

Inhoud | Contents

Artikelen | Features

- Onderzoek | Research**
- 236 Grootschalig rekenen in de getaltheorie
Herman te Riele
- Vakantiecursus | Summer School**
- 244 Navier–Stokes
Barry Koren
- De oplossing | The Solution**
- 251 Priemparen
Jaap Korevaar
- Onderwijs | Education**
- 253 Veranderingen in het eindexamenprogramma?
Joke Zwarteveen, Nellie Verhoef
- Onderzoek | Research**
- 259 KAM-theorie en de stabiliteit van het zonnestelsel
Thomas de Jong
- Overzichtsartikel | Overview**
- 263 Chaos, uitgedoofde hype of gevestigde wetenschap?
Ferdinand Verhulst
- Vakantiecursus | Summer School**
- 267 Het vermoeden van Birch en Swinnerton-Dyer
Jaap Top
- Boekbespreking | Book Review**
- 275 Het vinden van ε -dekpunten
Marco Swaen
- Maatschappij | Society**
- 279 SWI 2012: Spotting damaged strips
Ionica Smeets
- Maatschappij | Society**
- 281 SWI 2012: Keep the messages flowing
Ionica Smeets
- Maatschappij | Society**
- 283 SWI 2012: Check the lights
Ionica Smeets
- Maatschappij | Society**
- 285 SWI 2012: Calculating the response of a ship
Ionica Smeets

Rubrieken | Departments

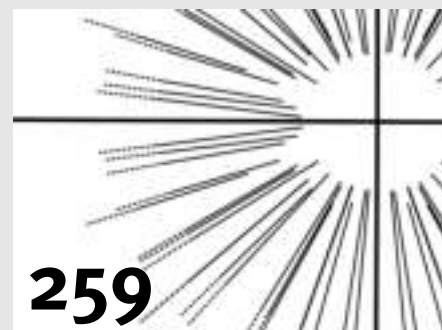
- 226 Colofon
- 227 Redactioneel
Jan van Neerven
- 228 Servicepagina
- 229 Agenda
Patrick Hafkenscheid
- 231 Nieuws
Patrick Hafkenscheid
- 257 Het keerpunt van Jan Beuving
Ionica Smeets
- 273 In de verdediging
Geertje Hek
- 287 Boekbesprekingen
- 293 Problemen

Uitgelicht

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31),
(41, 43), ...

251

De nieuwe rubriek 'De oplossing' start met een column van Jaap Korevaar over het door Yitang Zhang onlangs gevonden resultaat voor priemparen.



Thomas de Jong gaat in op de vraag of er een wiskundige theorie bestaat die de stabiliteit van ons zonnestelsel kan garanderen.

Colofon

Het Nieuw Archief voor Wiskunde is een uitgave van het Koninklijk Wiskundig Genootschap en verschijnt vier maal per jaar. Het tijdschrift richt zich op een ieder die zich beroepsmatig met wiskunde bezighoudt, als academisch of industrieel onderzoeker, student, leraar, journalist of beleidsmaker. Het stelt zich ten doel te berichten over ontwikkelingen in de wiskunde in het algemeen en in de Nederlandse wiskunde in het bijzonder.

ISSN 0028-9825

Adres

Nieuw Archief voor Wiskunde
Centrum Wiskunde & Informatica
Postbus 94079, 1090 GB Amsterdam
tel. 020-5924288
redactie@nieuwarchief.nl
www.nieuwarchief.nl

Hoofredactie

Barry Koren (b.koren@tue.nl)
Jan van Neerven (j.m.a.m.vanneerven@tudelft.nl)

Eindredactie/Bladmanager

Fred Drissen (fred@nieuwarchief.nl)

Redactie

Patrick Hafkenscheid (p.hafkenscheid@vu.nl)
Nellie Verhoef (n.c.verhoef@utwente.nl)
Steven Wepster (s.a.wepster@uu.nl)

Bureau redactie

Gianni van den Braak
Lætitia Diemer

Medewerkers

Johan Bosman (IEM Essen), Hans Cuyper (TU/e),
Gabriele Dalla Torre (UL), Christophe Debry (KU
Leuven), Geertje Hek (UvA), Jinbi Jin (UL), Teun
Koetsier (VU), Derk Pik (JSG Maimonides), Sjoerd
Rienstra (TU/e), Hans Sterk (TU/e), Marco Streng
(VU), Jan Ten Thije Boonkamp (TU/e), Wouter
Zomervrucht (UL)

Illustraties

Ryu Tajiri, Amsterdam

Advertenties

advertenties@nieuwarchief.nl

Abonnementen/Subscriptions

Abonnementenservice NAW
Postbus 2238, 5600 CE Eindhoven
admin@wiskgenoot.nl, tel. 088-2265256

Abonnementsperiode/Subscription period

Een abonnement gaat in op de dag dat uw aanmelding ontvangen wordt. De opzegtermijn is twee maanden vóór het verstrijken van de abonnementsperiode.

The subscription starts on the day that your application is received. The term of notice is two months before the end of the current subscription period.

Exchange subscriptions

Koninklijk Wiskundig Genootschap Library
Centrum voor Wiskunde en Informatica
Postbus 94079, NL-1090 GB Amsterdam
KWG-exchange@cw.nl, fax +31 20 5924026

Vormgeving

Kitty Molenaar (ontwerp)
Susanne Laws (omslag, begeleiding binnenwerk)
Programmatuur (CONTEX)
Hans Hagen, PRAGMA-ADE, Hasselt (Overijssel)
Druk
Drukkerij Ten Brink, Meppel

Koninklijk Wiskundig Genootschap

Het Koninklijk Wiskundig Genootschap (KWG) is een landelijke vereniging van beoefenaren van de wiskunde. In 1778 opgericht onder de zinspreuk: 'Een onvermoeide arbeid komt alles te boven' is het 's werelds oudste nationale wiskundegenootschap. Leden ontvangen het Nieuw Archief voor Wiskunde als onderdeel van hun lidmaatschap.

De contributie voor gewone leden bedraagt €80 per jaar. Voor gepensioneerden en werklozen €40. Voor studenten aio's en oio's van een Nederlandse universiteit of hbo-opleiding €30. Studenten en pas afgestudeerden kunnen een jaar lang gratis lid worden. Voor leden van de wiskundige vakverenigingen VVS, NVvW en NVORWO geldt het gereduceerd tarief van €60. Leden die het Nieuw Archief voor Wiskunde niet willen ontvangen, betalen slechts €40 contributie. Losse nummers zijn te bestellen voor €20.

Members of SIAM, the *Société Mathématique de France*, the *Gesellschaft für Angewandte Mathematik und Mechanik*, the *Deutsche Mathematiker-Vereinigung*, and of the *American, Australian, Belgian, Indian, London, Spanish, and South-African Mathematical Societies* living outside of the Netherlands pay €60 instead of the full membership fee of €80 a year. Conversely, these foreign societies, as well as the VVS and the NVORWO, have reduced membership fees for KWG-members. A postage charge of €10 is added for members living abroad but in Europe, and a charge of €12,50 for members living outside of Europe. Instituten in Nederland en buitenland kunnen zich abonneren op het Nieuw Archief voor Wiskunde voor €100 (Nederland), €110 (Europa) of €112,50 (buiten Europa).

Website: www.wiskgenoot.nl

Ledenadministratie

Abonnementenservice NAW
Postbus 2238, 5600 CE Eindhoven
admin@wiskgenoot.nl, tel. 088-2265256
Bestuur (wiskgenoot@wiskgenoot.nl)

André Ran (VU, voorzitter), Joke Blom (CWI, secretaris), Onno van Gaans (UL, penningmeester), Geurt Jongbloed (TUD, ondervoorzitter), Jenneke Krüger (SLO), Herman te Riele (CWI), Arjen Sevenster, Gert Vegter (RUG), Mark Veraar (TUD)

Informatie voor auteurs

Kopij

Het Nieuw Archief voor Wiskunde is een geredigeerd tijdschrift. Kopij dient elektronisch te worden aangeboden aan de hoofdredactie. Uitgebreide informatie en auteursinstructies kunt u vinden op www.nieuwarchief.nl.

Reprints

Auteurs ontvangen een elektronische reprint in pdf-formaat.

Volgende nummers

nummer	verschijningsdatum	deadline kopij
1	03-03-2014	verstreken
2	02-06-2014	01-02-2014
3	01-09-2014	01-05-2014
4	01-12-2014	01-08-2014

Instituutsleden

De publicaties van het Koninklijk Wiskundig Genootschap worden mede mogelijk gemaakt door de bijdragen van de volgende instituten.



Centrum Wiskunde
& Informatica



Rijksuniversiteit Groningen



Universiteit van Amsterdam



Universiteit Leiden



Vrije Universiteit



Universiteit Utrecht



Technische Universiteit
Eindhoven



Eurandom



Technische Universiteit Delft



Universiteit Twente



Radboud Universiteit
Nijmegen

Fishe

Freudenthal Instituut

Op het omslag

Stomingsleer is de wetenschap die zich bezighoudt met de bestudering van de stroming van gassen en vloeistoffen. Voor de berekening van allerlei stromingen gebruiken we de Navier-Stokes-vergelijkingen. Lees het artikel van Barry Koren op pagina 244. (Foto: deviantART/Sbojnik.)

Gaten opvullen

In april van dit jaar verraste de vrijwel onbekende Yitang Zhang de wiskundige gemeenschap met een bewijs van de ‘bounded prime gap conjecture’: er bestaat een eindig getal N (het bewijs geeft als bovengrens 70.000.000) met de eigenschap dat er oneindig veel priemgetalparen zijn waarvan de onderlinge afstand ten hoogste N bedraagt. Het bestaan van zo’n getal N werd al lang vermoed (het vermoeden dat er voor ieder even getal N oneindig veel priemparen met afstand N bestaan is een generalisatie van het priemparenvermoeden dat al rond 1850 werd geformuleerd), maar tot nu toe was niemand er in geslaagd dit ook werkelijk te bewijzen. Meer hierover vindt u in een lezenswaardige bijdrage van Jaap Korevaar verderop in dit nummer, die de aftrap vormt van een nieuwe rubriek over recente wiskundige doorbraken met raakvlakken aan de Nederlandse wiskunde-beoefening.

Zhangs verhaal heeft zeker iets romantisch. Na zijn promotie in 1991 had hij grote moeite met het vinden van een academische positie en hield hij het hoofd boven water met verschillende banen (op internet lezen we dat hij accountant was en in een broodjeszaak werkte). In 1999 kreeg hij uiteindelijk een positie aangeboden aan de Universiteit van New Hampshire. Hier broedde hij jarenlang in stilte op het bewijs van zijn stelling. In de tussentijd publiceerde hij zo goed als niets: op MatSciNet vinden we slechts twee artikelen van zijn hand, het meest recente uit 2001. Artikelen bovendien met niet meer dan een handjevol citaties. Zijn verhaal doet onwillekeurig denken aan dat van Andrew Wiles, die vele jaren in het diepste geheim werkte aan zijn bewijs van de laatste stelling van Fermat, al gaat de vergelijking op een belangrijk punt mank: Wiles was op dat moment al een gevierd wiskundige.

In het huidige onderzoeksbestel hebben briljante eenlingen als Zhang het bepaald niet gemakkelijk. Zonder uitgebreide publicatielijst en hoge citatiescores ben je vrijwel kansloos bij het binnenhalen van beurzen en subsidies, en dat laatste wordt steeds bepalender bij het verwerven van een vaste aanstelling. Een gezonde mate van competitie is natuurlijk prima. Jonge onderzoekers worden zo gestimuleerd om aan courante onderwerpen te werken. Het aantal beurzen dat jaarlijks kan worden gegeven is echter gering, terwijl de aanvraagdruk enorm is toegenomen. Daardoor blijven veel excellente onderzoekers buiten de prijzen. Jaarlijks besteedt de Nederlandse wiskundige gemeenschap naar schatting enkele manjaren onderzoekstijd aan het schrijven (en beoordelen) van onderzoeksvoorstellen die het

veelal niet halen. In de Vernieuwingsimpuls zouden de beurzen voor wiskundigen, die geen dure laboratoria in de lucht houden, best iets kleiner kunnen. Op deze wijze zouden meer wetenschappers van de onderzoeksgelden kunnen profiteren.

Intussen verheugen de wiskundeopleidingen zich over een steeds verder toenemende populariteit. Met een instroom van ruim 500 studenten zet de opgaande lijn zich ook dit jaar weer voort. Dat is een prima zaak, voor de Nederlandse economie waar een grote vraag naar wiskundigen bestaat, en ook voor de opleidingen zelf, die het dal van het voorgaande decennium duidelijk achter zich laten. Het succes van dubbele bacheloropleidingen laat zien dat studenten uitdagingen zoeken. Wiskunde doet het goed bij scholieren, zo goed zelfs dat de KRO er dit seizoen met Ionica Smeets een wekelijks TV-programma aan wijdt.

De aanwas van studenten heeft ook een keerzijde. De werkdruk onder wiskundigen neemt toe doordat de omvang van de staf geen gelijke tred houdt. Dit probleem zal duidelijk zichtbaar worden als al deze nieuwe studenten toe zijn aan hun bachelorscriptie. Het wordt welhaast ondoenlijk die op individuele basis te begeleiden. Het is daarom verheugend dat met de recentelijk toegekende cluster gelden nu twaalf nieuwe vaste aanstellingsplaatsen worden gecreëerd. Deze ronde, uniek en competitief qua opzet met lokale voorselecties en eindrondes in de clusters, betekent een belangrijke kwaliteitsimpuls voor de Nederlandse wiskunde.

Op bestuurlijk vlak zijn twee initiatieven gaande die de aandacht verdienen. Er wordt hard gewerkt aan een visiedocument voor de Nederlandse wiskunde, waarin, uitgaande van belangrijke trends in maatschappij en wetenschap en de grote uitdagingen in de moderne wiskunde, wordt geanalyseerd waar en hoe de Nederlandse wiskunde een prominente rol kan spelen. Tegelijkertijd verricht Deloitte in opdracht van PWN een onderzoek naar de economische waarde van wiskunde voor de Nederlandse economie. Een soortgelijk onderzoek is eerder in Groot-Brittannië verricht en bracht aan het licht dat wiskundig onderzoek een economische factor van veel grotere betekenis is dan menigeen denkt. We wachten de uitkomsten van dit onderzoek met belangstelling af. In een volgend nummer van het NAW hopen we over beide initiatieven uitgebreider te berichten.

Jan van Neerven, hoofdredacteur

Delft Institute of Applied Mathematics, TU Delft

Koninklijk Wiskundig Genootschap

❑ **Secretariaat**

Joke Blom, CWI
Postbus 94079, 1090 GB Amsterdam
wiskgenoot@wiskgenoot.nl
www.wiskgenoot.nl

❑ **Wintersymposium 2014**

Het wintersymposium 2014 heeft als thema 'Mathematics of Planet Earth'. Onder deze noemer zijn in 2013 wereldwijd meer dan honderd instellingen en organisaties voor onderzoek en onderwijs actief. Voor Nederland was de opening van MPE tijdens de Nationale Wiskunde Dagen 2013; het *Nieuw Archief voor Wiskunde* van september 2013 is helemaal gewijd aan MPE. Het wintersymposium op 11 januari 2014 vormt een afsluiting voor docenten. In dit symposium gaat de aandacht, na een inleiding op modellen, vooral uit naar uitdagingen die met water te maken hebben. De sprekers zijn Ferdinand Verhulst (Universiteit Utrecht), Leo Maas (NIOZ, Universiteit Utrecht), Geert Lenderink (KNMI) en Carel Eijgenraam (CPB). www.wiskgenoot.nl/watbiedt

❑ **NMC 2014**

Het 50ste Nederlands Mathematisch Congres wordt georganiseerd in Delft op woensdag en donderdag 16–17 april 2014. Nadere informatie volgt. www.wiskgenoot.nl/watbiedt

Platform Wiskunde Nederland

❑ **Bureau PWN**

Science Park 123, L013, 1098 XG Amsterdam
bureau@platformwiskunde.nl
pr@platformwiskunde.nl (publiciteit)
Tel: 020-5924006/06-51892525
www.platformwiskunde.nl

❑ **Publieksevenement in Utrecht**

Op zaterdag 21 december organiseert PWN in het Educatorium te Utrecht een publieksevenement omtrent het thema 'Mathematics of Planet Earth', met keynote spreker Ken Golden (wiskundige en zeeijs-expert). Andere sprekers zijn Arjen Doelman, Ute Ebert, Carel Eijgenraam, Kees Roos en Antonios Zagari. Meer informatie is op de PWN-website te vinden. Graag dit nieuws verspreiden! www.platformwiskunde.nl

❑ **PWN Nieuwsbrief**

PWN publiceert eens in de drie maanden een PWN Nieuwsbrief, die op de website te vinden is. Actuele PWN-informatie wordt verder zowel via de website als via Twitter gegeven.

European Mathematical Society

❑ **European Research Council**

Jean-Pierre Bourguignon, de tweede president van de EMS, wordt de volgende president van de European Research Council (ERC). Sinds 2007 financiert de ERC grants voor Europese toponderzoekers, zoals ERC starting grants, consolidator grants, advanced grants en grants via de kaderprogramma's FP7 en Horizon 2020. www.euro-math-soc.eu/node/4178

❑ **EMS Newsletter**

Van de drie-maandelijkse EMS Newsletter is de elektronische versie van de meest recente uitgave beschikbaar op de EMS website: www.ems-ph.org/publications.php.

International Mathematical Union

❑ **IMU Newsletter**

De twee-maandelijkse IMU Newsletter is beschikbaar via www.mathunion.org/imu-net.

Recente publicaties van het KWG

❑ **Indagationes Mathematicae** (www.elsevier.com/locate/indag)

Special issue in memory of Nicolaas Govert de Bruijn (1918–2012); J.W. Klop, R. Tijdeman and J.J.O.O. Wiergerinck (eds.), Volume 24, Issue 4, 2013 (dit issue is gratis toegankelijk op www.sciencedirect.com/science/journal/00193577).

❑ **Epsilon Uitgaven** (www.epsilon-uitgaven.nl)

- 77. *Hemelverschijnselen nabij de Horizon*, Henk Broer, €22,00, 2013.
- 76. *Inleiding in de Statistiek*, F. Bijma, M. Jonker en A. van der Vaart, €32,00, 2013.
- 75. *An Invitation to Functional Analysis*, B. de Pagter en A.C.M. van Rooij, €25,00, 2013.
- 74. *L.E.J. Brouwer - van Mystiek tot Wiskunde*, D. van Dalen, €26,00, 2013.
- 73. *Honderd gevangenen en een gloeilamp*, H. van Ditmarsch en B. Kooi, €20,00, 2013.
- ❑ **Zebra-reeks** (Epsilon Uitgaven)
- 38. *SpiroSporen*, Stephan Berendonk en Leon van den Broek, €10,00, 2013.
- 37. *Moiré-kunst met niveaulijnen*, Luc Van den Broeck, €10,00, 2013.
- 36. *Muziek uitgedrukt in getallen*, Aline K. Honingh en Michiel Schuijjer, €10,00, 2013.

Manuscripten voor Epsilon Uitgaven kunt u mailen naar redactie@epsilon-uitgaven.nl.

Agenda

| Upcoming Events

december 2013

17 december 2013

Studiedag voor wiskundeleraren

Studiedag met lezingen en workshops voor wiskundeleraren, met als thema 'Denken en Doen: wiskunde per 2015'.

plaats Bernouilliborg, Groningen

info nhl.nl/9700

21 december 2013

Publieksevenement MPE 2013

Publieksevenement over het wereldwijde thema 'Mathematics of Planet Earth'. Hoofdspreker is Ken Golden (University of Utah) en dagvoorzitters zijn Sofie van den Enk en Ionica Smeets.

plaats Educatorium Utrecht

info www.platformwiskunde.nl

januari 2014

6–10 januari 2014

Workshop Probability and Graphs

Onderdeel van de themamaand kansrekening en grafen. Een workshop over de connecties tussen grafentheorie en kansrekening.

plaats TU Eindhoven

info eurandom.tue.nl

11 januari 2014

KWG Wintersymposium 2014

Jaarlijks symposium van het KWG met dit jaar als thema 'Mathematics of Planet Earth'.

plaats Academiegebouw, Utrecht

info www.wiskgenoot.nl

13 januari 2014

Mini Course: Graphs Limits

Onderdeel van de themamaand kansrekening en grafen. Lezing gegeven door Christian Borgs en Jennifer Chayes.

plaats TU Eindhoven

info eurandom.tue.nl

16–17 januari 2014

Panamacongres

Jaarlijkse conferentie over de ontwikkeling van reken- en wiskundeonderwijs.

plaats De Leeuwenhorst, Noordwijkerhout

info fisme.science.uu.nl/panama

20–22 januari 2014

13th Winter School on Mathematical Finance

Jaarlijkse winterschool over Mathematical Finance. Met lezingen en mini-cursussen.

plaats Congrescentrum De Werelt, Lunteren

info mathfin.nl

20–30 januari 2014

1ste ronde Nederlandse Wiskunde Olympiade

Eerste ronde van jaarlijkse wiskundewedstrijd voor leerlingen van havo en vwo. De circa 800 beste leerlingen worden uitgenodigd voor de tweede ronde in maart.

plaats heel Nederland

info wiskundeolympiade.nl

20–31 januari 2014

Workshop Representing Streams II

Workshop over *streams*; oneindige rijtjes symbolen die voorkomen in combinatoriek, getaltheorie en kansrekening.

plaats Lorentz Center, Leiden

info lorentzcenter.nl

14 januari 2014

39ste Lunteren Conferentie Mathematische Besliskunde

Jaarlijkse conferentie van het Landelijk Netwerk Mathematische Besliskunde.

plaats Congrescentrum De Werelt, Lunteren

info lnmb.nl

27–31 januari 2014

SWI 2014

Studiegroep Wiskunde met de Industrie, jaarlijkse studiegroep waar wiskundigen werken aan problemen uit de industrie.

plaats Faculteit EWI, TU Delft

info www.ewi.tudelft.nl/swi2014

30–31 januari 2014

The Geometry of Special Functions

Tweedaagse conferentie over special functions met als sprekers onder anderen Masaaki Yoshida (Kyushu University, Fukuoka) en Daniel Allcock (University of Texas, Austin).

plaats Radboud Universiteit Nijmegen

info www.ru.nl/math/research/geometry-special

Suggesties voor deze agenda zijn welkom.

Redacteur: Patrick Hafkenscheid

agenda@nieuwarchief.nl

februari 2014

31 januari–1 februari 2014

□ Nationale Wiskunde Dagen

20ste Editie van de Nationale Wiskunde Dagen, met lezingen, werkgroepen en een uitgebreide informatiemarkt, bedoeld voor wiskundeleraren.

plaats Noordwijkerhout

info www.fi.uu.nl/nwd

12 februari 2014

□ OnderbouwWiskundeDag

Scholenwedstrijd voor de onderbouw. Leerlingen werken in teams van 3–4 leerlingen aan een grote opdracht. Scholen kunnen het beste werkstuk insturen voor deelname aan de wedstrijd.

plaats eigen school

info www.fi.uu.nl/nl/onderbouw/wiskundedag

maart 2014

10–14 maart 2014

□ Workshop YEP XI: Mass Transport in Analysis and Probability

Workshop voor 'Young European Probabilists'.

plaats TU Eindhoven

info eurandom.tue.nl

12 maart 2014

□ Worlds Maths Day

Wereldwijde reken- en wiskundewedstrijd voor scholieren.

plaats overal ter wereld

info worldmathsday.com

14 maart 2014

□ 2de ronde Nederlandse Wiskunde Olympiade

Tweede ronde van jaarlijkse wiskundewedstrijd voor leerlingen van havo en vwo. De circa 130 beste leerlingen gaan door naar de finale in september.

plaats heel Nederland

info wiskundeolympiade.nl

14–28 maart 2014

□ Spring School and Conference in Representation Theory and Geometry of Reductive Groups

Lenteschool in de representatietheorie mede georganiseerd door Eric Opdam.

plaats Kloster Heiligkreuztal, Duitsland

info tinyurl.com/pa3r6zv

april 2014

2 april 2014

□ Grote Rekendag

12de editie van de Grote Rekendag waarop leuke rekenactiviteiten centraal staan.

plaats scholen over het hele land

info groterekendag.nl

10–16 april 2014

□ European Girls' Mathematical Olympiad

3de editie van de EGMO, een Europese wiskundeolympiade voor meisjes.

plaats Antalya, Turkije

info egmo.org

11 april 2014

□ Leve de Wiskunde!

Jaarlijks wiskundecongres voor wiskundedocenten waarin de actuele ontwikkelingen in het vakgebied langskomen.

plaats UvA, Amsterdam

info betaonderwijs.uva.nl

14–17 april 2014

□ New Frontiers in Random Geometric Graphs: Beyond Euclidean Geometry

Workshop georganiseerd door Ross Kang (UU) en Tobias Müller (UU).

plaats Lorentz Center, Leiden

info lorentzcenter.nl

16–17 april 2014

□ NMC 2014

50ste editie van de jaarlijkse bijeenkomst van wiskundig Nederland. Dit jaar georganiseerd door de Universiteit Leiden en de TU Delft.

plaats EWI-gebouw, TU Delft

info wiskgenoot.nl

24–25 april 2014

□ PhD Days in Analysis and Dynamics

Conferentie voor en door aio's in de analyse met korte voordrachten over hun onderzoek.

plaats Congrescentrum De Werelt, Lunteren

info www.staff.science.uu.nl/~3130487/phddays

24–28 april 2014

□ Workshop on Port-Hamiltonian Systems: Approximations, Theory and Practice

Workshop met als doel onderzoekers uit verschillende Hamiltonian-gerelateerde gebieden bijeen te brengen.

plaats Lorentz Center, Leiden

info lorentzcenter.nl

mei–juli 2014

2–4 mei 2014

□ Benelux Mathematical Olympiad

De jaarlijkse gedeelde wiskundeolympiade van de Benelux-landen. Dit jaar in Brugge.

plaats Brugge, België

info wiskundeolympiade.nl

23–27 juni 2014

□ Geometric Algorithms in the Field

Workshop over meetkundige algoritmes.

plaats Lorentz Center, Leiden

info lorentzcenter.nl

23–27 juni 2014

□ From Topological to Stochastic Techniques in Dynamical Systems

Workshop over topologische en stochastische methoden toepasbaar in dynamische systemen.

plaats Lorentz Center, Leiden

info lorentzcenter.nl

14–18 juli 2014

□ European Summer University on History and Epistemology in Mathematics Education

7de zomerschool over de geschiedenis en filosofie van het wiskundeonderwijs, met diverse lezingen en panels over gevarieerde onderwerpen.

plaats Kopenhagen

info conferences.au.dk/ESU-7

Nieuws

| News

CWI-onderzoeker bewijst beroemde Vermoeden van Rota

Wiskundige Bert Gerards van het Centrum Wiskunde & Informatica (CWI) in Amsterdam en zijn collega's Jim Geelen (University of Waterloo, Canada) en Geoff Whittle (Victoria University of Wellington, Nieuw-Zeeland) hebben het beroemde veertig jaar oude Vermoeden van Rota bewezen. Het team heeft meer dan vijftien jaar gewerkt aan de oplossing van dit wiskundige probleem dat in 1970 door Gian-Carlo Rota werd geformuleerd. Dit jaar kwam het trio tot de conclusie dat ze alle essentiële onderdelen ontwikkeld hebben.

Het Vermoeden van Rota behoort tot de matroïdentheorie, een moderne vorm van meetkunde waarin Gerards en zijn collega's gespecialiseerd zijn. De theorie bestudeert meetkundige structuren die totaal kunnen verschillen van die in onze wereld, en het Vermoeden van Rota is een manier om deze alternatieve structuren met behulp van wiskunde te beschrijven. Het probleem werd door Rota geformuleerd op basis van het werk van de wereldberoemde wiskundigen Bill Tutte en Paul Seymour.

Rond de eeuwwisseling bundelden Gerards, Geelen en Whittle hun krachten om zowel aan het Vermoeden van Rota als aan de uitbreiding van de beroemde graafminorentheorie van Robertson en Seymour naar matroïden te werken. Vorig jaar was die theorie van matroïdenminoren af. Het bewijs van het Vermoeden van Rota berust op de volle omvang van die theorie, aangevuld met substantiële andere resultaten.

Volgens het trio begon het echt zware werk pas toen ze eerder dit jaar begonnen met het opschrijven van de resultaten. Het team verwacht dat dit enkele jaren zal vergen en honderden pagina's aan wetenschappelijke artikelen zal opleveren.

Prof.dr.ir. Bert Gerards is onderzoeker op het CWI sinds 1989. Hij is gespecialiseerd in combinatorische optimalisatie. In 2003 ontving hij de Fulkerson Prijs. Gerards is daarnaast deeltijdhoogleraar bij de Maastricht University School of Business and Economics. CWI



Foto: Observant

Deze rubriek is een kroniek van wiskundige activiteiten in Nederland. Toekomstige activiteiten worden aangekondigd en van voorbijgaande activiteiten wordt verslag gedaan. Wilt u uw aankondiging of verslag in deze rubriek geplaatst zien? Stuur ons dan uw bijdrage van ± 350 woorden, zo mogelijk met illustratie. De redactie behoudt zich het recht voor berichten te weigeren of in te korten.

Redacteur: Patrick Hafkenscheid

nieuws@nieuwarchief.nl

TU Eindhoven start Data Science Center

De Technische Universiteit Eindhoven opent begin december het Data Science Center Eindhoven (DSC/e). Dit onderzoeksinstituut onder

leiding van prof.dr.ir. Wil van der Aalst zal een samenwerking worden tussen verschillende TU/e-faculteiten en bedrijven. Ook is een van de doelen uiteindelijk een aparte bachelor- en masteropleiding aan het moderne vakgebied Data Science te wijden.

Data Science is tegenwoordig erg populair. *Harvard Business Review* noemt het zelfs “The sexiest Job of the 21st century”. Van der Aalst (hoogleraar Process Mining and Business Process Management) verklaart: “De hoeveelheid data groeit nog altijd enorm. Negentig procent van alle wereldwijd beschikbare data werd de voorbije twee jaar geproduceerd. Deels zijn we ons niet zo bewust van al die informatie die wordt vergaard, anderzijds raken mensen er ook heel snel aan gewend.”

Ook in de wetenschap worden de harde feiten steeds belangrijker. Vandaar dat het belangrijk is dat ingenieurs goed leren registreren, analyseren, interpreteren en waarderen. Zo is een van de kernvraagstukken in de Data Science: “Hoe zet je groeiende bergen aan data om in *echte* waarde?”

Verder ziet Van der Aalst de Data Science ook als brug tussen de wiskunde en de informatica. Nog meer dan dat zal het de verbinding vormen tussen op het eerste gezicht vakgebieden die niet zo veel met elkaar te maken hebben, zoals de sociale wetenschappen, industrial design en informatica.

Het DSC/e moet al die vakgebieden bij elkaar brengen, en meer dan dat, moet de expertise van de TU/e in de Data Science zichtbaar maken aan de buitenwereld. Dit zouden de eerste stappen kunnen zijn richting de eerder genoemde nieuwe opleidingen Data Science.

Cursor

Groepsdruk in kaart gebracht

De Britse wiskundige professor Ernesto Estrada van de Universiteit van Strathclyde heeft onderzoek gedaan naar de wiskunde achter directe en indirecte sociale invloed — ook wel groepsdruk genoemd — en hoe deze invloed uiteindelijk belangrijke beslissingen tot stand brengt. Met wiskundige modellen heeft hij data geanalyseerd uit vijftien verschillende netwerken, waaronder een netwerk van Braziliaanse boeren en eentje van Amerikaanse schoolinspecteurs.

Professor Estrada: “Onze moderne maatschappij is er eentje die onderling erg verbonden is. Deze verbindingen werden naarmate de tijd vorderde steeds intensiever, vanaf de prehistorische grotbewoners tot de technologie-gedreven maatschappij van vandaag.”

“Beslissingen nemen over cruciale vraagstukken, zoals de opwarming van de aarde, de kosten van de zorg en verzekeringen en gezonde levenswijzen, zijn nodig om als maatschappij vooruit te gaan.” Dit is waarom professor Estrada het belangrijk vindt dat vele verschillende academische disciplines bekijken hoe groepsdruk beslissingen beïnvloedt.

Professor Estrada's onderzoek toont aan dat beslissingen beginnen wanneer alle directe invloeden hun eerste overeenkomst bereiken. Daarna spelen de indirecte invloeden een rol — de gehele sociale groep komt uiteindelijk tot een consensus. Als voorbeeld geeft Estrada coma-zuipende tieners. Een tiener wordt door zijn vrienden onder druk gezet om te drinken. Dit is de directe invloed waar Estrada het over heeft.

Maar de tiener ziet alle andere tieners hetzelfde doen op zaterdagavond, dit is wat Estrada bedoelt met indirecte invloeden. De tiener wordt indirect onder druk gezet om het algemene gedrag te kopiëren. Een ander voorbeeld dat Estrada geeft is het rookgedrag. In de jaren zeventig was het heel gewoon om te roken omdat iedereen in de om-

geving het deed (directe invloed) maar ook omdat de filmsterren het deden (indirect).

Tegenwoordig is roken veel minder populair, met name door de indirecte invloeden (roken is verboden in openbare gebouwen). Op deze manier is dus indirecte groepsdruk gebruikt om de maatschappij gezonder te maken.

strath.ac.uk

Nobelprijs literatuur dit jaar ook een beetje Nobelprijs wiskunde

Vandaag werd bekend dat de Canadese schrijfster Alice Munro de Nobelprijs voor literatuur heeft gewonnen. In haar verhalenbundel *Too much happiness* (in het Nederlands vertaald als *Te veel geluk*) handelt het titelverhaal over de vrouwelijke Russische wiskundige Sofia (Sonya) Kovaleskaya (1850–1891), die studeerde bij Weierstrass en die op voorspraak van Mittag-Leffler professor in Stockholm werd.

Tom H. Koornwinder



Sofia Kovaleskaya

Wetenschappers maken 3D-prints van schilderijen oude meesters

Van drie beroemde schilderijen (Rembrandts ‘Joodse bruid’, een zelfportret van Rembrandt en ‘Bloemen in Blauwe Vaas’ van Van Gogh) zijn hoge resolutie 3D-prints gemaakt. Hiervoor tekenden het onderzoeksteam van TU Delft-hoogleraren Joris Dik, Pieter Jonker en Jo Geraedts en het printtechnologiebedrijf Océ. Op 23 september presenteerden de makers hun replica's op de conferentie Technart in het Rijksmuseum. Dit is een internationale conferentie van kunstexperts en wetenschappers, gewijd aan de nieuwste natuurwetenschappelijke technieken om kunstwerken te onderzoeken.

Een ‘lookalike-wedstrijd’ met de originelen was niet het doel van de makers van de 3D-prints. Joris Dik benadrukt: “Het is een techniek in ontwikkeling, met het doel de oppervlakte-eigenschappen van het origineel zo dicht mogelijk te benaderen. We combineren nu reliëf en

kleur in 3D, wat al een heel nieuwe dimensie is. Op termijn willen we ook andere relevante eigenschappen kunnen printen, zoals bijvoorbeeld glans en transparantie.”

Schilderijen zijn opgebouwd uit verschillende lagen en materialen, en vaak aangetast door de tand des tijds. Met scans en 3D-prints kunnen onderzoekers het maakproces blootleggen en achterhalen hoe het schilderij eruitzag voordat bijvoorbeeld de kleuren vervaagden. Océ heeft op basis hiervan een hoge kwaliteit reproductie van het schilderij gemaakt. Het resultaat is uniek in de wereld.

Dik: “We kunnen op dit moment 3D-prints maken van de Joodse Bruid zoals die er nu uit ziet, maar op termijn willen we ook replica’s maken van eerdere fasen. Wat kunsthistorici en restauratoren nooit kunnen en mogen doen met het origineel kan en mag wel met de 3D-replica’s: experimenteren.” Stephan Koopman van Océ voegt toe: “Nu wordt zichtbaar welke verborgen figuren of details eerder in het schilderij waren verwerkt. Maar ook het samenstellen van verschillende kunstwerken voor exposities, die normaal nooit worden uitgeleend, is mogelijk en scholieren en studenten kunnen dankzij de 3D-printtechnologie met hun handen voelen welk effect reliëf aan schilderijen geeft.”

tudelft.nl



Afbeelding (rechts): Tim Zaman

Nederland investeert in de computer van de toekomst

Nederland gaat onder leiding van de TU Delft werken aan de bouw van de nieuwe generatie computer: de kwantumcomputer. Via een samenwerking van wetenschap, bedrijfsleven en overheid is het instituut *QuTech* opgericht. Dit alles werd bekend gemaakt tijdens de innovatieconferentie 2013 door minister Kamp van Economische Zaken.

“QuTech is een voorbeeldig resultaat van samenwerking op het gebied van innovatie. De beste onderzoekers werken samen met de meest innovatieve ondernemers en de overheid om een revolutionaire techniek door te ontwikkelen tot nieuwe producten,” aldus Kamp. “Dit kan leiden tot nieuwe maatschappelijk relevante producten en diensten, zoals het voorspellen van de werking van medicijnen. En natuurlijk voor meer inkomsten en banen in Nederland.”

De kwantumcomputer moet te realiseren zijn binnen vijftien jaar. Belangrijkste aspect van de nieuwe computer is dat deze *kwantumbits* vervangen de huidige aan-uitbits in de moderne computers waardoor de rekenkracht exponentieel groeit.

Een van de toepassingen die het instituut voor ogen heeft wanneer het gaat over de kwantumcomputer is het simuleren van de effecten van medicijnen per individu. Ook zou je kunnen denken aan berekeningen en voorspellingen wat betreft materialen en bodemlagen.

In de komende maanden zal door de TU Delft gezocht worden naar samenwerking met andere onderzoeksinstituten zoals TNO en SRON, die beschikken over aanvullende expertise op het gebied. Ook de Nederlandse wetenschapsfinanciers NWO, FOM en STW, die het begin van het onderzoek al steunden, blijven betrokken bij het project.

rijksoverheid.nl

Facebook en Twitter als voorspellers van epidemieën

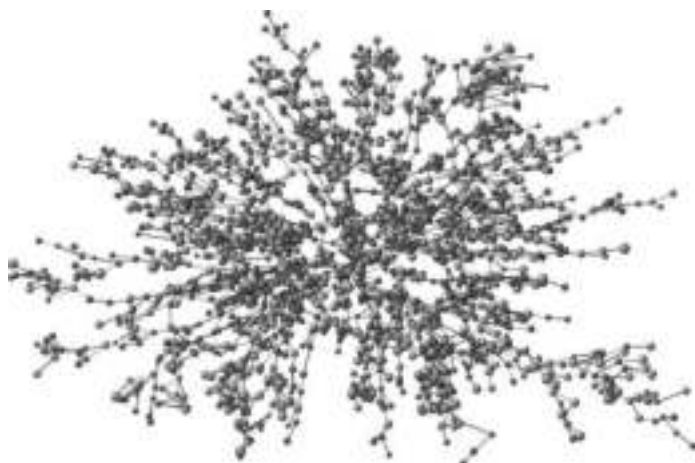
Facebook en Twitter zouden cruciale aspecten kunnen belichten over hoe de effecten van maatregelen tegen epidemieën. Dit kan gedaan worden via wiskundige modellen om te begrijpen hoe we sociaal reageren op biologische besmettingen.

Het is weer het seizoen voor verkoudheid en griep, en dus zullen we manieren moeten vinden om te voorkomen dat de ziektes zich te veel verspreiden. Bijvoorbeeld door vaccinatie en door een hand voor de mond te houden tijdens het hoesten. Deze sociale gebeurtenissen zijn veel moeilijker te voorspellen dan de daadwerkelijke verspreiding van de ziekte. Om dit vraagstuk te beantwoorden worden nu modellen gemaakt.

In oktober verscheen in *Science* een artikel dat behalve de fysieke verspreiding van een besmetting ook de sociale factoren meewoog. Met behulp van data verkregen uit de sociale media zijn voorspellingen gedaan wat betreft de verspreiding van ziektes. Dit werd gedaan door een zogenaamd *biologische besmettingennetwerk* te maken.

De onderzoekers kwamen erachter dat behalve de ziekte ook ideeën, informatie en sentimenten besmettelijk kunnen zijn. “Voorspellend modelleren is niet perfect, maar het kan helpen peilen hoe mensen willen reageren op bepaalde ziektecontrolerende maatregelen”, zegt professor Bauch, die samenwerkt met epidemiologen en populatie gezondheidsonderzoekers. “Allerlei variabelen kunnen een effect hebben op iets dat zo complex is als het verspreiden van ziektes. Dat is waarom het belangrijk is om gevarieerde perspectieven te belichten.”

eurekalert.org



Human Brain Project van start

Het meest ambitieuze neurowetenschappelijke project ter wereld is van start gegaan. De deelnemers aan het project, dat 135 partners telt en mede wordt gefinancierd door de EU, komen in Zwitserland samen voor de officiële start. Het budget dat beschikbaar is voor deze missie is ongeveer 1,2 miljard euro (!).

Doel van het project is het ontwikkelen van methoden die kunnen helpen bij het beter begrijpen van de werking van het brein. Dit zal gebeuren via zes verschillende platformen: neuroinformatica, simulatie van de hersenen, high-performance computation, medische informatica, neuromorphic computing en neurorobotica. Deze platformen moeten er voor zorgen dat de doelen van het project behaald worden.

Tijdens de bijeenkomst op de EPFL (École Polytechnique Fédérale de Lausanne), dat ook als het coördinerende instituut zal optreden, komen neurowetenschappers, dokters, informatici en robotica bijeen om de precieze details te verfijnen.

Het CWI is een van de partners voor dit project. De wetenschappers van het CWI zullen zich vooral bezighouden met de high-performance computing en het analyseren van grote stromen data.

Uiteindelijk is het idee achter het project niet alleen maar om meer te weten te komen over hoe het brein werkt, maar ook om deze technologie toe te passen in applicaties. Zo zou je kunnen denken aan microchips die op eenzelfde soort manier werken als een netwerk van neuronen in de hersenen.

actu.epfl.ch



Voorstelling van neurale verbindingen in de hersenen

Afbeelding: Thomas Schultz

Antieke wiskundedictaten online

De volledige set collegedictaten wiskunde (196 stuks) waar Jan de Graaf zeven jaar geleden een cd-rom van gemaakt heeft, zijn vanaf nu online toegankelijk.

Michiel Wijers heeft veel moeite gestoken in het ontwikkelen van deze openbare website, die het materiaal op de cd-rom *Antieke Wiskundedictaten 1956–1982* ontsluit. De site betreft zowel het ‘basisonderwijs voor alle faculteiten’ zoals dat destijds gebruikelijk was, als het eigen wiskundeonderwijs. Vele van deze dictaten zijn tot ver in de negentiger

jaren gebruikt. Jan de Graaf: “Ter vervaardiging van stevige tentamens kunnen de vele ‘opgavenbundels en uitwerkingen’ ook thans nog van groot nut zijn. De wiskunde heeft immers eeuwigheidswaarde! Lees vooral het, lichtelijk ironisch getinte, voorwoord.”

Op de website staan verschillende dictaten voor vrijwel alle hoofdvakken die gedoceerd worden aan de universiteit, denk aan bijvoorbeeld analyse, mechanica, kansrekening en numerieke wiskunde.

De wiskundedictaten zijn te vinden op de volgende website: www.win.tue.nl/doc/AntiekeWiskundeDictaten. *tue.nl*



Wiskunde 2025

Het Platform Wiskunde Nederland (PWN) heeft een schrijfgroep ingesteld onder leiding van Jan Karel Lenstra, de voormalige directeur van het Centrum Wiskunde & Informatica (CWI). De schrijfgroep gaat een visie voor de wiskunde formuleren voor de middellange termijn. In 2008 verscheen het *Masterplan Toekomst Wiskunde*, dat in 2012 werd aangepast aan de actualiteit in het *Masterplan Wiskunde 2.0*. Het visiedocument dat nu geschreven gaat worden, zal meer uitgaan van de inhoud en zal de grote uitdagingen voor de wiskunde voor de komende periode beschrijven. Bovendien zullen de rol en impact van de wiskunde op andere wetenschappen en de maatschappij worden belicht, evenals het onderwijs in de wiskunde. In de Verenigde Staten is onlangs een dergelijk visiedocument verschenen van de National Research Council, getiteld *The Mathematical Sciences in 2025*. Men is er bij de wiskunde van overtuigd, dat het nu de tijd is voor het formuleren van een dergelijke visie. Het onderzoekslandschap is drastisch veranderd; we staan aan de vooravond van het nieuwe kaderprogramma Horizon 2020 van de EU en het belang van de wiskunde voor het oplossen van de problemen van de complexe moderne maatschappij dringt zich steeds meer op. Bij de natuurkunde en de scheikunde worden ook visiedocumenten geschreven voor die vakgebieden. De schrijfgroep visiedocument wiskunde zal haar werkzaamheden zoveel mogelijk coördineren met de natuurkunde en de scheikunde.

Het visiedocument zal tot stand komen in nauw overleg met de wiskundeachterban, NWO, universiteiten en vertegenwoordigers van maatschappij en bedrijfsleven (topsectoren).

De schrijfgroep bestaat uit Petra de Bont (NWO), Jason Frank (CWI/UvA), Remco van der Hofstad (TU/e), Jan van Neerven (TUD), Frank

Roos (CWI, secretaris), Wil Schilders (PWN), Jasper Stokman (UvA) en Lenny Taelman (UL).

Platform Wiskunde Nederland

Wiskundeonderwijs in Nederland met buurlanden vergeleken

Afgelopen jaar heeft Linda Kaper, student bij de lerarenopleiding in Utrecht een onderzoek gedaan waarin het wiskundeonderwijs in Nederland wordt vergeleken met de buurlanden. De onderzoeksvraag die centraal stond in dit onderzoek was: "Welke verschillen zijn er in het wiskundeonderwijs op het gebied van onderwijstijd, curriculum, examinering, toelating tot de universiteit en opleiding van de docenten tussen Nederland en het buitenland?" Ze heeft zich hierbij beperkt tot het wiskundeonderwijs in de bovenbouw van het vwo. De buurlanden die meegenomen werden in de analyse zijn België (Vlaanderen) en Duitsland.

Om een vergelijkende analyse te maken heeft ze samengewerkt met experts uit de desbetreffende landen. Met name mensen die werkzaam zijn bij verschillende instituten voor lerarenopleidingen.

Een van de grote verschillen in het onderwijs is de opsplitsing van de onderwerpen in andere vakken zoals we dat hier in Nederland kennen als wiskunde A, B, C en D. In de buurlanden kennen ze dit concept niet, en is de keuze voor een ander wiskundevak alleen een keuze voor minder uren over dezelfde onderwerpen.

Een van de hypothesen die Linda Kaper had, was dat er in vergelijking met de buurlanden in Nederland veel minder uren aan wiskunde besteed wordt. Met name de laatste jaren zijn het aantal uren in Nederland flink afgenomen. Ook heeft ze gekeken naar het precieze doel van het onderwijs, en in welk kader het wordt gebracht.

Conclusies van het onderzoek zijn onder andere dat het aantal uren niet bijzonder veel minder is dan in de buurlanden, wat betreft wiskunde A en C. De bèta-variant daarentegen kan alleen concurreren als wiskunde D ook gevolgd wordt. Een ander bijzonder verschil is dat de keuze voor een bepaald wiskunde vak in Nederland de andere vakken ook tot zekere hoogte vast legt, dit is in de buurlanden veel vrijer. *PWN*

Nederland scoort hoog op rekenvaardigheid

In het rapport 'Kernvaardigheden voor werk en leven', een rapport waarin de resultaten van het onderzoek PIAAC (Programme for the International Assessment of Adult Competencies) worden gepresenteerd, blijkt dat Nederland hoog scoort op rekenvaardigheid.

Sterker nog, Nederland staat boven aan het lijstje van rekenvaardigheden in de categorie van 16–24 jaar, direct gevolgd door Finland, Japan en België.

De PIAAC wordt jaarlijks uitgevoerd onder leiding van de OECD (Organisation for Economic Co-operation and Development), om de algemene vaardigheden van personen in de leeftijd van 16–65 jaar in kaart te brengen in de 24 landen die meedoen.

Over de hele groep van 16–65 jaar scoren we ook hoog, daar staan we op de vierde plek. Qua probleemoplossend vermogen scoren we helaas iets minder goed en moeten we het doen met een zesde plek.

piaac.nl

Panorama's plakken

Panoramafoto's geven een mooi overzicht van een groot landschap. Tegenwoordig hebben veel smartphones en camera's een panoramafunctie, helaas werkt deze niet altijd even prettig, je moet op het precie-

ze tempo draaien om ervoor te zorgen dat de camera zijn knip-en-plakwerk kan doen. Dat hoeft nu niet langer!

Wetenschappers Wei Wang en Michael Ng hebben een algoritme bedacht dat op een functionele manier twee foto's aan elkaar kan plakken. Het artikel waarin ze dat beschrijven is deze zomer verschenen in *SIAM Journal on Imaging Sciences*.

Het proces van het plakken bestaat uit twee delen. De eerste stap is om alle afbeeldingen in dezelfde richting te zetten. Dit betekent dus dat de originele foto's niet per se dezelfde richting op hoeven te staan. De tweede stap is om de foto's aan elkaar te plakken.

