter wilde hier niet aan, en bleef maar vragen 'als u het niet met de statisticus E. eens bent, wat is volgens u de kans dan wèl?'

Normaalgesproken worden nulhypothese toetsen toegepast in situaties waarbij de nul- en alternatieve hypothese van te voren geformuleerd worden, en getest worden op nieuwe, onafhankelijk verkregen gegevens. Er wordt bijvoorbeeld een speciaal experiment opgezet om die gegevens te verkrijgen. Als men dit zorgvuldig doet, dan kan men garanderen dat *gemiddeld van alle keren dat iemand, in wat voor context dan ook, een nulhypothesetoets* **correct** *uitvoert, de nulhypothese maar 1 op de 10000 keer onterecht verworpen zal worden.* De verschillende toetsen hoeven niet over hetzelfde fenomeen te gaan: sommige van die 10000 toetsen kunnen bijvoorbeeld gaan over een nieuw geneesmiddel, andere over de levensduur van gloeilampen of wat dan ook; als we alle toetsen bij elkaar nemen, dan kan de 1 op 10000 garantie toch gegeven worden. Maar zo een domein-onafhankelijke garantie kan alleen gegeven worden als de toetsen op nieuwe gegevens worden toegepeast. In het geval van Lucia wordt de nulhypothese echter getoetst aan dezelfde data waardoor hij gesuggereerd is. Dan kan de 1 op 10000 garantie alleen gegeven worden als bekend is in wat voor context de toets uitgevoerd wordt, en als die context niet bekend is, is de uitkomst van de toets feitelijk

betekenisloos.[4]

Het voorgaande suggereert dat de statistische analyse, hoewel die een zeer grote impact heeft gehad, eigenlijk niet zoveel zegt. Wanneer we andere relevante gegevens (beschikbaar ten tijde van de rechtszaak maar genegeerd door het hof) bekijken, dan krijgen we de indruk dat 'de statistiek', zo die überhaupt al iets kan zeggen, Lucia eerder vrijpleit dan verdacht maakt. Het blijkt nl. dat in de drie jaar dat Lucia op de medium care unit van het JKZ werkte, er daar **zes** sterfgevallen waren. *In de drie voordat ze er werkte, waren er **zeven**.* Voor een nadere analyse van wat dit betekent, verwijs ik naar Derksen's boek. Derksen maakt ook aannemelijk dat de gegevens waarop de statisticus zijn analyse baseerde niet betrouwbaar zijn. Verder werd er ook nog een rekenfout gemaakt (vermenigvuldigen van p-waarden). Hiermee blijft er niets, maar dan ook niets van de oorspronkelijke statistiek over.

## Tot Slot

Het zal sommigen van u bekend zijn dat er twee belangrijke stromingen in de statistiek bestaan: enerzijds de orthodoxe of frequentistische school, anderzijds de Bayesiaanse school. Op het Europese continent, en met name in Nederland, is de frequentistische school dominant, en is er weinig Bayesiaans onderwijs: de 'standaard statistiek' zoals men die op de universiteit leert is frequentistisch. In de Angelsaksische wereld is de Bayesiaanse stroming veel groter, zo'n 30% van alle publicaties in statistische toptijdschriften zijn daar "Bayesiaans". Het belangrijkste verschil zit 'm in de interpretatie van kansen:

---

[4] De statisticus E. realiseert zich wel dat er een probleem is, en past daarom een 'post-hoc correctie' op zijn hypothesetoets toe – hij vermenigvuldigt de overschrijdingskans met het aantal verpleegkundigen op Lucia's afdeling. Maar met deze correctie kan nog steeds niet gegarandeerd worden dat maar 1 op de 10000 gevallen onterecht gezegd wordt 'het is geen toeval', omdat nog steeds onduidelijk is wat de context is: 1 op *welke* 10000 gevallen? Elffers correctie zou min of meer overeenkomen met de eerste interpretatie in het lijstje hierboven (we testen iedereen op Lucia's afdeling, elk jaar). Maar, voor zover we uberhaupt iets over de "echte" context kunnen zeggen, lijkt die eerder op interpretatie (4). In dat geval moet de vermenigvuldigingsfactor vele duizenden malen groter worden. Maar hoe groot precies? Het blijft hoe dan ook natte vinger werk – een "kansloze" situatie dus.

zijn kansen denkbeeldige frequenties, die als limiet optreden als een experiment maar vaak genoeg herhaald worden? (frequentistische kijk) Of zijn kansen algemene uitdrukkingen van persoonlijke onzekerheid, die vertaald kunnen worden in de hoeveelheid geld die men maximaal in zou willen zetten in bepaalde weddenschappen (modern-Bayesiaanse kijk). Volgens een frequentist is een uitspraak als 'volgens mij is de kans dat McCain de verkiezingen wint 30%' betekenisloos, omdat het bij de wel/niet-verkiezing van McCain om een niet-herhaalbaar experiment gaat. Volgens een Bayesiaan kan er wel degelijk een betekenis aan worden gegeven. Omdat in mijn uitleg gebaseerd was op frequentistische overwegingen, kan de indruk ontstaan dat ik Bayesiaanse kansen voor betekenisloos houd. Dat is zeker niet het geval. Zoals (tegenwoordig) de meeste statistici, denk ik dat Bayesiaanse kansen onder sommige omstandigheden wel degelijk zinvol gebruikt kunnen worden. De Bayes-frequentistisch discussie is in feite onafhankelijk van het punt dat ik hier gemaakt heb. Waar het mij hierom gaat is dat soms aan een gebeurtenis geen *puntkans* gegeven kan worden, maar alleen bijv. een interval van kansen, en dat soms zelfs alleen gezegd kan worden dat interval gelijk is aan [0,1]. Dit geldt zowel voor persoonlijke, Bayesiaanse, als voor empirisch gegronde frequentistische kansen.

## Colofon

Deze voordracht is een variatie op een lezing gehouden 12-12 2006, ter ere van het 60-jarig bestaan van het Centrum voor Wiskunde en Informatica (CWI) te Amsterdam.

# Literatuur

P.D. Grünwald and J. Halpern. When ignorance is bliss. *Proceedings of the Twentieth Annual Conference on Uncertainty in Artificial Intelligence (UAI 2004)*, Banff, Canada, July 2004 (beschikbaar via mijn homepage)

P.D. Grünwald and J. Halpern. Updating probabilities. *Journal of Artificial Intelligence Research (JAIR)* 19, pages 243-278, 2003 (beschikbaar via mijn homepage; bevat verdere verwijzingen naar literatuur over het quizmaster probleem)

T. Derksen. Lucia de B. Reconstructie van een gerechtelijke dwaling. Veen Magazines, Diemen, 2006.

R. Meester , M. Collins, R. Gill, M. van Lambalgen,. On the (ab)use of statistics in the legal case against the nurse Lucia de B (with discussion by David Lucy) . *Law, Probability and Risk*, 2007.

# RSA

Lenny Taelman
Mathematisch Instituut, Universiteit Leiden

## Inleiding

Dat het geheimschrift niet zo veel jonger is dan het schrift zelf zal weinig verbazen. Het zal in ieder geval duidelijk zijn dat er altijd vraag is geweest naar technieken om vertrouwelijke communicatie af te schermen van ongewenste meelezers. De eerste gebruikte encryptietechnieken waren vrij naïef (en, achteraf gezien, gemakkelijk te kraken), zoals verzender en ontvanger die afspreken 'A' voortaan te schrijven als bijvoorbeeld 'F', en 'B' als 'Z', 'C' als 'O', enzovoort. Meer geavanceerde methoden combineren de geheime boodschap met een van te voren afgesproken hulptekst, zodoende dat de versleutelde boodschap ontcijferd kan worden door eenieder die beschikt over de hulptekst (hopelijk enkel de verzender en ontvanger).

In de twintigste eeuw maakten mechanische en later ook electronische technieken het gebruik van veel ingewikkeldere schema's mogelijk. Doch in feite is er weinig verschil tussen de (handmatige) versleuteling gebruikt in de oudheid en de (mechanische) versleuteling van bijvoorbeeld de Wehrmacht Enigma machine. Voor al deze vercijfertechnieken is het essentieel dat verzender en ontvanger van te voren samen een geheime sleutel (zoals een hulptekst) hebben afgesproken.

Dit lijkt misschien een strikt noodzakelijke voorwaarde om op veilige wijze geheime informatie te communiceren, maar dat is het, verbazend genoeg, helemaal niet. In de jaren zeventig van de twintigste eeuw vond een ware revolutie plaats in de cryptografie met de ontwikkeling van verschillende zogenaamde *publieke sleutel*-methoden. Bij deze methoden bezit de ontvanger een geheime sleutel die hij aan niemand meedeelt, en een publieke sleutel die, zoals de naam doet vermoeden, publiek is: zowel vriend als vijand mogen hem kennen. Een met de publieke sleutel versleutelde boodschap kan enkel met de geheime sleutel worden ontsleuteld. En hoewel in theorie de geheime sleutel uit de publieke berekend kan worden, is dat in de praktijk ondoenbaar, zelfs niet door een vijand die beschikt over miljoenen computers en jaren geduld.

Elk van deze 'publieke sleutel'-systemen maakt op ingenieuze wijze gebruik van wiskunde. Een van de meest elegante methoden is RSA, vernoemd naar haar ontdekkers Rivest, Shamir en Adleman. (Tevens is het een van de in de praktijk meest gebruikte methoden, bijvoorbeeld bij het online versturen van

credit-cardgegevens.) Bij RSA bestaat de geheime sleutel uit twee priemgetallen, elk meer dan honderd cijfers lang, en de publieke sleutel (onder meer) uit het product van deze twee priemgetallen. In principe hoeft men slechts de publieke sleutel te ontbinden in priemfactoren om de geheime sleutel te bemachtigen, doch helaas zal dat met de gekende methoden 'tien tot de heel veel' jaren rekentijd kosten. Deze asymmetrie (vermenigvuldigen van priemgetallen is gemakkelijk, ontbinden in priemfactoren is moeilijk) is fundamenteel voor de werking van RSA.

In deze voordracht zullen we de getaltheorie toelichten die RSA mogelijk maakt, en daarna in detail uitleggen hoe RSA ten werk gaat.

# 1 Machtsverheffen modulo $n$

Laten we even een aantal machten van 3 uitrekenen:

$$\begin{aligned} 3^0 &= 1 \\ 3^1 &= 3 \\ 3^2 &= 9 \\ 3^3 &= 27 \\ 3^4 &= 81 \\ 3^5 &= 243 \\ 3^6 &= 729 \\ 3^7 &= 2187 \\ 3^8 &= 6561 \end{aligned}$$

Er valt meteen op dat het laatste cijfer een periodiek patroon vormt: 1, 3, 9, 7, 1, 3, 9, 7, ... (en het is niet moeilijk te *bewijzen* dat dit inderdaad zo is). We zien dus dat het laatste cijfer van $3^k$ enkel afhangt van $k$ modulo 4, met andere woorden, dat $3^k$ modulo 10 bepaald is door $k$ modulo 4.

Coderen en decoderen in het RSA-systeem is in essentie niets anders dan machtsverheffen modulo het product van twee (grote) priemgetallen, en de periodiciteit van machtsverheffen, zoals in het voorbeeld hierboven, speelt hierin een cruciale rol. In deze sectie gaan we deze bewerking wat nader bekijken.

## 1.1 Machtsverheffen modulo een priemgetal

Hoewel we in het RSA-systeem gaan machtsverheffen modulo het product van twee verschillende priemgetallen, is het handig om eerst te begrijpen wat er gebeurt als we gaan machtsverheffen modulo een priemgetal $p$.

In feite wordt alles hierover gezegd door de beroemde kleine stelling van Fermat (niet te verwarren met de "laatste stelling" die Fermat in 1637 in de kantlijn krabbelde, maar die pas in 1994 door Andrew Wiles bewezen werd):

**Stelling 1.2 (Kleine stelling van Fermat)** *Als $p$ een priemgetal is en $a$ niet deelbaar door $p$, dan geldt*

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

Bijvoorbeeld: $2^6 = 64 \equiv 1 \pmod 7$.

Er zijn verschillende elegante bewijzen van deze stelling, de volgende is misschien de meest bekende:

**Proof 1** *Beschouw de afbeelding*

$$\delta : \{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, p-1\}$$

*gegeven door vermenigvuldiging met a modulo p. Dit geeft wel degelijk altijd een element van* $\{1, 2, \ldots, p-1\}$ *omdat a niet deelbaar is door p. Bovendien is de afbeelding injectief: immers als* $\delta(x) = \delta(y)$*, dus als* $ax \equiv ay \pmod p$ *dan geldt* $a(x-y) \equiv 0 \pmod p$*, dus p deelt* $a(x-y)$*, maar omdat p geen deler is van a volgt dat p een deler is van* $x - y$*, dus dat* $x = y$*. Er volgt meteen dat* $\delta$ *ook surjectief is, want het is een afbeelding tussen eindige verzamelingen met evenveel elementen. In het kort:* $\delta$ *is een* permutatie *van de verzameling* $\{1, 2, \ldots, p-1\}$.

*Nu zijn we met een slim truukje snel klaar, we rekenen uit (alles modulo p):*

$$\begin{aligned} 0 &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) - \delta(1)\delta(2)\cdots\delta(p-1) \\ &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) - a \cdot 2a \cdot 3a \cdots (p-1)a \\ &\equiv (1 - a^{p-1}) 1 \cdot 2 \cdot 3 \cdots (p-1) \end{aligned}$$

*en we vinden dat* $(1 - a^{p-1}) 1 \cdot 2 \cdot 3 \cdots (p-1)$ *deelbaar is door p, en dus dat* $1 - a^{p-1}$ *deelbaar is door p.*

De kleine stelling van Fermat impliceert meteen:

**Gevolg 1.3** *Voor alle n met* $n \equiv 1 \pmod{p-1}$ *en voor alle a geldt*

$$a^n \equiv a \pmod p.$$

Stel nu dat $e$ en $f$ natuurlijke getallen zijn met $ef \equiv 1 \pmod{p-1}$, dan zien we dat als we een getal $a$ eerst tot de $e$-de, en daarna tot de $f$-de macht verheffen, we $a$ terugkrijgen, modulo $p$. We zullen zoiets straks gaan toepassen in RSA: een boodschap coderen door hem "tot de $e$-de macht verheffen" en daarna de gecodeerde boodschap "tot de $f$-de macht te verheffen" om de oorspronkelijke boodschap terug te vinden.

Het volgende is hierbij van belang:

**Propositie 1.4** *Zij n een natuurlijk getal. Voor elke e die onderling ondeelbaar is met n bestaat er een f zodat* $ef \equiv 1 \pmod n$.

**Proof 2** *We zoeken* $f = x$ *en y die voldoen aan de vergelijking*

$$ex + ny = 1. \tag{1}$$

*Zonder verlies van algemeenheid kunnen we aannemen dat $n > e > 0$. We gaan nu $n$ delen door $e$ met rest:*

$$n = eq + r \text{ met } 0 < \text{r} < \text{e}.$$

*Substitutie in (1) levert:*

$$e(x - qy) + ry = 1$$

*wat we kunnen oplossen zodra we $x'$ en $y'$ vinden met $ex' + ry' = 1$. Maar aangezien $e$ en $r$ onderling ondeelbaar zijn is dit terug een vergelijking van het type (1), doch met kleinere coëfficiënten: $r < e < n$. Door dit proces te herhalen komen we uiteindelijk uit op een vergelijking met een van de coëfficiënten gelijk aan 1, dus van het type $x'' + ay'' = 1$, die de triviale oplossing $(1, 0)$ heeft.*

Het bewijs laat niet alleen zien dat $f$ bestaat, maar ook dat die snel berekend kan worden, gegeven $e$ en $n$. Het (impliciet) gegeven algoritme is het *Euclidische algoritme.*

## 1.5 Machtsverheffen modulo $pq$

Vanaf nu zijn $p$ en $q$ verschillende priemgetallen. In de toepassing (RSA) zullen zij typisch groter dan $10^{100}$ zijn.

**Propositie 1.6** *Voor alle $n$ zodat $n \equiv 1 \pmod{(p-1)(q-1)}$ en voor alle $a$ geldt*

$$a^n \equiv a \pmod{pq}.$$

Voorbeeld: $a^9 \equiv a \pmod{10}$, want $9 \equiv 1 \pmod{(5-1)(2-1)}$, dus als we een cijfer tot de derde macht verheffen modulo 10, dan kunnen we het oorspronkelijke cijfer terugvinden door nogmaals tot de derde macht te verheffen.

## 1.7 Opgaven

**Opgave 1.8** *Bewijs propositie 1.6.*

**Opgave 1.9** *Vind alle $n$ zodat voor alle $a$ geldt: $a^n \equiv a \pmod{9}$.*

**Opgave 1.10** *Toon aan dat $n^{n^n} \pmod{10}$ enkel afhangt van $n \pmod{20}$.*

**Opgave 1.11** *$2^{29}$ is een getal van 9 cijfers, en alle cijfers zijn verschillend. Er is dus precies één cijfer wat niet in $2^{29}$ voorkomt. Bedenk welk cijfer ontbreekt, en dit zonder potlood, papier, noch mechanisch of elektronisch rekenhulpmiddel.*

# 2 RSA

Nu gaan we beschrijven hoe RSA te werk gaat. Alice heeft een geheime sleutel en een publieke sleutel, en Bob gaat een boodschap naar Alice sturen, die hij zal coderen met de publieke sleutel. Hoewel iedereen de gecodeerde boodschap mag zien, en ook iedereen de publieke sleutel kent, kan enkel Alice, met behulp van de geheime sleutel de boodschap ontcijferen.

(In de *cryptografie* heten de personen die een geheime boodschap uitwisselen bijna altijd Alice en Bob. De eventuele kwaadwillige derde persoon die probeert een onderschepte boodschap te ontcijferen heet gewoonlijk Eve, wij zullen het op Eva houden.)

## 2.1 Publieke en geheime sleutel

Alvorens Bob wat naar Alice kan sturen moet Alice (eenmalig) een geheime en een publieke sleutel aanmaken, en de publieke sleutel bekend maken.

Dit gebeurt als volgt:

1. Alice produceert twee grote verschillende priemgetallen: $p$ en $q$, en houdt deze geheim;
2. Alice publiceert het product $pq$;
3. Alice kiest een $e$ die onderling ondeelbaar is met $(p-1)(q-1)$, en publiceert $e$;
4. Alice berekent $f$ zodat $ef \equiv 1 \pmod{(p-1)(q-1)}$ en houdt $f$ geheim.

De *publieke sleutel* bestaat nu uit de *modulus* $pq$ en de *publieke exponent* $e$. De *geheime sleutel* bestaat uit de *geheime exponent* $f$.

## 2.2 Coderen

Stel dat de boodschap $m$ (voor message) die Bob naar Alice wil versturen bestaat voldoet aan $0 \leq m \leq pq-1$. (Indien Bob meer informatie wil versturen moet hij zijn boodschap in stukjes knippen). Bob gaat als volgt te werk:

1. Bob berekent $m^e$ modulo $pq$;
2. Bob verstuurt $m^e \pmod{pq}$ naar Alice.

## 2.3 Decoderen

Nu is het duidelijk wat Alice met de ontvangen boodschap moet doen:

1. Alice ontvangt $m^e \pmod{pq}$;
2. Alice berekent $m \equiv (m^e)^f \pmod{pq}$ door gebruikt te maken van de geheime exponent $f$.

## 2.4 Veiligheid

En nu verschijnt Eva ten tonele. Zij heeft de versleutelde boodschap $m^e \pmod{pq}$ onderschept en wil die ontsleutelen.

Hiervoor zal ze een "$e$-de wortel" uit $m^e$ modulo $pq$ moeten berekenen. Daar zijn verschillende methoden voor maar geen enkele praktisch haalbare. De best bekende methode bestaat eruit $pq$ te ontbinden in $p$ en $q$, en daarna $f$ uit te rekenen, dus een $f$ te vinden met

$$ef \equiv 1 \pmod{(p-1)(q-1)}.$$

Doch, als $p$ en $q$ uit meer dan honderd cijfers bestaan zal het met de grootste supercomputers en de meest geavanceerde algoritmen niet lukken om $pq$ te factoriseren.

Als Eva kan raden wat $m$ is (bijvoorbeeld "ja" of "nee"), dan kan ze eenvoudigweg haar gok tot de $e$-de macht verheffen en die vergelijken met de onderschepte $m^e$. Ook als $m$ zo klein is dat $m^e < pq$ (als gehele getallen), dan kan Eva gewoon de gewone $e$-de wortel uit $m^e$ berekenen.

Om dit soort kwetsbaarheden te vermijden wordt bij het toepassen van RSA altijd een stuk willekeurige informatie aan de boodschap $m$ toegevoegd ("jaSZDFOEK034ojisce0u9342" ipv "ja").

## 2.5 Opgaven

**Opgave 2.6** *Toon aan dat $p$ en $q$ makkelijk te vinden zijn als zowel $(p-1)(q-1)$ als $pq$ bekend zijn. Het berekenen van $(p-1)(q-1)$ uit $pq$ is dus "even moeilijk" als het ontbinden van $pq$ in priemfactoren.*

# 3 Algoritmische overwegingen

## 3.1 Het ontbinden in priemfactoren

Wie RSA wil kraken die zal uit de publieke sleutel, uit het publieke getal $n = pq$ de geheime priemgetallen $p$ en $q$ moeten afleiden: die zal moeten ontbinden in priemfactoren.

Stel dat we weten dat $p$ en $q$ uit honderd cijfers bestaan. Hoe kunnen we die terugvinden uit $n$? De meest voor de hand liggende methode is om voor alle priemgetallen $r$ die uit honderd cijfers bestaan te testen of ze $n$ delen, totdat we $r = p$ of $r = q$ vinden. Hoeveel priemgetallen van honderd cijfers zijn er? De priemgetallenstelling zegt dat een getal van honderd cijfers priem is met "kans" ongeveer $1/\log(10^{100}) \approx 1/231$. Dat zijn er zoveel dat geen enkele computer ze allemaal binnen de levensduur van het heelal kan uitproberen.

Nu bestaan er wel (zeer geavanceerde) algoritmen die veel sneller kunnen ontbinden in priemfactoren. Maar zelfs voor die algoritmen is een getal van twee honderd cijfers hopeloos te groot.

Men kan desalniettemin niet uitsluiten dat iemand ooit een betere methode ontdekt, die wel in staat is om zulke grote getallen te factoriseren.

