

Inhoud | Contents

Artikelen | Features

- Evenement | Event**
 88 **Andrew Wiles en de Abelprijs**
Sander R. Dahmen, Arno Kret
- Column | Column**
 99 **Lies, damn lies en tijdreeksen** *Casper Albers*
- Reis naar het bewijs | Trip to the Proof**
 101 **How I discovered Euclidean proofs** *M. Ram Murty*
- Evenement | Event**
 103 **NWD 2017: Hoe vaak is oneindig?** *Rob van Oord*
- De oplossing | The Solution**
 107 **Tegenvoorbeelden voor het Helton–Nievermoe-
den** *Jan Draisma*
- Evenement | Event**
 110 **NMC 2017: Een congres door jong en oud**
Frits Beukers, Rob Bisseling
- Evenement | Event**
 113 **Laudation for Kenneth Ribet** *Hendrik Lenstra*
- Interview | Interview**
 115 **Kenneth Ribet: “No one had ever accused me of
proving a theorem before”**
Gunther Cornelissen, Jan van Neerven
- Evenement | Event**
 122 **Wie en wat mij geholpen heeft om wiskundige
te worden** *Jaap Korevaar*
- Onderwijs | Education**
 128 **The use of games and their history to improve
secondary school students’ skills in mathema-
tics reasoning and problem solving** *Lisa Rougetet*
- In Memoriam | Obituary**
 133 **Wolf Barth: Remembering a friend and colleague**
Chris Peters
- Vakantiecursus | Summer School**
 136 **Krommen pletten: kegelsneden in de Gouden
Eeuw** *Fokko Jan Dijksterhuis*
- Boekbespreking | Book Review**
 142 **De Malosz en de Abendroth: over wiskundig on-
derzoek in een roman** *Ronald Meester*

Rubrieken | Departments

- 83 **Redactioneel** *Robbert Fokkink*
- 84 **Agenda** *Nicolaos Starreveld*
- 86 **Nieuws** *Nicolaos Starreveld*
- 131 **Het keerpunt van Annelie Vink**
Jan Beuving
- 140 **In de verdediging** *Geertje Hek*
- 144 **Boekbesprekingen**
- 149 **Problemen**

Uitgelicht

107



Jan Draisma bespreekt de tegenvoorbeelden van Claus Scheiderer voor het Helton–Nievermoe-
den.

128



Lisa Rougetet bespreekt het gebruik van games in de wiskundeles.

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 eenieder 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

Robbert Fokkink (r.j.fokkink@tudelft.nl)
Jan van Neerven (j.m.a.m.vanneerven@tudelft.nl)

Eindredactie/Bladmanager

Fred Drissen (fred@nieuwarchief.nl)

Redactie

Hans Cuypers (TU/e), Jan Draisma (Universität Bern en TU/e), Geertje Hek (UvA), Jan Hogendijk (UU), Teun Koetsier (VU), Sjoerd Rienstra (TU/e), Nicolaos Starreveld (UvA), Hans Sterk (TU/e), Mark Timmer (UT)

Problemenrubriek

Gabriele Dalla Torre (UL), Christophe Debry (KU Leuven), Jinbi Jin (UL), Marco Streng (UL), Wouter Zomervrucht (UL)

Bureau redactie

Claartje Ottens

Illustraties

Ryu Tajiri

Vormgeving

Susanne Laws (omslag, begeleiding binnenwerk)
Kitty Molenaar (ontwerp)

Druk

Veldhuis Media

Advertenties

advertenties@nieuwarchief.nl

Koninklijk Wiskundig Genootschap

www.wiskgenoot.nl

Platform Wiskunde Nederland

www.platformwiskunde.nl

European Mathematical Society

www.euro-math-soc.eu

International Mathematical Union

www.mathunion.org

Koninklijk Wiskundig Genootschap

Het Koninklijk Wiskundig Genootschap (KWG) is een landelijke vereniging van beoefenaars 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.

Bestuur

Erik van den Ban (UU, voorzitter), Joke Blom (CWI, penningmeester), Sonja Cox (UvA, secretaris), Theo van den Bogaart (HU), Marije Elkenbracht (ABN AMRO), André Ran (VU), Herman te Riele (CWI), Mark Veraar (TUD), Jan Wiegerinck (UvA)

Secretariaat

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

Ledenadministratie KWG / Abonnementen

Postbus 1064, 7940 KB Meppel
admin@wiskgenoot.nl, tel. 085-0160252

Contributie

De contributie voor gewone leden bedraagt in 2016 € 90 per jaar. Voor gepensioneerden en werklozen € 45. Voor studenten, aio's en oio's van een Nederlandse universiteit of hbo-opleiding € 35. Studenten en pas afgestudeerden kunnen een jaar lang gratis lid worden. Voor leden van de wiskundige vakverenigingen VvS+OR, NVvW en NVORWO geldt het gereduceerd tarief van € 70. Leden die het Nieuw Archief voor Wiskunde niet willen ontvangen, betalen slechts € 50 contributie. Losse nummers zijn te bestellen voor € 20. Instituten in Nederland en buitenland kunnen zich abonneren op het Nieuw Archief voor Wiskunde voor € 100 (Nederland), € 110 (Europa) of € 112,50 (buiten Europa).

Members of foreign societies

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 € 70 instead of the full membership fee of € 90 a year. Conversely, these foreign societies, as well as the VvS+OR 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.

Exchange subscriptions

Koninklijk Wiskundig Genootschap Library
Centrum Wiskunde & Informatica
P.O. Box 94079, NL-1090 GB Amsterdam
KWG-exchange@cw.nl

Informatie voor auteurs

Kopij

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

Volgende nummers

nummer	maand	verschijnen	deadline kopij
18(3)	september	2017	verstreken
18(4)	december	2017	01-08-2017
19(1)	maart	2018	01-11-2017
19(2)	juni	2018	01-02-2018

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



Freudenthal Instituut

Op het omslag

Door de eeuwen heen hebben vele wiskundigen tevergeefs geprobeerd een bewijs te vinden voor de Laatste Stelling van Fermat, totdat het Andrew Wiles in 1994 eindelijk lukte. Vorig jaar ontving hij de Abelprijs. Lees het artikel van Sander Dahmen en Arno Kret op pagina 88.

Versnelde IQ-stijging

Dit is mijn allereerste redactioneel voor het *Nieuw Archief voor Wiskunde* en omdat ik pas kom kijken, heb ik er wat oude redactionelen van tien jaar terug bij gepakt. Wat daarin opvalt is de pessimistische ondertoon. Tien jaar geleden waren de studentenaantallen veel lager dan tegenwoordig. Opleidingen dreigden te verdwijnen, wiskunde stond onder druk. Hoe anders is het nu. De studentenaantallen stijgen, Nederlandse jongeren winnen goud op de wiskundeolympiade. De toekomst ligt er zonnig bij.

Het is niet helemaal duidelijk waarom wiskunde zo in de lift zit. Misschien heeft het te maken met het feit dat mensen steeds slimmer worden. Psychologen constateren al sinds jaar en dag dat het IQ toeneemt met 3 punten per decennium. Zo schuift onze intelligentie almaar dieper de staart van de normale verdeling in. De hersens draaien steeds sneller, de behoefte aan abstractie wordt steeds groter, vandaar dat er steeds meer wiskundestudenten bijkomen. Ik zeg maar wat.

Deze toename van 3 punten, een meer nauwkeurige schatting is 2,9, ligt hoger bij vrouwen dan bij mannen en verschilt van land tot land. Culturele verschillen spelen dus een rol en daarom lijkt het erop dat we de natuur een handje kunnen helpen. Waar kan dat beter dan in Nederland? In het midden van de negentiende eeuw waren wij Nederlanders nog de kleinste inwoners van Europa en nu, honderdvijftig jaar later, zijn wij het langste van de hele wereld. De oorzaak van deze bijzondere groei is niet echt bekend, maar wat zou het mooi zijn als wij met ons IQ hetzelfde zouden kunnen uithalen als met onze lichaamslengte. Cruciaal voor een dergelijke ontwikkeling is natuurlijk een uitgekiend onderwijsprogramma. In het buitenland zit men niet stil. Lisa Rougetet bericht in dit nummer over de Franse plannen om combinatorische speltheorie in te

voeren in het wiskundeonderwijs. Met name het spel Nim, maar ook een spelletje Tetris kan geen kwaad, zoals valt te lezen in de laudatio van Ken Ribet. Het is misschien een goed idee om een spelletjeshoek in te ruimen binnen ons nationale wiskundehuis.

Het juninummer van NAW schenkt traditioneel veel aandacht aan het NMC. Dit jaar is het niet anders. Naast de al genoemde laudatio en een verslag van het congres brengen we een uitgebreid interview met Brouwermedaillewinnaar Ken Ribet en de lezing van Jaap Korevaar, die 75 jaar lid is van het KWG en allerlei oude herinneringen ophaalt aan de hand van Tauberstellingen. Een andere grote bijdrage is het overzichtsartikel over de betekenis van het werk van de Abelprijswinnaar van vorig jaar, Andrew Wiles. De column van Casper Alberts is weer scherp en actueel. Voordat hij mij op de vingers tikt vanwege de puntschatter 2,9 hierboven, haast ik mij om toe te voegen dat het 95 procent betrouwbaarheidsinterval gelijk is aan $(2,3,3,5)$. Een nieuwe rubriek is 'Trip to the Proof', waarin een wiskundige verhaalt over de ontstaansgeschiedenis van een resultaat, in plaats van over het bewijs. De eerste bijdrage is van Ram Murty, die uitlegt hoe een intrigerende opmerking uit een artikel in de *Monthly* hem op het spoor zette van euclidische bewijzen van Dirichlets priemgetalstelling. Bijzonder instructief voor jonge wiskundigen. Laat dit nummer van NAW na lezing achter in de bibliotheek, of een andere openbare ruimte voor leergierigen. Dan kunnen meer mensen het lezen en zo werken we toe naar een versnelde stijging van ons nationaal IQ. 

Robbert Fokkink, hoofdredacteur
Delft Institute of Applied Mathematics, TU Delft

Agenda

| Upcoming Events

juni 2017

6–9 juni 2017

□ Emerging Topics in Network Dynamical Systems

Een workshop over netwerk dynamische systemen. Mede georganiseerd door Eddie Nijholt (Amsterdam) en Bob Rink (Amsterdam).

plaats Lorentz Center, Leiden

info lorentzcenter.nl

7–9 juni 2017

□ Complexe Netwerken

Internationale conferentie georganiseerd door het wiskundeconsortium NETWORKS.

plaats CWI, Amsterdam

info thenetworkcenter.nl

19 juni – 7 juli 2017

□ IMAGINARY, Wiskunde in beelden

Tijdens het schooljaar 2016–2017 trekt IMAGINARY door Nederland, een tentoonstelling georganiseerd door Platform Wiskunde Nederland (PWN) en de Nederlandse universiteiten.

plaats Nijmegen

info imaginarymaths.nl

19–23 juni 2017

□ 8th General AMAmEF (Advanced Mathematical Methods in Finance) Conference

Een tweejaarlijkse conferentie over wiskundige methoden toegepast in finance.

plaats Amsterdam

info 8amamef.nl

22–23 juni 2017

□ Workshop Quantum Probability and Information Theory

Ter gelegenheid van de 66ste verjaardag van Hans Maassen wordt deze workshop georganiseerd door Eric Cator.

plaats Nijmegen

info ru.nl/wiskunde/events/news/calendar

26–30 juni 2017

□ 10th Extreme Value Analysis Conference

Een conferentie georganiseerd door J.J. Cai (TU Delft) en J. Einmahl (Universiteit Tilburg) over extreme value analysis en zijn toepassingen.

plaats TU Delft

info eva2017.nl

29–30 juni 2017

□ INFORMS Revenue Management and Pricing Section Conference

Een jaarlijkse conferentie op het gebied van prijsanalyse en revenue management.

plaats CWI, Amsterdam

info cwi.nl

juli 2017

2–5 juli 2017

□ 24th International Conference of Adults Learning Mathematics

De focus van deze conferentie ligt op de methodes van wiskunde- en rekenonderwijs voor volwassenen.

plaats Rotterdam

info alm-online.net/conference

3–7 juli 2017

□ GQT Graduate School and Colloquium

Een colloquium georganiseerd door het onderzoekcluster voor wiskunde GQT (Meetkunde en Quantumtheorie).

plaats Ernst Sillem Hoeve, den Dolder

info www.gqt.nl

3–8 juli 2017

□ 32nd International Workshop on Statistical Modeling

Een workshop over statistisch modelleren in verschillende vakgebieden.

plaats Rijksuniversiteit Groningen

info iws2017.webhosting.rug.nl

7–10 juli 2017

□ Conference on Learning Theory (COLT 2017)

Een conferentie gericht op nieuwe ontwikkelingen op het gebied van Learning Theory.

plaats Amsterdam

info www.learningtheory.org/colt2017

17–21 juli 2017

□ Hamiltonian and Reed Dynamics: New Methods and Applications

Een workshop over nieuwe ontwikkelingen en toepassingen van symplectische meetkunde in het bestuderen van dynamische systemen.

plaats Lorentzcenter, Leiden

info lorentzcenter.nl

Suggesties voor deze agenda zijn welkom.