Voor de eerste stap zoekt het algoritme naar overlappende stukjes foto. Deze worden dan gebruikt om een idee van de hoek of richting van de foto's te krijgen. Als de foto's dezelfde richting op staan kan het plakken beginnen.

Traditioneel zijn er al verschillende manieren van foto's aan elkaar plakken bedacht. De meeste zoeken naar een curve in het overlappende gebied en proberen dan de verschillen van de input minimaal te maken. Het probleem is dat deze curve niet altijd goed gedefinieerd is.

In plaats daarvan gebruiken de wetenschappers een variationele methode om een staat van de laagste energie te vinden, een methode die in de natuur ook veel voorkomt. Ng en Wang zijn nu van plan om verder te gaan dan tweedimensionale foto's en willen proberen hetzelfde idee toe te passen in drie dimensies.

eurekalert.org



Foto: Blanka M. Lukes

Heeft wiskunde de Amerikaanse overheid kunnen voorspellen?

De Amerikaanse 'shutdown' van de overheid heeft het nieuws een tijdje in zijn grip gehad. Ook op wiskundig niveau is er veel over gezegd. Zo zegt Peter Turchin, wiskundig ecooloog aan de Universiteit van Connecticut, dat de 'shutdown' van tevoren was te voorspellen met wiskunde. Turchin is een van de kleine groep onderzoekers die complexe wiskundige modellen toepassen om politieke instabiliteit te onderzoeken. Ook beweert Turchin dat als er niets gedaan wordt het eerder erger wordt dan beter.

Turchin denkt historische cycli gevonden te hebben die twee tot drie eeuwen duren. In zo'n cyclus van politieke instabiliteit en uiteindelijk het afbrokkelen van een maatschappij zit de Amerikaanse overheid op dit moment, volgens Turchin. Hij geeft toe dat deze theorie getest moet worden maar zegt dat dit nu daadwerkelijk mogelijk is.

Een onderdeel van de cycli is dat als de bevolking groeit er steeds meer werkers dan banen komen, en dat daardoor de salarissen omlaag gedreven worden. Alles fulmineert uiteindelijk in het opheffen van de staat waarna een nieuwe cyclus begint.

Het lijkt nogal vergezocht maar veel voorspellingen uit de theorie van Turchin zijn de laatste jaren echt uitgekomen, zoals de cijfers betreffende de gezondheid van de bevolking, de verdeling van de welvaart en de werkgelegenheid.

NewsScientist

Herman te Riele

CWI, Amsterdam

herman@cwi.nl

Onderzoek

Grootschalig rekenen in de getaltheorie

De getaltheorie kent bekende onbewezen beweringen, zoals het vermoeden van Goldbach en de Riemann-hypothese. Er is een tijd geweest dat wiskundigen nogal neerkeken op hen die aan dit soort problemen gingen rekenen. Met de komst van steeds snellere computers die enorm veel saai rekenwerk uit handen kunnen nemen, is echter een nieuw vakgebied ontstaan, dat van de ‘Computationele getaltheorie’. Hierin wordt geprobeerd om algoritmen voor allerlei problemen uit de getaltheorie te vinden en/of te verbeteren en met behulp hiervan onze kennis van deze problemen te vergroten. Tegenwoordig worden hierbij allerlei soorten en maten van computers ingezet. Herman te Riele illustreert deze ontwikkelingen aan de hand van een aantal voorbeelden, inclusief toepassingen in de cryptografie. Dit artikel is een uitgewerkte versie van zijn voordracht tijdens het Wintersymposium van het KWG op 7 januari 2012 in Utrecht.

Aan de hand van de volgende vijf klassieke problemen uit de getaltheorie laten we zien hoe grootschalige computerberekeningen hebben geholpen om onze kennis van deze problemen aanzienlijk te vergroten en ons inzicht erin te verdiepen:

- het zoeken naar volmaakte getallen en generalisaties;
- het ontbinden in priemfactoren van zeer grote getallen (met implicaties voor de cryptografie);
- de Riemann-hypothese;
- het vermoeden van Goldbach met varianten;
- het vermoeden van Mertens.

In alle gevallen is bijzonder veel — vaak brute force — rekenkracht gebruikt, op allerlei soorten computers, inclusief supercompu-

ters. Ook in alle gevallen, behalve voor zover bekend het laatste, is in grote *collectieve* rekenprojecten op tienduizenden thuiscomputers van vrijwilligers aan deze problemen gerekend.

De Riemann-hypothese staat op een lijst van de zeven grootste onderzoeksvragen van de moderne wiskunde [2]. Het waar zijn hiervan heeft belangrijke gevolgen voor onze kennis van de verdeling van de priemgetallen in de verzameling van de natuurlijke getallen. Steeds uitgebreidere numerieke verificaties van de Riemann-hypothese hebben de plausibiliteit van dit vermoeden alleen maar versterkt. De juistheid van het vermoeden van Mertens impliceert het waar zijn van de Riemann-hypothese en dit verklaart de belangstelling voor dit vermoeden, totdat het

onjuist zijn hiervan werd bewezen. Het ontbinden in priemfactoren van grote getallen is voor zover bekend een lastig rekenprobleem. Hierop is de vermeende veiligheid van het veelgebruikte *RSA public-key cryptosysteem* gebaseerd. Aangetoond is dat er voor kwantumcomputers een snel algoritme voor het ontbinden in priemfactoren bestaat dat RSA in de praktijk onbruikbaar zou maken [6]. De huidige kwantumcomputers zijn echter hiervoor nog veel te primitief.

De problemen van het zoeken naar volmaakte getallen en het vermoeden van Goldbach behoren tot de categorie van wiskundi-

Gevolg waar zijn Riemann-hypothese

Zij $\pi(x)$ het aantal priemgetallen $\leq x$ en $\text{li}(x) := \int_2^x dt/\log t$. De beroemde Priemgetalstelling zegt dat $\pi(x)$ van de orde van grootte $x/\log x$ is. Het waar zijn van de Riemann-hypothese impliceert dat het verschil $\pi(x) - \text{li}(x)$ ruwweg van de orde van grootte $\sqrt{x} \log x$ is, veel kleiner dus dan de grootte van $\pi(x)$ zelf. Dit gedrag wordt bevestigd door berekeningen van $(\pi(x) - \text{li}(x))/(\sqrt{x} \log x)$, uitgevoerd voor $x = 10^k$, $k = 1, 2, \dots, 21$ [6, Table 1.1].

ge vragen die eenvoudig zijn te stellen — en die daardoor veel belangstelling trekken en hebben getrokken bij amateurs — maar die, naar blijkt, uiterst lastig zijn te beantwoorden. Toepassingen hiervan zijn niet bekend maar het zijn en blijven wel problemen die tot de verbeelding spreken en een voortdurende uitdaging vormen voor hen die geboeid worden door rekenkundige vragen.

Notatie: met ‘de complexiteit van een algoritme (of formule) is $\mathcal{O}(f(t))$ ’ geven we aan dat voor de hoeveelheid rekenwerk $R(t)$ om dit algoritme uit te voeren (of deze formule te berekenen) geldt dat $\lim_{t \rightarrow \infty} R(t)/f(t)$ begrensd is. Met ‘CPU-tijd’ geven we aan de Central Processing Unit-rekentijd van een computer om een gegeven rekenklus uit te voeren. Hierbij wordt niet de I/O-tijd meegeteld, dat is de tijd nodig om data in en uit te voeren die bij de rekenklus worden gebruikt, respectievelijk worden afgeleverd.

Volmaakte en bevriende getallen

Zij $s(n)$ de som van alle delers van n behalve n zelf, dus $s(n) := \sigma(n) - n$. Een *volmaakt* getal is een positief geheel getal n waarvoor geldt: $n = s(n)$. Bijvoorbeeld:

$$\begin{aligned} 6 &= 2 \cdot 3 = 2 \cdot (2^2 - 1) = 1 + 2 + 3, \\ 28 &= 2^2 \cdot 7 = 2^2 \cdot (2^3 - 1) = 1 + 2 + 4 + 7 + 14, \\ 496 &= 2^4 \cdot 31 = 2^4 \cdot (2^5 - 1) \\ &= 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248. \end{aligned}$$

Er zijn geen *oneven* volmaakte getallen bekend. De *even* volmaakte getallen worden als volgt gekarakteriseerd:

Stelling 1 (Euclides, Euler). *Een even getal n is volmaakt dan en slechts dan als $n = 2^{k-1}M_k$ waarbij $M_k = 2^k - 1$ een (zogenaamde Mersenne-) priemgetal is.*

Momenteel zijn er 48 volmaakte getallen, en dus Mersenne-priemgetallen, bekend. Het tot nu toe grootste, op 25 januari 2013 ontdekt, heeft $k = 57885161$ en is een getal van 17425170 cijfers. De veertien grootste bekende Mersenne-priemgetallen zijn gevonden in het ‘Great Internet Mersenne Prime Search’-project, een wereldwijd zoekproject op vele tienduizenden PC’s [12]. Voor het bewijzen van de primaliteit van M_k is de zeer snelle zogenaamde Lucas–Lehmer-test beschikbaar [6, Section 4.2.1]. De complexiteit van deze test is $\mathcal{O}(k^2 \log k \log \log k)$.

oneven volmaakte getallen zijn zoals gezegd niet bekend maar het is ook niet bekend

of ze bestaan. Pomerance bewees in 1973 dat ieder oneven volmaakt getal tenminste zeven verschillende priemfactoren zou moeten hebben [39]. Nielsen verhoogde dit aantal naar negen in 2007 [28]. In 2001 heeft Brent met uitgebreide berekeningen aangetoond dat een oneven volmaakt getal, als het bestaat, groter is dan 10^{300} [3]. Deze ondergrens is kort geleden door Ochem en Rao verhoogd naar 10^{1500} [29]. Zij toonden daarbij ook aan dat de grootste priemmacht in een oneven volmaakt getal groter is dan 10^{62} en dat het aantal priemfactoren van een oneven volmaakt getal (multipliciteit meetellend) tenminste 101 is.

Volmaakte getallen kunnen worden beschouwd als dekpunten na één iteratie van de functie $s(n)$. Dekpunten na twee iteraties voldoen aan de vergelijkingen

$$m = s(n) \text{ en } n = s(m) = s(s(n)), \quad n \neq m.$$

Zo’n paar getallen (m, n) met $m < n$ heet *bevriend*. Voorbeeld:

$$(220, 284) = (2^2 \cdot 5 \cdot 11, 2^2 \cdot 71)$$

is een bevriend getallenpaar omdat

$$\begin{aligned} 220 &= s(284) = 7 \cdot 72 - 284 \text{ en} \\ 284 &= s(220) = 7 \cdot 6 \cdot 12 - 220. \end{aligned}$$

Analoog aan even volmaakte getallen is er een *regel* waarmee nieuwe bevriende getallenparen kunnen worden gevonden:

Regel van Thabit ibn Kurrah (negende eeuw). $2^k p q$ en $2^k r$ vormen een bevriend getallenpaar als $p = 3 \cdot 2^{k-1} - 1$, $q = 3 \cdot 2^k - 1$ en $r = 9 \cdot 2^{2k-1} - 1$ alle priem zijn en $k > 1$.

Voor $k = 2$ geeft deze regel het bovengenoemde bevriende getallenpaar $(220, 284)$. Ook voor $k = 4$ en $k = 7$ vinden we zo bevriende getallenparen, maar dan lijkt de koek op: voor geen andere waarden van $k \leq 6090515$ is deze regel succesvol [36].

Zij $a(X)$ het aantal bevriende getallenparen (m, n) , $m < n$, met $m \leq X$. Er is een tabel [33] met een totaal van 11 994 387 bekende bevriende getallenparen (bijgewerkt tot 28 september 2007), met daarin *alle* bevriende getallenparen $\leq 10^{14}$. Zie Tabel 1. Dit suggereert dat het quotiënt $\log a(X)/\log X$ naar een limiet convergeert, als $X \rightarrow \infty$, met mogelijke waarde $\frac{1}{3}$.

De meeste bekende bevriende getallenparen zijn gevonden met behulp van varia-

X	$a(X)$	$\log(a(X))/\log(X)$ (4 decimalen)
10^5	13	0,2228
10^6	42	0,2705
10^7	108	0,2905
10^8	236	0,2966
10^9	586	0,3075
10^{10}	1427	0,3154
10^{11}	3340	0,3203
10^{12}	7642	0,3236
10^{13}	17519	0,3264
10^{14}	39374	0,3282

Tabel 1 Aantallen bevriende getallenparen

ties van de Regel van Thabit ibn Kurrah. Voor een overzicht, zie [11]. Dekpunten van $s(n)$ na $j \geq 3$ iteraties zijn verder bekend voor $j = 4, 5, 6, 8, 9$, en $j = 28$, met aantallen, respectievelijk, 206, 1, 5, 3, 1, 1 [26].

Grote getallen en cryptografie

Het ontbinden in (priem)factoren van grote getallen is een getaltheoretisch probleem dat ook voorkomt in het leven van alledag. Het heeft vast al belangstelling getrokken in de oudheid, bijvoorbeeld met de vraag: hoe kan een herder een flink aantal schapen eerlijk verdelen over zijn kinderen? Daarvoor moet iets als een deling met rest worden uitgevoerd. Als die rest dan toevallig 0 is, zal dat de aandacht getrokken hebben omdat dat veel minder vaak voorkomt dan een rest die ongelijk is aan 0.

In 1978 hebben Rivest, Shamir en Adleman het *RSA public-key cryptosysteem* geïntroduceerd [41]. De mogelijkheid om dit systeem te kraken hangt af van de moeilijkheidsgraad van het ontbinden van grote getallen in priemfactoren. Deze eigenschap van RSA heeft de belangstelling voor het ontbindingsprobleem en voor snellere ontbindingsalgoritmen enorm gestimuleerd. Verscheidene nieuwe ontbindingsalgoritmen zijn dan ook sinds 1978 ontdekt: de kwadratische zeef van Pomerance [37–38] (waarvan het basis-idee teruggaat tot Kraitichik [20]), de getallenlichaamszeef van Pollard [35] met vele verbeteringen door Pomerance en H.W. en A.K. Lenstra [21], en de elliptische krommenmethode van H.W. Lenstra [22].

Om de complexiteit van deze algoritmen te beschrijven, definiëren we

$$L_X[v, \lambda] := \exp(\lambda(\log x)^v (\log \log x)^{1-v})$$

voor reële getallen x , v en λ met $x > e$.

Voor het gemak korten we de uitdrukking $L_X[v, \lambda + o(1)]$ af tot $L_X[v, \lambda]$, waarbij we met $o(1)$ een term aangeven die naar 0 conver-

geert als $x \rightarrow \infty$. Deze functie interpoleert tussen machten van n en machten van $\log n$:

$$L_n[1, \lambda] = n^\lambda, \quad L_n[0, \lambda] = (\log n)^\lambda.$$

De belangrijkste parameter is ν . De traditionele probeermethode (probeer of het getal deelbaar is door de priemgetallen 2, 3, 5, 7, ...) heeft $\nu = 1$, exponentiële tijd. Polynomiale tijd heeft $\nu = 0$. Er zijn veel algoritmen waarvan men vermoedt dat $\nu = \frac{1}{2}$, dus deze liggen 'halverwege' tussen exponentiële en polynomiale tijd. Op basis van heuristische overwegingen wordt de complexiteit van de kwadratische zeef geschat op $(n \text{ is het te ontbinden getal}): L_n[\frac{1}{2}, 1]$ en die van de getallenlichaamszeef op $L_n[\frac{1}{3}, c]$ met $c = (\frac{64}{9})^{1/3} \approx 1,9230$. Voor de elliptische krommenmethode is de geschatte complexiteit gelijk aan $L_p[\frac{1}{2}, \sqrt{2}]$ waarbij p de kleinste priemfactor is van het te ontbinden getal. Hier zien we een belangrijk verschil tussen de elliptische krommenmethode en bovengenoemde zeefmethoden: de complexiteit van de eerstgenoemde hangt af van de kleinste priemdeler van het te ontbinden getal, terwijl die van de zeefmethoden afhangt van het te ontbinden getal zelf.

Het beste in 1978 gepubliceerde ontbindingsresultaat was een getal van 39 decimalen dat in twee uur CPU-tijd gekraakt was [27]. Extrapolatie van dit resultaat gaf aan dat het, op één computer met 1978-technologie, naar schatting 62 miljard jaar rekenen zou kosten om een getal van 512 bits te ontbinden. Getallen van 512 bits waren in die tijd een populaire keuze voor RSA-sleutels die toen als veilig werd beschouwd, dat wil zeggen onkraakbaar voor de best bekende algoritmen en snelste computers uit die tijd. De bovengenoemde nieuwe ontbindingsalgoritmen én de komst van steeds snellere computers met steeds meer geheugen, hebben ervoor gezorgd dat het ontbindingsrecord van 39 decimalen in 1978 naar 512 bits (155 decimalen) in 1999 [4] en naar 768 bits (232 decimalen) in 2009 is opgevoerd [17].

De twee genoemde zeefmethoden proberen het te factoriseren getal te schrijven als verschil van twee kwadraten. Bij de kwadratische zeef gaat dat in principe als volgt. Kies bijvoorbeeld $n = 1649$, dan geldt:

$$41^2 = 1681 \equiv 32 \pmod{n},$$

$$42^2 = 1764 \equiv 115 \pmod{n},$$

$$43^2 = 1849 \equiv 200 \pmod{n}.$$

Als we de eerste en de derde congruentie met

elkaar vermenigvuldigen, krijgen we:

$$(41 \cdot 43)^2 \equiv 6400 \equiv 80^2 \pmod{n},$$

$$(41 \cdot 43)^2 = 1763^2 \equiv 114^2 \equiv 80^2 \pmod{n},$$

dus $n = 1649$ is een deler van $(114 - 80) \cdot (114 + 80)$. Berekenen we nu de grootste gemeenschappelijke deler (ggd) van 1649 en $114 - 80 = 34$ dan vinden we:

$$\text{ggd}(1649, 34) = \text{ggd}(34, 17) = 17,$$

dus 17 is een deler van 1649. Het quotiënt is 97, de tweede (priem)factor van 1649. De ggd van twee getallen kan snel worden gevonden met behulp van het euclidische algoritme, dat gebaseerd is op de relatie $\text{ggd}(m, n) = \text{ggd}(n, m \bmod n)$.

Het principe van RSA werkt als volgt. Elke deelnemer heeft een *openbare* en een *geheime* sleutel die als volgt worden gegenereerd. Neem twee grote priemgetallen, p en q , en bereken hun product $n = pq$. Kies nu een getal e zodanig dat

$$1 < e < n \text{ en } \text{ggd}(e, (p-1)(q-1)) = 1.$$

Vind nu d zodanig dat

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

Dit kan snel gebeuren met behulp van het euclidische algoritme [6, Section 2.1.1]. De openbare sleutel is nu het paar getallen (n, e) en de geheime sleutel is het getal d .

Stel nu dat Alice een boodschap m wil versturen aan Bob. Alice neemt Bobs openbare sleutel (n, e) uit het openbare sleutelboek, vercijfert haar boodschap door $c = m^e \bmod n$ uit te rekenen, en stuurt c naar Bob. Bob ontcijfert de ontvangen boodschap c met behulp van zijn geheime sleutel d door $c^d \bmod n$ te berekenen. Met behulp van de Stelling van Euler:

$$\text{als } \text{ggd}(m, n) = 1, \text{ dan } m^{\phi(n)} \equiv 1 \pmod{n}$$

(waarbij $\phi(n)$ Euler's ϕ -functie is die het aantal natuurlijke getallen m met $1 \leq m \leq n$ telt, die relatief priem zijn ten opzichte van n), leiden we af, gebruikmakend van (1), dat

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{k\phi(n)+1} \equiv m \pmod{n}.$$

Als nu m zo was gekozen dat $1 < m < n$ dan

volgt dat $c^d \bmod n = m$. Als men de priemfactoren p en q van n zou weten, dan zou het niet moeilijk zijn om d (uit (1)) te vinden.

Alice kan op de boodschap die ze aan Bob wil versturen ook nog haar handtekening zetten met behulp van haar eigen geheime sleutel. Bob kan die handtekening verifiëren met behulp van de openbare sleutel van Alice. Dit illustreert een belangrijke eigenschap van RSA: symmetrie.

Het onderzoek van public-key cryptosystemen en hun betrouwbaarheid vraagt een brede kennis van wiskunde en informatica. Problemen die daarbij aan de orde komen zijn: het ontbinden in priemfactoren van (zeer) grote getallen; primaliteitstests; berekening van discrete logaritmen; analyse van elliptische krommen; complexiteitsanalyse; het vinden van polynomen met ongebruikelijk veel gladde waarden (dat wil zeggen waarden waarin veel kleine priemfactoren zitten); het oplossen van grote ijle stelsels van lineaire vergelijkingen over eindige lichamen; het berekenen van wortels van grote algebraïsche getallen; modulaire aritmetiek; multiprecisie-aritmetiek; computerproblemen zoals cache-optimalisatie, parallel programmeren en het efficiënt omgaan met grote hoeveelheden data.

De Riemann-hypothese

De Riemann-zeta-functie is de analytische functie van $s = \sigma + it$, voor $\sigma > 1$ gedefinieerd door:

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

en, door middel van analytische voortzetting, voor $\sigma \leq 1, \sigma \neq 1$. Deze functie heeft nulpunten in de negatieve even gehele getallen (de zogenaamde triviale nulpunten, zo genoemd omdat ze op tamelijk eenvoudige wijze zijn te vinden) en in de zogenaamde *kritieke strip* $0 < \sigma < 1$ (de zogenaamde niet-triviale nulpunten). Hierin liggen de nulpunten symmetrisch om de lijn $\sigma = \frac{1}{2}$ en symmetrisch om de lijn $t = 0$.

De *Riemann-hypothese* [40] is de bewering dat alle niet-triviale nulpunten op de zogenaamde kritieke lijn $\sigma = \frac{1}{2}$ liggen. Voorbeeld: met behulp van het *Mathematica*-pakket [24] vinden we (een numerieke benadering van) de nulpunten in respectievelijk $s = -2$ (bij startpunt $s = 0$) en $s = \frac{1}{2} + 14,1347 \dots$ (bij startpunt $s = 0,4 + 12i$). Zie Figuur 1. $\zeta(s)$ voldoet aan de volgende functionaal

```

In[39] := FindRoot[Zeta[s] == 0, {s, 0}]
Out[39] = {s -> -2.}

{s -> -1.9999999999999973`}

In[40] := FindRoot[Zeta[s] == 0, {s, 0.4 + 12 I}]
Out[40] = {s -> 0.5 + 14.1347 I}

{s -> 0.50000000000000071` + 14.134725141734693` I}

```

Figuur 1 Twee nulpunten van $\zeta(s)$

vergelijking [10]:

$$\xi(s) = \xi(1-s) \text{ met}$$

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Het is niet zo lastig om te laten zien [15, Theorem 15] dat $\xi(s)$ reëel is voor reële s en dat $\xi(s) = \overline{\xi(\bar{s})}$. Daaruit volgt dat ook $\xi(\frac{1}{2} + it)$ reëel is. Om de niet-triviale nulpunten van de *complexe* functie $\zeta(s)$ op de lijn $s = \frac{1}{2}$ te bestuderen kan men dus de *reële* functie $\xi(\frac{1}{2} + it)$ gebruiken, en proberen tekenwisselingen van deze — continue — functie op te sporen.

We schrijven nu, met $s = \frac{1}{2} + it$,

$$\xi\left(\frac{1}{2} + it\right) = \left[e^{\Re \log \Gamma(s/2)} \pi^{-1/4} \frac{(-t^2 - \frac{1}{4})}{2} \right] \times \left[e^{i \Im \log \Gamma(s/2)} \pi^{-it/2} \zeta(s) \right].$$

Hierin is de factor binnen de eerste verzameling rechte haken een negatief reëel getal, dus is het teken van $\xi(\frac{1}{2} + it)$ tegengesteld aan het teken van de factor binnen de tweede verzameling rechte haken. De standaardnotatie

voor deze tweede factor is $Z(t)$, dat wil zeggen

$$Z(t) = e^{i\theta(t)} \zeta\left(\frac{1}{2} + it\right),$$

waarbij $\theta(t)$ gedefinieerd wordt door

$$\theta(t) = \Im \left[\log \Gamma\left(\frac{1}{4} + \frac{it}{2}\right) \right] - \frac{t}{2} \log \pi.$$

Aangezien $|Z(t)| = |\zeta(\frac{1}{2} + it)|$, vallen de nulpunten van Z samen met de imaginaire delen van de nulpunten van $\zeta(s)$ op de kritieke lijn. $Z(t)$ staat bekend als de *Riemann–Siegel* functie. Zie Figuur 2. Zij $N(T)$ het totale aantal complexe nulpunten ρ van $\zeta(s)$ met $0 < \Im(\rho) < T$ (rekening houdende met multipliciteit van de nulpunten). In 1914 heeft Backlund bewezen [1] dat onder bepaalde voorwaarden $N(T)$ gelijk is aan het natuurlijke getal dat het dichtst bij $\theta(T)/\pi + 1$ ligt. Om $\theta(t)$ uit te rekenen kan men gebruik maken van de expansie [10, Section 6.5]:

$$\theta(t) = \frac{t}{2} \log \frac{t}{2\pi} - \frac{t}{2} - \frac{\pi}{8} + \frac{1}{48t} + \mathcal{O}(t^{-3}),$$

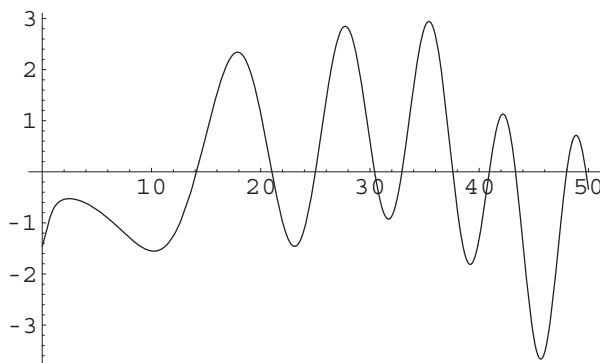
voor $t \rightarrow \infty$.

In principe is het op deze manier mogelijk

```

In[63] := Plot[RiemannSiegelZ[t], {t, 0, 50}]

```



```

Out[63] = - Graphics -

```

Figuur 2 De Riemann–Siegel-functie $Z(t)$ met de eerste 10 nulpunten op de kritieke lijn

om alle niet-triviale nulpunten van $\zeta(s)$ in een gegeven deel $T_1 < \Im(s) < T_2$ van de kritieke strip te tellen, inclusief eventuele nulpunten die *niet* op de kritieke lijn $\Re(s) = \frac{1}{2}$ liggen: bepaal zo goed mogelijk het aantal tekenwisselingen van $Z(t)$ voor $T_1 < t < T_2$ ($Z(t)$ is continu, dus tussen elke tekenwisseling ligt tenminste één nulpunt) en pas het resultaat van Backlund toe om te verifiëren of daarmee *alle* nulpunten in het gebied $T_1 < \Im(s) < T_2$ zijn geteld. In de praktijk blijkt dit perfect te werken. Om de nulpunten van ζ in de kritieke strip te bepalen moeten we dus $\zeta(s)$ voor $s = \frac{1}{2} + it$ en $Z(t)$ kunnen uitrekenen, inclusief een veilige bovengrens voor de fout (want dan kunnen we het aantal tekenwisselingen van $Z(t)$ exact bepalen). Voor de eerste nulpunten kunnen we de zogenaamde Euler–Maclaurin-formule [10, Chapter 6] gebruiken, zoals ook de eerste zeta-nulpuntenrekenaars Gram, Backlund en Hutchinson hebben gedaan. De complexiteit van de Euler–Maclaurin-formule is $\mathcal{O}(t)$ (voor $s = \frac{1}{2} + it$). Voor hoger gelegen nulpunten is de Riemann–Siegel-formule geschikter. Deze is door Siegel in 1932 gepubliceerd [42] en afgeleid uit nagelaten aantekeningen van Riemann.

Vele wiskundigen vóór Siegel hadden tevergeefs geprobeerd deze aantekeningen te ontcijferen en uit te werken. De complexiteit van de Riemann–Siegel-formule is $\mathcal{O}(\sqrt{t})$. Dankzij deze formule was het mogelijk om de Riemann-hypothese te verifiëren tot het 10 biljoenste nulpunt. Tabel 2 geeft een overzicht van de geschiedenis van de partiële verificatie van de Riemann-hypothese. Odlyzko [30] en Gourdon [13] hebben de Riemann-hypothese geverifieerd in hogere stukken van de kritieke strip. Odlyzko deed dat voor 10^{10} nulpunten in de buurt van nulpunt met rangnummer 10^{22} en Gourdon voor 2×10^9 nulpunten in de buurt van de nulpunten met rangnummer 10^{23} en 10^{24} .

Het is hier niet de plaats om op details van het rekenen aan de Riemann-hypothese in te gaan. De lezer zij hiervoor verwezen naar het boek van Edwards [10]. Een mooie inleiding in de Riemann-hypothese is het boek [44] dat een neerslag is van een UvA-webklas wiskunde voor vwo-leerlingen in de periode 2006–2010.

De 3 Priemen-stelling

Het bekende Goldbach-vermoeden [32] beweert dat elk even getal ≥ 4 kan worden geschreven als de som van twee priemgetallen. Hoewel er sterke numerieke aanwijzingen zijn dat het Goldbach-vermoeden waar is,

jaar	n	auteur(s)
1903	15	Gram
1914	79	Backlund
1925	138	Hutchinson
1935	1 041	Titchmarsh
1953	1 104	Turing
1956	25 000	Lehmer
1958	35 337	Meller
1966	250 000	Lehman
1968	3 502 500	Rosser, Yohe, Schoenfeld
1979	81 000 001	Brent
1982	200 000 001	Brent, Van de Lune, Te Riele, Winter
1983	300 000 001	Van de Lune, Te Riele
1986	1 500 000 001	Van de Lune, Te Riele, Winter
2001	10 000 000 000	Van de Lune
2004	900 000 000 000	Wedeniowski [45]
2004	10 000 000 000 000	Gourdon en Demichel [13]

Tabel 2 Geschiedenis van partiële bewijzen van de Riemann-hypothese (voor de eerste n niet-triviale nulpunten)

is dit nooit bewezen. Het is geverifieerd voor alle even getallen $\leq 4 \times 10^{18}$ [32]. Als het Goldbach-vermoeden waar is, volgt daar triviaal de zogenaamde *3 Priemen-stelling* uit, namelijk dat ieder *oneven* getal ≥ 7 geschreven kan worden als de som van drie priemgetallen. Wat is hierover bekend, zonder aanname vooraf? In 1989 is bewezen [5] dat ieder oneven getal $> 10^{43\,000}$ kan worden geschreven als de som van drie priemgetallen. Onder aanname van het waar zijn van de zogenaamde Gegeneraliseerde Riemann-hypothese (GRH, namelijk dat het reële deel van alle niet-triviale nulpunten van elke Dirichlet- L -functie gelijk is aan $\frac{1}{2}$) is in 1997 bewezen [7] dat ieder oneven getal ≥ 7 kan worden geschreven als de som van drie priemgetallen. Het bewijs hiervan kan in drie delen worden opgesplitst:

- (Zinoviev, 1997) Onder de aanname van GRH kan ieder oneven getal $> 10^{20}$ worden geschreven als de som van drie priemgetallen.
- Onder de aanname van GRH is ervoor iedere $6 \leq n \leq 10^{20}$ een priemgetal p zodanig dat $4 \leq n-p \leq 1,615 \times 10^{12}$. Als n nu een oneven getal $\leq 10^{20}$ is dan is $m = n-p$ even en $m \leq 1,615 \times 10^{12}$. Dan passen we het volgende resultaat toe:
- (Deshouillers en Te Riele, 1997) Ieder even getal m met $4 \leq m \leq 10^{13}$ kan geschreven worden als som van twee priemgetallen (dit verbeterde de toentertijd beste bovengrens voor het Goldbach-vermoeden van Sinisalo uit 1993: 4×10^{11}).

We zullen hier twee manieren beschrijven om het Goldbach-vermoeden (GV) te verifiëren.

- Zij p_i het i -de oneven priemgetal. De gebruikelijke manier om GV op een gegeven interval $[a, b]$ te verifiëren is om bij ieder even getal $e \in [a, b]$ het kleinste priemgetal p_i te vinden waarvoor $e - p_i$ ook priem is. Een efficiënte manier om dit te doen is

om eerst de verzameling priemgetallen

$$Q(a, b) = \{q \mid q \text{ priem en } a - \epsilon_a \leq q \leq b\},$$

te genereren (met de bekende Zeef van Eratosthenes), waarbij ϵ_a op een geschikte manier gekozen wordt (niet te klein, zie verder) en om dan de verzamelingen van even getallen $\mathcal{E}_0 \subset \mathcal{E}_1 \subseteq \mathcal{E}_2 \subseteq \dots$ te genereren, gedefinieerd door $\mathcal{E}_0 = \emptyset$,

$$\mathcal{E}_{i+1} = \mathcal{E}_i \cup (Q(a, b) + p_{i+1}), \quad i = 0, 1, \dots,$$

totdat, voor één of andere waarde van j , $\mathcal{E}_j$ alle even waarden in $[a, b]$ bevat. Hierbij moet ϵ_a groter zijn dan het grootste oneven priemgetal dat gebruikt wordt bij het genereren van de verzamelingen $\mathcal{E}_i$.

- Een ander idee is om voor alle even getallen $e \in [a, b]$ een priemgetal q te vinden dat dichtbij a ligt, waarvoor $e - q$ priem is. Daarvoor genereren we een verzameling van k opeenvolgende priemgetallen $q_1, q_2, \dots, q_k$ dichtbij a , voor geschikt gekozen k (zie verder), en een grote verzameling priemgetallen $\mathcal{P}$ van alle oneven priemgetallen tot ongeveer $b - a$ (met de Zeef van Eratosthenes) waarmee we $e - q$ testen op primaliteit. Voor de actuele check genereren we de verzamelingen van even getallen $\mathcal{F}_0 \subset \mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq \dots$ gedefinieerd door $\mathcal{F}_0 = \emptyset$,

$$\mathcal{F}_{i+1} = \mathcal{F}_i \cup (\mathcal{P} + q_{i+1}), \quad i = 0, 1, \dots,$$

totdat, voor één of andere waarde van j , $\mathcal{F}_j$ alle even waarden in $[a, b]$ bevat.

In de eerste genoemde aanpak om GV te verifiëren wordt een verzameling van kleine priemgetallen tot, zeg, 5000 gebruikt en voor ieder interval $[a, b]$ moeten dan alle priemgetallen in dat interval $[a, b]$ gegenereerd wor-

den. In de tweede genoemde aanpak wordt eenmalig een grote verzameling van priemgetallen $\mathcal{P}$ tot ongeveer $10^8 + 10^4$ gegenereerd, en voor ieder interval $[a, b]$ moet men dan de k grootste priemgetallen $\leq a$ genereren. Dit is natuurlijk qua rekentijd veel goedkoper dan de eerste aanpak. Het *verschil* is dat in de eerste aanpak voor ieder even getal e het *kleinste* oneven priemgetal p wordt gezocht waarvoor $e - p$ priem is. In de tweede aanpak wordt *een of ander* priemgetal p gezocht waarvoor $e - p$ priem is, maar in het algemeen is dit noch het kleinste noch het grootste priemgetal met die eigenschap.

In hun experimenten om GV tot 10^{13} te verifiëren [8] hebben Deshouillers, Te Riele en Saouter de tweede aanpak gevolgd. De lengte van het te verifiëren interval $[a, b]$ werd steeds gelijk gekozen aan 10^8 . Hoe groot moest hierbij k worden gekozen? De dichtheid van de priemgetallen in de verzameling van oneven getallen $< 10^8$ is ongeveer 0,115 (er zijn 5 761 454 oneven priemgetallen $< 10^8$ en 5×10^7 oneven getallen $< 10^8$). Dus een fractie van ongeveer 0,885 van de even getallen in $[a, b]$ wordt *niet* bedekt door de verzameling $\mathcal{F}_1 = \mathcal{P} + q_1$. Als we uniforme verdeling van de priemgetallen aannemen wordt ongeveer 0,885² van de even getallen in $[a, b]$ *niet* bedekt door $\mathcal{F}_2$, enzovoorts. Na 151 stappen is deze fractie gereduceerd tot ongeveer 10^{-8} . Voor onze experimenten bleek $k = 360$ ruim groot genoeg te zijn. Voor $a \approx 10^{13}$ impliceert dit dat het grootste priemgetal in de verzameling $\mathcal{P}$ in de buurt van $10^8 + 10^4$ moet liggen. De hoeveelheid CPU-tijd nodig om zo GV tot 10^{13} te verifiëren bedroeg ongeveer vijftig uur op een Cray C98 vector computer, gemiddeld iets minder dan twee seconden CPU-tijd per interval $[a, b]$ ter lengte van 10^8 .

Het vermoeden van Mertens

De Möbius-functie $\mu(n)$ wordt als volgt gedefinieerd:

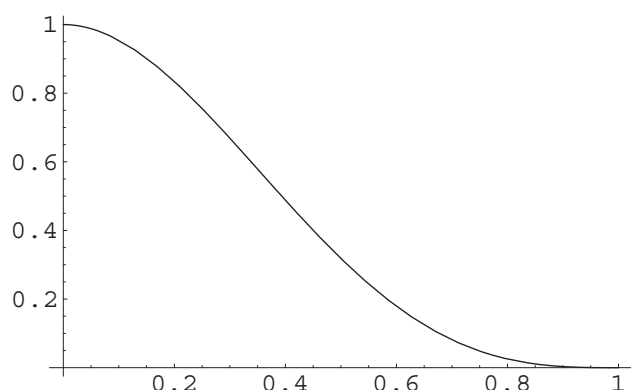
$$\mu(n) := \begin{cases} 1, & n = 1, \\ 0, & \text{als } n \text{ deelbaar is door het kwadraat van een priemgetal,} \\ (-1)^k, & \text{als } n \text{ het product is van } k \text{ verschillende priemgetallen.} \end{cases}$$

Als we de waarden $\mu(n)$ voor $1 \leq n \leq x$ sommeren krijgen we de functie

$$M(x) = \sum_{1 \leq n \leq x} \mu(n),$$

die het verschil telt tussen het aantal kwa-

Plot[(1 - t) * Cos[Pi * t] + Sin[Pi * t] / Pi, {t, 0, 1}]



Figuur 3

draatvrije natuurlijke getallen $n \leq x$ met een *even* aantal priemfactoren en dat met een *on-even* aantal priemfactoren. In 1885 claimde Stieltjes in een brief aan Hermite dat hij een bewijs had dat de functie $M(x)/\sqrt{x}$ tussen twee *vaste* grenzen oscilleert, ongeacht hoe groot x is. In het voorbijgaan merkte Stieltjes op dat men voor die grenzen waarschijnlijk -1 en $+1$ kan nemen. Het is mogelijk dat Stieltjes zijn bewering baseerde op tabellen van waarden van $M(x)$ (die in zijn nalatenschap zijn teruggevonden). De motivatie voor Stieltjes om $M(x)$ te bestuderen was dat de grootte van $M(x)$ nauw gerelateerd is aan de locatie van de complexe nulpunten van de Riemann-zeta-functie. Om precies te zijn: het begrensd zijn van $M(x)/\sqrt{x}$ impliceert de juistheid van de Riemann-hypothese! Dat is als volgt in te zien. Voor $\sigma = \Re s > 1$ geldt (met behulp van partiële sommatie):

$$\begin{aligned} 1/\zeta(s) &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \\ &= \sum_{n=1}^{\infty} \frac{M(n) - M(n-1)}{n^s} \\ &= \sum_{n=1}^{\infty} M(n) \left\{ \frac{1}{n^s} - \frac{1}{(n+1)^s} \right\} \\ &= \sum_{n=1}^{\infty} M(n) \int_n^{n+1} \frac{s dx}{x^{s+1}} \\ &= s \sum_{n=1}^{\infty} \int_n^{n+1} \frac{M(x) dx}{x^{s+1}} \\ &= s \int_1^{\infty} \frac{M(x) dx}{x^{s+1}}, \end{aligned}$$

omdat $M(x)$ constant is op ieder interval $[n, n+1)$. De begrensdheid van $M(x)/\sqrt{x}$ impliceert dat de laatste integraal in bovenstaande formule een functie definieert die analytisch is in het halfvlak $\sigma > \frac{1}{2}$, en dit zou een analytische voortzetting geven van $1/\zeta(s)$ van $\sigma > 1$ naar $\sigma > \frac{1}{2}$. In het bijzonder zou

dat impliceren dat $\zeta(s)$ geen nulpunten heeft in het halfvlak $\sigma > \frac{1}{2}$ wat vanwege de functionaalvergelijking voor $\zeta(s)$ equivalent is met de Riemann-hypothese. Bovendien is het niet moeilijk om uit bovenstaande formules af te leiden dat alle complexe nulpunten van $\zeta(s)$ enkelvoudig zijn (aangenomen dat $M(x)/\sqrt{x}$ begrensd is) [31]. Na Stieltjes hebben ook anderen tabellen van $M(x)$ berekend met het doel om meer data te verzamelen omtrent het gedrag van $M(x)/\sqrt{x}$. In 1897 publiceerde Mertens een artikel met een tabel van $M(x)$ voor $n = 1, 2, \dots, 10\,000$ die vijftig bladzijden in beslag nam [25]. Op basis van deze data concludeerde Mertens dat de ongelijkheid $|M(x)| < \sqrt{x}$, $x > 1$ 'zeer waarschijnlijk' is. Deze bewering staat bekend als 'het vermoeden van Mertens'. De meest recente systematische berekeningen van $M(x)$ (voor alle $x \in [1, X]$) zijn uitgevoerd door Kotnik en Van de Lune [18], voor $X = 10^{14}$. De grootste *positieve* waarde die ze voor $M(x)/\sqrt{x}$

vonden is 0,571, voor $x = 7\,766\,842\,813$, en de grootste *negatieve* waarde is $-0,525$, voor $x = 71\,578\,936\,427\,177$ maar het is nu wel duidelijk dat op deze manier het vermoeden van Mertens niet kan worden weerlegd.

In 1942 publiceerde Ingham [9] een artikel dat de eerste serieuze twijfel uitsprak met betrekking tot het vermoeden van Mertens. Inghams artikel liet zien dat het mogelijk is om te bewijzen dat er bepaalde grote waarden van $|M(x)|/\sqrt{x}$ bestaan *zonder dat daarvoor $M(x)$ expliciet hoeft te worden berekend*. Dit stimuleerde verder onderzoek dat in 1985 resulteerde in een artikel van Odlyzko en Te Riele [31] met een bewijs van het *bestaan* van een x waarvoor $M(x)/\sqrt{x} > 1,06$ en een andere x waarvoor $M(x)/\sqrt{x} < -1,009$. Het vermoeden van Mertens was hiermee dus weerlegd. Odlyzko en Te Riele maakten gebruik van het toentertijd nieuwe *rooster-basis-reductie*-algoritme van A.K. Lenstra, H.W. Lenstra, Jr., en L. Lovász uit 1982 [23]. In 1987 gaf Pintz [34] een *effectieve* weerlegging van het vermoeden van Mertens in de zin dat hij bewees dat $|M(x)|/\sqrt{x} > 1$ voor een of andere $x \leq \exp(3,21 \times 10^6)$. Tegenwoordig wordt algemeen aangenomen dat de functie $M(x)/\sqrt{x}$ *onbegrensd* is, zowel in positieve als in negatieve richting.

We zullen hier een schets geven van de indirecte weerlegging van het vermoeden van Mertens door Odlyzko en Te Riele. We schrijven $x = e^y$, $-\infty < y < \infty$ en definiëren

$$m(y) := M(x)x^{-1/2} = M(e^y)e^{-y/2}$$

en

Berekeningen van Kotnik en Te Riele uit 2006

De waarde van y waarvoor het positieve lokale maximum van $h(\cdot, \cdot)$ werd gevonden is

$$y = -233029271\,5134531215\,0140181996\,7723401020\,4456785091\,6681557518\,6743434036\,9240230890\,8933261706\,9029233958\,2730162362,807965$$

met

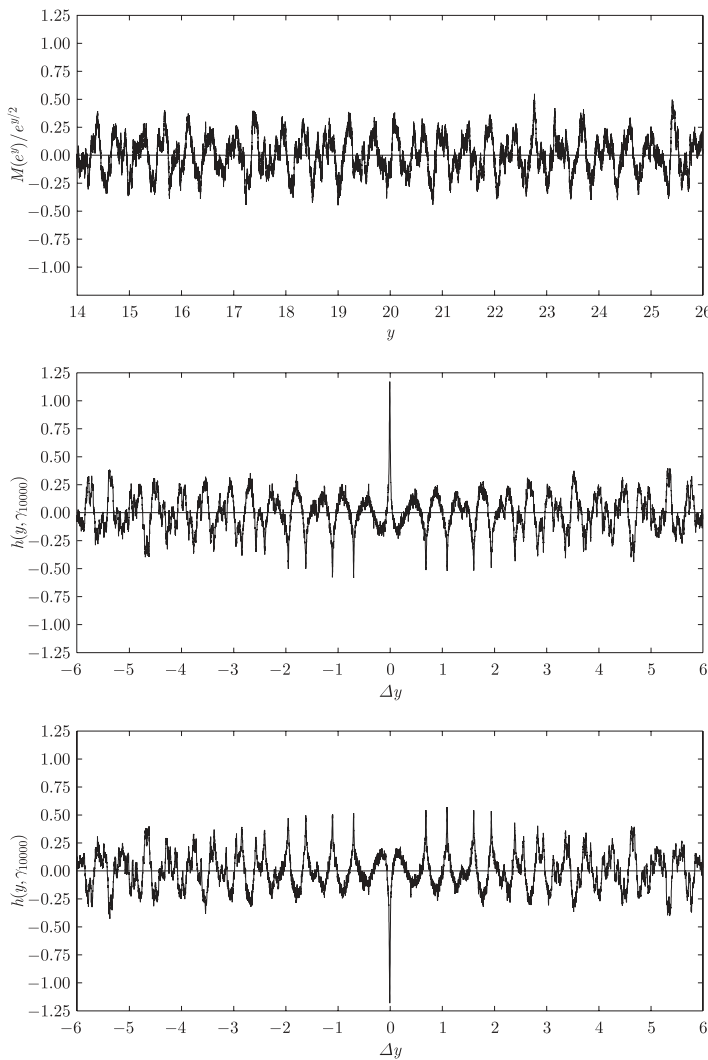
$$h(y, y_{10\,000}) = 1,218429$$

en de waarde van y waarvoor het negatieve lokale minimum werd gevonden is

$$y = -1608\,7349754400\,0919817483\,9640165505\,4685212472\,2284778177\,5539303027\,5350690810\,7957194829\,6433602695\,1442102295\,3212754000,679958$$

met

$$h(y, y_{10\,000}) = -1,229385.$$



Figuur 4 Typisch gedrag van $M(e^y)/e^{y/2}$ vergeleken met atypisch gedrag

$$\underline{m} := \liminf_{y \rightarrow \infty} m(y), \quad \overline{m} := \limsup_{y \rightarrow \infty} m(y).$$

Dan geldt [9, 16, 31]:

Stelling 2. Zij

$$h(y, T) := 2 \sum_{0 < \gamma < T} \left[\left(1 - \frac{\gamma}{T}\right) \cos\left(\pi \frac{\gamma}{T}\right) + \pi^{-1} \sin\left(\pi \frac{\gamma}{T}\right) \right] \cdot \frac{\cos(\gamma y - \psi_\gamma)}{|\rho \zeta'(\rho)|} \quad (2)$$

waarbij $\rho = \beta + i\gamma$ de complexe nulpunten van de Riemann-zeta-functie zijn met $\beta = \frac{1}{2}$ en enkelvoudig. Dan geldt voor ieder reëel getal y_0 dat $\underline{m} \leq h(y_0, T) \leq \overline{m}$ en dat iedere waarde $h(y, T)$ willekeurig dicht benaderd wordt, en oneindig vaak, door $M(x)/\sqrt{x}$.

Dus, door grote waarden van $|h(y, T)|$ te vinden — iets wat veel minder moeilijk is dan het vinden van grote waarden van $|M(x)|/\sqrt{x}$ — zou het misschien mogelijk zijn om het vermoeden van Mertens te weerleggen. Aangezien $(1-t)\cos(\pi t) + \pi^{-1}\sin(\pi t) > 0$ voor $0 < t < 1$, zie Figuur 3, en de som $\sum_\rho |\rho \zeta'(\rho)|^{-1}$ divergeert [43, Section 14.27], kan de som van de coëfficiënten van $\cos(\gamma y - \psi_\gamma)$ in Stelling 2 willekeurig groot gemaakt worden door T maar groot genoeg te kiezen. Daaruit volgt dat als we een waarde van y zouden kunnen vinden zodanig dat alle $\gamma y - \psi_\gamma$ dichtbij gehele veelvouden van 2π liggen (zodat de waarden van $\cos(\gamma y - \psi_\gamma)$ alle dicht bij 1 liggen), we de waarde van $h(y, T)$ willekeurig groot zouden kunnen maken. Dit zou dan, als we een y en een T zouden vinden waarvoor $|h(y, T)| > 1$, de weerlegging van het vermoeden van Mertens inhouden. Als de y 's lineair onafhankelijk zouden zijn over de rationale

getallen dan zouden er volgens een Stelling van Kronecker [14, Theorem 442] voor elke $\epsilon > 0$ gehele waarden van y bestaan en gehele getallen m_y waarvoor

$$|\gamma y - \psi_\gamma - 2\pi m_y| < \epsilon$$

voor alle $y \in (0, T)$. Dit zou betekenen dat $h(y, T)$, en dus $M(x)/\sqrt{x}$, willekeurig groot gemaakt kan worden. Onder dezelfde aannamen kan afgeleid worden dat $M(x)/\sqrt{x}$ willekeurig groot aan de negatieve kant kan worden gemaakt. Er is geen goede reden bekend waarom de y 's niet lineair onafhankelijk zouden zijn over de rationale getallen. Bovengenoemd probleem staat bekend als een *inhomogeen Diophantisch approximatieprobleem*.