## 3.2 Het produceren van grote priemgetallen

De geheime sleutel bestaat uit twee priemgetallen, $p$ en $q$, elk bestaande uit zo'n paar honderd cijfers. Hoe vindt men zulke grote priemgetallen? Het is duidelijk gevaarlijk om ze uit een voorgeschreven lijst van priemgetallen te halen, want dan zou men de publieke sleutel $pq$ gemakkelijk kunnen kraken (ontbinden) door te testen of $n$ deelbaar is door priemgetallen uit het lijstje. Om veilig te zijn moeten $p$ en $q$ "willekeurig" zijn, het moet praktisch onmogelijk zijn te raden wat $p$ of $q$ zijn.

Gelukkig zijn er heel veel priemgetallen van honderd cijfers lang, zoals reeds opgemerkt is een getal van honderd cijfers priem met "kans" ongeveer $1/231$.

Dus we moeten maar een paar honderd willekeurige getallen van honderd cijfers proberen om een willekeurig priemgetal van honderd cijfers te vinden. Maar hoe testen we of een getal priem is? De naïeve methode, delen door 2, 3, 5, etc, is vrij hopeloos, dat hadden we al gezien. Maar deze methode doet natuurlijk veel te veel: deze test niet alleen of een getal priem is, maar vindt zelfs een deler als een getal niet priem is: het is geen *priemtest*, maar een *factorisatie-algoritme.*

Verbazend genoeg bestaan er geavanceerde priemtests die heel snel beslissen of een getal al dan niet priem is, maar die geen delers kunnen vinden. Mijn computer heeft dan ook maar een halve seconde nodig om een priemgetal van honderd cijfers te produceren, hier is het kleinste: $10^{99} + 289$.

## 3.3 Machtsverheffen: herhaald kwadrateren

Om 3 tot de miljoenste macht te verheffen moet men op het eerste zicht 999.999 vermenigvuldigingen uitvoeren. Maar het kan wat slimmer: door herhaald te kwadrateren heeft men slechts $n$ vermenigvuldigingen nodig om $3^{2^n}$ uit te rekenen: $3^2 = 3 \cdot 3$, $3^4 = 3^2 \cdot 3^2$, $3^8 = 3^4 \cdot 3^4$, enzovoort. Door deze machten te onthouden en te combineren blijkt dat $3^{1.000.000}$ met slechts 25 vermenigvuldigen te berekenen valt.

Die vermenigvuldigen worden natuurlijk wel steeds groter en kosten dus steeds meer tijd, het eindresultaat is tenslotte een getal bestaande uit zo'n vijfhonderd duizend cijfers.

Als men enkel geïnteresseerd is in de miljoenste macht van 3 modulo zeg maar $n = 34.518.765$, dan vervalt het probleem dat de vermenigvuldigen gigantisch groot worden: na elke stap kan men reduceren modulo $n$, de te vermenigvuldigen getallen zijn dus nooit meer dan 8 cijfers lang. Mijn computer heeft dan ook maar een miljoenste van een seconde nodig om het antwoord te geven: $3^{1.000.000}$ is 31743636 modulo 34518765.

Deze techniek staat toe zonder al te veel moeite de machtsverheffingen $m^e$ en $(m^e)^f$ modulo $pq$ die in RSA voorkomen uit te voeren.

# 4 Conclusies

De asymmetrie in complexiteit tussen de inverse operaties "vermenigvuldigen" (triviaal) en "factoriseren" (zeer moeilijk) staat toe dat Alice en Bob op een veilige manier informatie kunnen uitwisselen zonder van de te voren een geheime sleutel te moeten afspreken. Behalve RSA zijn er nog enkele andere gelijkaardige encryptie-schema's, die gebruik maken van andere asymmetrieën in complexiteit van inverse getaltheoretische operaties. Hoewel deze systemen dagelijks en op grote schaal gebruikt worden, valt niet te bewijzen dat ze veilig zijn: er valt niet uit te sluiten dat een nieuw wiskundig idee zoals een nieuw factorisatie-algoritme ze volledig nutteloos maakt.

# Zwevende getallen

Marco Swaen
Hogeschool Amsterdam

**Inleiding**

In 1907, nu iets meer dan een eeuw geleden verscheen het proefschrift "over de grondslagen der wiskunde" waarin de dan nog onbekende L.E.J. Brouwer een nieuwe visie op de wiskunde ontvouwt, sindsdien aangeduid als het "intuïtionisme". Brouwer liet het niet bij filosofische beschouwing maar werkte in latere jaren zijn ideeën uit tot een nieuwe stijl van wiskunde beoefenen.
De intuïtionistische wiskunde kreeg niet veel navolging, en is tegenwoordig vooral een curiositeit voor specialisten.

L.E.J. Brouwer

Dat is jammer want met name Brouwers behandeling van reële getallen en functies sluit eigenlijk beter aan bij de manier waarop wij in concreto met getallen en functies omgaan.

In dit artikel wil ik de lezer op een informele manier kennis laten maken met de intuïtionistische kijk op reële getallen en functies. Met het oog op de toegankelijkheid zal het een losse interpretatie zijn van de uitgangspunten, en zal ik in terminologie en technische uitwerking niet proberen de presentatie zoals Brouwer die in zijn artikelen gaf te vertolken.

## I historie

### §1 over de grondslagen der wiskunde

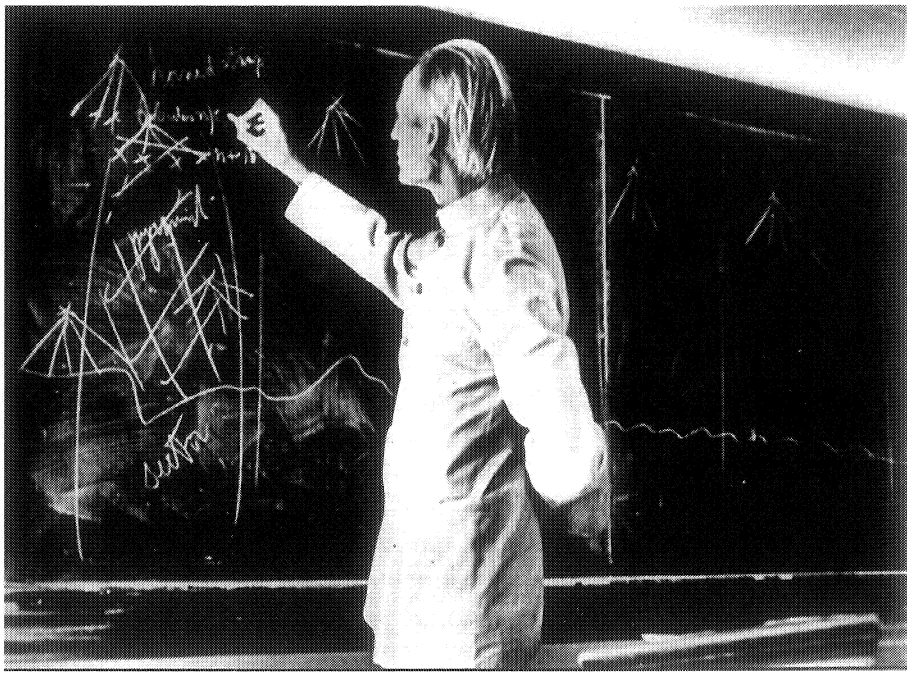
Als jong wiskundige nam Bouwer stormenderhand zijn plaats in op het wereldtoneel met de succesvolle toepassing van algebraïsche technieken in de topologie. De naar hem genoemde dimensiestelling en dekpuntstelling herinneren aan dat sprankelende begin. Maar Brouwer ambieerde meer dan het leveren van memorabele bijdragen aan het corpus van de klassieke wiskunde. Hij was gegrepen door het toendertijd levendige debat over de vraag wat wiskunde nu eigenlijk is. In zijn proefschrift liet hij zien de diverse stromingen in dat debat goed te kennen en uitte fundamentele kritiek op elk van die scholen. Brouwer stelt dat taal en logica slechts hulpmiddelen zijn in de beoefening van de wiskunde. Daarom zal het, in weerwil van wat logicisten als Frege en Russell hoopten, nooit mogelijk zijn de wiskunde te herleiden tot logica. Noch is de wiskunde terug te brengen tot een formeel spel zoals David Hilbert beoogde. En tenslotte moet ook Cantor het ontgelden met zijn verzamelingenleer, die volgens Brouwer niet veel meer is dan een betekenisloos woordspel.

Brouwer laat het niet bij kritiek op de dominante stromingen van zijn tijd, hij komt ook met een eigen karakterisering van het wezen der wiskunde. Wiskunde is een vrije schepping van onze geest, waarbij wij wiskundige objecten - getallen, functies, systemen - bedenken en bestuderen. Brouwer spreekt van mentale constructies die ontspruiten aan onze intuïtie - a priori kennis in de zin van Kant. Vandaar dat zijn opvattingen bekend zijn komen te staan onder de naam 'intuïtionisme'.

### §2 de intuïtionistische reconstructie

Toen tijdens de Eerste Wereldoorlog de internationale uitwisseling stilviel vatte Brouwer de taak op zijn filosofische standpunt concreet te maken door de wiskunde van de grond af op te bouwen volgens de inzichten die hij in zijn proefschrift ontwikkeld had. In 1918 verscheen zijn eerste artikel in een reeks waarin hij deze intuïtionistische reconstructie aanvangt met een verzamelingentheorie en de theorie van het reële getal. Zijn belangrijkste leerling Arend Heyting (1898-1980) concipieerde in de twintiger jaren een intuïtionistische logica die de positie ten opzichte van de klassieke wiskunde verhelderde. Ook andere gebieden der wiskunde werden intuïtionistisch verkend, waarbij soms mooie resultaten werden geboekt. Hoe complexer de materie, hoe ingewikkelder het begrippenapparaat echter werd als gevolg van het verschijnsel dat één klassieke notie

aanleiding gaf tot een waaier aan intuïtionistische, zodat niet-ingewijden al gauw het spoor bijster waren.



Brouwer over keuzerijen

In de nadruk op constructieve methoden heeft Brouwers intuïtionisme inmiddels gezelschap gekegen van een schare aan andere alternatieve wiskunden onder exotische namen als de Russische recursief constructivisten, de constructieve analyse van Bishop, predicativistische wiskunde, finitisme en ultrafinitisme.
Het aantal wiskundigen dat heden ten dage uit overtuiging de bewijzen Brouweriaans levert is overigens bijzonder klein. Wel blijft er interesse voor de intuïtionistische wiskunde als wiskundig systeem in verhouding tot de klassieke wiskunde.
Ook binnen de traditionele wiskunde is er altijd een voorkeur voor constructieve bewijzen omdat die algoritmen opleveren waarmee wiskunde uitvoerbaar en toepasbaar wordt.

## II uitgangspunten en kenmerken

### §3 bewijs uit ongerijmde

De axiomatische methode is sinds Euclides het model geweest voor de opbouw van een solide wiskundige theorie. Daarbij worden bewijzen streng gevoerd op basis van een uitputtende lijst van uitgangspunten - de axioma's - en volgens afleidingsregels: de logica. Een belangrijk

kenmerk van Brouwers intuïtionistische wiskunde is de tweeledige afwijzing van de axiomatische methode. Ten eerste zal men vergeefs in Brouwers artikelen zoeken naar een lijst met axioma's waarop de intuïtionistische wiskunde gefundeerd kan worden. Brouwer formuleert alleen aldoende wiskundige principes als hij het nodig vindt zijn bewijsvoering te verduidelijken. Ten tweede hanteert Brouwer in de bewijzen niet de vertrouwde logica, omdat volgens hem redeneringen moeten wortelen in wiskundige inhoud en niet mogen berusten op de klakkeloze toepassing van logische wetten. Met name verzet Brouwer zich tegen het principe van de uitgesloten derde, de wet die zegt dat er voor elke goed geformuleerde uitspraak A maar twee mogelijkheden zijn: A is waar, of A is niet waar, in formule: $A \vee \neg A$.
De wet van de uitgesloten derde vormt de grondslag voor het bewijs uit het ongerijmde, een methode waarbij men om A te bewijzen, eerst aanneemt dat A niet waar is, en uit die aanname een tegenspraak afleidt. Gaat het bijvoorbeeld om een uitspraak van de vorm: "er is een *x* met eigenschap E", dan levert een bewijs uit het ongerijmde de conclusie dat het *niet* mogelijk is dat er *geen x* is met eigenschap E. Maar daarmee geeft het bewijs doorgaans geen manier aan om die *x* daadwerkelijk te vinden, en wordt daarom niet als constructief beschouwd.

## §4 het wiskundig universum

De afwijzing van bewijs uit het ongerijmde wordt soms wel eens voorgesteld als de essentie van Brouwers intuïtionisme. Zij is echter geen fundamentele leerstelling, maar eerder een consequentie van de overtuiging dat wiskunde gaat over dingen die wij *maken*, en niet over dingen die los van ons bestaan. Anders dan sterren of geldstromen zijn getallen en systemen er alleen maar voorzover wij ze willen zien. Het zijn bedenksels, die wij zelf oproepen, en die wij alleen aan anderen tonen door aan te geven hoe wij ze in onze gedachten tot stand hebben gebracht. De wiskundige objecten zijn dus mentale constructies. Hebben wij geen constructie voor *x*, dan is *x* er niet.
Het wiskundige universum waarin wij al denkend vertoeven is noodzakelijk onaf, alleen dat wat wij er gemaakt hebben, danwel waarvan wij inzien dat wij het in een afzienbaar aantal stappen zouden kunnen maken, bestaat er.
Wiskunde is 'uitvinden' en niet 'ontdekken'. De objecten moeten wij uitvinden voor we ze kunnen bestuderen. Vervolgens kunnen we al studerend eigenschappen ontdekken, maar welbeschouwd is dat ontdekken het vinden van sluitende redeneringen, van bewijzen, dus ook 'uitvinden' in de vorm van het leveren van een gedachteconstructie.

## §5 de tijdsintuïtie

Ook fantasieën en dromen zijn mentale constructies, het bijzondere aan de constructies waarmee wij ons als wiskundige bezig houden is dat wij ze maken vanuit een bepaald inzicht, onze tijdsintuïtie in Brouwers terminologie. Het is inzicht waarmee wij zijn toegerust om de wereld waarin wij moeten overleven te begrijpen en naar onze hand te zetten. Men kan ook denken aan een instinct, of in de terminologie van Kant: a priori kennis, kennis die wij bezitten zonder deze eerst afgeleid te hebben uit ervaringen.
In zijn proefschrift heeft Brouwer het over de tijdsintuïtie en noemt daarbij het gegeven dat wij gedachten en gewaarwordingen niet gelijktijdig maar achtereen hebben, en beschikken over het vermogen de ene ervaring te onthouden en te vergelijken met een volgende. In ons denken figureert een tijdslijn,waarlangs wij gewaarwordingen rangschikken, waarmee wij oorzaak en gevolg onderscheiden en waarmee wij onze handelingen kunnen beramen en overdenken.

De telrij 1,2,3,4,... komt direct voort uit ons vermogen ons in gedachten een eenheid voor te stellen, daar in gedachte een eenheid aan toe te voegen, en dit proces eindeloos te herhalen. Zien wij die telgetallen als stappen op de tijdslijn, dan kunnen we ook terugtellen en komen op 0, -1, -2, ... . Maar ook is de tijdslijn vloeiend, waarbij tussen momenten steeds weer nieuwe momenten onderscheiden kunnen worden, zodat we een beeld krijgen van wat wij noemen: het continuüm.
In onze gedachten zijn wij vrij; al zullen wij in de werkelijkheid nooit erg ver tellen, wij beseffen dat het tellen niet eindigt omdat wij in principe altijd weer één stap verder kunnen. Zo loopt het continuüm eindeloos voort en is het aantal telgetallen oneindig. Evenzeer is het oneindige aanwezig in de mogelijkheid in het continuüm tussen elk tweetal momenten weer een nieuw moment te onderscheiden.

## §6 de natuurlijke getallen

Met onze telgetallen kunnen wij rekenen, en zo ontdekken wij allerlei eigenschappen: een getal kan priem zijn, of samengesteld, even, of de som van twee priemgetallen. Heb ik een getal gemaakt dan kan ik de eigenschappen ervan onderzoeken. Maar als het aantal getallen oneindig is, hoe zou ik dan ooit kunnen vaststellen of álle getallen een bepaalde eigenschap hebben ?
Omdat ik weet hoe ik de getallen maak, namelijk elk getal is een directe opvolger van een eerder gemaakt getal en uiteindelijk een opvolger van 1, kan ik toch het geheel der natuurlijke getallen overzien.

In het geval dat ik weet dat de eigenschap voor 1 geldt, en altijd wordt doorgegeven van een getal naar zijn directe opvolger, kan ik concluderen dat de eigenschap vanaf 1 aan elke opvolger wordt doorgegeven en geen enkel getal zal overslaan.
Dit is het bekende principe van "bewijs door volledige inductie", en is voor de intuïtionist nog acceptabeler dan voor een klassiek wiskundige, die denkt dat de natuurlijke getallen ergens buiten ons bestaan, en zich eigenlijk zorgen zou moeten maken of er behalve die opvolgers van 1 misschien nog andere natuurlijke getallen zijn.

## §7 even of niet even

Zoals wij al vertelden verzette Brouwer zich tegen het klakkelooos toepassen van logica, met name tegen het principe van de uitgesloten derde. Dat wil niet zeggen dat in zijn wiskunde $A \vee \neg A$ nooit geldt. Ter verduidelijking zullen wij twee voorbeelden bekijken, één van een uitspraak waarop het principe wel, en één waarop het niet van toepassing is.
De volgende stelling is niet moeilijk te bewijzen:

elk natuurlijk getal is even of oneven.

Met *even* bedoelen we dat het getal van de vorm $2n$ is, met oneven dat het van de vorm $2n-1$ is, waarbij $n$ een willekeurig natuurlijk getal voorstelt. Om te beginnen is het getal 1 oneven, want $1 = 2 \cdot 1 - 1$.
Als een getal $n$ even is, dan is zijn opvolger van de vorm $2n+1 = 2(n+1) - 1$ dus oneven. Is een getal oneven, dan is het zelf van de vorm $2n - 1$, dan is zijn opvolger $2n - 1 + 1 = 2n$, dus even.
Verder is het niet heel moeilijk te beredeneren dat een getal niet even en oneven tegelijk kan zijn, dus we hebben ook: voor elk natuurlijk getal $n$ geldt

$$n \text{ is even } \vee \neg(n \text{ is even})$$

## §8 Goldbach of niet Goldbach

De methode van volledige inductie biedt vaak geen soelaas. Dat is (tot op heden) bijvoorbeeld het geval bij het (sterke) vermoeden van Goldbach, dat teruggaat op een correspondentie tussen Goldbach en Euler van 1742 en behelst dat elk even getal groter dan 2 de som van twee priemgetallen zou zijn.

Probeer maar:

$4 = 2 + 2$
$6 = 3 + 3$
$8 = 3 + 5$
$10 = 3 + 7 = 5 + 5$
.....

Met G($n$) geven we aan dat het getal $2n$ voldoet aan de eigenschap in het vermoeden, oftewel:

G($n$) = als $n > 1$ dan zijn er priemgetallen $p$ en $q$ zodat $2n = p + q$

Daarmee is het vermoeden van Goldbach dus te schrijven als: $\forall n$ G($n$)
Van een gegeven getal $n$ is deze eigenschap te controleren binnen afzienbaar aantal stappen. Wil je bijvoorbeeld weten of G(100), maak dan een lijst van de priemgetallen tussen 1 en 200, kijk dan of 1 en 199 misschien priem zijn, zoniet dan misschien 2 en 198 enz. ben je tegen de tijd dat je 100 bereikt nog geen paar priemgetallen tegengekomen dat samen 200 is, dan weet je dat G(200) niet geldt. Ben je wel zo'n paar tegengekomen dan geldt G(200) wel.
Dit is inmiddels al voor vele getallen gedaan, ongetwijfeld met handigere methodes, en terwijl de grens $10^{17}$ al gepasseerd is, is er nog steeds geen getal gevonden dat niet voldoet. Maar langs deze weg zal nooit zekerheid ontstaan dat er verderop niet toch getallen zullen opduiken die het vermoeden van Goldbach ontkrachten. Vooralsnog is het vermoeden van Goldbach dus een open probleem, en daarmee een voorbeeld van
een wiskundige bewering waarvan noch de bevestiging noch de ontkenning op dit moment bewezen is. Dat zulke uitspraken bestaan is inherent aan de wiskundige arbeid, waarin er altijd weer nieuwe vragen zullen zijn. In het vervolg zullen we regelmatig teruggrijpen op het vermoeden van Goldbach als voorbeeld van een open vraag. Mocht Goldbach's vermoeden bij het lezen van dit artikel al beslist zijn, dan zijn er ongetwijfeld nog genoeg andere vermoedens die als voorbeeld kunnen dienen.

## §9 logica en constructie

In overzichtelijke situaties, zoals we die in de werkelijkheid tegenkomen, zijn eenduidige uitspraken wel of niet waar. Dat inzicht maakt onderdeel uit van de logica die wij in dergelijke situaties hanteren. Het wiskundig universum is echter niet overzichtelijk, het is

onaf, en het is oneindig, en laat zich daarom niet zomaar begrijpen met de logica die wij ontleend hebben aan de werkelijkheid.
Voor Brouwer gaat logica niet vooraf aan de wiskunde, maar moet er uit worden afgeleid. Het constructieve karakter van zijn wiskunde heeft directe gevolgen voor de te hanteren logica. De logische voegwoorden krijgen bij hem een constructieve inhoud. Voor de twee uitspraken uit het voorafgaande is die constructieve betekenis als volgt:

1) De uitspraak $A \vee \neg A$ betekent:
ik heb een bewijs voor A of ik heb een bewijs voor $\neg A$.

We legden al uit dat dit bij het vermoeden van Goldbach niet het geval is, daarom is Goldbach $\vee \neg$ Goldbach géén stelling.

2) De uitspraak $\forall n$ ($n$ is even $\vee$ $n$ is oneven) betekent:
ik heb een methode waarmee ik voor elk natuurlijk getal $n$ beslissen kan of $n$ even is, danwel oneven.

Deze uitspraak is wel een stelling, de benodigde methode is te halen uit het inductiebewijs dat wij boven gaven voor deze uitspraak. Die methode kunnen we ook geven in de vorm van een functie $f$, bijvoorbeeld met het volgende recursieve voorschrift:

$$f(1) = 1$$
$$f(n+1) = 1 - f(n)$$

Deze $f$ is dan een constructie die berekent of $n$ even is of oneven, hetgeen wordt gemeld met een 0, respectievelijk een 1.