Redacteur: Nicolaos Starreveld

agenda@nieuwarchief.nl

augustus 2017

25–26 augustus

□ Vakantiecursus 2017

Vakantiecursus georganiseerd door PWN, voor leraren, studenten van lerarenopleidingen en andere belangstellenden. Dit jaar is het thema ‘De computer in de wiskunde: breekijzer of oud schroot’.

plaats Technische Universiteit Eindhoven

info platformwiskunde.nl

28 augustus – 1 september 2017

□ Bayesian and Nonlinear Inverse Problems

Workshop mede gereorganiseerd door Johannes Schmidt-Hieber (LU) en Aad van der Vaart (LU).

plaats Lorentz Center@Oort, Leiden

info lorentzcenter.nl

31 augustus – 1 september 2017

□ Workshop on New Advances on Epidemics in Complex Networks

Een workshop georganiseerd door Daniel Valesin (Groningen), Julia Komjathy (Eindhoven) en Piet van Mieghem.

plaats Delft

info eurandom.nl

september 2017

1–2 september 2017

□ Vakantiecursus 2017

Vakantiecursus georganiseerd door PWN, voor leraren, studenten van lerarenopleidingen en andere belangstellenden. Dit jaar is het thema ‘De computer in de wiskunde: breekijzer of oud schroot’.

plaats CWI, Amsterdam

info platformwiskunde.nl

4–8 september 2017

□ YEP XIV on Networks: Probability, Combinatorics and Algorithms

De veertiende YEP (Young European Probabilists) conferentie is gefocust op netwerken.

plaats Eurandom, Eindhoven

info eurandom.nl

4–8, 11–15 en 18–22 september 2017

□ Stochastic Activity Month

Tijdens de Stochastic Activity Month (SAM) zullen er drie workshops zijn, beginnend met de Young European Probabilists workshop (YEP).

plaats Eurandom, Eindhoven

info eurandom.nl

11–15 september 2017

□ Randomness and Graphs: Processes and Structures

Een workshop over random graphs, discrete processen en algoritmen op grafen.

plaats Eurandom, Eindhoven

info eurandom.nl

12–15 september 2017

□ Statistical Theory and the Real World

Een workshop georganiseerd door Giulia Cereda, Peter Grünwald en Aad van der Vaart.

plaats Lorentz Center@Oort, Leiden

info lorentzcenter.nl

15 september 2017

□ Finale Nederlandse Wiskunde Olympiade

De prijswinnaars van deze finale worden uitgenodigd om deel te nemen aan een speciaal trainingsprogramma voor de internationale wiskundewedstrijden.

plaats Technische Universiteit Eindhoven

info wiskundeolympiade.nl

18–22 september 2017

□ Community Detection and Network Reconstruction

Een workshop georganiseerd door Luva Avena (Leiden), Jop Briët (Amsterdam, CWI), Rui Castro (Eindhoven) en Diego Garlaschelli (Leiden).

plaats Eurandom, Eindhoven

info eurandom.nl

oktober 2017

4–6 oktober 2017

□ 42ste Woudschoten Conferentie

Een jaarlijkse conferentie van de Nederlands-Vlaamse Numerieke Analyse-groepen, georganiseerd door de Werkgemeenschap Scientific Computing (WSC).

plaats Woudschoten, Zeist

info wsc.project.cwi.nl/events

23–27 oktober 2017

□ On Growth and Form

Een workshop in het kader van het honderd-jarig bestaan van de eerste druk van het wereldberoemde boek *On Growth and Form* van D'Arcy Thompson.

plaats Lorentz Center@Oort, Leiden

info lorentzcenter.nl

november 2017

10 november 2017

□ Prijsuitreiking van de Nederlandse Wiskunde Olympiade

De prijsuitreiking van de finale van de Nederlandse Wiskunde Olympiade.

plaats Eindhoven

info wiskundeolympiade.nl

december 2017

4–8 december 2017

□ Random Dynamical Systems

Een workshop mede georganiseerd door Ale Jan Homburg (Amsterdam).

plaats Lorentz Center@Oort, Leiden

info lorentzcenter.nl

4–8 december 2017

□ Random Structures on the Brain

Een workshop mede georganiseerd door Luca Avena (Leiden), Roberto Fernandez (Utrecht) en Martijn van den Heuvel (Utrecht).

plaats Lorentz Center@Oort, Leiden

info lorentzcenter.nl

11–15 december 2017

□ Future and Emerging Mathematical Technologies in Europe

Een workshop mede georganiseerd door Wil Schilders (Eindhoven), Evgeny Verbitskiy (Leiden) en Kees Vuurik (Delft).

plaats Lorentz Center@Oort, Leiden

info lorentzcenter.nl

Nieuws

| News

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

Redacteur: Nicolaos Starreveld
 nieuws@nieuwarchief.nl

Abelprijs voor Yves Meyer

De Noorse Academie van Wetenschappen heeft de Abelprijs voor 2017 toegekend aan de Franse wiskundige Yves Meyer (1939) voor zijn bijdrage aan de wiskundetheorie van wavelets. De hoogleraar wiskunde aan de École normale supérieure Paris-Saclay krijgt een bedrag van zes miljoen Noorse kronen (€ 635.000).

Yves Meyer was de eerste die wavelets in de wiskunde introduceerde. De wiskundetheorie van wavelets ligt op de grens van wiskunde, informatica en computationele wetenschap. Oorspronkelijk was Meyer onderzoeker in de getaltheorie, maar daarna raakte hij gefascineerd door de harmonische analyse, een gebied waarin onderzoekers zich toeleggen op het simplificeren van complexe wiskundige objecten naar eenvoudiger golfachtige componenten. Geïnspireerd door de methoden van de harmonische analyse begon Meyer een theorie te construeren om ingewikkelde signalen te kunnen analyseren.

De feestelijke uitreiking van de prijs vond plaats op dinsdag 23 mei in Oslo, alwaar Meyer de prijs ontving uit handen van de Noorse koning Harald V.

abelprize.no

Wiskundige Clara Stegehuis één van de nieuwe 'Faces of Science'

Faces of Science is een project van de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW), De Jonge Akademie en NEMO Kennislink met als doel jonge talentvolle wetenschappers in de schijnwerpers te zetten. Op de site Facesofscience.nl bloggen de promovendi over hun ervaringen en passies om de bezoekers te laten zien hoe de wetenschappelijke wereld eruitziet. Via de ogen van promovendi worden de deuren van conferenties, laboratoria en bibliotheken geopend voor het publiek!

Promovenda Clara Stegehuis van de faculteit Wiskunde en Informatica in Eindhoven is gekozen als één van de nieuwe twaalf 'Faces of Science'. Dit zijn door KNAW gekozen jonge talenten die in filmpjes en blogs verslag gaan doen van hun dagelijkse bestaan in de wetenschap. Als studente deed Stegehuis al aan voorlichting en organiseerde ze wiskundewedstrijden voor 4 en 5 vwo-scholieren. Als promovenda zette zij die lijn door, als host bij een wiskundetentoonstelling en als spreker in een theatervoorstelling. Het onderwerp van haar promotieonderzoek is complexe netwerken. Dit soort netwerken zijn overal om ons heen. Denk aan sociale netwerken, communicatienetwerken of citatienetwerken.

KNAW, NEMO Kennislink, TU/e

CWI ontwikkelt algoritmes die aanrijtijd ambulances verkorten

In levensbedreigende noodgevallen waarin elke seconde telt, kan het al dan niet op tijd ter plaatse zijn van een ambulance het verschil maken tussen leven en dood. In Nederland bedraagt deze normtijd 15 minuten voor ongevallen van de hoogste urgentieklasse. In de praktijk blijkt echter dat niet altijd aan deze gestelde normtijd wordt voldaan. De aanrijtijd van ambulances kan verkort worden door de ambulances efficiënt over de regio te verdelen. De locatie van het hulpvoertuig op het moment van het ongeval is namelijk in hoge mate bepalend voor het al dan niet halen van de normtijd. CWI-promovendus Thijs van Barneveld bespreekt in zijn proefschrift verschillende modellen en algoritmen voor het optimaliseren van de gebiedsdekking door middel van het uitvoeren

van zogenaamde proactieve relocaties. Dit houdt in dat een of meerdere hulpvoertuigen tijdelijk geherpositioneerd worden. Dit is de kern van het zogenaamde Dynamisch Ambulance Management (DAM).
cwi.nl

Zilver en brons voor Nederlandse dames bij Europese Olympiade

Bij de zesde editie van de European Girls' Mathematical Olympiad van 6–12 april in Zürich heeft het Nederlandse team een zilveren en een bronzen medaille behaald. Christel van Diepen (16) uit Malden loste drie van de zes opgaven foutloos op en sleepte hiermee zilver in de wacht. Esther Steenkamer (16) uit Roggel behaalde zoveel punten dat ze voor brons in aanmerking kwam. Aimée Jacobs (17) uit Nieuw-Vennep loste een opgave foutloos op en verdiende hiermee een eervolle vermelding. Aimée, Christel en Esther vertegenwoordigden ook vorig jaar Nederland bij deze olympiade. Christel: "De opgaven bij dit soort wedstrijden zijn echt heel moeilijk, dus is het enorm cool om er drie op te lossen. Volgend jaar mag ik weer meedoen en dan ga ik voor goud!" In het officiële landenklassement haalde Nederland een 17e plaats van de 44 deelnemende landen.
wiskundeolympiade.nl



Foto: Birgit van Dalen

Booking.com wint Wiskunde Olympiade voor Bedrijven

De Wiskunde Olympiade voor Bedrijven is een jaarlijks evenement dat voor het eerst op vrijdag 27 januari 2012 plaatsvond. Bedrijven kunnen meedoen en kunnen tot drie werknemers afvaardigen. Deze wiskundewedstrijd wordt georganiseerd door de Stichting Nederlandse Wiskunde Olympiade. Op vrijdag 27 januari vond de zesde editie plaats bij Optiver aan de Amsterdamse Zuidas. Bij de wedstrijd kregen de deelnemers een uur de tijd om in totaal twaalf opgaven op te lossen. De eerste prijs ging naar het team van Booking.com, bestaande uit Jeroen van Wolffelaar, Oli Thuong en Roman Lyapin. De teams van ABN-Amro en ORTEC behaalden een eervolle tweede en derde plaats. Het individueel klassement werd aangevoerd door Allard Veldman van CrossmarX die beide wedstrijdonderdelen foutloos had gemaakt. De tweede en derde plaats waren voor Tejaswi Navilarekallu van Optiver en Erik van Holland van ORTEC.
wiskundeolympiade.nl

Het vermoeden van de eenzame loper

Het vermoeden van de eenzame loper ('lonely runner's conjecture') werd geuit door J.M. Wills in 1967. Beschouw een eindig aantal lopers, stel K , op een cirkelvormige baan. Op tijdstip 0 staan ze allemaal op hetzelfde punt en beginnen ze met lopen met verschillende snelheden. Op tijd t wordt een loper benoemd als 'eenzaam' als alle andere lopers minstens op een afstand van $1/K$ van hem zijn. Volgens het vermoeden van de eenzame loper bestaat er, voor een gegeven aantal lopers K , een tijd t waarop alle lopers eenzaam zijn. In algemene vorm is dit nog steeds een open probleem in de wiskunde, maar er zijn wel een aantal resultaten te vinden. Bijvoorbeeld de gevallen van twee tot en met zeven lopers zijn wel bewezen. De wiskundige en Fieldsmedaillewinnaar Terence Tao deed afgelopen jaar een poging tot het bewijzen van dit vermoeden. Helaas is het hem niet gelukt om een definitief antwoord te geven. Maar in januari 2017 uploadde hij een artikel op ArXiv waarin hij de moeilijkheden van het bewijzen van dit vermoede bespreekt. Bovendien presenteert hij een potentiële strategie om het vermoeden te bewijzen.
terrytao.wordpress.com, arxiv.org/abs/1701.02048

Nederlandse Data Science Prijzen

Het bestuur van de Koninklijke Hollandsche Maatschappij der Wetenschappen en de Big Data Alliance (BDA) maken bekend dat — met ingang van 2017 — jaarlijks de Nederlandse Data Science Prijzen worden uitgereikt. De Nederlandse Data Science Prijzen zijn in het leven geroepen om uitzonderlijk innovatief ondernemerschap en wetenschappelijk onderzoek op het gebied van data science in de schijnwerpers te zetten. De initiatiefnemers willen hiermee Nederland op de kaart zetten als data science-land bij uitstek.
khw.nl

Koninklijk Wiskundig Genootschap

Algemene Ledenvergadering

Op 11 april vond de 240ste Algemene Ledenvergadering van het KWG plaats. Tijdens deze ALV zijn Fetsje Bijma en Geurt Jongbloed uit het bestuur getreden, en Marije Elkenbracht is toegetreden tot het bestuur. Op een extra ingelaste ALV op 2 mei is ook Jan Wiegerinck toegetreden tot het bestuur. Hij kon 11 april niet benoemd worden omdat zijn kandidatuur niet op tijd was aangekondigd door het bestuur.

NMC 2017

Op 11 en 12 april vond het 53ste Nederlands Mathematisch Congres plaats in Utrecht. Een verslag hiervan is elders in dit nummer te vinden.

Nieuwe hoofdredacteur NAW

Robbert Fokkink heeft Richard Boucherie per 1 januari opgevolgd als hoofdredacteur van het NAW. Hij vormt nu samen met Jan van Neerven de hoofdredactie.

Recent verschenen:

Epsilon Uitgaven (www.epsilon-uitgaven.nl)

88. *Handboek natuurkundendidactiek*, Koos Kortland, Ad Moeldijk en Hans Poorthuis (red.), € 36 (€ 30 tot 1 juli), 2017.

Sander R. Dahmen

Afdeling Wiskunde
Vrije Universiteit Amsterdam
s.r.dahmen@vu.nl

Arno Kret

Korteweg-de Vries Instituut
Universiteit van Amsterdam
a.l.kret@uva.nl

Evenement Abelprijs 2016

Andrew Wiles en de Abelprijs

Op 24 mei 2016 ontving Sir Andrew J. Wiles de Abelprijs ‘for his stunning proof of Fermat’s Last Theorem by way of the modularity conjecture for semistable elliptic curves, opening a new era in number theory’. In dit artikel schetsen Sander Dahmen en Arno Kret wat Wiles bewezen heeft en laten zien wat voor prachtig onderzoek er uit zijn werk voortgekomen is.

De Laatste Stelling van Fermat luidt als volgt.

Stelling 1. *Laat x , y en z gehele getallen ongelijk 0 zijn en $n \geq 3$ geheel. Dan geldt*

$$x^n + y^n \neq z^n.$$

Wiles leverde het finale ingrediënt voor deze stelling door de modulariteit van grote klassen van elliptische krommen te laten zien, wat feitelijk de oplossing is van een deel van de Langlands-vermoedens. Hiermee werd de weg geopend tot het verkrijgen van nog veel verder reikende modulariteitsresultaten en bijbehorende gevolgen, inclusief het oplossen van vele andere diofantische vergelijkingen. In dit artikel zullen we ons vooral richten op de wiskundige kant van het verhaal. Zie ook de referenties [2, 5, 13] die gericht zijn op een breed publiek, en voor het originele werk zie de artikelen [29, 30]. We gaan eerst uitleggen wat modulariteit van elliptische krommen betekent. Hiervoor komen modulaire vormen en elliptische krommen uitgebreid aan bod. Daarna geven we verbanden met andere problemen in de wiskunde, zoals het vermoeden van Birch en Swinnerton-Dyer,

de Langlands-vermoedens en problemen in de theorie van diofantische vergelijkingen.

In 1967 schreef Langlands een brief aan André Weil [16], waarin hij een aantal ver-

moedens formuleerde. Zijn vermoedens, nu bekend als de *Langlands-vermoedens*, brengen de getaltheorie en representatietheorie met elkaar in verband. Bovendien zijn ze gerelateerd aan en kunnen ze gecombineerd worden met andere stellingen en vermoedens uit de getaltheorie en algebraïsche meetkunde, zoals klassenlichamentheorie, de Riemann-hypothese, het Sato–Tate-vermoeden, het Hasse–Weil-vermoeden, het Fontaine–Mazur-vermoeden en het eerder genoemde Birch–Swinnerton-Dyer-vermoeden.

Voordat Wiles in 1994 zijn stelling bewees, was buiten het geval van eendimensionale representaties weinig van de vermoedens bekend in hogere dimensies. Men kon zien dat de vermoedens van Langlands consistent waren met andere vermoedens (in de zin dat er geen tegenspraak is), maar men kon niet veel bewijzen of narekenen. Hoewel het eendimensionale geval volgt uit klassenlichamentheorie, is dit geval ook enorm gedegeneerd. Dus eigenlijk was het helemaal niet duidelijk of je Langlands’ vermoedens moest geloven of niet. Misschien was dit ook de reden dat Weil nooit gereageerd heeft op de brief van Langlands. Het werk van Wiles heeft grote invloed gehad op de Langlands-vermoedens, omdat het een substantiële klasse van bewezen gevallen toevoegt, die daarvoor als onbereikbaar werden gezien



Andrew Wiles voor het standbeeld van Pierre de Fermat in Beaumont-de-Lomagne, 1995

Foto: Klaus Barner / CC BY-SA

met de toenmalige wiskundige technieken. Na Wiles hebben veel wiskundigen het argument van Wiles uitgebreid, en op deze manier meer delen van de Langlands-vermoedens bewezen.