Met behulp van het genoemde roosterbasis-reductie-algoritme van Lenstra, Lenstra en Lovász (LLL) kon het bovengenoemde inhomogene Diophantische approximatieprobleem worden opgelost voor een veel groter aantal termen dan met oudere bekende benaderingsmethoden. Enkele experimenten vooraf wezen uit dat de kans op slagen groot was als in de som in (2) de eerste 2000 nulpunten van $\zeta(s)$ zouden worden meegenomen. De 'prijs' die hiervoor betaald moest worden was dat de waarden van y in de met LLL gevonden oplossing behoorlijk groot konden zijn, namelijk orde van grootte 10^{70} . Om voor zulke y -waarden de som in (2) te berekenen was het nodig om de y 's uit te rekenen met een precisie van tenminste 75 decimalen (in de praktijk werd voor de zekerheid met 100 decimalen gerekend). De beste boven- en ondergrens die gevonden werden voor $\underline{m}$ en $\overline{m}$ waren, respectievelijk, $-1,009$ en $+1,06$, waarmee het vermoeden van Mertens dus was weerlegd.

In 2006 hebben Kotnik en Te Riele [19] de berekeningen van Odlyzko en Te Riele uit 1985 verbeterd tot reep. $-1,229$ en $+1,218$. Bovendien hebben ze de expliciete bovengrens van Pintz voor het kleinste getal waarvoor het vermoeden van Mertens onjuist is, verlaagd van $\exp(3, 21 \times 10^{64})$ naar $\exp(1,59 \times 10^{40})$. Hierbij werkten zij in de som in (2) met 10000 in plaats van met 2000 nulpunten van $\zeta(s)$. Zie kader voor de bijbehorende waarden van y .

In Figuur 4 wordt het typische gedrag van $M(e^y)/e^{y/2}$ (bovenste grafiek) vergeleken met het gedrag van $h(y, y_{10000})$ in de buurt van de 1,218-piek (middelste grafiek) en dat in de buurt van de $-1,229$ -piek (onderste grafiek). Merk de vier betrekkelijk grote negatieve pieken links en rechts van de 1,218-piek op en de vier betrekkelijk grote positieve

pieken links en rechts van de $-1,229$ -piek. Als we de onderste grafiek spiegelen ten opzichte van de horizontale as krijgen we een

grafiek die sterk lijkt op de middelste grafiek. Dat kan verklaard worden uit het feit dat de twee functies die hier zijn geplot lineaire com-

binaties van cosinussen zijn waarvan de eerste 98 termen ongeveer gelijk zijn op basis van het gebruikte LLL-algoritme [19].

Referenties

- 1 R. Backlund, Sur les zéros de la fonction $\zeta(s)$ de Riemann, *C.R. Acad. Sci. Paris* 158 (1914), 1979–1982.
- 2 Alex van den Brandhof, Roland van der Veen, Jan van de Craats en Barry Koren, *De zeven grootste raadsels van de wiskunde*, Bert Bakker, 2012.
- 3 R.P. Brent, G.L. Cohen en H.J.J. te Riele, Improved techniques for lower bounds for odd perfect numbers, *Math. Comp.* 57 (1991), 857–868.
- 4 Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Walter M. Lioen, Peter L. Montgomery, Brian Murphy, Herman J.J. te Riele, Karen Aardal, Jeff Gilchrist, Gérard Guillerm, Paul C. Leyland, Joël Marchand, François Morain, Alec Muffett, Chris Putnam, Craig Putnam, Paul Zimmermann, Factorization of a 512-bit RSA modulus, pp. 1–18 in: Bart Preneel (ed.), *Advances in Cryptology – EUROCRYPT 2000*, Lecture Notes in Computer Science, Vol. 1807, Springer, 2000.
- 5 Jingrun Chen en Tianze Wang, On the odd Goldbach problem, *Acta Math. Sinica* 32 (1989), 702–718.
- 6 Richard Crandall en Carl Pomerance, *Prime Numbers – A Computational Perspective*, Springer, 2001.
- 7 J.-M. Deshouillers, G. Effinger, H. te Riele en D. Zinoviev, A complete Vinogradov 3-primes theorem under the Riemann hypothesis, *Electr. Res. Ann. of the AMS* 3 (Sept. 17, 1997), 99–104.
- 8 J.-M. Deshouillers, H.J.J. te Riele en Y. Saouter, New experimental results concerning the Goldbach conjecture, pp. 204–215 in: J.P. Buhler (ed.), *Proc. of ANTS III, Portland, Oregon, USA, June 21st–25*, Lecture Notes in Computer Science, Vol. 1423, Springer, 1998.
- 9 A.E. Ingham, On two conjectures in the theory of numbers, *Amer. J. Math.* 64 (1942), 313–319.
- 10 H.M. Edwards, *Riemann's Zeta Function*, Dover, New York, 2001 (herdruk van de uitgave van Academic Press, Inc. uit 1974).
- 11 M. García, J.M. Pedersen en H.J.J. te Riele, Amicable numbers – a Survey, pp. 179–197 in: Alf van der Poorten en Andreas Stein (eds.), *High primes and Misdemeanours: Lectures in Honour of the Sixtieth Birthday of Hugh Cowie Williams*, Fields Institute Communications 41, AMS, 2004.
- 12 GIMPS, <http://www.mersenne.org>.
- 13 Xavier Gourdon, The 10^{13} first zeros of the Riemann zeta function, and zeros computation at very large height, oktober 2004, <http://numbers.computation.free.fr/Constants/Miscellaneous/zetazeros1e13-1e24.pdf>.
- 14 G.H. Hardy en E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford at the Clarendon Press, Fourth Edition, 1975.
- 15 A.E. Ingham, *The Distribution of Prime Numbers*, Cambridge Mathematical Library, 1990 (herdruk van de uitgave van Cambridge University Press uit 1932, met een voorwoord door R.C. Vaughan).
- 16 W. Jurkat, A. Peyerimhoff, A constructive approach to Kronecker approximations and its application to the Mertens conjecture, *J. reine angew. Math.* 286/287 (1976), 332–340.
- 17 Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen Lenstra, Emmanuel Thomé, Joppe Bos, Pierrick Gaudry, Alexander Kruppa, Peter Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev en Paul Zimmermann, Factorization of a 768-bit RSA modulus, pp. 333–350 in: T. Rabin (ed.), *Advances in Cryptology – CRYPTO 2010*, Lecture Notes in Computer Science, Vol. 6223, Springer, 2010.
- 18 Tadej Kotnik en Jan van de Lune, *Further systematic computations on the summatory function of the Möbius function*, CWI Report MAS-R0313, 2003.
- 19 Tadej Kotnik en Herman te Riele, The Mertens Conjecture Revisited, pp. 156–167 in: F. Hess, S. Pauli en M. Pohst (eds.), *Proc. of the Seventh Algorithmic Number Theory Symposium*, Lecture Notes in Computer Science, Vol. 4076, Springer, 2006.
- 20 M. Kraitchik, *Recherches sur la Théorie des Nombres*, Tome II, Factorisation, Gauthiers-Villars, Paris, 1929.
- 21 A. Lenstra en H. Lenstra, Jr., eds., *The Development of the Number Field Sieve*, Lecture Notes in Mathematics, Vol. 1554, Springer, 1993.
- 22 H. Lenstra, Jr., Factoring integers with elliptic curves, *Ann. of Math.* 126 (1987), 649–673.
- 23 A.K. Lenstra, H.W. Lenstra, Jr. en L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* 261 (1982), 515–534.
- 24 Mathematica, <http://www.wolfram.com/mathematica>.
- 25 F. Mertens, Über eine zahlentheoretische Funktion, *Sitzungsberichte Akad. Wien* 106, Abt. 2a (1897), 761–830.
- 26 David Moews, *A list of aliquot cycles of length greater than two*, <http://djm.cc/sociable.txt>.
- 27 M. Morrison en J. Brillhart, A method of factoring and the factorization of F_7 , *Math. Comp.* 29 (1975), 183–205.
- 28 P.P. Nielsen, Odd perfect numbers have at least nine distinct prime factors. *Math. Comp.* 76 (2007), 2109–2126.
- 29 Pascal Ochem en Michaël Rao, Odd perfect numbers are greater than 10^{1500} , *Math. Comp.* 81 (2012), 1869–1877.
- 30 A.M. Odlyzko, The 10^{22} -nd zero of the Riemann zeta function, pp. 139–144 in: M. van Frankenhuyzen en M.L. Lapidus (eds.), *Dynamical, Spectral, and Arithmetic Zeta Functions*, Amer. Math. Soc., Contemporary Math. Series, no. 290, 2001.
- 31 A.M. Odlyzko en H.J.J. te Riele, Disproof of the Mertens conjecture, *J. reine angew. Math.* 357 (1985), 138–160.
- 32 Thomas Oliveira e Silva, Siegfried Herzog en Silvio Pardi, Empirical verification of the even Goldbach conjecture, and computation of prime gaps, up to $4 \cdot 10^{18}$, *Math. Comp.*, to appear.
- 33 J.M. Pedersen, *Known Amicable Pairs*, <http://amicable.homepage.dk/kwnnap.htm>.
- 34 J. Pintz, An effective disproof of the Mertens conjecture, *Astérisque* 147/148 (1987), 325–333.
- 35 J.M. Pollard, *Factoring with cubic integers*, pp. 4–10 in [21].
- 36 PrimeGrid, <http://www.primegrid.com>.
- 37 C. Pomerance, The quadratic sieve factoring algorithm, pp. 169–182 in: *Advances in Cryptology, Proc. Eurocrypt 1984*, Lecture Notes in Computer Science, Vol. 209, Springer, 1985.
- 38 C. Pomerance, Analysis and comparison of some integer factoring algorithms, pp. 89–139 in: H.W. Lenstra, Jr. en R. Tijdeman, eds., *Computational methods in number theory, Part I*, Math. Centre Tracts, Vol. 154, Mathematisch Centrum, Amsterdam, 1982.
- 39 C. Pomerance, Odd perfect numbers are divisible by at least seven distinct primes, *Acta Arithm.* 25 (1973/74), 265–300.
- 40 Bernhard Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Grösse, *Monatsberichte Königl. Preuss. Akad. Wiss. Berlin* (1859), 671–680. Herdrukt in [10].
- 41 R. Rivest, A. Shamir en L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM* 21 (1978), 120–126.
- 42 C.L. Siegel, Über Riemanns Nachlass zur analytischen Zahlentheorie, *Quellen Studien zur Geschichte der Math. Astron. und Phys. Abt. B: Studien* 2 (1932), 45–80.
- 43 E.C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford, 1951.
- 44 Roland van der Veen en Jan van de Craats, *De Riemann-hypothese – een miljoenenprobleem*, Epsilon Uitgaven, Utrecht, 2011.
- 45 Sebastian Wedeniwski, <http://www.zetagrid.net>.

Barry Koren

Faculteit Wiskunde & Informatica
Technische Universiteit Eindhoven
b.koren@tue.nl

Vakantiecursus

Navier–Stokes

De Navier–Stokes-vergelijkingen behoren tot de meeste gebruikte vergelijkingen voor de berekening van gas- en vloeistofstromingen. Op de Vakantiecursus 2013 van het Platform Wiskunde Nederland vertelt Barry Koren over de Navier–Stokes-vergelijkingen, over stromingsleer en over het openstaande millenniumprobleem.

We berekenen allerlei stromingen met de Navier–Stokes-vergelijkingen, luchtstromingen om vliegtuigontwerpen bijvoorbeeld. Vliegtuigen waar we dan vervolgens gewoon instappen als ze gebouwd zijn, ofschoon we niet zeker weten of de bij het ontwerpen van die vliegtuigen met de Navier–Stokes-vergelijkingen berekende luchtstromingen wel echt betrouwbaar zijn. Een van de zes nog openstaande millenniumproblemen betreft het leveren van een bewijs voor het bestaan van betrouwbare oplossingen van de Navier–Stokes-vergelijkingen. De bijna twee eeuwen oude Navier–Stokes-vergelijkingen vormen nog steeds een uitdagend werkterrein voor wiskundigen.

Navier–Stokes-vergelijkingen

Vergelijkingen van Euler

Om de beweging van een vloeistof (het kan ook een gas zijn) in een driedimensionaal, vast, rechthoekig x, y, z -assenstelsel te beschrijven beschouwen we een oneindig kleine kubus van die vloeistof met snelheidscomponenten u, v en w in respectievelijk de x -, y - en z -richting. Deze snelheidscomponen-

ten zijn in het algemeen functies van de drie plaatscoördinaten en de tijd. Noteren we de tijd met t , dan kunnen we dus schrijven voor de snelheidscomponenten van onze oneindig kleine vloeistofkubus: $u = u(x, y, z, t)$, $v = v(x, y, z, t)$, $w = w(x, y, z, t)$. Voor de kleine verandering van bijvoorbeeld de snelheidscomponent u van het vloeistofkubusje, van tijdstip t naar het iets latere tijdstip $t + dt$, kunnen we schrijven:

$$du = \frac{\partial u}{\partial t} dt + \frac{\partial u}{\partial x} dx + \frac{\partial u}{\partial y} dy + \frac{\partial u}{\partial z} dz, \quad (1)$$

waarin

$$dx = u dt, \quad dy = v dt, \quad dz = w dt. \quad (2)$$

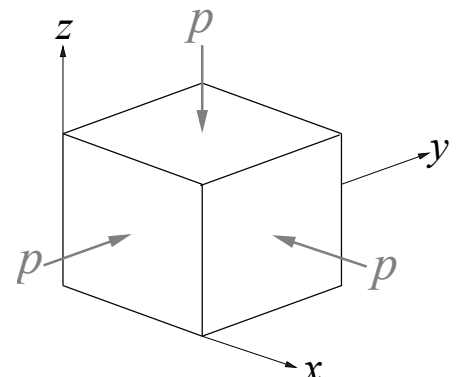
In (2) zijn dx, dy en dz de in het tijdstapje dt door het vloeistofkubusje afgelegde afstanden in respectievelijk x -, y - en z -richting. Invulling van (2) in (1) levert

$$\frac{du}{dt} = \frac{\partial u}{\partial t} + u \frac{\partial u}{\partial x} + v \frac{\partial u}{\partial y} + w \frac{\partial u}{\partial z}.$$

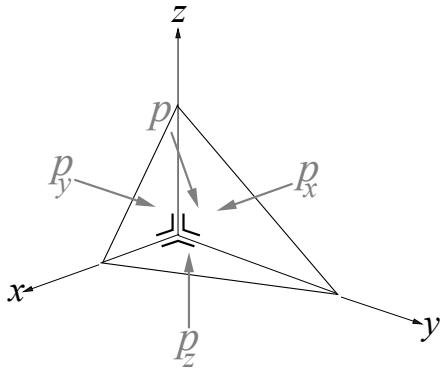
Voor $\lim_{dt \rightarrow 0} \frac{du}{dt}$ is $\frac{du}{dt}$ de versnelling in x -richting van het vloeistofkubusje op tijdstip t . Voor de versnelling in y - en z -richting gelden vergelijkbare uitdrukkingen. Voor de versnellingsvector van het vloeistofkubusje kunnen we schrijven:

$$\frac{d}{dt} \begin{pmatrix} u \\ v \\ w \end{pmatrix} = \left(\frac{\partial}{\partial t} + u \frac{\partial}{\partial x} + v \frac{\partial}{\partial y} + w \frac{\partial}{\partial z} \right) \begin{pmatrix} u \\ v \\ w \end{pmatrix}.$$

Volgens de Tweede Wet van Newton geldt dat



Figuur 1 Oneindig kleine vloeistofkubus met drukkracht op de zijwandjes.



Figuur 2 Oneindig klein, rechthoekig vloeistofviervlak met drukkrachten op de zijwandjes. De wet van Pascal zegt dat in elk punt (x, y, z) de druk in alle richtingen even groot is; $p_x = p_y = p_z = p$.

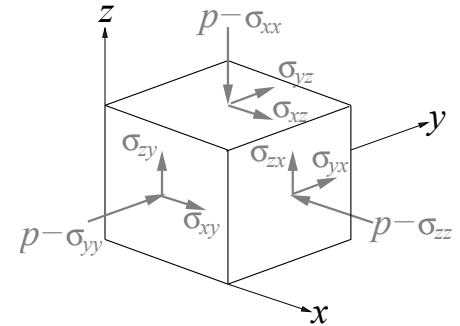
massa $\times$ versnelling van onze oneindig kleine vloeistofkubus gelijk is aan de som van de krachten op het kubusje. Als notatie voor de dichtheid (massa van de vloeistof per volume-eenheid) voeren we ρ in, waarbij, evenals voor de snelheidscomponenten, ook voor de dichtheid geldt: $\rho = \rho(x, y, z, t)$. Vervolgens beschouwen we — in navolging van Euler — als kracht die vanuit de omringende vloeistof op dit vloeistofkubusje kan werken: een oppervlaktekracht *loodrecht* op de zijwandjes van het kubusje, de drukkracht (Figuur 1). Verder beschouwen we ook een volumekracht,

een kracht die van buitenaf op alle vloeistof *in* het kubusje werkt, bijvoorbeeld de zwaartekracht.

Het bijzondere van de drukkracht is dat deze, in tegenstelling tot de snelheid en de versnelling, in elk punt in alle richtingen hetzelfde is. De druk is isotroop; de drukkracht is geen vector maar een scalar. Dit resultaat staat bekend als de Wet van Pascal en kan worden afgeleid door te eisen dat de versnelling van een oneindig klein, rechthoekig vloeistofviervlak (Figuur 2) in geen van de drie coördinaatrichtingen oneindig groot mag worden. De volumekracht kan wel een vector zijn (opgebouwd uit bijvoorbeeld de componenten van de zwaartekracht in elk van de drie coördinaatrichtingen).

De (scalaire) drukkracht noteren we met p en de (vectoriële) volumekracht met (f, g, h) , waarbij ook hier druk- en volumekracht functies van de ruimtecoördinaten en de tijd kunnen zijn; $p = p(x, y, z, t)$, enzovoort. De Tweede Wet van Newton kunnen we dan uiteindelijk voor de oneindig kleine vloeistofkubus schrijven als:

$$\rho \left(\frac{\partial}{\partial t} + u \frac{\partial}{\partial x} + v \frac{\partial}{\partial y} + w \frac{\partial}{\partial z} \right) \begin{pmatrix} u \\ v \\ w \end{pmatrix}$$



Figuur 3 Oneindig kleine vloeistofkubus met druk- en schuifkrachten op de zijwandjes.

$$= - \begin{pmatrix} \frac{\partial}{\partial x} \\ \frac{\partial}{\partial y} \\ \frac{\partial}{\partial z} \end{pmatrix} p + \begin{pmatrix} f \\ g \\ h \end{pmatrix}.$$

Dit zijn de in 1755 gepubliceerde Euler-vergelijkingen [6]. De vergelijkingen lieten al snel de juistheid zien van het reeds eerder door Daniel Bernoulli voorgestelde verband tussen druk en snelheid in bepaalde eenvoudige stromingen. Echter, de Euler-vergelijkingen toonden ook de ‘juistheid’ aan van de eveneens eerder gevonden Paradox van d’Alembert, welke zegt dat een lichaam



Sir George Gabriel Stokes (1819–1903)

George Gabriel Stokes werd op 13 augustus 1819 geboren, in Skreen, een plaatsje in het noorden van Ierland. Hij groeide op in een godsdienstig milieu; zijn vader was predikant, zijn grootvader aan de kant van zijn moeder ook, en drie van zijn broers waren voorganger in de kerk. Stokes koos voor de wetenschap en bleef zijn gehele leven ook belijdend christen. Hij was sterk geïnteresseerd in geloof en wetenschap. Zo was hij president van een vereniging ter bestudering van de relatie tussen het christelijk geloof en wetenschap.

Stokes genoot degelijk onderwijs, als kind thuis van zijn vader en als tiener op het Bristol College in Engeland. Op 18-jarige leeftijd ging hij studeren, aan het Pembroke College aan de Universiteit van Cambridge. Hij moet een uitstekend student zijn geweest; bij zijn afstuderen kreeg hij een beurs aangeboden om als wetenschappelijk medewerker op Pembroke College te blijven. En acht jaar later al werd hij hoogleraar op dezelfde leerstoel waar Newton bijna twee eeuwen daarvoor hoogleraar was geweest, de Lucasian Chair. Stokes was meer theoretisch natuurkundige dan wiskundige. Zijn onderzoeksonderwerp was eigenlijk niet stromingsleer, maar optiek, in het bijzonder de voortplanting van licht door de ether, een denkbeeldige, dunne vloeistof waar de aarde doorheen zou bewegen in het hemelruim. Het doel van Stokes’ afleiding van vergelijkingen voor de beschrijving van vloeistofstroming was niet het berekenen van zoiets aards als bijvoorbeeld de stroming van water door een rivier, maar de berekening van de stroming van hemelse ether om de aarde. Als opticus was Stokes zeer succesvol. Zo gaf hij een verklaring voor het verschijnsel van zichtbaar licht uitgestraald door een kleurloze stof als daar onzichtbare ultravioletstraling op invalt, een verklaring waarin hij het woord fluorescentie invoerde en waarvoor hij in 1852 een prijs ontving van de Royal Society. Hij stelde ook voor om met fluorescentie de moleculaire eigenschappen van stoffen te onderzoeken en legde daarmee mede de basis voor de spectraalanalyse.

Stokes bleef de Lucasian Chair tot aan zijn dood bezetten.

dat in zijn geheel wordt omstroomd door een vloeistof, daarvan geen weerstand ondervindt, hetgeen in strijd is met onze alledaagse ervaring.

Vergelijkingen van Stokes

De Euler-vergelijkingen veronderstellen dat de enige vloeistofkracht die in vloeistofstromingen kan optreden de drukkracht is. Voor praktische toepassingen schieten de Euler-vergelijkingen vaak tekort. In vloeistofstromingen kunnen naast de drukkracht ook schuifkrachten (wrijvingskrachten) optreden; krachten tangentieel aan de zijvlakjes van ons vloeistofkubusje (Figuur 3).

Het was in 1845 dat in Cambridge de natuur- en wiskundige Stokes een beter model invoerde dan dat van Euler, een model met schuifkrachten [14]. Voor het modelleren van de schuifkrachten maakte Stokes gebruik van stromingsleerwerk van Newton, werk dat in het algemeen veel minder bekend was dan de Tweede Wet van Newton, zij het waarschijnlijk niet bij Stokes als houder van de Lucasian Chair. Stokes postuleerde dat Eulers scalaire druk in feite een krachttensor is:

$$\begin{pmatrix} -p & 0 & 0 \\ 0 & -p & 0 \\ 0 & 0 & -p \end{pmatrix},$$

en wel een te eenvoudige. Stokes breidde Eulers tensor uit tot:

$$\begin{pmatrix} -p + \sigma_{xx} & \sigma_{xy} & \sigma_{xz} \\ \sigma_{yx} & -p + \sigma_{yy} & \sigma_{yz} \\ \sigma_{zx} & \sigma_{zy} & -p + \sigma_{zz} \end{pmatrix}, \quad (3)$$

waarin de niet-diagonaaltermen schuifkrachten zijn, en hij drukte alle nieuwe σ -termen uit in partiële differentiaal van u , v en w . Om te beginnen schreef hij voor de nieuwe diagonaaltermen σ_{xx} , σ_{yy} en σ_{zz} :

$$\sigma_{xx} = \lambda \left(\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial w}{\partial z} \right) + 2\mu \frac{\partial u}{\partial x}, \quad (4)$$

$$\sigma_{yy} = \lambda \left(\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial w}{\partial z} \right) + 2\mu \frac{\partial v}{\partial y}, \quad (5)$$

$$\sigma_{zz} = \lambda \left(\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial w}{\partial z} \right) + 2\mu \frac{\partial w}{\partial z}, \quad (6)$$

waarin λ en μ uit metingen bekende eigen-

schappen zijn van de specifieke beschouwde vloeistof (water, lucht of wat dan ook). Dit zijn de viscositeitscoëfficiënten, getallen die de mate van viscositeit (stroperigheid) van de vloeistof kwantificeren. De belangrijkste van de twee is μ , de afschuifviscositeit, de mate van weerstand die een vloeistof biedt tegen afschuiving (uitsmering). Hoe groter μ , hoe stroperiger (minder goed uitsmeerbaar) de vloeistof. Honing heeft bijvoorbeeld een grotere μ dan water. Bij temperatuurverlaging neemt μ in het algemeen toe; honing wordt minder goed uitsmeerbaar als het kouder wordt. De viscositeitscoëfficiënt λ hangt samen met de visceuze weerstand die een vloeistof biedt tegen samendrukking of uitzetting. Het vakgebied waarin vloeistofkrachten worden gemodelleerd, beschreven in termen van vervormingstermen, heet reologie. De door Stokes voorgestelde reologische relaties (4), (5) en (6) lijken misschien ingewikkeld, maar zijn in feite eenvoudig; ze veronderstellen een lineair (en dus eenvoudig) verband tussen krachten en vervormingssnelheidstermen. Voor de niet-diagonaalelementen in (3), de schuifkrachten, schreef Stokes nog eenvoudiger lineaire verbanden:

$$\sigma_{xy} = \sigma_{yx} = \mu \left(\frac{\partial v}{\partial x} + \frac{\partial u}{\partial y} \right),$$

$$\sigma_{yz} = \sigma_{zy} = \mu \left(\frac{\partial w}{\partial y} + \frac{\partial v}{\partial z} \right),$$

$$\sigma_{zx} = \sigma_{xz} = \mu \left(\frac{\partial u}{\partial z} + \frac{\partial w}{\partial x} \right).$$

Het argument dat hij gebruikte voor het symmetrisch laten zijn van de krachttensor ($\sigma_{xy} = \sigma_{yx}$, $\sigma_{yz} = \sigma_{zy}$, $\sigma_{zx} = \sigma_{xz}$) was vergelijkbaar met het argument dat al door Pascal was gebruikt in het isotroop laten zijn van de druk: de hoekversnellingen van het vloeistofkubusje zijn eindig aldus Stokes. Stokes ging nog verder in zijn vereenvoudiging: hij stelde voor om de zogenaamde bulkviscositeit $\tilde{\mu} \equiv \lambda + \frac{2}{3}\mu$, de visceuze weerstand tegen samendrukking en uitzetting, gelijk aan nul te nemen, dus:

$$\lambda = -\frac{2}{3}\mu.$$

Tot zover de bijdrage van Stokes.

Vergelijkingen van Navier en Saint-Venant

Als we aannemen dat $\rho = \rho(x, y, z, t) = \text{constant}$, dat wil zeggen, als we aannemen dat onze vloeistof incompressibel (onsamendruk-

baar) is, dan vereenvoudigen de door Stokes afgeleide bewegingsvergelijkingen nog verder, en wel tot:

$$\begin{aligned} & \rho \left(\frac{\partial}{\partial t} + u \frac{\partial}{\partial x} + v \frac{\partial}{\partial y} + w \frac{\partial}{\partial z} \right) \begin{pmatrix} u \\ v \\ w \end{pmatrix} \\ &= - \begin{pmatrix} \frac{\partial}{\partial x} \\ \frac{\partial}{\partial y} \\ \frac{\partial}{\partial z} \end{pmatrix} p \\ &+ \mu \left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2} \right) \begin{pmatrix} u \\ v \\ w \end{pmatrix} + \begin{pmatrix} f \\ g \\ h \end{pmatrix}. \end{aligned} \quad (7)$$

Stelsel (7) is een gekoppeld stelsel van drie partiële differentiaalvergelijkingen, met vier te bepalen oplossingscomponenten: $u = u(x, y, z, t)$, $v = v(x, y, z, t)$, $w = w(x, y, z, t)$, $p = p(x, y, z, t)$. Om het stelsel vergelijkingen sluitend te maken wordt de wet van behoud van massa toegevoegd, welke zich voor een incompressibele vloeistofstroming laat schrijven als

$$\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial w}{\partial z} = 0. \quad (8)$$

Vergelijking (8) is al stilzwijgend gebruikt bij het afleiden van (7). Stelsel (7) met daaraan toegevoegd vergelijking (8) vormen tezamen de wijd en zijd gebruikte incompressibele Navier–Stokes-vergelijkingen, de vergelijkingen waarvoor een van de zes nog openstaande millenniumproblemen is geformuleerd [7].

Het stelsel vergelijkingen (7)–(8) is reeds in 1822 afgeleid door de Fransman Navier [10]. Navier was niet uitgegaan van de in Figuur 3 geschetste situatie, de situatie met normaal- en tangentialkrachten werkend op de zijvlakjes van de oneindig kleine vloeistofkubus. Naviers uitgangspunt was het aanpassen van de Euler-vergelijkingen voor krachten die tussen vloeistofmoleculen kunnen werken. Navier nam aan dat deze krachten afstotend zijn bij kleine afstanden tussen de moleculen en aantrekkend bij grotere afstanden. Daarnaast nam hij aan dat deze krachten evenredig zijn met de snelheid van moleculen ten opzichte van elkaar. Navier leidde op basis hiervan als stelsel vergelijkingen af: de Euler-vergelijkingen met daaraan toegevoegd termen voor intermoleculaire krachten;



Claude Louis Marie Henri Navier (1785–1836)

Claude Louis Marie Henri Navier werd geboren op 10 februari 1785 in Dijon en bracht zijn kinderjaren grotendeels door in Parijs, waar zijn vader juridisch medewerker was in de Nationale Assemblee. Toen de kleine Claude acht jaar oud was overleed zijn vader en werd hij voor zijn opvoeding toevertrouwd aan een oom van zijn moeder, Emiland Gauthey. Oudoom Emiland was een uitstekend ingenieur. Onder zijn invloed ging Claude Navier in 1802 studeren aan de École Polytechnique. In 1806 studeerde hij af, als ingenieur in de weg- en waterbouwkunde. Hij pakte door; hij ging studeren bij Fourier. Fouriers invloed op Navier was groot en blijvend; Navier werd zijn beschermeling en vriend voor het leven.

Navier werkte zich op tot een van Frankrijks beste ingenieurs. Hij publiceerde ook; hij gaf het werk van zijn oudoom uit en schreef ook zelf. In zijn publicaties legde hij, met zijn bij Fourier verworven analytische inslag, mede de wetenschappelijke basis voor de ingenieurswetenschappen, een basis die tot dan toe tamelijk empirisch was. Het belang van Naviers vernieuwende ingenieursstijl werd erkend. In 1819 werd hij docent aan de École des Ponts et Chaussées. Zijn ster als wetenschapper begon ook te rijzen. In 1826 werd hij lid van de Academie van Wetenschappen in Parijs. Hij ontwikkelde zich steeds meer tot wiskundige, maar bleef ook ingenieur; in 1831 volgde hij Cauchy op als docent aan de prestigieuze École Polytechnique, maar bleef ook nog bruggen ontwerpen.

termen die precies hetzelfde waren als die welke later formeel werden afgeleid als zijnde schuifkrachten in incompressibele vloeistofstromingen. Navier kende het begrip schuifkrachten in vloeistofstromingen vermoedelijk niet eens, maar vond deze indirect in feite toch. Naviers afleiding en resultaat waren geen kwestie van geluk. Uit de kinetische gastheorie weten we nu dat de viscositeitscoëfficiënt μ te maken heeft met de vrije weglengte tussen de moleculen. Al met al knap fundamenteel werk van Navier, die was opgeleid als ingenieur en was gespecialiseerd in het ontwerpen van bruggen.

Navier overleed op betrekkelijk jonge leeftijd, in 1836. Zijn werk aan de beschrijving van vloeistofstromingen was echter niet onopgemerkt gebleven. Op zijn hypothese over de intermoleculaire krachten werd voortgeborduurd door Cauchy en Poisson. En de ingenieur Adhémar Jean Claude Barré de Saint-Venant (1797–1886) was er ook mee bekend, zoals blijkt uit een boek van hem [2]. Zeven jaar na Naviers dood leidde Saint-Venant de door Navier gevonden vergelijkingen opnieuw af, nu echter wel uitgaande van schuifkrachten in de vloeistofstroming, en zonder gebruik te maken van Naviers moleculaire aanpak. Hij had het helemaal bij het juiste eind en publiceerde de resultaten van zijn onderzoek [3], twee jaar voor de publicatie van Stokes! Eigenlijk zouden we van de *Navier–Barré de Saint-Venant–Stokes-vergelijkingen* moeten spreken, maar dat is natuurlijk wel een hele mond vol. De geschiedenis vertelt dat Stokes ook niet van dit werk van Saint-Venant wist.

Paradox

Met de introductie van de Navier–Stokes-vergelijkingen, nu al bijna twee eeuwen geleden, leek het probleem van het begrijpen en beheersen van een grote klasse stromingen onder handbereik. Het probleem was immers teruggebracht tot het oplossen van een handvol partiële differentiaalvergelijkingen.

Hoewel de Navier–Stokes-vergelijkingen grote vooruitgang brachten, bleek de analytische oplossing van de complete vergelijkingen, de ‘oplossing met potlood en papier’, te hoog gegrepen. Het gevolg was het ontstaan van een groot aantal van Navier–Stokes afgeleide, vereenvoudigde vergelijkingen voor speciale gevallen, die *wel* analytisch waren aan te pakken. Het was paradoxaal om te zien dat de invoering van de Navier–Stokes-vergelijkingen leidde tot een steeds grotere fragmentatie in verschillende stromingsmodellen, die *allemaal* de stroming beschreven van hetzelfde medium, een theoretisch hoogst ongewenste situatie.

Experimentele stromingsleer ontwikkelde zich sterk tijdens de industriële revolutie. Theoretische stromingsleer daarentegen stagneerde langs een front van niet-lineaire problemen. Het doorbreken daarvan zou uiteindelijk pas in de tweede helft van de twintigste eeuw gebeuren, met numeriek-wiskundige methoden: met getallen, bij benadering, en ten koste van veel, vaak heel veel rekenwerk. Een sleutelrol hierbij zou worden gespeeld door de oorspronkelijk uit Hongarije afkomstige wiskundige John von Neumann. Hoe dit is gegaan illustreren we aan de hand van het probleem van weersvoorspelling.

Numerieke Stromingsleer

Numerieke weersvoorspelling

Een alledaagse toepassing van de Navier–Stokes-vergelijkingen is weersvoorspelling. Voor de Tweede Wereldoorlog was weersvoorspelling meer een kunst dan een kunde. Elke dag werden weergegevens van verschillende plaatsen verzameld. Deze gegevens werden op land- en zeekaarten uitgezet, waarna er lijnen van constante druk en temperatuur op deze kaarten werden geschetst. Door vergelijking met oude druk- en temperatuurverdelingen en bijbehorende, bekende weersverlopen werd vervolgens door een weerkundige een weersvoorspelling gedaan. De persoonlijke deskundigheid van deze meteoroloog drukte een zwaar subjectief stempel op de weersvoorspelling. Wat wiskunde betreft werd slechts gebruik gemaakt van elementaire statistiek en wat eenvoudige interpolatie- en extrapolatiemethoden.

In een poging om tot een meer wetenschappelijk gefundeerde weersvoorspelling te komen had de Noor Vilhelm Bjerknes aan het begin van de twintigste eeuw het idee geopperd om het weer te voorspellen op basis van de Navier–Stokes-vergelijkingen, waar nodig aangevuld met andere vergelijkingen [4]. Voor een weersvoorspelling wil je verdelingen weten in ruimte en tijd — de toekomst uiteraard — van onder andere windsnelheid en luchtdruk. Deze verdelingen zitten diep in de Navier–Stokes-vergelijkingen verpakt; ze zijn er niet gemakkelijk uit op te lossen. Exacte oplossing van de Navier–Stokes-vergelijkingen is vandaag de dag nog steeds onmogelijk. Bjerknes kwam



John von Neumann (1903–1957)

niet verder dan zijn idee, wel een belangrijk idee.

Het niet exact, maar bij benadering oplossen van de Navier–Stokes-vergelijkingen is wel te doen. In het geval van weersvoorspelling gaat dat bijvoorbeeld als volgt. In de atmosfeer om de gehele aarde leggen we een grote verzameling netjes verdeelde punten neer (bijvoorbeeld 1000 punten in lengterichting, helemaal rondom de aarde; 500 punten in breedterichting, van pool tot pool; en 100 punten in hoogterichting, vanaf het aardoppervlak tot ergens hoog in de atmosfeer, totaal in dit voorbeeld dus $1000 \times 500 \times 100 = 50$ miljoen punten). De driedimensionale verzameling punten noemen we het rooster. Het rooster zit aan de aarde vast. In elk roosterpunt willen we de snelheidsvector en de druk uitrekenen op één of meerdere tijdstippen in de toekomst. We nummeren de roosterpunten in elk van de drie coördinaatrichtingen, bijvoorbeeld met $i = 1, 2, 3, \dots, i_{\max}$, $j = 1, 2, 3, \dots, j_{\max}$, $k = 1, 2, 3, \dots, k_{\max}$. In het getallenvoorbeeld van hiervoor geldt: $i_{\max} = 1000$, $j_{\max} = 500$, $k_{\max} = 100$. Deze discrete (puntsge- wijze) benadering van de continue driedimensionale ruimte kan nauwkeuriger worden gemaakt door met kleinere onderlinge afstanden tussen de roosterpunten te werken; door meer roosterpunten te gebruiken. Echter, hoe meer roosterpunten, hoe meer rekenwerk en dus rekentijd. We willen geen ‘weersnaspelling’.

Niet alleen in de ruimte maar ook in de tijd passen we een discrete benadering toe; we vervangen de continue tijd t door de discrete tijd $l\Delta t$, $l = 0, 1, 2, \dots, l_{\max}$, waarbij Δt een te kiezen, kleine stap vooruit in de tijd is, en $l_{\max}$ het nummer van een eindtijdstip tot waaraan toe we willen rekenen. Voor $l = 0$ zitten we op het begintijdstip van *waaraf* we willen gaan rekenen.

De Navier–Stokes-vergelijkingen (7)–(8) worden nu herschreven op dit discrete ruimtetijdrooster. We vervangen hiertoe alle partiële differentiaal in de Navier–Stokes-vergelijkingen door eindige differenties. Hier enige voorbeelden (alternatieven zijn mogelijk) van deze eindige differenties, waarbij een viervoudig subscript aangeeft in welk punt we ons bevinden in ruimte en tijd:

$$\begin{aligned} \left(\frac{\partial u}{\partial t}\right)_{i,j,k,l} &\rightarrow \frac{u_{i,j,k,l+1} - u_{i,j,k,l}}{\Delta t}, \\ \left(\frac{\partial u}{\partial x}\right)_{i,j,k,l} &\rightarrow \frac{u_{i+1,j,k,l} - u_{i-1,j,k,l}}{x_{i+1,j,k} - x_{i-1,j,k}}, \\ \left(\frac{\partial^2 u}{\partial x^2}\right)_{i,j,k,l} &\rightarrow \frac{\frac{u_{i+1,j,k,l} - u_{i,j,k,l}}{x_{i+1,j,k} - x_{i,j,k}} - \frac{u_{i,j,k,l} - u_{i-1,j,k,l}}{x_{i,j,k} - x_{i-1,j,k}}}{\frac{1}{2}(x_{i+1,j,k} - x_{i-1,j,k})}, \end{aligned}$$

enzovoort. (Tweede-orde-differentiaal worden dus herschreven als differenties van differenties.) Op deze manier vervangen we het stelsel van vier partiële differentiaalvergelijkingen door een stelsel van, in ons voorbeeld, 4×50 miljoen eindige-

differentievergelijkingen. Dus geen onoplosbare partiële differentiaalvergelijkingen meer, maar relatief gemakkelijke algebraïsche vergelijkingen. De algebraïsche vergelijkingen zijn wel groot in aantal, niet-lineair en bovendien gekoppeld. Het laatste omdat elk roosterpunt is gekoppeld aan buurpunten.

Het rekenwerk kan nu beginnen. Op basis van meetgegevens van het weer over de gehele aarde op een bepaald tijdstip kunnen we een beginoplossing voor onze numerieke weersvoorspelling definiëren: in elke roosterpunt de daar ter plaatse *gemeten* waarden van windsnelheid en luchtdruk. Voor roosterpunten waar meetgegevens ontbreken moet de beginoplossing door interpolatie of extrapolatie vanuit de meetgegevens worden aangemaakt. Deze beginoplossing kunnen we vervolgens invullen in het stelsel eindige-differentievergelijkingen, en uit dat stelsel kunnen we dan in alle roosterpunten de oplossing op het nieuwe tijdsniveau $l = 1$ uitrekenen, dus voor alle i, j, k de numerieke oplossing op tijdstip $t = \Delta t$: $u_{i,j,k,l=1}$, $v_{i,j,k,l=1}$, $w_{i,j,k,l=1}$, $p_{i,j,k,l=1}$, $i = 1, 2, 3, \dots, i_{\max}$, $j = 1, 2, 3, \dots, j_{\max}$, $k = 1, 2, 3, \dots, k_{\max}$. Een complicatie is dat in het stelsel (7)–(8) geen term $\frac{\partial p}{\partial t}$ voorkomt. Met de druk kunnen we dus niet rechthoekig rechtaan vooruit stappen in de tijd. Voor wie wil weten hoe dit probleem is opgelost, zij verwezen naar bijvoorbeeld het klassieke numerieke stromingsleerboek van Pieter Wesseling [16]. Een subtiliteit tenslotte is de keuze van de tijdstap Δt . Deze kan gemakkelijk te groot worden genomen, met numerieke instabiliteit tot gevolg.

We hebben hier in grote lijnen al een numeriek algoritme te pakken. We zagen: hoe fijnmaziger het rooster, hoe nauwkeuriger de ruimtelijke weergave van het weer. Hetzelfde geldt voor het verloop van het weer in de tijd; hoe kleiner de stap Δt vooruit in de tijd, hoe nauwkeuriger de voorspellingen, maar ook hier: hoe meer rekenwerk tot we bij de gewenste eindtijd zijn. De hoeveelheid rekenwerk voor betrouwbare weersvoorspelling over een redelijk lange termijn is gigantisch.

De Britse meteoroloog Lewis Fry Richardson was de eerste die aan echte numerieke weersvoorspelling ging doen [12]. Richardson deed in de jaren twintig van de vorige eeuw een poging om het reeds voorbijgeen van 20 mei 1910 over een tijdsduur van zes uur te ‘voorspellen’. Hij koos die dag omdat het een internationale ballonvaartdag was geweest, een dag waarvoor veel weergegevens voor zijn beginoplossing beschikbaar waren. Richardsons numerieke weersvoorspelling werd een grote teleurstelling, in twee opzichten. De

voorspelling was helemaal fout en kostte bovendien veel te veel tijd: zes weken hard rekenen voor zes uur ‘weersnaspelling’. Alle rekenwerk was nog met de hand gedaan, in teamverband, dat wel. Bjerknes’ idee van numerieke weersvoorspelling op basis van de Navier–Stokes-vergelijkingen ging weer de mottenballen in, tot de Tweede Wereldoorlog.

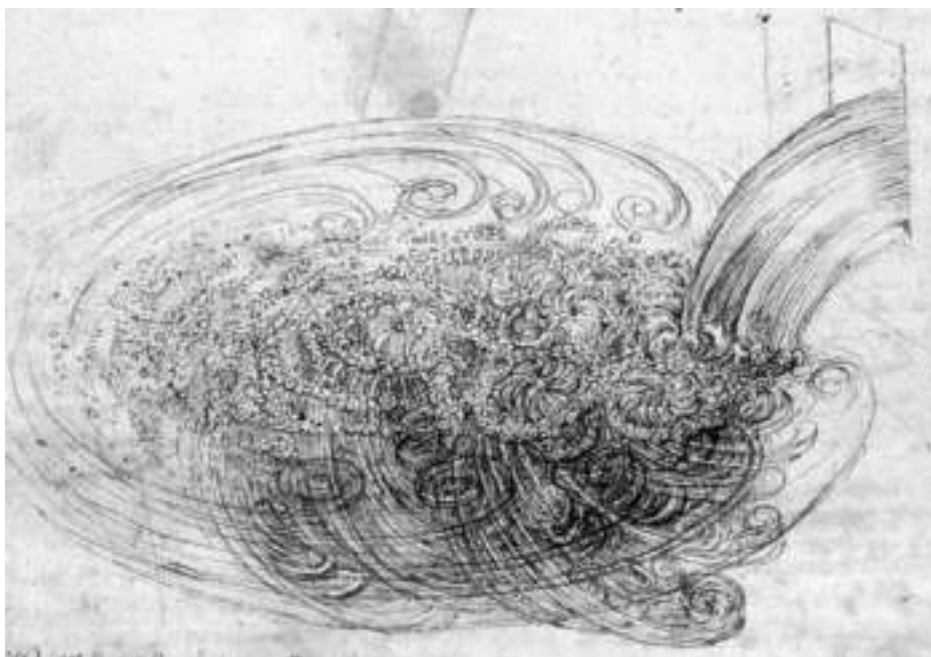
Een goede weersvoorspelling is van groot militair-strategisch belang. Toen de Verenigde Staten in de Tweede Wereldoorlog werden betrokken besloot men daar tot opleiding van maar liefst 5000 extra weerambtenaren. En in 1942 pakte de Hongaars-Amerikaanse wiskundige John von Neumann er de handschoen van numerieke weersvoorspelling weer op. Voor numerieke berekeningen waarin heel veel keer dezelfde soort sommen worden herhaald is numerieke stabiliteit, het niet buitensporig groeien van kleine foutjes (afrondfoutjes bijvoorbeeld), van cruciaal belang. Von Neumann bedacht een goede methode voor het vooraf analyseren (en zo nodig verbeteren) van de stabiliteit van numerieke methoden. De eerder door Richardson gebruikte numerieke methode voor weersvoorspelling bleek altijd instabiel te zijn volgens Von Neumanns stabiliteitsanalyse, dat wil zeggen voor elke positieve tijdstap Δt . Dat verklaart mogelijk ook waarom Richardsons resultaten niet klopten.

Von Neumann ging verder. Hij zag de ontwikkeling van een automatische, elektronische, digitale rekenmachine met interne programma-opslag — de computer zoals we die nu kennen — als de manier om onder de te lange rekentijden uit te komen. Hij stortte zich ook op de ontwikkeling van zo’n machine, in al zijn facetten: van abstracte computerarchitectuur tot concrete invoer- en uitvoerapparatuur, en van algemene richtlijnen voor programmeren tot details over getallenrepresentatie.

Von Neumann had veel succes met al dit werk. Hij is de grondlegger van het vak numerieke stromingsleer. Numerieke weersvoorspelling is de manier van weersvoorspellen van vandaag de dag. Een gedetailleerd overzicht van Von Neumanns werk aan numerieke weersvoorspelling, aan numerieke wiskunde en informatica in het algemeen, is te vinden in [1].

Numerieke wiskunde

Met het werk van Von Neumann kwam de numerieke stromingsleer en daarmee numerieke wiskunde tot grote groei en bloei. Er kwam financiering voor onderwijs en onderzoek in de numerieke wiskunde. Wiskundig



Figuur 4 Tekening van turbulente stroming aan de voet van een waterval, Leonardo da Vinci (1508).

talent voelde zich steeds meer aangetrokken tot het vak. Allerlei elegante en krachtige numerieke algoritmen werden en worden nog steeds ontwikkeld. Numerieke wiskunde is een breed vakgebied geworden met daarin allerlei specialismen.

Numerieke algoritmen speciaal ontwikkeld voor de Navier–Stokes-vergelijkingen zijn misschien wel het verst ontwikkeld van alle numerieke algoritmen. Nog steeds echter — ondanks het zeer wijdverbreide numeriek-wiskundige gebruik van de Navier–Stokes-vergelijkingen — is het niet met zekerheid bekend of er nog wel een oplossing bestaat in het limietgeval waarin roosterpuntafstanden en tijdstapgrootte naar nul gaan (de existentievraag).

Millenniumprobleem

Turbulentie

Oplossing van het Navier–Stokes-millenniumprobleem is niet alleen vanuit wetenschappelijk maar ook vanuit praktisch oogpunt van groot belang. Binnen de stromingsleer is bijvoorbeeld turbulentie een uitgebreid, reeds lang bestaand onderzoeksterrein. Turbulentie is het (ogenschijnlijk?) wanordelijk door elkaar heen bewegen van wervels in stromingen, wervels van allerlei lengteschalen, van groot tot zeer klein. Leonardo Da Vinci had dat al gezien, waarbij hij ook coherente structuren meende te zien in de wirwar van wervels (Figuur 4).