Nu uitspraken een constructieve inhoud hebben kunnen ze ook gebruikt worden als basis voor nieuwe constructies.
Omdat we weten: $n$ is even $\vee$ $n$ is oneven, kunnen we een functie $g$ maken met het voorschrift:

$$g(n) = \begin{cases} 0 & \text{als} \quad n \text{ is even} \\ 1 & \text{als} \quad n \text{ is oneven} \end{cases}$$

Die functie is effectief dezelfde als de zojuist gedefinieerde functie $f$.

En daarom juist wijzen we een definitie als de volgende af:

$$x = \begin{cases} 0 & \text{als} \quad \text{Goldbach} \\ 1 & \text{als} \quad \neg\text{Goldbach} \end{cases}$$

want om $x$ te construeren moeten wij eerst beslissen welk van beide gevallen geldig is, maar vooralsnog hebben wij geen procedure om dat te doen. Dit ding $x$ is geen wiskundig object, en dus ook geen natuurlijk getal, want een natuurlijk getal kunnen we binnen een afzienbaar aantal eenduidige stappen maken.

## §10 dubbele ontkenning

Nu we logische formules lezen als mededelingen met een constructieve inhoud ontstaat er ook een wezenlijk verschil tussen een bewering "A"(A is waar) en de bewering "$\neg\neg A$" (A is niet nietwaar). Stel je zoekt een oplossing voor een bepaalde vergelijking $h(x) = 0$, dan ben je gesteld voor de vraag: " $\exists x \ h(x) = 0$ ?" . Het kan zijn dat de aanname dat er géén $x$ zou zijn tot een tegenspraak leidt; dan weten we dus dat het niet zo is dat er geen nulpunt is, oftewel

$$\neg\neg \exists x \ h(x) = 0.$$

Maar dat bewijs op zich levert nog geen methode om dat nulpunt te vinden. Pas als we het nulpunt hebben, oftewel een constructie kunnen aangeven die het nulpunt levert, dan kunnen we beweren

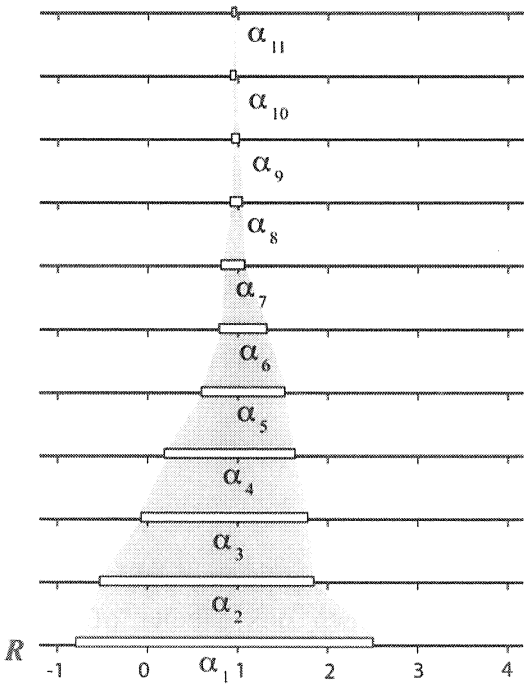
$$\exists x \ h(x) = 0.$$

# III de reële getallen

## §11 een plaats op het continuüm

De stappen die wij aanbrachten op het continuüm zijn van een willekeurige maat, we zouden die stappen ook kleiner of groter hebben kunnen kiezen. Het is een wezenlijk kenmerk van het continuüm dat het er lokaal na uitvergroting altijd weer netzo uitziet als voorheen. Zo kunnen we het stuk tussen 0 en 1 onderverdelen in tien kleinere stukjes, die we op hun beurt ook weer kunnen onderverdelen in 10 nog kleinere, enzovoorts, zodat we een schaalverdeling krijgen die met factor 10 omlaag steeds verder verfijnt. (Wij hadden natuurlijk netzo goed een andere basis dan 10 kunnen kiezen.) Al die schaalstreepjes zijn eindige decimaalbreuken en vullen het continuüm allerminst op, we kunnen terwijl wij de schaal verfijnen immers steeds tussen twee maatstreepjes gaan zitten, bij uitvergroting zien we dat daar altijd weer genoeg ruimte voor is. Zo kunnen wij al afdalend van verfijning naar verfijning een plaats aanwijzen in het continuüm met almaar toenemende nauwkeurigheid. Die aanwijzing bestaat dan uit opeenvolgende paren van maatstreepjes waartussen wij hebben besloten te blijven. Deze weg komt nooit tot een einde omdat we na uitvergroting altijd weer voor in wezen dezelfde overweldigende keuzeruimte staan.

Zo komen we tot het begrip "reëel getal", als een eindeloze rij intervallen (dwz paren maatstreepjes), waarbij de volgende altijd bevat is in de voorgaande en de breedte gedurig inkrimpt om smaller te worden dan elke verfijning van de schaal.



Figuur 3

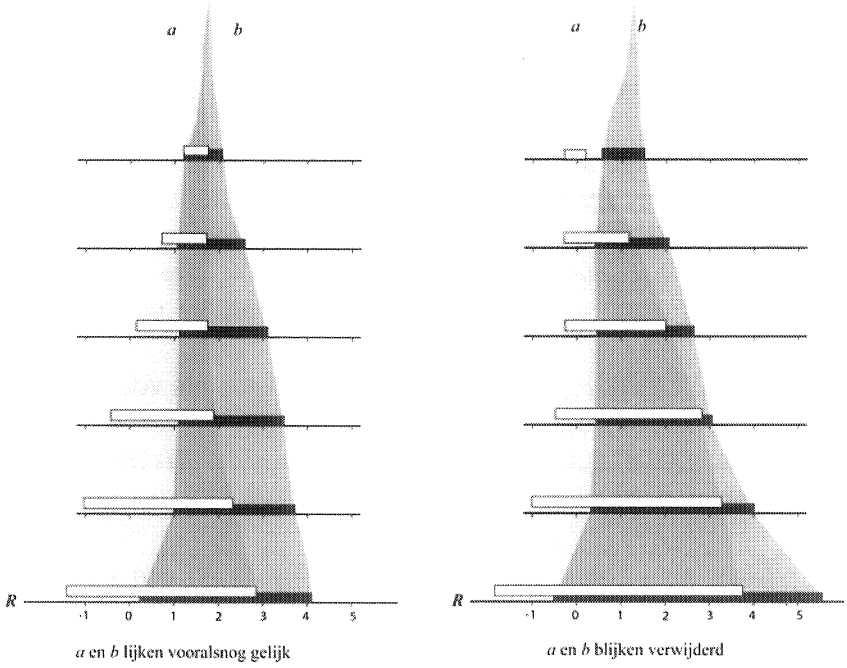
Dit is theoretisch wat ons te wachten staat als we een bepaalde lengte volmaakt nauwkeurig zouden willen opmeten. Vergeten wij even de kwantumfysica dan is die lengte altijd nog nauwkeuriger op te meten, omdat we altijd weer verder kunnen uitvergroten.
Het is ook het beeld dat wij oproepen als we een reëel getal voorstellen met een eindeloze rij decimalen. In elk stadium geeft de nog onvoltooide rij een gebied aan waarbinnen we verder zullen blijven. Hebben wij bijvoorbeeld 3,1415 dan beperken wij ons daarmee tot het gebied tussen 3,141 en 3,142. Bij de volgende decimaal 3,14159 is dit verder ingeperkt tot 3,1415 en 3,1416. (Waarmee niet gezegd is dat deze twee concepten geheel samenvallen, zie §15.)
Hierbij laten we het beeld los van reële getallen als minuscule stipjes zonder omvang die tezamen de getallenlijn te vormen. Een reëel getal is niet een punt zonder afmeting maar een voortschrijdend proces van inperking dat nooit voltooid is waarbij wij steeds scherper een deel van het continuüm afbakenen.
Dit concept strookt ook met het karakter van elk concreet reëel getal waar wij in de wiskunde mee rekenen; wortels, machten, logaritmen, goniometrische waarden constanten als $\pi$, e en $\gamma$, we kennen er, (enkele bijzondere rationale waarden daargelaten), altijd maar een beginstukje van.
Voor een platonist is $\pi$ een oneindige rij decimalen die ergens in een gouden boek zijn opgeschreven, in de praktijk echter is het een eindig aantal decimalen dat wij uitgerekend hebben en dat op dat moment voldoet voor onze berekeningen.

## §12 De onderlinge ligging van getallen

Bekijken we de onderlinge ligging van twee van zulke reële getallen dan kunnen zich verschillende mogelijkheden voordoen.

1) $a = b$

Als we weten dat de intervallen in elk stadium blijven overlappen, dan zijn de twee plaatsen die wij aanwijzen niet van elkaar te onderscheiden en hebben we dus met hetzelfde reële getal te maken. Hieronder links is dit gesuggereerd.




Figuur 4

2) $a \# b$

Als we weten dat op een bepaald moment de intervallen losraken, dan zijn $a$ en $b$ verschillende reële getallen. Zulks is in bovenstaande figuur rechts gevisualiseerd. Blijkbaar weten wij dan in welk stadium zij losraken en kunnen dan aan de bijbehorende intervallen zien welke links en welke rechts ligt, dus beslissen

$$a < b \vee a > b.$$

We noemen een tweetal getallen dan *verwijderd* van elkaar, notatie $a \# b$.

3) $a \neq b$

Het kan ook zijn dat we alleen weten dat de intervallen niet altijd zullen blijven overlappen, maar geen aanwijzing hebben in welk stadium ze van elkaar losraken. De getallen zijn dan in elk geval

ongelijk (anders zouden ze altijd blijven overlappen) maar we hebben niet voldoende kennis om te besluiten dat ze van elkaar verwijderd zijn. In feite is $a \neq$ b hetzelfde als $\neg\neg\, a \# b$.

De klassieke wiskunde kent de zogenaamde trichotomie die behelst dat voor reële getallen $a$ en $b$ er precies drie mogelijkheden zijn: $a < b \vee a = b \vee a > b$. In bewijsvoering is dit een graag toegepaste gevalonderscheiding. Intuïtionistisch is een dergelijke opsplitsing niet mogelijk omdat de onderlinge ligging van reële getallen niet altijd te bepalen is. Wij geven twee voorbeelden.

**§13 een zwevend getal**

De situatie kan zich voordoen dat we van een getal niet weten waar het zich ten opzichte van 0 bevindt, we spreken dan van een zwevend getal. Dat kan zijn omdat wij niet weten of $a = 0 \vee a \neq 0$, zoals bij het volgende getal $g$ dat wij constueren op basis van het vermoeden van Goldbach.

De rij intervallen voor $g$ vormen wij stap-voor-stap als volgt:

Onderzoek G($n$), te beginnen bij $n = 1$.

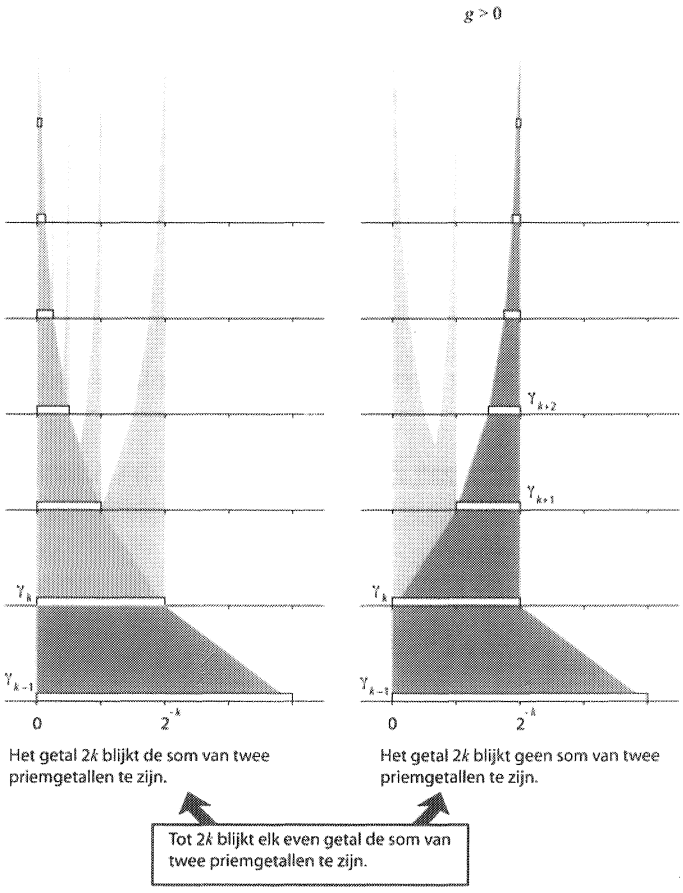
Zolang G($n$) voor de oplopende $n$ nog geldt, laat je het interval inkrimpen rond 0, met

$$\gamma_n = [\ 0\ ,\ 2^{-n}\ ]$$

Maar als je op een gegeven moment stuit op een $k$ waarvoor G($k$) niet geldt, laat je het interval voor verdere $n$ inkrimpen rond $2^{-k}$

$$\gamma_n = [2^{-k} - 2^{-n},\ 2^{-k}\ ] \text{ met}$$

Als er nooit een Goldbach-tegenvoorbeeld opduikt komt $g$ uit op 0. Verschijnen er wel tegenvoorbeelden dan blijft het getal $g$ steken op zekere $2^{-m}$ en is dus ongelijk aan 0. Zolang het Goldbach's vermoeden open blijft, zal ook de ligging van $g$ t.o.v. 0 ongewis zijn, en mogen wij niet stellen dat $g = 0 \vee g \neq 0$.




Figuur 5. *Zwevend getal g*

## §14 nog een zwevend getal

Op een vergelijkbare manier kunnen we een zwevend getal $d$ construeren waarvan niet uitgemaakt kan worden of $d \leq 0 \vee d \geq 0$.

Daarbij baseren wij ons op de decimaalontwikkeling van het getal $\pi$. Op dit moment zijn er van $\pi$ zo'n $10^{12}$ cijfers berekend, zonder dat daarin een duidelijk patroon zichtbaar is geworden.

Vooralsnog zijn er geen series van dezelfde cijfers gevonden langer dan zo'n 10. Wij stellen dus de volgend open vraag: komt in de decimaalontwikkeling van $\pi$ eerder een aaneengesloten rijtje van 100 nullen voor of eerder een rijtje van 100 negens. Het is duidelijk dat de twee series niet gelijktijdig kunnen optreden. Op basis van deze vraag construeren wij het volgende getal $d$.

Begin de rij intervallen van $d$ met

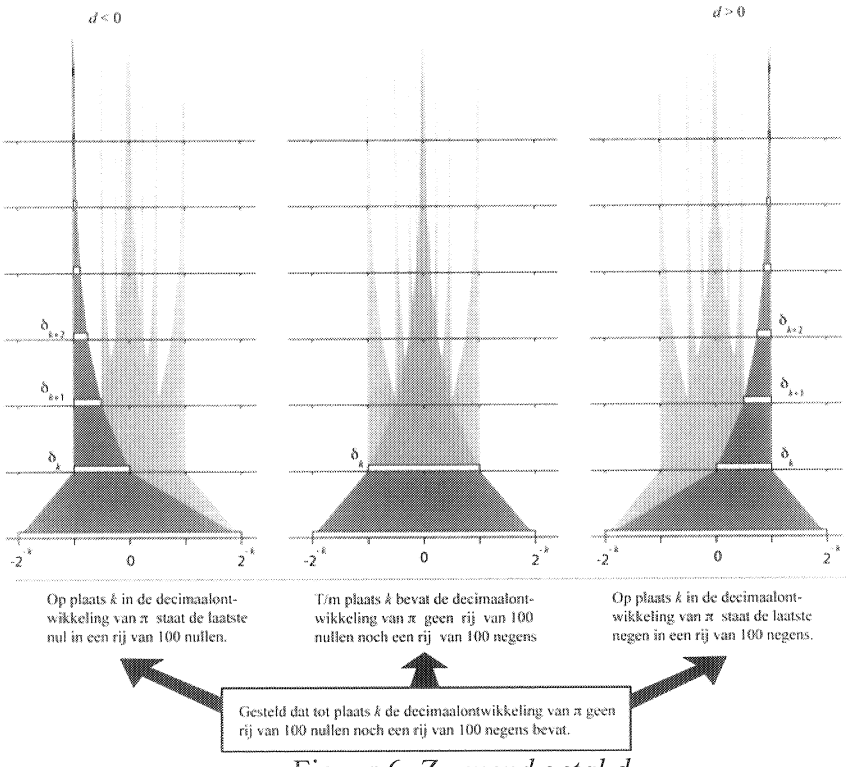
$$\delta_1 = [-½, ½].$$

Zolang je noch 100 opeenvolgende nullen, noch 100 opeenvolgende negens bent tegengekomen in de decimaalontwikkeling van $\pi$ laat je

het interval symmetrisch rond 0 inkrimpen. Zie je op een gegeven moment in de decimaalontwikkeling van $\pi$ op de $k$-de decimaal de laatste nul in een rijtje van 100 nullen, zet dan de linkergrens van het interval vast en laat het interval verder daarheen inkrimpen. Kom je daarentegen eerst een rijtje van100 negens tegen eindigend op de $k$-de decimaal, dan dwing je de rij intervallen naar rechts.
In formulevorm:

$$\delta_n = \begin{cases} [-2^{-k}, -2^{-k} + 2^{-n}] & \text{als er eerst 100 nullen t/m plaats } k \text{ voorkomen} \\ [2^{-k} - 2^{-n}, 2^{-k}] & \text{als er eerst 100 negens t/m plaats } k \text{ voorkomen} \\ [-2^{-n}, 2^{-n}] & \text{anders} \end{cases}$$

De constructie van het getal $d$ kan de lezer zich zo voorstellen:




Figuur 6. *Zwevend getal d*

Zou je nu kunnen beslissen of $d \leq 0 \vee d \geq 0$, dan zou je al weten welk van beide series in elk geval niet als eerste komt. Hieronder is de constructie van het getal $d$ gevisualiseerd.

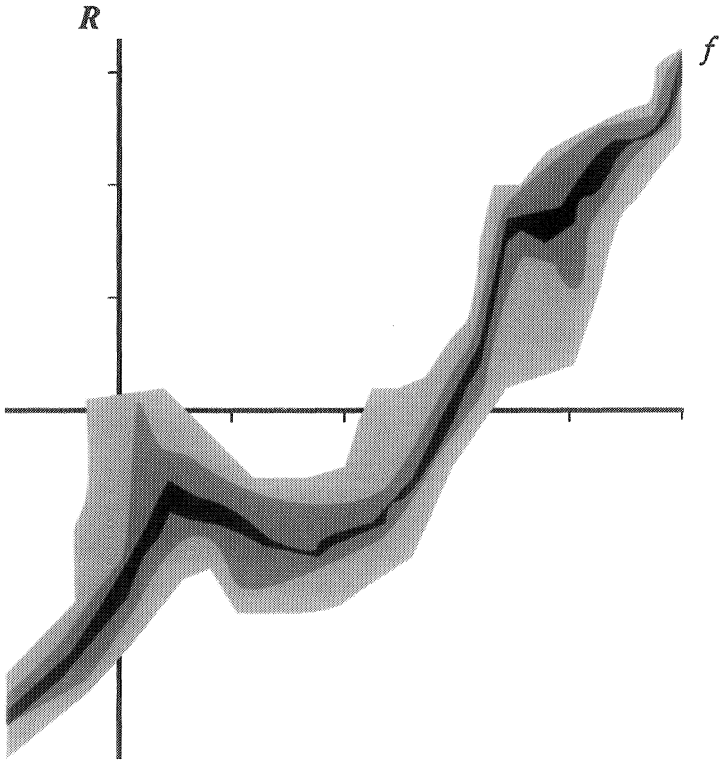
### §15 een getal zonder decimaalontwikkeling

Brouwer gaf een soortgelijk voorbeeld om te laten zien dat niet elk reëel getal een decimaalontwikkeling heeft (1920). Beschouw daartoe het getal $d + 1/10$ , waarbij $d$ het zwevende getal uit §14 is. Is de eerste decimaal van dit getal een 0, dan begint de decimaalontwikkeling met 0,0 en is het getal $d + 1/10$ blijkbaar niet groter dan $1/10$, dus $d \leq 0$. Is de eerste decimaal daarentegen een 1, dan ligt $d + 1/10$ blijkbaar niet onder $1/10$, en is dus $d \geq 0$. Maar we hadden $d$ juist geconstrueerd als een voorbeeld waarvoor de beslissing $d \leq 0 \vee d \geq 0$ buiten ons bereik ligt.

## IV functies

### §16 van reëel naar reëel

Met de reële getallen kunnen we rekenen zonder problemen. Willen wij bijvoorbeeld twee getallen $a$ en $b$ bij elkaar optellen, dan moeten we een rij intervallen construeren voor de uitkomst $a + b$. Die intervallen kunnen we bepalen vanuit de intervallen van $a$ en van $b$. Willen wij bijvoorbeeld een interval voor $a + b$ waarvan de grenzen niet meer dan $1/10$ uiteenliggen, vraag van $a$ en $b$ dan intervallen waarvan de grenzen minder dan $1/20$ uit elkaar liggen, zeg $[a_l, a_r]$ en $[b_l, b_r]$. Het interval $[a_l + b_l, a_r + b_r]$ voldoet dan aan de gestelde eis.
Bij een functie van reële getallen naar reële getallen, construeren wij beginstukken van het beeld op basis van beginstukken van het origineel, zowel $x$ als $f(x)$ zijn immers reële getallen en dus onaf. Wil je $f(x)$ met een bepaalde nauwkeurigheid weten, dan is dat mogelijk mits je $x$ met een bepaalde nauwkeurigheid aanlevert. We kunnen ons een reëelwaardige functie voorstellen als een rij grafieken waarbij de lijn van de grafiek met steeds scherpere pen getrokken wordt.




Figuur 7. *Functie*

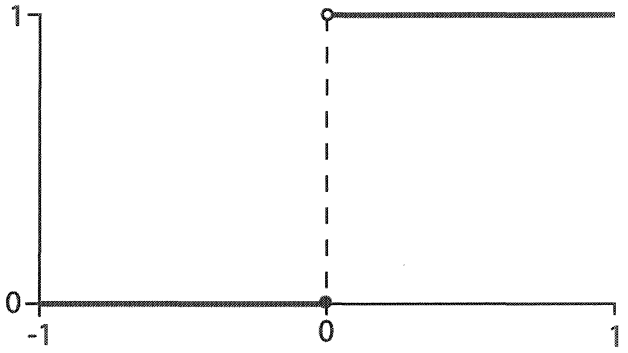
**§17 geen sprongen**

De bekende functies uit de analyse zoals polynoomfuncties, e-macht, logaritme, en goniometrische functies zijn constructief en stellen ons niet voor problemen. Treffen we een $x$-waarde die zweeft, dan kunnen we het beeld gewoon ook laten zweven, de aard van de reële getallen is dat wij $f(x)$ stap voor stap kunnen bijstellen, alnaargelang wij $x$ beter in beeld hebben.