Wiskundige objecten: de spelers

We zullen eerst twee basisobjecten introduceren, namelijk elliptische krommen en modulaire vormen. We beperken ons hier tot enkele basale definities en eigenschappen. Gedegen introducties zijn op veel plekken te vinden, bijvoorbeeld de tekstboeken [25] en [8]. Vervolgens gaan we in op de relatie tussen de twee spelers in het beschrijven van modulariteit van elliptische krommen. Ten slotte bespreken we nog even kort de rol hiervan in het beroemde vermoeden van Birch en Swinnerton-Dyer.

Elliptische krommen

Laat K een lichaam zijn, zoals bijvoorbeeld $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ of $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ met p een priemgetal. Een *Weierstrass-vergelijking* over K is een vergelijking van de vorm

$$y^2 + dxy + ey = x^3 + ax^2 + bx + c \quad (1)$$

met $a, b, c, d, e \in K$. Zo'n vergelijking definieert een algebraïsche kromme E over K . Als de karakteristiek van K niet 2 is (wat betekent dat $1 + 1 \neq 0$ in K , waarmee bijvoorbeeld $K = \mathbb{F}_2$ afvalt), kun je een dergelijke vergelijking altijd omschrijven naar een vergelijking waarbij $d = e = 0$. Laten we dit nu voor het gemak aannemen, dan worden de formules eenvoudiger. We hebben nu een vergelijking voor E van de vorm $y^2 = f(x)$, waarbij f een monisch kubisch polynoom $f = x^3 + ax^2 + bx + c$ is. Hoewel de vergelijking $y^2 = f(x)$ suggereert dat we gewoon in het affiene vlak K^2 werken, beschouwen we de kromme E ingebed in het projectieve vlak (en compleet, wat concreet betekent dat we één formeel extra punt aan de kromme toevoegen: het punt op oneindig). De K -rationale punten op E , genoteerd als $E(K)$, zijn de punten $(x, y) \in K^2$ in het vlak K^2 die aan bovenstaande vergelijking voldoen, samen met het punt op oneindig O . De niet-singuliere punten in

$$E(K) = \{(x, y) \in K^2: y^2 = x^3 + ax^2 + bx + c\} \cup \{O\}$$

vormen op natuurlijke wijze een groep, met O als neutraal punt, door middel van de beroemde 'koorde- en raaklijn-constructie'. Dit is ook de reden om het punt O toe te voegen.

Als E niet-singulier is, spreken we van een *elliptische kromme* over K . We definiëren de discriminant $\Delta(E)$ van de Weierstrass-vergelijking door $\Delta(E) = 2^4 \cdot \Delta(f)$. Hierin is $\Delta(f)$ de discriminant van het kubische polynoom f , welke in het geval dat $a = 0$ simpelweg gegeven wordt door $-4b^3 - 27c^2$. Er geldt dat E niet-singulier is (en dus een elliptische kromme geeft) dan en slechts dan als $\Delta(E) \neq 0$. Twee krommen $E: y^2 = f(x)$ en $E': y'^2 = g(x')$ zijn isomorf dan en slechts dan als ze gerelateerd zijn via een variabelentransformatie van de vorm

$$x = u^2x' + r, \quad y = u^3y' \quad (2)$$

waarbij $r, u \in K$ met $u \neq 0$. In dat geval zijn de discriminanten gerelateerd via $\Delta(E) = u^{12} \Delta(E')$. Als E singulier is, dat wil zeggen dat $\Delta(E) = 0$, dan liggen de singuliere punten op de x -as (nog steeds aangenomen dat $d = e = 0$ en de karakteristiek van K niet 2 is), en heeft f meervoudige nulpunten, welke automatisch in K liggen als K een deellichaam van $\mathbb{C}$ of een eindig lichaam is. Er zijn nu twee mogelijkheden. Als $f(x)$ twee verschillende nulpunten heeft waarvan één dus een dubbel nulpunt is, dan zeggen we dat E een *knooppunt* heeft. Als $f(x)$ één nulpunt van orde drie heeft, dan zeggen we dat E een *spits* heeft.

Laat nu E een elliptische kromme over $\mathbb{Q}$ zijn, gegeven door een Weierstrass-vergelijking. Er zijn oneindig veel andere Weierstrass-vergelijkingen (1) die door variabelentransformaties, waarvan (2) speciale gevallen zijn, uit de oorspronkelijke vergelijking voor E verkregen kunnen worden. Een Weierstrass-vergelijking uit deze familie wordt *minimaal* genoemd als alle coëfficiënten in $\mathbb{Z}$ liggen en de absolute waarde van de discriminant minimaal is (onder de Weierstrass-vergelijkingen met coëfficiënten in $\mathbb{Z}$ in de familie). Voor zo'n minimale vergelijking kunnen we de coëfficiënten van E reduceren modulo een priemgetal p en zo een Weierstrass-vergelijking voor de reductie modulo p krijgen: de kromme $\tilde{E}$ over $\mathbb{F}_p$. Het reductietype en het aantal punten $\#\tilde{E}(\mathbb{F}_p)$ hangt niet van de gekozen minimale Weierstrass-vergelijking af.

Een belangrijke invariant voor elliptische krommen E over $\mathbb{Q}$ is de *conductor* van E , genoteerd als $N(E)$. De volledige definitie is behoorlijk subtiel (zie Hoofdstuk 4, §10 van [26]). We geven hier een gedeeltelijke definitie. Voor elk priemgetal p beschouwen we de conductor-exponent

$$e_p(E) := \begin{cases} 0 & \text{als } E \text{ niet singulier is mod } p \\ 1 & \text{als } E \text{ een knooppunt heeft mod } p \\ 2 + \delta_p & \text{als } E \text{ een spits heeft mod } p \end{cases}$$

waarbij $\delta_p \in \mathbb{Z}_{\geq 0}$. Verder geldt $\delta_2 \leq 6$, $\delta_3 \leq 3$ en $\delta_p = 0$ als $p \geq 5$. Nu is de conductor $N(E) := \prod_p p^{e_p(E)}$. In het bijzonder, als de reducties van E modulo 2 en modulo 3 geen spits oplevert, dan legt bovenstaande $N(E)$ volledig vast. Als voor geen enkel priemgetal p de reductie van E modulo p een spits geeft, dan noemen we E *semi-stabiel*; dit komt op hetzelfde neer als dat $N(E)$ kwadraatvrij is.

Voor een elliptische kromme $E/\mathbb{Q}$ definiëren we $a_p(E) := p + 1 - \#\tilde{E}(\mathbb{F}_p)$ voor elk priemgetal p . De L -functie van E is nu

$$L_E(s) := \prod_{p \nmid N(E)} (1 - a_p(E)p^{-s} + p^{1-2s})^{-1} \cdot \prod_{p \mid N(E)} (1 - a_p(E)p^{-s})^{-1}$$

waar de producten over priemgetallen p lopen. Het is klassiek bekend dat $|a_p(E)| \leq 2\sqrt{p}$ voor alle priemen p en dat de Dirichlet-reeks corresponderend met $L_E(s)$ convergeert naar een holomorfe functie voor $s \in \mathbb{C}$ met reëel deel strikt groter dan $3/2$.

Veel van het bovenstaande voor $K = \mathbb{Q}$ kunnen we generaliseren naar getallenlichamen K . Dit betekent dat K een eindige lichaamsuitbreiding van $\mathbb{Q}$ is, zoals bijvoorbeeld $\mathbb{Q}(i) = \{a + bi: a, b \in \mathbb{Q}\}$, $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2: a, b, c \in \mathbb{Q}\}$ of $\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}\}$ waarbij α een nulpunt (laten we zeggen in $\mathbb{C}$) is van een polynoom van graad n met rationale coëfficiënten dat irreducibel over $\mathbb{Q}$ is. Dit laatste is het generieke voorbeeld en omvat alle getallenlichamen (ingebod in $\mathbb{C}$). Binnen zo'n getallenlichaam K definieert men de *ring van gehelen* $\mathcal{O}_K$ als die elementen van K die nulpunt zijn van een monisch polynoom met coëfficiënten in $\mathbb{Z}$. Om in te zien dat $\mathcal{O}_K$ inderdaad een ring is, moet men nog een beetje werk verzetten. De ring van gehelen in $\mathbb{Q}$ is $\mathbb{Z}$ en de rol die $\mathbb{Z}$ binnen $\mathbb{Q}$ speelt, is analoog aan de rol die $\mathcal{O}_K$ binnen K speelt. Voor bijvoorbeeld $K = \mathbb{Q}(i)$ hebben we eenvoudig dat de ring van gehelen $\mathcal{O}_K = \mathbb{Z}[i] = \{a + bi: a, b \in \mathbb{Z}\}$ de ring van Gaussische gehelen is. Voor een elliptische kromme E over een getallenlichaam K kunnen we weer een Weierstrass-vergelijking opschrijven, maar dan met coëfficiënten in $\mathcal{O}_K$. Voor elk priem-

ideaal $\wp \subset \mathcal{O}_K$ ongelijk 0 kunnen we nu de reductie van de Weierstrass-vergelijking nemen modulo $\wp$ om zo een kromme $\tilde{E}$ over een eindig lichaam $\mathbb{F}_\wp := \mathcal{O}_K/\wp$ te krijgen. Is de vergelijking gekozen zodat de macht van $\wp$ minimaal is in (het ideaal voortgebracht door) de discriminant van de vergelijking (weer onder alle relevante variabelentransformaties), dan is het reductietype weer uniek bepaald evenals het gehele getal $a_\wp(E) := N(\wp) + 1 - \#\tilde{E}(\mathbb{F}_\wp)$, waarbij $N(\wp) := \#\mathbb{F}_\wp$. De elliptische kromme E heeft, net als in het geval waar $K = \mathbb{Q}$, een conductor N , die nu een ideaal is in $\mathcal{O}_K$. De kromme E heeft niet-singuliere reductie modulo precies die priemidealen $\wp \subset \mathcal{O}_K$ die N niet delen. De L -functie gekoppeld aan E is

$$L_E(s) := \prod_{\wp \nmid N} (1 - a_\wp(E)N(\wp)^{-s} + N(\wp)^{1-2s})^{-1} \cdot \prod_{\wp \mid N} (1 - a_\wp(E)N(\wp)^{-s})^{-1}.$$

Modulaire vormen

Klassieke (of elliptische) modulaire vormen zijn holomorfe functies op het complexe bovenhalfvlak $\mathbb{H} := \{x+yi \in \mathbb{C} : y > 0\}$ met bepaalde transformatie- en groei-eigenschappen. Spitsvormen zijn modulaire vormen met nog een wat sterkere groei-eigenschap en we beperken ons in dit artikel tot deze klasse. In de rest van deze subparagraaf zullen k en N staan voor positieve gehele getallen. Om alles precies te maken, introduceren we eerst een aantal groepen. Namelijk

$$\mathrm{GL}_2^+(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc > 0 \right\},$$

een discrete ondergroep hiervan

$$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

en een ondergroep (van eindige index) van laatstgenoemde groep

$$\Gamma(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Een congruentieondergroep van $\mathrm{SL}_2(\mathbb{Z})$ is een ondergroep Γ van $\mathrm{SL}_2(\mathbb{Z})$ die $\Gamma(N)$ bevat voor een N . De kleinste N voor zo'n Γ waarvoor $\Gamma(N) \subset \Gamma$ heet het niveau van Γ . Men gaat eenvoudig na dat voor $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$ en $\tau \in \mathbb{H}$ de formule

$$\gamma\tau := \frac{a\tau + b}{c\tau + d} \quad (3)$$

een actie van $\mathrm{GL}_2^+(\mathbb{R})$ op $\mathbb{H}$ definieert (oftewel, $\gamma\tau \in \mathbb{H}$, $(\gamma\gamma')\tau = \gamma(\gamma'\tau)$ en $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\tau = \tau$). Dezelfde formule geeft dus ook een actie van elke ondergroep van $\mathrm{GL}_2^+(\mathbb{R})$, zoals de congruentieondergroepen, op $\mathbb{H}$.

Laat Γ een congruentieondergroep van $\mathrm{SL}_2(\mathbb{Z})$ van niveau N zijn. We definiëren nu een spitsvorm voor Γ van gewicht k als een holomorfe (dat wil zeggen complex differentieerbare) functie $f : \mathbb{H} \rightarrow \mathbb{C}$ met de transformatie-eigenschap (voor alle $\tau \in \mathbb{H}$)

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\tau\right) = (c\tau + d)^k f(\tau) \quad (4)$$

voor alle $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$

en groei-eigenschap

$$\tau = x + yi \mapsto y^{k/2} |f(\tau)| \text{ is begrensd op } \mathbb{H}. \quad (5)$$

Men gaat gemakkelijk na dat de spitsvormen voor Γ van gewicht k een $\mathbb{C}$ -vectorruimte vormen (onder de gebruikelijke operaties), die we noteren als $S_k(\Gamma)$. Met wat meer werk is ook aan te tonen dat $S_k(\Gamma)$ eindigdimensionaal is.

Laat $f : \mathbb{H} \rightarrow \mathbb{C}$ nu een holomorfe functie zijn met transformatie-eigenschap (4). Voor $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$ specialiseert (4) tot $f(\tau + N) = f(\tau)$ voor alle $\tau \in \mathbb{H}$, oftewel f is periodiek met periode M een deler van N . Samen met de holomorfie van f geeft dit direct dat f een Fourier-ontwikkeling heeft: $f(\tau) = \sum_{n=-\infty}^{\infty} a_n \exp(2\pi i \tau n / M)$ met alle $a_n \in \mathbb{C}$ uniek bepaald. De groei-eigenschap (5) impliceert dat $f(x + yi) \rightarrow 0$ als $y \rightarrow \infty$ (aangezien $k > 0$ per aanname), wat equivalent is met $a_n = 0$ voor alle $n \leq 0$. Voor $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ is dit laatste equivalent met (5), maar voor algemene Γ is dit niet noodzakelijk waar. Namelijk, de formule (3) definieert een actie van Γ op $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, met een eindig aantal banen, de zogenaamde spitsen van Γ . Bij elke spits kan men een bepaalde Fourier-ontwikkeling in $\exp(2\pi i \tau / N)$ kiezen, en (5) is equivalent met dat al deze Fourier-ontwikkelingen enkel positieve machten van $\exp(2\pi i \tau / N)$ bevatten. Algemene modulaire vormen mogen ook nog een constante term in zulke Fourier-ontwikkelingen hebben, maar voor spitsvormen moet per definitie bij elke spits de constante dus nul zijn. Hier komt de naam spitsvorm vandaan.

De belangrijkste congruentieondergroepen om het werk van Wiles te beschrijven, zijn gegeven door

$$\Gamma_0(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

hierbij betekent $*$ dat elke mogelijke waarde toegestaan is, dus de conditie op $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is simpelweg dat $N \mid c$. Voor later gebruik introduceren we ook

$$\Gamma_1(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Merk op dat $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ en verder dat alle inclusies gelijkheden zijn dan en slechts dan als $N = 1$. Laat $f \in S_k(\Gamma_i(N))$ (met $i \in \{0, 1\}$). Aangezien $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_i(N)$ is f periodiek met periode 1. Schrijven we q voor de functie gegeven door $q(\tau) = \exp(2\pi i \tau)$, dan krijgen we zo de zogenaamde q -expansie

$$f = \sum_{n=1}^{\infty} a_n(f) q^n. \quad (6)$$

Bovenstaande notatie $a_n(f)$ voor de (uniek bepaalde) Fourier-coëfficiënten van $f \in S_k(\Gamma_i(N))$ zullen we in de rest van dit artikel aanhouden.