Turbulentie treedt op in bijna alle vloeistofstromingen, ten goede of ten kwade. Tur-

bulentie is goed bij bijvoorbeeld het roeren van melk door koffie. U maakt met een lepelje één korte beweging in uw kopje waardoor er één of twee grote wervels in de koffie ontstaan. De grote wervels vervallen snel in vele, steeds kleinere en steeds chaotischer bewegend wervels. De vele kleine wervels zorgen voor een prima menging van de melk door uw koffie; turbulentie als nuttig proces. Turbulentie treedt echter ook op in bijvoorbeeld de torusvormige vaten waarin, in een magneetveld en bij extreem hoge temperatuur een plasma van deuterium en tritium wordt opgesloten ten behoeve van de opwekking van energie uit de fusie van hun atoomkernen. Hierbij is turbulentie juist ongewenst; het deel van het plasma waarin kernfusie optreedt mag namelijk niet te veel mengen met koeler plasma; de kernfusie zou daardoor immers kunnen stilvallen.

Turbulentie is een onderzoeksonderwerp met nog veel onbeantwoorde vragen.

Existentie

Het Navier–Stokes-millenniumprobleem betreft de bewegingsvergelijkingen (7) plus massabehoudsvergelijking (8). Om stelsels partiële differentiaalvergelijkingen te kunnen oplossen moet de oplossing (of differentiaal daarvan) op het begintijdstip en op de ruimtelijke randen van het rekengebied worden voorgeschreven; er moeten begin- en randvoorwaarden worden gespecificeerd. Begin- en randvoorwaarden zijn meestal probleemspecifiek; ze beschrijven bijvoorbeeld de initiële stromingstoestand (de beginvoorwaar-

de) van de koffie in het koffiekopje van hier voor, alsmede de geometrie van het kopje en de stromingstoestand van de koffie op de binnenkant van het kopje (de randvoorwaarden).

In de beschrijving van het Navier–Stokes-millenniumprobleem [7] zijn ook beginvoorwaarden gegeven. Deze zijn echter niet probleemspecifiek, maar zeer algemeen. Aan de beginoplossing wordt ‘slechts’ de voorwaarde opgelegd dat deze oneindig vaak differentieerbaar is. En voor wat betreft de randvoorwaarden: deze zijn er in feite niet; de randen mogen worden beschouwd als aan elkaar vastgeplakt; de rechter rand op de x -as is vastgeplakt aan de linker rand op die as, idem voor de randen op de y - en z -as: zogenaamde periodieke randvoorwaarden. Van de volumekracht tenslotte wordt geëist dat deze oneindig vaak differentieerbaar is op alle tijdstippen.

Oplossingen van het aldus gespecificeerde algemene begin-randwaardenprobleem kunnen dus in principe slechts in zeer algemene termen worden bepaald, aannemen dat er een oplossing bestaat. Dit laatste is nu een vraag in het Navier–Stokes-millenniumprobleem: heeft het hiervoor beschreven algemene begin-randwaardenprobleem geen, één, of meerdere oplossingen,

waarbij van deze oplossingen wordt geëist dat zij oneindig vaak differentieerbaar zijn en blijven, en tevens dat de totale hoeveelheid bewegingsenergie die zij bevatten begrensd is op elk tijdstip na het begintijdstip. Voor het Navier–Stokes-millenniumprobleem hoeft dus geen exacte, algemene oplossing van de Navier–Stokes-vergelijkingen te worden bepaald. ‘Slechts’ het *wel of niet bestaan* van zo’n oplossing hoeft te worden bewezen, een oplossing die voldoende differentieerbaar is en begrensd in bewegingsenergie. Voor het aantonen dat er een oplossing bestaat mag de volumekracht zelfs gelijk aan nul worden genomen; een moeilijkheid minder. Wat dit millenniumprobleem toch nog zo moeilijk blijft maken is dat er in de vergelijkingen (7) niet-lineaire termen voorkomen, termen als $u \frac{\partial u}{\partial x}$ bijvoorbeeld.

Onderzoek

In de vorige eeuw is al veel onderzoek gedaan aan de existentie van Navier–Stokes-oplossingen. Te denken valt aan het werk van Oseen [11], Leray [9], Hopf [8], Schaffer [13], en Caffarelli en collega’s [5]. Onderzoek op het snijvlak van klassieke en numerieke analyse is dat van Temam [15]. Het is precies dit overgangsgebied in de wiskunde waar mijns inziens vooruitgang is te

verwachten met betrekking tot het Navier–Stokes-millenniumprobleem. Binnen de numerieke analyse wordt onderzoek gedaan aan de existentie van numerieke oplossingen, onderzoek dat niet gericht is op het oplossen van het Navier–Stokes-millenniumprobleem, maar dat mogelijk wel van belang kan zijn daarvoor.

Behalve het prestigieuze wetenschappelijke belang van het oplossen van het Navier–Stokes-millenniumprobleem is er dus ook het minstens even grote praktische belang van het vinden van antwoorden op openstaande vragen over turbulentie. Oplossing van het Navier–Stokes-millenniumprobleem zou wel eens direct, veel voor de praktijk belangrijke turbulentievragen kunnen beantwoorden. Over turbulentie, als berucht moeilijk onderwerp, heeft iemand ooit gezegd, als variatie op wat Sir Winston Churchill ooit over een bepaalde politieke stroming heeft gezegd: ‘Als je als onderzoeker in de stromingleer voor je dertigste niet aan turbulentie hebt gewerkt, dan heb je geen hart. Als je na je dertigste echter nog aan turbulentie werkt dan heb je geen verstand.’ Veel onderzoekers zijn gelukkig nog geen dertig jaar oud. En veel senior-onderzoekers *voelen* zich nog geen dertig; wiskundeonderzoek houdt je jong.

Referenties

- 1 W. Aspray, *John von Neumann and the Origins of Modern Computing*, MIT Press, 1990.
- 2 A.J.C. Barré de Saint-Venant, *Mécanique appliquée de Navier*, Paris, 1858.
- 3 A.J.C. Barré de Saint-Venant, Note à joindre au mémoire sur la dynamique des fluides, *Comptes Rendus des Séances de l'Académie des Sciences* 17 (1843), 1240.
- 4 V. Bjerknes, Das Problem der Wettervorhersage, betrachtet von Standpunkte der Mechanik und der Physik, *Meteorologische Zeitschrift* 21 (1904), 1–7.
- 5 L. Caffarelli, R. Kohn and L. Nirenberg, Partial regularity of suitable weak solutions of the Navier–Stokes equations, *Communications on Pure and Applied Mathematics* 35 (1982), 771–831.
- 6 L. Euler, Principes généraux du mouvement des fluides, *Mémoires de l'Académie des Sciences de Berlin* 11 (1755), 274–315.
- 7 C.L. Fefferman, Existence and smoothness of the Navier–Stokes equations, www.claymath.org/millennium/Navier-Stokes.Equations
- 8 E. Hopf, Über die Anfangswertaufgabe für die hydrodynamischen Grundgleichungen, *Mathematische Nachrichten* 4 (1951), 213–231.
- 9 J. Leray, Sur le mouvement d'un liquide visqueux emplissant l'espace, *Acta Mathematica* 63 (1934), 193–248.
- 10 C.L.M.H. Navier, Mémoire sur les lois du mouvement des fluides, *Mémoires de l'Académie des Sciences* 6 (1822), 389–440.
- 11 G.W. Oseen, Sur les formules de Green généralisées qui se présentent dans l'hydrodynamique et sur quelques-unes de leurs applications, *Acta Mathematica* 34 (1911), 205–284.
- 12 L.F. Richardson, *Weather Prediction by Numerical Process*, Cambridge University Press, 1922.
- 13 V. Scheffer, Hausdorff measure and the Navier–Stokes equations, *Communications in Mathematical Physics* 55 (1977), 97–112.
- 14 G.G. Stokes, On the theories of the internal friction of fluids in motion, and of the equilibrium and motion of elastic solids, *Transactions of the Cambridge Philosophical Society* 8 (1845), 287.
- 15 R. Temam, *Navier–Stokes Equations. Theory and Numerical Analysis*, American Mathematical Society, 1984.
- 16 P. Wesseling, *Principles of Computational Fluid Dynamics*, Springer, 2000.

Jaap Korevaar

Korteweg-De Vries Instituut voor Wiskunde

Universiteit van Amsterdam

j.korevaar@uva.nl

Column De oplossing

Priemparen

‘De oplossing’ is een nieuwe rubriek over onlangs opgeloste vermoedens in de wiskunde die een raakvlak hebben met de Nederlandse wiskundepraktijk. Jaap Korevaar opent de rubriek met een verhaal over de verrassende oplossing van een beroemd probleem in de getaltheorie door de betrekkelijk onbekende wiskundige Yitang Zhang. Is er in uw onderzoeksgebied een belangrijke doorbraak te melden? Laat het ons weten!

Dat er aan de rij priemgetallen

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37,
41, 43, 47, 53, ...

nooit een eind komt is natuurlijk al bekend sinds de oudheid. Maar er zijn nog veel open vragen over de priemgetallen. Een van de bekendste is of er in bovenstaande rij oneindig veel sprongen van lengte twee voorkomen. Met andere woorden, zijn er oneindig veel *priemtweelingen* $(p, p + 2)$:

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31),
(41, 43), ...

Dit lijkt heel waarschijnlijk, omdat er steeds weer grotere priemtweelingen gevonden worden. Op Internet [11] wordt een tweeling vermeld uit 2011 waarbij p meer dan 200 duizend cijfers heeft.

Een algemenere vraag is of er voor *elk* even verschil d , oneindig veel *priemparen*

$(p, p + d)$ zijn. Er lijken zelfs meer priemparen te zijn met verschil zes dan met verschil twee:

(5, 11), (7, 13), (11, 17), (13, 19),
(17, 23), (23, 29), (31, 37), (37, 43),
(41, 47), (47, 53), ...

Als men ver doortelt lijken het er ongeveer tweemaal zoveel te zijn.

Vermoedens

De beroemde priemgetalstelling van Hadamard en de la Vallée Poussin uit 1896 zegt dat voor grote x het aantal $\pi(x)$ van de priemgetallen $p \leq x$ goed vergelijkbaar is met het quotiënt $x / \log x$. (Hier is $\log x$ de natuurlijke logaritme, en ‘goed vergelijkbaar’ betekent dat de verhouding van $\pi(x)$ tot $x / \log x$ limiet één heeft als x naar oneindig gaat.)

In een baanbrekend artikel uit 1923 maakten de Engelse wiskundigen Hardy en Littlewood [6] plausibel dat er een analoge asymptotische gelijkheid moet gelden voor priemtweelingen. Voor grote x zou het aantal $\pi_2(x)$

van die tweelingen $(p, p + 2)$, met $p \leq x$, goed vergelijkbaar moeten zijn met $K_2 x / \log^2 x$, waarbij de constante K_2 in termen van de priemgetallen gegeven wordt door de formule

$$K_2 = 2 \prod_{p \text{ priem } p \geq 3} \left\{ 1 - \frac{1}{(p-1)^2} \right\} \\ = 1.320323 \dots$$



Yitang Zhang

Recente uitgebreide tellingen van priemtweelingen, door Nicely (Virginia) [8] en anderen, geven sterke ondersteuning voor het vermoeden.

Algemener formuleerden Hardy en Littlewood een vermoeden voor het aantal $\pi_d(x)$ van de priemparen $(p, p+d)$ met $p \leq x$. Ook dat aantal zou goed vergelijkbaar moeten zijn met een uitdrukking $K_d x / \log^2 x$. De formule voor K_d laat in het bijzonder zien dat K_6 gelijk is aan $2K_2$! Tellingen door Fokko van de Bult [3] (destijds aan de UvA) voor alle verschillen $d \leq 1000$ zijn in goede overeenstemming met het algemene vermoeden.

Recente artikelen

Na de oorlog is er door veel onderzoekers aan de priempaarvermoedens gewerkt. Tal van wiskundigen, waaronder Pólya (Stanford) in 1959 [10], hebben redeneringen bedacht die de vermoedens ondersteunen. Met name de wiskundige Goldston (San José) heeft jarenlang aan de problemen bijgedragen. Tenslotte kon hij omstreeks 2006, samen met

Pintz (Boedapest) en Yıldırım (Istanbul), het volgende frappante resultaat bewijzen [5]. Er bestaat een verschil $d \leq 16$ zodanig dat er oneindig veel priemparen $(p, p+d)$ zijn. Jammer genoeg moesten Goldston, Pintz en Yıldırım gebruik maken van een onbewezen vermoeden van Elliott (Colorado) en Halberstam (Illinois) [4]. Dat vermoeden zegt dat, met geschikte normalisatie, alle rekenkundige rijen positieve gehele getallen van de vorm $a + kq$ met $\text{ggd}(a, q) = 1$, in een bepaalde sterke zin evenveel priemgetallen bevatten. Het vermoeden is een verscherping van een wel bewezen resultaat in die richting van Bombieri (Princeton) [1] en Vinogradov (Moskou) [12], en het is aanzienlijk sterker dan het Riemann-vermoeden. Tot zover de stand van zaken begin 2013; voor meer informatie verwijzen wij de geïnteresseerde lezer naar het artikel [7].

Doorbraak

In januari van dit jaar kwam er een verrassende doorbraak. De betrekkelijk onbekende wiskundige Yitang Zhang (New Hampshire)

beweest, *zonder* gebruik van enig onbewezen vermoeden, dat er oneindig veel priemparen $(p, p+d)$ moeten zijn voor een of ander verschil d kleiner dan 70 miljoen. Voor zijn bewijs heeft hij de methode van Goldston, Pintz en Yıldırım verfijnd; hij kon het Elliott–Halberstam-vermoeden omzeilen door slim gebruik te maken van werk van Bombieri, Friedlander (Toronto) en Iwaniec (Rutgers) [2] over aantallen priemgetallen in rekenkundige rijen. Zijn artikel ‘Bounded gaps between primes’ is geaccepteerd door de *Annals of Mathematics* [13].

Na de aankondiging van Zhangs artikel is er een ware industrie ontstaan met het doel de bovengrens van 70 miljoen omlaag te brengen. Door successieve verfijningen van de methode is reeds een bovengrens tussen vier- en vijfduizend verkregen; zie de website ‘Bounded gaps between primes’ [9] onderhouden door Michael Nielsen. Volgens Goldston is het echter twijfelachtig of men zonder nieuwe ideeën de grens tot twee zal kunnen verlagen. 

Referenties

- 1 E. Bombieri, On the large sieve, *Mathematika* 12 (1965), 201–225.
- 2 E. Bombieri, J.B. Friedlander en H. Iwaniec, Primes in arithmetic progressions to large moduli, *Acta Math.* 156 (1986), 203–251; II, *Math. Ann.* 277 (1987), 361–393; III, *J. Amer. Math. Soc.* 2 (1989), 215–224.
- 3 F.J. van de Bult, Counts of prime pairs, persoonlijke communicatie, februari 2007.
- 4 P.D.T.A. Elliott en H. Halberstam, A conjecture in prime number theory, *Symposia Mathematica*, Vol. 4 (INDAM, Rome, 1968/69), Academic Press, London, pp. 59–72.
- 5 D. Goldston, J. Pintz en C.Y. Yıldırım, Primes in tuples. I, *Ann. of Math.* (2) 170 (2009), 819–862.
- 6 G.H. Hardy en J.E. Littlewood, Some problems of ‘partitio numerorum’. III: On the expression of a number as a sum of primes, *Acta Math.* 44 (1923), 1–70.
- 7 J. Korevaar, Hoe springen de priemgetallen, *Nieuw Archief voor Wiskunde* 5/11 (2010), 244–249.
- 8 T.R. Nicely, Enumeration of the twin-prime pairs to $2 \cdot 10^{16}$, www.trnicely.net, maart 2010.
- 9 M. Nielsen, Bounded gaps between primes, michaelsen.org/polymath1, 2013.
- 10 G. Pólya, Heuristic reasoning in the theory of numbers, *Amer. Math. Monthly* 66 (1959), 375–384.
- 11 Twin prime in Wikipedia 2013; en.wikipedia.org/wiki/Twin_prime#Largest_known_twin_prime_pair, 15 september 2013.
- 12 A.I. Vinogradov, The density hypothesis for Dirichlet L -series, *Izv. Akad. Nauk SSSR Ser. Mat.* 29 (1965), 903–934.
- 13 Y. Zhang, Bounded gaps between primes. To appear in *Ann. of Math*

Joke Zwarteveen*Deltion Sprint Lyceum**Zwolle**jzwarteveen@deltion.nl***Nellie Verhoef***ELAN**Universiteit Twente**n.c.verhoef@utwente.nl*

Onderwijs

Veranderingen in het eindexamenprogramma?

De commissie Toekomst Wiskunde Onderwijs (cTWO) kwam in januari 2013 met het voorstel 'Denken & doen, wiskunde op havo en vwo per 2015'. Wat is er veranderd? Joke Zwarteveen, docent wiskunde op een Vavo (Voortgezet algemeen volwassenenonderwijs), gaat op zoek, vakdidacticus Nellie Verhoef kijkt mee.

Het rapport beschrijft de nieuwe opzet voor wiskunde A, B, C en D op havo en vwo. De verschillen tussen A, B, C en D hebben te maken met de vervolgopleidingen. Wiskunde A bereidt voor op vervolgopleidingen in de sectoren economie, gezondheidszorg en landbouw & natuurlijke omgeving. Begrippen als standaardfuncties, formules en statistiek en de bijbehorende algebraïsche vaardigheden en rekenvaardigheden spelen een grote rol. Wiskunde B bereidt voor op bèta- en technische wetenschappen. Inhoudelijk ligt de nadruk op analyse en meetkunde, met ruime aandacht voor algebraïsche vaardigheden en de inzichtelijke toepassingen. Bij wiskunde C gaat het om gedragswetenschappen, de sectoren recht en taal & cultuur. Het programma richt zich op algemene wiskundige vorming en de historische en culturele plaats van wiskunde in wetenschap en maatschappij. Wiskunde D, dat in tegenstelling tot de andere wiskundevakken een keuzevak is, is verbredend en verdiepend, maar niet noodzakelijk (lees: verplicht) voor exacte vervolgstudies. Leerlingen met wiskunde D zijn beter voorbereid op een exacte vervolgstudie. De aantrekkingskracht van de wiskunde en de uitdaging die leerlingen ervaren is maatgevend voor wiskunde D.

Een stukje voorgeschiedenis

In het door cTWO gepresenteerde rapport ontbreekt wiskunde C havo, wiskunde is dus niet

verplicht voor alle havoleerlingen. Er is echter een voorstel ingediend (november 2012) om (opnieuw) wiskunde voor iedereen in te voeren. Dat betekent dat er dan geen mogelijkheid meer is om na de derde klas havo te kiezen voor 'geen wiskunde'. Het nieuwe wiskunde C zal overigens ingevoerd worden zonder experimenten vooraf. Het voorstel heeft het niet gehaald, gelukkig maar. Met cTWO zou je eigenlijk medelijden moeten hebben na alle politieke commotie. Denk bijvoorbeeld terug aan de studentenactie 'Lieve Maria' (begin 2006). In die tijd ageerde de eerste lichting eindexamenkandidaten met wiskunde in hun pakket tegen een slechte aansluiting met de universiteit. De eerstejaarsstudenten gaven aan dat het beheersen van de knoppen van de grafische rekenmachine ten koste was gegaan van het beheersen van op de universiteit (als bekend veronderstelde) algebraïsche vaardigheden. Bijspijkeren was kennelijk nodig om alsnog de spoedig daarna ingevoerde instap- of aansluitingstoetsen te halen. Eisten de universiteiten te veel, of was de vooropleiding niet toereikend? Ook werd geconstateerd dat veel hbo's het wiskundeniveau verlaagden om nog te kunnen aansluiten bij de gebrekkige kennis van aankomende havoleerlingen. Al dat gedoe heeft programmamakers voorzichtig gemaakt. Kortom, cTWO had geen gemakkelijke start.

Op de homepage <http://staff.science.uva.nl/~craats/TweeBewogenJaren.pdf> van Jan van de Craats vindt u een handig overzicht van de ontwikkelingen vanaf 2008. In dat jaar maakte staatssecretaris Marja van Bijsterveldt-Vliegthart van OCW haar beslissingen bekend over de voorgestelde examenprogramma's wiskunde havo en vwo. In dat besluit wordt de schoolwiskunde gezien als een concentrisch opgebouwd geheel: (1) een harde kern van traditionele algebraïsche vaardigheden met wat elementaire meetkunde en 'functies en grafieken'; daarbuiten (2) onderdelen van hoger niveau voortbouwend op de kern; daaromheen (3) onderdelen die op een langere termijn gezien minder belangrijk zijn in schoolwiskunde; uitmondend in (4) onderdelen waarin de wiskunde grenst aan contexten en maatschappelijke en natuurwetenschappelijke toepassingen. Deze visie viel zware kritiek ten deel met het oog op de plaats van de diverse onderdelen van de schoolwiskunde. Desondanks kreeg cTWO de opdracht om voorstellen voor vernieuwde examenprogramma's te formuleren, rekening houdend met deze visie. In het eindrapport leest u hoe omzichtig cTWO te werk is gegaan (p. 3): "Met de presentatie van de programma's is de ontwikkeling nog niet afgesloten, want er zijn nog diverse stappen te nemen in het implementatietraject. Alle bij het wiskundeonderwijs betrokken partijen zullen daarvoor hun bijdrage moeten leveren. Het onderwijs en de wiskunde ontwikkelen zich in een geleidelijk en voortdurend proces. Er is binnen het wiskundeonderwijs daarom behoefte aan een continue, reflectieve heroverweging. Daartoe

lijkt ons een breed samengestelde permanente curriculumcommissie een belangrijk instrument.” Hoe breed zal deze commissie moeten zijn samengesteld om overeenstemming te vinden?

Veranderingen

Welke zijn de in het oog lopende veranderingen in de voorstellen? We zullen deze veranderingen bekijken en van opmerkingen voorzien aan de hand van het persbericht waarin cTWO de veranderingen kort en krachtig samenvat:

1. Een andere behandeling van statistiek die beter voorbereidt op de wijze waarop in de vervolgoopleidingen statistiek wordt gebruikt.
2. De vergaande vernieuwing van wiskunde C op het vwo, toegesneden op leerlingen met interesse voor cultuur en maatschappij.
3. Wiskunde B havo dat beter past in het beperkte aantal studielasturen.
4. Een grotere rol voor analytische meetkunde bij wiskunde B, waardoor het programma coherenter wordt en de algebraïsche vaardigheden worden versterkt.
5. Bijgestelde programma's voor wiskunde D, het aanvullende wiskundekeuzevak voor bètaleerlingen, op grond van ervaringen die sinds de invoering in 2007 zijn opgedaan.
6. Wiskundige denkactiviteiten als een rode draad door alle wiskundevakken.

Ad 1. Een andere aanpak van statistiek. Waarom is dat nodig? Wel, in het moderne wetenschappelijke onderzoek wordt met grote datasets gewerkt die vervolgens statistisch bewerkt worden om er conclusies uit te kunnen trekken. Het is daarbij belangrijk te beseffen dat deze conclusies geen harde uitspraken zijn, maar een mate van waarschijnlijkheid hebben. Daarom moeten leerlingen niet alleen leren omgaan met computerprogramma's die grote datasets statistisch kunnen bewerken, maar ook leren kritisch te kijken naar de conclusies die worden getrokken. Er doemen wel problemen en vragen op, want hoe toets je het praktisch kunnen omgaan met grote datasets? Dat kan niet op het centraal schriftelijke examen omdat je dan een computer nodig hebt. Dat kan dus alleen in het schoolonderzoek aan de orde komen. Hoe toets je vervolgens de kritische houding ten opzichte van de getrokken conclusies? En: hoe onderwijs je dat? Het begrip significant(ie) is voor een havoleerling best moeilijk, zo schatten we in. Kunnen havoleerlingen

met wiskunde A het begrip betrouwbaarheid begrijpen zoals het omschreven staat (p. 158): “De kandidaat kan een betrouwbaarheidsinterval opstellen (...) met behulp van de vuistregel steekproefgemiddelde $\pm 2S/\sqrt{n}$ (waarbij S de steekproefstandaardafwijking is).”? Leidt dat tot het aanleren van trucs? De wortel n -wet is voor vwo-leerlingen al niet eenvoudig te begrijpen, laat staan voor havoleerlingen. Kortom, bij deze nieuwe aanpak zal de docent hard nodig zijn om leerlingen te begeleiden.

De statistieksituatie bij wiskunde D is weer anders. De onderwerpen hypothesetoetsen en correlatie en regressie horen er helemaal bij. Dat is nieuw. Dit zijn ‘talige’ onderwerpen waar bètaleerlingen, en dan vooral havoleerlingen, moeite mee hebben. Ze vinden de formuleringen van de opgaven al lastig, laat staan het onder woorden brengen van eigen gedachten. Jammer eigenlijk dat deze onderwerpen niet voorkomen in wiskunde A en/of C. Maar er is hoop. In de specificaties van wiskunde A en C lezen we (p. 181, 207): “De kandidaat kan (...) bij een relatie tussen twee variabelen de data uitbeelden in een kruistabel en in een grafiek.” Deze zinsnede biedt ruimte om puntenwolken en daarmee het begrip correlatie en regressie toch aan de orde te stellen. Bovendien kunnen docenten dan het nut van hypothesetoetsen duidelijk maken door een aantal opgaven aan te passen.

Ad 2. De vernieuwing van het wiskunde C-programma op het vwo. Wat betekent de vernieuwing voor vwo-leerlingen met wiskunde C? In ‘Denken & doen’ lezen we (p. 119): “Het programma richt zich op algemene wiskundige en statistische vorming, in samenhang met de historische en culturele plaats van wiskunde in wetenschap en maatschappij. Daarnaast heeft dit vak een algemeen vormende waarde doordat het leerlingen voorbereidt op de (informatie)maatschappij en hen leert in verschillende situaties wiskundige aspecten te herkennen, te interpreteren en te gebruiken.” Dat is een mond vol! Leerlingen met wiskunde C zijn niet zomaar te karakteriseren. Waren ze allemaal maar cultuurgeïnteresseerd! Er zitten ook leerlingen bij die gewoon niks met wiskunde hebben, en een ingebakken angst voor getallen koesteren. Zijn dat cultuurliefhebbers? Niet zonder meer... Voor de groep angsthazen zou het kunnen helpen over de getallenangst heen te komen door op een creatieve wijze met ‘Algebra en tellen’, ‘Verbanden’ en ‘Veranderingen’ om te leren gaan. Toch zijn er twijfels. Waarom moeten deze leerlingen rijen leren? Prak-

tische toepassingen van rijen vind je vooral bij het berekenen van annuïteiten, geschikt voor leerlingen met wiskunde A. Een ander voorbeeld, het veranderingsgedrag van functies, is aanleiding tot differentiëren met technische toepassingen en een enkele economische toepassing: dus prima passend bij wiskunde A, B en D. Waarom dit onderwerp voor leerlingen met wiskunde C?

Dan zijn er nog twee nieuwe domeinen toegevoegd: ‘Vorm en ruimte’ en ‘Logisch redeneren’. cTWO zegt daarover (p. 120): “In Vorm en ruimte vinden meetkundige principes hun plaats in toepassingen in de maatschappij en de beeldende kunst.” Bedoelt cTWO hier het berekenen van de hoeveelheid verf die nodig is om de dokwerker in Amsterdam met een 1 mm dikke verflaag te bedekken? Helemaal niet. Zo blijkt dat de leerlingen vooral moeten leren om figuren in puntperspectief te tekenen, en moeten kunnen rekenen aan eenvoudige meetkundige figuren. Maar gaat het dan om de maatschappij en beeldende kunst vraag je je af. Het gaat hier eigenlijk om basiswiskunde, en dat is nuttig.

Wat het domein logica betreft, dit komt toch ook aan de orde bij de vakken filosofie en Nederlands? Onlangs vertelde een vwo-leerling mij dat zelfs bij het schrijven van een essay voor Engels wordt gelet op een correcte logische redenering. Het enige verschil met de talen is dat bij wiskunde gebruik gemaakt wordt van tabellen en diagrammen. Lijkt uitdagend! Hoe zullen wiskunde C-leerlingen de omgang met tabellen en diagrammen oppakken? Een combinatie met Nederlands lijkt geen gek idee.

Ad 3. Een beter passend programma Wiskunde B havo. Tot onze verbijstering besloot de minister in 2007 de studielast voor wiskunde B havo te beperken: een nare, ongefundeerde miskennen van het vak wiskunde B. Deze inperking maakt het voor de havoleerlingen die voor techniek kiezen noodzakelijk om wiskunde D erbij te nemen. Terwijl bekend is dat technische hbo-opleidingen zelfs het vak wiskunde B veelal niet in de toelatingseisen hebben opgenomen! Havoleerlingen hebben op het hbo problemen met wiskunde, als zij op de havo geen wiskunde B én D hebben gevolgd (of erger nog: als zij vanuit het mbo komen, maar dit terzijde). cTWO constateert dit (p. 14, 18 en 25): “Verhoog het voorgeschreven aantal studielasturen voor wiskunde B havo, teneinde dit vak voor een grotere groep leerlingen studeerbaar te maken”, “Verstevig de positie van wiskunde D en zorg dat de verbreding, de verdieping en de gelegenheid tot

talentontwikkeling die wiskunde D biedt, behouden blijft” en “Overweeg op termijn de invoering van twee robuuste wiskundevakken, wiskunde α voor de maatschappijprofielen en wiskunde β voor de natuurprofielen, door wiskunde A en C respectievelijk B en D samen te voegen in vakken met een kerncurriculum en een bescheiden differentiatie”. Waarbij cTWO bij het robuuste vak wiskunde β ook vast en zeker denkt aan een substantiële uitbreiding van het aantal studielasturen. Hier zijn we het hartgrondig mee eens.

Ad 4. Een grotere rol voor analytische meetkunde in de meetkundedomeinen. Er zijn docenten die het betreuen dat analytische meetkunde een grotere rol gaat spelen in de meetkundedomeinen van wiskunde B. Het klopt inderdaad dat hiermee het wiskunde-programma coherenter wordt en dat de algebraïsche vaardigheden worden versterkt. Een grotere rol van algebraïsche vaardigheden impliceert echter een verschraling van de transfer van synthetische naar analytische meetkunde en omgekeerd [3]. Er zijn ook docenten die er blij mee zijn dat de leerlingen meetkundige problemen kunnen oplossen door eraan te rekenen. Voor een substantieel deel van de leerlingen is meetkunde echt een struikelblok.

Ad 5. De bijgestelde programma's voor wiskunde D. De domeinnamen bij het vwo-programma zijn (vrijwel) gelijk, maar pas op! In de specificaties zijn opvallende veranderingen te bespeuren. Het onderscheid tussen school- en samenwerkingsmodel is losgelaten en een enkel onderwerp is naar wiskunde B verplaatst. In het samenwerkingsmodel werd expliciet samengewerkt met een universiteit. Als er geen samenwerking mogelijk was, moest het schoolmodel worden gekozen, waarin de onderdelen complexe getallen en een voortzetting van dynamische modellen aangeboden worden.

In het bijgestelde programma zijn complexe getallen verplichte kost voor iedereen. En gelukkig (dat is nieuw) wordt de relatie met de vlakke meetkunde genoemd. Het onderwerp voortzetting van dynamische modellen vervalt. Met het oog op een technische universitaire vervolgopleiding is dit jammer. Zo is het zelf modelleren van veranderingsverschijnselen zinvol [4]. En het oplossen van sommige tweede-orde-differentiaalvergelijkingen met complexe getallen is nuttig om bijvoorbeeld de relatie met natuurkunde te ervaren. Daarbij is het, vinden wij, een prachtige toepassing van com-

plexe getallen, die je wiskunde D-leerlingen niet mag onthouden. Overigens zullen vindingrijke docenten vast weer mogelijkheden vinden!

In het wiskunde D-programma voor de havo zijn eveneens flinke veranderingen aangebracht. Ook hier is het onderscheid tussen school- en samenwerkingsmodel losgelaten. Het onderwerp exponentiële, logaritmische en goniometrische functies, inclusief de afgeleide ervan, is vervallen. Slechts een klein onderdeel (evenredigheden en de goniometrische functie, zonder de afgeleide) is verplaatst naar wiskunde B. De reden voor deze keuze is niet duidelijk. Het toepassen van de kettingregel op samengestelde machtsfuncties van alleen lineaire uitdrukkingen, zoals bijvoorbeeld $f(x) = \sqrt{2x-3}$, is wel erg eenvoudig, en weinig uitdagend.

Ruimtmeetkunde wordt net als wiskunde en technologie nu verplicht, in tegenstelling tot het huidige programma.

Ad 6. Wiskundige denkactiviteiten als een rode draad door alle wiskundevakken. En nu komt dan het heikele punt: wiskundige denkactiviteiten. Menig een heeft zich afgevraagd wat daarmee precies wordt bedoeld. Wat is een denkactiviteit en wat is een wiskundige denkactiviteit? cTWO probeert dat uit te

leggen door de vinger te leggen op verschillende typen wiskundige kennis en vaardigheden, procedureel en conceptueel. Vervolgens worden er zes voorbeelden van denkactiviteiten ten tonele gevoerd die een balans tussen de twee typen dienen te waarborgen (p. 30): modelleren en algebraïseren (Mo-Al), ordenen en structureren (Or-St), analytisch denken en probleemoplossen (An-Pr), formules manipuleren (Fo), abstraheren (Ab) en logisch redeneren en bewijzen (Lo-Be). In het eindrapport schrijft cTWO daarover (p. 31): “Hoe wel deze denkactiviteiten door wiskundigen herkend worden als karakteristieke elementen in de uitvoering van het vak, zijn ze in curricula, schoolmethoden en wiskundelessen veelal niet goed zichtbaar of slechts impliciet aanwezig (...). Denkactiviteiten zijn onverbrekkelijk verbonden met de inhoudelijke subdomeinen en zullen dus nooit los getoetst worden (...).” cTWO heeft het idee van wiskundige denkactiviteiten geoperationaliseerd door in een kruisjeslijst aan te geven welke denkactiviteiten er bij welk domein aan de orde (moeten) komen. In Figuur 1 een voorbeeld van wiskunde B vwo (p. 111).

Het College voor Examen, dat van overheidswege de opdracht heeft de examenstof in syllabi te beschrijven, heeft een poging gedaan deze denkactiviteiten zichtbaar te ma-

		Mo - Al	Or - St	An - Pr	Fo	Ab	Lo - Be
B1	Formules en functies	x			x	x	
B2	Standaardfuncties		x		x		
B3	Functies en grafieken	x	x		x	x	x
B4	Inverse functies			x		x	
B5	Vergelijkingen en ongelijkheden	x	x	x	x	x	x
B6	Asymptoten en limietgedrag van functies				x	x	x
C1	Afgeleide functies				x	x	x
C2	Technieken voor differentiëren		x		x		
C3	Integraalrekening			x	x		
D1	Goniometrische functies en vergelijkingen	x			x		x
E1	Meetkundige vaardigheden	x			x		x
E2	Algebraïsche methoden in de vlakke meetkunde	x	x	x	x	x	x
E3	Vectoren en inproduct	x	x	x			x
E4	Toepassingen		x		x		x

Figuur 1 Een kruisjeslijst voor wiskunde B vwo

Subdomein B1 Formules en functies

4 De kandidaat kan formules interpreteren en bewerken, bij een verband tussen twee variabelen een grafiek tekenen in een assenstelsel en bepalen of een gegeven formule herschreven kan worden als functievoorschrift.

Parate kennis. De kandidaat kent:
de voorwaarden waaronder een verband een functie is.

Reproductie. De kandidaat kan:
4.1 de structuur van een formule analyseren;
4.2 een formule herschrijven tot een gelijkwaardige formule;
4.3 een formule — indien mogelijk — herleiden tot een functievoorschrift;
4.4 bij een verband tussen twee variabelen een grafiek tekenen.

Productie. De kandidaat kan:
4.5 formules combineren tot een nieuwe formule;
4.6 bij een verband, afhankelijk van de probleemstelling, bepalen welke variabele als onafhankelijk en welke als afhankelijk beschouwd wordt;
4.7 aan de hand van een formule uitspraken doen over de bijbehorende probleemsituatie.

Figuur 2 Citaat uit de conceptsyllabus voor wiskunde B

ken, door parate kennis, reproductie (routine) en productie (met inzicht) van elkaar te onderscheiden. Het is een moedige poging, maar de indeling in reproductie en productie — of zo u wilt in procedureel en conceptueel, of welke termen men er ook voor bedacht heeft — is niet sterk afgebakend [2]. Ter illustratie in Figuur 2 een citaat uit de conceptsyllabus voor wiskunde B vwo (p. 11). De definitie “een verband is een functie dan en slechts dan als aan iedere element uit het domein precies één element uit het bereik wordt toegevoegd” moet inderdaad gewoon uit het hoofd geleerd worden, en daarmee paraat zijn. Echter, de leerling heeft aan deze parate kennis niets als de specificatie 4.6 niet wordt beheerst. Dit vraagt inzicht en staat daarom onder het kopje Productie. Pa-

rate kennis over welk verband een functie is heeft geen zin als de leerling niet weet wat een domein en een onafhankelijke variabele is. Ook productie en reproductie lopen door elkaar. Zo kan de specificatie 4.2, die onder reproductie valt, dus een wiskundige routine is, slechts volledig beheerst worden als er ook inzicht in de vorm van formules (ook wel *symbol sense* genoemd) is. Productie dus. Misschien dat daarom ook specificatie 4.5, die erg op 4.2 lijkt is opgenomen in Productie?

De implementatie van denkactiviteiten in het onderwijs is een nieuw fenomeen. cTWO ziet dit dan ook als een punt van zorg (p. 96). In verband daarmee verwijst zij naar aanbeveling 2 en 3 (p. 14, 15): “Geef een vervolg aan de vernieuwingen die zijn ingezet rondom wiskundige denkactiviteiten (...)” en “Zorg voor

professionaliseringsactiviteiten ten behoeve van het welslagen van enkele centrale aspecten van de vakvernieuwing in 2015. Het betreft met name (...) wiskundige denkactiviteiten.”

Waarom zouden deze denkactiviteiten nu expliciet in de curricula, schoolmethoden en wiskundelessen aan de orde moeten komen? We veronderstellen dat de (terechte) zorg van cTWO is dat veel van deze denkactiviteiten weinig of niet in schoolboeken voorkomen. We wezen bij het punt over wiskunde D al op het feit dat leerlingen bij het onderwerp differentiaalvergelijkingen zelf geen differentiaalvergelijking hoeven op te stellen, wat juist een unieke kans is om leerlingen nu eens echt te laten modelleren, structureren, analyseren en formules manipuleren. Vreemd eigenlijk dat we nergens iets tegenkomen over het opstellen van een differentiaalvergelijking.

In de schoolboeken zal er een accentverschuiving plaatsvinden. Minder aandacht voor reproductie (voordoen — nadoen), meer gelegenheid scheppen voor de leerlingen om zelfstandig na te denken. Hier liggen kansen voor docenten om materiaal te ontwerpen dat recht doet aan denkactiviteiten. Natuurlijk bedoelen we niet dat parate kennis en routine overbodig zijn. Elke docent weet dat aan begrip basiskennis ten grondslag ligt, en dat routinematige handelingen het werkgeheugen ontlasten om ruimte te kunnen maken voor denkactiviteiten. En dat daarom niet naar ‘inzichtopgaven’ moet worden overgestapt voordat de daarvoor benodigde kennis en vaardigheden worden beheerst. Helaas maken de meest gebruikte schoolboeken op dit moment deze overstap amper.

Wij hopen dat er meer contacttijd voor wiskundedocenten kan worden vrijgemaakt zodat zij in staat zijn eigen onderwijs te ontwerpen en met elkaar te delen.

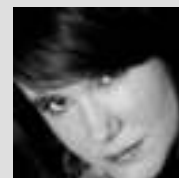
Referenties

- 1 cTWO, *Denken & doen, wiskunde op havo en vwo per 2015*, Eindrapport van de vernieuwingscommissie wiskunde cTWO, december 2012, <http://www.fisme.science.uu.nl/ctwo/publicaties/docs/CTWO-Eindrapport.pdf>
- 2 R. Skemp, Relational understanding and instrumental understanding, *Mathematics Teaching* 77 (1976), 20–26.
- 3 M. Timmer en N.C. Verhoef, Increasing insightful thinking in analytic geometry, *Nieuw Archief voor Wiskunde* 5/13(3) (2012), 217–219.
- 4 N.C. Verhoef, J.A. Zwarteveen-Roosenbrand, W.R. van Joolingen en J.M. Pieters, Wiskundig begrip bij het modelleren van veranderingsprocessen met differentiaalvergelijkingen, *Pedagogische Studiën* 90(1) (2013), 33–46.

Ionica Smeets

wetenschapsjournalist, Leiden

i@ionica.nl



Het keerpunt van Jan Beuving

Ik heb één ding overgehouden aan mijn wiskundestudie: ik treed altijd op in een ruitjesoverhemd

Theatermaker Jan Beuving (1982) bereikte in 2013 de finale van het Leids Cabaret Festival. Datzelfde jaar won het lied Vinkeveen waarvan hij de tekst schreef de Annie M.G. Schmidt-prijs voor het beste theaterlied. Beuving maakt naast liedjes ook vragen voor televisiequizzen, schrijft voor *de Volkskrant* kort over sport (zie ook kortoversport.nl) en komt eind 2014 met een avondvullend programma over wetenschap. Maar voordat hij in deze artistieke hoek belandde, studeerde Beuving wiskunde in Utrecht: "Het had voor de hand gelegen dat ik wiskundeleraar zou worden, of consultant."

Had je vroeger een droomberoep?

"Als kind wilde ik later iets met cijfertjes doen. Waarschijnlijk kwam dat door mijn vader. Als hij mij in de auto stil wilde houden, gaf hij mij een lange som over een boer met kippen die een bepaald aantal eieren legden, die de boer kon verkopen op de markt. Maar hij moest ook graan voor de kippen kopen, enzovoorts. Hoeveel winst maakt de boer? Dan ging ik als een malle rekenen en riep mijn vader: 'In je hoofd.' Ik heb in de auto leren hoofdrekenen en daar heb ik nog steeds veel plezier van. Mijn vader gaf me ook logische puzzels over leugenaars en waarheidssprekers bij kruisingen. Daar dacht ik uren over na en ik kon niet slapen voor ik het antwoord wist."

Koos je daarom voor wiskunde?

"Halverwege 5-vwo zei ik tegen mijn decaan dat ik het liefste de hele dag puzzels wilde oplossen. Hij antwoordde dat er niets an-

ders opzat: ik moest wiskunde gaan studeren."

Je ging naar Utrecht, hoe beviel de wiskunde daar?

"De mensen waren geweldig en de studie ging de eerste twee jaar goed, maar daarna kwam de klad erin. Na een bestuursjaar van de studievereniging A-Eskwadraat kon ik de motivatie niet meer opbrengen. Ik vergelijk wiskundigen graag met een groep mensen die op een open plek in het bos staan en naar een andere open plek willen. Tussen die open plekken zit een heel dicht woud. Je hebt dan drie soorten wiskundigen. Je hebt de groep die eerst heel lang nadent en dan in één keer een rechte weg naar de andere open plek hakt. Je hebt ook wiskundigen die in het wilde weg beginnen te slaan en uiteindelijk via een kronkelweg bij de andere plek belanden. De derde categorie wiskundigen kan alleen maar achter iemand anders aanlopen; en daar val ik onder. Ik houd van de weg rechtdoor en ik snap de omwegen, maar ik verzin ze allebei niet. Ik haalde mijn tentamens door heel goed te kijken hoe het eerder gedaan was, maar de echte Eureka-momenten waren zeldzaam tijdens wiskunde. Die heb ik nu veel meer als ik liedjes schrijf en precies de juiste zin bedenken."



Jan Beuving

Foto: Maartje ter Horst

Was het lastig om je studie af te maken?

"Ik had het een afgang gevonden om te stoppen. Bovendien zag ik in een onderwijscommissie de nieuwe master History and Philosophy of Science voorbijkomen. Dát moest ik natuurlijk gaan doen, de alfakant van de bètawetenschappen. In die master bleken helemaal geen deadlines te zitten op de essays die je moest schrijven. Terwijl ik die juist nodig heb, ik werk echt op de deadline. Mijn huidige werk is daarom heel prettig: iemand belt me dat hij volgende week een tekst nodig heeft. Dan maak ik het wel af. Uiteindelijk heb ik lang over mijn wiskundestudie gedaan, in totaal negen jaar. Netto is het misschien zeven jaar met dat bestuur en al die onderwijsraden die ik deed. En het laatste jaar studeerde ik ook al aan de Konings theateracademie in Den Bosch."

Hoe kwam je daar terecht?

"Er zijn natuurlijk veel bèta's die een instrument bespelen en de natuurkundefaculteit organiseerde elk jaar met kerst een muziekfestijn. In 2002 zong ik daar met twee vrienden een politiek jaaroverzicht en dat sloeg enorm aan. Later deed ik het een keer zelf achter de piano en toen werd duidelijk dat mijn teksten een stuk beter waren dan mijn pianospel. Toen stelde iemand me voor aan natuurkundige Daan van Eijk die heel handig is met een piano."

Een vruchtbare samenwerking, want in 2013 haalden jullie de finale van het Leids Cabaret Festival en nu werken jullie samen aan een avondvullend programma. Maar wanneer besloot je nu om de wiskunde te verlaten?

Juryrapport Leids Cabaret Festival

Als Jan Beuving het toneel opstapt zie je niet meteen een natuurlijke podiumpersoonlijkheid. Daar staat een bètaman in de alfa-wereld van het theater. De jury ervaart zijn insteek als verfrissend. Zijn liedjes zijn opgebouwd uit complexe rijmschema's. Ze doen ouderwets degelijk aan, maar in de goede betekenis van het woord. Deze wiskundige blijkt over een fijnzinnige poëtische geest te beschikken waarmee hij de zaal moeiteloos op zijn hand krijgt. Jan Beuving heeft een volkomen ongekunstelde aanwezigheid op het podium. Hij straalt de natuurlijke autoriteit uit van mensen die samenvallen met wie ze zijn.

"Ik ging altijd veel naar toneel, maar ik wist dat ik geen echte acteur ben. Maar toen zag ik cabaretier Kees Torn op televisie en besepte ik dat er ook andere vormen van theater bestonden. Misschien wilde ik ook wel liedjes zingen op een toneel. Ik bezocht daarna allerlei kleinkunstvoorstellingen en in het Konings theater in Den Bosch lag een folder van hun academie vol hoogdravende taal over hoe cabaret moest zijn. 'Geen kunstje maar kunst.' Zij zochten mensen die fatsoenlijk nadachten over de wereld. Daar was ik het volkomen mee eens. Veel teksten vond ik maar slecht, het rijm deugde niet en cabaret was nauwelijks nog politiek. Ik had een soort ideaal en dacht dat ik dat wel zou kunnen maken. Ik realiseerde me helemaal niet hoe moeilijk het is om politiek cabaret te maken."

Ik deed vooral auditie omdat ik niet over veertig jaar spijt wilde hebben dat ik het níet gedaan had. Mijn moeder zei grappig genoeg na mijn auditie: 'Dan komt het wel goed met die wiskundestudie.' En dat was ook zo, door auditie te doen gaf ik mezelf een harde deadline op mijn scriptie. Want toen ik werd aangenomen op de academie, moest ik wel gaan. Zodra ik daar binnenkwam, kreeg ik gelijk het stempel ouderwets. Maar dat is *the story of my life*."

Wat vind je daarvan?

"In het juryrapport van het Leids Cabaret Festival stond het als 'degelijk': ouderwets in de goede zin van het woord. Ik sta natuurlijk ook in een ouderwetse traditie, maar ik hoop wel dat het nu nog aanspreekt. De laatste tijd zit ik bijvoorbeeld heel veel Tom Lehrer te kijken. Hij is ongelooflijk grappig. Al zijn liedjes zijn te vinden op YouTube, hij heeft maar heel kort opgetreden, daarna ging hij weer lesgeven. Hij is trouwens nooit gepromoveerd en gaf wiskunde voor niet-wiskundigen. Het is moeilijk om als theatermaker genoeg mensen in je zaal te krijgen. Maar als het publiek sowieso zou komen, dan zou ik een hommage aan Tom Lehrer maken. Gewoon omdat hij het verdient."

Wat is je favoriete grap over wiskunde?

"Wat bij de zaal altijd goed werkt is dat ik zeg dat ik maar één ding heb overgehouden aan mijn wiskundestudie: dat ik altijd optreed in een ruitjesoverhemd. Wat gegoochel met getallen vinden ze meestal ook leuk. Maar een goede wiskundige grap is vaak een redeneringsfout die toch leuk is. Wie veel bijna mathematische grappen heeft, is Herman Finkers. Hij neemt je helemaal mee één kant

op en doet dan iets heel anders. 'Einstein: mijn vrouw begrijpt mij niet.' Dat is zo'n goede grap, mijn pianist Daan gebruikte hem als motto in zijn proefschrift."

Drs. P doet ook zoiets in het lied Ripspiqué, dan zingt hij: 'Tijdens die nacht van het eerste couplet.' Als kunstenaar moet je niet te meta zijn. Maar Drs. P is zo slim dat hij tijdens het lied een opmerking over het lied kan maken. Het is moeilijk om uit te leggen wat dat nou is. Mensen houden van een soort gekte. Als ze zien dat jij de orde volledig in je vingers hebt en dat je daar dan mee durft te spelen."

In mijn voorstelling zeg ik ergens op vertoondwaardig toon: 'Dan kijken mensen me aan alsof ik in de vorige eeuw geboren ben.' Per zaal is de reactie heel verschillend, soms hoor je iemand op de eerste rij zeggen: 'Maar dat is hij toch ook?' Het duurt even voordat de lach komt en mensen doorhebben dat het grappig is."

Heb je weleens spijt dat je niet verder bent gegaan in de wiskunde?