Dit gaat echter mis als wij voor de $y$-waarde een abrupte keuze willen maken, zoals het geval was bij het bepalen van de eerste decimaal van een getal als $d$ in §14 en §15. We lichten dit toe door nog een ander voorbeeld uit te werken.

Stel we willen een functie $S$ maken op het interval [-1,1] met

$$S(x)=\begin{cases}0 & \text{als } x\leq 0\\ 1 & \text{als } x>0\end{cases}$$




Figuur 8. *Sprongfunctie*

Neem nu het zwevende getal $g$ uit §13 waarvan niet beslist kan worden of $g = 0 \vee g \neq 0$ Het beeld $S(g)$ moet tot op elke nauwkeurigheid bepaald kunnen worden, laten we zeggen dat we voor het beeld van $g$ een interval willen met een breedte niet groter dan ½ . Omdat 0 en 1 te ver uit elkaar liggen is $S$ dan genoodzaakt het beeldinterval voor $S(g)$ hetzij bij 0 hetzij bij 1 te kiezen.
Om die keuze te maken mag $S$ vragen om een interval van $g$ dat willekeurig smal is. De breedte van dat interval, hoe nietig ook, correspondeert met een $n$ tot waar Goldbach dan gecontroleerd is. Op grond van die $n$ moet $S$ dan beslissen of het beeld van $g$ in de buurt van 0 zal liggen danwel in de buurt van 1. Maar dan zou $S$ op grond van die eerste $n$ getallen het vermoeden van Goldbach moeten kunnen beslissen, hetgeen wij aannamen dat niet mogelijk is.

**§18 twee centrale stellingen**
Dat reëelwaardige functies geen sprongen kunnen vertonen maakten wij aannemelijk met een beroep op de aard van het reele getal als eindeloze keuzerij, en op een notie van wat functies uitvoerbaar of 'constructief' maakt. Daarbij namen we stilzwijgend aan dat de functie totaal is, dat wil zeggen voor alle reële getallen gedefinieerd moet zijn. In de aangevoerde argumenten ligt in feite besloten dat een reëelwaardige functie wel continu *moet* zijn om uitvoerbaar te zijn. Binnen het bestek van dit artikel voert het te ver een technische uitwerking te geven, wij vermelden derhalve zonder bewijs de twee stellingen die de essentie van reëelwaardige functies vastleggen:

Stelling 1
Elke totale functie $f : \mathbf{R} \to \mathbf{N}$ is constant.

Stelling 2
Elke totale functie $f : \mathbf{R} \to \mathbf{R}$ is continu.

Het is interessant de eerste stelling te bezien in relatie tot de verzamelingenleer van Cantor waarin steeds grotere verzamelingen worden opgebouwd door machtsverzamelingen te nemen, dwz verzamelingen van alle deelverzamelingen van een bepaalde verzameling. Bij Cantor is de machtsverzameling altijd 'groter' dan de verzameling zelf. De machtsverzameling van $A$ kunnen wij voorstellen als alle functies van $A$ naar $\{0,1\}$. Uit stelling 1 volgt dat voor intuïtionisten deze machtsverzameling van $\mathbf{R}$ maar twee elementen heeft, namelijk de functie $f$ met constant $f(x) = 0$ en die met constant $f(x) = 1$.

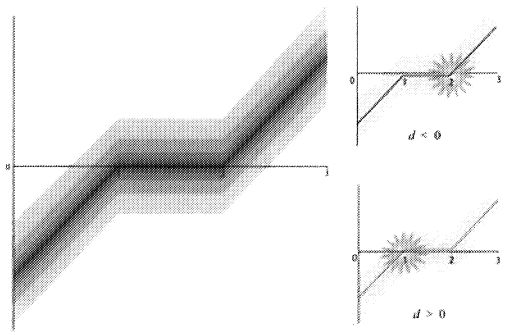
**§19 geen tussenwaardestelling**
Een ander mooi resultaat over reëelwaardige functies betreft zogenaamde tussenwaarden van functies. In de klassieke analyse hebben we

Tussenwaardestelling :
Gegeven een continue functie $f : \mathbf{I} \to \mathbf{R}$ met $f(0) < 0$ en $f(1) > 0$
dan is er een $x \in \mathbf{I}$ met $f(x) = 0$

Waarbij $\mathbf{I}$ staat voor het eenheidsinterval [0,1]. Intuïtionistisch geldt deze stelling niet. We zullen laten zien dat het vinden van zo'n nulpunt net zo veel voorzienigheid vergt als nu beslissen of Goldbach wel of niet waar is.
Om het noteren iets te vergemakkelijken rekken wij het eenheidsinterval uit tot [0,3], en beschouwen daarop de functie: $f$: [0,3] $\to \mathbf{R}$ met

$$f(x) = \min(x-1,0) + \max(0, x-2) + d$$

waarbij $d$ het zwevende getal is uit §14 waarvan niet achterhaald kan worden of $d \geq 0 \vee d \leq 0$.



Figuur 9. *Tussenwaarde*

Hierboven links zien wij het verloop van de functie. In het gebied van 1 tot 2 bevindt $f$ zich rond de $x$-as. Terwijl de decimalen van $\pi$ worden afgezocht naar een rij van 100 nullen danwel 100 negens verscherpt het beeld en trekt $f$ zich van 1 tot 2 steeds dichter rond de $x$-as samen. Mocht zich nu voor het eerst een rijtje van100 nullen voordoen in de decimaalontwikkeling van $\pi$, dan tilt $d$ de grafiek iets omhoog en zal er alleen nog een nulpunt ontstaan rond 1 (zie rechtsboven). Mocht daarentegen eerder een rijtje van 100 negens verschijnen dan trekt $d$ de grafiek een stukje omlaag en komt het enige nulpunt helemaal bij 2 (zie rechtsonder). Een minuscule verschuiving in de $y$-richting duwt het nulpunt zo een hele eenheid van zijn plaats. Wil nu de ligging van het nulpunt bepaald worden dan moet al gekozen worden hetzij in de buurt van 1 te gaan zitten, hetzij bij 2, maar de kennis om dat te doen is dezelfde die nodig is om te beslissen of $d \geq 0 \vee d \leq 0$.

Tegenover dit negatieve resultaat staan twee positieve:

- Voor belangrijke deelklassen van functies is de tussenwaarde-stelling intuïtionistisch wel geldig. Stijgt $f$ monotoon, of is $f$ bijvoorbeeld een polynoomfunctie, dan is er wel een constructie om een nulpunt te vinden.
- Bij elke functie kan een bijna-nulpunt gevonden worden dwz een $x$ waarvoor
  $f(x)$ minder dan $10^{-n}$ van 0 verschilt.

De bovenstaande weerlegging van de tussenwaardestelling heeft ook in de klassieke wiskunde een plaats. Daar toont deze functie aan dat er geen continue operatie op $C(\mathbf{I}, \mathbf{I})$ kan bestaan die een nulpunt van $f$ geeft.

## §20 geen dekpuntstelling

In 1952 schreef Brouwer een artikel waarin hij zijn eigen dekpuntstelling intuïtionistisch weerlegt. De situatie is vergelijkbaar met die bij de tussenwaardestelling. Het vinden van een dekpunt bij een willekeurige continue afbeelding $f : \mathbb{I}^k \to \mathbb{I}^k$ veronderstelt een constructie om van een reëel getal $x$ te kunnen beslissen $x \geq 0 \vee x \leq 0$. Omdat die constructie niet bestaat blijkens getallen als $d$ in §14, is het dekpunt niet vindbaar. Ook hier is er echter wel een bijna-dekpunt te vinden, een punt dat minder dan $10^{-n}$ van zijn plaats gaat. Brouwer laat in het artikel zien hoe dit voor dimensie $k = 2$ gedaan kan worden.

## §21 deels onbekende getallen

De intuïtionistische analyse behandelt reële getallen als onaffe objecten. De grootheden die optreden in dagelijks rekenwerk zijn meestal ook onaf. Dat kan zijn omdat de grootheid een lengte is die altijd nog nauwkeuriger opgemeten had kunnen worden. Maar ook als de grootheid in principe geheel is of rationaal, kan hij onbepaald zijn omdat de precieze getalwaarde schommelt danwel niet definieerbaar is. Denk aan getallen als: het aantal inwoners van Nederland, het aantal gezinnen met kinderen, de gemiddelde leeftijd van die Nederlanders, de leeftijd van de Aarde.

Bij deze grootheden zien we dezelfde kwesties optreden als bij de intuïtionistische reëlen. Als $N$ het aantal inwoners van Nederland is, dan is het moeilijk vast te stellen of $N \geq 16.421.651$ danwel $N \leq 16.421.651$, dat zal per minuut kunnen verspringen en ook gevoelig zijn voor hoe wij het exacte moment van geboorte of sterfte definiëren.

Zijn wij in een berekening uitgekomen op $x \approx 0{,}25$, dan ligt $x$ blijkbaar tussen $^{245}/_{1000}$ en $^{255}/_{1000}$ en is niet meer vast te stellen of $x \geq \frac{1}{4} \vee x \leq \frac{1}{4}$.

In de schoolwiskunde hinken wij vaak op twee gedachten. Enerzijds is er de nagestreefde exactheid uit de klassieke analyse, anderzijds willen we dat de leerling zich realiseert dat de getallen slechts benaderingen zijn.

De zaak loopt regelmatig door elkaar, bijvoorbeeld:

1) Los op voor $x \in [0,\pi]$ $\quad \sin \frac{1}{2} x < 0{,}8$.
   Wat is hier het verschil met de vraag $\sin \frac{1}{2} x \leq 0{,}8$?
2) Het gewicht van appels (in grammen) is bij benadering normaal verdeeld met $\mu = 48$ en $\sigma = 12$ g.
   Moet hier continuïteitscorrectie worden toegepast ?

## § Referenties


[Brouwer 1952] L.E.J. Brouwer: "Door klassieke theorema's gesignaleerde pinkernen die onvindbaar zijn" Kon. Nederlandse Academie van Wetenschappen. Proc. Ser. A55 blz 443-445 (1952)

[Brouwer 1907] L.E.J. Brouwer: "Over de grondslagen der wiskunde" proefschrift. Uitgegeven in epsilonreeks "LE.J. Brouwer en de grondslagen der wiskunde" D.van Dalen. deel 51 ISBN 978-90-5041-093-9

[Brouwer 1908] L.E.J. Brouwer: "Over de onbetrouwbaarheid der logische principes" Tijdschrift voor Wijsbegeerte 2, 152-158, in bovenvermelde epsilonuitgave.

[Brouwer 1918] L.E.J.Brouwer: " Begründung der Mengenlehre unabhängig vom logischen Satz vom ausgeschlossenen Dritten" Verhandelinghen KNAW in " Brouwer Collected Works" ed. A.Heyting (North Holland, Amsterdam)

[Brouwer 1921] "Besitzt jede reelle Zahl eine Dezimalbruchentwicklung?" Mathematische Annalen vol 83, nr 3-4 september 1921 (via www.springerlink.com/content/j610803w2l7x4192/)

[Troelstra/van Dalen 1988] Constructivism in Mathematics volume 1. (North Holland, Amsterdam).

# Fibonacci aan de universiteit

Bart Zevenhek
Mathematisch Instituut Radboud Universiteit

*Welke* Fibonaccigetallen zijn veelvoud van een gegeven $n$? Welke daarvan is de kleinste? Is er een verband tussen $n$ en de bijbehorende periode? Over deze vragen blijkt heel wat te zeggen. Als $n$ een *priemgetal* ongelijk aan 5 is, dan geldt bijvoorbeeld dat $n$ een deler is van $F_{n-1}$ of van $F_{n+1}$. Het bewijs hiervan is heel wat lastiger, maar met behulp van enige kennis van getaltheorie, (uitbreidings)ringen en algebra valt dit mooi te bewijzen.

Voor de beantwoording van de genoemde vragen in het geval $n$ een macht is van een priemgetal kom je op het terrein van de $p$-adische analyse. De periode van de rij van Fibonacci modulo machten van 10 en 10-adische analyse verklaren ook goed het merkwaardige gedrag van de rij zoals die in de volgende tabel naar voren komt:

| $n$ | $F_n$ | $n$ | $F_n$ |
|---:|---:|---:|---:|
| 19 | 4181 | 29 | 514229 |
| 199 | 1942044301 | 299 | 7264610201 |
| 1999 | 4076005501 | 2999 | 7655102001 |
| 19999 | 9011617501 | 29999 | 7451020001 |
| 199999 | 7967737501 | 299999 | 4510200001 |
| 1999999 | 7528937501 | 2999999 | 5102000001 |
| 19999999 | 3140937501 | 29999999 | 1020000001 |

De laatste 10 cijfers van $F_n$

Nog veel interessanter wordt de rij als je die onderzoekt binnen $\widehat{\mathbb{Z}}$, de verzameling van de pro-eindige getallen. Pro-eindige getallen lijken op $p$-adische getallen en vormen in feite een uitbreiding van de gehele getallen, zoals de reële getallen dat ook zijn. De rij van Fibonacci laat zich eenvoudig uitbreiden tot een functie van $\mathbb{Z}$ naar $\mathbb{Z}$, maar bijvoorbeeld een uitbreiding tot een functie van $\mathbb{R}$ naar $\mathbb{R}$ stuit op grote problemen. De rij laat zich echter wel uitbreiden tot een fraaie *continue* functie van $\widehat{\mathbb{Z}}$ naar $\widehat{\mathbb{Z}}$. De periode van de rij van Fibonacci modulo $n$ speelt daarbij een belangrijke rol.

# 1 De resten-rij van Fibonacci

De rij van Fibonacci bevat voor ieder positief geheel getal $n$ oneindig veel veelvouden van $n$. Met behulp van modulorekenen is dit niet moeilijk om in te zien. Als je modulo $n$ rekent, dan kijk je naar de resten van getallen die je krijgt na deling door $n$. Laten we als voorbeeld eens $n = 8$ nemen. Wanneer je door 8 deelt, dan is de rest gelijk aan $0, 1, 2, \ldots, 7$. Nemen we de rij van Fibonacci modulo 8, dan krijgen we:

$$1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0, 1, 1, \ldots.$$

Deze *resten-rij* vormt weer een soort rij van Fibonacci. Je ziet bijvoorbeeld dat $5 + 5 = 10$ en als je 10 deelt door 8 krijg je inderdaad rest 2. Dit wordt opgeschreven als:

$$5 + 5 \equiv 2 \pmod 8.$$

Je kunt ook voorgaande termen uitrekenen. De term die bijvoorbeeld vóór $7, 1$ staat is $1 - 7 = -6 \equiv 2 \pmod 8$.

Hoe volgt hieruit dat de rij van Fibonacci voor ieder geheel getal $n$ oneindig veel veelvouden van $n$ bevat? We laten dat zien voor $n = 8$, voor andere getallen werkt het precies zo. Zoals gezegd zijn er modulo 8 slechts 8 verschillende resten mogelijk. Voor twee opeenvolgende termen van de resten-rij van de rij van Fibonacci modulo 8 zijn er dan slechts $8^2 = 64$ mogelijkheden. Als je de eerste 66 termen van de resten-rij opschrijft (je krijgt dan 65 opeenvolgende tweetallen) dan *moeten* er twee identieke opeenvolgende tweetallen tussen zitten. Deze twee identieke tweetallen leggen echter de rij ervoor en die erna vast, zodat de hele rijen volgend op en voorafgaand aan deze tweetallen identiek moeten zijn. Dit kan alleen als de resten-rij *periodiek* is. In het voorbeeld zie je dat de resten-rij zich na 12 stappen al gaat herhalen. Voor willekeurige $n$ geldt op de zelfde wijze dat de bijbehorende resten-rij periodiek is. De rij van Fibonacci begint met $1, 1, \ldots$ en evenzo begint de resten-rij voor iedere $n$ met $1, 1, \ldots$. Daaraan voorafgaand kan alleen een 0 komen, die zich vervolgens oneindig vaak herhaalt. Een rest die gelijk is aan 0 betekent natuurlijk dat het bijbehorende getal in de rij van Fibonacci deelbaar is door $n$. Klaar is Kees!

Is, bij gegeven $n$, te voorspellen waar een veelvoud van $n$ in de rij van Fibonacci te vinden is en wat de kortste periode modulo $n$ is? Om deze vragen te beantwoorden nemen we een duik in de algebra van groepen, ringen en lichamen. Een *groep* is een verzameling waarop een bewerking zoals optellen of vermenigvuldigen is gedefiniëerd, die aan een aantal elementaire algebra-regels voldoet. Ieder element van een groep heeft bijvoorbeeld een inverse. Een *ring* is een verzameling waarvan je de elementen op een fatsoenlijke manier kunt optellen en vermenigvuldigen. Aftrekken is binnen een ring eveneens geen probleem, maar delen kan niet altijd: niet ieder element hoeft een inverse te hebben. De elementen van een ring $R$ die wel een inverse hebben, vormen een groep die aangeduid wordt als $R^*$. Als in een ring ieder element, behalve 0, een inverse heeft, wordt van een *lichaam* gesproken. Het eenvoudigste voorbeeld

van een ring is $\mathbb{Z}$, de ring van de gehele getallen. Modulorekenen vindt plaats in de ring $\mathbb{Z}/n\mathbb{Z}$, een ring met $n$ elementen die je kan voorstellen met de getallen 0 tot en met $n-1$, waarmee modulo $n$ gerekend wordt.

We geven de rij van Fibonacci aan met $F_n$. Laten we eens naar de eerste termen van de rij kijken.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $F_n$ | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | 89 | 144 | 233 | 377 |

De keuze om de rij met $n = 1$ te beginnen is vrij willekeurig. Aangezien twee opeenvolgende termen van de rij van Fibonacci niet alleen de *volgende* term maar ook de *voorgaande* term vastleggen, namelijk als het verschil van beide termen, valt eenvoudig in te zien dat $F_0 = 1 - 1 = 0$ en bijvoorbeeld $F_{-1} = 1 - 0 = 1$. Op deze wijze voortgaande is het mogelijk om de rij van Fibonacci op te vatten als functie van $\mathbb{Z}$ naar $\mathbb{Z}$. De keuze $F_1 = F_2 = 1$ is wel essentieel in de komende theorie.

Controleer nu de volgende stelling voor de waarden van $n$ die in de tabel staan.

**Stelling 1.1** *Als $n$ een priemgetal ongelijk aan 5 is, dan is $n$ een deler van $F_{n-1}$ of van $F_{n+1}$.*

Deze stelling zullen we in de volgende paragraaf onder de loep nemen.

# 2 Nulpunten van de rij van Fibonacci

Om te beginnen zullen we de zogenaamde formule van Binet bewijzen. We werken binnen een ring die een element $\alpha$ bevat waarvoor geldt dat $\alpha^2 = \alpha + 1$. Dit element $\alpha$ is dus een oplossing van de vergelijking $x^2 - x - 1 = 0$. Binnen $\mathbb{R}$ zijn er twee oplossingen: $\frac{1}{2}(1 \pm \sqrt{5})$, maar binnen $\mathbb{Z}$ zijn er geen. Als er één oplossing $\alpha$ is, dan is er over het algemeen nog een tweede oplossing $\beta = 1 - \alpha$. Het is een aardige oefening om aan te tonen dat $\beta$ inderdaad een oplossing is en om de volgende regels na te gaan.

$$\alpha \cdot \beta = -1 \tag{1}$$

$$5 = (\alpha - \beta)^2 = (2\alpha - 1)^2 = (2\beta - 1)^2 \tag{2}$$

$$\alpha^n = \alpha^{n-1} + \alpha^{n-2} \tag{3}$$

Bekijk nu de volgende meetkundige rijen.

$$1, \alpha, \alpha^2, \alpha^2, \alpha^3, \ldots \text{ en } 1, \beta, \beta^2, \beta^3, \ldots$$

Evenals de rij van Fibonacci voldoen ze aan de regel dat een term de som is van de twee voorgaande termen (regel(3)!). Een lineaire combinatie $L_n = a \cdot \alpha^n + b \cdot$

$\beta^n$ voldoet ook aan deze regel. We keizen nu $a = \frac{1}{\alpha-\beta}$ en $b = -\frac{1}{\alpha-\beta}$, zodat de eerste twee termen van $L_n$ beiden gelijk zijn aan 1 (Dit kan trouwens alleen als $\alpha - \beta$ een inverse heeft. Dit is één van de oorzaken van de uitzonderingspositie die het getal 5 in stelling 1.1 in neemt). De ontstane rij $L_n$ heeft dan dezelfde beginwaarden en de dezelfde recursieve definitie als de rij van Fibonacci. Beide rijen moet dan gelijk zijn. Het resultaat is de formule van Binet:

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{4}$$

We zullen ook gebruik maken van de kleine stelling van Fermat.

**Stelling 2.1 (Kleine stelling van Fermat)** *Voor een priemgetal $p$ en een positief geheel getal $n$ dat geen veelvoud is van $p$ geldt:*

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

Voor een bewijs verwijs ik naar [1], [2], [4] of [5].

Neem nu een priemgetal $p \neq 5$ en bekijk de ring $\mathbb{Z}/p\mathbb{Z}$. Er zijn waarden van $p$ waarvoor $\mathbb{Z}/p\mathbb{Z}$ een element $\alpha$ bezit waarvoor $\alpha^2 = \alpha + 1$. Bijvoorbeeld, voor $p = 11$ geldt dat $4^2 \equiv 16 \equiv 5 \equiv 4 + 1 \pmod{11}$. Met behulp van de 'kwadratische reprociteitswet' kan aangetoond worden dat dit altijd lukt voor priemgetallen die eindigen op een 1 of op een 9. Aangezien in zulke gevallen $\alpha$ en $\beta$ gewoon elementen zijn van $\mathbb{Z}/p\mathbb{Z}$, geldt de kleine stelling van Fermat: $\alpha^{p-1} = 1$ en $\beta^{p-1} = 1$. Invullen in de formule van Binet geeft dan:

$$F_{p-1} = \frac{\alpha^{p-1} - \beta^{p-1}}{\alpha - \beta} = \frac{1 - 1}{\alpha - \beta} = 0 \pmod{p},$$

oftewel: $p$ is een deler van $F_{p-1}$.