Laten we eens naar het eenvoudigste geval $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ kijken. Het kleinste gewicht k waarvoor $S_k(\mathrm{SL}_2(\mathbb{Z})) \neq \{0\}$, is $k = 12$. In dat geval is de ruimte eindigdimensionaal en voortgebracht door de discriminant functie

$$\begin{aligned} \Delta &:= q \prod_{n=1}^{\infty} (1 - q^n)^{24} \\ &= q - 24q^2 + 252q^3 - 1472q^4 \\ &\quad + 4830q^5 - 6048q^6 + \dots \end{aligned}$$

Deze functie kan worden verkregen als discriminant van een op natuurlijke wijze geparametriseerde familie van elliptische krommen, vandaar de naam. De coëfficiënt $a_n(\Delta)$ van q^n in bovenstaande q -expansie van Δ wordt traditioneel als $\tau(n)$ genoteerd. De functie $n \mapsto \tau(n)$ heet Ramanujans tau-functie en in 1916 vermoedde Ramanujan een aantal opmerkelijke eigenschappen ervoor, namelijk

- τ is multiplicatief, oftewel $\tau(nm) = \tau(n)\tau(m)$ voor alle $n, m \in \mathbb{Z}_{>0}$ met $\mathrm{ggd}(m, n) = 1$;
- $\tau(p^r) = \tau(p)\tau(p^{r-1}) - p^{11}\tau(p^{r-2})$ voor alle priemgetallen p en $r \in \mathbb{Z}_{\geq 2}$;
- $|\tau(p)| \leq 2p^{11/2}$ voor alle priemgetallen p .

De eerste twee eigenschappen zijn al in 1917 bewezen door Mordell en de laatste is in 1974 door Deligne bewezen als (niet-triviaal) gevolg van zijn bewijs van de beroemde Weil-vermoedens. Voor dit laatste kreeg Deligne in 1978 de Fieldsmedaille, verder heeft hij onder meer ook de Abel-



Foto: abelprijs.no, Audun Braastad

Andrew Wiles tijdens de prijsuitreiking van de Abelprijs op 24 mei 2016 in Oslo

prijs ontvangen in 2013; voor meer info zie [18]. Er is ook nog veel onbekend over Ramanujans tau-functie. Zo weten we bijvoorbeeld niet of $\tau(n)$ gelijk aan nul kan zijn voor een $n \in \mathbb{Z}_{>0}$. Men vermoedt van niet, dit staat ook wel bekend als Lehmers vermoeden, zie [17]. Het is momenteel bekend dat $\tau(n) \neq 0$ voor $n < 8 \times 10^{23}$, maar een bewijs dat dit voor alle n geldt, lijkt voorlopig nog niet in zicht.

De eerste twee eigenschappen kunnen het best verklaard worden met behulp van *Hecke-operatoren*. Voor elke priem p hebben we een lineaire operator

$$T_p : S_k(\Gamma) \rightarrow S_k(\Gamma).$$

Een natuurlijke manier om deze in te voeren is met behulp van representanten $\gamma_1, \gamma_2, \dots, \gamma_{d_p}$ van nevenklassen van Γ in een decompositie

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma = \coprod_{j=1}^{d_p} \Gamma \gamma_j$$

(waarbij de eindigheid van d_p niet geheel triviaal is). Voor $f \in S_k(\Gamma)$ definiëren we nu

$$T_p(f) : \mathbb{H} \rightarrow \mathbb{C} \\ \tau \mapsto \sum_{j=1}^{d_p} \frac{\det(\gamma_j)^{k-1}}{(c\tau + d)^k} f(\gamma_j \tau).$$

Er kan eenvoudig aangetoond worden dat dit niet van de keuze van de representanten $\{\gamma_j\}_{j=1}^{d_p}$ afhangt en dat $T_p(f) \in S_k(\Gamma)$. Dat T_p lineair is, volgt direct uit de definities.

Het *Petersson-inproduct* op $S_k(\Gamma)$ wordt gegeven door

$$\langle f, g \rangle := \int_{\Gamma \backslash \mathbb{H}} f(\tau) \overline{g(\tau)} y^k d\nu(\tau)$$

waarbij $\tau = x + yi$ en $d\nu(\tau) := dx dy / y^2$ de hyperbolische maat op $\mathbb{H}$ is. Deze is namelijk invariant onder de actie van $\mathrm{GL}_2^+(\mathbb{R})$ op $\mathbb{H}$. Convergentie van de integraal volgt in essentie uit de groei-eigenschap (5).

We zullen ons vanaf nu beperken tot $\Gamma = \Gamma_0(N)$. Het mooie is dat alle T_p 's onderling commuteren en dat het Hermitische operatoren zijn voor $p \nmid N$ ten aanzien van het Petersson-inproduct op $S_k(\Gamma_0(N))$. Voor elke positieve echte deler M van N en positieve deler d van N/M geldt voor $f \in S_k(\Gamma_0(M))$ dat $g \in S_k(\Gamma_0(N))$ met $g(\tau) := f(d\tau)$. Zo'n g wordt een *oudvorm* van $S_k(\Gamma_0(N))$ genoemd. De deelruimte van $S_k(\Gamma_0(N))$ omspannen door de oudvormen heet de *oudruimte*, genoteerd $S_k(\Gamma_0(N))^{\mathrm{oud}}$. Het orthogonaal complement met betrekking tot het Petersson-inproduct heet de *nieuwruimte*, genoteerd

$$S_k(\Gamma_0(N))^{\mathrm{nieuw}} := (S_k(\Gamma_0(N))^{\mathrm{oud}})^{\perp}.$$

De Hecke-operatoren T_p behouden de beide ruimtes en op de nieuwruimte zijn alle T_p 's Hermitisch. De spectraalstelling uit de lineaire algebra geeft nu dat $S_k(\Gamma_0(N))^{\mathrm{nieuw}}$ een gemeenschappelijke basis van eigenvectoren, genaamd *Hecke-eigenvormen*, heeft ten aanzien van alle T_p 's. Het blijkt dat voor zulke eigen-

vormen f automatisch $a_1(f) \neq 0$ en we kunnen dus normaliseren tot $a_1(f) = 1$. Zo'n genormaliseerde Hecke-eigenvorm in de nieuwruimte noemen we een *nieuwvorm*. Deze nieuwvormen spelen een belangrijke rol in de beschrijving van Wiles' resultaat. We noemen nog dat voor een nieuwvorm f geldt dat $T_p(f) = a_p(f)f$ voor alle priemen p en dat f volledig vast ligt door alle $a_p(f)$ met p priem. De nieuwvormen in $S_k(\Gamma_0(N))$ vormen zo een canonieke basis voor $S_k(\Gamma_0(N))^{\mathrm{nieuw}}$. Aan elke $f \in S_k(\Gamma_0(N))$ kunnen we een L -reeks koppelen middels de Dirichlet-reeks

$$L_f(s) := \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s}. \quad (7)$$

Deze convergeert voor $s \in \mathbb{C}$ met $\Re s > 1 + k/2$ tot een holomorfe functie. Voor een nieuwvorm $f \in S_k(\Gamma_0(N))$ wordt de L -reeks ook gegeven door het Euler-product

$$L_f(s) = \prod_{p \nmid N} (1 - a_p(f)p^{-s} + p^{k-1-2s})^{-1} \cdot \prod_{p \mid N} (1 - a_p(f)p^{-s})^{-1}$$

waarbij p over de priemgetallen loopt. Vergelijking met (7) geeft weer hoe alle Fourier-coëfficiënten van f recursief bepaald worden door de $a_p(f)$ met p priem. In het bijzonder geeft dit zo voor $\Delta \in S_{12}(\Gamma_0(1))$ de eerste twee eerder genoemde eigenschappen van τ . Laat verder voor een nieuwvorm f ,

$$\xi_f(s) := N^{s/2} (2\pi)^{-s} \Gamma(s) L_f(s).$$

Deze functie voldoet aan de functionaal-vergelijking

$$\xi_f(s) = \pm \xi_f(k-s)$$

voor alle $s \in \mathbb{C}$ en een teken $\pm$ dat alleen van f afhangt (de eigenwaarde van de bijbehorende Fricke-involutie). In het bijzonder heeft $L_f(s)$ een analytische voortzetting tot het hele complexe vlak.

Voor $\Gamma_1(N)$ geldt een soortgelijk verhaal als boven, alleen moeten we dan nog een extra type (eenvoudige) Hecke-operatoren introduceren en de Hermitische eigenschap wordt vervangen door 'normaal', wat volstaat voor de benodigde spectraalstelling. Uiteindelijk krijgen we dan ook *nieuwvormen* voor $S_k(\Gamma_1(N))$ die op een canonieke wijze een basis voor $S_k(\Gamma_1(N))^{\mathrm{nieuw}}$ vormen.

Modulariteit

Definitie 2. Een elliptische kromme E over $\mathbb{Q}$ heet *modulair* als er een nieuwvorm $f \in S_2(\Gamma_0(N(E)))$ is zodat $a_p(E) = a_p(f)$ voor alle priemgetallen p .

Merk op dat dit laatste direct equivalent is met $L_E(s) = L_f(s)$. Er zijn vele andere equivalente definities, ook meer meetkundig georiënteerde, maar daar gaan we nu niet verder op in. Het vermoeden dat alle elliptische krommen over $\mathbb{Q}$ modulair zijn, stond bekend als het vermoeden van Shimura–Taniyama–Weil (en onder vele andere namen, inclusief de meeste permutaties van niet lege deelverzamelingen van de drie namen). Inmiddels is het volledig bewezen.

Stelling 3 (Modulariteit). *Alle elliptische krommen over $\mathbb{Q}$ zijn modulair.*

Modulariteit van alle semi-stabiele elliptische krommen over $\mathbb{Q}$ is in 1994 bewezen door Wiles [30], met hulp van Taylor [29]. Dit volstond voor het voltooien van een bewijs voor de Laatste Stelling van Fermat. Vervolgens werden de methoden van Wiles en Taylor gegeneraliseerd, waarbij een aantal gecompliceerde technische problemen overwonnen werden, totdat uiteindelijk in 1999 de volledige modulariteitsstelling hierboven werd bewezen door Breuil, Conrad, Diamond en Taylor [3].

Beschouw als voorbeeld van modulariteit de elliptische kromme E gegeven door de minimale Weierstrass-vergelijking

$$y^2 + y = x^3 - x^2.$$

De kromme heeft enkel voor $p = 11$ een singuliere reductie, waar het een knooppunt heeft. Dit geeft voor de conductor $N(E) = 11$. Verder hebben we heel concreet voor alle priemen p ,

$$\#\tilde{E}(\mathbb{F}_p) = \#\{(x, y) \in \mathbb{F}_p^2 : y^2 + y = x^3 - x^2\} + 1.$$

De extra +1 komt van het ‘punt op oneindig’. We kunnen een klein tabelletje maken van $\#\tilde{E}(\mathbb{F}_p)$ en dus ook van $a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p)$:

p	2	3	5	7	11	13	17	19	...	2017
$\#\tilde{E}(\mathbb{F}_p)$	5	5	5	10	11	10	20	20	...	2035
$a_p(E)$	-2	-1	1	-2	1	4	-2	0	...	-17

Volgens de modulariteitstelling is er een

nieuwvorm $f \in S_2(\Gamma_0(11))$ zodanig dat $a_p(E) = a_p(f)$ voor alle priemen p . Met standaard theorie kan men checken dat $S_2(\Gamma_0(11))^{\text{nieuw}} = S_2(\Gamma_0(11))$ eendimensionaal is en dat $f := q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2$ een genormaliseerde vorm in deze ruimte definieert. Dus dit moet de nieuwvorm f uit de modulariteitstelling zijn. Inderdaad geeft (formeel) expanderen van het product dat

$$\begin{aligned} f = & q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 \\ & - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} \\ & + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} \\ & + 4q^{18} + 2q^{20} + \dots - 17q^{2017} + \dots \end{aligned}$$

Hier is een klein tabelletje voor $a_p(f)$:

p	2	3	5	7	11	13	17	19	...	2017
$a_p(f)$	-2	-1	1	-2	1	4	-2	0	...	-17

We zien dat voor alle priemen p in de voorgaande twee tabellen we inderdaad hebben dat $a_p(E) = a_p(f)$.

Vermoeden van Birch en Swinnerton-Dyer
Laat E een elliptische kromme over $\mathbb{Q}$ zijn. Het is een stelling dat de groep van rationale punten $E(\mathbb{Q})$ eindig voortgebracht is, oftewel

$$E(\mathbb{Q}) \simeq T \times \mathbb{Z}^r$$

voor een eindige groep T en $r \in \mathbb{Z}_{\geq 0}$ die de *rang* van E wordt genoemd en genoteerd als $\text{rang}(E(\mathbb{Q}))$. Aangezien dankzij de modulariteit van E geldt dat $L_E(s) = L_f(s)$ voor een nieuwvorm f en $L_f(s)$ een analytische voortzetting tot $\mathbb{C}$ heeft, volgt nu direct dat $L_E(s)$ een analytische voortzetting tot $\mathbb{C}$ heeft. Evenzo voldoet de functie

$$\xi_E(s) := N(E)^{s/2} (2\pi)^{-s} \Gamma(s) L_E(s)$$

aan de functionaalvergelijking

$$\xi_E(s) = \pm \xi_E(2-s)$$

voor alle $s \in \mathbb{C}$ en een zeker teken $\pm$ dat enkel van E afhangt, welke vermoedelijk $(-1)^{\text{rang}(E(\mathbb{Q}))}$ is. Merk op dat $N(E)^{s/2} (2\pi)^{-s} \Gamma(s) \neq 0$ als $s = 1$, dus $L_E(s)$ is analytisch in een omgeving van $s = 1$. Vermoedelijk reflecteert $L_E(s)$ bij $s = 1$ diepe aritmetische informatie over E . Introduceer de *analytische rang* $r_{\text{an}}(E) := \text{ord}_{s=1}(L_E(s))$, oftewel de nulpuntsorde van $L_E(s)$ bij $s = 1$. Introduceer ook de *algebraïsche rang* $r_{\text{al}}(E) := \text{rang}(E(\mathbb{Q}))$.

Vermoeden 4 (Zwak Birch–Swinnerton-Dyer-vermoeden). *Voor alle elliptische krommen E over $\mathbb{Q}$ geldt*

$$r_{\text{an}}(E) = r_{\text{al}}(E).$$

Er bestaat ook een sterkere versie van dit vermoeden, die de eerste coëfficiënt ongelijk 0 in de Taylor-expansie van $L_E(s)$ rond $s = 1$ relateert aan andere (aritmetische) invarianten van E . Met name de orde van zijn zogenaamde *Shafarevich–Tate-groep*, waarvan men *vermoedt* dat die eindig is. Verder zijn er natuurlijke generalisaties waarbij $\mathbb{Q}$ wordt vervangen door een algemeen getallenlichaam, en eventueel tevens E wordt vervangen door een zogenaamde ‘abelse variëteit’ van willekeurige dimensie. Vermoeden 4 is echter al moeilijk genoeg en staat, naast andere grote problemen zoals de Riemann-hypothese, bekend als één van de zeven millenniumproblemen van het Clay Mathematics Institute (CMI), waarvan de oplossing naast eeuwige roem ook nog een miljoen dollar oplevert. (Eén zo’n probleem, bekend als het Poincaré-vermoeden, is inmiddels opgelost.) De officiële beschrijving voor het CMI van Vermoeden 4 als millenniumprobleem is trouwens door Wiles gegeven.