"Ik studeerde af bij Jan Hogendijk, op een scriptie over Pieter Wils' Wis-konstige Wercken. Hogendijk zei dat hij me nooit zou aannemen als aio, omdat hij vond dat een historisch wiskundige in de eerste plaats een wiskundige moest zijn. Dat was hard, maar ik onderschrijf zijn visie wel. Op dat soort momenten heb ik spijt dat ik niet wat meer die harde wiskunde heb gedaan. De wetenschap heeft toch mijn hart. Soms zou ik weer onderzoek willen doen. Ik fantaseer weleens over onopgeloste verhalen in de wiskunde. Bijvoorbeeld Ludolph van Ceulen die verschrikkelijk moeilijke vergelijkingen tot de negende graad op acht cijfers na de komma perfect uitrekende. Niemand weet hoe hij het deed. Dat is zó frustrerend. Misschien heeft hij daarover weleens gecorrepondeerd met François Viète en dan fantaseer ik hoe ik die brief in een Frans archief ontdek."

Al denk ik ook meteen: ik kan er er ook een liedje van maken. Over dat er altijd meer is dan mensen kunnen weten, omdat het toeval er altijd voor zorgt dat mensen die iets willen weten niet op de plek zijn waar die kennis is. En dat doe ik dan liever. Uiteindelijk ben ik toch gewoon een kunstenaar geworden."

Heeft u een goede suggestie voor een (Nederlandse) wiskundige met een bijzonder keerpunt in zijn of haar carrière? Stuur dan een e-mail naar i@ionica.nl.

Thomas de Jong

Faculteit Wiskunde & Informatica, Technische Universiteit Eindhoven

Afdeling Wiskunde, Vrije Universiteit Amsterdam

t.g.d.jong@tue.nl

Onderzoek

KAM-theorie en de stabiliteit van het zonnestelsel

Het stabiliteitsprobleem in de hemelmechanica van het zonnestelsel stelt de vraag of de planeten hun huidige regelmatige banen om de zon zullen voortzetten in de verre toekomst. Op een kleine storing na beschrijven de huidige planeetbanen Keplerse ellipsen. Deze storing zou ten gevolge van de interacties tussen de planeten kunnen groeien. Op de lange duur zou deze zelfs zo groot kunnen worden dat ze op onregelmatige wijze gaan bewegen. Hierdoor zouden planeten het zonnestelsel kunnen verlaten of onderling kunnen botsen. Bestaat er een onderliggende wiskundige theorie die de stabiliteit kan garanderen? Thomas de Jong beschouwt een sterk versimpeld model van het zonnestelsel en laat schetsmatig zien dat door toepassing van de theorie van Kolmogorov, Arnold en Moser (KAM-theorie) er condities gegeven kunnen worden voor de stabiliteit van de planeetbanen. Vervolgens bekijkt hij of ons zonnestelsel aan deze voorwaarden voldoet.

De formulering van het stabiliteitsprobleem gaat al terug naar de tijd van Newton. Sindsdien hebben vele grote wiskundigen, zoals Laplace, Lagrange en Poincaré, hun bijdrage geleverd. In de jaren zestig van de vorige eeuw begon Arnold met toepassing van de Kolmogorov–Arnold–Moser-theorie op een sterk versimpeld model van het zonnestelsel beschreven door de gravitatiewet van Newton [1]. Bewijzen voor uitbreidingen van dit model kwamen daarna van Robutel, Herman en Féjoz [8, 11, 16, 24], een ontwikkeling die in 2004 leidde tot de Arnold–Robutel–Herman–Féjoz-stelling. Dit artikel ligt in het verlengde en zal het bewijs van de Arnold–Robutel–Herman–Féjoz-stelling voor een algemeen wiskundig publiek weergeven.

Een model voor het zonnestelsel

De eerste redelijke benadering van planeetbanen werd gedaan door Kepler aan het begin van de zeventiende eeuw. Door een kromme te interpoleren door de empirische data van de Marsbaan concludeerde Kepler dat banen ellipsen zijn met de zon in een van de brandpunten. De Keplerse theorie, die kan worden

samengevat in een drietal wetten, geeft ook de bewegingen langs de ellipsen. Dit leidde tot meer accurate omlooptijden van de planeten om de zon. Toepassingen in die tijd waren bijvoorbeeld de verificatie van de Gregoriaanse schrikkeljaarconventie en de bepaling van de datum voor Pasen, welke berust op de stand van de aarde en de maan. Deze toepassingen formuleren al aspecten van het stabiliteitsprobleem als ze op grote tijdschalen worden bekeken. In de zeventiende eeuw formuleerde Newton de universele gravitatiewet, waarmee de bewegingsvergelijkingen voor het zonnestelsel konden worden opgesteld. Het hiermee verkregen mechanische model geeft een betere benadering dan die van Kepler aangezien de effecten van zwaartekracht worden meegenomen.

Voor de eenvoud beschouwen wij in dit artikel een zonnestelsel met twee planeten waarin de krachten tussen de hemellichamen worden gegeven door de universele gravitatiewet. Dit model bevat veel van de essentiële moeilijkheden. De planeten 1 en 2 hebben posities x_1 en x_2 in $\mathbb{R}^3$ met bijbehorende snelheden en versnellingen $\dot{x}_j$ en $\ddot{x}_j$ en

massa's m_j . Voor de zon wordt analoog het subscript 0 gebruikt en we nemen aan dat net zoals in ons zonnestelsel m_0 veel groter is dan die van de planeten. De bewegingsvergelijking voor planeet 1 wordt dan gegeven door

$$m_1 \ddot{x}_1 = G \frac{m_1 m_0}{|x_0 - x_1|^3} (x_0 - x_1) + G \frac{m_1 m_2}{|x_2 - x_1|^3} (x_2 - x_1). \quad (1)$$

Hierin is G de gravitatieconstante. Merk op dat vergelijking (1) een interactie expliciet maakt tussen planeet 1 en de twee andere hemellichamen, waar die met de zon met zijn grote massa m_0 in geval van ons zonnestelsel veruit dominant is. Dit leidt tot een klassiek storingsprobleem, want dit drielichamenprobleem is een benadering van de situatie waarbij de interactie tussen de beide planeten onderling is 'uitgeschakeld'. Zoals bekend leidt dit tot de vertrouwde Keplerse ellipsbewegingen, die worden verstoord zodra de planetaire interactie weer wordt 'ingeschakeld'. Omdat de sterkte hiervan relatief klein is, kan het effect op de beweging van het oorspronkelijke drielichamenprobleem goed in wiskundige termen worden beschreven. Grofweg krijgt het geheel hierdoor de structuur

$$\text{Gravitatie interactie zon met planeet} + \varepsilon \times \text{interactie met de andere planeten} \quad (2)$$

waarbij ε een kleine reële parameter is.

In het zonnestelsel zijn de benaderende Keplerse planeetbanen bijna cirkels die vrijwel in één vlak liggen. Dit leidt tot een verdere vereenvoudiging van het ongestoorde pro-

bleem zoals dat optreedt voor $\varepsilon = 0$, namelijk dat de planeten bijna uniforme cirkelbewegingen uitvoeren die in één vlak liggen. Men spreekt hier van bijna circulaire, co-planaire banen.

Het probleem van de kleine delers

Het meest fundamentele en historisch oudste dilemma over de stabiliteit van dit Newtoniaanse model is het probleem van de kleine delers. Wij onderbreken de bestudering van het model om de benodigde achtergrond te geven. In de eenvoudigste opzet kunnen wij een storingsprobleem van de vorm

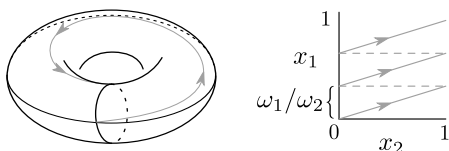
$$\dot{x} = \omega + \varepsilon f(x), \quad x \in \mathbb{T}^n := (\mathbb{R}/\mathbb{Z})^n \quad (3)$$

beschouwen, waarin x op een n -torus ligt waarop de oplossingen met frequenties ω_i in de frequentievector $\omega := (\omega_1, \omega_2, \dots, \omega_n)$ worden gestoord door $\varepsilon f(x)$ met ε weer een kleine reële parameter. Voor $\varepsilon = 0$ krijgen we het ongestoorde probleem met alleen 'lineaire' oplossingen op de n -torus gegeven door $t \mapsto x_0 + t\omega \pmod{\mathbb{Z}^n}$ met x_0 in $\mathbb{T}^n := \mathbb{R}^n/\mathbb{Z}^n$, zie Figuur 1. Deze 'lineaire' oplossingen delen we op in twee klassen op basis van de frequentievector: resonant en quasi-periodiek. De frequentievector ω is resonant als er gehele getallen $k_1, k_2, \dots, k_n$ bestaan, die niet allemaal nul zijn, zodanig dat

$$k_1\omega_1 + k_2\omega_2 + \dots + k_n\omega_n = 0 \quad (4)$$

en ω is quasi-periodiek als ω niet resonant is. Dit onderscheid wordt gemaakt vanwege de eigenschap dat voor een quasi-periodieke frequentievector elke 'lineaire' oplossing dicht in de n -torus $\mathbb{T}^n$ ligt; dit terwijl in het resonante geval elke oplossing periodiek is met dezelfde periode [2], zie Figuur 1.

Uit een wiskundige analyse [3, 5] van de oplossingen van (3) blijkt dat er storingsreeksen



Figuur 1 Beschouw het tweedimensionale geval, $n = 2$, met frequentievector $\omega = (\omega_1, \omega_2)$. Als de 2-torus wordt ontvouwen zoals in de rechter figuur dan zijn de oplossingen van het ongestoorde systeem 'lineair' met helling ω_1/ω_2 . Als ω resonant is, dan is ω_1/ω_2 een rationaal getal, en dan zijn de oplossingen periodiek. Als ω quasi-periodiek is, dan is ω_1/ω_2 een irrationeel getal, en dan liggen de oplossingen dicht op de torus.

van de vorm

$$\sum_{k \in \mathbb{Z}^n \setminus \{0\}} \frac{c_k}{k_1\omega_1 + k_2\omega_2 + \dots + k_n\omega_n} \cdot e^{2\pi i \langle k, x \rangle}, \quad x \in \mathbb{T}^n, \quad (5)$$

in (3) optreden. Indien deze convergeren, bestaat er een diffeomorfisme ϕ zodanig dat we in (3) de lineaire oplossingen terugkrijgen:

$$\dot{\tilde{x}} = \tilde{\omega} \quad \text{met} \quad \tilde{x} = \phi \circ x. \quad (6)$$

Voor generieke f zijn in (5) alle coëfficiënten c_k typisch ongelijk aan nul. Dat betekent dat voor formele existentie van deze reeks voor elke $k \in \mathbb{Z} \setminus \{0\}$ moet gelden dat $\langle \omega, k \rangle \neq 0$. Maar de vraag is of convergentie van (5) gegarandeerd is voor quasi-periodieke frequentievectoren. Voor specifieke quasi-periodieke frequentievectoren zou de deler van de termen in (5) arbitrair dicht bij nul kunnen komen, wat zou kunnen leiden tot divergentie van de som: het probleem van de kleine delers. Dit probleem gaat al terug naar het werk van Dirichlet en Weierstraß [18] maar het was Poincaré die de moeilijkheden voor het eerst vastlegde in [23].

In 1950–1960 werd de theorie ontwikkeld voor het omgaan met kleine delers. Deze theorie heet Kolmogorov–Arnold–Moser-theorie (KAM-theorie) en is vernoemd naar de drie belangrijkste bijdragers. Informeel gesproken, zegt KAM-theorie dat ω in (3) ver genoeg verwijderd moet zijn van resonante frequentievectoren. Merk op dat dit slim gedaan moet worden aangezien de resonante frequentievectoren dicht liggen in $\mathbb{R}^n$. Door de afstand tot de resonante frequentievectoren af te laten hangen van de mate van resonantie, verkrijgen wij de gewenste ω : de Diophantische frequentievectoren gegeven door

$$|\langle \omega, k \rangle| > \gamma |k|^{-\tau} \quad \text{voor alle } k \in \mathbb{Z}^n \setminus \{0\}, \text{ met } \tau, \gamma > 0. \quad (7)$$

De (τ, γ) zijn parameters van het probleem waarbij τ typisch vastligt op basis van de dimensie van de tori terwijl in het algemeen $\gamma = o(\varepsilon)$ als $\varepsilon \downarrow 0$, op een geschikte manier gespecificeerd [9]. Uit overwegingen als in [21] volgt dat de Diophantische frequentievectoren (7) voor $\tau > n - 1$ en $\gamma > 0$ een nergens dichte verzameling van positieve Lebesgue maat vormen. De informele KAM-stelling luidt dan dat in (3) het volgende geldt:

KAM-stelling. Voor voldoende kleine ε bestaat er een positieve maat van Diophantische frequentievectoren waarvoor de lineaire quasi-periodieke dynamica persisteert op de n -torus. Sterker nog, in de limiet $\varepsilon \downarrow 0$ gaan deze frequentievectoren naar volle maat.

Wij beëindigen hiermee onze discussie over KAM-theorie. Voor meer achtergrond zie [3–6, 9].

Toepassing KAM-theorie

Terugkerend naar ons drielichamenprobleem wordt in het algemeen de stabiliteit van het zonnestelsel opgevat als de existentie van een positieve Lebesgue-maat van oplossingen met quasi-periodiek gedrag. Dat zou betekenen dat, op een geschikte coördinatentransformatie na, in het drielichamenprobleem 'lokaal' een situatie als (3) ontstaat waarop KAM-theorie kan worden toegepast. De hiermee verkregen KAM-toepassing, de Arnold–Robutel–Herman–Féjoz-stelling (ARHF-stelling) voor twee planeten, ziet er als volgt uit [1, 8, 11, 24]:

ARHF-stelling. Voor voldoende kleine $\varepsilon > 0$ geldt dat in een voldoende kleine omgeving van de gestoorde circulaire, co-planaire Keplerse ellipsen, er oplossingen bestaan die invariante 5-tori bedekken die de faseruimte met volle maat vullen. Deze 5-tori reduceren tot 4-tori bedekt met quasi-periodieke oplossingen als de rotatie-invariantie van oplossingen om het totale impulsmoment van het zonnestelsel eruit wordt gedeeld. In de limiet $\varepsilon \downarrow 0$ convergeren de 5-tori naar 2-tori die samen volle maat hebben.

Waar de 5-, 4- en 2-tori vandaan komen zal later duidelijk worden. Voordat KAM-theorie kan worden toegepast, moeten we in de buurt van de circulaire, co-planaire Keplerse ellipsen via coördinatentransformaties een vergelijking als (3) ontwikkelen.

De bewegingsvergelijkingen voor het model In euclidische coördinaten heeft de bewegingsvergelijking voor een hemellichaam de vorm (1). Door de impulsvector te introduceren, $U_i = m_i \dot{x}_i$ ($i = 0, 1, 2$), kan het systeem als een eerste-orde gewone differentiaalvergelijking geschreven worden. De faseruimte wordt dan gegeven door

$$M := \{(x_0, x_1, x_2, U_0, U_1, U_2) \in \mathbb{R}^{18} : x_i, U_i \in \mathbb{R}^3\}. \quad (8)$$

Door translatie-invariantie en behoud van im-

puls te gebruiken, kunnen we de positie van de zon vastzetten, waarna de vergelijkingen voor de zon buiten beschouwing kunnen worden gelaten. In euclidische coördinaten heeft (1) echter niet de juiste vorm voor toepassing van KAM-theorie en het systeem kan ook niet zonder meer in de vorm (3) geschreven worden. Dit kan echter wel als we ons beperken tot een voldoende kleine omgeving van de ongestoorde Keplerse ellipsen. De faseruimte is dan

$$\mathcal{M} := \{(x, y, p, q) \in \mathbb{T}^2 \times Y \times Z \times Z \mid (x, y, p, q) \in \mathbb{T}^2 \times \mathbb{R}^2 \times \mathbb{R}^4 \times \mathbb{R}^4\}, \quad (9)$$

met $Z \subset \mathbb{R}^4$ een open omgeving van de oorsprong. Het storingsprobleem wordt dan gegeven door

$$\begin{aligned} \dot{x} &= \omega(y) + \varepsilon f_1(x, y, p, q), \\ \dot{y} &= 0 + \varepsilon f_2(x, y, p, q), \\ \begin{bmatrix} \dot{p} \\ \dot{q} \end{bmatrix} &= \begin{bmatrix} 0 & -\varepsilon \lambda(y) \\ \varepsilon \lambda(y) & 0 \end{bmatrix} \begin{bmatrix} p \\ q \end{bmatrix} + \varepsilon f_3(x, y, p, q). \end{aligned} \quad (10)$$

De frequentievector van dit systeem volgen uit de frequentieafbeelding $\mathcal{F}_\varepsilon : Y \subset \mathbb{R}^2 \rightarrow \mathbb{R}^6$ gegeven door

$$\mathcal{F}_\varepsilon : y \mapsto (\omega(y), \varepsilon \lambda(y)) = (\omega_1(y), \omega_2(y), \varepsilon \lambda_1(y), \varepsilon \lambda_2(y), \varepsilon \lambda_3(y), \varepsilon \lambda_4(y)). \quad (11)$$

Informeel gesproken, worden de coördinaten voor dit systeem verkregen door elke positievariabele in de euclidische ruimte te identificeren met een punt op een ellips. De x_i komen overeen met de frequenties over de ellipsen en de y_i zijn gerelateerd aan de halve lange assen van de ellipsen. De p_j, q_j zijn gerelateerd aan de excentriciteiten en inclinaties van de ellipsen. Voor $\varepsilon = 0$, het ongestoorde systeem, is er alleen interactie tussen de zon en de planeten afzonderlijk. De excentriciteiten en inclinaties zijn dan constant. De oplossingen van het systeem zijn dan de verwachte twee Keplerse ellipsen waarover de planeten bewegen met frequenties ω_1, ω_2 . Deze twee ellipsen geven aanleiding tot de 2-tori in de Arnold–Robutel–Herman–Féjóz-stelling.

In ons geval is de vergelijking (3) Hamiltoniaans, hetgeen betekent dat de variabelen in paren voorkomen, (x_i, y_i) en (p_i, q_i) . Een paar als (x_i, y_i) lijkt nog het meest op een stel poolcoördinaten met x_i als hoek en y_i als de bijbehorende poolstraal. In de 12-

dimensionale faseruimte $\mathcal{M}$, zie (9), zijn wij dus niet op zoek naar één torus, zoals in (3), maar naar een familie van tori die worden geparametriseerd door de poolstraal-variabelen y .

Het systeem (10) is nog geen goed gedefinieerd storingsprobleem, want de afbeelding $\varepsilon \lambda$ heeft dezelfde orde van grootte als de storingsterm εf_3 . Indien ω voldoende Diophantisch is, bestaat er een transformatie die op $O(\varepsilon^2)$ na overeenkomt met middeling over de x -variabelen. Onder middeling wordt de storing εf_3 van orde $\varepsilon O(\|p\|^2 + \|q\|^2)$. Dus voor een voldoende kleine omgeving van circulaire, co-planaire Keplerse ellipsen, oftewel p, q klein, krijgen we een storingsprobleem op de frequentieafbeelding $\mathcal{F}_\varepsilon$.

Rüssmann-niet-gedegenereerdheidsconditie

Zoals moge blijken uit de eerdere behandeling van (3) is het van belang te kijken in het frequentiedomein, dat wil zeggen in het beeld van de afbeelding $\mathcal{F}_\varepsilon : Y \rightarrow \mathbb{R}^6$. Aangezien $Y \subset \mathbb{R}^2$, kan dit beeld niet open zijn en zou het a priori kunnen dat alle beeldpunten in een resonantie-gat van de Diophantische frequentieverzameling vallen. In principe is hiervoor de Rüssmann-niet-gedegenereerdheidsconditie een uitgelezen wapen [4, 6, 9, 25]. Die zegt dat als het beeld van $\mathcal{F}_\varepsilon$ voldoende gekromd is dit in geen enkel resonantie-hypervlak kan liggen en zelfs een maattheoretisch kleine doorsnijding met de resonantie-gaten heeft, zie Figuur 2. De bijbehorende KAM-stelling zegt dan dat de waarden van $y \in Y$ met de KAM-tori ook een verzameling van positieve maat vormen.

De vraag is nu of de frequentieafbeelding $\mathcal{F}_\varepsilon$ Rüssmann-niet-gedegenereerd is. Dit blijkt niet zonder meer het geval te zijn.

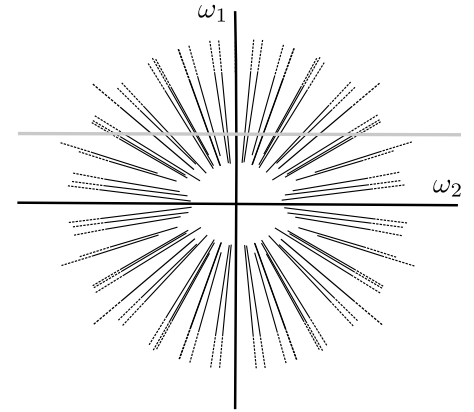
Resonanties

Door de frequentieafbeelding gaan twee resonante hypervlakken [8]:

$$\lambda_4 = 0, \quad \lambda_1 + \lambda_2 + \lambda_3 = 0. \quad (12)$$

De frequentieafbeelding is dus niet Rüssmann-niet-gedegenereerd en KAM-theorie kan nog niet worden toegepast.

Resonanties vernietigen het lineaire gedrag doordat er een interactie is tussen de variabelen die de resonantie bepalen. Echter, indien zelfs onder storing deze variabelen onafhankelijk van elkaar zijn, heeft dit geen gevolgen voor persistentie van de ongestoorde tori, bijvoorbeeld als de oplossingen van het gestoorde systeem een 2-torus met invariante



Figuur 2 Schets van de Diophantische frequenties in $\mathbb{R}^2$ die een verzameling van positieve maat vormen. Deze verzameling is een overaftelbare vereniging van gesloten halfrechten. Een kromme in deze frequentieruimte zou gemakkelijk in een resonantie-gat kunnen liggen, maar een kromme die transversaal op de halfrechten staat, de grijze lijn $\omega_1 = \text{constant}$, is Rüssmann-niet-gedegenereerd. In hogere dimensie zouden hogere afgeleiden van de kromme ook een rol spelen.

cirkels bedekken. Dan kan het systeem gereduceerd worden tot de studie van invariante cirkels en hoeft er geen rekening te worden gehouden met de resonantie die de symmetrie induceert.

Het zonnestelsel bevat nog drie behouden grootheden, $C = (C_1, C_2, C_3)$, die overeenkomen met het totale impulsmoment van het zonnestelsel op het gemeenschappelijk zwaartepunt, i.e., de som van de impulsmomentvectoren van alle hemellichamen in $\mathbb{R}^3$. Als dit impulsmoment in twee richtingen wordt vastgezet, bijvoorbeeld $C = (0, 0, C_3)$, dan ligt het resonante hypervlak ten gevolge van $\lambda_4 = 0$ niet in de verkregen faseruimte [8]. We kunnen dan alleen in één richting het impulsmoment variëren met C_3 . Als vervolgens C_3 constant wordt genomen, dan zijn de oplossingen rotatie-invariant om de bijbehorende as en kan deze $\mathbb{S}^1$ -symmetrie om het gemeenschappelijk zwaartepunt eruit worden gedeeld. Deze laatste reductie geeft een faseruimte zonder de resonantie door $\lambda_1 + \lambda_2 + \lambda_3 = 0$. Dit levert een 8-dimensionaal systeem waarop KAM-theorie kan worden toegepast. Wij krijgen dan een positieve maat van quasi-periodieke oplossingen op 4-tori. De voorgaande argumentatie is onafhankelijk van de keuze van het impulsmoment maar doordat de $\mathbb{S}^1$ -symmetrie eruit is gedeeld zullen de 4-tori in de volledige faseruimte op 5-tori liggen. Dit voltooit de schets van het bewijs voor de Arnold–Robutel–Herman–Féjóz-stelling.

Opmerkingen.

- Arnold beweerde dat het ruimtelijke probleem kan worden gezien als een storing

op het planaire probleem [1]. Dit bleek niet waar te zijn, want zelfs na reducties bevat het systeem variabelen ten gevolge van de inclinaties [8, 24].

- De reducties door gebruik van de eerste integralen C_1, C_2, C_3 komen overeen met de klassieke Jacobi-eliminatie van de knoop in de zin van de hemelmechanica [7, 13].
- In het bewijs van Robutel wordt zonder naar de frequentieafbeelding te kijken de klassieke Jacobi-eliminatie van de knoop uitgevoerd. Hoewel $\lambda_4 = 0$ al bewezen was door Arnold [1], miste hij hiermee de resonantie door $\lambda_1 + \lambda_2 + \lambda_3 = 0$, die als eerste werd ontdekt door Herman [11].
- De oplossingen op de invariante 5-tori liggen niet op invariante 4-tori die de 5-tori volledig bedekken [14].
- Het Newtoniaanse model neemt niet alle effecten mee die een rol spelen bij de beweging van de hemellichamen. De bewegingen ten gevolge van onder andere de getijden, relativiteitstheorie en massaverlies van de zon over de tijd zouden meegenomen moeten worden voor een accurater model.

Stabiliteit van het zonnestelsel

De ARHF-stelling voor twee planeten kan direct uitgebreid worden naar n planeten [8]. Voor het toepassen van dit KAM-

stabiliteitsresultaat op het echte zonnestelsel hebben we een kwantitatieve theorie nodig die een bovengrens geeft op ε en de afwijking tot circulaire co-planaire banen. Werk van Hénon in het planaire geval suggereert dat voor de massa van onze zon (10^{30} kg) de massa's van de planeten kleiner dan die van een elektron moeten zijn om KAM-theorie toe te kunnen passen [10]. De afwijking tot circulaire co-planaire banen wordt gemeten in inclinaties en excentriciteiten. Er bestaan realistische bovengrenzen voor de inclinaties [24], terwijl bovengrenzen op de excentriciteiten nog absurd kleine waardes moeten aannemen.

KAM-theorie eist dat over een oneindig lang tijdsinterval de planeten stabiel moeten blijven, terwijl in de werkelijkheid dit alleen hoeft te gelden voor de leeftijd van de zon. De KAM-gerelateerde Nehorošev-stelling zegt dat oplossingen dichtbij KAM-tori, dichtbij de tori blijven over een tijdsinterval afhankelijk van de storingsgrootte [19]. Voor een zonnestelsel met twee planeten kunnen de planeten dan massa's van orde 10^6 kg hebben [20]. Dit is nog steeds niet dichtbij de werkelijke massa's, aangezien de zwaarste planeet een massa van orde 10^{27} kg heeft.

Het is maar de vraag of KAM-theorie en gerelateerde theorieën behulpzaam kunnen zijn voor het aantonen van de stabili-

teit van het zonnestelsel. Zeer veel orbitale frequenties zitten dicht in de buurt van 'lage orde'-resonanties, bijvoorbeeld Jupiter-Saturnus ($2\omega_{\text{Jupiter}} - 5\omega_{\text{Saturnus}} \approx 0$), Mars-Aarde ($2\omega_{\text{Mars}} - \omega_{\text{Aarde}} \approx 0$). Dit geeft aan dat zelfs als de planeetbanen Diophantische frequenties hebben, de storing zeer klein moet zijn.

Numerieke wiskunde heeft meer succes in stabiliteitsonderzoek. Recent werk suggereert dat in de beweging van de buitenplaneten (Jupiter, Saturnus, Uranus, Neptunus) weinig zal veranderen terwijl de binnenplaneten (Mercurius, Venus, Aarde, Mars) zich onregelmatig zouden kunnen gedragen over een tijdspanne van miljoenen jaren, met als gevolg dat planeten over miljarden jaren het zonnestelsel zouden kunnen verlaten [15, 17]. Daarmee blijft het stabiliteitsprobleem van het zonnestelsel, althans voor de komende miljoenen jaren, meer een wetenschappelijk dan een praktisch probleem. $\leftarrow$

Dankwoord

Ik wil graag professor Henk Broer, professor Jacques Féjoz, dr. Heinz Hanßmann, professor Barry Koren, professor Ferdinand Verhulst en de CASA groep (TU Eindhoven) bedanken voor de discussies en opmerkingen gedurende het schrijven van dit artikel.

Referenties

- 1 V.I. Arnold, Small denominators and problems of stability of motion in classical and celestial mechanics, *Russ. Math. Surv.* 18 (1963), 85–193.
- 2 V.I. Arnold en A. Avez, *Ergodic Problems of Classical Mechanics*, Addison-Wesley, 1979.
- 3 H.W. Broer, G.B. Huitema en M.B. Sevryuk, *Quasi-Periodic Motions in Families of Dynamical Systems*, Springer, 2002.
- 4 H.W. Broer, G.B. Huitema en F. Takens, Unfoldings of quasi-periodic tori, *Mem. Amer. Math. Soc.* 83(421) (1990), 1–82.
- 5 H.W. Broer en F. Takens, *Dynamical Systems and Chaos*, Epsilon Uitgaven, 2009.
- 6 H.W. Broer, H. Hanßmann en F.O.O. Wagener, *Quasi-Periodic Bifurcation Theory*, Springer, 2013.
- 7 A. Deprit, Elimination of the nodes in problems of n bodies, *Celestial Mechanics and Dynamical Astronomy* 30 (1983), 181–195.
- 8 J. Féjoz, Démonstration du théorème d'Arnold sur la stabilité du système planétaire (d'après M. Herman), <http://www.ceremade.dauphine.fr/~fejoz/Articles/arnold.pdf>, herziene versie van het artikel in *Michael Herman Memorial Issue, Ergodic Theory Dyn. Sys.* 24(5) (2004), 1521–1582.
- 9 H. Hanßmann, Non-degeneracy conditions in KAM theory, *Indagationes Mathematicae* 22(3-4) (2011), 241–256.
- 10 M. Hénon, Exploration numérique du problème restreint IV. Masses égales orbites non périodiques, *Bull. Astronom.* 31(1-2) (1966), 49–66.
- 11 M.R. Herman, Démonstration du théorème de V.I. Arnold, Séminaire de systèmes dynamiques, 1998.
- 12 G. Holton en S.G. Brush, *Physics, the Human Adventure: From Copernicus to Einstein and Beyond*, Rutgers University Press, 2004.
- 13 C.G.J. Jacobi, Sur l'élimination des noeuds dans le problème des trois corps, *Astronomische Nachrichten*, Bd XX (1842), 81–102.
- 14 T.G. de Jong, Stability of planetary motions in a model of the solar system with two planets: A note on the Arnold–Robutel–Herman–Féjoz theorem, www.win.tue.nl/~tjong/index.html, Masterscriptie Rijksuniversiteit Groningen, 2012.
- 15 J. Laskar, The chaotic motion of the solar system, a numerical estimate of the size of the chaotic zones, *Icarus* 88 (1990), 266–291.
- 16 J. Laskar en P. Robutel, Stability of the planetary three-body problem, I. Expansion of the planetary Hamiltonian, *Celestial Mech. Dynam. Astronom.* 62 (1995), 193–217.
- 17 S. Marmi, Chaotic behaviour in the solar system (following J. Laskar), Séminaire Bourbaki, Exp. 854, 1998/99.
- 18 J. Moser, *Stable and Random Motions in Dynamical Systems*, Princeton Landmarks, 1973.
- 19 N.N. Nehorošev, An exponential estimate of the time of stability of nearly integrable Hamiltonian systems II, *Trudy Sem. Petrovsk.* 5 (1979), 5–50.
- 20 L. Niederman, Stability over exponentially long times in the planetary problems, *Nonlinearity* 9 (1996), 1703–1751.
- 21 J.C. Oxtoby, *Measure and Category*, Springer, 1971.
- 22 J.H. Poincaré, Mémoire sur les courbes définies par une équation différentielle, *J. de mathématiques*, 3e série, 7 (1881), 375–422, 8 (1882), 251–296, *Annalen* 19 (1882), 553–564.
- 23 J.H. Poincaré, *Les méthodes nouvelles de la mécanique céleste*, 3 vols., Gauthier-Villars, Paris, 1892, 1893, 1899.
- 24 P. Robutel, Stability of the planetary three-body problem, II. KAM theory and existence of quasiperiodic motions, *Celestial Mech. Dynam. Astronom.* 62 (1995), 219–261.
- 25 H. Rüssmann, Invariant tori in non-degenerate nearly integrable Hamiltonian systems, *Regular Chaotic Dynamics* 6 (2001), 119–204.

Ferdinand Verhulst*Mathematisch instituut**Universiteit Utrecht**f.verhulst@uu.nl***Overzichtsartikel**

Chaos, uitgedoofde hype of gevestigde wetenschap?

Dit voorjaar werd Ferdinand Verhulst benaderd door Martin van Kalmthout, redacteur wetenschap van *De Volkskrant*, met de vraag hoe het toch stond met de chaostheorie. Dat was 25 jaar geleden een hype en nu hoor je er niets meer over. Was het achteraf allemaal niet zo belangrijk? Er volgde een interview, ook telefoongesprekken met andere wiskundigen. Op 22 juni 2013 resulteerde dit in een enthousiast artikel in *De Volkskrant* over de chaostheorie in de huidige wetenschap. Verhulst geeft hier een nadere reflectie over deze zaken.

In de jaren tachtig ontstond rond chaos een hype waarbij veel populaire artikelen in kranten, lezingen en mogelijke toepassingen een rol speelden. De wetenschappelijke discussie speelde zich de eerste jaren af in de wiskunde, de meteorologie en de sterrenkunde. De belangstelling van natuurkundigen kwam wat later (dat wiskundigen en anderen iets fundamenteel nieuws in de klassieke mechanica

zouden produceren: te gek om los te lopen). Het begon in de toepassingen met de berekeningen voor opstijgende lucht in de atmosfeer door Edward Lorenz (1963) en voor de dynamica van melkwegstelsels door Hénon en Heiles (1964). Een verband tussen die drie vakgebieden werd toen door bijna niemand gezien. De numerieke berekeningen verbijsterden de wetenschappers tot men ontdekte dat Henri Poincaré deze chaotische dynamica al gedetailleerd had beschreven aan het eind van de negentiende eeuw. Die bewustwording was het begin van fundamenteel werk, een voortzetting van Poincarés theorie (eindelijk!) en vele toepassingen. Belangrijke resultaten van de wiskundigen Kolmogorov, Arnold, Moser en Smale in de zestiger en zeventiger jaren werden in dit verband geplaatst en kregen grote bekendheid in de wetenschap.

Hoe kan het dat een wereldomvattende hype in de jaren tachtig zo om zich heen greep, terwijl het nu lijkt of het onderwerp bij het grote publiek min of meer vergeten is? Andy Warhol 'voorspelde' in de jaren zeventig dat iedereen in de toekomst vijftien minuten wereldberoemd zou kunnen zijn. Dat kunnen we nu beter modifieren tot: niemand kan heden langer dan vijftien minuten beroemd zijn en

iets kan niet langer dan vijftien minuten de publieke aandacht gevangen houden.

Voor wetenschappers die in de bestendigheid van hun vakgebied geloven, is dat een ontvullende constatering. Echter, voor wiskundigen zou het optreden van zo'n hype en het daarna wegvallen van de aandacht een leerzaam verschijnsel moeten zijn. In het verleden waren we gewend aan voldoende geld voor onderzoek, nu moeten we nog steeds kwaliteit leveren maar tegelijk surfen op de golven van de publieke belangstelling. Wie dat niet kan, maakt weinig kans op onderzoeksgelden. Wiskundigen zijn hier meestal nog niet aan gewend. In Duitsland was Heinz-Otto Peitgen

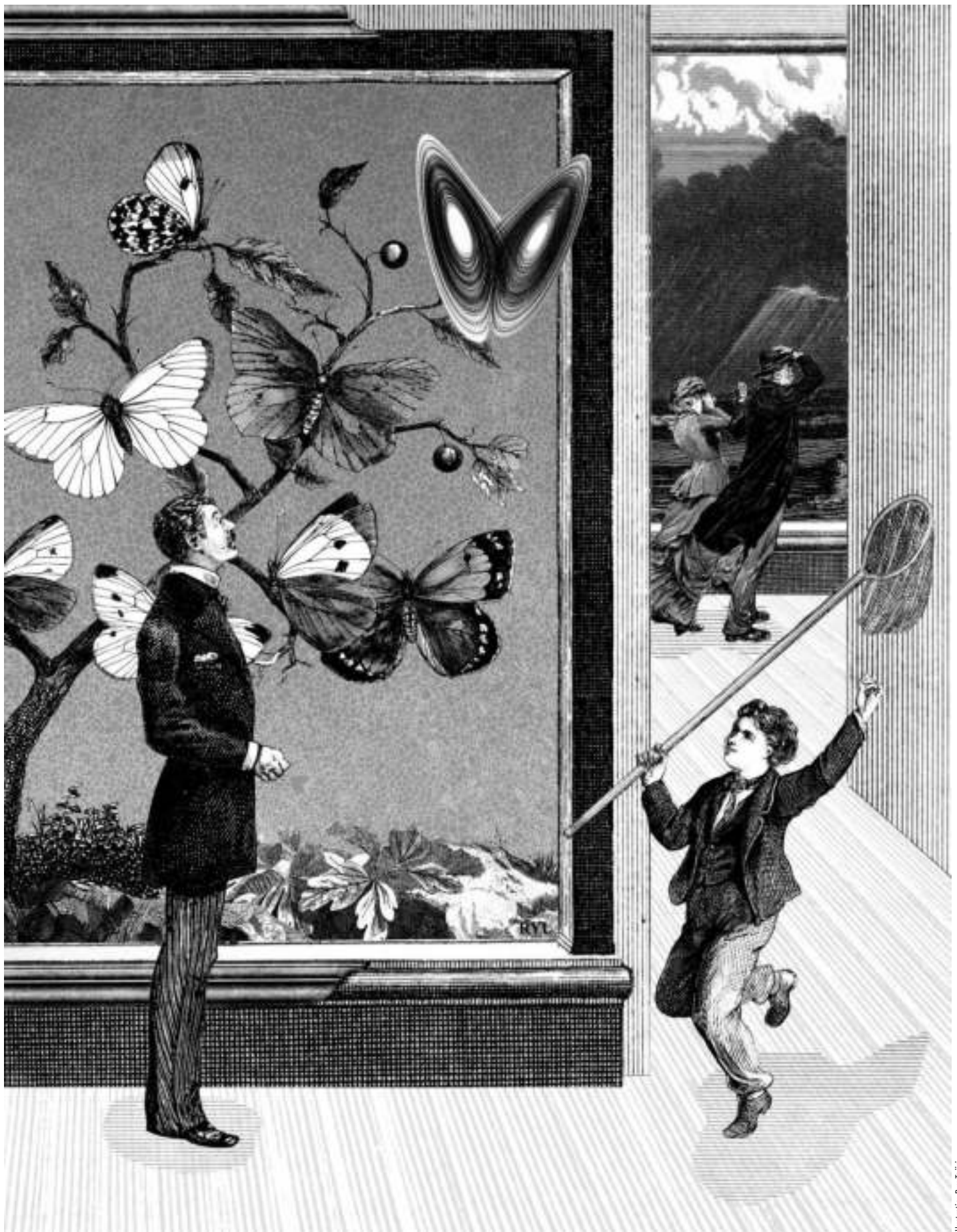


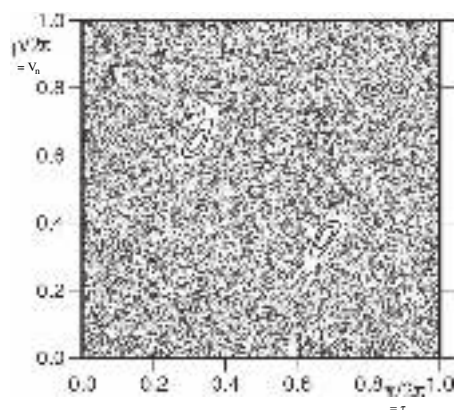
Foto: Kim Moser

Jürgen Moser



Vladimir Arnold





Figuur 1 Dit is een afbeelding die ontstaat is uit een model voor een stuitende bal (zie bijvoorbeeld [5]). De puntenwolk is ontstaan uit één beginvoorwaarde.

een belangrijk vertolker en propagandist van de nieuwe theorie van dynamische systemen. Dat kwam hem op bijtende en nogal onredelijke kritiek in het blad van de Duitse vereniging van wiskundigen (DMV) te staan.

Wat is chaos?

Bekijk eens een dynamisch systeem, bijvoorbeeld een dynamica beschreven door een differentiaalvergelijking, een differentie-vergelijking of afbeelding. Neem aan dat alle ontwikkelingen in het systeem (evoluties) begrensd zijn; denk aan voorbeelden als een door de lucht vliegende bal of de grootte van een populatie op een eiland. Zo'n dynamisch systeem heeft vaak een of meer instabiele toestanden, een balletje op de top van een heuvel, een potlood op zijn punt, enzovoorts. De ontwikkeling van het systeem in de tijd zal dan meestal in de richting van een stabiele toestand gaan. In een chaotisch systeem gebeurt er wat anders. Zo een systeem is namelijk bezaaid met instabiele toestanden, in elke omgeving van een toestandspunt zijn instabiele toestanden, er bestaat helemaal geen stabiele toestand terwijl de evoluties toch begrensd zijn. Als er oneindig veel instabiele toestanden zijn in een begrensd gebied, is het resultaat een dynamica die in hoge mate onvoorspelbaar is. De ontwikkeling kan zich nergens in een stabiele omgeving vestigen, de beweging blijft allerlei kanten op schieten. In Figuur 1 is een puntenwolk te zien die het resultaat is van de iteratie van een afbeelding waarbij één begintoestand gebruikt is.

Bij de toepassingen waren het in het begin meestal ik-ook-artikelen, dat wil zeggen beschrijvingen van chaotische effecten die nu opeens in chemische processen, mechanische modellen en allerlei andere problemen herkend werden. Een moeilijkheid is dat chaotisch gedrag wiskundig zeer gecompliceerd

is en diepgaande kennis van dynamische systemen vereist. Veel toepassingen in de jaren tachtig beperkten zich daarom tot numerieke berekeningen. Er ontstond soms een wat haastige wetenschap. Zo werd er nogal slordig omgesprongen met het begrip dimensie: Hausdorff-dimensie werd klakkeloos verward met limietcapaciteit, sommige auteurs bestonden het om te beweren dat het niet veel uitmaakte welk dimensiebegrip men gebruikte. Ondertussen ging het fundamentele onderzoek aan chaos met grote stappen verder, zodat er nu kan worden gesproken van een volwassen maar nog niet afgeronde chaostheorie. Er zijn daarbij in allerlei vakgebieden toepassingen die goed begrepen worden.

Een bijzonder mooie inleiding in de wetkunde van chaos is het boek van Peitgen, Jürgens en Saupe [4]. Een uitvoerige populaire inleiding is [1].

Een revolutie in de wetenschap?

Beoefenaars van de geschiedenis en de grondslagen van de wetenschap hanteren het begrip 'revolutie in de wetenschap'. Kenmerkend voor zo'n revolutie is het optreden van een crisis in een deel van de wetenschap, gevolgd door een doorbraak in het denken, een kennis-discontinuïteit ('epistemic rupture' [3]), die een geheel nieuwe kijk op het vak levert met allerlei consequenties, vaak ook maatschappelijke. Een bekend voorbeeld is de klassieke mechanica van Newton en anderen, die niet blijkt te gelden bij hoge relatieve snelheden. Dat leidde tot de relativiteitstheorie met een wezenlijk andere visie op het begrip tijd en beweging. De maatschappelijke gevolgen zijn kernenergie, de atoombom en filosofische discussies; ook kunstenaars hebben zich hier door laten inspireren.

Een beschrijving van wetenschappelijke revoluties is gegeven in het bekende boek van Kuhn [2]. Merkwaardig genoeg worden in dit boek geen wiskundige ontdekkingen als wetenschappelijke revoluties herkend, het boek beperkt zich in zijn voorbeelden vooral tot natuur- en scheikunde. Het ligt voor de hand om bijvoorbeeld de axiomatisering van de meetkunde, de opkomst van de algebra en het ontstaan van de functionaalanalyse als wetenschappelijke revoluties te zien. Die axiomatisering van de meetkunde bijvoorbeeld heeft eeuwenlang via de euclidische meetkunde mede de vorming van het denken in het onderwijs bepaald.

Conceptueel betekent het verschijnsel chaos een revolutie in de wetenschap en in ons denken. Het gaat namelijk om onvoorspelbaarheid in deterministische dynamische

systemen waarbij we de wetten die het systeem regeren per definitie precies kennen. Verschijnselen als gekoppelde slingers, het zonnestelsel, zijn misschien wiskundig lastig te beschrijven, maar de evolutie van zulke systemen is volkomen gedetermineerd door de gegeven natuurwetten. Niemand, behalve Poincaré, had aan de mogelijkheid gedacht dat het gedetermineerd vastleggen van de toekomst onvoorspelbare verschijnselen zou kunnen opleveren. Inderdaad, chaos. Dat juist ook de klassieke mechanica deze verschijnselen herbergt was een grote verrassing.

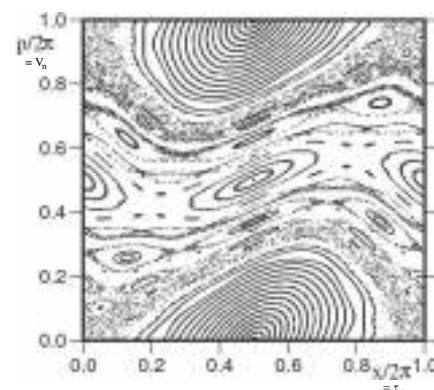
Het concept chaos is een duidelijk voorbeeld van een revolutie in het wetenschappelijk denken door de geheel nieuwe kijk die het op bepaalde wiskundige en natuurwetenschappelijke processen levert. Het heeft maatschappelijke aspecten omdat allerlei onvoorspelbaarheden in het weer en de economie hier deels een verklaring vinden.

Huidig onderzoek in theorie en toepassingen

Het onderwerp chaos is een vast bestanddeel geworden van boeken en cursussen over dynamische systemen, mathematische biologie en mechanica. We noemen enkele tijdschriften die geheel of gedeeltelijk aan het onderwerp gewijd zijn:

- *Chaos* (American Institute of Physics);
- *International Journal of Bifurcation and Chaos*;
- Het onderwerp komt verder veelvuldig voor in de tijdschriften *Nonlinearity*, *Physica D*, *Journal of Sound and Vibration*, *Nonlinear Dynamics*, *Journal of Nonlinear Science* en andere.

Chaos is dan wel een gevestigd onderdeel geworden van de dynamische systeemtheorie, maar in de theorie is het 'laaghangend fruit' nu wel geplukt, zodat er vooral veel moeilij-



Figuur 2 Dit is ook een afbeelding die ontstaat is uit een model voor een stuitende bal, zoals in Figuur 1, echter met andere fysische parameters. Er is nog steeds chaos, maar minder prominent.

ke problemen over zijn. Bijvoorbeeld de vraag hoe prominent chaos in een systeem is. Chaos is er niet altijd en overal (zie Figuur 2). In zeer veel toepassingen wordt zowel energie toegevoerd als energie afgestaan, in het algemeen kun je dan chaos verwachten. Hoe dat uitpakt in een concreet geval kun je alleen door gedetailleerd onderzoek achterhalen. Voor het zonnestelsel blijkt chaos pas over miljarden jaren een rol te spelen (gelukkig maar). Ook zijn er in het zonnestelsel gebieden waar de chaotische verschijnselen verwaarloosbaar zijn. In de aardatmosfeer speelt het elke dag een rol, hetgeen beperkingen oplegt aan de weersvoorspelling. De invloed van chaos op oceaanstromingen en economie is nog weinig bekend.

In de theorie van dynamische systemen zijn een aantal scenario's ontwikkeld die tot chaotisch gedrag leiden, maar bij een toepassing moet je dan nog langdurig aan het werk om te zien of zo'n scenario geïdentificeerd kan worden in het model dat bestudeerd wordt.

In het algemeen kun je zeggen dat in systemen die onder controle zijn, denk aan een wasmachine of een brugconstructie, chaos kan en moet worden vermeden. Zo zijn er

mensen die denken dat door gebrek aan onderhoud duizenden bruggen in de Verenigde Staten op instorten staan. Dit is geen chaosprobleem, maar wel een dynamisch systeemprobleem (en natuurlijk een groot politiek probleem). In veel ingenieursproblemen loop je dus om chaostheorie heen, je vermijdt zulke verschijnselen zoveel mogelijk, maar het negeren van chaostheorie in ingenieurswerk is niet altijd terecht. Bij geheel nieuwe ontwerpen kunnen onverwacht chaosproblemen optreden, denk aan een nieuw ontwerp van een grote brug waarbij een wisselend windveld zich kan laten gelden of een stormvloedkering in sterk wisselende getijdestroming.

Chaos is niet te vermijden in systemen waar je weinig controle over hebt: het weer, gravitatie-theorie, astrofysica, economie. Het laatste is een relatief verwaarloosd gebied, er wordt wel gecontroleerd (economische en monetaire maatregelen), maar vaak zonder goede resultaten. Het ontbreekt hier, met name in crisistijd waar bifurcaties een rol zullen spelen, aan een redelijk samenhangende theorie.

Tijdelijke hype of nieuwe wetenschap?