Er zijn echter ook vele priemgetallen $p$ waarvoor $\mathbb{Z}/p\mathbb{Z}$ niet in het fortuinlijke bezit is van zo een element $\alpha$. In zulke gevallen breiden we de ring $\mathbb{Z}/p\mathbb{Z}$ uit tot een ring $(\mathbb{Z}/p\mathbb{Z})[\alpha]$ die bestaat uit elementen van de vorm $a + b\alpha$, met $a, b \in \mathbb{Z}/p\mathbb{Z}$. Formeel is $(\mathbb{Z}/p\mathbb{Z})[\alpha]$ gelijk aan

$$(\mathbb{Z}/p\mathbb{Z})[X]/(X^2 - X - 1),$$

maar je kunt ook denken aan de ring van getallen van de vorm $a + b \cdot \frac{1}{2}(1 + \sqrt{5})$, met $a, b \in \mathbb{Z}/p\mathbb{Z}$. De constructie heeft in feite veel weg van die van de complexe getallen, waarbij aan $\mathbb{R}$ een element $i$ wordt toegevoegd waarvoor geldt dat $i^2 = -1$.

Een wiskundige met voldoende kennis van ringen van het type $(\mathbb{Z}/p\mathbb{Z})[\alpha]$ weet dat $(\mathbb{Z}/p\mathbb{Z})[\alpha]$ in dit geval zelfs een lichaam is, dat net als in $\mathbb{R}$ een polynoom van graad $k$ hoogstens $k$ nulpunten heeft en dat de volgende wonderlijke regel geldt binnen $(\mathbb{Z}/p\mathbb{Z})[\alpha]$: $(a + b)^p = a^p + b^p$. Gewapend met deze kennis kost het niet veel moeite om in te zien dat $\alpha^p = \beta$ en $\beta^p = \alpha$. Met (4) volgt dan:

$$F_{p+1} = \frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta} = \frac{\alpha^p\alpha - \beta^p\beta}{\alpha - \beta} = \frac{\beta\alpha - \alpha\beta}{\alpha - \beta} = 0.$$

We zien dus dat $p$ in dit geval een deler is van $F_{p+1}$.

# 3 Perioden van de rij van Fibonacci

Ook vragen die betrekking hebben op de periode modulo een getal $n$ zijn met hulp van voorgaande theorie goed aan te pakken. De volgende stelling speelt daarin een belangrijke rol:

**Stelling 3.1** *De kortste periode van de rij van Fibonacci modulo $n$ is gelijk aan de orde van $\alpha$ in $(\mathbb{Z}/n\mathbb{Z})[\alpha]^*$.*

De orde van een element $a$ van $(\mathbb{Z}/n\mathbb{Z})[\alpha]^*$ is per definitie het kleinste getal $k$ waarvoor $a^k = 1$. Laten we voortaan als we het over *de* periode hebben de korste periode bedoelen en die aangeven met $\text{per}(n)$. Iedere andere periode is dan een veelvoud van $\text{per}(n)$. Om de stelling te bewijzen is de volgende formule van belang:

$$\alpha^n = F_{n-1} + F_n\alpha \tag{5}$$

Deze formule volgt met volledige inductie uit (3) of uit de formule van Binet en (1):

$$\begin{aligned} F_{n-1} + F_n\alpha &= \frac{\alpha^{n-1} - \beta^{n-1} + \alpha^n\alpha - \beta^n\alpha}{\alpha - \beta} = \frac{-\alpha^n\beta - \beta^{n-1} + \alpha^n\alpha + \beta^{n-1}}{\alpha - \beta} \\ &= \frac{\alpha^n(\alpha - \beta)}{\alpha - \beta} = \alpha^n \end{aligned}$$

Voor de periode moeten we het kleinste getal $k > 0$ vinden waarvoor $F_k = 0$ en $F_{k-1} = F_{k+1} = 1$, want we willen dat het rijtje $\ldots, 1, 0, 1, 1, \ldots$ weer in de resten-rij opduikt. Kijk nog maar eens terug naar het voorbeeld van $n = 8$. Maar uit (5) volgt dan dat $k$ tevens de kleinste waarde is waarvoor $\alpha^k = 1 + 0 \cdot \alpha = 1$.

Neem nu wederom een priemgetal $p \neq 5$. Voor het geval $\mathbb{Z}/p\mathbb{Z}$ een element $\alpha$ bevat met $\alpha^2 = \alpha + 1$ zagen we in de voorgaande paragraaf dat $\alpha^{p-1} = 1$. Dus de orde van $\alpha$ en daarmee de periode modulo $p$ is een deler van $p - 1$. Als $\mathbb{Z}/p\mathbb{Z}$ niet zo een element $\alpha$ bevat zagen we dat $\alpha^p = \beta$. Hieruit volgt met (1) dat $\alpha^{p+1} = \alpha\alpha^p = \alpha\beta = -1$ en $\alpha^{2(p+1)} = 1$. In deze situatie is de periode dus een deler van $2(p + 1)$. Voor $p = 5$ gelden deze twee opties overigens geen van beiden, maar geldt dat $\text{per}(5) = 20$.

Wat is de periode van de rij van Fibonacci bij samengestelde getallen $n$? In de bewijzen van de voorgaande paragraaf wordt het feit dat $p$ een priemgetal is veelvuldig gebruikt. Geen wonder dat stelling 1.1 voor samengestelde getallen zelden opgaat. In de situatie waarin $n$ een macht is van een priemgetal $p$, zeg $n = p^k$, blijkt *meestal* de periode modulo $p^k$ gelijk te zijn aan $p^{k-1}$ maal de periode van $p$. Wat wordt bedoeld met 'meestal', een preciezere formulering en een bewijs (met behulp van $p$-adische analyse) is te vinden in [6]. Ook wordt daarin bewezen dat voor getallen $n$ en $m$ met GGD gelijk aan 1 de periode van $n \cdot m$ gelijk is aan de KGV van de periode van $n$ en de periode van $m$. Gevolg is dat ook voor samengestelde getallen, na priemfactorontbinding, de periode voor de rij van Fibonacci te vinden is.

Laten we bij wijze van voorbeeld de periode modulo 264 bepalen. Aangezien $264 = 2^3 \cdot 3 \cdot 11$, moeten we eerst de periode modulo $2^3$, modulo 3 en modulo 11 bepalen. De periode van 2 is een deler van $2(2+1) = 6$ en blijkt gelijk te zijn aan 3. De periode van $2^3$ is dan $2^2 \cdot 3 = 12$. De periode van 3 is $2(3+1) = 8$ en van 11 is deze $11 - 1 = 10$. De periode van 264 is dus de KGV van 12, 8 en 10, hetgeen gelijk is aan 120. In het bijzonder weten we nu ook dat 264 een deler is van $F_{120}$.

# 4 De rij van Fibonacci 10-adisch

De opgedane kennis van perioden van de rij van Fibonacci heeft vele toepassingen. Neem bijvoorbeeld de volgende merkwaardige tabel:

| $n$ | $F_n$ |
|---|---|
| 29 | 514229 |
| 299 | 7264610201 |
| 2999 | 7655102001 |
| 29999 | 7451020001 |
| 299999 | 4510200001 |
| 2999999 | 5102000001 |
| 29999999 | 1020000001 |

*Tabel 1.* De laatste 10 cijfers van $F_n$

Het lijkt erop dat de laatste $k$ cijfers van $F_n$ voor $k \geq 2$ bepaald worden door de laatste $k$ cijfers van $n$. Dit valt in te zien door middel van de periode van de rij van Fibonacci modulo $10^k$. Probeer zelf met de kennis van de voorgaande paragraaf de volgende tabel te verklaren:

| $n$ | 10 | 100 | 1000 | 10000 | 100000 | $10^k$ voor $k \geq 3$ |
|---|---|---|---|---|---|---|
| per($n$) | 60 | 300 | 1500 | 15000 | 150000 | $15 \cdot 10^{k-1}$ |

*Tabel 2.* De periode modulo $10^k$

Als de periode van de rij van Fibonacci modulo $n$ gelijk is aan per($n$), dan geldt voor iedere $x \in \mathbb{N}$: dat $F_{x+\text{per}(n)} \equiv F_x \pmod{n}$. In modulo-notatie kan dit nog korter worden opgeschreven:

$$i \equiv j \pmod{\text{per}(n)} \Rightarrow F_i \equiv F_j \pmod{n}. \tag{6}$$

Laten we kijken naar de laatste twee kolommen van tabel 1. In de linker kolom staan elementen van de rij $u_k = 3 \cdot 10^k - 1$ en rechts daarvan staat dan $F_{u_k}$.

Laten we (6) toepassen met $i = u_k$, $j = u_{k+1}$ en $n = 10^k$, waarbij $k \geq 3$. Er komt dan:

$$3 \cdot 10^k - 1 \equiv 3 \cdot 10^{k+1} - 1 \pmod{15 \cdot 10^{k-1}} \Rightarrow F_{u_k} \equiv F_{u_{k+1}} \pmod{10^k}. \quad (7)$$

Nu is $3 \cdot 10^k = 30 \cdot 10^{k-1}$ een veelvoud van $15 \cdot 10^{k-1}$, waardoor $3 \cdot 10^{k+1} \equiv 3 \cdot 10^k \equiv 0 \pmod{15 \cdot 10^{k-1}}$. De linkerkant van de implicatie in (7) is dus waar voor $k \geq 3$. Dit heeft tot gevolg dat:

$$F_{u_k} \equiv F_{u_{k+1}} \equiv F_{-1} \pmod{10^k}. \quad (8)$$

Als getallen modulo $10^k$ gelijk aan elkaar zijn, zijn de laatste $k$ cijfers gelijk. De laatste $k$ cijfers van $F_{u_k}$ en $F_{u_{k+1}}$ komen dus overeen en zijn bovendien gelijk aan de laatste $k$ cijfers van $F_{-1}$. We vonden al eerder dat $F_{-1}$ gelijk is aan 1. De rechter twee kolommen van tabel 2 zijn nu duidelijk. Voor de linker twee kolommen geldt een soortgelijke redenering, alleen kom je daar niet mooi uit op $F_{-1} = 1$.

Met het voorgaande onderzoek zitten we op het terrein van $\mathbb{Z}_{10}$, de 10-adische gehele getallen, waarover eerder in deze serie syllabi is geschreven [3]. Een gewoon positief geheel getal kan je in de decimale notatie vooraf laten gaan door oneindig veel nullen. Daarmee is dat getal een 10-adisch getal geworden. Een 10-adisch geheel getal kan namelijk gezien worden als een (naar links toe) oneindig lange rij cijfers van 0 tot en met 9. Met 10-adische getallen reken je van rechts naar links, precies als met 'eindige' natuurlijke getallen. Zo valt eenvoudig na te rekenen dat

$$\ldots 9999999999 + \ldots 0000000001 = \ldots 0000000000,$$

zodat het 10-adische getal $\ldots 9999999999$ het equivalent is van het gehele getal $-1$. Dit geeft een hele andere interpretatie van de rechter twee kolommen van tabel 1: Als de rij $u_k$ naar $\ldots 9999999999 = -1$ gaat dan gaat $F_{u_k}$ naar $F_{-1} = 1$. Dit lijkt erg op continuïteit, waarbij we aannemen dat twee 10-adische getallen 'dicht bij elkaar' liggen als veel cijfers *van achteren af* gelijk zijn. Dit is een totaal andere notie dan 'dichtbij elkaar liggen' van natuurlijke getallen en een essentieel verschil tussen 10-adische getallen en normale gehele getallen.

In de volgende tabel verloopt dit proces minder fraai:

| $n$ | $F_n$ |
|---:|---:|
| 99 | 4555169026 |
| 999 | 8474174626 |
| 9999 | 1238230626 |
| 99999 | 6278790626 |
| 999999 | 6684390626 |
| 9999999 | 0740390626 |
| 99999999 | 1300390626 |

*Tabel 3.* De laatste 10 cijfers van $F_n$

Blijkbaar is het niet zo dat voor *iedere* rij $u_k$ die naar $-1$ convergeert, de bijbehorende rij $F_{u_k}$ naar $F_{-1}$ convergeert. Zo een mooie continue funktie op de 10-adische getallen is de rij van Fibonacci nu ook weer niet. In de volgende paragraaf zullen we zien dat dit probleem verholpen wordt bij de *pro-eindige* getallen.

# 5 Pro-eindige Fibonacci getallen

Reële getallen zijn getallen die bestaan uit een teken, + of −, gevolgd door een eindig aantal cijfers, dan een komma en vervolgens een oneindig lange rij cijfers. Geen enkele wiskundige zou de reële getallen zo definiëren, al was het maar omdat het optellen van reële getallen zich vervolgens moeilijk definiëren laat. Probeer maar eens... Toch is dit in feite de manier waarop veel docenten het begrip reëel getal aan leerlingen uitleggen. Een goede definitie van de reële getallen is dan ook niet eenvoudig en werd pas in de 19-de eeuw op verschillende wijzen gegeven.

De 10-adische getallen zijn in de vorige paragraaf ook met zo een 'cijferdefinitie' gegeven. Maar anders dan bij reële getallen laat deze definitie het rekenen met 10-adische getallen eenvoudig definiëren. Hendrik Lenstra geeft in zijn artikel 'Profinite Fibonaccinumbers' [7] eveneens zo een cijferdefinitie van pro-eindige getallen. Net als 10-adische getallen bestaat een pro-eindig getal uit een oneindig lange rij cijfers

$$(\ldots c_5 c_4 c_3 c_2 c_1)_!,$$

maar de *cijfers* $c_i$ zijn nu *getallen* met $0 \leq c_i \leq i$. De uitroepteken geeft aan dat het een pro-eindig getal betreft. Net als bij 10-adische getallen blijken positieve gehele getallen te identificeren met pro-eindige getallen waarvan $c_k = 0$ voor alle $k$ voorbij een zekere grens. Vervolgens wordt in het artikel uitgelegd hoe er met deze pro-eindige getallen gerekend kan worden en wordt duidelijk gemaakt dat bijvoorbeeld het getal $-1$ ook binnen de pro-eindige getallen een equivalent heeft, namelijk:

$$(\ldots 7654321)_!.$$

Met behulp van een limietproces laat Hendrik Lenstra zien wat, voor een pro-eindig getal $s$, verstaan kan worden onder het $s$-de Fibonacci getal. Het idee is om het pro-eindige getal $s$ te benaderen met behulp van een rij $s_n$ van *gehele* getallen. Voor iedere $s_n$ kan het bijbehorende Fibonacci getal $F_{s_n}$ bepaald worden. De limiet hiervan levert dan $F_s$ op. Hij demonstreert dit procédé voor $s = (\ldots 7654321)_! = -1$ door dit pro-eindige getal te benaderen met het rijtje $(\ldots 00001)!, (\ldots 00021)!, (\ldots 00321)!, (\ldots 04321)!, \ldots$. Het resultaat levert inderdaad keurig $F_{-1} = 1$ op!

De formele definitie van $\widehat{\mathbb{Z}}$, de ring van de pro-eindige getallen, is niet eenvoudig:

$\widehat{\mathbb{Z}} = \{(a_n)_{n\geq 1} \in \prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z} :$

voor elke $n \geq 1$ en elke deler $d$ van $n$ geldt $a_n \equiv a_d \pmod{d}\}$

Je ziet dat een element van $\widehat{\mathbb{Z}}$ een oneindig lange rij elementen van $\mathbb{Z}/n\mathbb{Z}$ is, of beter gezegd: het $n$-de element van de rij zit in $\mathbb{Z}/n\mathbb{Z}$. Net als $\mathbb{R}$ is $\widehat{\mathbb{Z}}$ een overaftelbare verzameling en is er een zinnige topologie op te geven. Deze topologie maakt het mogelijk om limietprocessen te gebruiken en om te spreken over continuïteit van functies.

Om nu de rij van Fibonacci op een fatsoenlijke manier uit te breiden tot een functie van $\widehat{\mathbb{Z}}$ naar $\widehat{\mathbb{Z}}$ wordt (6) gebruikt. Deze eigenschap maakt het namelijk mogelijk om de rij van Fibonacci voor iedere $n$ te definiëren als functie

$$F : \mathbb{Z}/\mathrm{per}(n)\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}.$$

De periodiciteit van de rij van Fibonacci modulo $n$ speelt dus een belangrijke rol in de uitbreiding. De aldus verkregen functie blijkt bovendien een *continue* functie op te leveren. Hierdoor wordt het limietproces waarmee Hendrik Lenstra de uitbreiding naar de pro-eindige getallen verkreeg gerechtvaardigd: van ieder rijtje pro-eindige getallen $s_n$ dat naar een gegeven pro-eindig getal $s$ convergeert zal $F_{s_n}$ naar dezelfde $F_s$ convergeren.

Net zoals er op de reële en complexe getallen analyse bedreven kan worden, is dit ook mogelijk op de pro-eindige getallen. De rij van Fibonacci is getransformeerd tot een continue functie die gedifferentieerd kan worden en waarvoor machtreeksen ontwikkeld kunnen worden. In de tweede helft van zijn artikel gaat Hendrik Lenstra op informele wijze hiermee aan de slag, hetgeen een efficiënte methode oplevert om voor gegeven pro-eindige $s$ de bijbehorende $F_s$ te benaderen. Tenslotte worden de dekpunten van de functie bepaald: de waarden $s$ waarvoor $F_s = s$. Er blijken precies elf dekpunten te zijn. Hendrik Lenstra benadert de waarden van deze dekpunten door middel van iteratie en met hulp van de methode van Newton en vindt enkele merkwaardige eigenschappen van deze dekpunten.

In dit artikel van vier pagina's ontsluit Hendrik Lenstra op meesterlijke wijze een nieuwe wiskundige wereld. Door de informele wijze van benadering is het goed te volgen. Onder andere in mijn document 'Profinite Fibonaccinumbers revisited' [6] is een poging gewaagd om de formele wiskunde achter het artikel op te bouwen. Een taak die nog lang niet afgerond is.

# Referenties


[1] P.Stevenhagen, *Syllabi ALGEBRA* 1,2 en 3,
http:websites.math.leidenuniv.nl/algebra/

[2] Frits Beukers, *Getaltheorie voor beginners*
blz. 43,61,62 Epsilon Uitgaven 1991

[3] CWI Syllabus 35, Vakantiecursus 1993, blz 23-34

[4] Bart Zevenhek, *Priemgetallen en de rij van Fibonacci*
Euclides december 2007, nr. 3, jaargang 83, blz. 108-110
zie ook: http://www.math.leidenuniv.nl/∼bzeven/

[5] Bart Zevenhek, *Periode en nulpunten van de rij van Fibonacci*
http://www.math.leidenuniv.nl/∼bzeven/

[6] Bart Zevenhek, *Profinite Fibonacci numbers revisited*
http://www.math.leidenuniv.nl/∼bzeven/

[7] Hendrik Lenstra, *Profinite Fibonacci numbers*
NAW 5/6 nr 4 december 2005, blz. 297
http://www.math.leidenuniv.nl/∼hwl/papers/fibo.pdf

# De kunst van het bewijzen

Freek Wiedijk
Radboud Universiteit Nijmegen

## 1 Lagere en hogere wiskunde

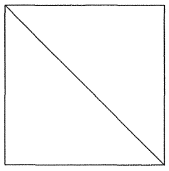
In de wiskunde kunnen we twee soorten van activiteiten onderscheiden:

- **Berekenen.** Hierbij gaat het om het *wat*.
- **Bewijzen.** Hierbij gaat het om het *waarom*.

Het gaat in deze classificatie om *groepen* van activiteiten. Zo vallen zowel het uitwerken van een merkwaardig product als het maken van een grafiek van een functie in de 'berekenen' categorie, terwijl het definiëren van een nieuw begrip in termen van al bestaande begrippen in de categorie 'bewijzen' valt. Merk op dat we met 'berekenen' niet alleen rekenen met getallen bedoelen, maar ook het symbolisch uitwerken van een antwoord (ook daarbij gaat het om het 'wat'.)

Men kan berekenen als 'lagere' wiskunde, en bewijzen als 'hogere' wiskunde beschouwen. Iemand die alleen de berekeningskant van de wiskunde kent heeft geen goed beeld van wat wiskunde is. Iemand met aanleg voor wiskunde die daarom wiskunde erg de moeite waard zou kunnen vinden, maar die de bewijzenkant van wiskunde niet kent, zal waarschijnlijk menen dat wiskunde een stuk saaier is dan het in werkelijkheid is.

Een voorbeeld van het onderscheid tussen deze twee soorten activiteit is de volgende. Bekijk het volgende plaatje van een diagonaal in een vierkant:



Hierover kunnen we de volgende twee vragen stellen:

- **Bereken** de verhouding tussen de lengte van de diagonaal van het vierkant en de lengte van de zijde van het vierkant. (Met de stelling van Pythagoras is het antwoord op deze vraag natuurlijk dat deze verhouding $\sqrt{2}$ is. Hierbij wordt de stelling van Pythagoras gebruikt als een *rekenregel*.)

- **Bewijs** dat de verhouding tussen de lengte van de diagonaal van het vierkant en de lengte van de zijde van het vierkant niet te schrijven is als de verhouding tussen twee gehele getallen. (En een bewijs hiervan is natuurlijk het klassieke bewijs van deze stelling uit de school van Pythagoras. We komen in Sectie 3 op dit bewijs terug.)

Het gaat hierbij duidelijk om twee heel verschillende soorten vragen.

Begin jaren zeventig werd er een nieuwe vorm van bewijzen ontwikkeld die *formalisatie* heet. Hierbij worden de bewijzen in de computer gecodeerd in een vorm waarbij een computerprogramma kan nagaan of deze bewijzen volledig correct zijn. Zo'n computerprogramma heet een *bewijschecker* of *bewijsassistent.*

Voordat de formalisatietechnologie was ontwikkeld was een bewijs altijd iets dat zich in een mensenhoofd afspeelde, en met schoolbord of papier aan andere wiskundigen werd doorgegeven. De wiskundigen realiseerden zich wel dat het mogelijk was bewijzen in een *formeel systeem* te representeren (dit is het onderwerp van de *mathematische logica*), maar hoewel wel geprobeerd werd dit echt te doen (het verst in de beroemde *Principia Mathematica* van Alfred North Whitehead en Bertrand Russell, dat gepubliceerd werd in 1910–1913), was het zonder computers te onpraktisch om op deze manier serieuze wiskunde weer te geven.

Begin jaren zeventig veranderde dit dus door de opkomst van de computer, en sindsdien bestaat er met formalisatie een vorm van wiskundig bewijzen die een objectieve status heeft, buiten de menselijke geest.

Met formalisatie heeft de kunst van het wiskundige bewijs een essentieel nieuwe vorm bereikt. We zullen in de rest van deze tekst een introductie geven tot formalisatie van wiskunde.

# 2 Wiskunde in de computer

*Computerwiskunde* is het gebruik van computers in de wiskunde. Dit bestaat in verschillende soorten, die significant van elkaar verschillen. Het gaat ons bij formalisatie om de vierde en laatste soort.