Hij heeft ook, samen met Coates, in de jaren zeventig één van de eerste resultaten in de richting van het Birch–Swinnerton-Dyer-vermoeden voor een grote klasse van elliptische krommen verkregen [6]. In de jaren tachtig volgde nog belangrijke resultaten van Gross–Zagier en Kolyvagin. Hiermee was toen bekend dat voor *modulaire* elliptische krommen E over $\mathbb{Q}$ geldt dat

$$r_{\text{an}}(E) \leq 1 \Rightarrow r_{\text{an}}(E) = r_{\text{al}}(E). \quad (8)$$

Samenvattend heeft de modulariteit van elliptische krommen dus (ten minste) twee directe belangrijke implicaties voor het Birch–Swinnerton-Dyer-vermoeden. Voor elke elliptische krommen E over $\mathbb{Q}$ geldt ten eerste dat de L -functie $L_E(s)$ een analytische continuatie tot een omgeving van $s = 1$ (zelfs heel $\mathbb{C}$) heeft, waarmee $r_{\text{an}}(E)$ überhaupt gedefinieerd kan worden. En ten tweede is (8) nu onvoorwaardelijk waar.

Generalisaties van Wiles’ resultaten

We bespreken eerst enkele generalisaties van Wiles’ modulariteitsresultaat. Deze maken het (onder andere) mogelijk dat som-

mige generalisaties van de Laatste Stelling van Fermat verkregen kunnen worden. Dit zullen we ook aanstippen.

Modulariteitsresultaten

Er zijn veel richtingen waarin modulariteit gegeneraliseerd is (en nog kan worden). We zullen ons hier voornamelijk beperken tot enige belangrijke klassen van elliptische krommen over getallenlichamen, maar maken ook een klein uitstapje naar Galois-representaties.

Alle elliptische krommen over $\mathbb{Q}$. De methoden van [30] en [29] werden snel uitgebreid om modulariteit aan te tonen van een veel grotere klasse van elliptische krommen over $\mathbb{Q}$ dan de semi-stabiele. De verwachting was verder dat de modulariteit van *alle* elliptische krommen over $\mathbb{Q}$ binnen handbereik was. Hoewel natuurlijk zeker niet eenvoudig, duurde het niet lang voordat de modulariteit van alle elliptische krommen over $\mathbb{Q}$ met conductor niet deelbaar door 3^3 bewezen was. Dit laatste komt neer op $\delta_3 = 0$. Om ‘technische problemen bij reductie modulo 3’ te boven te komen als $\delta_3 > 0$ moest zeker nog verder hard gewerkt worden. Dit lukte inderdaad door Breuil, Conrad, Diamond en Taylor [3], waarmee Stelling 3 uiteindelijk bewezen was. Zie [9] voor een uitgebreid overzicht.

Serres modulariteitsvermoeden. Dit is een vergaand vermoeden van Serre [23] dat zegt dat bepaalde Galois-representaties isomorf zijn aan (reducties van) Galois representaties die komen van nieuwvormen voor $\Gamma_1(N)$. Het is uiteindelijk volledig bewezen door Khare, Wintenberger en Kisin, zie [14] en [15].

We beginnen met een elementair voorbeeld waarin we in eerste instantie de Galois-representaties even onder tafel vegen. Beschouw het polynoom met gehele coëfficiënten $g = x^3 - x - 1$. We merken op dat g geen nulpunten in $\mathbb{Q}$ heeft en dat de discriminant -23 is. Voor elk priemgetal p noteren we met n_p het aantal nulpunten (zonder op de multipliciteit te letten) van g modulo p , oftewel

$$n_p := \#\{x \in \mathbb{F}_p : x^3 - x - 1 = 0\}.$$

Voor $p \neq 23$ kan g modulo p irreducibel blijven, splitsen in een (irreducibel) kwadratisch en een lineair stuk, of splitsen in drie verschillende (monische) lineaire stukken.

Voor zulke p hebben we dus $n_p \in \{0, 1, 3\}$. Verder $g \equiv (x-10)^2(x-3) \pmod{23}$, dus $n_{23} = 2$. Hieronder staat een klein tabelletje voor n_p :

p	2	3	5	7	11	13	17	19	23	29	...	59
n_p	0	0	1	1	1	0	1	1	2	0	...	3

We brengen de nieuwvorm

$$\begin{aligned} \Delta &:= q \prod_{n=1}^{\infty} (1 - q^n)^{24} \\ &= \sum_{n=1}^{\infty} \tau(p) q^n \in S_{12}(\Gamma_0(1)) \end{aligned}$$

in herinnering. Noteren we met $\overline{\tau(p)} \in \mathbb{F}_{23} = \{0, 1, 2, \dots, 22\}$ de reductie van $\tau(p)$ modulo 23, dan hebben we hiervoor het volgende tabelletje:

p	2	3	5	7	11	13	17	19	23	29	...	59
$\overline{\tau(p)}$	22	22	0	0	0	22	0	0	1	22	...	2

Bij vergelijking van de tabellen voor n_p en $\overline{\tau(p)}$ vindt de lezer waarschijnlijk snel het opzienbarende patroon

$$n_p - 1 \equiv \overline{\tau(p)} \pmod{23}. \quad (9)$$

Men kan bewijzen dat dit inderdaad voor alle priemgetallen p geldt!

We willen dit resultaat nog even herschrijven in termen van een *Galois-representatie*. Laat K het kleinste deellichaam van $\mathbb{C}$ zijn waarin de drie nulpunten $\alpha_1, \alpha_2, \alpha_3$ van g liggen. Dan is K een getallenlichaam van graad 6 over $\mathbb{Q}$. De Galoisgroep $\text{Gal}(K/\mathbb{Q})$ is per definitie de groep van lichaamsautomorfismen $\sigma: K \rightarrow K$ (met samenstelling als operatie), waarbij lichaamsautomorfisme betekent dat σ bijectief is en voldoet aan $\sigma(x+y) = \sigma(x) + \sigma(y)$ en $\sigma(xy) = \sigma(x)\sigma(y)$ voor alle $x, y \in K$. Elke $\sigma \in \text{Gal}(K/\mathbb{Q})$ induceert een permutatie van de nulpunten $\alpha_1, \alpha_2, \alpha_3$ en wordt hier volledig door bepaald. In dit geval is elke permutatie van de nulpunten van g voort te zetten tot een $\sigma \in \text{Gal}(K/\mathbb{Q})$ (want g is irreducibel en $\text{Discriminant}(g) = -23$ is geen kwadraat in $\mathbb{Q}$). Derhalve kunnen we $\text{Gal}(K/\mathbb{Q})$ identificeren met de volledige permutatiegroep op drie elementen. We schrijven $\text{Gal}(K/\mathbb{Q}) = \{e, (12), (13), (23), (123), (132)\}$, waarbij bijvoorbeeld een permutatie zoals (123) staat voor het lichaamsautomorfisme $\sigma: K \rightarrow K$ met $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_3$, $\sigma(\alpha_3) = \alpha_1$, en e staat voor de identiteit. We definiëren nu het groepshomomorfisme

$$\rho: \text{Gal}(K/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_{23})$$

door middel van

$$\begin{aligned} (123) &\mapsto R := \begin{pmatrix} 11 & 8 \\ -8 & 11 \end{pmatrix}, \\ (12) &\mapsto S := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned}$$

Voor elk priemgetal $p \neq 23$ definiëren we nu een *Frobenius-element* $\text{Frob}_p \in \text{Gal}(K/\mathbb{Q})$ als volgt

$$\text{Frob}_p := \begin{cases} (123), & \text{als } n_p = 0, \\ (12), & \text{als } n_p = 1, \\ e, & \text{als } n_p = 3. \end{cases}$$

Merk op dat voor de sporen (de som van de diagonaalelementen, genoteerd als Tr) van S , T en I (de identiteit in $\text{GL}_2(\mathbb{F}_{23})$) we hebben $\text{Tr}(R) = 22$, $\text{Tr}(S) = 0$, $\text{Tr}(I) = 2$. Voor all $p \neq 23$ zien we nu dat (9) equivalent is met $\text{Tr}(\rho(\text{Frob}_p)) = \overline{\tau(p)}$. Het bovenstaande kunnen we als volgt generaliseren. Laat h een irreducibel polynoom van graad $n > 0$ met rationale coëfficiënten zijn en laat L het kleinste deellichaam van $\mathbb{C}$ zijn waarin alle n nulpunten $\alpha_1, \alpha_2, \dots, \alpha_n$ van h liggen. De groep $\text{Gal}(L/\mathbb{Q})$ van lichaamsautomorfismen van L kunnen we identificeren met een ondergroep van de permutatiegroep op n elementen door te kijken wat de acties van de automorfismen $\sigma \in \text{Gal}(L/\mathbb{Q})$ op de n nulpunten van h zijn. Laat l een priemgetal en $\mathbb{F}$ een eindige lichaamsuitbreiding van $\mathbb{F}_l$ zijn en beschouw een Galois-representatie

$$\rho: \text{Gal}(L/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}),$$

oftewel ρ is een groepshomomorfisme. Laat $c \in \text{Gal}(L/\mathbb{Q})$ complexe conjugatie beperkt tot L zijn, dan noemen we ρ *oneven* als $\det(\rho(c)) = -1$. Verder noemen we ρ *absoluut irreducibel* als er geen $M \in \text{GL}_2(\overline{\mathbb{F}})$ is (met $\overline{\mathbb{F}}$ een algebraïsche afsluiting van $\mathbb{F}$) zodat $M \text{Beeld}(\rho) M^{-1}$ bestaat uit bovendiagonaalmatrices. In het voorgaande voorbeeld is eenvoudig in te zien dat de Galois-representatie oneven is, met ietsje meer werk kan ook aangetoond worden dat deze absoluut irreducibel is. Serres modulariteitsvermoeden zegt nu in essentie dat voor een Galois-representatie ρ zoals hierboven die oneven en absoluut irreducibel is er een nieuwvorm $f \in S_k(\Gamma_1(N))$ bestaat voor zekere $k \geq 2$ en $N \geq 1$ en een priemideaal λ (in de ring van gehelen van het getallenlichaam voortgebracht door de Fourier-coëfficiënten van f) met $l \in \lambda$ zodat voor alle priemgetallen $p \nmid Nl$,

$$\text{Tr}(\rho(\text{Frob}_p)) = \overline{a_p(f)}$$

waarbij $\overline{a_p(f)}$ de reductie van a_p modulo

λ is (op een consistente wijze ingebed in $\mathbb{F}$). Hierbij is een *Frobenius-element* $\text{Frob}_p \in \text{Gal}(L/\mathbb{Q})$ een afbeelding waarvoor er een priemideaal $\wp \subset \mathcal{O}_L$ bestaat met $p \in \wp$, zó dat $\text{Frob}_p(\wp) = \wp$ en $\text{Frob}_p(x) \equiv x^p \pmod{\wp}$ voor alle $x \in \mathcal{O}_L$. Voor $p \nmid N$ is zo'n Frobenius-element Frob_p uniek op conjugatie na, zodat $\text{Tr}(\rho(\text{Frob}_p))$ dus uniek bepaald is.

Q-krommen. Bovenstaande heeft als gevolg dat bepaalde hogerdimensionale generalisaties van elliptische krommen over $\mathbb{Q}$, namelijk zogenaamde GL_2 -type abelse variëteiten over $\mathbb{Q}$, modulaire zijn. Wat dit precies inhoudt, gaan we hier verder niet bespreken, maar nauw hiermee samenhangend is de modulariteit van Q-krommen. Dat dit een gevolg van Serres modulariteitsvermoeden is, was al door Ribet bewezen in [21]. Om uit te leggen wat een Q-kromme is, beginnen we met een willekeurige elliptische kromme E over een getallenlichaam K . Zonder verlies van algemeenheid kunnen we K indien nodig iets groter kiezen zodat K een eindige Galois-uitbreiding van $\mathbb{Q}$ is, dat wil zeggen dat er een polynoom g met rationale coëfficiënten is zodat K het kleinste deellichaam van $\mathbb{C}$ is dat alle nulpunten van g bevat (zo'n g kan trouwens altijd irreducibel en niet-constant gekozen worden). Voor elke $\sigma \in \text{Gal}(K/\mathbb{Q})$ krijgen we een elliptische kromme E^σ door σ simpelweg los te laten op alle coëfficiënten van een Weierstrass-vergelijking voor E . Is E bijvoorbeeld gegeven door $y^2 = x^3 + ax^2 + bx + c$ (met $a, b, c \in K$), dan wordt E^σ gegeven door $y^2 = x^3 + \sigma(a)x^2 + \sigma(b)x + \sigma(c)$. Voor een niet-triviale σ kan men afvragen of E^σ isogeen is aan E . Dit laatste houdt grosso modo in dat er rationale functies (quotiënten van polynomen) in x en y met coëfficiënten in K zijn die E afbeelden op E^σ . Dit is equivalent met de uitspraak dat $a_\wp(E) = a_\wp(E^\sigma)$ voor alle priemidealen $\wp \subset \mathcal{O}_K$ met $\wp \neq 0$, maar deze equivalentie is hoogst niet-triviaal. Als voor elke $\sigma \in \text{Gal}(K/\mathbb{Q})$ nu geldt dat E^σ isogeen is aan E , dan noemen we E een Q-kromme. We merken op dat alle elliptische krommen over $\mathbb{Q}$ Q-krommen zijn, maar er zijn ook oneindig veel essentieel verschillende andere Q-krommen. Als voorbeeld geven we

$$E: y^2 = x^3 + (156\sqrt{-3} - 135)x + 2(546\sqrt{-3} + 41).$$

De Galoisgroep van $K := \mathbb{Q}(\sqrt{-3})$ bestaat uit de identiteitsafbeelding op K en complexe conjugatie c (beperkt tot K). Door in de vergelijking voor E elke $\sqrt{-3}$ te vervangen voor $-\sqrt{-3}$ krijgen we

$$E^c: y^2 = x^3 + (-156\sqrt{-3} - 135)x + 2(-546\sqrt{-3} + 41).$$

Dat E een Q-kromme is, volgt nu omdat we een afbeelding (een 3-isogenie) met behulp van rationale functies van E naar E^c hebben, expliciet:

$$\begin{aligned} x &\mapsto \frac{-x^3/3 - 6x^2 - (104\sqrt{-3} + 99)x - (520\sqrt{-3} + 4216/3)}{x^2 + 18x + 81} \\ y &\mapsto \frac{\sqrt{-3}x^3y/9 + 3\sqrt{-3}x^2y + (104 + 3\sqrt{-3})xy + (104 - 5759\sqrt{-3}/9)y}{x^3 + 27x^2 + 243x + 729}. \end{aligned}$$

Het begin van de q -expansies van de nieuwvormen in $S_2(\Gamma_0(63))$ worden gegeven door

$$\begin{aligned} f &= q + q^2 - q^4 + 2q^5 - q^7 - 3q^8 \\ &\quad + 2q^{10} - 4q^{11} + \dots \\ g_1 &= q + \sqrt{3}q^2 + q^4 - 2\sqrt{3}q^5 + q^7 \\ &\quad - \sqrt{3}q^8 - 6q^{10} + 2\sqrt{3}q^{11} + \dots \\ g_2 &= q - \sqrt{3}q^2 + q^4 + 2\sqrt{3}q^5 + q^7 \\ &\quad + \sqrt{3}q^8 - 6q^{10} - 2\sqrt{3}q^{11} + \dots \end{aligned}$$

Nu is E modulaire in de zin dat

$$L_E(s) = L_{g_1}(s)L_{g_2}(s).$$

Voor algemene Q-krommen over een getallenlichaam K houdt modulariteit in dat na het eventueel vervangen van K voor een groter getallenlichaam (ook al was K Galois en alle relevante isogenieën gedefinieerd over K) dat hun L -functie gelijk is aan een product van L -functies van nieuwvormen in $S_2(\Gamma_1(N))$ voor zekere waarden van N .