Chaos-theorie is ongetwijfeld een integraal en

belangrijk onderdeel van de theorie van dynamische systemen geworden. Het is het nieuwste voorbeeld van een wetenschappelijke revolutie in en door de wiskunde doordat we zijn gaan inzien dat er een grens is aan de voorspelbaarheid in een aantal systemen die we toch goed dachten te begrijpen, bijvoorbeeld het zonnestelsel of de beweging van vloeistoffen.

Verhelderend is de vergelijking met een andere kortlopende hype, de catastrofetheorie van Christopher Zeeman in de jaren zeventig. Zeeman beging de fout om allerlei toepassingen te melden zoals gevangenisoproer en territoriumdrift bij dieren. De catastrofe- of singulariteitentheorie doet echter geen voorspellingen, deze bevat geen dynamica. Het geeft wel een idee van mogelijke uitkomsten van dynamische processen. Singulariteitentheorie is een gevestigd onderdeel van de theorie van dynamische systemen, maar geen wetenschappelijke revolutie. Het is jammer dat Zeeman met het noemen van mogelijke toepassingen een verkeerde indruk heeft gewekt.

Chaos-theorie is van blijvend belang voor het begrip van voorspelbaarheid van dynamische processen. 

Referenties

- 1 Henk Broer, Jan van de Craats en Ferdinand Verhulst, *Chaos-theorie, het einde van de voorspelbaarheid?*, Epsilon-reeks, deel 35, Epsilon Uitgaven, 3de druk, 2008.
- 2 Thomas S. Kuhn, *The Structure of Scientific Revolutions*, International Encyclopedia of Unified Science, The University of Chicago Press, 1962 (6de druk 1975).
- 3 Ladislav Kvasz, *Pattern of Change, Linguistic Innovations in the Development of Classical Mechanics*, Birkhäuser, 2008.
- 4 H.-O. Peitgen, H. Jürgens en D. Saupe, *Chaos and Fractals, New Frontiers of Science*, Springer, 2004.
- 5 Ferdinand Verhulst, *Chaos en Orde*, Zebra-reeks, deel 16, Epsilon Uitgaven, 2de druk, 2007.

Jaap Top

Johann Bernoulli Instituut voor Wiskunde en Informatica
Rijksuniversiteit Groningen
j.top@rug.nl

Vakantiecursus

Het vermoeden van Birch en Swinnerton-Dyer

Op de Vakantiecursus 2013 van het Platform Wiskunde Nederland besprak Jaap Top een van de zeven millenniumproblemen: het vermoeden van Birch en Swinnerton-Dyer. Welke vooruitgang is er geboekt sinds dit probleem uit de getaltheorie vijftig jaar geleden werd geformuleerd?

Precies vijftig jaar geleden, in 1963, publiceerden Bryan Birch en Peter Swinnerton-Dyer in het *Journal für die reine und angewandte Mathematik* het eerste gedeelte [1] van hun artikel 'Notes on Elliptic Curves'. De tweede helft [2] verscheen in 1965 in hetzelfde tijdschrift. In de artikelen doen beide wiskundigen uit Cambridge (Engeland) verslag van hun jarenlange onderzoek betreffende elliptische krommen over de rationale getallen $\mathbb{Q}$. Daarbij was een voor hun tijd nieuw middel ingezet: de EDSAC 2 [16], een computer die de universiteit van Cambridge in 1958 had aangeschaft en die tot 1965 dienst deed.

Een (over)versimpelde versie van de vraag die Birch en Swinnerton-Dyer probeerden te beantwoorden is de volgende. Begin met een polynoom

$$F(x) := ax^3 + bx^2 + cx + d,$$

waarbij $a \neq 0$ en b, c, d rationale getallen zijn. Bestaan er rationale getallen r zodat $F(r)$ een kwadraat is (dat wil zeggen, $F(r) = s^2$ voor zeker rationaal getal s). En zo ja, zijn er eindig veel, of zelfs oneindig veel zulke r ?

Fermat (1601–1665) en ook Euler (1707–1783) hadden al een methode aangegeven waarmee uit een oplossing $x = r$ in veel gevallen een andere oplossing gevonden kon worden. We komen hier straks op terug. Op p. 171 van een artikel [11] van Henri Poincaré (1854–1912) staat een uitspraak die in feite

betekent dat uit een eindig aantal oplossingen $x = r_1, x = r_2, \dots, x = r_q$ door herhaald toepassen van methoden als die van Fermat en Euler, alle oplossingen geconstrueerd kunnen worden. Poincaré verzuimt echter een bewijs of zelfs maar een schets van een argumentatie bij zijn uitspraak te geven. L.J. Mordell (1888–1972) toonde overigens in 1922 aan dat de uitspraak van Poincaré correct was, zie [10].

Wiskundig gezien is het nieuwe idee van Birch en Swinnerton-Dyer vooral dat ze het polynoom $F(x)$ modulo zoveel mogelijk priemgetallen p gaan bekijken. Voor zo'n priemgetal p kan je tellen hoeveel verschillende $r \bmod p$ er zijn met de eigenschap dat $F(r) \equiv s^2 \bmod p$ voor een zekere gehele s . Een heel naïeve en niet erg precieze vorm van het vermoeden van Birch en Swinnerton-Dyer, helemaal in de stijl van de inleiding van hun eerste artikel, luidt dan:

Als er voor de meeste priemgetallen p onverwacht veel verschillende $r \bmod p$ bestaan waarvoor $F(r) \bmod p$ een kwadraat modulo p is, dan neemt $F(x)$ voor oneindig veel rationale waarden $x = r$ een kwadraat als waarde aan.

De verdienste van de twee artikelen van Birch en Swinnerton-Dyer is dat dit is omgesmeed tot een precieze formulering, waarvoor ze bovendien een enorme numerieke eviden-

tie gegeven hebben. In de afgelopen vijftig jaar is flink wat vooruitgang geboekt, maar het vermoeden is nog altijd niet bewezen. In het jaar 2000 werd het vermoeden gekozen als een van de problemen in de beroemde Claylijst. Andrew Wiles schreef voor die gelegenheid een korte en heel leesbare introductie [15].

In de voor u liggende tekst gaan we vooral niet proberen de meest algemene en precieze formulering te geven. Wel hopen we wat handvatten te leveren waarmee u zelf kan rekenen aan en experimenteren met speciale gevallen van het vermoeden, en we geven een kort overzicht van tot nu toe behaalde resultaten.

Constructies van Fermat en Euler

Gegeven zijn rationale getallen a, b, c, d met $a \neq 0$, en de bijbehorende derdegraads veelterm

$$F(x) := ax^3 + bx^2 + cx + d.$$

Een methode waarmee zowel Fermat als Euler in diverse voorbeelden indrukwekkende rationale getallen r (met tellers en noemers die te groot zijn voor een moderne standaard grafische rekenmachine) vonden, zodat $F(r)$ een kwadraat is, werkt als volgt. We gaan ervan uit dat al zo'n oplossing $x = r$ gevonden is en we zoeken een nieuwe. Daartoe schrijven we $x = \xi + r$, zodat de gegeven oplossing correspondeert met $\xi = 0$. Als veelterm in ξ hebben we dan

$$\tilde{F}(\xi) = F(\xi + r) = a\xi^3 + \tilde{b}\xi^2 + \tilde{c}\xi + \tilde{d},$$

met rationale getallen $a \neq 0$ (dezelfde

waarmee we begonnen) en $\tilde{b}, \tilde{c}, \tilde{d}$. Merk op dat

$$\tilde{d} = \tilde{F}(0) = F(r),$$

en daarvan is gegeven dat het een kwadraat is. Dus we kunnen schrijven $\tilde{d} = e^2$ voor een zeker rationaal getal e . Dit zorgt ervoor, dat we een uit het wat ouderwetse middelbaar onderwijs beproefde rekentechniek kunnen toepassen: 'kwadraat afsplitsen'. In dit geval houdt dit in dat rationale getallen α, β gezocht worden zodat geldt

$$\tilde{F}(\xi) = (\alpha\xi^2 + \beta\xi + e)^2 + \gamma\xi^3 + \delta\xi^4$$

voor zekere rationale γ, δ . Door de coëfficiënten van de machten van ξ te vergelijken, zien we dat moet gelden

$$\begin{cases} 2\beta e = \tilde{c}, \\ 2\alpha e + \beta^2 = \tilde{b}. \end{cases}$$

Dit levert precies één oplossing (β, α) , behalve in het speciale geval dat $e = 0$ geldt. Dat laatste komt overeen met de voorwaarde dat we waren begonnen met een nulpunt $x = r$ van de veelterm $F(x)$. Gaan we er vanuit dat r geen nulpunt is, dan hebben we nu een schrijfwijze

$$\tilde{F}(\xi) = (\alpha\xi^2 + \beta\xi + e)^2 + \gamma\xi^3 + \delta\xi^4$$

gevonden. Hoe helpt dit alles bij het vinden van een $r' \neq r$ zodat $F(r')$ een kwadraat is, of equivalent, een $r'' \neq 0$ zodat $\tilde{F}(r'')$ een kwadraat is? Wel, in de gevonden uitdrukking voor $\tilde{F}(\xi)$ is de eerste term zonder meer een kwadraat, wat ook voor ξ wordt ingevuld. Dus we hebben een voorbeeld als de resterende termen samen de waarde 0 opleveren. Het resterende stuk laat zich schrijven als

$$\xi^3(\gamma + \delta\xi).$$

Voor $\xi = 0$ levert dit de waarde 0, maar deze ξ hadden we al. Een andere waarde voor ξ die werkt, is te vinden in het geval dat $\delta \neq 0$.

Een voorbeeld: begin met

$$F(x) := x^3 + 2x + 1.$$

Deze is te schrijven als

$$F(x) = \left(-\frac{1}{2}x^2 + x + 1\right)^2 + 2x^3 - \frac{1}{4}x^4.$$

Omdat $2x^3 - \frac{1}{4}x^4$ als nulpunt $x = 8$ heeft,

geldt $F(8)$ is een kwadraat. Verder is

$$\begin{aligned} F(x+8) &= x^3 + 24x^2 + 194x + 529 \\ &= \left(-\frac{3287}{24334}x^2 - \frac{97}{23}x - 23\right)^2 \\ &\quad - \frac{38998}{279841}x^3 - \frac{10804369}{592143556}x^4. \end{aligned}$$

Een nulpunt van

$$-\frac{38998}{279841}x^3 - \frac{10804369}{592143556}x^4$$

is

$$x = -\frac{82519768}{10804369}$$

en door hier 8 bij op te tellen, volgt dat $F\left(\frac{3915184}{10804369}\right)$ een kwadraat is. Bij zowel Fermat als Euler komen aanzienlijk omvangrijkere rekenvoorbeelden voor...

Als $\delta = 0$, dan levert de methode geen nieuwe waarde r' zodat $F(r')$ een kwadraat is. Nagaande hoe de $\delta, \gamma, \beta, \alpha$ bepaald worden, blijkt dat $\delta = 0$ equivalent is met $\alpha = 0$, oftewel dat was begonnen met een veelterm

$$\tilde{F}(\xi) = \alpha\xi^3 + \tilde{b}\xi^2 + \tilde{c}\xi + \tilde{d} = \gamma\xi^3 + (\beta\xi + s)^2.$$

Een meer analytische beschrijving van wat hier gebeurt, werkt dan als volgt. De vraag is waarden voor ξ te vinden zodat $\tilde{F}(\xi)$ een kwadraat is, oftewel zodat $\sqrt{\tilde{F}(\xi)}$ bestaat, en rationaal is. De functie

$$\xi \mapsto \alpha\xi^2 + \beta\xi + s$$

die hierboven bepaald wordt, is precies de tweede-orde-Taylorbenadering bij $\xi = 0$ van $\pm\sqrt{\tilde{F}(\xi)}$ (met teken $+$ als $s > 0$ en teken $-$ als $s < 0$). En deze tweede-orde-benadering voldoet aan $\alpha = 0$ (oftewel, heeft slechts graad ≤ 1), precies dan als de functie

$$\xi \mapsto \sqrt{\tilde{F}(\xi)}$$

voor $\xi = 0$ een buigpunt heeft.

Ook als $\delta \neq 0$ kan er iets misgaan: namelijk, we zoeken naar een nulpunt van $\gamma + \delta\xi$, en dat is natuurlijk $\xi = -\gamma/\delta$. Dat zou de nieuwe waarde voor ξ moeten zijn zodat $\tilde{F}(\xi)$ een kwadraat is. Echter, als $\gamma = 0$ dan geeft dit gewoon weer de al bekende waarde $\xi = 0$.

Terugvertaald naar $F(x)$: gegeven een rationaal getal r zodat $F(r)$ een kwadraat is. Dan levert de door Fermat en Euler gebruikte methode een ander rationaal getal $r' \neq r$ waar

voor eveneens geldt $F(r')$ is een kwadraat, behalve in drie gevallen:

- $F(r) = 0$;
- voor $x = r$ heeft $\sqrt{F(x)}$ een buigpunt;
- de methode levert dezelfde r weer op omdat " $\gamma = 0$ ".

Het bovenstaande laat zich vrij eenvoudig vertalen in de moderne manier waarop 'elliptische krommen' behandeld worden. Daartoe eerst heel kort iets over de theorie. Een goed leesbare, elementaire inleiding in dit fascinerende onderwerp is het boek van Joe Silverman en John Tate [12]. Allereerst eisen we van de veelterm $F(x)$ dat deze geen meervoudige nulpunten heeft, dus $F(x)$ is niet te schrijven in de vorm $a(x-\lambda)^2(x-\mu)$ of zelfs $a(x-\lambda)^3$ (was dat wel het geval, dan is het oorspronkelijk gestelde probleem heel simpel op te lossen, en er zijn dan in alle gevallen oneindig veel verschillende rationale waarden $x = r$ waarvoor $F(r)$ een kwadraat is). Voldoet $F(x)$ aan de bovengenoemde eis, definieer dan een 'elliptische kromme' als de collectie van alle paren (x, y) die voldoen aan

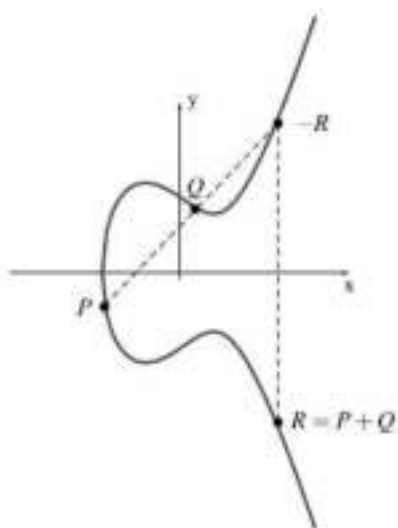
$$y^2 = F(x).$$

Hier voegt men nog een extra punt aan toe dat O genoemd wordt. Dat is niet een van de paren (x, y) , maar een nieuw punt, waaraan gedacht mag worden als een oneindig ver van de oorsprong verwijderd punt. De aanname dat $F(x)$ geen meervoudige nulpunten heeft, betekent dat in elk punt (α, β) van de kromme een unieke raaklijn aan de kromme is gedefinieerd, namelijk de lijn met vergelijking

$$2\beta(y - \beta) = F'(\alpha)(x - \alpha).$$

Op de collectie van alle punten op de kromme laat zich dan als volgt een optelling definiëren:

1. $P + O = P$.
2. $P + Q = O$ als P en Q elkaars gespiegelde zijn ten opzichte van de x -as.
3. Als $P \neq Q$ en P en Q zijn niet elkaars gespiegelde ten opzichte van de x -as, dan snijdt de verbindingslijn van P en Q de kromme in drie punten (het derde punt kan samenvallen met P of met Q in het geval dat de verbindingslijn een raaklijn is). Nu geldt $P + Q = R$ waarbij R de gespiegelde in de x -as is van het derde gevonden punt.
4. Als $P = Q$ en dit punt ligt niet op de x -as (in dat geval was de optelling al in punt 2 hiervoor gedefinieerd), neem dan de raaklijn door P aan de kromme en het derde snijpunt van die raaklijn met de kromme. Dan geldt $P + P = R$ waarbij R de gespie-



Figuur 1

gelde in de x -as is van het derde snijpunt. Zie Figuur 1.

De zo gegeven optelling blijkt aan de gebruikelijke regels te voldoen, dus bijvoorbeeld geldt $(P + Q) + R = P + (Q + R)$ voor elk drietal P, Q, R , en elk punt P heeft een unieke tegengestelde Q (namelijk de gespiegelde in de x -as) zodat $P + Q = O$. Die tegengestelde wordt als $-P$ geschreven. Pas op: we zijn misschien een beetje gewend om bij $-(x, y)$ beide coördinaten van het punt van teken te veranderen, maar voor de hier gegeven regel geldt $-(x, y) = (x, -y)$. Tenslotte geldt per definitie dat de gemaakte optelling commutatief is: er geldt $P + Q = Q + P$ voor elk paar punten P, Q .

Als begonnen wordt met punten P, Q die beide coördinaten rationaal hebben, dan geldt hetzelfde voor $P + Q$ en voor $-P$ (voor zover die $\neq O$ is). Dus samen met O is de collectie van al zulke punten gesloten onder de bewerkingen optellen en tegengestelde nemen. Deze collectie wordt in de artikelen van Birch en Swinnerton-Dyer met de letter Γ aangeduid.

In termen van de optelling blijkt de constructiemethode van Fermat en van Euler het volgende te doen: gegeven een punt $P \in \Gamma$ wordt het 'nieuwe' punt

$$R := -3P = -(P + P + P)$$

bepaald. Als begonnen wordt met een P op de x -as, dan is $P + P = O$, en dus $R = P$. Die hadden we al. En als begonnen was met een buigpunt van de grafiek van $\sqrt{F(x)}$, dan geldt $R = O$, dus ook hier krijgen we geen 'echte' oplossing. Het derde geval waar geen nieuwe oplossing gekregen wordt is nu ook eenvoudig te verklaren: als geldt $4P = O$, dan

is $R = P$, dus dan levert de methode hetzelfde punt op waarmee was begonnen. In termen van de gebruikte variabelen, gebeurt dit als $y = 0$, dus als geldt

$$\begin{aligned}\tilde{F}(\xi) &= (\alpha\xi^2 + \beta\xi + e)^2 - \alpha^2\xi^4 \\ &= 2\alpha\beta\xi^3 + (2\alpha e + \beta^2)\xi^2 + 2\beta e\xi + e^2.\end{aligned}$$

Deze veelterm heeft graad 3 en geen meervoudige nulpunten als aan de drie eisen

$$\begin{cases} \alpha \neq 0, \\ e \neq 0, \\ \beta^2 \neq 8\alpha e. \end{cases}$$

is voldaan. In dat geval voldoet $P = (0, e)$ aan $4P = O$ op de kromme gegeven door $y^2 = \tilde{F}(\xi)$.

Nog een voorbeeld: begin met

$$F(x) := x^3 + 9x^2 - 16x + 64.$$

Beginnend met $x = 0$ levert de methode van Fermat en Euler dan achtereenvolgend (reken maar na!) de waarden $x = 8$ en $x = -8$ op, gevolgd door (opnieuw) $x = 0$, enzovoort. Dus we krijgen een periodieke baan, met periode 3. Het punt $P = (0, 8)$ op de kromme met vergelijking $y^2 = x^3 + 9x^2 - 16x + 64$ blijkt in dit geval te voldoen aan $7P = O$.

Ten slotte: de methode zoals hier beschreven houdt zoals we zagen nauw verband met de tweede-orde-Taylorbenadering van de functie $\sqrt{\tilde{F}(\xi)}$ om $\xi = 0$. Maar we hadden ook kunnen volstaan met de eerste-orde-Taylorbenadering! Dat levert een schrijfwijze

$$\tilde{F}(\xi) = (\beta\xi + e)^2 + \alpha\xi^3 + \epsilon\xi^2.$$

Door ξ zo te kiezen dat $\alpha\xi^3 + \epsilon\xi^2$ de waarde 0 krijgt, wordt weer een oplossing verkregen. In termen van de gegeven optelling betekent dit, dat uitgaande van een punt P op de kromme, het nieuwe punt

$$R' = -2P = -(P + P)$$

wordt geconstrueerd. Oftewel: neem het derde snijpunt met de kromme van de raaklijn door P aan de kromme. Deze 'raaklijnmethode' staat in veel teksten over elliptische krommen vermeld, maar de 'paraboolmethode' die door Fermat en Euler veel vaker wordt toegepast, lijkt wat in de vergetelheid geraakt.

Modulorekenen

Het probleem van kwadraten als waarden

$F(x)$ bij een rationale x te vinden, verandert niet als x met een vast rationaal getal $\neq 0$ wordt vermenigvuldigd, en evenmin als $F(x)$ met een vast kwadraat wordt vermenigvuldigd. Door $F(x) = ax^3 + bx^2 + cx + d$ te vermenigvuldigen met a^2 en vervolgens x te vervangen door $X = ax$, mogen we dus aannemen

$$F(X) = X^3 + bX^2 + cX + d$$

voor zekere (misschien nieuwe) rationale b, c, d . Vermenigvuldigen we dit met n^6 en schrijven we $x := n^2X$ (een nieuwe variabele x), dan staat er

$$x^3 + n^2bx^2 + n^4cx + n^6d.$$

Voor een geschikte keuze van n is dit een veelterm die alle coëfficiënten geheel heeft. Kortom, zonder verlies van algemeenheid kan worden aangenomen dat

$$F(x) = x^3 + bx^2 + cx + d$$

voor zekere gehele getallen b, c, d . Dit stelt ons in staat de veelterm te reduceren modulo ieder geheel getal, in het bijzonder modulo priemgetallen.

Daartoe eerst kort iets over het rekenen modulo een priemgetal. Kies een willekeurig priemgetal p . De 'getallen modulo p ' zijn de uitdrukkingen $\bar{a} = a \bmod p$ waarin a een geheel getal is. Hierbij geldt de regel

$$\bar{a} = \bar{b} \Leftrightarrow p \text{ is een deler van } b - a.$$

Anders gezegd: $\bar{a}$ hangt alleen maar af van de rest die overblijft wanneer a door p gedeeld wordt, niet van het gehele getal a zelf. Er zijn dus in totaal precies p 'getallen modulo p ', namelijk

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

Met 'getallen modulo p ' valt net zo te rekenen als met gewone gehele getallen:

$$\overline{a+b} := \overline{a+b}$$

en

$$\overline{a \cdot b} := \overline{a \cdot b}$$

blijken goed-gedefinieerde bewerkingen op te leveren.

Tot nu toe is niet gebruikt dat p wordt verondersteld een priemgetal te zijn. Die eigenschap levert iets speciaals voor de vermenig-

Een groot probleem bij het vermoeden in het algemene geval was het uitbreiden van de functie $L(s)$. Dankzij ouder werk van Martin Eichler (1912–1992) en Goro Shimura (geboren in 1930) was dat echter geen probleem voor de ‘modulaire elliptische krommen over $\mathbb{Q}$ ’. Onderzoek in de jaren tachtig ging daarom met name uit van de voorwaarde dat de elliptische kromme over $\mathbb{Q}$ die beschouwd werd, ‘modulair’ was. In 1986 publiceerden Dick Gross en Don Zagier een resultaat [7] over zogeheten ‘Heegner punten’ op modulaire elliptische krommen. Ze lieten zien dat zo’n punt P oneindig veel verschillende veelvouden nP heeft, precies dan als $L(1) = 0$ en $L'(1) \neq 0$. En dus

$$\begin{aligned} L(1) = 0 \text{ en } L'(1) \neq 0 \\ \Rightarrow \Gamma \text{ heeft oneindig veel elementen} \end{aligned}$$

voor modulaire elliptische krommen. Kort daarop completeerde de Russische wiskundige Victor Kolyvagin [9] dit werk van Gross en Zagier met de twee stellingen

$$L(1) \neq 0 \Rightarrow \Gamma \text{ is eindig}$$

en ook

$$L(1) = 0 \text{ en } L'(1) \neq 0 \Rightarrow \Gamma \text{ heeft rang 1.}$$

Ook hier onder de aanname dat het om modulaire elliptische krommen over $\mathbb{Q}$ gaat.

In 1998 (de publicatie volgde in 2001) vulden Christophe Breuil, Brian Conrad, Fred Diamond en Richard Taylor [3] het werk dat een paar jaar eerder was begonnen door Andrew Wiles [13,14]: het resultaat is, dat *elke* elliptische kromme over $\mathbb{Q}$ ‘modulair’ is. Daarmee gelden dus de stellingen van Gross en Za-

gier, en die van Kolyvagin, voor alle elliptische krommen over $\mathbb{Q}$. Toch is hiermee het originele vermoeden van Birch en Swinnerton-Dyer nog zeker niet bewezen. De Amerikaan Chris Skinner geeft de afgelopen maanden (zomer 2013) voordrachten over de omkering van Kolyvagin’s stellingen: als Γ eindig is, of rang 1 heeft, hoe zou je dan kunnen aantonen dat $L(1) \neq 0$ respectievelijk $L'(1) \neq 0$? Skinner heeft ideeën hoe je dit wellicht kan aanpakken. En zodra $L(s)$ in $s = 1$ een nulpunt heeft met multipliciteit minstens 2, dan is uit de tot nu toe bewezen stellingen nog niet te concluderen of Γ oneindig is. Ook omgekeerd, bevat Γ oneindig veel elementen, dan volgt dat $L(s)$ in $s = 1$ een nulpunt heeft, maar over de multipliciteit ervan valt nog niks te concluderen. Kortom, het laatste woord over het vermoeden van Birch en Swinnerton-Dyer is nog zeker niet gezegd! $\leftarrow$

Referenties

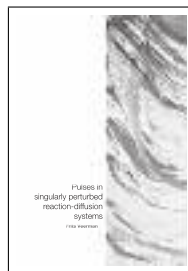
- 1 B.J. Birch en H.P.F. Swinnerton-Dyer, Notes on elliptic curves. I, *J. reine angew. Math.* 212 (1963), 7–25.
- 2 B.J. Birch en H.P.F. Swinnerton-Dyer, Notes on elliptic curves. II, *J. reine angew. Math.* 218 (1965), 79–108.
- 3 C. Breuil, B. Conrad, F. Diamond en R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* 14 (2001), 843–939.
- 4 J. Coates en A. Wiles, On the Conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* 39 (1977), 223–252.
- 5 K. Conrad, Partial Euler products on the critical line, *Canad. J. Math.* 57 (2005), 267–297.
- 6 D. Goldfeld, Sur les produits eulériens attachés aux courbes elliptiques, *C.R.Acad. Sci. Paris Sér. I Math.* 294 (1982), 471–474.
- 7 B.H. Gross en D.B. Zagier, Heegner points and derivatives of L-series, *Invent. Math.* 84 (1986), 225–320.
- 8 H. Hasse, Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F.K. Schmidtschen Kongruenzetafunktionen in gewissen elliptischen Fällen, *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen* (1933), 253–262.
- 9 V.A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and $\mathbb{W}(E, \mathbb{Q})$ for a subclass of Weil curves (Russisch), *Izv. Akad. Nauk SSSR Ser. Mat.* 52 (1988), 522–540, 670–671; Engelse vertaling in *Math. USSR-Izv.* 32 (1989), 523–541.
- 10 L.J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, *Proc. Cambridge Phil. Soc.* 21 (1922), 179–192.
- 11 H. Poincaré, Sur les propriétés arithmétiques des courbes algébriques, *J. de math. pures et appl. 5e série* 7 (1901), 161–234.
- 12 J.H. Silverman en J.T. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer, New York, 1992.
- 13 R. Taylor en A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* 141 (1995), 553–572.
- 14 A. Wiles, Modular elliptic curves and Fermat’s last theorem, *Ann. of Math.* 141 (1995), 443–551.
- 15 A. Wiles, The Birch and Swinnerton-Dyer Conjecture, www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/birchswin.pdf, 2000.
- 16 M.V. Wilkes, Edsac 2, *IEEE Annals of the History of Computing* 14 (1992), 49–56.

In de verdediging

| In defence

*Pas gepromoveerden brengen hun werk onder de aandacht.
Heeft u tips voor deze rubriek of bent u zelf pas gepromoveerd?
Laat het weten aan onze redacteur.*

Redacteur: Geertje Hek
la Voie-du-Coin 7
1218 Grand-Saconnex
Zwitserland
verdediging@nieuwarchief.nl



Pulses in singularly perturbed reaction-diffusion systems

Frits Veerman

Op 25 september 2013 promoveerde Frits Veerman aan de Universiteit Leiden. Vlak na de verdediging van zijn proefschrift *Pulses in singularly perturbed reaction-diffusion systems* blikte hij terug op de afgelopen vier jaren. Die terugblik was vooral positief: hij heeft nooit echt vastgezeten met zijn onderzoek en de samenwerking met zijn begeleiders prof.dr. Arjen Doelman en dr. Vivi Rottschäfer was stimulerend en vruchtbaar. Hij noemt het zelfs hun verdienste dat zijn promotietijd zo soepel verliep. En niet alleen wiskundig-inhoudelijk ging het goed; hij denkt ook met veel plezier terug aan de tijd die hij doorbracht met zijn mede-aio's, vooral aan de keren dat ze samen op stap waren in het kader van conferenties of winter- of zomerscholen.

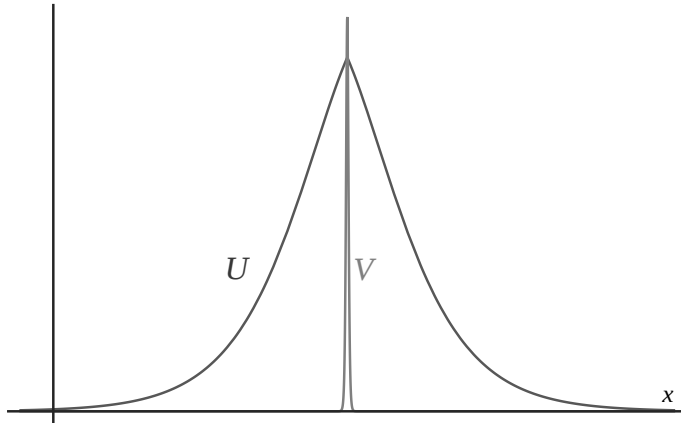
En plotseling ben je wiskunde aan het doen

Hoewel Veerman het voldoen aan de stellingen-eis van de Universiteit Leiden vooral als een procedurele kwestie heeft opgevat, is er toch een stelling die eruit springt: "Het feit dat toegepaste wiskunde de mogelijkheid biedt haar onderzoek op een toegankelijke manier uit te leggen, schept de verplichting dit ook te doen." Deze stelling sluit naadloos aan bij de introductie en samenvatting bij zijn proefschrift, waarin Veerman buitengewoon goed zijn best heeft gedaan om zijn werk aan een breder publiek uit te leggen. Voordat hij de titel van zijn proefschrift stap voor stap verklaart, besteedt hij zelfs aandacht aan de manier waarop wiskunde bedreven en beschreven wordt met behulp van symbolen en formules. "Als je symbolen en formules begint te gebruiken, en gaandeweg ervaren wordt in het lezen ervan, zul je merken dat de symbolen (en de ideeën die ze symboliseren) tastbaarder worden. Je krijgt meer en meer het gevoel waar het symbool eigenlijk voor staat, hoe het zich gedraagt, hoe het reageert op andere symbolen, wat het doet. Vervolgens kun je de symbolen heen en weer gaan schuiven, ze manipuleren, en ondertussen nieuwe symbolen introduceren omdat dat de handigste manier is om weer te geven wat je wil zeggen, en plotseling ben je wiskunde aan het doen."

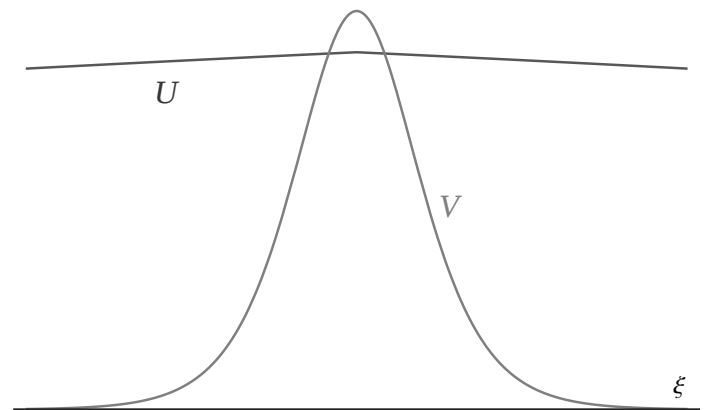
Pulsen als patronen

Binnen het onderzoeksgebied 'patroonvorming in natuurlijke systemen' worden (ruimtelijke) patronen onderzocht die kunnen ontstaan in modellen uit diverse natuurwetenschappen. Een pulsoplossing van zo'n model stelt een heel eenvoudig 'patroon' voor: bijvoorbeeld één hobbel en verder niks, of in twee dimensies één vlek op een dierenhuid, of één oase in de woestijn. Veermans onderzoek was gericht op de constructie en het gedrag van dergelijke pulsoplossingen in reactie-diffusiesystemen.

De reactie-diffusiesystemen waarin hij pulsoplossingen onderzocht vormen een klasse gekoppelde partiële differentiaalvergelijkingen. Veerman heeft zich beperkt tot twee gekoppelde vergelijkingen met een eendimensionale ruimtevariabele x , maar heeft de vorm van de



De U - en V -componenten van een typische één-pulsoplossing van (1) met $0 < \varepsilon \leq 1$. Het singuliere karakter van (1) leidt tot een zeer gelokaliseerde en steile puls voor V .



Een zoom van de linkerfiguur rond de puls in V . Het is duidelijk te zien dat de U -component nauwelijks varieert ten opzichte van de herschaalde ruimtelijke coördinaat $\xi = x/\varepsilon$.

vergelijkingen verder zo algemeen mogelijk gehouden. Dat is meteen een eerste bijzonder aspect aan zijn onderzoek: daar waar soortge-lijk onderzoek tot nu toe bijna uitsluitend gedaan werd in de context van een vooraf gekozen (canoniek) modelprobleem, heeft Veerman laten zien dat het bestaan en het gedrag van pulsoplossingen expliciet kan worden geanalyseerd voor een grote algemene klasse reactie-diffusievergelijkingen van de vorm

$$\begin{cases} U_t = U_{xx} - [\mu U - \nu_1 F_1(U; \varepsilon)] + \frac{\nu_2}{\varepsilon} F_2(U, V; \varepsilon), \\ V_t = \varepsilon^2 V_{xx} - V + G(U, V; \varepsilon). \end{cases} \quad (1)$$

Hierin is ε een (asymptotisch) kleine parameter, stellen de subscripts afgeleiden naar t en x voor en zijn F_i en G vrij algemene niet-lineaire termen. Het onderzoek van Veerman richtte zich op puls-vormige oplossingen $(U(x, t), V(x, t))$ van deze vergelijkingen en hun afhankelijkheid van de parameters μ en ν_i .

Algemene analyse met onverwachte resultaten

Niet alleen heeft Veerman laten zien dat expliciete analyse van pulsoplossingen in een heel algemene klasse vergelijkingen mogelijk is, er bleek bovendien dat deze algemene klasse systemen een veel diversere verzameling pulsoplossingen toestaat dan de tot nu toe bestudeerde modelproblemen. Na de existentie-analyse is lineaire en niet-lineaire stabiliteitsanalyse een natuurlijke volgende stap: stabiele oplossingen kunnen 'in het echt' worden waargenomen en bifurcaties waarin een stabiele puls instabiel wordt, geven aanleiding tot (interessante) dynamica. Ook hierbij heeft Veerman laten zien dat zelfs een kleine uitbreiding van een canoniek model (het Gierer–Meinhardt-model) grote invloed heeft: pulsen gaan meteen heel ander, nieuw gedrag vertonen.

Singuliere verstoringen

Een eerste belangrijke eigenschap van (1) is dat de kleine parameter ε zich op een 'handige' plaats bevindt, waardoor de systemen *singulier verstoord* zijn. In tegenstelling tot reguliere verstoringen, kunnen (kleine) singuliere verstoringen in het model een grote invloed hebben op de grootheden die door het model worden beschreven. In het bijzonder verdwijnt in Veermans vergelijkingen de (cruciale) diffusie-term $\varepsilon^2 V_{xx}$ in de limiet $\varepsilon = 0$. Bovendien vraagt de vergelijking

voor U om een herschaalde ruimtelijke variabele $\xi = x/\varepsilon$ om nog zinvol te zijn in diezelfde limiet (en reduceert de vergelijking dan tot $U_{\xi\xi} = 0$).

De niet-lineaire termen koppelen de vergelijkingen voor U en V zodat deze variabelen elkaar wederzijds beïnvloeden. Veerman legt enkele eisen op aan F_i en G , die ervoor zorgen dat er in de singuliere limiet $\varepsilon = 0$ sprake is van een familie van pulsoplossingen.

Vanwege deze eigenschappen kan de zogenaamde 'geometrische singuliere perturbatietheorie', een collectie technieken uit de theorie van dynamische systemen, worden gebruikt om het bestaan van pulsoplossingen in de algemene klasse systemen (1) te bewijzen. Het 'geometrische' zit hem hierbij in het definiëren van meetkundige objecten, zoals gladde variëteiten of hypervlakken. Het al dan niet snijden van deze objecten ligt aan de basis van de existentie- en stabiliteitsbewijzen. Op deze manier krijgt asymptotische analyse een stevige basis.

De onderzoeker kan er vaak zijn voordeel mee doen, dat belangrijke termen uit de vergelijkingen verdwijnen voor $\varepsilon = 0$. Veerman ziet dit als een soort compromis: in de singuliere limiet $\varepsilon = 0$ wordt het opeens mogelijk om vergelijkingen op te lossen omdat het aanvankelijk complexe systeem behoorlijk is versimpeld. Aan de andere kant is er ook een hoop informatie weggegooid en is het vaak onduidelijk hoe resultaten die behaald zijn in de singuliere limiet kunnen worden vertaald naar het geval dat ε niet nul is, maar wel heel klein.

In Veermans geval was de asymptotisch kleine parameter ε cruciaal. Zonder de structuur die deze parameter met zich mee bracht had hij het grootste deel van de analyse niet kunnen doen. Met behulp van deze parameter bleek het echter zelfs in de vrij complexe, algemene niet-lineaire gekoppelde systemen van de vorm (1) mogelijk om nauwkeurige uitspraken te doen over de existentie en de stabiliteit (en daarmee het tijdsafhankelijke gedrag) van een puls.

Verder in een toegepaste omgeving

Inmiddels is Veerman met een Rubicon-subsidie naar Oxford gegaan, om daar als postdoc twee jaar lang onderzoek te doen naar patronen op groeiende domeinen. Nog steeds onderzoek naar patroonvorming dus, maar nu in een meer biologische context. Hij hoopt dat hij zich daarbij niet alleen wiskundig verder kan ontwikkelen, maar dat zijn ervaring met niet-lineaire analyse ook tot nieuwe inzichten voor de biologen kan leiden.



Marco Swaen

Korteweg-de Vries Instituut voor Wiskunde
Universiteit van Amsterdam
m.d.g.swaen@uva.nl

Boekbespreking Dirk van Dalen: Intuitionistische Analyse

Het vinden van ε -dekpunten

Dirk van Dalen, emeritus hoogleraar logica en wijsbegeerte van de wiskunde aan de Universiteit Utrecht, geeft in zijn boek een snelle rondleiding door de intuitionistische wiskunde, waarbij hij voor een aantal concrete gevallen een constructieve behandeling geeft. Marco Swaen bespreekt het boek en gaat nader in op de dekpuntstelling van Brouwer.

Dat je geen topoloog of grondslagenspecialist hoeft te zijn om wel eens gehoord te hebben van L.E.J. Brouwer, is in belangrijke mate te danken aan Dirk van Dalen, die de afgelopen decennia met een reeks publicaties en heruitgaven de belangstelling voor deze markante Nederlandse wiskundige heeft gevoed. Spil in die reeks is de biografie *Mystic, Geometer, and Intuitionist*, die ons op meeslepende manier een inkijk geeft in het leven en de denkwereld van Brouwer [2]. Met *Intuitionistische Analyse* uit 2011 biedt Van Dalen het wiskundig enigszins geschoolde publiek toegang tot Brouwers reconstructie van de analyse naar intuitionistisch inzicht. Het boek, verschenen in de Epsilonreeks, bedient de geïnteresseerde lezer voor wie het servet van een wetenschapsbijlage inmiddels te klein is, maar het tafellaken van de stevige handboeken op dit gebied nog te groot. Bij het tafellaken moeten we dan in de eerste plaats denken aan het tweedelige *Constructivism* van Anne Troelstra, waarvan Van Dalen de co-auteur is [4].

Intuitionistische wiskunde

Is Brouwers verdienste in de topologie onomstreden, over het belang van zijn werk op het gebied van de grondslagen zijn de meningen nog steeds verdeeld. Brouwer formuleerde een standpunt over het wezen van de wiskunde waar men in de filosofie moeilijk omheen kan. Maar zijn intuitionisme

behelsde meer dan filosofie, het was een oproep de wiskunde van onbetrouwbare principes te zuiveren en op een nieuwe leest te schoeien, en die oproep heeft maar weinig weerklank gevonden. Weliswaar hebben enkelen zijn intuitionistische hervormingsprogramma opgepakt, zodat men inmiddels in de vakliteratuur kan nagaan hoe bijvoorbeeld intuitionistische topologie of groepentheorie eruit ziet, maar de meeste activiteit rond intuitionistische wiskunde is sinds de jaren zestig metamathematisch van aard, waarbij fragmenten van de intuitionistische wiskunde middels deductiesystemen en modellen ingebed worden in klassiek wiskundige systemen.

Een intuitionistisch leerboek

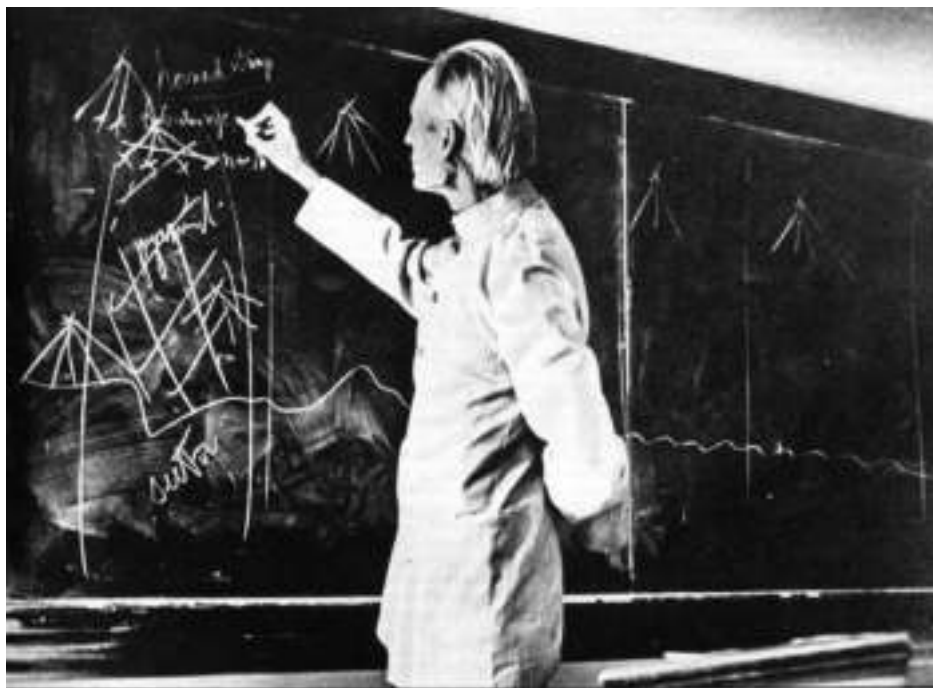
Voor Brouwer is wiskunde mentale activiteit van het individu, van het *creatieve subject*. De wiskundige objecten bestaan alleen als gedachtenconstructies in de individuele denkwereld, ontspruitend aan ingeboren oerintuïties. Taal en logica zijn slechts hulpmiddelen om die gedachten te ordenen en over te brengen op anderen. De verwoording van wiskundige inzichten mag nooit de plaats innemen van die inzichten zelf.

In deze filosofie blijft het collectieve karakter van wiskundige kennis onderbelicht. Het creatieve subject staat ver van de wiskundige in levenden lijve die zich als beginner noties met vallen en opstaan eigen maakt, die vergissingen begaat en vaak pas in

contact met anderen tot dieper inzicht komt. Concurrerende filosofieën als het platonisme en het formalisme weten met dit aspect beter raad. Het platonisme dicht wiskundige noties een objectief bestaan toe buiten het denkende individu, waarmee het verklaarbaar wordt dat de ene persoon een bepaalde notie beter begrijpt dan de andere. Het formalisme op zijn beurt biedt de wiskundige een gemeenschappelijk afgesproken systeem dat wiskundige waarheid controleerbaar maakt. intuitionistische wiskunde is krachtens haar eigen filosofie geen objectieve leerstof, maar meer een kunstuiting die ons tot herschepping inspireert, zonder dat we ooit zullen weten of wij daarbij de kunstenaar helemaal hebben begrepen. Dit aspect herken ik in de foto op de kaft van Van Dalens boek. Die foto plaatst ons als toeschouwers in de collegezaal waar Brouwer ongenaakbaar als in een *performance* met krijt zijn mentale constructies schetst.

Diplomatiek heeft Van Dalen de oorspronkelijke foto ingekaderd en het boek de onder-titel ‘Een constructief denkraam’ meegegeven, als wil hij Brouwers subjectieve kunstuiting behapbaar maken en in een objectiever — constructief — kader plaatsen. De lezer van *Intuitionistische Analyse* zit dan ook niet op harde klapstoeltjes te luisteren naar prediking van Brouwers waarheid. Eerder is het boek een rondrit in een touringcar langs de intuitionistische monumenten, terwijl gids Dirk Van Dalen aanwijst en enthousiast toelicht.

De rondleiding begint bij de intuitionistische opbouw van $\mathbb{N}$, $\mathbb{Z}$ en $\mathbb{Q}$, die slechts weinig afwijkt van de klassieke. In hoofdstuk 2 wordt het intuitionistisch redeneren verkend



De oorspronkelijke foto van Brouwer die gebruikt is op het omslag van het boek van Van Dalen

om in hoofdstuk 3 de analyse te beginnen met de invoering van de reële getallen. Hoofdstuk 4 vormt dan de kern met Brouwerse tegenvoorbeelden tegen bekende klassieke stellingen als de middelwaardstelling, en hun intuïtionistisch wel houdbare versies. Het boek besluit met een boeiend hoofdstuk 'Voorts' waar dieper op de logica wordt ingegaan en constructieve axioma's behandeld worden zoals die gebruikt dan wel afgewezen worden in de elkaar beconcurrerende scholen van het constructivisme.

De wiskundige inhoud is versneden met toelichtingen en wetenswaardigheden van algemeen wiskundige, filosofische, historische en biografische aard, zodat je, ook als je over de technische details heen leest, het idee krijgt al aardig mee te kunnen praten over het intuïtionistische hervormingsprogramma. Om het technische handwerk echt in de vingers te krijgen, lijkt het boek mij minder geschikt; ik heb ook niet de indruk dat het daarvoor bedoeld is. Sowieso bevat het weinig opgaven, en hoewel Van Dalen veel vertelt om de definities en stellingen heen, laat hij soms na de brug van de intuïtieve concepten naar de formele definities en stellingen te slaan, en houdt het erop dat 'de wiskundigen het nu eenmaal zo doen'. Zo verschijnt bijvoorbeeld na een heel algemeen verhaal over de interpretatie van de logische voegwoorden en kwantoren (de zogenaamde Brouwer–Heyting–Kolmogorov-interpretatie) en het creatieve subject, pardoos de formele definitie van Kripke-modellen,

waarmee de lezer dan de intuïtionistische geldigheid van redeneerprincipes moet kunnen toetsen. Op dat moment echter heeft de lezer nog geen besef van hoe dat redeneren feitelijk verloopt, laat staan dat de lezer kan begrijpen waarom het instrument van de Kripke-modellen werkt.

Ik wil het boek zeker niet ontraden, integendeel, het is zeer leeswaardig en bevat veel interessant materiaal, ook al is dat nog niet overal aaneengesmeed tot een strak geheel en is menig zet- of spelfoutje blijven staan.

Intuïtionistische analyse

Na deze algemene opmerkingen wil ik op de behandeling van één stelling nader ingaan, namelijk de dekpuntstelling ($n = 2$), in paragraaf 4.5. Enerzijds is aan de hand van deze stelling mooi te demonstreren hoe intuïtionistische analyse afwijkt van de klassieke, anderzijds geeft Van Dalen juist bij deze stelling een ander bewijs dan Brouwer, en is het de moeite waard deze twee bewijzen te

vergelijken met betrekking tot hun constructieve karakter.

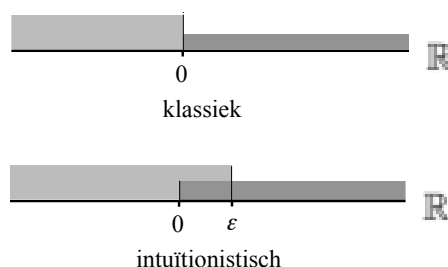
Om in de juiste sfeer te komen voor het bedrijven van intuïtionistisch analyse stelle de lezer zich voor dat wij reële getallen en hun functies slechts met een beperkte scherpthe kunnen oproepen. Die scherpthe is variabel, naar believen kunnen wij inzoomen, maar punten worden nooit Euclides' omvangsloze stippen, zij blijven een zekere dikte hebben. Zo kunnen we niet van elk reëel getal x uitmaken of $x > 0$ dan wel $x \leq 0$. De intuïtionist spreekt in dit verband van de *onsplitsbaarheid* van het continuüm. Daarentegen kunnen we wel voor elke gewenste marge $\varepsilon > 0$ altijd uitmaken door voldoende in te zoomen of $x > 0 \vee x < \varepsilon$. Concreet voor het vervolg betekent dit dat we de reële rechte of het vlak niet scherp kunnen verdelen in disjuncte delen, maar moeten leven met plakstrookjes, die een naar believen kleine, maar positieve marge ε smal zijn. Voor elk punt of getal is dan een deel te noemen waar het zeker in ligt, maar niet altijd te zeggen of het ook nog in het andere deel ligt. Zie Figuur 1.