De soorten computerwiskunde zijn:

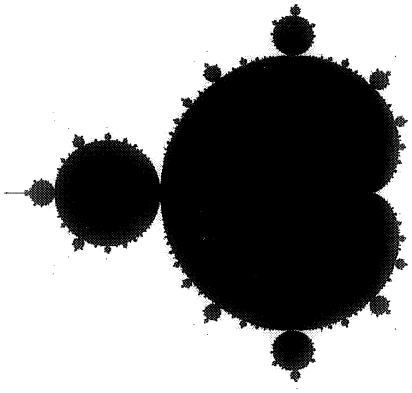
## Computerwiskunde soort 1: numerieke wiskunde

Hierbij worden computers gebruikt om met *getallen* te rekenen, het zogenaamde 'number crunching'. Hieronder valt ook het gebruik van computers voor visualisatie.

Bij het rekenen met computers wordt vaak gebruik gemaakt van 'floating point' ('drijvende komma') berekeningen volgens de zogenaamde IEEE 754 standaard, waarbij na iedere rekenkundige bewerking het resultaat wordt afgerond om de uitkomsten in een eindig aantal cijfers na de komma te kunnen

blijven representeren. Het zal duidelijk zijn dat hierdoor alleen een benadering van het wiskundig correcte antwoord wordt bereikt, en niet de exacte waarde.

Voor experimentatie en visualisatie is dit niet heel erg. Zo kan bijvoorbeeld een plaatje van de bekende Mandelbrot-verzameling:



(de verzameling van punten $c$ in het complexe vlak waarvoor de rij gegeven door $x_0 = 0$ en $x_{n+1} = {x_n}^2 + c$ niet naar het oneindige wegloopt) prima worden gemaakt met floating point-berekeningen. Het feit dat bij de rand misschien door afrondfouten een enkele pixel verkeerd wordt gekleurd geeft daarbij niets.

Evenwel kun je numerieke methoden ook gebruiken om wiskundig harde informatie te verzamelen. Om dit te bereiken moeten afrondfouten expliciet worden bijgehouden, zodat er bekend is wat de relatie tussen de uitkomst van de berekening en het wiskundig correcte antwoord is.

Dit betekent dat numerieke methoden ondanks de afrondfouten wel degelijk bruikbaar zijn om harde wiskundige bewijzen mee te ondersteunen.

Een voorbeeld van een bewijs waarbij numeriek gebruik van de computer essentieel was, was de ontkrachting in 1985 door Andrew Odlyzko en Herman te Riele van het *Mertens-vermoeden*. Het Mertens-vermoeden zegt dat voor de 'Mertens-functie'

$$M(n) = \sum_{k=1}^{n} \mu(k)$$

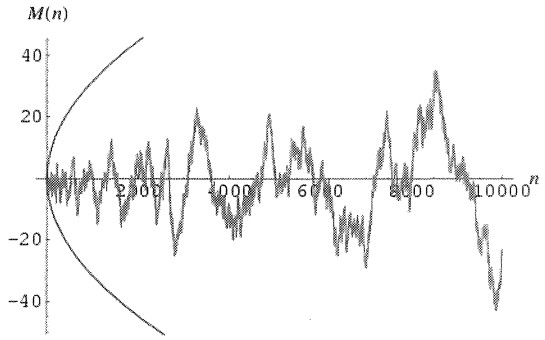
waarbij $\mu(k)$ de Möbius-functie is gedefinieerd door

$$\mu(k) = \begin{cases} 1 & \text{als } k \text{ kwadraatvrij is met een even aantal priemfactoren} \\ -1 & \text{als } k \text{ kwadraatvrij is met een oneven aantal priemfactoren} \\ 0 & \text{als } k \text{ deelbaar is door een kwadraat} \end{cases}$$

geldt dat

$$|M(n)| \leq \sqrt{n}$$

Numerieke evidentie lijkt erop te wijzen dat dit vermoeden waar is:




(het vermoeden zegt dat deze bibberlijn, die de grafiek van de Mertens-functie is, binnen de parabool blijft), maar uiteindelijk werd dus bewezen dat dit niet het geval is. Hiervoor was een ingewikkeld bewijs nodig. (Het is tot nog toe *niet* mogelijk gebleken om $M(n)$ expliciet uit te rekenen voor een $n$ die groot genoeg is dat $|M(n)| \leq \sqrt{n}$ niet langer geldt. In plaats daarvan werd het Mertens-vermoeden via een indirecte redenering weersproken.)

Voor dit bewijs waren 2000 nulpunten in het complexe vlak van de Riemann zeta-functie

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

nodig, met een precisie van minstens 100 decimalen:

$0.5 + i \cdot 14.134725141734693790457251983562470270784257115699243175685567460149963429809256764949010393171561012 7\ldots$
$0.5 + i \cdot 21.022039638771554992628479593896902777334340524902781754629520403587598586068890799713658514180151419 5\ldots$
$0.5 + i \cdot 25.010857580145688763213790992562821818659549672557996672496542006745092098441644277840238224558062440 7\ldots$
$0.5 + i \cdot 30.424876125859513210311897530584091320181560023715440180962146036993329389333277920290584293902089110 6\ldots$
$0.5 + i \cdot 32.935061587739189690662368964074903488812715603517039009280003440784815608630551005938848496135348724 5\ldots$
$0.5 + i \cdot 37.586178158825671257217763480705332821405597350830793218333001113622149089618537264730329104945823803 4\ldots$
$0.5 + i \cdot 40.918719012147495187398126914633254395726165962777279536161303667253280528720071282996003719889546875 5\ldots$
$0.5 + i \cdot 43.327073280914999519496122165406805782645668371836871446878893685521088322305053626456349371063190933 5\ldots$
$0.5 + i \cdot 48.005150881167159727942472749427516041686844001144425117775312519814090216416308281330335372305400997 7\ldots$
$0.5 + i \cdot 49.773832477672302181916784678563724057723178299676662100781955750433511611515739278732707507400931330 0\ldots$
*... nog 1990 nulpunten ...*

Dat is een veel grotere precisie dan de floating point-hardware van een computer levert, maar is prima met een computer te berekenen. En de ontkrachting van het Mertens-vermoeden is dus niet alleen 'correct op afrondfouten na', maar wiskundig volkomen zeker.

## Computerwiskunde soort 2: computer algebra

Bij computer algebra gaat het niet om het berekenen van getallen maar om *symbolisch* rekenen. Evenwel gaat het hier nog steeds om activiteiten uit de 'berekenen' categorie en niet uit de 'bewijzen' categorie. De bekendste computerprogramma's voor computer algebra zijn Mathematica en Maple.

Een voorbeeld van een 'berekening' die een computer algebra systeem voor je kan doen is het symbolisch uitrekenen van een integraal (dit voorbeeld is een Maple sessie):

```
> Int(ln(x)/(1 - x), x = 0..1);
```

$$\int_0^1 \frac{\ln x}{1-x}\,dx$$

```
> value(%);
```

$$-\frac{\pi^2}{6}$$

```
> evalf(%);
```

$$-1.644934068$$

Het is duidelijk dat Maple de integraal zowel symbolisch als numeriek kan uitrekenen.

Evenwel is er *niet* duidelijk *hoe* Maple aan zijn antwoord is gekomen. Het gaat hier om een berekening en niet om een bewijs.

Ook was Maple iets te onvoorzichtig met de afronding. De echte waarde van de integraal is $-1.644934066848...$ wat afrondt naar $-1.644934067$ en niet naar $-1.644934068$. Hoewel dat niet *heel* erg incorrect is, is incorrectheid van resultaten van computer algebra systemen (om verschillende redenen, maar vooral door te enthousiaste vereenvoudigingen) een algemeen fenomeen. Resultaten van computer algebra moeten dus altijd met een kritisch oog gebruikt worden.

Computer algebra systemen bevatten allerlei hele krachtige algoritmen om symbolisch te rekenen. Een voorbeeld hiervan is het *algoritme van Risch*, die *als* de uitkomst van een onbepaalde integraal in 'gesloten vorm' (een expressie in termen van de rekenkundige bewerkingen en de elementaire transcendente functies, te weten: exponentiatie, logaritme, de trigonometrische en de inverse trigonometrische functies) kan worden geschreven dit altijd zal doen, en dat ook altijd zal vertellen *of* de integraal in zo'n gesloten vorm te schrijven is. Evenwel is het algoritme van Risch zo verschrikkelijk ingewikkeld dat bestaande software tot nog toe altijd alleen maar een deel ervan heeft geïmplementeerd.

## Computerwiskunde soort 3: automatische stellingenbewijzers

Bij computer algebra *berekent* de computer, maar bij automatische stellingenbewijzers levert de computer automatisch *bewijzen*. De gebruiker geeft het programma een uitspraak, en het systeem probeert hier automatisch een bewijs voor te vinden.

Er is een hele industrie van dit soort programma's, die allemaal proberen om zoveel mogelijk uitspraken automatisch te kunnen bewijzen. De bekendste programma's van dit type zijn Otter (met als recente opvolger een stellingenbewijzer met de naam 'Prover9'), Vampire en de E prover.

Om deze programma's te ontwikkelen en te vergelijken is er een database van 'problemen' gemaakt met de naam TPTP ('Thousands of Problems for

Theorem Provers') waar momenteel 7.068 problemen in zitten. Ook is er jaarlijks de CASC competitie ('CADE Systems Competition') als onderdeel van de CADE conferentie ('Conference on Automated Deduction'). Deze competitie wordt vrijwel altijd door Vampire gewonnen.

Helaas staan dit soort programma's nog in de kinderschoenen. Er zijn eigenlijk geen interessante wiskundige bewijzen die door dit soort programma's automatisch gevonden kunnen worden. Zelfs voor een kleine stapje in een bewijs, iets wat een mens onmiddellijk ziet, zijn ze vaak nog te zwak. De stellingen die dit soort programma's kunnen bewijzen zijn altijd of van het type 'puzzel', of van een vorm dat het bewijs bestaat uit het nagaan van een groot aantal gevallen, zonder dat er enige creativiteit voor nodig is.

Het gaat bij deze programma's dus eerder om onderzoek in het onderzoeksgebied van de *kunstmatige intelligentie*, dan om software die bruikbaar is om echte wiskunde mee te doen.

Er zijn *enkele* bewijzen die met de hulp van automatische stellingenbewijzers zijn gevonden. Het bekendste hiervan is het bewijs van het Robbins-vermoeden. Robbins vroeg zich af welke structuren er allemaal zijn waarin de volgende drie vergelijkingen gelden:

$$a \vee b = b \vee a$$
$$a \vee (b \vee c) = (a \vee b) \vee c$$
$$\neg(\neg(a \vee b) \vee \neg(a \vee \neg b) = a$$

Een verzameling met daarop een unaire operatie $\neg$ en een binaire operatie $\vee$ die hieraan voldoet (voor alle $a$, $b$ en $c$ uit de verzameling) heet een *Robbins algebra*. Robbins vroeg zich af of iedere Robbins algebra altijd de structuur van een *Boolse algebra* heeft. Een Boolse algebra is een structuur waarin je de objecten als verzamelingen kunt representeren waarbij dan $\neg$ complementatie ten opzichte van een grootste verzameling en $\vee$ vereniging van verzamelingen zijn. Het blijkt inderdaad zo te zijn dat een Robbins algebra altijd een Boolse algebra is.

Het Robbins-vermoeden was onbewezen van 1933 tot 1996, en beroemde wiskundigen hebben er aan gewerkt zonder het op te lossen. Uiteindelijk werd het opgelost met de hulp van de automatische stellingenbewijzer EQP, een variant van Otter, die daar (in 1996) acht dagen computertijd voor nodig had. Het uiteindelijke bewijs was overigens vrij kort en bestond uit slechts 34 stappen, die zelfs door een mens gecontroleerd kunnen worden.

Hoewel bij het Robbins-vermoeden de computer (met menselijke sturing) een onopgelost probleem wist op te lossen, ging het hierbij om een probleem van het type 'bekijk zeer veel gevallen'. Zoals al gezegd zijn automatische stellingenbewijzers nauwelijks bruikbaar voor het doen van wiskunde, en alleen nuttig bij dit specifieke soort problemen.

### Computerwiskunde soort 4: bewijsassistenten

Dit zijn de systemen voor *formalisatie*. Hierbij gaat het om het uitwerken van wiskundige bewijzen met de computer. Evenwel is het nu niet de computer die het bewijs produceert, maar de mens. De computer fungeert slechts als 'domme boekhouder' die het bewijs netjes op een rijtje zet, en ervoor zorgt dat de mens zich niet vergist. Hoogstens helpt de computer soms een beetje met de eenvoudigste stapjes van het bewijs.

De meeste bewijsassistenten zijn ontwikkeld voor het doen van bewijzen in de informatica. Het gaat daarbij om het bewijzen van eigenschappen van hardware of van software. Zo worden bewijsassistenten gebruikt om te bewijzen dat microprocessors en *compilers* voor programmeertalen geen 'bugs' bevatten.

De bekendste bewijsassistenten van dit type zijn HOL, Isabelle, Coq, PVS en ACL2. Hoewel deze voor informatica-toepassingen zijn ontwikkeld, zijn ze ook bruikbaar om wiskundige bewijzen op correctheid te controleren. In de volgende sectie zullen we in detail kijken naar die systemen die specifiek voor wiskunde erg geschikt zijn.

Er kunnen dus vier soorten computerwiskunde worden onderscheiden. Idealiter zou je een systeem willen hebben waarin al deze soorten tot een geheel zijn samengevoegd. Helaas bestaat zo'n systeem nog niet. Het ontwikkelen van een dergelijk systeem is het onderwerp van een internationaal project met de naam *Calculemus*. Dit is een citaat van de laat-zeventiende eeuwse filosoof Gottfried Leibniz. Hij was één van de eersten die inzag dat redeneren in een formeel systeem mogelijk is. Hij had een wereld voor ogen waar bij inhoudelijke meningsverschillen (ook in de politiek) er zou kunnen worden *uitgerekend* wie er gelijk heeft. In dat geval zou men zeggen 'Calculemus!' ('laten we het uitrekenen!'), en zou er daarna geen onenigheid meer kunnen zijn.

Uiteraard is dit, ondanks de stormachtige ontwikkeling van de computerwiskunde, nog altijd een utopie.

## 3 Vier bewijsassistenten voor wiskunde

Stel je hebt een wiskundig bewijs, en je wil zeker weten dat bewijs absoluut correct is. Wat je dan moet doen is het bewijs invoeren in een bewijsassistent, die dan de correctheid van het bewijs voor je controleert. De eerste stap die je dan moet nemen is het selecteren van de bewijsassistent die je daarvoor wilt gebruiken.

Nu bestaan er veel bewijsassistenten, en zelfs al veel bewijsassistenten die voor specifiek wiskundige bewijzen geschikt zijn. Een overzicht van een aantal van deze bewijsassistenten is te vinden in het boekje *The Seventeen Provers of the World*, dat in de Springer LNAI reeks is uitgegeven als deeltje 3600. De voorbeelden in deze sectie komen uit dit boekje. De bijbehorende formalisaties kunnen worden gevonden op de webpagina:

http://www.cs.ru.nl/~freek/comparison/

In *The Seventeen Provers of the World* wordt voor elke bewijsassistent een bewijs van de irrationaliteit van $\sqrt{2}$ (de eigenschap van de diagonaal van het vierkant op pagina 128) als formalisatie gepresenteerd.

Er zijn dus minstens zeventien bewijsassistenten die bruikbaar zijn voor wiskunde. Hieronder zijn zowel de populaire bewijsassistenten van vandaag die boven al werden genoemd – HOL, Isabelle, Coq, PVS en ACL2 – als bewijsassistenten die specifiek zijn ontworpen voor het formaliseren van wiskunde – zoals Mizar en Metamath.

Enige tijd geleden vond ik een top 100 van 'leuke stellingen' op het Internet. In deze lijst stonden een groot aantal stellingen waarvan ik wist dat er al een bewijs van was geformaliseerd. En de irrationaliteit van $\sqrt{2}$ was zelfs de eerste in de lijst! Vandaar dat ik een onderzoekje begon naar welke van deze stellingen in welke systemen waren geformaliseerd. Het resultaat hiervan staat op de webpagina:

http://www.cs.ru.nl/~freek/100/

Momenteel zijn er 80 van de 100 stellingen geformaliseerd. En hier is dit aantal uitgesplitst naar bewijsassistent:

| | |
|---|---|
| HOL Light | 69 |
| Mizar | 44 |
| ProofPower | 42 |
| Isabelle | 40 |
| Coq | 39 |
| PVS | 15 |
| ACL2 | 12 |

Het moge duidelijk zijn dat er vijf systemen zijn die echt gebruikt zijn voor het formaliseren van wiskunde: HOL Light, Mizar, ProofPower, Isabelle en Coq. Nu zijn HOL Light en ProofPower vrijwel hetzelfde systeem (ze zijn allebei herimplementaties van het HOL systeem), en heeft HOL Light een betere bibliotheek van geformaliseerde wiskunde. Daarom zullen we hier ProofPower buiten beschouwing laten.

Dat laat vier systemen over die we nu één voor één onder de loep zullen nemen: HOL Light, Isabelle, Coq en Mizar.

## HOL Light

HOL is misschien wel de meest bekende bewijsassistent. Het systeem werd ontwikkeld in Engeland aan de Universiteit van Cambridge door Michael Gordon. Omdat het zo bekend is zijn er in de loop van de tijd een aantal herimplementaties van gemaakt, waaronder HOL Light en ProofPower. (Het originele HOL systeem heet nu HOL4.) Het Isabelle systeem is ook een variant van HOL, maar één die inmiddels wat meer van het originele systeem is gaan verschillen.

HOL Light werd ontwikkeld door John Harrison als onderdeel van zijn promotieonderzoek aan de Universiteit van Cambridge. Het is een zeer elegante en gestroomlijnde versie van HOL, en is door John Harrison gebruikt voor het formaliseren van allerlei stukken van de wiskunde (wat hij doet naast zijn baan bij Intel waar hij floating point processors correct bewijst).

*John Harrison*

Hier is hoe een bewijs er in HOL Light uitziet (dit lijkt sterk op hoe het er in de andere varianten van HOL uitziet):

```
let NSQRT_2 = prove
 (`!p q. p * p = 2 * q * q ==> q = 0`,
  MATCH_MP_TAC num_WF THEN REWRITE_TAC[RIGHT_IMP_FORALL_THM] THEN
  REPEAT STRIP_TAC THEN FIRST_ASSUM(MP_TAC o AP_TERM `EVEN`) THEN
  REWRITE_TAC[EVEN_MULT; ARITH] THEN REWRITE_TAC[EVEN_EXISTS] THEN
  DISCH_THEN(X_CHOOSE_THEN `m:num` SUBST_ALL_TAC) THEN
  FIRST_X_ASSUM(MP_TAC o SPECL [`q:num`; `m:num`]) THEN
  POP_ASSUM MP_TAC THEN CONV_TAC SOS_RULE);;

let SQRT_2_IRRATIONAL = prove
 (`~rational(sqrt(&2))`,
  SIMP_TAC[rational; real_abs; SQRT_POS_LE; REAL_POS; NOT_EXISTS_THM] THEN
  REPEAT GEN_TAC THEN DISCH_THEN(CONJUNCTS_THEN2 ASSUME_TAC MP_TAC) THEN
  DISCH_THEN(MP_TAC o AP_TERM `\x. x pow 2`) THEN
  ASM_SIMP_TAC[SQRT_POW_2; REAL_POS; REAL_POW_DIV; REAL_POW_2; REAL_LT_SQUARE;
               REAL_OF_NUM_EQ; REAL_EQ_RDIV_EQ] THEN
  ASM_MESON_TAC[NSQRT_2; REAL_OF_NUM_EQ; REAL_OF_NUM_MUL]);;
```

Het eerste lemma zegt dat voor natuurlijke getallen

$$p^2 = 2q^2$$

alleen kan gelden als

$$q = 0$$

Het zal duidelijk zijn dat de bewijzen die hier worden gecodeerd alleen te begrijpen zijn door de 'scripts' die hier staan op een computer te executeren. (We

zullen hier niet uitleggen welk bewijs hier precies staat. Het voorbeeld dient slechts om een indruk te geven van hoe geformaliseerde wiskunde er uit ziet.)

De webpagina van het HOL Light systeem is:

`http://www.cl.cam.ac.uk/~jrh13/hol-light/`

Het HOL Light systeem is moeilijk te leren, en waarschijnlijk buiten het bereik van iemand zonder achtergrond in de logica, en zonder hulp van iemand die direct naast hem of haar achter de computer zit.

## Isabelle

Het Isabelle systeem is ook een variant van HOL, maar is daarna verder ontwikkeld en lijkt tegenwoordig niet meer zo op de oorspronkelijke HOL. Het is ontwikkeld in Engeland door Larry Paulson van de Universiteit van Cambridge en in Duitsland door Tobias Nipkow en Markus Wenzel van de Technische Universiteit München.

Isabelle is waarschijnlijk het breedste systeem voor het formaliseren van wiskunde. Het combineert eigenschappen van allerlei andere systemen in een gebalanceerd geheel. Hier is hoe een bewijs er in Isabelle uitziet:

```
theorem sqrt_prime_irrational: "p ∈ prime ⟹ sqrt (real p) ∉ ℚ"
proof
  assume p_prime: "p ∈ prime"
  then have p: "1 < p" by (simp add: prime_def)
  assume "sqrt (real p) ∈ ℚ"
  then obtain m n where
      n: "n ≠ 0" and sqrt_rat: "|sqrt (real p)| = real m / real n"
    and gcd: "gcd (m, n) = 1" ..
  have eq: "m^2 = p * n^2"
  proof -
    from n and sqrt_rat have "real m = |sqrt (real p)| * real n" by simp
    then have "real (m^2) = (sqrt (real p))^2 * real (n^2)"
      by (auto simp add: power_two real_power_two)
    also have "(sqrt (real p))^2 = real p" by simp
    also have "... * real (n^2) = real (p * n^2)" by simp
    finally show ?thesis ..
  qed
  have "p dvd m ∧ p dvd n"
  proof
    from eq have "p dvd m^2" ..
    with p_prime show "p dvd m" by (rule prime_dvd_power_two)
    then obtain k where "m = p * k" ..
    with eq have "p * n^2 = p^2 * k^2" by (auto simp add: power_two mult_ac)
    with p have "n^2 = p * k^2" by (simp add: power_two)
    then have "p dvd n^2" ..
    with p_prime show "p dvd n" by (rule prime_dvd_power_two)
  qed
  then have "p dvd gcd (m, n)" ..
```

```
  with gcd have "p dvd 1" by simp
  then have "p ≤ 1" by (simp add: dvd_imp_le)
  with p show False by simp
qed

corollary "sqrt (real (2::nat)) ∉ ℚ"
  by (rule sqrt_prime_irrational) (rule two_is_prime)
```

Het is hopelijk duidelijk dat een Isabelle bewijs in tegenstelling tot een HOL bewijs ook zonder computer te begrijpen valt.