Hilbert-modulariteit. Voor bepaalde elliptische krommen over getallenlichamen groter dan $\mathbb{Q}$ hebben we in het voorgaande een vorm van modulariteit gezien. Echter, Q-krommen zijn relatief 'zeldzaam'. De hoop is dat alle elliptische krommen over alle getallenlichamen modulaire zijn op één of andere manier (wat een speciaal geval van de Langlands-vermoedens is). In het geval dat het getallenlichaam totaal reëel is (zie hieronder), is er aardige progressie geboekt op dit terrein en kan de modulariteit uitgedrukt worden met behulp van zogenaamde Hilbert-modulaire vormen.

Laat g een irreducibel polynoom van graad $n > 0$ met rationale coëfficiënten zijn. Stel verder dat alle (a priori complexe) nulpunten $\alpha := \alpha_1, \alpha_2, \dots, \alpha_n$ van g reëel zijn.

Een getallenlichaam van de vorm $K := \mathbb{Q}(\alpha)$ noemen we *totaal reëel*. Elk element in K is van de vorm $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$, met unieke $a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$. We beschouwen voor $i = 1, 2, \dots, n$ de inbedding

$$\begin{aligned} \sigma_i: K &\rightarrow \mathbb{R} \\ a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} &\mapsto a_0 + a_1\alpha_i + \dots + a_{n-1}\alpha_i^{n-1}. \end{aligned}$$

Nemen we bijvoorbeeld het totaal reële getallenlichaam $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, dan hebben we naast de identiteitsafbeelding $K \rightarrow \mathbb{R}: x \mapsto x$ nog de afbeelding die een element $a + b\sqrt{2}$ naar $a - b\sqrt{2}$ stuurt.

Voor het bespreken van Hilbert-modulaire vormen beschouwen we om te beginnen de groepen

$$\text{GL}_2(\mathcal{O}_K) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathcal{O}_K, \right. \\ \left. ad - bc \in \mathcal{O}_K^* \right\},$$

$$\text{GL}_2^+(\mathcal{O}_K) := \{ \gamma \in \text{GL}_2(\mathcal{O}_K) : \sigma_i(\det(\gamma)) > 0 \text{ voor } i = 1, \dots, n \}.$$

We kunnen $\text{GL}_2^+(\mathcal{O}_K)$ inbedden in $(\text{GL}_2^+(\mathbb{R}))^n$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(\begin{pmatrix} \sigma_1(a) & \sigma_1(b) \\ \sigma_1(c) & \sigma_1(d) \end{pmatrix}, \dots, \begin{pmatrix} \sigma_n(a) & \sigma_n(b) \\ \sigma_n(c) & \sigma_n(d) \end{pmatrix} \right).$$

Via de actie (3) van $\text{GL}_2^+(\mathbb{R})$ op $\mathbb{H}$ verkrijgen we zo een actie van $\text{GL}_2^+(\mathcal{O}_K)$ op het n -voudig bovenhalfvlak $\mathbb{H}^n$. Merk op voor $K = \mathbb{Q}$ dat $\text{GL}_2^+(\mathcal{O}_K) = \text{SL}_2(\mathbb{Z})$ en dat bovenstaande actie reduceert tot de 'standaard' actie van $\text{SL}_2(\mathbb{Z})$ op $\mathbb{H}$. Voor elk ideaal $0 \neq \mathcal{N} \subset \mathcal{O}_K$ introduceren we, analoog aan $\Gamma_0(N)$ in het $\text{SL}_2(\mathbb{Z})$ geval, de groep

$$\begin{aligned} \Gamma_0(\mathcal{N}) &:= \left\{ \gamma \in \text{GL}_2^+(\mathcal{O}_K) \right. \\ &\quad \left. \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{\mathcal{N}} \right\}. \end{aligned}$$

Evenzo kunnen we $\Gamma_1(N)$ generaliseren (evenals andere congruentieondergroepen). Globaal gezegd is een *Hilbert-modulaire spitsvorm* voor $\Gamma_0(\mathcal{N})$ van (parallel) gewicht k een holomorfe functie $f: \mathbb{H}^n \rightarrow \mathbb{C}$ die voor alle $z = (z_1, \dots, z_n) \in \mathbb{H}^n$ en $\gamma \in \Gamma_0(\mathcal{N})$ transformeert als

$$f(\gamma z) = \left(\prod_{i=1}^n \frac{(\sigma_i(c)z_i + \sigma_i(d))^k}{\sigma_i(\det(\gamma))^{k-1}} \right) f(z)$$

en verder bepaald (begrensd) groeigedrag heeft (dit wordt ook wel omschreven als 'nul zijn op de spitsen'). Deze functies vormen weer een eindigdimensionale $\mathbb{C}$ -vectorruimte, genoteerd als $S_k(\Gamma_0(\mathcal{N}))$.

Aan de hand hiervan kan men uiteindelijk weer bepaalde $\mathbb{C}$ -vectorruimtes $S_k(\mathcal{N})^{\text{nieuw}} \subset S_k(\mathcal{N})$ introduceren (met $S_k(\mathcal{N}) = S_k(\Gamma_0(\mathcal{N}))$) als het zogenaamde strikte klassegetal h gelijk aan 1 is, maar $S_k(\mathcal{N})$ is ingewikkelder voor $h > 1$, en daarop werkende Hecke-operatoren $T_\wp$ voor priemidealen $0 \neq \wp \subset \mathcal{O}_K$. Dit geeft het analogon van $S_k(\Gamma_0(N))^{\text{nieuw}} \subset S_k(\Gamma_0(N))$ en Hecke-operatoren T_p voor p priem. Een *Hilbert-nieuwvorm* is dan een $f \in S_k(\mathcal{N})^{\text{nieuw}}$ die simultaan eigenvector is voor alle $T_\wp$'s (+ een keuze van normalisatie van f). Voor zo'n f definiëren we $a_\wp(f)$'s als bijbehorende eigenwaardes, oftewel

$$T_\wp f = a_\wp(f)f.$$

De $a_\wp(f)$'s kunnen trouwens ook weer gerelateerd worden aan coëfficiënten van een (n -dimensionale) Fourier-ontwikkeling van f . Er is ook weer een L -functie,

$$L_f(s) := \prod_{\wp \nmid N} (1 - a_\wp(f)N(\wp)^{-s} + N(\wp)^{1-2s})^{-1} \cdot \prod_{\wp \mid N} (1 - a_\wp(f)N(\wp)^{-s})^{-1}$$

die convergeert voor $s \in \mathbb{C}$ met reëel deel strikt groter dan $3/2$, een analytische continuïteit heeft tot heel $\mathbb{C}$ en aan een natuurlijke functionaalvergelijking voldoet.

Het *Hilbert-modulair* zijn van een elliptische kromme E over een totaal reëel getallenlichaam K is nu per definitie dat er een Hilbert-nieuwvorm $f \in S_2(\mathcal{N})$ is, met $\mathcal{N}$ de conductor van E en voor alle priemidealen $0 \neq \wp \subset \mathcal{O}_K$ geldt $a_\wp(E) = a_\wp(f)$. Merk op dat dit laatste equivalent is aan $L_E(s) = L_f(s)$. Of alle elliptische krommen over alle totaal reële getallenlichamen Hilbert-modulair zijn, is een groot open probleem en vergaande generalisatie van het Shimura–Taniyama–Weil-vermoeden. In een aantal gevallen is die modulariteit echter recentelijk bewezen. Een spectaculair voorbeeld is het bewijs door Freitas, Siksek en Le Hung [11] van Hilbert modulariteit voor alle elliptische krommen over alle reële kwadratische getallenlichamen, oftewel lichamen van de vorm $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ met d positief geheel en geen kwadraat.

Trouwens, stel K is een totaal reëel lichaam en $F = K(\sqrt{x})$ is een kwadratische uitbreiding verkregen door een kwadratische wortel van een element $x \in K$ toe te voegen, onder de extra voorwaarde dat $\sigma(x) < 0$ voor elke inbedding $\sigma : K \rightarrow \mathbb{R}$.

Dan kondigen Allen, Calegari, Caraiani, Gee, Helm, Le Hung, Newton, Scholze, Taylor en Thorne [27] aan dat elliptische krommen over K modulair worden (in een zin die we niet nader zullen omschrijven hier) na eventueel een eindige uitbreiding K'/K , alhoewel er op het moment van het schrijven van dit artikel nog geen preprint beschikbaar is. Dit nieuwe bewijs is mogelijk door nieuwe technieken die in de laatste jaren zijn ontwikkeld door Scholze [22] en Caraiani en Scholze [4].

Diofantische resultaten

De oorspronkelijke motivatie voor Wiles om de modulariteit van (semi-stabiele) elliptische krommen over $\mathbb{Q}$ te bewijzen, was om een bewijs voor de Laatste Stelling van Fermat te verkrijgen. Dit modulariteitsbewijs en generalisaties hiervan vinden hun toepassingen ook weer in het oplossen van andere diofantische vergelijkingen. Een belangrijke klasse zijn de zogenaamde gegeneraliseerde Fermat-vergelijkingen: laat $p, q, r \in \mathbb{Z}_{\geq 2}$ en beschouw de diofantische vergelijking

$$x^p + y^q = z^r, \quad x, y, z \in \mathbb{Z}, \quad \gcd(x, y, z) = 1. \quad (10)$$

De extra gcd-eis staat er om allerlei ‘flauwe’ oplossingen uit te sluiten: voor de exponenten $(p, q, r) = (3, 5, 7)$ bijvoorbeeld vindt men eenvoudig de identiteit

$$(r^{12}s^{28}(r+s)^{30})^3 + (r^7s^{17}(r+s)^{18})^5 = (r^5s^{12}(r+s)^{13})^7.$$

Verder noemen we een oplossing $(x, y, z) = (a, b, c)$ van (10) *niet-triviaal* als $abc \neq 0$.

Voor het bewijs van de Laatste Stelling van Fermat begint men met het construeren van een zogenaamde Frey-kromme: aan een hypothetische niet-triviale oplossing $a^l + b^l = c^l$ met $l \geq 5$ priem kent men toe de elliptische kromme over $\mathbb{Q}$,

$$E : y^2 = f(x), \quad f(x) := x(x - a^l)(x + b^l).$$

Voor de discriminant van f geldt

$$\Delta(f) = a^{2l}b^{2l}(a^l + b^l)^2 = (abc)^{2l}.$$

Om tot een tegenspraak te komen, gebruikt men zogenaamde niveauverlaging à la Ribet [20]. Hiervoor heeft men naast een technisch ‘irreducibiliteits-ingrediënt’ (à la Mazur) nodig dat E modulair is. De verdere aritmetische eigenschappen van E die gebruikt worden, zijn ten eerste dat $\Delta(f) = \alpha\beta^l$ met $\alpha, \beta \in \mathbb{Z}$ en α een getal dat niet van de (hypothetische) oplossing afhangt (in dit geval is simpelweg $\alpha = 1$).

Ten tweede moeten de priemgetallen p waarvoor $f(x)$ modulo p een drievoudig nulpunt krijgt ook niet van de (hypothetische) oplossing afhangen. In dit geval krijgen we dat voor elkaar om zonder verlies van algemeenheid aan te nemen dat $\gcd(a, b, c) = 1$, zodat voor geen enkel priemgetal p alle drie de nulpunten $0, a^l$ en $-b^l$ van $f(x)$ gelijk worden modulo p . Na het samensmeden van alle ingrediënten komt men er in dit geval op uit dat er bij een oplossing een nieuwvorm in $S_2(\Gamma_0(2))$ hoort. Laatstgenoemde ruimte is nuldimensionaal, zodat de geconstrueerde nieuwvorm niet kan bestaan, een tegenspraak. Samen met de exponentengevallen $l = 3, 4$, volgt de Laatste Stelling van Fermat.

In andere gevallen kan men soms ook een bijbehorende Frey-kromme construeren. Om zo de diofantische vergelijking op te lossen is in ieder geval modulariteit van de kromme nodig. We geven een paar voorbeelden.

Neem $(p, q, r) = (l, l, 2)$ met $l \geq 7$ priem in (10), dus we beschouwen een (hypothetische) oplossing $a^l + b^l = c^2$. In [7] is bewezen dat er dan geen niet-triviale oplossingen zijn. De Frey-kromme is

$$E : y^2 = f(x), \quad f(x) := x^3 + 2cx^2 + a^p x,$$

met discriminant

$$\Delta(f) = 4a^{2l}(c^2 - a^l) = 4(a^2b)^l.$$

We merken op dat E niet semi-stabiel is, maar de modulariteit van E is een relatief kleine uitbreiding van het semi-stabiele geval, welke vrijwel na Wiles' resultaat beschikbaar kwam. Verder kan men samen met een paar gevallen voor kleine exponenten aantonen dat voor $(p, q, r) = (l, l, 2)$ er geen niet-triviale oplossingen zijn voor alle gehele $l \geq 4$.

Nemen we nu het geval $(p, q, r) = (l, l, 3)$, ook beschouwd in [7], dan heeft de bijbehorende Frey-kromme E een conductor N die deelbaar is door 3^3 . Bij publicatie was de modulariteit van zulke E nog niet bekend, waardoor het diofantisch resultaat nog voorwaardelijk was. Dankzij de volle kracht van de modulariteit van alle elliptische krommen over $\mathbb{Q}$, samen met wat gevallen voor kleine exponenten, is nu onvoorwaardelijk bewezen dat er in dit geval geen niet-triviale oplossingen zijn voor gehele $l \geq 3$.

Voor $(p, q, r) = (4, 2, l)$ met $l \geq 211$ wordt in [10] de Frey-kromme

$E: y^2 = f(x)$,
 $f(x) := x^3 + 2(1+i)ax^2 + (b+ia^2)x$,
 beschouwd (met $i = \sqrt{-1}$), waarbij

$$\Delta(f) = -4i(a^2 - ib)^2(a^2 + ib).$$

De factorisatie $(a^2 - ib)(a^2 + ib) = c^l$ geeft dat $\Delta(f)$ van de gewenste vorm is. Nu is E een $\mathbb{Q}$ -kromme over $\mathbb{Q}(i)$ en derhalve modulair. Een isogenie van E naar de Galoisgeconjugeerde van E (gegeven door de vergelijking van E met overal i vervangen door $-i$) wordt expliciet gegeven door

$$(x, y) \mapsto \left(\frac{1}{2}i(y^2/x^2), -\frac{1}{4}(1-i)y(b+ia^2-x^2)/x^2\right).$$

Samen met gevallen voor kleine exponenten is er inmiddels bekend dat voor $(p, q, r) = (4, 2, l)$ er geen niet-triviale oplossingen zijn voor gehele $l \geq 4$.