De dekpuntstelling

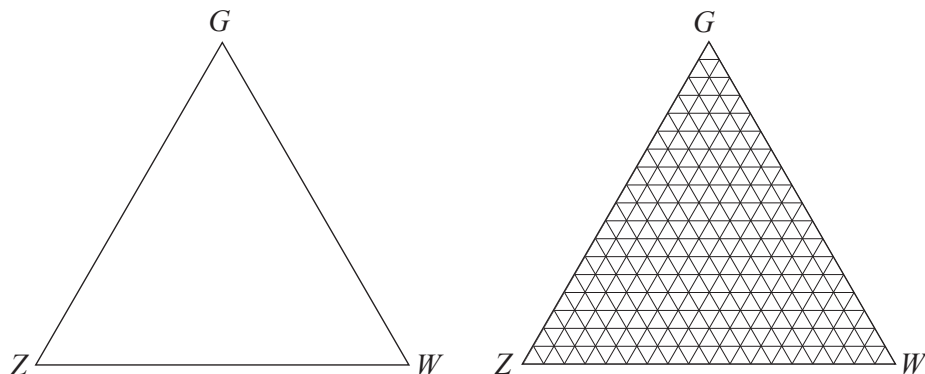
De klassieke dekpuntstelling (dimensie n) zegt dat elke continue afbeelding die een compact, convex deel $D \subset \mathbb{R}^n$ op zichzelf afbeeldt daarbij altijd minstens één punt op zijn plaats zal laten. Een dergelijk punt x met $f(x) = x$ heet dan een dekpunt van f . Brouwer zelf bewees deze stelling klassiek en liet later zien dat deze stelling intuïtionistisch niet houdbaar is. intuïtionistisch heeft een dergelijke afbeelding echter wel 'bijna-dekpunten', dat wil zeggen: voor willekeurig kleine marges $\varepsilon > 0$ zijn er punten die bij toepassing van f minder dan ε van hun plaats gaan. In zijn publicatie [1] met de prachtige titel 'Door klassieke theorema's gesignaleerde pinkeren die onvindbaar zijn', geeft Brouwer een bewijs voor het bestaan van ε -dekpunten op grond van windingsgetallen.

Via Sperner, klassiek

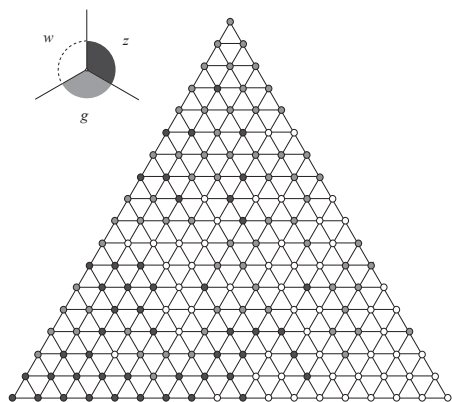
Van Dalen behandelt Brouwers bewijs niet, maar komt met een eigen bewijs (voor $n = 2$) op basis van het lemma van Sperner, waarmee zoals bekend de klassieke dekpuntstelling zich aanzienlijk gemakkelijker laat bewijzen dan met Brouwers afbeeldingsgroepen. Dit bewijs publiceerde Van Dalen in [3]. Om de bewijzen met elkaar te vergelijken voer ik een gemeenschappelijke terminologie in. Kies als domein D een gelijkzijdige driehoek, en zij f een continue afbeelding van deze driehoek op zichzelf. De hoekpunten van



Figuur 1 Splitsing versus plakrandjes



Figuur 2 Netwerk over de driehoek WGZ



Figuur 3 Netwerk met aangebrachte kleuring

de driehoek noemen wij W , G en Z , verwijzend naar de kleuring (wit, grijs, zwart) die wij verderop zullen aanbrengen. Ons doel is te bewijzen dat f een ε -dekpunt bezit, oftewel dat er een x in WGZ moet zijn met $|f(x) - x| < \varepsilon$. Krachtens Brouwers waaierstelling is f uniform continu zodat wij bij de gegeven ε een afstand δ kunnen vinden zodat als $|x - y| < \delta$, hun beelden $f(x)$ en $f(y)$ minder dan een handig gekozen fractie van ε uit elkaar moeten liggen. Leg nu over WGZ een driehoekig netwerk van strooipunten x_i met δ als lengte van de zijden van de driehoekige mazen (in het vervolg ‘de kleine driehoekjes’ geheten). Zie Figuur 2 en 3. Bekijk dan in welke richting bij toepassing

van f deze strooipunten (inclusief W, Z, G) bewegen. Aan de hand van die verplaatsingen zullen wij dan in staat zijn een ε -dekpunt te traceren. Laten wij eerst klassiek te werk gaan. Wij redeneren dan vanuit het ongerijmde. Stel dat er geen ε -dekpunt is, dan hoort er bij elke x_i een verplaatsingsvector $f(x_i) - x_i$ ongelijk $\vec{0}$, waarvan beoordeeld kan worden in welke richting deze wijst. Daarbij onderscheiden wij de drie sectoren: wit (w), grijs (g) en zwart (z), zoals in het linker diagram in Figuur 4.

Aldus brengen wij een kleuring k aan op de strooipunten van het netwerk. Deze kleuring is een zogenaamde Sperner-labeling, in de zin dat:

1. $k(Z) = z$, $k(G) = g$ en $k(W) = w$;
2. ligt x_i op zijde AB van driehoek WGZ , dan $k(x_i) = A$ of $k(x_i) = B$, met $A, B \in \{W, G, Z\}$.

Sperners lemma zegt dan dat hoe je de strooipunten binnen WGZ ook kleurt, er altijd een driehoekje zal zijn dat ‘volledig gekleurd’ is, dat wil zeggen waarvan de drie hoekpunten allen verschillend van kleur zijn. Die drie hoekpunten gaan dus ieder een andere kant op, terwijl hun beelden maar een fractie van ε uit elkaar kunnen liggen. Dat kan alleen als minstens één van hen minder dan ε van zijn plaats gaat, oftewel een ε -dekpunt is. Daarmee is dan klassiek de ε -versie van de dekpuntstelling bewezen.

Via Sperner, intuïtionistisch

Nu werken wij het bewijs om naar het intuïtionistische bewijs van Van Dalen. In plaats van een plaatsvector gebruikt Van Dalen barycentrische coördinaten, maar dat maakt geen wezenlijk verschil. In verband met de onplitsbaarheid van het reële vlak moet hij de drie sectoren overlappend kiezen (zie het middelste diagram in Figuur 4). Merk op dat de nulvector nu in alle drie de sectoren ligt. Door de overlap is de keuze van de kleur niet meer eenduidig. Van Dalen laat zien dat wij de kleur van strooipunten op de buitenomtrek wel zo kunnen kiezen dat er toch een Sperner-labeling ontstaat. Het lemma van Sperner is combinatorisch van aard en daarom ook intuïtionistisch correct, zodat wij een driehoekje kunnen vinden waarvan minstens een van de hoekpunten een ε -dekpunt is. Klaar.

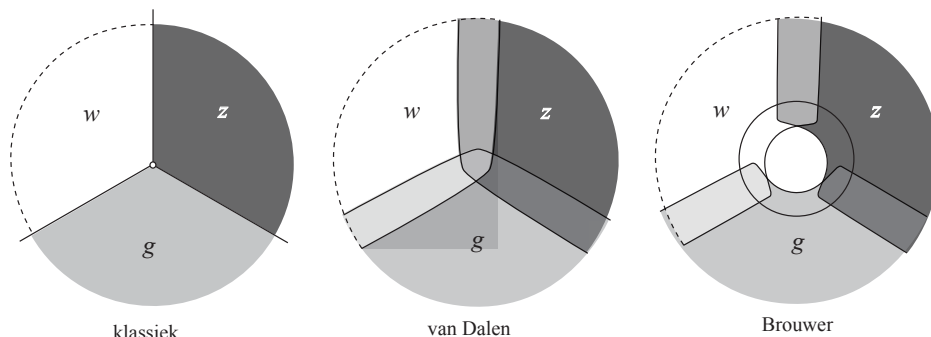
Merk op dat ten opzichte van het klassieke bewijs Van Dalen niet begint met de ongerijmde aanname dat er geen ε -dekpunt zou zijn. Van Dalens bewijs is intuïtionistisch gevoerd en zou dus ‘constructief’ moeten zijn in de zin dat het aangeeft hoe je het ε -dekpunt vindt. Het bewijs vertelt daarover: breng een voldoende-fijnmazig netwerk aan, bereken de kleuren van alle strooipunten, zoek dan een volledig gekleurd driehoekje op (dat er volgens Sperner moet zijn). Minstens één van de hoekpunten van dat driehoekje is dan een ε -dekpunt. Maar in deze gevolgde weg zit een procedurele kronkel. Het hoekpunt van het volledig gekleurde driehoekje is namelijk een strooipunt, en omdat dit strooipunt als ε -dekpunt maar weinig van zijn plaats gaat, zullen wij tevoren al flink hebben moeten rekenen voor wij het een juiste kleur konden toekennen. Zo ver dat wij het toen al hadden moeten herkennen als een ε -dekpunt.

Daarmee geeft Van Dalens bewijs weliswaar aan hoe wij een ε -dekpunt kunnen vinden, maar vertelt ons niet hoe dat proces feitelijk zal verlopen. In zijn inleiding (p. 6) zegt Van Dalen: “De constructieve wiskunde beschouwt het als haar taak om die belofde getallen, punten lijnen, matrices, ... echt uit te rekenen.” Maar zijn bewijs van de ε -dekpuntstelling stopt als de redenering rond is, en geeft geen rekenschap van het onderliggende constructieproces.

Laten wij nu de blik richten naar Brouwers oorspronkelijke bewijs.

Via windingsgetallen

Brouwers bewijs oogt heel anders. Dat het domein bij hem vierkant is, en onderverdeeld wordt in vierkantjes is niet wezenlijk. Brouwer gebruikt de verplaatsingsvectoren



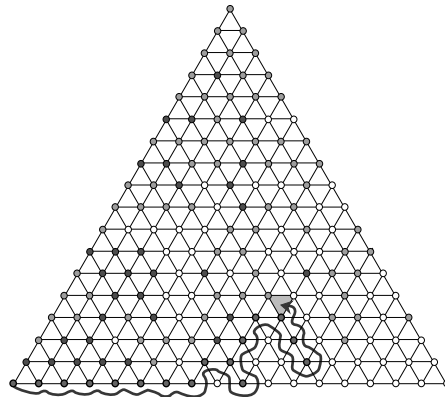
Figuur 4 Sectoren klassiek (links), sectoren Van Dalen (midden) en sectoren Brouwer (rechts)

$f(x_i) - x_i$ niet om een Sperner-labeling te maken, maar om de windingsgetallen uit te rekenen van enerzijds een wandeling over de buitenomtrek WGZ en anderzijds over alle kleine driehoekjes van het netwerk afzonderlijk. Onder het windingsgetal van een wandeling verstaan wij het aantal draaien dat de verplaatsingsvector maakt tijdens die wandeling. De windingsgetallen zijn gemakkelijk te berekenen aan de hand van de richting van de verplaatsingsvectoren in de strooipunten op die wandeling, omdat die zo dicht bij elkaar liggen dat de verplaatsingsvector nooit tussen twee strooipunten in een hele draaiing kan maken, tenzij deze zo kort is dat we een ε -dekpunt passeren. Vertaald naar bovenstaande terminologie gebruikt Brouwer voor de richting van die verplaatsingsvector feitelijk vier gebieden: w , g , z en o . Zie het rechter diagram in Figuur 4. Wederom is er overlap noodzakelijk in verband met de onplitsbaarheid van het continuüm. Brouwer onderscheidt dan twee gevallen:

1. er is een strooipunt dat minder dan ε beweegt;
2. alle strooipunten gaan meer dan $\frac{1}{2}\varepsilon$ van hun plaats.

Die gevalsonderscheiding is voor een intuitionist verdacht, misschien dat Van Dalen hem daarom in zijn bewijs vermeden heeft. Maar hij is wel degelijk geoorloofd, immers voor een reëel getal x kunnen wij beoordelen of $x < \varepsilon \vee x > \frac{1}{2}\varepsilon$. En omdat wij maar eindig veel strooipunten hebben kunnen wij die beoordeling ook voor alle strooipunten doen.

Uiteraard behoeft geval 1 geen verdere behandeling, het ε -dekpunt is dan reeds gevonden. In geval 2 komt geen enkele verplaatsingsvector in gebied o , en geven de kleuren w , g , z van de strooipunten genoeg informatie om de windingsgetallen correct te berekenen. Bij de wandeling over de buitenomtrek WGZ verschijnen dan afwisselend w , g en z terwijl daartussen wat haperingen van de soort $-aba-$ voorkomen, die je kunt gladstrijken tot $-a-$. Het windingsgetal van de omtrek is dus 1. De wandelingen over de kleine driehoekjes passeren steeds maar drie strooipunten. Hebben twee van die hoekpunten dezelfde kleur dan is het blijkbaar niet gelukt een hele winding te maken en is het windingsgetal dus 0. Zijn de drie hoekpunten verschillend van kleur dan is het windingsgetal 1 of -1 . In plaats van het lemma van Sperner gebruikt Brouwer dan het net zo combinatorische argument dat de som van de windingsgetallen over de samenstellende driehoekjes gelijk moet zijn aan het windingsgetal van buitenomtrek WGZ .



Figuur 5 Route naar het bijna-dekpunt

Derhalve moet minstens één van de kleine driehoekjes windingsgetal 1 hebben en is er dus een driehoekje waarvan alle hoekpunten verschillend van kleur zijn. Zodat minstens een van deze hoekpunten toch slechts $\frac{1}{2}\varepsilon$ van zijn plaats gaat. De behandeling van dit geval 2 verschilt dus eigenlijk maar weinig van wat Van Dalen doet met de Sperner-kleuringen. Het wezenlijke verschil is dat Brouwer eerst geval 1 noemt, en na afhandeling van geval 2 concludeert dat 1 de enige mogelijkheid is. Zo is in zijn bewijs meer terug te zien van hoe je het ε -dekpunt vindt, namelijk door van elk strooipunt te bekijken of de verplaatsingsvector kleiner is dan ε .

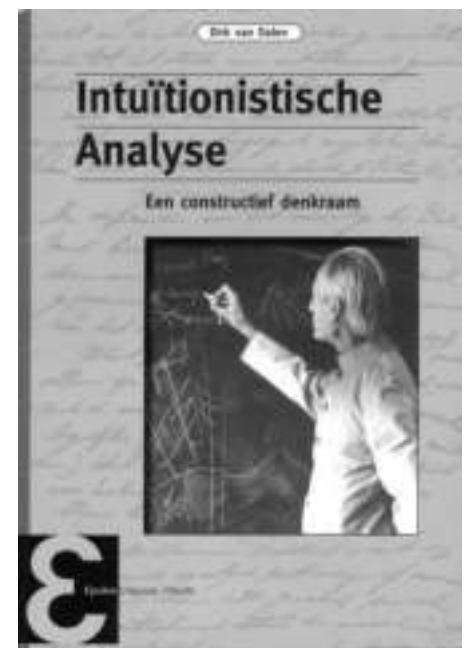
Over beide bewijzen wil ik nog opmerken dat zij weliswaar een constructie geven om een ε -dekpunt te vinden, maar zeker geen handige constructie. Om het ε -dekpunt doelmatig uit de strooipunten te vissen zou je natuurlijk kunnen navigeren aan de hand van de verplaatsingsvectoren. Bijvoorbeeld (zie Figuur 5), begin in Z en wandel over ZW tot je een zijde met de kleuren zw tegenkomt. Steek vanuit dat driehoekje steeds via een zw -kant over naar een aangrenzend driehoekje. Op het moment dat dat niet meer kan, ben je in een zwg -driehoekje aangeland. Op die manier benut je de reeds berekende kleuren. Met de windingsgetallen is het mogelijk het hele gebied steeds te delen en aan de hand van het windingsgetal van de twee delen te besluiten in welk deel je dan verder gaat zoeken. Het is toch opmerkelijk dat hoewel constructivisten vanuit hun filosofie erop gericht zijn hun objecten 'te maken', er in hun bewijzen soms heel weinig aandacht is voor effectieve constructies.

Van Dalen heeft ons taalgebied verrijkt met een interessant boek aan de hand waarvan een breder publiek zich bezig kan houden met de vraag hoe wiskunde eruit komt te zien als objecten niet uit tegenspraken geboren worden maar 'echt' gemaakt moeten

worden. De genoemde onvolkomenheden daargelaten biedt het boek de lezer de gelegenheid de mogelijke keuzes en hun consequenties te verkennen.

Referenties

- 1 L.E.J. Brouwer, Door klassieke theorema's gesignaleerde pinkern die onvindbaar zijn, *KNAW Proc. Ser. A* 55 (1952), 443–445.
- 2 D. van Dalen, *Mystic, Geometer and Intuitionist* (2 delen), Clarendon Press, Oxford, 1999.
- 3 D. van Dalen, How to constructivize Brouwer's fixed point theorem, E. Rajan et al., *International Conference on Systemics, Cybernetics and Informatics*, Hyderabad, 2009, pp. 654–656.
- 4 A.S. Troelstra en D. van Dalen, *Constructivism in Mathematics* (2 delen), North-Holland, Amsterdam, 1988.



Dirk van Dalen, *Intuitionistische Analyse*, Epsilon Uitgaven, Amsterdam, 2011, 152 p., ISBN 9789050411240, prijs €21,00.

Ionica Smeets

wetenschapsjournalist, Leiden

i@ionica.nl

Society Study Group Mathematics with Industry 2012

Spotting damaged strips

How can you tell from a picture if a steel strip is pinched? This was Tata Steel's question for the Study Group Mathematics with Industry. The mathematicians found a surprisingly simple way to detect damaged strips.

Participants of the study group

Evgeniya Balmashnova (TU/e)

Mark Bruurmijn (TU/e)

Ranjan Dissanayake (Rajarata University)

Remco Duits (TU/e)

Leo Kampmeijer (Tata Steel)

Tycho van Noorden (Universität Erlangen-Nürnberg)

Glowing red hot strips of steel, shooting by with a speed of 70 km/h. This is daily business at the IJmuiden site of Europe's second largest steel producer Tata Steel. Their hot strip mill (see Figure 1) yearly produces 250.000 coils of steel. The steel enters the mill in slabs with a length of a few meters and a thickness of two centimeters. The slabs are heated up to a temperature of 1200 °C (which is around the temperature of magma) and step by step rolled into strips with a length of

up to two kilometers and a thickness of two millimeters. Then they are cooled down to 600 °C and coiled up generally in less than a minute.

During the final reduction step (see Figure 2) the steel can reach a speed of 70 km/h. This step is very critical. Any process error may lead to a defect in the shape of the strip. Especially at the tailing out of the strip such shape defects may make the steel pinch. This pinching is visible as ripples in the strip. The biggest problem is not that the strip is ruined, but that the machines might be damaged too. And stopping the machines is very expensive.

Leo Kampmeijer, researcher at Tata Steel, asked the study group to devise an algorithm that can automatically determine from a grey scale picture whether a strip is pinched at the tail. The main goal is to detect slight pinches before they cause any real damage. A second goal is a better understanding of what causes the pinches. This might be used to modify the process to prevent them altogether.

Detection

In the hot strip mill a camera already takes images of the steel strips and an automatic surface inspection system scans these pictures. This software is trained with categorized images and can spot simple defects. But pinching is very hard to detect automatically, partly because it can appear in different forms.

Mathematician Remco Duits specializes in image analysis and explains the limits of the available commercial software: "This system is trained to find small holes in the steel. It is highly specialized for this task and does this very well. But it cannot do other things,

it cannot even detect the end of the strip." Duits usually works on medical imaging. The problem reminded him of MRI scans of the human heart and he was curious to see whether his techniques from medical imaging would work for steel strips too. Leo Kampmeijer was cautiously optimistic at the beginning of the study group: "I am used to working with mathematicians and I know that a lot is possible mathematically. But I also know how hard it is to get something that works in the real world."

The study group decided to focus on two properties of pinched strips: their elongated tails and their ripples. Sometimes the medical background of the researchers shone through when they talked about the steel as if it were a patient: "In a healthy strip... I mean, a normal strip..."

On the tail

To automatically compare tails the mathematicians defined the tail length as the distance between the top point of the strip and the place where the strip first reaches its full width. See Figure 3. In the lower half of the image the width of the strip is almost constant



Figure 1 The hot strip mill with glowing hot slab of steel.



Figure 2 The final reduction step in the finishing mill.

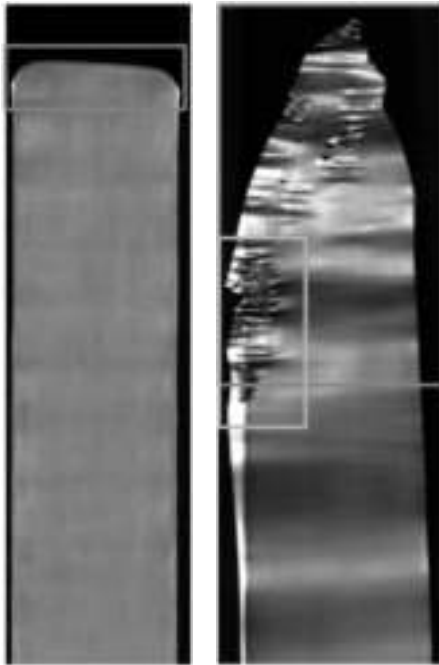


Figure 3 It is quite easy to spot the pinched strip with the naked eye. It has a long, irregular tail and ripples.

for both pinched and normal strips. Therefore the median width in this part is taken as the width of the strip. In practice this is done by counting the number of black background pixels in a horizontal line. As an example, if the image has a width of 200 pixels and the median number of black pixels in the lower half of the image is 30 in a line, then the width of the strip is taken as 170 pixels.

To find the tail length we start by scanning the image line by line, starting from the top row. In the first few rows there will be no strip visible, so here the number of black pixels will be 200. As soon as the number of black pixels drops below 200, we have found the beginning of the tail. We remember this as the first line number. Now we keep going until we find a line where the strip first reaches full width. In our example we would continue until we have a line with 30 black pixels, this is the second line number. The tail length is the difference between the second and first line number.

Shadowy figures

There is a small problem with the described method: shadows in the image might be seen as background pixels. In that case the estimation for the tail length will be off. Therefore the mathematicians developed a second approach in which the width of each row is computed (by taking the distance between the first and last non-black pixel). Then the mean of these values is used and a more accurate tail length is found.

The images from the factory do not have too many shadows and in most cases the first and second approach yield exactly the same tail length. If the two results differ, this indicates that there is something wrong with the image. It could be a shadow, or a hole in the strip. So using two different methods of finding the tail length and comparing the results can be useful for detecting holes.

Ripples

Strips that are pinched, have vertical ripples. They show up in the images as fast changing, periodic changes of grey values. A common strategy for finding such distortions is using the Fourier transform. Unfortunately, the ripples have local frequencies and Fourier only detects global ones. Luckily, the related Gabor transformation could do the job. This transformation filters the images and gives more weight to the higher frequencies. In the end the transformation yields just one number that measures how rippled a strip is. A *rippleness* of 0 is a perfectly flat strip, a rippleness of 10.000 is the worst possible.

Classifying

For each image of the strip this results in two numbers: one for the tail length and one for the rippleness. A scatter plot shows how these two numbers are distributed for pinched and normal strips. See Figure 4. A line separates the normal strips from the pinched ones.

This criterion correctly identifies all of the pinched strips. Of the normal strips 96.3 percent is correctly seen as good, less than 4 per-

cent is wrongfully seen as pinched. In most cases this seems to be caused by a problem in the lighting.

Future work

Remco Duits is happy with the results, but emphasizes that the classification can go much faster: "We cut some corners and did everything rather roughly. The goal of the study group was to make it work, to get some first results within a week. Things could look much better, there is a huge mathematical framework behind all this." At the end of their paper the mathematicians list the possibilities for further research. The pinches can be classified based on severity and other types of defects might be detected with similar methods.

Leo Kampmeijer from Tata Steel is already very pleased with the results: "We could start using these methods tomorrow. As soon as I have time, I will do more tests to see which of the methods is most workable." He was surprised that it was possible to detect pinched strips from just the tail length and rippleness: "I thought that you would need more properties of the strip." The mathematicians also suggested more future applications than Kampmeijer expected when he prepared the questions: "So I hope to stay in touch".

This is a brief report on the Study Group Mathematics with Industry, held from 30 January to 3 February 2012 at Eindhoven University of Technology. The scientific proceedings are available on www.eurandum.nl/events/workshops/2012/SWI_2012.

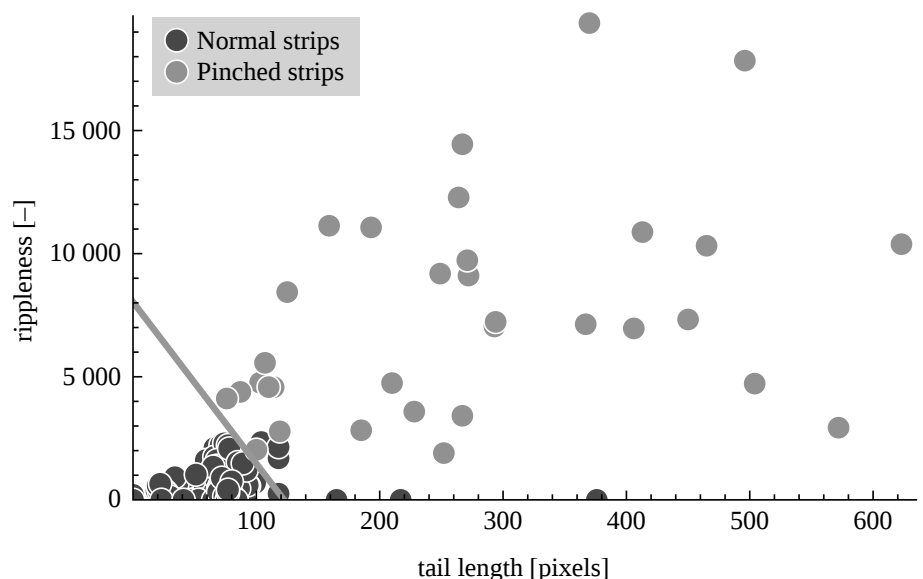


Figure 4 The tail-length is on the horizontal axis, the rippleness on the vertical axis. Most normal strips are in the lower left corner. The line indicates the criterion for classifying strips.

Ionica Smeets

wetenschapsjournalist, Leiden

i@ionica.nl

Society Study Group Mathematics with Industry 2012

Keep the messages flowing

How do you maximize the lifetime of a network of communication devices? The Study Group Mathematics with Industry investigated approaches inside and outside the usual framework. After two days, they had an answer that gave Thales unexpected new ideas.

Participants of the study group

Nikhil Bansal (TU/e)
David Bourne (TU/e)
Murat Firat (TU/e)
Maurits de Graaf (Thales)
Stella Kapodistria (TU/e)
Kundan Kumar (TU/e)
Corine Meerman (UL)
Mihaela Mitici (UT)
Francesca R. Nardi (TU/e)
Björn de Rijk (UL)
Suneel Sarswat (NISM, India)
Lucia Scardia (TU/e)

Imagine a group of firefighters at a big disaster site. Each firefighter has a device for communicating with the rest of the group. Every time one of them sends a message, for instance a position update, the information must be broadcasted to all the others in a wireless network. The communication devices have a limited battery capacity, and sending a message takes energy. How should the messages be sent through the network to keep the flow

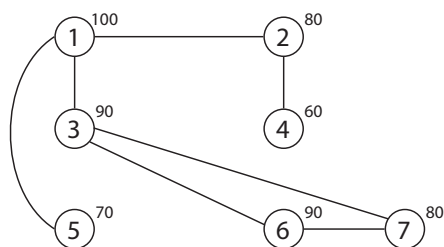


Figure 1 An example of a network with seven nodes. Next to each node is the current battery level (so node 3 has level 90 left). Nodes are neighbors if they are connected, so node 1 and 2 are each others neighbors, but 3 and 4 are not.

of information running for as long as possible? This is an example of the more general problem that Maurits de Graaf from Thales brought to the study group. De Graaf develops algorithms that increase the lifetime of wireless ad-hoc networks of communicating nodes. In this setting the lifetime of a network is defined as the time until the first node runs out of energy. The goal is to find a broadcasting protocol that maximizes this lifetime.

De Graaf had three questions for the study group. The first one was about the current heuristic algorithm that Thales uses, how far is that from the optimal solution? The second was about a more intricate model for sending the messages and the third about variations in battery consumption. In preparing his questions, he tried to make them appealing to mathematicians from different areas. “I hoped for a diverse group, to get a new and fresh perspective.”

Mathematician Nikhil Bansal from Eindhoven University of Technology joined the Thales team because the questions were theoretically most interesting: “It is a precise and technical problem with nice applications.” His group started working on the first question about the quality of the heuristic algorithm from Thales. The mathematicians made two basic assumptions about the network. First they assumed it is stationary, so the connections between the nodes do not change over time. Secondly, they assumed battery use is linear and sending a message decreased the battery level by one. Receiving a message does not consume energy. See Figure 1.

Willing and able

Thales currently uses the Maximum Willing-

ness Heuristic (MaxWill for short). This algorithm tries to use the neighboring nodes with the highest remaining battery level for relaying messages. A key feature of MaxWill is its layered structure. A node that is broadcasting automatically sends the message to all its neighbors, the nodes that are just one hop away in the network. MaxWill selects a set of these neighbors as relays such that all the nodes that are two hops away will receive the message. The one-hop-neighbors can be seen as the first layer, the two-hop-neighbors as the second. Nodes with higher battery levels get selected first as relays, because they are most willing to sacrifice their batteries.

Nikhil Bansal: “We soon found some examples that showed that MaxWill is not always optimal. We devised another algorithm that seemed to do better.” Their new algorithm carefully avoids nodes with the lowest battery level. This results in a longer lifetime of the network, because more messages can be sent before the first node runs out of

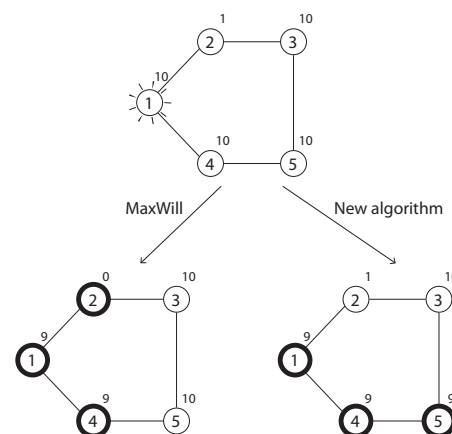


Figure 2 With MaxWill this network is down after sending one message from node 1, because its neighbors 2 and 4 have to relay the message to reach all two-hop neighbors. So node 2 will immediately run out of battery. In the new algorithm, nodes 4 and 5 relay the message and it is possible to send at least one more message.



During a forest fire the firefighters update each other on the fire details at different locations.

battery. In a number of simulations the new algorithm gave on average a 60 percent longer life-time of the network.

A hard problem

The new method does not always find the optimal solution. In fact, it is impossible to find a fast algorithm that does this. The mathematicians proved that the problem of maximizing the network life-time is NP-hard. This is a class of problems for which a solution can be checked efficiently, but for which there is no fast algorithm for finding such a solution. You may think of a sudoku puzzle. It takes quite some time to finish one, but it is really easy to quickly verify that a given solution is correct.

So there is no algorithm that rapidly gives the optimal way of sending messages. Even more depressingly, the study group showed that it is also NP-hard to approximate the best solution. So every fast algorithm will find a solution that is at least a factor worse than the optimal lifetime.

The study group emailed their results to Thales on Tuesday night, feeling that they had solved the first problem and were ready to move on to the other two questions. Bansal: "But on Wednesday Maurits de Graaf came to Eindhoven explained that their real problem was slightly different. The demand that all the second-hop-nodes were covered after the first relay was not a choice from their algorithm, it was a constraint. This layered approach

was obliged in the way all their systems were implemented. Our algorithm was impossible to use for Thales, we picked the wrong layers."

It took De Graaf some time to appreciate the new algorithm: "My first reaction was that this was all wrong. However, the more I thought about it, the more I liked this new simple mechanism. We would not have come up with something like this at Thales, because the idea is different from the framework we are currently using. However, the algorithm from the study group performs so much better that we now consider adapting or even leaving the framework."

Layered approach

After De Graaf's visit the study group went back to the first question, but now with the layers as in the preconditions. To compare MaxWill with the optimal solution, the problem was reformulated as a linear program. In this setting there is a target number of rounds of messages. A round is series of broadcasts where each node occurs exactly once as the source. It is a reasonable assumption that the nodes all have to send regular updates, because they have to update the information from their location. The problem is now to decide if there is a way to send the target number of rounds through the network. When the number of nodes is not too large, this decision problem can be solved rather fast. Repeating this procedure for higher and higher numbers

of rounds until the problem becomes infeasible, yields the optimal number of rounds.

To compare the results from MaxWill with the optimal solution a number of networks were randomly generated. Two nodes had a probability of 50 percent of being connected and each node started with a randomly chosen battery level between 20 and 30. In small networks of five nodes, MaxWill gave the optimal solution in 98 percent of the cases. If the networks became bigger, this percentage dropped, to 58 percent for networks of ten nodes and to 45 percent for fifteen nodes. Simulations with other types of networks showed that MaxWill performs best in sparse networks.

In their final presentation the mathematicians apologized for not answering the other questions: "We had too much fun with problem one to start on the rest, but if the study group had been one week longer we would have done more." Their paper gives some first ideas for the other questions, but these topics would deserve a separate article.

Two directions

For the first question the final conclusion of the study group is twofold. If Thales decides to switch to a protocol that does not require the layered approach, their new algorithm performs much better than MaxWill. If they want to stay within the current framework, the linear problem indicates in which types of networks MaxWill performs well and not so well. For the latter cases another approach would be useful. For small networks the linear program can serve as a better heuristic.

Thales decided to further investigate both directions. Maurits de Graaf: "A student is coming to do an internship at Thales, he will find the report from the study group on his desk. Part of his task will be to look at the impact of dispensing our framework. Can we retain the good properties of the current setup and combine them with the new algorithm? And if we remain within the framework, how can we use the ideas from the study group to improve the MaxWill heuristic?" He concludes that the study group is a great initiative: "Even if you can not directly implement the results, you gain better insight and departure points for further research." ◀

This is a brief report on the Study Group Mathematics with Industry, held from 30 January to 3 February 2012 at Eindhoven University of Technology. The scientific proceedings are available on www.eurandum.nl/events/workshops/2012/SWI.2012.

Ionica Smeets

wetenschapsjournalist, Leiden

i@ionica.nl

Society Study Group Mathematics with Industry 2012

Check the lights

Headlights, LED spots and other optical systems produce complicated light patterns. Philips Lighting checks the output of their new designs by tracing millions of rays through the system. A reliable method, but very time-consuming. For advanced solutions, the calculations may take days. Can the Study Group Mathematics with Industry come up with a faster approach?

Participants of the study group

Jan Bouwe van den Berg (UvA)
Rui Castro (TU/e)
Jan Draisma (TU/e)
Joep Evers (TU/e)
Maxim Hendriks (TU/e)
Oleh Krehel (Universität Erlangen-Nürnberg)
Ivan Kryven (UvA)
Karin Mora (University of Bath)
Botond Szabó (TU/e)
Piotr Zwiernik (TU/e)

Philips Lighting develops optical systems. Since the introduction of LEDs these systems have become more and more intricate. A naive method to predict the brightness and intensity of a new system is to trace a random ray of light through it. For a single ray this is an easy calculation, but for a realistic image you need to track up to a million rays. The devil is in the details, skipping a small number of rays may result in an incorrect pattern. Altogether the computations can take an entire weekend to run. One of Philips Lighting's long-term goals is developing faster methods, so they can more easily test and optimize their designs.

Wilbert Ijzerman, department head of Philips' LED Platform development group, knew about a different approach, but he never had any time to look into it. When he was home with the flu he started thinking about it again: "The walls were closing in on me and

I started tinkering." The key idea is to look at groups of rays that leave the light source close to each other with a similar angle. These rays will roughly follow the same path through the optical system. The initial position and angle of a ray form a two-dimensional phase-space. How can this phase-space be partitioned in areas that show the same behavior? More specifically, how can the edge between two such areas be determined? These were the questions Ijzerman and his colleagues asked the study group.

They knew that their problem was tough, so they suggested that the study group focused on two-dimensional models. Mathematician Maxim Hendriks from Eindhoven University of Technology: "The problem itself was immediately clear, but only later we understood what made it so hard. It is impossible to find exact solutions for some of the problems. You can do it numerically by solving the same problem many times. Actually many, many times. Which is troublesome in practice too."

A cup with two facets

The study group decided to start with a very simple light fixture: a symmetric cup with a flat base and two inclined facets. The entire base is the light source. See Figure 1. This models a simple torch or bike light. The light intensity is not equally strong in all directions; it varies with the cosine of the angle of the light ray. These sources are called Lambertian and to the human eye they appear to have the

same brightness when viewed from different angles.

The quality of the light bundle is assessed on a screen that is parallel to the light source. In most real life applications it is unknown how far away a wall will be from the lamp. Therefore only the far-field is considered, this may be seen as a target screen at infinity. The distance is in practice always much larger than the size of the optics and hence you can apply the far field approximation.

For an elementary two-faceted cup it was possible to analytically determine the number of reflections before a ray left the cup. To ease counting the reflections, the mathematicians mirrored the cup and not the rays. See Figure 2. They divided the phase-space in regions where rays had the same number of reflections. The boundaries between these regions turned out to be nearly straight lines for their

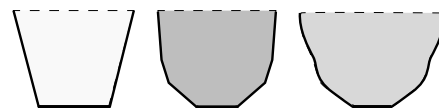


Figure 1 Three cups that are increasingly hard to analyze. The two-faceted cup on the left is the easiest, the multi-faceted in the middle a bit harder and the smooth cup on the right is the hardest.

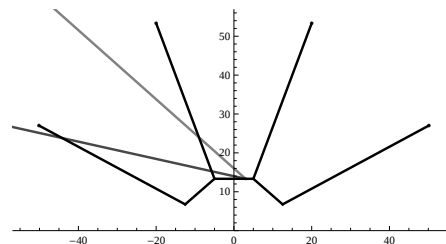


Figure 2 The number of reflections of a ray is the same as the number of reflected cups it passes. So in this example the red ray (dark grey) is reflected once and the blue ray (light grey) twice.

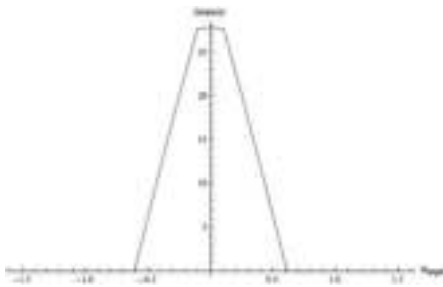


Figure 3 For the example cup suggested by Philips the intensity became a nice and simple peak.

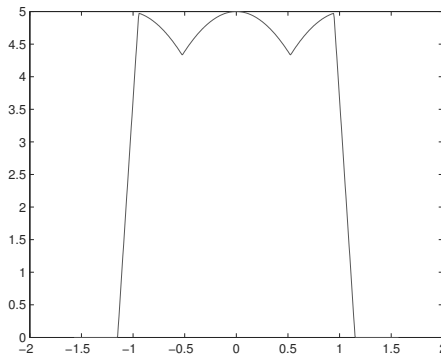


Figure 4 For a cup with slightly different inclined edges the intensity pattern was something like a batman mask. This is the torch light effect.

simple example. The next step was to calculate how a reflection changes the angle of a light ray and use that to determine the exiting angle of each ray. Finally, from all this they computed the intensity pattern at the far field. For some cups a familiar pattern arose. The light was brightest right in front of the fixture, but just right and left of this bright core was a darker ring, which in turn was surrounded by a bright ring. Hendriks: "I remember this effect from when I held a torch light as a kid. There was always a black spot close to the middle of the light bundle." See Figures 3 and 4.

Different cups

Multi-faceted cups can be seen as a stack of two-faceted cups. By careful retracing the beams of light that emanate from the cup back to the source, the results from two-faceted cups can be used to find the intensity for these multi-faceted cups. The study group also managed to generalize part of the results to polygonal cups.

For smooth cups things became much harder. To make things workable the study group made the rather limiting assumption that the ray trajectory always alternated between the left and right side of the cup. So cups that would reflect a ray from the left side back onto the left side were not allowed. Even with this restriction it was impossible to reconstruct the exact partitioning of the phase-

space. The study group showed how finding the boundary of regions in the partition is equivalent to finding the zeroes of a (sophisticated) function. They indicated a whole ensemble of numerical tricks that could do this.

Faster simulations

Finally, the group considered how Philips' current method of ray tracing could be sped up using the partitioned phase-space. Instead of using random rays, one could smartly select a small number of rays to trace and derive the rest of the paths from there. The study group proposed two different methods. The first assumes that the partition of the phase-space is known. The method starts by taking a small preliminary sample of uniformly distributed points from the phase-space. For each of these points their path is determined by traditional ray-tracing. Then a much larger sample of points is randomly selected from the phase-space as an estimation sample. For these points there is no need for ray-tracing, because their path can be computed from the paths of the nearest points in the preliminary sample. See Figure 5.

The resulting intensity pattern was very close to the true profile, but there were some striking differences. This was mainly caused by errors in the approximation of the phase-space partition. Therefore the team came up with a second method that does not need the partition of the phase-space and only makes some very weak assumptions about this partition. As before the method starts by tracing a small preliminary sample of rays and selecting a larger estimation sample. But now for each point in the estimation sample the method takes different groups of nearby points in the preliminary sample that all have the same number of reflections. If the estimation point fits nicely into one of these groups,

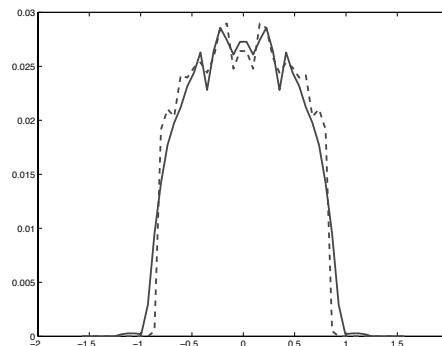


Figure 5 The results from the first method on a smooth cup (solid line). The preliminary sample contained 512 rays, the estimation sample 2^{18} . They compared the pattern with the naive ray-tracing of 2^{18} rays (dashed line).

it must have the same number of reflections as these points. Otherwise, ray-tracing is performed and this ray is added to the preliminary sample as extra data. This method simultaneously estimates the partition of the phase-space and the intensity profile. In general only points close to the boundary of a region in the phase-space need to be traced. The method was tested on a smooth cup with a preliminary sample of 512 points and an estimation sample of 2^{19} points.

The method only used 38,006 ray tracings, which is about 7 percent of the rays. The resulting intensity plot is almost identical to the one from doing 2^{18} ray tracings. This naive method however takes hours, while the new method runs in a few minutes.

First steps

Wilbert IJzerman is not sure that Philips will implement this faster method: "We have to be really sure that we are not missing some details." He is however very happy with the results from the study group. "For the industry this week is the perfect way to explore new directions. If the study group solves your problem, then it is too easy and not very interesting for further research. If they do not make any progress, your problem is too hard. But if they manage to make some first steps in a week, you get the feeling that you could really do something with this problem if you worked on it for a year."

Two ideas from the study group were new to him. The first was the backward tracing of the light that was used in the multi-faceted cups: "We had never done something like that in this context. This method gives our designers a better understanding of what happens with the phase-space." The other fresh idea was searching the boundaries in the phase-space by determining zeroes of a function.

IJzerman has decided that his questions deserve further research, starting with a student and hopefully later a research project from the Dutch Technology Foundation STW. "These are deep questions, both analytically and numerically. I think that the mathematicians in the study group saw that our problems are just as hard as those in academics."

This is a brief report on the Study Group Mathematics with Industry, held from 30 January to 3 February 2012 at Eindhoven University of Technology. The scientific proceedings are available on www.eurandum.nl/events/workshops/2012/SWI.2012.

Ionica Smeets

wetenschapsjournalist, Leiden

i@ionica.nl

Society Study Group Mathematics with Industry 2012

Calculating the response of a ship

How does a ship react to the continuously wave action? MARIN asked the Study Group Mathematics with Industry to find a way to calculate the response from the ship from a bulk of measurements. They found a solution, but was it more clever than what MARIN was doing?

Participants of the study group

Giovanni A. Bonaschi (TU/e)
Ingo Drummen (MARIN)
Olena Filatova (TU/e)
Carlo Mercuri (TU/e)
Adrian Muntean (TU/e)
Mark A. Peletier (TU/e)
Volha Shchetnikava (TU/e)
Eric Siero (UL)
Iason Zisis (TU/e)

Maritime Research Institute Netherlands (MARIN) is a familiar face around the study group. The previous years they brought problems about extreme rolling of vessels in head waves, thruster allocation and maneuvering behavior of ships. Naturally, their 2012 question was also about ships: this time floating production, storage and offloading units (abbreviated as FPSO's). Offshore companies use these vessels for storing and processing oil and gas. Most of these ships are moored at a fixed position at the sea. They are huge. The study group used data from an FPSO that is 230 meters long.

An FPSO typically has a lifespan of twenty to thirty years. Cyclic loading from waves slowly degrades the structure. How can you determine this consumed fatigue life time? Over time the draft of the ship is recorded, a buoy around it measures wave elevation and angle, and strain gauges continuously

monitor the strains in the structure. These measurements can be related to design limits to predict when the structure will fail, or even better: to prevent the structure from failing.

There is a small problem: the amount of data is overwhelming. For instance, one buoy provides twice an hour the incoming waves in 91 angles, for 64 frequencies each. After two years this adds up to more than two hun-

dred million data points. The question for the study group was to find a new mathematical way to compute the response of the structure from this giant heap of data. The main goal was to determine the response amplitude operators, or more informally, the response of the structure to the incoming waves.

Ingo Drummen, project manager at MARIN, knew this was a tough problem: "We had spent a lot of time on it and I mainly wanted to get a fresh perspective. Could the mathematicians come up with something more clever than what we were doing?" It was Drummen's



Example of an floating production, storage and offloading unit

first personal experience with the study group and he was amazed how much time it took to communicate the problem: "I have been in this field for many years and it was hard to go back to the basics. It surprised me that people didn't know what the draft of a ship is." Just to be sure: the draft of a ship is the vertical distance between the waterline and the bottom of the hull.

Cherry-picking

Iason Zisis from Eindhoven University of Technology chose this problem because he liked the engineering and mathematics behind it: "It is about doing something smart with the data." He and his colleagues soon decided that they should limit themselves to the mathematical part of the problem and not advice MARIN about the ship: "We truncated the problem to pure data-analysis."

It was not easy to handle the data. During their presentation the mathematicians joked that in their normal work there was too little data: "But here we had more than enough. It was hard to figure out what to do with it." They decided to only use a small part of

data. Firstly they picked just one draft range of the ship and just used the measurements in which the draft was between 12.5 and 13 meters. This left 'only' 1176 measurements for each wave frequency. The system was still over-determined, because for each frequency there were 91 unknowns, one for each of the angles. But not every measurement is good. For instance, when a ship passes the measuring buoy, this will affect the local measurements, but not the reaction of the vessel. To exclude such erroneous measurements the mathematicians selected for each frequency only the data point with the highest response of the ship.

Least squares

Even after cherry-picking the data the system was overdetermined, there were still many possible solutions. So they needed a way to choose the best solution. A standard solution for such overdetermined problems is fitting the data with a least squares approximation. This method finds the solution for which the sum of the squared errors is minimal. See Figures 1 and 2.

More assumptions

The study group decided to further limit the allowed solutions. They assumed that the reaction of the ship was a periodic function in terms of the direction of the waves. To be more precise, they assumed that it could be written as a truncated Fourier series using cosines of the wave direction. Zisis: "In reality waves come from the front or the side. The ship shows a big response in one direction and a small one on the other side. Therefore it makes sense to use cosines."

This approach yielded a reasonable solution, but for some small frequencies the approximation error was still very high. In their report the mathematicians note that this is probably caused by measurement errors. They conclude that you need at least 500 data points to make a reasonable approximation. They also observe that if the number of free parameters in the Fourier function increases, the solution becomes bad.

Ingo Drummen from MARIN: "I deliberately did not tell the study group what the solution should look like, because I wanted to give them as much freedom in modeling as possible. But during their presentation I noticed that their solution became worse when it had too many free parameters. In such cases you start explaining errors of measurement with physics. This was the biggest eye-opener for me. A few weeks later with another project I was in the exact same situation, trying to find the balance between keeping the system as free as possible and avoiding that too much freedom produces nonsense."