De webpagina van het Isabelle systeem is:

`http://isabelle.in.tum.de/`

Isabelle is makkelijker te leren dan de traditionele HOL systemen, maar er is waarschijnlijk toch nog steeds een gedegen kennis van de mathematische logica voor nodig om enigszins met Isabelle uit de voeten te kunnen.

## Coq

Het Coq systeem is ontwikkeld in Frankrijk door INRIA, het Franse onderzoeksinstituut voor informatica. Oorspronkelijk is de ontwikkeling ervan begonnen door Gérard Huet en Thierry Coquand, maar in de loop van de tijd is er door vele mensen aan gewerkt.

Coq lijkt aan de ene kant sterk op HOL, in de zin dat de manier van bewijzen in beide systemen erg verwant is, en dat daardoor Coq bewijzen net als HOL bewijzen ook niet zonder computer te begrijpen zijn:

```
Theorem main_thm: forall (n p : nat), n * n = double (p * p) ->  p = 0.
intros n; pattern n; apply lt_wf_ind; clear n.
intros n H p H0.
case (eq_nat_dec n 0); intros H1.
generalize H0; rewrite H1; case p; auto; intros; discriminate.
assert (H2: even n).
apply even_is_even_times_even.
apply double_even; rewrite H0; rewrite double_div2; auto.
assert (H3: even p).
apply even_is_even_times_even.
rewrite <- (double_inv (double (div2 n * div2 n)) (p * p)).
apply double_even; rewrite double_div2; auto.
rewrite main_thm_aux; auto.
assert (H4: div2 p = 0).
apply (H (div2 n)).
apply lt_div2; apply neq_0_lt; auto.
apply double_inv; apply double_inv; (repeat rewrite main_thm_aux); auto.
rewrite (even_double p); auto; rewrite H4; auto.
Qed.
```

Evenwel zijn er ook een aantal verschillen. In twee opzichten staat Coq veel meer in de Nederlandse traditie dan de HOL varianten.

Ten eerste representeert Coq bewijzen intern met behulp van de zogenaamde *lambda-calculus*. Dit is een aanpak die zijn oorsprong heeft in één van de allereerste bewijsassistenten ooit (er werd al aan begonnen in 1968), het Automath systeem. Dit was een Nederlandse product, ontwikkeld door N.G. de Bruijn en zijn onderzoeksgroep aan de Technische Universiteit Eindhoven.

*N.G. de Bruijn*

Eén van de vooraanstaande experts op het gebied van de lambda-calculus is Henk Barendregt van de Radboud Universiteit Nijmegen, vandaar dat aan deze universiteit veel met Coq geformaliseerd wordt.

Ten tweede werkt Coq met een variant van wiskunde die *intuïtionisme* wordt genoemd. Deze soort wiskunde werd ontwikkeld door L.E.J. Brouwer in het begin van de twintigste eeuw om de paradoxen in de logica die toen werden ontdekt te vermijden. Evenwel is het intuïtionisme nooit meer dan een marginale stroming geworden, en is vrijwel alle hedendaagse wiskunde niet-intuïtionistisch. Om een voorbeeld te geven van hoe intuïtionisme afwijkt van gewone wiskunde: in het intuïtionisme kun je niet bewijzen dat ieder reëel getal altijd óf gelijk is aan nul, óf verschillend van nul. Een wat geavanceerdere stelling die hierdoor in het intuïtionisme onbewijsbaar is, is de *tussenwaardenstelling*: dat een continue functie van $\mathbb{R}$ naar $\mathbb{R}$ die ergens negatief en ergens anders positief is altijd een nulpunt heeft.

*L.E.J. Brouwer*

De intuïtionistische basis van Coq is geen reden om Coq niet te gebruiken. Dit komt omdat je in Coq ook op de gewone, niet-intuïtionistische manier kunt redeneren. Veel Coq-gebruikers, inclusief de meeste Coq-gebruikers aan de Radboud Universiteit, werken desondanks intuïtionistisch.

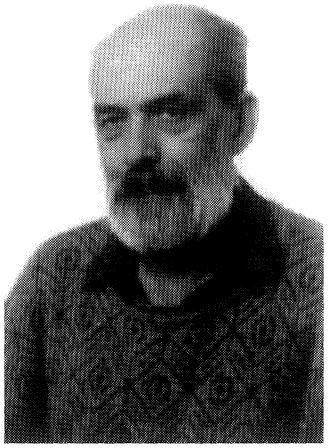
De webpagina van het Coq systeem is:

`http://coq.inria.fr/`

Coq is ongeveer even moeilijk te leren als Isabelle. Dat betekent dat je een stevige basis in de mathematische logica moet hebben voordat je met Coq aan de slag kunt gaan.

## Mizar

Het Poolse systeem Mizar, ontwikkeld door Andrzej Trybulec aan de universiteit van Białystok, is een beetje een vreemde eend in de bijt tussen deze vier systemen. Ten eerste is het specifiek voor wiskunde ontworpen, terwijl de andere drie systemen in eerste instantie voor informatica-toepassingen zijn ontwikkeld. Ten tweede is het systeem lange tijd 'achter het ijzeren gordijn' ontwikkeld, zonder veel contact met de rest van de onderzoeksgemeenschap voor bewijsassistenten. Hierdoor verschilt het in veel opzichten van de andere systemen.



*Andrzej Trybulec*

Evenwel worden er tegenwoordig meer en meer concepten van het Mizar systeem door andere systemen overgenomen. Zo is de bewijstaal van Isabelle direct gebaseerd op de bewijstaal van Mizar:

```
theorem
  sqrt 2 is irrational
proof
 assume sqrt 2 is rational;
 then consider i being Integer, n being Nat such that
W1: n<>0 and
W2: sqrt 2=i/n and
W3: for i1 being Integer, n1 being Nat st n1<>0 & sqrt 2=i1/n1 holds n<=n1
      by RAT_1:25;
A5: i=sqrt 2*n by W1,XCMPLX_1:88,W2;
C: sqrt 2>=0 & n>0 by W1,NAT_1:19,SQUARE_1:93;
 then i>=0 by A5,REAL_2:121;
 then reconsider m = i as Nat by INT_1:16;
A6: m*m = n*n*(sqrt 2*sqrt 2) by A5
  .= n*n*(sqrt 2)^2 by SQUARE_1:def 3
  .= 2*(n*n) by SQUARE_1:def 4;
 then 2 divides m*m by NAT_1:def 3;
 then 2 divides m by INT_2:44,NEWTON:98;
 then consider m1 being Nat such that
W4: m=2*m1 by NAT_1:def 3;
 m1*m1*2*2 = m1*(m1*2)*2
    .= 2*(n*n) by W4,A6,XCMPLX_1:4;
 then 2*(m1*m1) = n*n by XCMPLX_1:5;
 then 2 divides n*n by NAT_1:def 3;
 then 2 divides n by INT_2:44,NEWTON:98;
```

```
 then consider n1 being Nat such that
W5: n=2*n1 by NAT_1:def 3;
A10: m1/n1 = sqrt 2 by W4,W5,XCMPLX_1:92,W2;
A11: n1>0 by W5,C,REAL_2:123;
  then 2*n1>1*n1 by REAL_2:199;
 hence contradiction by A10,W5,A11,W3;
end;
```

In Sectie 5 verderop zullen twee andere kleine Mizar-formalisaties in enig detail worden uitgelegd.

Mizar heeft de grootste bibliotheek van geformaliseerde stellingen van alle momenteel bestaande bewijsassistenten. De Mizar Mathematical Library (MML) bestaat uit 1.005 zogenaamde *artikelen*, formalisaties van een paar duizend regels per stuk, en is in totaal 68 megabyte ofwel 2,1 miljoen regels code groot, waarin in totaal 55.536 kleinere en grotere stellingen worden bewezen.

De webpagina van Mizar is:

`http://www.mizar.org/`

Mizar is door de bank genomen geen moeilijk systeem, maar het heeft een paar moeilijke kanten en er is helaas weinig documentatie, waardoor het toch niet aan te bevelen is om zonder hulp Mizar proberen te leren.

# 4 Geformaliseerde stellingen

Toen bewijsassistenten voor het eerst werden geïntroduceerd (door N.G. de Bruijn in Nederland dus) verwachten velen dat de technologie niet voor serieuze bewijzen bruikbaar zou zijn. In het begin van de twintigste eeuw hadden Alfred North Whitehead en Bertrand Russell al geprobeerd bewijzen in volledige precisie op te schrijven in hun *Principia Mathematica*, en daarin was het pas op pagina 379 gelukt om de stelling

$$1 + 1 = 2$$

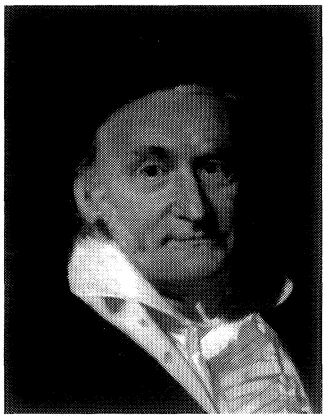
te bewijzen. Om deze reden ging men er aanvankelijk van uit dat het onpraktisch was serieuze wiskunde op een soortgelijke manier te behandelen.

Deze verwachting is niet bewaarheid: men had buiten de enorme toegevoegde waarde van het gebruik van computers gerekend. In de loop van de tijd zijn er meerdere zeer niet-triviale stellingen geformaliseerd. We bespreken nu de markantste voorbeelden.

## De hoofdstelling van de algebra

Deze stelling was het onderwerp van het proefschrift van de 'Prins der Wiskundigen' Carl Friedrich Gauss. Dit proefschrift getiteld *Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse*, ofwel *Een nieuw*

*bewijs van de stelling dat iedere gehele rationale algebraïsche functie van één variabele in reële factoren van de eerste of tweede graad kan worden opgelost*, werd gepubliceerd in 1799. Gauss gaf in de loop van zijn leven vier bewijzen van de hoofdstelling van de algebra.



*Carl Friedrich Gauss*

De stelling zegt dat *iedere* niet-triviale vergelijking met alleen de basale rekenkundige operaties (optellen, aftrekken, vermenigvuldigen en delen) in de complexe getallen altijd een oplossing heeft. Voor de reële getallen geldt dit niet. Er is bijvoorbeeld geen reëel getal $x$ waarvoor

$$x^2 + 1 = 0$$

Maar als we zo'n getal, $i = \sqrt{-1}$, toevoegen geldt dit wel, en geldt dit zelfs voor alle andere vergelijkingen, inclusief de vergelijkingen die we met deze extra getallen kunnen maken. Zo hoeven we bijvoorbeeld niet ook een wortel van $i$ toe te voegen, want de vergelijking

$$x^2 - i = 0$$

heeft al de oplossingen

$$x = \frac{1}{2}\sqrt{2} + i\frac{1}{2}\sqrt{2} \quad \text{en} \quad x = -\frac{1}{2}\sqrt{2} - i\frac{1}{2}\sqrt{2}$$

De hoofdstelling van de algebra is in meerdere bewijsassistenten geformaliseerd. Er zijn formalisaties in Mizar, in HOL Light, in Coq (een intuïtionistisch bewijs, geformaliseerd aan de Radboud Universiteit Nijmegen) en in Isabelle.

## De priemgetalstelling

We bedoelen met de priemgetalstelling *niet* de simpele stelling dat er oneindig veel priemgetallen zijn, maar de veel sterkere stelling dat de priemgetallen in de

buurt van $n$ ongeveer een dichtheid van $1/\ln(n)$ hebben. De precieze uitspraak van de priemgetalstelling is dat

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1$$

waarbij $\pi(n)$ het aantal priemgetallen kleiner of gelijk $n$ is. Om een indruk te geven van hoe goed deze limiet convergeert: voor $n$ een biljoen (dus $n = 1.000.000.000.000$) geldt dat

$$\pi(n) = 37.607.912.018$$

(er zijn dus dit aantal priemgetallen kleiner dan een biljoen), terwijl

$$\frac{n}{\ln(n)} = 36.191.206.825,27\ldots$$

Een betere benadering krijg je overigens door de uitspraak over de dichtheid van $1/\ln(n)$ serieus te nemen en de *logaritmische integraal* uit te rekenen:

$$\mathrm{li}(n) = \int_0^n \frac{dt}{\ln(t)} = 37.607.950.280,80\ldots$$

(Het is makkelijk te bewijzen dat de priemgetalstelling equivalent is aan de stelling die zegt dat de limiet van de verhouding van $\pi(n)$ en $\mathrm{li}(n)$ ook naar één gaat.)

Het bewijs van deze stelling door Jacques Hadamard en Charles-Jean de la Vallée-Poussin, voortbouwend op de ideeën van Bernhard Riemann, was één van de hoogtepunten van de negentiende eeuwse wiskunde. Het maakt essentieel gebruik van de analytische theorie over complexe functies, en gebruikt in het bijzonder eigenschappen van de verdeling van de complexe nulpunten van de Riemann zeta-functie

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

die we boven al hebben genoemd. Midden twintigste eeuw werd er door Atle Selberg en Paul Erdős ook een 'elementair' bewijs gevonden dat geen analyse nodig heeft.

Beide bewijzen van de priemgetalstelling zijn geformaliseerd. Het analytische bewijs uit de negentiende eeuw die een heleboel complexe functietheorie nodig heeft is zeer recent geformaliseerd door John Harrison in HOL Light, en het elementaire bewijs was al eerder geformaliseerd in Isabelle door een groepje mensen onder leiding van Jeremy Avigad van de Carnegie Mellon universiteit.

## De stelling over Jordan-krommen

Deze stelling is interessant omdat het een heel eenvoudige uitspraak betreft die als je hem probeert te bewijzen heel erg moeilijk blijkt. Hij werd bewezen door

Oswald Veblen in 1905, en leidde tot het vakgebied van de *topologie*, waarvan bovengenoemde L.E.J. Brouwer één van de grondleggers is geweest. De stelling zegt dat iedere *Jordan kromme* (een continue gesloten kromme in het platte vlak die zichzelf niet doorsnijdt: een gesloten lus dus) het vlak in precies twee delen verdeelt, een eindige binnenkant en een oneindige buitenkant, waarbij de kromme de rand van beide delen is. Intuïtief lijkt het alsof hier niets te bewijzen is ('dat zie je toch zo'), maar als je het wiskundig precies maakt is dit dus een moeilijk resultaat.

In het Mizar project is er jaren gewerkt aan de formalisatie van een bewijs van deze stelling, vooral omdat er voor een onhandig bewijs was gekozen. Inmiddels zijn er twee formalisaties, één in HOL Light door Tom Hales, en één in Mizar door een groep mensen onder leiding van Andrzej Trybulec, waarbij het bewijs uiteindelijk werd voltooid door Artur Korniłowicz.

## De onvolledigheidsstelling van Gödel

Dit is waarschijnlijk de beroemdste stelling van de twintigste eeuw, bewezen door Kurt Gödel in 1931. De stelling komt erop neer dat voor *iedere* enigszins redelijke collectie axioma's er ware uitspraken bestaan die niet uit die axioma's bewezen kunnen worden. (Om het interessant te maken heeft Gödel ook een *volledigheidsstelling* – die ook heel belangrijk is, en trouwens ook geformaliseerd – maar de onvolledigheidsstelling is veel schokkender.)

In feite zijn er *twee* onvolledigheidsstellingen, de eerste en de tweede. De tweede onvolledigheidsstelling voegt aan de eerste toe dat je uit een *consistent* stel axioma's – dat betekent dat je met de axioma's geen onwaarheden kan bewijzen – nooit kan bewijzen dat die axioma's inderdaad consistent zijn. Een systeem kan zijn eigen redelijkheid niet inzien, zeg maar.

De eerste onvolledigheidsstelling is een aantal keer geformaliseerd: in een voorganger van ACL2 door Natarajan Shankar (de maker van de PVS bewijsassistent), in Coq door Russell O'Connor, en in HOL Light door John Harrison. De tweede onvolledigheidsstelling is tot vandaag niet geformaliseerd, hoewel er wel een aantal mensen mee bezig is.

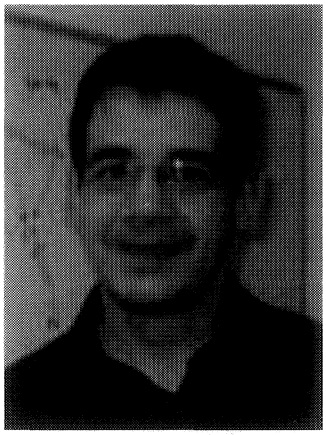
## De vierkleurenstelling

Deze stelling zegt dat je bij een kaart met een aantal landen altijd ieder land één van vier kleuren kan geven op zo'n manier dat er dan geen twee landen met dezelfde kleur aan elkaar grenzen.

Deze stelling was lange tijd een open probleem, en werd pas bewezen in 1975 door Kenneth Appel en Wolfgang Haken. Daarbij gebruikten ze een heleboel computertijd om ontzettend veel kleuringen van 1.936 specifieke kaarten te analyseren. Om deze reden was hun bewijs omstreden, aangezien het niet mogelijk was het bewijs te geloven zonder een computer te hoeven vertrouwen.

In 1996 werd het bewijs nog eens dunnetjes overgedaan door Neil Robertson, Daniel P. Sanders, Paul Seymour en Robin Thomas, waarbij het werd

teruggebracht tot een veel overzichtelijker vorm. Het bewijs en de bijbehorende computerprogramma's waren nu nog maar enige tientallen pagina's lang, en er waren nog maar 633 in plaats van 1.936 kaarten die moesten worden geanalyseerd.



*Georges Gonthier*

In 2004 werd de vierkleurenstelling in Coq geformaliseerd door Georges Gonthier, met de hulp van Benjamin Werner. Dit is één van de meest indrukwekkende formalisaties tot nog toe. In deze formalisatie werden zowel de computerprogramma's uit het bewijs correct bewezen, als de hele topologische theorie die bij het probleem hoort geformaliseerd.

Voor dit project werd door Georges Gonthier speciaal een nieuwe bewijstaal voor Coq ontwikkeld met de naam *ssreflect*. Deze taal geldt als een enorme stap voorwaarts in hoe efficiënt met het Coq systeem bewijzen kunnen worden geformaliseerd. Helaas is er momenteel nog geen goede documentatie van deze taal beschikbaar, en is deze dus nog moeilijk te leren.

Georges Gonthier werkt voor Microsoft research, en er is een instituut opgericht als samenwerking tussen Microsoft en INRIA, waarin hij momenteel met een groepje mensen de moeilijke Feit-Thompson stelling uit de groepentheorie aan het formaliseren is. Dit als mogelijke aanloop naar een toekomstige formalisatie van de beruchte stelling over de classificatie van de eindige groepen.

# 5 Voorbeelden van formalisaties

We zullen nu twee eenvoudige voorbeelden van een formalisatie laten zien. Omdat het het makkelijkst is om Mizar formalisaties te begrijpen (hoewel het helaas niet zo makkelijk is om Mizar te leren schrijven) hebben we hier gekozen voor voorbeelden in Mizar.

## Geen grootste getal

Het eerste voorbeeld is een formalisatie van een vrolijk rijmpje van Marjolein Kool dat ik vond op het weblog van de wiskundemeisjes, Ionica Smeets en Jeanine Daems:

`http://www.wiskundemeisjes.nl/`

Het gaat om een bewijs van de volkomen triviale stelling dat er geen grootste getal bestaat. We geven nu het rijmpje, met daarnaast hetzelfde bewijs in de Mizar bewijstaal:

*Een bolleboos riep laatst met zwier*
*gewapend met een vel A-vijf:*
*Er is geen allergrootst getal,*
*dat is wat ik bewijzen ga.*
*Stel, dat ik u nu zou bedriegen*
*en hier een potje stond te jokken,*
*dan ik zou zonder overdrijven*
*het grootste kunnen op gaan noemen.*
*Maar ben ik klaar, roept u gemeen:*
*'Vermeerder dat getal met twee!'*
*En zien we zeker en gewis*
*dat dit toch niet het grootste was.*
*En gaan we zo nog door een poos,*
*dan merkt u: dit is onbegrensd.*
*En daarmee heb ik q.e.d.*
*Ik ben hier diep gelukkig door.*
*'Zo gaan', zei hij voor hij bezwijmde,*
*'bewijzen uit het ongedichte'.*

```
theorem
  not ex n st for m holds n >= m
proof

  assume not thesis;
  then consider n such that
    for m holds n >= m;

  set n' = n + 2;

  n' > n;

  then not for m holds n >= m;

  hence contradiction;

end;
```

Mizar vindt deze vertaling helaas niet acceptabel. Het systeem kan namelijk niet uit zichzelf begrijpen waarom de twee onderstreepte regels volgen. In het bijzonder moeten we het systeem vertellen dat de contradictie volgt met de eigenschap van $n$, en ook is er een lemma nodig met de naam `XREAL_1:31`

`0 < a implies b < b+a`

om te bewijzen dat $n' > n$. Als we zo deze formalisatie afmaken wordt het:

```
theorem
  not ex n st for m holds n >= m
proof
  assume not thesis;
  then consider n such that
A1:  for m holds n >= m;
  set n' = n + 2;
  n' > n by XREAL_1:31;
  then not for m holds n >= m;
  hence contradiction by A1;
end;
```

Overigens kan Mizar, als we niet het rijmpje letterlijk hoeven te volgen, deze stelling ook wel sneller bewijzen:

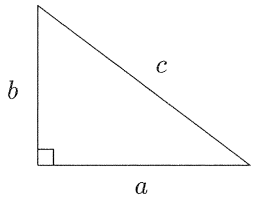
```
theorem
  not ex n st for m holds n >= m
proof
  let n;
  n + 2 > n by XREAL_1:31;
  hence thesis;
end;
```

## Een formule voor Pythagoreïsche drietallen

Een *Pythagoreïsche drietal* is een drietal positief gehele getallen $a$, $b$ en $c$ met

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

Het gaat hier dus met de stelling van Pythagoras om rechthoekige driehoeken




waarvan de lengtes van de zijden alledrie een geheel getal zijn. Nu is er een aardige formule – die al in Euclides' *De Elementen* voorkomt – om dit soort Pythagoreïsche drietallen te genereren:

$$\begin{aligned} a &= m^2 - n^2 \\ b &= 2mn \\ c &= m^2 + n^2 \end{aligned}$$

We krijgen met deze formule bijvoorbeeld de volgende voorbeelden:

$$\begin{array}{llcrcrcr} m = 2 & n = 1 & \longrightarrow & 3^2 & + & 4^2 & = & 5^2 \\ m = 3 & n = 2 & \longrightarrow & 5^2 & + & 12^2 & = & 13^2 \\ m = 4 & n = 1 & \longrightarrow & 15^2 & + & 8^2 & = & 17^2 \\ m = 4 & n = 3 & \longrightarrow & 7^2 & + & 24^2 & = & 25^2 \end{array}$$

Je kunt je nu de vraag stellen of je op deze manier *alle* Pythagoreïsche drietallen krijgt, en het antwoord is: bijna. Je krijgt ze niet allemaal – zo krijg je bijvoorbeeld niet $9^2 + 12^2 = 15^2$, want 15 is niet de som van twee kwadraten – maar je krijgt wel alle *vereenvoudigde* Pythagoreïsche drietallen, waarbij het drietal niet een veelvoud is van een ander Pythagoreïsch drietal.