Er zijn trouwens ook voorbeelden waarin er wel niet-triviale oplossingen zijn en een aanpak via modulariteit van Frey-krommen, naast andere methoden, de diofantische vergelijking kan oplossen. Voor $(p, q, r) = (2, 3, l)$ kan men bijvoorbeeld de Frey-kromme

$$E: y^2 = f(x), \quad f(x) = x^3 + 3bx - 2a$$

beschouwen met

$$\Delta(f) = -2^2 \cdot 3^3(a^2 + b^3) = -2^2 \cdot 3^3 c^l.$$

In [19] wordt het geval $l = 7$ volledig opgelost; er zijn 5 paren niet-triviale oplossingen. In dit geval is trouwens weer de modulariteit van alle elliptische krommen over $\mathbb{Q}$ nodig.

Voor sommige diofantische problemen over $\mathbb{Z}$ of $\mathbb{Q}$ kan het soms handig zijn om een Frey-kromme te construeren over een groter getallenlichaam K . Maar dit kan ook simpelweg het geval zijn voor generalisaties van diofantische problemen over $\mathbb{Q}$ naar problemen over K . Men kan bijvoorbeeld kijken naar een generalisatie van de Laatste Stelling van Fermat waarbij de vergelijking $x^n + y^n = z^n$ moet worden opgelost in $x, y, z \in \mathcal{O}_K$. Hiervoor kan men de 'standaard' Frey-kromme gebruiken, maar dit is nu een elliptische kromme over K geworden. Als K reëel kwadratisch is, hebben we Hilbert-modulariteit van de Frey-kromme. In dat geval zijn Freitas en Siksek in [12] erin geslaagd om de rest van de benodigde ingrediënten vaak werkzaam te krijgen en bewijzen onder andere dat voor oneindig veel verschillende reëel kwadratische getallenlichamen K er een constante

B_K is, zodat voor alle priemgetallen $l \geq B_K$ er geen niet-triviale oplossingen zijn van $x^l + y^l = z^l$ in $x, y, z \in \mathcal{O}_K$ (of K , dat maakt hier niet uit).

Bovenstaande vormt slechts een kleine selectie van diofantische vergelijkingen waarbij modulariteit een belangrijke rol speelt. Het is de verwachting dat er in de toekomst nog vele bij zullen komen, zowel voor de types van modulariteit die we besproken hebben als voor andere types, en zowel voor bewezen gevallen van modulariteit als voor nog te bewijzen gevallen.

De Langlands-vermoedens

Zoals eerder uitgelegd, het resultaat van Wiles kan gezien worden als een speciaal geval van de Langlands-vermoedens. Deze vermoedens zijn nog open, maar dankzij het werk van Wiles zijn er in de afgelopen jaren grote stappen gezet. In deze paragraaf willen we graag een tipje van de sluier oplichten en een idee geven waar de Langlands-vermoedens over gaan. Een probleem met de vermoedens is dat ze niet eenvoudig te formuleren zijn. Hierom geven we in dit overzichtsartikel alleen een speciaal geval, dat minder algemeen is dan de originele vermoedens. Dit speciale geval heeft een eenvoudigere formulering en is toch (hopelijk) nog steeds interessant.

Systemen van diofantische vergelijkingen

Met een *diofantisch systeem* bedoelen we een collectie van een eindig aantal ver-

gelijkingen

$$\begin{cases} F_1(x_1, x_2, \dots, x_b) = 0 \\ F_2(x_1, x_2, \dots, x_b) = 0 \\ \vdots \\ F_a(x_1, x_2, \dots, x_b) = 0 \end{cases} \quad (11)$$

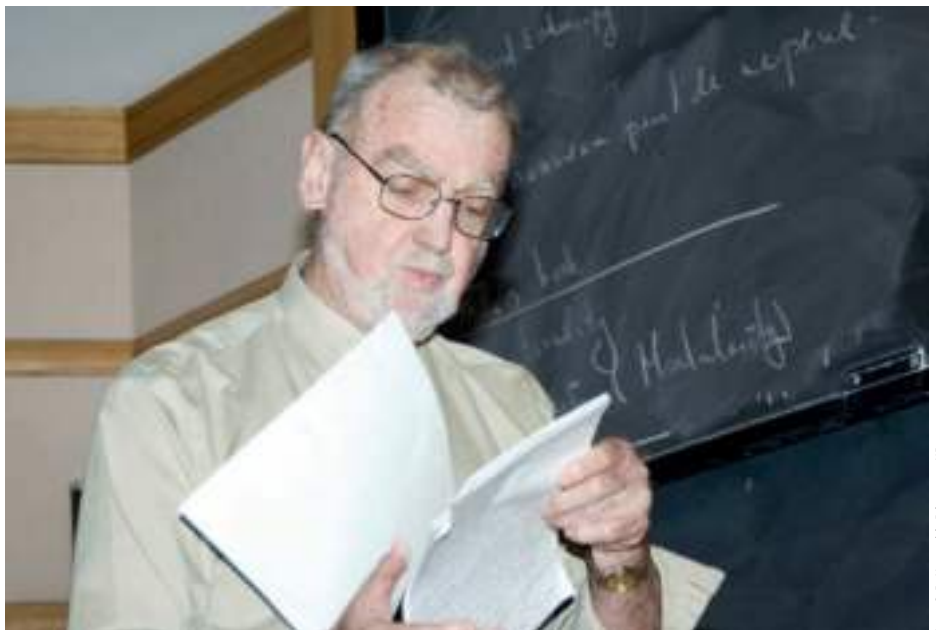
waarbij a, b positieve gehele getallen zijn en $F_1, \dots, F_a$ polynomen zijn met gehele coëfficiënten in variabelen $x_1, \dots, x_b$. Sinds de oudheid zijn wiskundigen geïnteresseerd in het oplossen van dergelijke systemen van diofantische vergelijkingen. Het voorbeeld van een elliptische kromme correspondeert met het geval waar $a = 1$, $b = 2$ en $F(x_1, x_2) = x_1^2 - (x_2^3 + Ax_2 + B)$.

Gegeven een diofantisch systeem van vergelijkingen X kunnen we voor alle priemgetallen p het aantal oplossingen $\#X(\mathbb{Z}/p\mathbb{Z})$ van X modulo p tellen. Merk op dat $(\mathbb{Z}/p\mathbb{Z})^b$ een eindige verzameling is, en voor elk element $(x_i) \in (\mathbb{Z}/p\mathbb{Z})^b$ kunnen we kijken of hij wel of niet aan de vergelijkingen in het systeem (11) modulo p voldoet. Bijvoorbeeld kunnen we kijken naar de vergelijking X gegeven door $x^4 + y^3 = z^2$. Het aantal oplossingen $\#X(\mathbb{Z}/p\mathbb{Z})$ voor priemgetallen p kunnen we weer in een tabel zetten:

p	2	3	5	7	11	13	...
$\#X(\mathbb{F}_p)$	4	18	100	1210	1210	2028	...

(12)

De Langlands-vermoedens voorspellen dat deze reeks getallen (op eindig veel priemgetallen p na) overeenkomt met 'Hecke-eigenwaarden' van 'automorfe vormen'.



Robert Langlands tijdens de conferentie 'The $\mathcal{L}$ -Group at 40', Institute for Advanced Study, Princeton, 2006

Een belangrijke vraag is, gegeven een diofantisch systeem X , in hoeverre het rijtje $\#X(\mathbb{Z}/p\mathbb{Z})$ ‘reducibel’ is, oftewel ontbonden kan worden als lineaire combinatie van meer eenvoudige rijtjes (die bijvoorbeeld afkomen van eenvoudigere diofantische systemen). Rond de tijd dat Langlands zijn brief aan Weil schreef, was de meetkundegroep van Alexander Grothendieck bezig met een hypothetische theorie van *motieven* van variëteiten. Elk motief M zou aanleiding geven tot een rijtje getallen $\#M(\mathbb{Z}/p\mathbb{Z})$ (mogelijk niet in $\mathbb{Z}$) waar p varieert over de priemgetallen, en voor elk diofantisch systeem X , zou het rijtje $\#X(\mathbb{Z}/p\mathbb{Z})$ moeten ontbinden als een lineaire combinatie van rijtjes die bij motieven horen. In deze zin zouden motieven de bouwstenen vormen van algebraïsche vergelijkingen. Wat motieven precies zijn, is tot nu toe nog onbekend en het vinden van de juiste definitie is een open probleem. Langlands formuleerde zijn originele vermoeden in termen van deze hypothetische theorie van motieven van Grothendieck.

Automorfe vormen

We gaan nu de analytische kant bekijken, en definiëren wat discrete automorfe vormen zijn. Kies positieve gehele getallen $n, N \in \mathbb{Z}_{\geq 1}$. We noteren $\mathrm{GL}_n(\mathbb{Z})$ voor de groep van alle inverteerbare $n \times n$ -matrices g met gehele coëfficiënten zó dat $\det(g) = \pm 1$ (dan heeft de inverse matrix g^{-1} ook gehele coëfficiënten). We beginnen met de *congruentieondergroepen* $\Gamma(N) \subset \mathrm{GL}_n(\mathbb{Z})$, gedefinieerd door

$$\Gamma(N) = \{g \in \mathrm{GL}_n(\mathbb{Z}) \mid g \equiv 1_n \pmod{N}\}.$$

We schrijven $\mathrm{GL}_n(\mathbb{R})$ voor de groep van reële inverteerbare $n \times n$ -matrices en $\mathrm{PGL}_n(\mathbb{R})$ voor het quotiënt $\mathrm{GL}_n(\mathbb{R})/\mathbb{R}^\times$, waar we $\mathbb{R}^\times$ zien in $\mathrm{GL}_n(\mathbb{R})$ als de scalaire matrices.

Kies een continu groepsmorphisme $\omega: \mathbb{R}^\times \rightarrow \mathbb{C}^\times$. We schrijven $H_\omega = L^2(\mathrm{GL}_n(\mathbb{R})/\Gamma(N), \omega)$ voor de ruimte van meetbare functies $f: \mathrm{GL}_n(\mathbb{R}) \rightarrow \mathbb{C}$, zó dat

- (A1) Voor zekere $N \in \mathbb{Z}_{\geq 1}$ groot genoeg (het *niveau* van f) geldt $f(g\gamma) = f(g)$ voor alle $\gamma \in \Gamma(N)$, en alle $g \in \mathrm{GL}_n(\mathbb{R})$.
- (A2) Er geldt $f(zg) = \omega(z)f(g)$.
- (A3) De integraal

$$\int_{\mathrm{PGL}_n(\mathbb{R})} |\det(g)|^{-2w/n} |f(g)|^2 \mu(g)$$

convergeert. Hier is μ de Haar-maat op

$\mathrm{PGL}_n(\mathbb{R})$, en $w \in \mathbb{R}_{>0}$ is het unieke reële getal zó dat $|\cdot|^{-w}\omega$ beeld heeft in de eenheidscirkel $S^1 \subset \mathbb{C}^\times$.

Per definitie zijn in H_ω twee functies $f, h \in H_\omega$ equivalent als het verschil $f - h$ support heeft op een verzameling van maat 0. Modulo deze equivalentierelatie is H_ω een Hilbertruimte. De groep $\mathrm{GL}_n(\mathbb{R})$ werkt op H_ω door translaties: Als $f \in H_\omega$ en $g \in \mathrm{GL}_n(\mathbb{R})$, dan hebben we de getransleerde functie $gf \in H$ met $gf(x) = f(gx)$ voor alle $x \in \mathrm{GL}_n(\mathbb{R})$.

De ruimte van discrete automorfe vormen $A_{N,\omega}$ is een bepaalde deelruimte van $H_{N,\omega}$. Het punt is dat er ontzettend veel L^2 -functies $f: \mathrm{GL}_n(\mathbb{R}) \rightarrow \mathbb{C}$ zijn, en je wilt de theorie algebraïsch maken. Dit kan door te beperken naar functies die voldoen aan bepaalde eindigheidscondities (K -eindig, $\mathbb{Z}$ -eindig) en groei-condities die we niet allemaal expliciet zullen maken (zie [1, 1.3(a,b,c,d)]), maar je kan ook representatietheorie gebruiken om de discrete automorfe vormen te definiëren. Neem eerst $H_{N,\omega}^{\mathrm{disc}} \subset H_{N,\omega}$, de complexe deelvectorruimte van H_ω opgespannen door alle deelruimten $V \subset H_{N,\omega}$, die $\mathrm{GL}_n(\mathbb{R})$ -stabiël zijn, ofwel $gf \in V$ voor alle $g \in \mathrm{GL}_n(\mathbb{R})$ en alle $f \in V$, en bovendien irreducibel, ofwel de enige gesloten $\mathrm{GL}_n(\mathbb{R})$ -stabiële deelruimten W van V zijn 0 en V zelf. De ruimte $H_{N,\omega}^{\mathrm{disc}}$ is geen Hilbertruimte meer, dit komt omdat de ruimte niet compleet is. Het orthogonale complement van de afsluiting van $H_{N,\omega}^{\mathrm{disc}}$ in $H_{N,\omega}$ is het continue spectrum. Deze ruimte is vooral belangrijk voor de theorie van Eisenstein-reeksen. De ruimte van discrete automorfe vormen $A_{N,\omega}$ is nu de ruimte van functies $f \in H_{N,\omega}^{\mathrm{disc}}$ die ‘ K -eindig’ zijn, ofwel zó dat de vectorruimte opgespannen door de getransleerde functies gf eindigdimensionaal is waarbij g varieert over de orthogonale matrices:

$$\dim_{\mathbb{C}} \langle gf \mid g \in \mathrm{GL}_n(\mathbb{R}), g^t g = 1 \rangle < \infty.$$

De ruimte $A_{N,\omega}$ ligt dicht in $H_{N,\omega}^{\mathrm{disc}}$. Als laatste: een discrete automorfe vorm is een functie $f: \mathrm{GL}_n(\mathbb{R}) \rightarrow \mathbb{C}$ zó dat voor N voldoende groot, en een $\omega: \mathbb{R}^\times \rightarrow \mathbb{C}^\times$ geldt $f \in H_{N,\omega}$. De ruimte van automorfe vormen $A_{N,\omega}$ ligt dicht in $H_{N,\omega}^{\mathrm{disc}}$.

We zijn vooral geïnteresseerd in *eigenfuncties*. Voor elke automorfe vorm $f: \mathrm{GL}_n(\mathbb{R}) \rightarrow \mathbb{C}$, definiëren we voor elk priemgetal p copriem met N een nieuwe automorfe vorm $T_p(f)$ op $\mathrm{GL}_n(\mathbb{R})$ door de formule

$$T_p(f)(x) = \sum_{i=1}^{\deg(T_p)} f(x \cdot \gamma_i). \quad (13)$$

Hier is $\deg(T_p)$ een natuurlijk getal en zijn $\gamma_i \in \mathrm{GL}_n(\mathbb{Z})$ matrices zó dat geldt

$$\Gamma(N) \cdot \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & & p \end{pmatrix} \cdot \Gamma(N) = \prod_{i=1}^{\deg(T_p)} \Gamma(N) \cdot \gamma_i \subset \mathrm{GL}_n(\mathbb{Z}).$$

Merk op dat de uitdrukking (13) onafhankelijk is van de keuze van de matrices γ_i .