The study group did not come with something more clever than MARIN was already doing. Drummen: "Their methods are as good as ours. This was both a disappointment and a relief. A disappointment, because it would have been nice to have a better solution. But also a relief, because this showed that MARIN had not overlooked something easy."

MARIN continues working on this problem with people from Eindhoven University of Technology. Ingo Drummen hopes to come back to the study group next year: "It is good to have a week of intense contact and then work together in the long run for more depth."

This is a brief report on the Study Group Mathematics with Industry, held from 30 January to 3 February 2012 at Eindhoven University of Technology. The scientific proceedings are available on www.eurandum.nl/events/workshops/2012/SWI_2012.

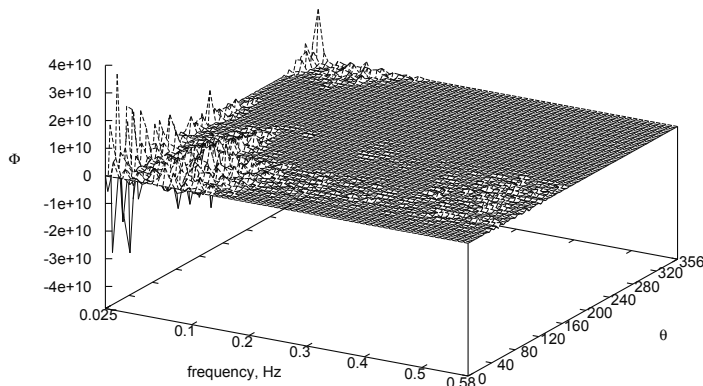


Figure 1 At the first try the least squares method found a solution with negative values. This might theoretically be the best solution for the given data, but in reality the response of the ship cannot be negative. Therefore a constrained least squares method was used that only returns positive solutions.

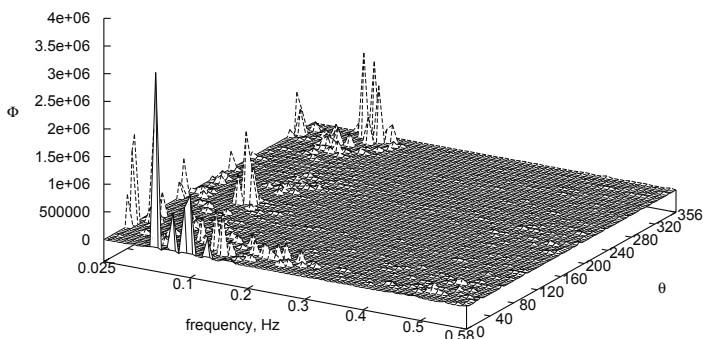


Figure 2 The resulting solution was very, very spiky. For a small change in the frequency or angle of the incoming wave, there would suddenly be a very strong reaction from the vessel. But the actual relation has to be smooth; changing the waves a bit should only change the reaction of the ship a bit.

Boekbesprekingen

| Book Reviews

Redactie: Hans Cuypers en Hans Sterk

Review Editors NAW - MF 5.101
Faculteit Wiskunde & Informatica
Technische Universiteit Eindhoven
Postbus 513
5600 MB Eindhoven
reviews@nieuwarchief.nl
www.win.tue.nl/wgreview



Enrico Arbarello, Maurizio Cornalba,
Phillip A. Griffiths

Geometry of Algebraic Curves

Grundlehren der mathematischen Wissenschaften, Volumen 268

Springer, Heidelberg, 2011

xxx + 963 p., prijs €95,35

ISBN 9783540426882

Dit boek met de enorme omvang van bijna duizend pagina's is het langverwachte vervolg op het eerste deel, dat in 1985 werd gepubliceerd als nummer 267 in de reeks 'Grundlehren der Mathematischen Wissenschaften' van Springer. Volume II is pas recent gepubliceerd, en wel als nummer 268, een plek in de reeks die kennelijk al die tijd door de uitgever is vrijgehouden.

Volume I sprong destijds in op belangrijke ontwikkelingen die er toen waren in de studie van complexe algebraïsche krommen, met name op het gebied van de (Brill–Noether-) theorie van (speciale) lineaire systemen. Het boek uit 1985 geeft van deze theorie een fraai overzicht, voorafgegaan door een uitgebreide inleiding op de theorie van complexe algebraïsche krommen en hun jacobianen.

Zoals aangekondigd in het voorwoord van Volume I, zou in Volume II het perspectief worden verlegd van de theorie van lineaire systemen voor een vaste onderliggende kromme naar de theorie voor krommen die veranderen in moduli. Zoals wellicht bekend kan een (gladde, projectieve, complexe) kromme beschouwd worden als een compact oriënteerbaar oppervlak, voorzien van een complexe differentieerbare structuur van dimensie één, dat wil zeggen, als een compact Riemannoppervlak. Door het onderliggende oppervlak (dat wordt gekarakteriseerd door zijn geslacht — het aantal 'hendels') vast te houden, maar de complexe structuur te variëren, verkrijgen we continue families van krommen, waarbinnen de structuur van de bijbehorende speciale lineaire systemen kan veranderen.

Wat de auteurs kennelijk niet hadden verwacht is dat de theorie van moduli van krommen vanaf halverwege jaren tachtig een enorme vlucht zou nemen. De theorie dijde uit in veel en vaak onverwachte richtingen. Zo is het onderwerp bijvoorbeeld de theoretische natuurkunde binnengedrongen, wat leidde tot spectaculaire nieuwe inzichten; een van de voorlopige hoogtepunten is zonder twijfel Kontsevich' bewijs (verkregen in zijn proefschrift uit 1992, waarmee hij de basis legde voor de latere toekenning van de Fields-medaille in 1998) van het Witten-vermoeden, waarmee opmerkelijke verbanden worden gelegd tussen snijtheorie op de moduli-ruimte van (stabiele) krommen aan de ene kant, en de KdV-hiërarchie aan de andere kant, gebruikmakend van methoden die toebehoren aan de topologie en de combinatoriek.

Doordat de ontwikkelingen zich in een zo snel tempo opstapelden, en zich veel verder uitstrekten dan alleen over Brill–Noether-theorie, werd het samenstellen van Volume II door de auteurs jarenlang naar voren geschoven. Uiteindelijk hebben de auteurs toch de tijd rijp geacht voor het schrijven van het vervolg, met als resultaat een kloek boek dat in zeer brede zin de theorie van de moduli-ruimte van (stabiele) krommen opzet, en in latere hoofdstukken een aantal specifieke moderne aspecten van deze theorie nader belicht.

Natuurlijk moesten er keuzes worden gemaakt, maar de presentatie zoals die er nu staat is bijna perfect uitgebalanceerd: deze gaat van fundamentele naar recente onderzoeksresultaten, en varieert wat betreft aanpak behendig tussen algebraïsch-meetkundige technieken (Hilbert-schema's, deformatietheorie, algebraïsche ruim-

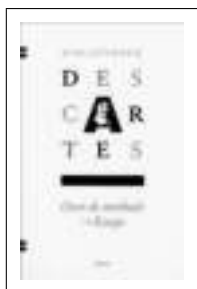
tes en stacks), topologische en combinatorische technieken (celdecomposities, bandgrafen) en reëel- en complex-analytische technieken (Teichmüller-theorie).

Een greep uit de onderwerpen: stabiele reductiestelling, lijnbundels op de moduli-ruimte, bewijs dat de moduli-ruimte van stabiele krommen projectief is, Galois-overdekkingen van de moduli-ruimte, structuur van de tautologische ring, verdwijnstellingen voor de cohomologie (een discussie gebaseerd op de dan al eerder ingevoerde celdecompositie), en uiteindelijk Kontsevich' bewijs van het Witten-vermoeden.

Het allerlaatste hoofdstuk XXI is ten slotte nog gewijd aan de 25 jaar eerder aangekondigde Brill–Noether-theorie in veranderende moduli, maar dit hoofdstuk ademt zeker niet de diepte en moderne insteek van alle overige hoofdstukken. Wat overigens door de auteurs wordt onderkend, met hun typering van de sfeer van dit hoofdstuk als 'archeologisch'.

Dit boek is onmisbaar voor iedereen die zich op de hoogte wil stellen van de huidige stand van zaken in de theorie van moduli van krommen. Stijl en notatie zijn bijzonder prettig, en de auteurs nemen de tijd, ook bij de meer technische gedeeltes, om de ideeën helder en rustig uit te leggen. De tekst wordt aangevuld met een enorme collectie aan opgaven, voor het overgrote deel van de hand van Joe Harris, aanwijzingen voor verdere kennismakingen met de literatuur, en een uitgebreide literatuurlijst die maar liefst 695 items omvat.

Robin de Jong



René Descartes
Over de methode – Essays

vertaling Jeanne Holierhoek
Bibliotheek Descartes, Band 3
Uitgeverij Boom, 2011
570 p., prijs €39,90
ISBN 9789085066590

De publicatie van het werk *Geometrie* (oorspronkelijke titel: *La Géométrie*) door René Descartes in 1637 is een mijlpaal in de geschiedenis van de wiskunde omdat dit het begin van de analytische meetkunde markeert. In het werk legt Descartes een verband tussen meetkundige figuren en algebraïsche vergelijkingen en dat betekent dat meetkundige problemen kunnen worden opgelost door gebruik te maken van algebraïsche technieken, en omgekeerd. Bovendien is *Geometrie* een belangrijk werk vanuit het oogpunt van wiskundige notatie: hier worden voor het eerst de letters x en y gebruikt voor onbekenden in een algebraïsche vergelijking. Er wordt wel bewezen dat *Geometrie* het eerste voor moderne wiskundigen leesbare wiskundeboek uit de geschiedenis is.

Oorspronkelijk was *Geometrie* een van de drie essays behorende bij Descartes' verhandeling *Over de methode* (oorspronkelijke titel: *Discours de la méthode*). Hiervan is nu de eerste moderne uitgave in het Nederlands verschenen waarbij de tekst wordt gepresenteerd in zijn oorspronkelijke vorm. Deze publicatie is het derde deel uit de Bibliotheek Descartes, het ambitieuze project om een moderne Nederlandse vertaling te bezorgen van de werken en correspondentie van Descartes. Het boek bevat eerst een inleiding op *Over de methode* geschreven door Han van Ruler. Dan volgt de daadwerkelijke vertaling van *Over de methode* met de drie essays, van de hand van Jeanne Holierhoek. Ten slotte is een nawoord opgenomen waarin Henk Bos dieper ingaat op de wiskundig-historische achtergrond van *Geometrie*.

Holierhoek is erin geslaagd de oorspronkelijke tekst te vertalen naar

een zeer goed leesbare moderne Nederlandse tekst. Daarbij heeft ze wiskundige termen en concepten juist vertaald. Opvallend is dat ervoor gekozen is om de notatie van de vele formules niet te moderniseren. Hierdoor blijft het originele karakter van de tekst bewaard.

De moderne wiskundige die in *Geometrie* een handboek over de analytische meetkunde verwacht aan te treffen, komt bedrogen uit. Want naast herkenbare wiskunde en formules bevat het werk ook formuleringen en ideeën die tegenwoordig niet meer gangbaar zijn, en die eerder verwondering dan herkenning zullen oproepen. Het nawoord van Henk Bos gaat in op deze spanning. Bos stelt terecht dat het voor een goed begrip belangrijk is om niet enkel de blijvende resultaten te beschouwen, maar om ook aandacht te schenken aan de vraagstukken die tijdens het leven van Descartes in het middelpunt van de wiskundige belangstelling stonden. Dit waren immers de vraagstukken die Descartes motiveerden om zijn werk te schrijven. Volgens Bos gaat het hierbij om twee grote kwesties: (1) Hoe mag men een meetkundig probleem oplossen als passer en liniaal niet lijken te voldoen?, en (2) Het ontbreken van een algemene methode voor het oplossen van meetkundige problemen. In een uitermate helder en scherpzinnig betoog zet Bos vervolgens uiteen hoe deze vraagstukken Descartes inspireerden en welke antwoorden Descartes heeft gevonden.

Het boek geeft de wiskundig geïnteresseerde lezer toegang tot een goede en leesbare moderne Nederlandse vertaling van Descartes' *la Géométrie*. Het inzichtelijke nawoord plaatst het werk in de tijd en geeft de lezer waardevolle handvatten om het werk beter te kunnen begrijpen en duiden.

Jantien Dopper



Kevin Houston
How to Think Like a Mathematician

Cambridge University Press, 2009
265 p., prijs £20.99
ISBN 9780521719780

De aanvang van een wiskundestudie gaat nogal eens gepaard met een cultuurschok veroorzaakt door onbekendheid met het wiskundig denken. Wiskundigen weten dat je wiskunde leert door het te doen, niet door te leren hoe je het moet doen als je het gaat doen. Het onderwijs moet wel zo zijn dat deze 'natuurmethode' het gewenste effect kan hebben. Daar ontbreekt het wel eens aan. Dat is de motivatie voor het schrijven van dit boek geweest. Er worden onderwerpen behandeld die de auteur in zijn studie gemist heeft: "I wish someone had told me that earlier."

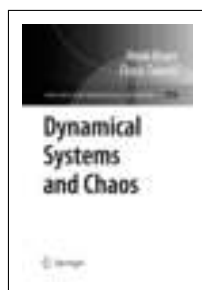
Dit boek heeft een ondertitel: 'A Companion to Undergraduate Mathematics'. Het is bedoeld als hulp bij de studie, niet om zo een nieuw wiskundevak te introduceren. Het gaat over de taal der verzamelingen en functies, hoe wiskundeteksten te lezen, het logisch redeneren, definities, stellingen, bewijzen. Het besluit met enige wiskunde waar alle wiskundigen vertrouwd mee moeten zijn, zoals het algoritme van Euclides, modulo rekenen, de begrippen injectief en surjectief. Als het goed is, is er in het eerste semester van een wiskundeopleiding minstens één vak waarbij je je dit allemaal al doende eigen maakt. Werkcolleges zijn daarbij onmisbaar. Let wel: ik bedoel een echt wiskundevak. Is er zo'n vak, dan is dit boek niet nodig.

Voor iemand met enige ervaring in het geven van wiskundeonderwijs zijn veel adviezen in dit boek zeer herkenbaar: over het gebruik van

implicaties, over de rol van voorbeelden en tegenvoorbeelden, over de betekenis van ‘als’ in een definitie, en nog heel veel meer. Over het algemeen zijn het waardevolle adviezen. Een paar niet zo heel belangrijke zaken vind ik wat minder gelukkig. Zelf hamer ik er altijd op dat het symbool $\Rightarrow$ niet als ‘dus’ moet worden gebruikt. De auteur gebruikt het wel op die manier, hoewel hij de echte betekenis ervan goed geeft. Hij adviseert om uitspraken die moeten gelden voor alle natuurlijke getallen te bewijzen met volledige inductie. Een beter advies lijkt mij om als het even kan volledige inductie niet te gebruiken. Voor veel studenten is het gebruik van volledige inductie een soort pavlovreactie, en dat geldt ook voor het bewijzen uit het ongerijmde.

Een waardevol boek voor studenten van een wiskundeopleiding die wat te wensen overlaat. Ervaart een tweedejaars student deze tekst als leerzaam, dan heeft hij/zij wel wat gemist.

Frans Keune



Henk Broer, Floris Takens
Dynamical Systems and Chaos

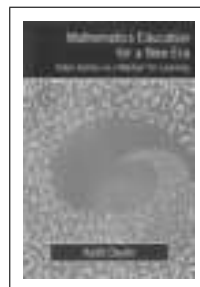
Applied Mathematical Sciences, Volume 172
Springer, Heidelberg, 2011
xvi + 313 p., prijs €63,55
ISBN 9781441968692

A brief introduction in the contents of this book can be found at the back cover: “Over the last four decades there has been extensive development in the theory of dynamical systems. This book starts from the phenomenological point of view reviewing examples. Hence the authors discuss oscillators, like the pendulum in many variations including damping and periodic forcing, the Van der Pol System, the Henon and Logistic families, the Newton algorithm seen as dynamical system and the Lorenz and Rossler system are also discussed. The phenomena concern equilibrium, periodic, multi- or quasi-periodic and chaotic dynamics as these occur in all kinds of modeling and are met both in computer simulations and in experiments. The application areas vary from celestial mechanics and economical evolutions to population dynamics and climate variability. The book is aimed at a broad audience of students and researchers. The first four chapters have been used for an undergraduate course in Dynamical Systems and material from the last two chapters and from the appendices has been used for master and PhD courses by the authors. All chapters conclude with an exercise section. One of the challenges is to help applied researchers acquire background for a better understanding of the data that computer simulation or experiment may provide them with the development of the theory.”

Indeed this positions the text well and forms, together with the reputation of the authors, an excellent motivation to study the book. There are today numerous books dealing with either dynamical systems and/or chaos but this one stands out in many ways. Its scope, depth and breath give it a feeling of a must read. However, the work falls short at one point, at least in my opinion, namely it attempts to be complete. Appendices of a few pages covering topology or differentiable manifolds or measure theory seem too ambitious for non-experts. In the same vain, I was surprised to see some typical partial differential equations reviewed, albeit the book mostly focuses on the more common ordinary differential equation type of systems. The exercises per chapter run from simple and straightforward to extended research questions forming time-consuming open challenges for the interested reader. All

in all a great text written in a very good style for which the authors deserve to be complemented. It is with sadness to mention that Floris Takens passed away before this book was finally delivered to the scientific community; it definitely forms a lasting account of some of his work on dynamical systems and chaos.

Henk Nijmeijer



Keith Devlin
**Mathematics Education for a New Era:
Video Games as a Medium for Learning**

A.K. Peters, Ltd/CRC Press, 2011
xiii + 203 p., prijs £26.99
ISBN 9781568814315

Recent bracht Keith Devlin (Stanford Universiteit), bekend van zijn nieuwsbrief en popularisering van de wiskunde, met zijn bedrijf Innertubegames een computerspel (app) voor de iPad uit genaamd Wuzzit Trouble (innertubegames.net). De game heeft verbanden met, zonder dit te benoemen, lineaire Diophantische vergelijkingen en bouwt voort op principes in Devlins boek over computerspellen en wiskunde, waarin Devlin uitlegt waarom computerspellen een ‘ideaal’ medium zijn om wiskunde in het voortgezet onderwijs aan te leren. Het boek behandelt in twaalf hoofdstukken onderwerpen als straatwiskunde in Brazilië, wiskundig denken, computerspellen en hoe deze kunnen bijdragen aan het leren van wiskunde, en eindigt met aanwijzingen voor succesvolle onderwijskundige computerspelletjes. Het boek heeft twee doelstellingen: 1. Het starten van een discussie in de wereld van het wiskundeonderwijs hoe deze voordeel kan halen uit de mogelijkheden van games in het onderwijs. 2. De lezer ervan te overtuigen dat goed ontworpen games een belangrijke rol gaan spelen in ons toekomstige wiskundeonderwijs, vooral in het voortgezet onderwijs. Naar mijn mening slaagt Devlin in het eerste door er überhaupt een boek over te schrijven. De tweede doelstelling komt naar mijn mening minder uit de verf. Ten eerste hanteert Devlin een wat onduidelijke definitie van ‘mathematical thinking’: eerst is het ‘simplificeren’, vervolgens ‘wat een wiskundige doet’, daarna weer wat anders. Gelukkig houdt Devlin wat slagen om de arm en ontkracht hij zijn eigen uitspraken later weer. Helaas boet daarmee ook de kracht van het betoog in. Bij tijd en wijle komt het boek over als een losse verzameling uitspraken die in dienst staan van de rode draad door het boek. Ten tweede is het boek erg gericht op de Verenigde Staten. Regelmatig worden impliciet uitdagingen in het wiskundeonderwijs in de Verenigde Staten beschreven, die in Europa wellicht minder relevant zijn. Dit verklaart misschien ook het overmatige gebruik van superlatieven als ‘het perfecte medium’. Bij dergelijke boude uitspraken verwacht je een goede onderbouwing. Dit is niet altijd het geval, bijvoorbeeld als Devlin het heeft over “to young players who have grown up in an era of multimedia multitasking, this is no problem at all” (p. 141) of “In fact, technology has now rendered obsolete much of what teachers used to do” (p. 181). Devlins ervaringen met de game World of Warcraft zijn aardig, maar anekdotisch en eenzijdig, aangezien er meer soorten games zijn. Daarnaast valt hieraan ook te zien dat de gameswereld snel verandert, een nadeel van een papieren boek uit 2011. Devlin schreef een origineel, maar weinig onderbouwd, boek over een onderwerp dat maatschappelijk steeds actueler gaat worden. Als fervente speler van games zie ook ik hoe computerspellen de wereld hebben veroverd. Het zou prachtig zijn als wiskunde een fractie van de daarmee gemoeide motivatie, bronnen

en/of concentratie kan aanboren. Het is voor mij duidelijk dat dit alleen kan met behoedzaam en gedegen onderzoek. *Christian Bokhove*



G. Frei, P. Roquette unter Mitwirkung von F. Lemmermeyer (Hg.)

**Emil Artin und Helmut Hasse
Die Korrespondenz 1923-1934**

Universitätsverlag Göttingen, 2008

499 p., prijs € 37,00

ISBN 9783940344502

Dit boek is een vermeldenswaardige metgezel van het boek getiteld *Helmut Hasse und Emmy Noether, Die Korrespondenz 1925-1935* dat in NAW 5/8, september 2007, p. 231, gerecenseerd staat. De opzet van het huidige boek is ongeveer gelijk aan die van zijn voorganger, maar er zijn verschillen. Zo is dit boek opgedeeld in drie stukken.

In het eerste stuk, getiteld 'Vorspann' (58 pagina's) treffen we een overzicht aan van Artins leven en werk, vergezeld van een bijzonder goede inleiding over het tijdsgewricht en de personen die daarbij een rol spelen. Dan komen herinneringen aan Hasse aan bod, zoals beleefd door Frei, en vervolgens een stevige dot wiskunde over reciprociteitsstellingen voor machtesten en over klassenlichamentheorie. Tot slot van het eerste stuk wordt een chronologisch overzicht van ontwikkelingen ervan gegeven en uitgewerkt.

In het tweede stuk, getiteld 'Die Briefe' (397 pagina's) treffen we de 49 brieven van Artin aan Hasse aan; in omgekeerde richting schijnt alles verloren gegaan te zijn, maar vaak is duidelijk, vanwege het geschrevene in de richting Artin naar Hasse, wat de inhoud geweest zou hebben kunnen zijn. Alles is voorzien van uitgebreid commentaar en essays door Frei, Roquette en Lemmermeyer. Het tweede stuk heeft eenzelfde opbouw als het eerdere boek. Ook hier passeren alle ontwikkelingsfasen en personages uit het betrokken tijdvak de revue, daar waar het de algebraïsche getaltheorie betreft. Excellent, commentaar van mijn zijde is feitelijk overbodig. Om in horecatermen te spreken: vijf sterren, eenzame klasse.

Het derde, laatste, stuk bevat een namenoverzicht van de personen die in het boek voorkomen (5 pagina's), een trefwoordenregister (10 pagina's), een literatuuroverzicht (28 pagina's) en een bladzijde met gegevens over figuren.

Al dit moois kan men kosteloos downloaden, maar veel beter en logischer is het om dit boek als écht boek zelf aan te schaffen. *Robert van der Waall*



Alan H. Schoenfeld (ed.)

Assessing Mathematical Proficiency

Mathematical Sciences Research Institute Publications 53

Cambridge University Press, 2007

391 p., prijs £21.99

ISBN 9780521697668 (Paperback)

In Nederland woedt de laatste jaren een felle discussie over de wiskundige vaardigheden die in het onderwijs aangeleerd worden en hoe deze getoetst moeten worden. In het heetst van deze strijd wordt nog wel eens de indruk gewekt dat hier sprake is van ontwikkelingen die uniek

zijn voor ons land en voor deze tijd. Het kan dan verfrissend zijn om eens over de muren van tijd en plaats te kijken. Dit kan onder andere met het boek *Assessing Mathematical Proficiency* (Toetsen van wiskundige vaardigheden), een conferentiebundel onder redactie van Alan Schoenfeld, met bijdragen van wiskundigen, onderwijsonderzoekers, toetsontwikkelaars en beleidsmakers over het toetsen van wiskundige vaardigheden. Een belangrijke aanleiding voor de conferentie was de invoer in de Verenigde Staten van landelijke onderwijsstandaarden en bijpassende gestandaardiseerde toetsen onder de wet No Child Left Behind (volgens Sir Ken Robinson het tegenvoorbeeld voor de stelling dat Amerikanen geen gevoel voor ironie hebben...). De belangen van deze toetsen voor leerlingen, leraren, scholen en beleidsmakers zijn bijzonder groot. Dit leidt tot twee elkaar versterkende processen. Ten eerste worden hierdoor zeer hoge eisen gesteld aan de validiteit en betrouwbaarheid van deze toetsen waardoor alleen die aspecten van wiskundige vaardigheid getoetst worden die op die manier getoetst kunnen worden. Vervolgens ontstaat er een grote druk op leraren om alleen deze aspecten in het onderwijs terug te laten komen (teaching to the test). In het boek wordt stilgestaan bij de vraag waaruit wiskundige vaardigheid bestaat, welke vormen van toetsing passen bij welke aspecten van wiskundige vaardigheid en hoe je deze toetsing zo kunt organiseren dat leerlingen en leraren ervan leren. Dit alles wordt rijk geïllustreerd aan de hand van voorbeelden uit de toetspraktijk van verschillende scholen (primair en voortgezet onderwijs) in verschillende landen. Een van de meest inzichtelijke voorbeelden is het transcript van een interview van Deborah Ball met een leerling over zijn kennis van breuken, waarin duidelijk wordt wat er allemaal bij komt kijken om breuken te begrijpen en ermee te kunnen rekenen. Dit is een complexiteit waaraan een gestandaardiseerde toets (alleen) geen recht doet. Het is ook deze complexiteit die soms ontbreekt in de discussie hier te lande. *Willem Hoekstra*



Helmut Schwichtenberg,

Stanley S. Wainer

Proofs and Computations

Perspectives in Logic

Cambridge University Press, 2012

xiii + 465 p., prijs £55.00

ISBN 9780521517690

We zouden heel blij moeten zijn met dit boek. Hoewel er op het gebied van de Bewijstheorie aardig wat op de markt is, ken ik geen ander boek waarin *alle* klassieke resultaten van deze discipline worden behandeld; en dat bovendien zonder de doorgaans loodzware notaties waar de meeste auteurs niet buiten lijken te kunnen. Het is ook leesbaarder dan *Basic Proof Theory* van Troelstra en Schwichtenberg (dat overigens een heel andere invalshoek heeft).

Bewijstheorie is de studie van *formele bewijzen*, dat zijn structuren die volgens stricte regels zijn opgebouwd en die wiskundige redeneringen weergeven. Een van de eerste resultaten is dat zulke structuren altijd zijn te transformeren tot een zogenaamde *normaalkvorm*. Uit een formeel bewijs in normaalvorm valt vaak veel meer informatie te halen dan alleen de wetenschap dat de conclusie een ware uitspraak is: vaak kan men uit zo'n bewijs ook een *algoritme* construeren. Formele bewijzen kunnen worden geanalyseerd vanuit het oogpunt van *complexiteit*, en een moderne toepassing van formele bewijsstructuren is dat ze gegenereerd kunnen worden door computers: het terrein van de

‘automated theorem proving’. De bewijstheorie vindt zijn oorsprong in het denken van David Hilbert, en voor een razendsnelle introductie verwijs ik de lezer naar Benno van den Bergs lichtvoetige artikel ‘Hilbert en de bewijstheorie’ in NAW 5/14, maart 2013.

In de eerste vijf hoofdstukken komen grofweg aan de orde: formele bewijsbomen met natuurlijke deductie (geïntroduceerd door Gentzen), normalisatie en de stelling van Herbrand (die merkwaardigerwijs niet als zodanig wordt genoemd), de theorie van algoritmen à la Turing (recursietheorie), de Onvolledigheidsstellingen van Gödel, Gentzens analyse van de consistentie van eerste-orde-rekenkunde via het ordinaalgetal ε_0 , en uitbreidingen hiervan tot subsystemen van tweede-orde-rekenkunde.

In het laatste deel komen recentere ontwikkelingen ter sprake die te maken hebben met constructieve wiskunde: abstracte berekenbaarheid in hogere typen middels ‘information systems’, ‘realizability’ en de Dialectica-vertaling, Gödels systeem T . Over dit deel ben ik wat minder enthousiast: de presentatie weerspiegelt de hobby’s van de auteurs, en een hoop van dit materiaal is ook goed te vinden in andere, oudere publicaties (zoals het onvolprezen *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis* onder redactie van Troelstra (Springer Lecture Notes in Mathematics 344, 1973). Verder kunnen we een behandeling van realizability die het standaardwerk *Realizability: an Introduction to its Categorical Side* (Studies in Logic, vol. 152, North-Holland, 2008) van ondergetekende niet eens *noemt*, natuurlijk niet serieus nemen...

Zeker, als de auteurs in hun voorwoord zeggen dat het eerste deel (hoofdstukken 1 t/m 3) de basis zou kunnen zijn voor een éénjarige cursus op masterniveau, dan ben ik dat met ze eens. Mits kundig begeleid.

Want als we in detail naar de behandeling van een aantal onderwerpen kijken, dan valt toch op dat het de lezer niet altijd even makkelijk wordt gemaakt. Allereerst is de stijl nogal stroef, wat mogelijk te maken heeft met de leeftijd van de auteurs (beiden emeriti). Zo begint sectie 1.1 (Natural deduction) met het weinig verhelderende “Rules come in pairs” (ik moet hier denken aan wijlen Professor Löb, een van de twee personen aan wier nagedachtenis dit boek is opgedragen, en van wie ik ook nog even college gehad heb; diens dictaat Logica begon met het kryptische “zij ϕ een tekenrijtje”). Soms is er sprake van onnodig moeilijk gedoe: de “transfinite induction on the well-founded partial order $\rightarrow^+$ ” kan gemakkelijk vervangen worden door gewone inductie over natuurlijke getallen. Het gebruik van niet-gedefinieerde (en geen precieze betekenis hebbende) pseudo-wiskunde als ‘local maximum’ in de behandeling van normalisatie, is oninformatief. De intuïtief bedoelde uitleg van een bewijs in normaalvorm als bewijs dat “does not make detours” (p. 20) is regelrecht misleidend, omdat we later zullen zien dat zulke bewijzen vaak veel langer zijn dan niet-normale bewijzen!

Behalve dat, worden begrippen regelmatig al gebruikt voordat ze gedefinieerd zijn (of zonder dat er ergens een definitie staat). Een paar voorbeelden: het begrip ‘normal derivation’ wordt gebruikt op p. 28 terwijl de Index hiervoor p. 40 geeft, waar men overigens de definitie niet vindt. In hoofdstuk 4 wordt op p. 154 een argument ‘by inversion’ gebruikt zonder nadere verklaring. Dit is een begrip dat voortkomt uit snede-eliminatie, maar dat is nu juist iets dat nog niet behandeld is. Op p. 162 vinden we ‘ ε_0 -recursive functions’ zonder vooruitwijzing naar de plaats waar ze ingevoerd worden.

Ik zou hiermee door kunnen gaan, maar dat zou niet fair zijn. Ik ben werkelijk erg blij met dit boek.

Jaap van Oosten

Recent verschenen publicaties. Als u een van deze boeken wil bespreken of als u suggesties heeft voor andere boeken voor deze rubriek, laat dit dan per e-mail weten aan reviews@nieuwarchief.nl.



Fetsje Bijma, Marianne Jonker, Aad van der Vaart

Inleiding in de statistiek

Epsilon Uitgaven, deel 76, 2013

ISBN 9789050411356

www.epsilon-uitgaven.nl/E76.php



Dirk van Dalen

L.E.J. Brouwer – van Mystiek tot Wiskunde

Epsilon Uitgaven, deel 74, 2013

ISBN 9789050411332

www.epsilon-uitgaven.nl/E74.php



A.C.M. van Rooij, B. de Pagter

An invitation to functional analysis

Epsilon Uitgaven, deel 75, 2013

ISBN 9789050411349

www.epsilon-uitgaven.nl/E75.php



Barteld Kooi, Hans van Ditmarsch

Honderd gevangenen en een gloeilamp

Epsilon Uitgaven, deel 73, 2013

ISBN 9789050411325

www.epsilon-uitgaven.nl/E73.php



Jacob P. Murre, Jan Nagel, Chris A.M. Peters
Lectures on the theory of pure motives

American Mathematical Society, 2013
 ISBN 9780821894347
www.ams.org/bookstore-getitem/item=ulect-61



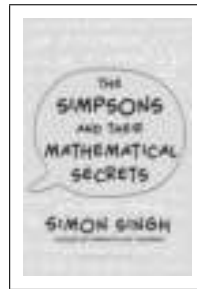
Kenneth Falconer
Fractals: A Very Short Introduction

Oxford University Press, 2013
 Very Short Introductions
 ISBN 9780199675982
ukcatalogue.oup.com/product/9780199675982.do



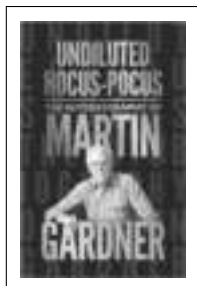
Dana Mackenzie
What's Happening in the Mathematical Sciences, Volume 9

American Mathematical Society, 2013
 ISBN 9780821887394
www.ams.org/bookstore-getitem/item=happening-9



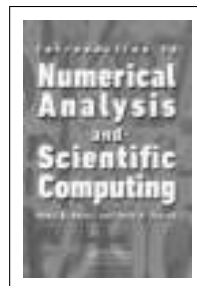
Simon Singh
The Simpsons and Their Mathematical Secrets

Bloomsbury Publishing, 2013
 ISBN 9781408835302
www.bloomsbury.com/9781408835302



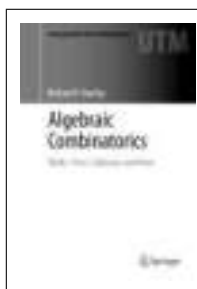
Martin Gardner
Undiluted Hocus-Pocus: The Autobiography of Martin Gardner

Princeton University Press, 2013
 ISBN 9780691159911
press.princeton.edu/titles/10066.html



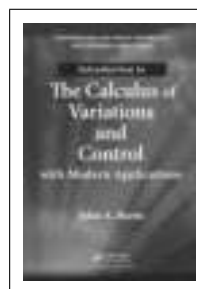
Nabil Nassif, Dolly Khuwayri Fayyad
Introduction to Numerical Analysis and Scientific Computing

Taylor & Francis, 2013
 ISBN 9781466589483
www.taylorandfrancis.com/9781466589483



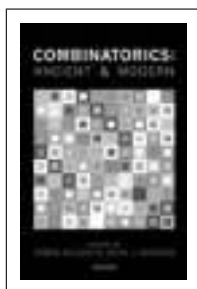
Richard P. Stanley
Algebraic Combinatorics

Springer, 2013
 Undergraduate Texts in Mathematics
 ISBN 9781461469971
www.springer.com/978-1-4614-6997-1



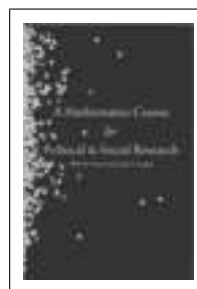
John A. Burns
Introduction to the Calculus of Variations and Control with Modern Applications

Taylor & Francis, 2013
 ISBN 9781466571396
www.taylorandfrancis.com/9781466571396



Robin Wilson, John J. Watkins
Combinatorics: Ancient & Modern

Oxford University Press
 ISBN 9780199656592
ukcatalogue.oup.com/product/9780199656592.do



Will H. Moore, David A. Siegel
A Mathematics Course for Political and Social Research

Princeton University Press, 2013
 ISBN 9780691159171
press.princeton.edu/titles/10143.html

Problemen

| Problem Section

This Problem Section is open to everyone; everybody is encouraged to send in solutions and propose problems. Group contributions are welcome.

For each problem, the most elegant correct solution will be rewarded with a book token worth €20. At times there will be a Star Problem, to which the proposer does not know any solution. For the first correct solution sent in within one year there is a prize of €100.

When proposing a problem, please either include a complete solution or indicate that it is intended as a Star Problem. Electronic submissions of problems and solutions are preferred (problems@nieuwarchief.nl).

The deadline for solutions to the problems in this edition is 1 March 2014.

Problem A (folklore, communicated by Jaap Top)

Does there exist an integer $n > 1$ such that the set of leading digits of $2^n, 3^n, \dots, 9^n$ is equal to $\{2, 3, \dots, 9\}$?

Problem B (proposed by Bart de Smit and Hendrik Lenstra)

Rings are unital, and morphisms of rings send 1 to 1.

Let A and B be commutative rings. Suppose that there exists a ring C such that there are injective morphisms $A \rightarrow C$ and $B \rightarrow C$ of rings. Show that there exists a *commutative* such ring.

Problem C (proposed by Jinbi Jin)

Let $C(\mathbb{R}, \mathbb{R})$ denote the set of continuous maps from $\mathbb{R}$ to itself. A (not necessarily continuous) map $f: C(\mathbb{R}, \mathbb{R}) \rightarrow C(\mathbb{R}, \mathbb{R})$ is called *good* if it satisfies, for all $s, t \in C(\mathbb{R}, \mathbb{R})$, the identity

$$f(s \circ t) = f(s)f(t),$$

where the product on the right hand side is the point-wise multiplication of maps.

- Find a non-constant good map $f: C(\mathbb{R}, \mathbb{R}) \rightarrow C(\mathbb{R}, \mathbb{R})$.
- Show that $f(\exp) = 0$ for all non-constant good maps $f: C(\mathbb{R}, \mathbb{R}) \rightarrow C(\mathbb{R}, \mathbb{R})$. (Here, $\exp$ is given by $x \mapsto e^x$.)

Edition 2013-2 We received solutions from Leon van den Broek (Nijmegen), Alex Heinis (Amsterdam), Jos van Kan (Delft), Thijmen Krebs (Nootdorp), Javier Sánchez-Reyes (Castilla-La Mancha, Spain) and Ángel Plaza (Las Palmas de Gran Canaria, Spain), and Robert van der Waall (Huizen).

Problem 2013-2A (based on a problem proposed by Gerard Renardel de Lavalette)

We have two hourglasses, A for a seconds and B for b seconds, where a and b are relatively prime integers and $0 < a < b$. Let t_0 be an integer with $t_0 \geq b + (\frac{1}{2}a - 1)^2$. Show that A and B can be used to identify the time $t = t_0$ if the upper bulbs are empty at $t = 0$.

Remark. The original problem received from the proposer was to prove a slightly stronger result. Let m be the remainder of b upon division by a . The original problem was to prove that for any integer $t_0 > b + m(a - m) - a$, the time $t = t_0$ can be identified using A and B .

Solution We received only one correct solution, from Thijmen Krebs, who will receive the book token. The following solution is based on that solution.

Let m be the remainder of b upon division by a . For any integer T that is a multiple of a or b , we can use the following strategy:

- while $t < T$, turn each hourglass whenever it is empty;
- while $t \geq T$, turn *both* hourglasses whenever at least one is empty.

If we apply this strategy to $T = b$, then we turn both hourglasses at the times $t = b + km$ for $k = 0, 1, 2, \dots$

Redactie:

Johan Bosman

Gabriele Dalla Torre

Christophe Debry

Jinbi Jin

Marco Streng

Wouter Zomervrucht

Problemenrubriek NAW

Mathematisch Instituut

Universiteit Leiden

Postbus 9512

2300 RA Leiden

problems@nieuwarchief.nl

www.nieuwarchief.nl/problems

If we apply this strategy to $T = a(1 + \frac{b-m}{a}) = b + (a - m)$, then we turn both hourglasses at the times $t = b + k(a - m)$ for $k = 1, 2, 3, \dots$

In particular, all elements of the following set are measurable times:

$$S = \{b + km : 0 \leq k < a - m\} \cup \{b + k(a - m) : 0 < k \leq m\}.$$

As a and b are coprime, so are m and a , hence S contains an element of each residue class modulo a . Moreover, the maximal element of S is $b + m(a - m)$.

Before starting the strategy above, we can measure any non-negative integer multiple of a seconds using A , while letting B stay empty. In particular, we can measure any time $t_0 \geq b + m(a - m) - a + 1$.

Finally, note $m(a - m) \leq (\frac{1}{2}a)^2$, so $b + m(a - m) - a + 1 \leq b + (\frac{1}{2}a)^2 - a + 1 = b + (\frac{1}{2}a - 1)^2$ and we can measure any time $t_0 \geq b + (\frac{1}{2}a - 1)^2$.

Problem 2013-2B (folklore, communicated by Jeanine Daems)

In a two-player game, players take turns drawing a number of coins from a pile that starts with n coins. The first player takes at least one coin from the pile, but not all. In the subsequent turns, each player takes at least one coin, and at most twice the number of coins taken in the previous turn. The player who takes the last coin wins. For which numbers n can the first player win?

Solution We received correct solutions from Alex Heinis and Thijmen Krebs. The book token is awarded to Alex Heinis. The game is known as *Fibonacci Nim*, and the first player can win for those integers $n > 1$ that are not a Fibonacci number.

Let $(F_k)_{k \geq 1}$ be the Fibonacci sequence: $F_1 = 1$, $F_2 = 2$ and $F_{k+2} = F_{k+1} + F_k$ for $k \geq 1$. The proof uses *Zeckendorf's theorem*: every positive integer can uniquely be written as the sum of non-consecutive Fibonacci numbers. Let z be the function on the positive integers that assign to m the smallest Fibonacci number occurring in the Zeckendorf decomposition of m . E.g., we can write $20 = 13 + 5 + 2 = F_6 + F_4 + F_2$ and $z(20) = F_2 = 2$.

We define a position in this game to be a pair (m, d) where m is number of coins left on the pile and d the maximal number of coins that may be taken (by the player who is to move). The initial position is $(n, n - 1)$ and the final positions are those of the form $(0, d)$. Call a position (m, d) 'good' if it is non-final and $d \geq z(m)$; call it 'bad' otherwise.

Lemma. *Let (m, d) be a good position. There exists a move to a bad position.*

Proof. Write $m = F_{k_1} + \dots + F_{k_r}$ for the Zeckendorf decomposition, with $k_i \geq k_{i+1} + 2$. By assumption, d is at least F_{k_r} . Our move is to take exactly F_{k_r} coins. The new position is $(m - F_{k_r}, 2F_{k_r})$. This is a bad position: in the case $r = 1$ it is even final, and otherwise it follows from $2F_{k_r} < F_{k_{r-1}}$. $\square$

Lemma. *Let (m, d) be a non-final bad position. All moves lead to a good position.*

Proof. Write $F_k = z(m)$. By assumption we have $d < F_k$. Suppose we take x coins, for some $x \in \{1, \dots, d\}$. Let $t \geq 0$ be the even number such that $F_{k-t-2} \leq x < F_{k-t}$. Then

$$F_k - F_{k-t} < F_k - x \leq F_k - F_{k-t-2}$$

hence

$$F_{k-1} + F_{k-3} + \dots + F_{k-t+1} < F_k - x \leq F_{k-1} + F_{k-3} + \dots + F_{k-t-1},$$

so $z(F_k - x) \leq F_{k-t-1}$, which is smaller than $2F_{k-t-2} \leq 2x$. Note further that $z(F_k - x) = z(m - x)$. Hence $(m - x, 2x)$ is a good position. $\square$

Together the lemmas show that the good positions are exactly the winning ones. The initial position $(n, n - 1)$ is good if and only if $z(n) \leq n - 1$, i.e., if and only if n is not Fibonacci.

Problem 2013-2C (proposed by Bas Edixhoven and Maarten Derickx)

Let $ABCD$ be a convex quadrilateral inside a plane U in $\mathbb{R}^3$. Suppose that $ABCD$ is not a parallelogram. Show that there exist a plane V in $\mathbb{R}^3$ and a point $P \in \mathbb{R}^3 - (U \cup V)$ such that if a light source is placed in P , then the shadow of $ABCD$ on V is a square.

Solution We received solutions from Leon van den Broek, Alex Heinis, Jos van Kan, Javier Sánchez-Reyes and Ángel Plaza, and Robert van der Waall. The book token goes to Jos van Kan. The main idea of the solution is to pick the plane V and the point P in such a way that the projection on V of the intersection of the lines AB and CD , and that of BC and AD is ‘at infinity’. Some extra conditions on P related to the diagonals and consecutive edges will then ensure that the projection of $ABCD$ on V is a square.

If the lines AB and CD intersect, denote their intersection by X_1 . Similarly, if BC and AD intersect, denote their intersection by X_2 .

We consider three cases, the first of which is the following.

Case 1. The lines AB and CD intersect, and so do BC and AD . Moreover, both of AC and BD intersect the line X_1X_2 .

First note that X_1X_2 does not intersect the quadrilateral $ABCD$, as $ABCD$ is convex. Let Y_1 be the intersection of AC and X_1X_2 , and likewise, let Y_2 be the intersection of BD and X_1X_2 .

Let W be a plane that has as intersection the line X_1X_2 with U . In particular, $U \neq W$. Let Γ_1, Γ_2 be the circles in W with the segments $\overline{X_1X_2}, \overline{Y_1Y_2}$ as diameter, respectively. Let P be an intersection of Γ_1 and Γ_2 , and let V be any plane parallel to W such that the quadrilateral $ABCD$ lies between V and W . This intersection exists as one of Y_1, Y_2 lies between X_1 and X_2 , and the other does not.

Then note that P does not lie in U , as the points X_1, X_2, Y_1, Y_2 are pairwise distinct, and that P does not lie in V , as P lies in W , which is parallel to V . Hence $P \in \mathbb{R}^3 - (U \cup V)$.

Now let A_0, B_0, C_0, D_0 be the respective intersections of AP, BP, CP, DP with V . They exist, as the given lines intersect in P with W , which is parallel to V . By construction of V , and as X_1X_2 does not intersect the quadrilateral $ABCD$, it now suffices to show that $A_0B_0C_0D_0$ is a square in V .

Let l be a line in U , not equal to X_1X_2 . Write $\mathcal{P}(l)$ for the unique plane through l and P , write $\mathcal{I}(l)$ for the intersection line of W with $\mathcal{P}(l)$, and write $\mathcal{I}_0(l)$ for the intersection line of V with $\mathcal{P}(l)$. (So for example, $\mathcal{I}_0(AB) = A_0B_0$.) As V and W are parallel, it follows that for all lines l, m in U , the angle between $\mathcal{I}(l)$ and $\mathcal{I}(m)$ is equal to the one between $\mathcal{I}_0(l)$ and $\mathcal{I}_0(m)$. Note that a square is a quadrilateral such that

- every two successive edges are perpendicular, and
- the diagonals are perpendicular.

Therefore, to show that $A_0B_0C_0D_0$ is a square, it suffices to show that the $\mathcal{I}(e)$ (with e an edge or a diagonal of the quadrilateral $ABCD$) satisfy the above properties.

Now we simply note that

$$\mathcal{I}(AB) = \mathcal{I}(CD) = PX_1, \quad \mathcal{I}(BC) = \mathcal{I}(AD) = PX_2,$$

and that

$$\mathcal{I}(AC) = PY_1, \quad \mathcal{I}(BD) = PY_2,$$

so by construction of P , the quadrilateral $A_0B_0C_0D_0$ is a square, as desired.

For the remaining cases, we will only state them, and the corresponding construction of P , as the proof (and the construction of V) is done in the same way.

Case 2. The lines AB and CD intersect, and so do BC and AD . Moreover, at most one of AC and BD intersects the line X_1X_2 .

Note here that at least one of AC and BD intersects the line X_1X_2 , as AC and BD intersect, so exactly one of them intersects X_1X_2 . We assume without loss of generality that AC and

Oplossingen

| Solutions

X_1X_2 intersect, and let Y be their intersection. Note that Y lies between X_1 and X_2 , as the line AC intersects the segment $\overline{BD}$, which is parallel to X_1X_2 . Let W be any plane that has as intersection the line X_1X_2 with U , and let Γ be the circle in W with diameter $\overline{X_1X_2}$. Then we take P to be an intersection of Γ with the line through Y perpendicular to X_1X_2 .

Case 3. Exactly one of the pairs of lines (AB, CD) and (BC, AD) intersect.

We assume without loss of generality that AB and CD intersect, and let X denote this intersection. Let l be the line through X parallel to BC (hence also to AD). Then the lines AC and BD both intersect l , as they intersect BC . Let Y_1 and Y_2 be their respective intersections. Then X lies between Y_1 and Y_2 , as for S the intersection of AC and BD , the line XS intersects the segments $\overline{BC}$ and $\overline{AD}$, which are parallel to l . Let W be any plane that has l as intersection with U , and let Γ be the circle with diameter $\overline{Y_1Y_2}$. Then we take P to be an intersection of Γ with the line through X perpendicular to l .

References. This problem turned out to be rather well-known, as we received a lot of references. Thanks to Leon van den Broek, Javier Sánchez-Reyes and Ángel Plaza, and Robert van der Waall for these. The references given were, respectively,

- L. van den Broek, Welke schaduwbeelden, *Euclides* 64, nr. 3 (1988, in Dutch).
- Problem 72 of H. Dörrie, *100 great problems of elementary mathematics, their history and solution* (translation of *Triumph der Mathematik*, 1932), reworked in 2010 by M. Woltermann <http://www2.washjeff.edu/users/MWoltermann/Dorrie/72.pdf>.
- E.J. Hopkins and J.S. Hails, *An Introduction to Plane Projective Geometry*, Clarendon Press (1953).