Het bewijs van dit feit is niet heel ingewikkeld, en we geven het hier in Mizar syntax:

```
let a,b,c; assume a^2 + b^2 = c^2;
assume a,b are_relative_prime;
then a is odd or b is odd; assume a is odd;

ex m,n st a = m^2 - n^2 & b = 2*m*n & c = m^2 + n^2
proof
  b is even; c is odd;
X: (c + a)/2,(c - a)/2 are_relative_prime;
  ((c + a)/2)*((c - a)/2) = (c^2 - a^2)/4 .= (b/2)^2;
  then ((c + a)/2)*((c - a)/2) is square;
  then (c + a)/2 is square & (c - a)/2 is square by X;
  consider m,n such that m^2 = (c + a)/2 & n^2 = (c - a)/2;
  take m,n;
  thus a = (c + a)/2 - (c - a)/2 .= m^2 - n^2;
  b^2 = (c + a)*(c - a) .= 4*m^2*n^2 .= (2*m*n)^2;
  hence b = 2*m*n;
  thus c = (c + a)/2 + (c - a)/2 .= m^2 + n^2;
end;
```

De clou van dit bewijs is dat geldt dat

$$\left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right) = \left(\frac{b}{2}\right)^2$$

een kwadraat is, terwijl de factoren $(c+a)/2$ en $(c-a)/2$ geen delers gemeenschappelijk hebben (dit zijn regels 2 en 4 in de Mizar-versie.) Daaruit volgt dat beide factoren ook een kwadraat moeten zijn (regel 5), en daarmee is het bewijs al bijna klaar.

Helaas is, net als bij het rijmpje van het grootste getal, bovenstaande Mizar tekst te kort door de bocht om door Mizar geaccepteerd te worden. Bij bijna iedere regel klaagt het systeem dat het niet begrijpt waarom dit volgt. Om het af te maken is er nog veel werk nodig: er moeten labels, verwijzingen naar lemmas, en extra stapjes worden toegevoegd. Het eindresultaat is daardoor helaas veel minder leesbaar dan bovenstaande versie. Om hier een indruk van te geven, de regels in bovenstaande tekst:

```
X: (c + a)/2,(c - a)/2 are_relative_prime;
  ((c + a)/2)*((c - a)/2) = (c^2 - a^2)/4 .= (b/2)^2;
  then ((c + a)/2)*((c - a)/2) is square;
  then (c + a)/2 is square & (c - a)/2 is square by X;
  consider m,n such that m^2 = (c + a)/2 & n^2 = (c - a)/2;
```

worden in de uiteindelijk Mizar-formalisatie die je krijgt door het verder uit te werken opdat het Mizar systeem het accepteert:

```
X: (c + a)/2,(c - a)/2 are_relative_prime by Lm3;
  ((c + a)/2)*((c - a)/2) = ((c + a)*(c - a))/(2*2) by REAL_1:35
    .= (c^2 - a^2)/4 by SQUARE_1:67
    .= (b^2)/(2*2) by H1,INT_1:3
    .= (b^2)/(2^2) by SQUARE_1:def 3
```

```
    .= (b/2)^2 by SQUARE_1:69;
  then ((c + a)/2)*((c - a)/2) is square by A1,Def1;
  then (c + a)/2 is square & (c - a)/2 is square by X,Lm4;
  then (ex m st m^2 = (c + a)/2) &
    (ex n st n^2 = (c - a)/2) by Def1;
  then consider m,n such that
A9: m^2 = (c + a)/2 & n^2 = (c - a)/2;
```

Hierin verwijzen `A1`, `Lm3`, `Lm4` en `Def1` naar labels elders in de formalisatie. Het lemma `Lm4` luidt bijvoorbeeld:

```
x,y are_relative_prime & x*y is square implies x is square & y is square
```

De volledige uitgewerkte formalisatie van het bewijs is uiteindelijk 97 in plaats van 11 regels lang. (En dat is exclusief de bewijzen van de hulplemma's.)

# 6 De drie revoluties in de wiskunde

In de geschiedenis van de wiskunde zijn drie revoluties geweest:

## Bewijzen

De eerste revolutie was de ontwikkeling van *bewijzen* in de Griekse oudheid. Vóór deze revolutie bestond wiskunde voornamelijk uit *berekeningen.* Deze Griekse ontwikkeling vond zijn hoogtepunt in *De Elementen* van Euclides, een boek waarin – bewijs na bewijs – de meetkunde systematisch werd ontwikkeld.

*Euclides van Alexandrië*

## Rigor

De tweede revolutie was de ontwikkeling van *rigor* aan het eind van de negentiende eeuw. Daarvóór was wiskunde niet volledig precies. Zo rammelt Euclides' ontwikkeling van de meetkunde als je er met moderne ogen naar kijkt,

en ook de ontwikkeling van de infinitesimaalrekening door Isaac Newton en Gottfried Leibniz was niet rigoreus, met referenties naar oneindig kleine grootheden. Eind negentiende eeuw kwam hieraan een eind met de ontwikkeling van $\epsilon/\delta$ definities van limieten door Augustin Louis Cauchy. Deze ontwikkeling culmineerde in de verzamelingenleer van Georg Cantor en de ontwikkeling van de mathematische logica door Gottlob Frege.

De meetkunde van Euclides werd voor het eerst rigoreus gemaakt rond de eeuwwisseling door David Hilbert. Een bijzonder fraaie variant hierop werd later ontwikkeld door Alfred Tarski.

## Formalisatie

De derde revolutie is de ontwikkeling van praktische *formele* wiskunde. Hierbij wordt wiskunde in de computer gerepresenteerd op een manier dat *alle* details in de computer aanwezig zijn. De computer kan hierdoor de correctheid van de wiskunde volledig mechanisch nagaan. Bij rigoreuze wiskunde is het *in principe* mogelijk om bewijzen volledig precies op te schrijven, maar bij formele wiskunde wordt dit ook *in de praktijk* gedaan. Deze derde revolutie is momenteel in volle gang.

## CWI SYLLABI

1 Vakantiecursus 1984: *Hewet - plus wiskunde.* 1984.
2 E.M. de Jager, H.G.J. Pijls (eds.). *Proceedings Seminar 1981–1982. Mathematical structures in field theories.* 1984.
3 W.C.M. Kallenberg, et al. *Testing statistical hypotheses: worked solutions.* 1984.
4 J.G. Verwer (ed.). *Colloquium topics in applied numerical analysis, volume 1.* 1984.
5 J.G. Verwer (ed.). *Colloquium topics in applied numerical analysis, volume 2.* 1984.
6 P.J.M. Bongaarts, J.N. Buur, E.A. de Kerf, R. Martini, H.G.J. Pijls, J.W. de Roever. *Proceedings Seminar 1982–1983. Mathematical structures in field theories.* 1985.
7 Vacantiecurus 1985: *Variatierekening.* 1985.
8 G.M. Tuynman. *Proceedings Seminar 1983–1985. Mathematical structures in field theories, Vol.1 Geometric quantization.* 1985.
9 J. van Leeuwen, J.K. Lenstra (eds.). *Parallel computers and computations.* 1985.
10 Vakantiecursus 1986: *Matrices.* 1986.
11 P.W.H. Lemmens. *Discrete wiskunde: tellen, grafen, spelen en codes.* 1986.
12 J. van de Lune. *An introduction to Tauberian theory: from Tauber to Wiener.* 1986.
13 G.M. Tuynman, M.J. Bergvelt, A.P.E. ten Kroode. *Proceedings Seminar 1983–1985. Mathematical structures in field theories, Vol.2.* 1987.
14 Vakantiecursus 1987: *De personal computer en de wiskunde op school.* 1987.
15 Vakantiecursus 1983: *Complexe getallen.* 1987.
16 P.J.M. Bongaarts, E.A. de Kerf, P.H.M. Kersten. *Proceedings Seminar 1984–1986. Mathematical structures in field theories, Vol.1.* 1988.
17 F. den Hollander, H. Maassen (eds.). *Mark Kac seminar on probability and physics. Syllabus 1985–1987.* 1988.
18 Vakantiecursus 1988. *Differentierekening.* 1988.
19 R. de Bruin, C.G. van der Laan, J. Luyten, H.F. Vogt. *Publiceren met LATEX.* 1988.
20 R. van der Horst, R.D. Gill (eds.). *STATAL: statistical procedures in Algol 60, part 1.* 1988.
21 R. van der Horst, R.D. Gill (eds.). *STATAL: statistical procedures in Algol 60, part 2.* 1988.
22 R. van der Horst, R.D. Gill (eds.). *STATAL: statistical procedures in Algol 60, part 3.* 1988.
23 J. van Mill, G.Y. Nieuwland (eds.). *Proceedings van het symposium wiskunde en de computer.* 1989.
24 P.W.H. Lemmens (red.). *Bewijzen in de wiskunde.* 1989.
25 Vakantiecursus 1989: *Wiskunde in de Gouden Eeuw.* 1989.
26 G.G.A. Bäuerle et al. *Proceedings Seminar 1986–1987. Mathematical structures in field theories.* 1990.
27 Vakantiecursus 1990: *Getallentheorie en haar toepassingen.* 1990.
28 Vakantiecursus 1991: *Meetkundige structuren.* 1991.
29 A.G. van Asch, F. van der Blij. *Hoeken en hun Maat.* 1992.
30 M.J. Bergvelt, A.P.E. ten Kroode. *Proceedings seminar 1986–1987. Lectures on Kac-Moody algebras.* 1992.
31 Vakantiecursus 1992: *Systeemtheorie.* 1992.
32 F. den Hollander, H. Maassen (eds.). *Mark Kac seminar on probability and physics. Syllabus 1987–1992.* 1992.
33 P.W.H. Lemmens (ed.). *Meetkunde van kunst tot kunde, vroeger en nu.* 1993.
34 J.H. Kruizinga. *Toegepaste wiskunde op een PC.* 1992.
35 Vakantiecursus 1993: *Het reële getal.* 1993.
36 Vakantiecursus 1994: *Computeralgebra.* 1994.
37 G. Alberts. *Wiskunde en praktijk in historisch perspectief. Syllabus.* 1994.
38 G. Alberts, J. Schut (eds.). *Wiskunde en praktijk in historisch perspectief. Reader.* 1994.
39 E.A. de Kerf, H.G.J. Pijls (eds.). *Proceedings Seminar 1989–1990. Mathematical structures in field theory.* 1996.
40 Vakantiecursus 1995: *Kegelsneden en kwadratische vormen.* 1995.
41 Vakantiecursus 1996: *Chaos.* 1996.
42 H.C. Doets. *Wijzer in Wiskunde.* 1996.
43 Vakantiecursus 1997: *Rekenen op het Toeval.* 1997.
44 Vakantiecursus 1998: *Meetkunde, Oud en Nieuw.* 1998.
45 Vakantiecursus 1999: *Onbewezen Vermoedens.* 1999.
46 P.W. Hemker, B.W. van de Fliert (eds.). *Proceedings of the 33rd European Study Group with Industry.* 1999.
47 K.O. Dzhaparidze. *Introduction to Option Pricing in a Securities Market.* 2000.
48 Vakantiecursus 2000: *Is wiskunde nog wel mensenwerk?* 2000.
49 Vakantiecursus 2001: *Experimentele wiskunde.* 2001.
50 Vakantiecursus 2002: *Wiskunde en gezondheid.* 2002.
51 G.M. Hek (ed.). *Proceedings of the 42nd European Study Group with Industry.* 2002.
52 Vakantiecursus 2003: *Wiskunde in het dagelijks leven.* 2003.
53 Vakantiecursus 2004: *Structuur in schoonheid.* 2004.
54 Vakantiecursus 2005: *De schijf van vijf – meetkunde, algebra, analyse, discrete wiskunde, stochastiek.* 2005.
55 J. Hulshof (ed.). *Proceedings of the 52nd European Study Group with Industry.* 2006.
56 Vakantiecursus 2006: *Actuele wiskunde.* 2006.
57 Vakantiecursus 2007: *Wiskunde in beweging.* 2007.
58 Vakantiecursus 2008: *Wiskunde en profil – het gezicht van de wiskunde.* 2008.

## MC SYLLABI

1.1 F. Göbel, J. van de Lune. Leergang besliskunde, deel I: wiskundige basiskennis. 1965.
1.2 J. Hemelrijk, J. Kriens. Leergang besliskunde, deel 2: kansberekening. 1965.
1.3 J. Hemelrijk, J. Kriens. Leergang besliskunde, deel 3: statistiek. 1966.
1.4 G. de Leve, W. Molenaar. Leergang besliskunde, deel 4: Markovketens en wachttijden. 1966
1.5 J. Kriens, G. de Leve. Leergang besliskunde, deel 5: inleiding tot de mathematische besliskunde. 1966.
1.6a B. Dorhout, J. Kriens. Leergang besliskunde, deel 6a: wiskundige programmering. 1967.
1.6b B. Dorhout, J. Kriens, J.Th. van Lieshout. Leergang besliskunde deel 6b: wiskundige programmering. 1967
1.7a G. de Leve. Leergang besliskunde, deel 7a: dynamische programmering 1. 1969
1.7b G. de Leve, H.C. Tijms. Leergang besliskunde, deel 7b: dynamische programmering 2. 1970.
1.7c G. de Leve, H.C. Tijms. Leergang besliskunde deel 7e: dynamische programmering 3. 1971.
1.8 J. Kriens, F. Göbel, W. Molenaar. Leergang besliskunde, deel 8: minimaxmethode, netwerkplanning, simulatie. 1968.
2.1 G.J.R. Förch, P.J. van der Houwen, RP. van de Riet. Colloquium stabiliteit van differentieschema's deel 1. 1967.
2.2 L. Dekker, T.J. Dekker, P.J. van der Houwen, M.N. Spijker. Colloquium stabiliteit van differentieschema's deel 2. 1968.
3.1 H.A. Lauwerier. Randwaardeproblemen, deel 1. 1967.
3.2 H.A. Lauwerier. Randwaardeproblemen, deel 2. 1968.
3.3 H.A. Lauwerier. Randwaardeproblemen, deel 3. 1968.
4 H.A. Lauwerier. Representaties van groepen. 1968.
5 J.H. van Lint, J.J. Seidel, P.C. Baayen. Colloquium discrete wiskunde. 1968.
6 K.K. Koksma. Cursus ALGOL 60. 1969.
7.1 Colloquium moderne rekenmachines, deel 1. 1969.
7.2 Colloquium moderne rekenmachines, deel 2. 1969.
8 H. Bavinck, J. Grasman. Relaxatietrillingen. 1969.
9.1 T.M.T. Coolen, G.J.R. Förch, E.M. de Jager, H.G.J. Pijls. Colloquium elliptische differentiaalvergelijkingen, deel 1. 1970.
9.2 W.P. van den Brink, T.M.T. Coolen, B. Dijkhuis, P.P.N. de Groen, P.J. van der Houwen, EM. de Jager, N.M. Temme, R.J. de Vogelaere. Colloquium elliptische differentiaalvergelijkingen, deel 2. 1970.
10 I. J. Fabius, W.R. van Zwet. Grondbegrippen van de waarschijnlijkheidsrekening. 1970.
11 H. Bart, M.A. Kaashoek, H.G.J. Pijls, W.J. de Schipper, J. de Vries. Colloquium halfalgebra's en positieve operatoren. 1971.
12 T.J. Dekker. Numerieke algebra. 1971.
13 F.E.J. Kruseman Aretz. Programmeren voor rekenautomaten; de MC ALGOL 60 vertaler voor de EL X8. 1971.
14 H. Bavinck, W. Gautschi, G.M. Willems. Colloquium approximatietheorie. 1971.
15.1 T.J. Dekker, P. W. Hemker, P.J. van der Houwen. Colloquium stijve differentiaalvergelijkingen, deel 1. 1972.
15.2 P.A. Beentjes, K. Dekker, H.C. Hemker, S.P.N. van Kampen, G.M. Willems. Colloquium stijve differentiaalvergelijkingen, deel 2. 1973.
15.3 P.A. Beentjes, K. Dekker, P.W. Hemker, M. van Veldhuizen. Colloquium stijve differentiaalvergelijkingen, deel 3. 1975.
16.1 L. Geurts. Cursus programmeren, deel 1: de elementen van het programmeren. 1973.
16.2 L. Geurts. Cursus programmeren, deel 2: de programmeertaal ALGOL 60. 1973.
17.1 P.S. Stobbe. Lineaire algebra, deel 1. 1973.
17.2 P.S. Stobbe. Lineaire algebra, deel 2. 1973.
17.3 N.M. Temme. Lineaire algebra, deel 3. 1976.
18. F. van der Blij, H. Freudenthal, J.J. de Iongh, J.J. Seidel, A. van Wijngaarden. Een kwart eeuw wiskunde 1946-1971, syllabus van de vakantiecursus 1971. 1973.
19 A. Hordijk, R. Potharst, J.Th. Runnenburg. Optimaal stoppen van Markovketens. 1973.
20 T.M.T. Coolen, P.W. Hemker, P.J. van der Houwen, E Slagt. ALGOL 60 procedures voor begin- en randwaardeproblemen. 1976.
21 J.W. de Bakker (red.). Colloquium programma-correctheid. 1975.
22 R. Helmers, J. Oosterhoff, F.H. Ruymgaart, M.C.A. van Zuylen. Asymptotische methoden in de toe-tsingstheorie; toepassingen van naburigheid. 1976.
23.1 J.W. de Roever (red.). Colloquium onderwerpen uit de biomathematica, deel I. 1976.
23.2 J.W. de Roever (red.). Colloquium onderwerpen uit de biomathematica. deel 2. 1977.
24.1 P.J. van der Houwen. Numerieke integratie van differentiaalvergelijkingen . deel 1: eenstapsmethaden. 1974.
25 Colloquium structuur van programmeertalen. 1976.
26.1 N.M. Temme (ed.). Nonlinear analysis, volume 1. 1976.
26.2 N.M. Temme (ed.). Nonlinear analysis, volume 2. 1976.
27. M. Bakker, P.W. Hemker, P.J. van der Houwen, S.J. Polak, M, van Veldhuizen. Colloquium discretiseringsmethoden. 1976.
28 O. Diekmann, N.M. Temme (eds.). Nonlinear diffusion problems. 1976.
29.1 J.C.P. Bus (red.). Colloquium numerieke programmatuur, deel 1A, deel 1 B. 1976.
29.2 H.J.J. te Riele (red.). Colloquium numerieke programmatuur, deel 2. 1977.
30 J. Heering, P. Klint (red.). Colloquium programmeeromgevingen. 1983.
31 J.H. van Lint (red.). Inleiding in de coderingstheorie. 1976.
32 L. Geurts (red.). Colloquium bedrijfsystemen. 1976.
33 P.J. van der Houwen. Berekening van waerstanden in zeeën en rivieren. 1977.
34 J. Hemelrijk. Oriënterende cursus mathematische statistiek. 1977.
35 P.J.W. ten Hagen (red.). Colloquium, computer graphics. 1978.
36 J.M. Aarts, J. de Vries. Colloquium topologische dynamische systemen. 1977.
37 J.C. van Vliet (red.). Colloquium capita datastructuren. 1978.
38.1 T.H. Koornwinder (ed.). Representations of locally compact groups with applications, part I. 1979.
38.2 T.H. Koornwinder (ed.). Representations of locally compact groups with applications, part II. 1979.
39 O.J. Vrieze, G.L. Wanrooy. Colloquium stochastische spelen. 1978.
40 J. van Tiel. Convexe analyse. 1979.
41 H.J.J. te Riele (ed.) Colloquium numerical treatment of integral equations. 1979.
42 J.C. van Vliet (red.). Colloquium capita implementatie van programmeertalen. 1980.
43 A.M. Cohen, H.A. Wilbrink. Eindige groepen (een inleidende cursus). 1980.
44 J.G. Verwer (ed.) . Colloquium numerical solution of partial differential equations. 1980.
45 P. Klint (red.). Colloquium; hogere programmeertalen en computerarchitectuur. 1980.
46.1 P.M.G. Apers (red.). Colloquium databankorganisatie, deel I. 1981.
46.2 P.G.M. Apers (red.). Colloquium databankorganisatie, deel 2. 1981.
47.1 P. W. Hemker (ed.). NUMAL, numerical procedures in ALGOL 60: general information and indices. 1981.
47.2 P.W. Hemker (ed.). NUMAL, numerical procedures procedures in ALGOL 60, vol. I: elementary procedures; vol. 2: algebraic evaluatons. 1981.
47.3 P.W. Hemker (ed.). NUMAL, numerical procedures in ALGOL 60, vol. 3A: linear algebra part I. 1981.
47.4 P.W. Hemker (ed.). NUMAL, numerical procedures in ALGOL 60, vol 3B: linear algebra, part II. 1981.
47.5 P.W. Hemker (ed.). NUMAL, procedures in ALGOL 60, vol. 4: analytical evaluations; vol. 5A: analytical problems. part I. 1981
47.6 P.W. Hemker (ed.). NUMAL, procedures in ALGOL 60, vol 5B: analytical problems, part II. 1981
47.7 P.W. Hemker (ed.). NUMAL, procedures in ALGOL 60, vol. 6: special functions and constants; vol. 7: interpolation and approximation. 1981
48.1 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). Colloquium complexiteit en algoritmen, deel 1. 1982.
48.2 P.M.B. Vitányi, J. van Leeuwen, P. van Emde Boas (red.). Colloquium complexiteit en algoritmen, deel II. 1982.
49 T.H. Koomwinder (ed.) The structure of real semisimple Lie groups. 1982
50 H. Nijmeijer. Inleiding systeemtheorie. 1982.
51 P.J. Hoogendoorn (red.). Cursus cryptografie. 1983.