Hier is een misschien meer intuïtieve manier om over formule (13) na te denken. Stel f is een automorfe vorm. Stel $g \in \mathrm{GL}_n(\mathbb{Z})$ is de diagonale matrix $\mathrm{diag}(1, \dots, 1, p)$. Definieer de functie $gf(x)$ door simpelweg met g te transleren: $gf(x) := f(xg)$ op $\mathrm{GL}_n(\mathbb{R})$. Dan is gf niet $\Gamma(N)$ -invariant, maar $g^{-1}\Gamma(N)g$ -invariant; om een $\Gamma(N)$ -invariante functie te krijgen, wil je het gemiddelde nemen van de $\Gamma(N)$ -translaties van gf (dit zijn er eindig veel). Als je dit op de juiste manier doet, dan kom je op de formule in (13) uit.

De automorfe vorm f is een eigenvorm als het een eigenvector is voor de operatoren T_p voor alle priemgetallen p met $p \nmid N$. De corresponderende eigenwaarden $\lambda_p \in \mathbb{C}$ met $T_p f = \lambda_p f$ zullen we de *Hecke-eigenwaarden* noemen. Voor elk priemgetal $p \nmid N$ hebben we dus zo’n eigenwaarde. Behalve de operatoren T_p kan je ook kijken naar andere Hecke-operatoren gegeven door een matrix verschillend van $\mathrm{diag}(1, \dots, 1, p)$. De reden voor onze keuze is dat de eigenwaarden van deze operator oplossingsaantallen van diofantische systemen geeft (zie (14)).

Voorbeeld 5. Laten we kijken hoe het voorbeeld van modulaire vormen in dit kader past. Stel $f: \mathbb{H} \rightarrow \mathbb{C}$ is een genormaliseerde modulaire eigenvorm van gewicht $k \geq 0$ voor $\Gamma_0(N)$. Laat $\mathbb{H}^\pm = \{x + yi \in \mathbb{C} \mid y \neq 0\}$ het complexe dubbelhalfvlak zijn. Dan kunnen we de functie f voortzetten naar een functie $\tilde{f}$ op $\mathbb{H}^\pm$ door de formule $\tilde{f}(\tau) = \tau^{-k} f(1/\tau)$ voor $\tau \in \mathbb{H}^\pm$ met negatief imaginair deel. We definiëren de functie $h: \mathrm{GL}_2(\mathbb{R}) \rightarrow \mathbb{C}$ door

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{(ad - bc)^{k-1}}{(ci + d)^k} \cdot \tilde{f}\left(\frac{ai + b}{ci + d}\right).$$

Dan is h een automorfe eigenvorm en er geldt $T_p \cdot h = a_p \cdot h$, waarbij a_p de p -de Fourier-coëfficiënt van f is, voor alle $p \nmid N$.

We zijn nu in staat het voorspelde verband tussen de automorfe vormen en de diofantische vergelijkingen te formuleren.

Vermoeden 6 (Langlands). *Stel X is een diofantisch systeem van vergelijkingen als in (11). Er bestaan positieve gehele getallen $n_1, \dots, n_r \in \mathbb{Z}_{\geq 1}$, eigenvormen $f_1, \dots, f_r$ van voldoende groot niveau N op de groepen $\mathrm{GL}_{n_1}(\mathbb{R}), \mathrm{GL}_{n_2}(\mathbb{R}), \dots, \mathrm{GL}_{n_r}(\mathbb{R})$, en gehele getallen $m_1, \dots, m_r \in \mathbb{Z}$ zó dat voor alle $p \nmid N$, geldt*

$$\#X(\mathbb{F}_p) = \sum_{i=1}^r m_i \cdot a_p(f_i), \quad (14)$$

waarbij $a_p(f_i)$ de eigenwaarde is van de operator T_p werkend op f_i .

Voor de experts refereren we naar [24, Theorem 6.1] en de vermoedens in [28, Section 4]. De oplettende lezer ziet dat Vermoeden 6 slechts één richting op gaat: van diofantisch naar automorf. De originele vermoedens van Langlands gaan ook in de omgekeerde richting.

Verder, in bovenstaand vermoeden hebben we een eindige hoeveelheid priemgetallen uitgesloten. Neem als voorbeeld een affiene Weierstrass-vergelijking X van een elliptische kromme die niet minimaal is.

Dan kunnen we nog steeds punten tellen op X , alleen bij de (eindig veel) priemgetallen waar de vergelijking niet minimaal is, hoeven aantallen niet gelijk te zijn aan $p - a_p(f)$ waar f de corresponderende eigenvorm is. Verder merken we op dat de functie $g(x) = |x|^{-1}$ op $\mathrm{GL}_1(\mathbb{R}) = \mathbb{R}^\times$ een automorfe eigenvorm is met eigenwaarde p voor T_p op GL_1 . We zien: de getallenrij $\#X(\mathbb{Z}/p\mathbb{Z})$ wordt beschreven door de twee automorfe vormen f en g . Wegens Stelling 3, een directe generalisatie van het resultaat van Wiles, weten we nu dus dat bovenstaand vermoeden waar is voor X . $\diamond$

Referenties

- Armand Borel en Herve Jacquet, Automorphic forms and automorphic representations, *Automorphic forms, representations and L-functions*, Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, OR, 1977, Part 1, 1979.
- Alex van den Brandhof, Abelprijs gaat naar Andrew Wiles, voor oplossing Fermat, *NRC Handelsblad*, 15 maart 2016.
- Christophe Breuil, Brian Conrad, Fred Diamond en Richard Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* 14(4) (2001), 843–939.
- Ana Caraiani en Peter Scholze, On the generic part of the cohomology of compact unitary Shimura varieties, *Annals of Math.*, arXiv:1511.02418.
- Davide Castelvocchi, Fermat's last theorem earns Andres Wiles the Abel prize, *Nature*, March 15 2016.
- John H. Coates en Andrew J. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* 39(3) (1977), 223–251.
- Henri Darmon en Loïc Merel, Winding quotients and some variants of Fermat's last theorem, *J. Reine Angew. Math.* 490 (1997), 81–100.
- Fred Diamond en Jerry Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics, No. 228, Springer, 2005, xvi+436 pp.
- Bas Edixhoven, Rational elliptic curves are modular, *Séminaire N. Bourbaki*, 1999–2000, exp. no. 871, pp. 161–188.
- Jordan S. Ellenberg, Galois representations attached to $\mathbb{Q}$ -curves and the generalized Fermat equation $A^4 + B^2 = C^p$, *Amer. J. Math.* 126(4) (2004), 763–787.
- Nuno Freitas, Bao V. Le Hung en Samir Siksek, Elliptic curves over real quadratic fields are modular, *Invent. Math.* 201(1) (2015), 159–206.
- Nuno Freitas en Samir Siksek, The asymptotic Fermat's Last Theorem for five-sixths of real quadratic fields, *Compositio Mathematica* 151(8) (2015), 1395–1415.
- Rishi Iyengar, British professor gets math's top prize for proving a 350-year-old theorem, *Time Magazine*, March 18 2016.
- Chandrashekhara Khare en Jean-Pierre Wintenberger, Serre's modularity conjecture. I, II, *Invent. Math.* 178(3) (2009), 485–504, 505–586.
- Mark Kisin, Modularity of 2-adic Barsotti-Tate representations, *Invent. Math.* 178(3) (2009), 587–634.
- Robert Langlands, Letter to André Weil, available at publications.ias.edu/rpl/section/21.
- Derrick H. Lehmer, The vanishing of Ramanujan's function $\tau(n)$, *Duke Math. J.* 14 (2017), 429–433.
- Frans Oort, The Weil conjectures, *Nieuw Archief Wisk.* 5/15(3) (2014), 211–219.
- Bjorn Poonen, Edward F. Schaefer en Michael Stoll, Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$, *Duke Math. J.* 137(1) (2007), 103–158.
- Kenneth A. Ribet, On modular representations of $\mathrm{Gal}(\mathbb{Q}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* 100(2) (1990), 431–476.
- Kenneth A. Ribet, Abelian varieties over $\mathbb{Q}$ and modular forms, *Algebra and Topology 1992 (Taejon)*, Korea Adv. Inst. Sci. Tech., Taejon, 1992, pp. 53–79.
- Peter Scholze, On torsion in the cohomology of locally symmetric varieties, *Ann. of Math.* (2) 182(3) (2015), 945–1066.
- Jean-Pierre Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.* 54(1) (1987), 179–230.
- Jean-Pierre Serre, *Lectures on $N_X(p)$* , CRC Press, 2011.
- Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Text of Mathematics, No. 106, Springer, 2009, 2nd edition.
- Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Text of Mathematics, No. 151, Springer, 1994.
- Richard L. Taylor, Potential automorphy of some non-self dual Galois representations, www.math.princeton.edu/events/seminars/princeton-universityias-number-theory-seminar/potential-automorphy-some-non-self.
- Richard L. Taylor, Galois representations, *Annales de la Faculté des Sciences de Toulouse* 13 (2004), 73–119.
- Richard L. Taylor en Andrew J. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* (2) 141(3) (1995), 553–572.
- Andrew J. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* (2) 141(3) (1995), 443–551.

Casper Albers

Psychometrie & Statistiek
Rijksuniversiteit Groningen
c.j.albers@rug.nl



Column Casper grijpt een kans

Lies, damn lies en tijdreeksen

Caspers Albers schrijft op regelmatige basis in dit blad een column over alledaagse statistische onderwerpen.

Stel dat je lobbyt voor een of andere maatregel. Om je argumenten kracht bij te zetten, wil je laten zien dat niet alleen jij dit een goed idee vindt, maar dat het volk dit ook wil. Je besluit wat mensen op straat te ondervragen, in een ochtend-, middag- en avondsessie. Elke keer ondervraag je 100 personen. 's Ochtends sta je bij een basisschool en krijg je steun van 62 van de 100 personen. 's Middags en 's avonds, op andere locaties in de stad, heb je minder succes: beide keren zijn maar 38 mensen het met je eens. In het persbericht van het lobbybedrijf schrijf je vervolgens "Bijna tweederde van de personen die we op maandagmorgen ondervraagd hebben, steunt ons voorstel. Nieuwe regering: luister naar het volk en pak die kans!"

Vanzelfsprekend is dit valsspelen. Het is een schoolvoorbeeld van de uitspraak 'Lies, damn lies and statistics' (die doorgaans onterecht wordt toegekend aan de Britse oud-premier Benjamin Disraeli [2]). Vanzelfsprekend had de uitspraak moeten zijn dat $m = 138$ van de $n = 300$ ondervraagden, dus $\hat{p} = m/n = 46\%$, het voorstel steunden. Bij voorkeur vul je dit nog aan met een uitspraak die de onzekerheid kwantificeert. Dit kan bijvoorbeeld met een 95% betrouwbaarheidsinterval via de normale benadering van de binomiale verdeling,

$$\hat{p} \pm 1,96 \times \sqrt{\frac{1}{n} \hat{p}(1 - \hat{p})} = (40,3\%; 51,6\%)$$

(waarbij 1,96 het bijbehorende percentiel van de standaardnormale verdeling is). Bovenstaande is niet de beste methode om zo'n interval te berekenen, maar wel een makkelijke. Het kan net iets beter via de *plus-four*-methode [1] waarbij $\hat{p} = m/n$ vervangen wordt door $\hat{p} = (m + 1,96) / (n + 2 \times 1,96)$, dat levert (40,4%; 51,7%).

Zo zijn er nog een aantal methoden om een puntschatter van een proportie te voorzien van een (betrouwbaarheids)interval. Het is makkelijk om je te richten op de wiskundige aspecten van al deze methoden. Ongeacht de wiskundige details geven alle aanpakken ongeveer hetzelfde beeld: vier à vijf van de tien ondervraagden zijn het met de stelling eens. Door alleen naar de wiskundige kant van de statistiek te kijken mis je echter een belangrijk aspect: de grote verschillen in de ochtend-, middag- en avondmeting moeten wel een alarmbelletje laten rinkelen. Misschien is de populatie waaruit gepeild werd niet zo homogeen: de ouders op het schoolplein staan blijkbaar veel positiever tegenover het voorstel dan andere personen. Waarom is dit? Wellicht gaat de maatregel over extra investeringen in de kwaliteit van basisscholen: de ouders van de kinderen op die school hebben daar natuurlijk direct belang bij en zullen dat eerder de kosten waard vinden dan een willekeurige andere Nederlander. Een goed statistisch model houdt met dit soort aspecten rekening.

Met gewoon het rapporteren van de 62% steun van de ochtendploeg kom je tegenwoordig niet meer makkelijk weg. Wetenschappers, journalisten, politici en andere belanghebbenden zijn tegenwoordig (redelijk) goed getraind in het herkennen van dit soort valsspelen (al kan het altijd beter). Er is echter één soort data waarbij stevast — bewust of onbewust — verkeerde conclusies getrokken worden: longitudinale of tijdreeksdata.

Tijdreeksdata

Tijdreeksen bestaan uit metingen die elkaar opvolgen in de tijd. Het kan de dagelijkse middagtemperatuur in De Bilt zijn, de hartslag die je hartslagmeter meet tijdens het hardlopen, of welke andere reeks gegevens ook. Veel tijdreeksen zijn fundamenteel anders dan gewone steekproeven, in de zin dat ze nooit 'klaar' zijn. Bij een gewone steekproef bepaal je doorgaans vooraf hoeveel

mensen je wilt ondervragen, en dan doe je dat en rapporteer je de resultaten. Een tijdreeks kan eindig zijn — bijvoorbeeld wanneer je wilt weten wanneer op de dag voor kerstmis de meeste omzetten in de supermarkt gedraaid worden: zodra die dag voorbij is, is je meting voorbij. Vaak houden tijdreeksen echter nooit op. Denk aan de peilingen van Maurice de Hond. Elke week komt er weer een nieuw antwoord op de vraag “Waar zou u op stemmen als er vandaag verkiezingen zouden zijn geweest?”, ondanks dat we weten dat er vandaag helemaal geen verkiezingen zijn. Elke keer komt er weer een piepklein stukje extra informatie. Bij een gewone steekproef zou geen krant er ook maar over denken om een nieuwsbericht te wijten aan hoe de resultaten gewijzigd zijn omdat de steekproefgrootte van $n = 1292$ naar $n = 1293$ is gegaan. Maar bij de politieke peilingen van De Hond is het wekelijks raak: ook als alle verschuivingen binnen de foutenmarge zijn, worden deze uitgebreid uitgemeten in de media en komen de experts om te duiden waar de verschuivingen door komen.

Een veelgemaakte denkfout bij tijdreeksdata is dat men inzoomt op een klein deel van de reeks metingen en daar conclusies aan verbindt zonder het grotere plaatje te bekijken. Bij de afgelopen Tweede Kamerverkiezingen behaalde het CDA 19 zetels, een stijging van 6 ten opzichte van de verkiezingen van 2012. Dit werd door CDA'ers uitbundig als iets moois gevierd. Het is echter ook een daling van 2 zetels ten opzichte van de uitslag van 2010, of een gigantische aderlating ten opzichte van de uitslagen van enkele decennia geleden.

In een tijdreeks zit zo nu en dan een opvallende patroon — een daling of stijging of juist een periode van stabiliteit — en dat kan gewoon toeval zijn. Het kan natuurlijk ook een ‘echte’ oorzaak hebben. Of dit zo is, zie je niet als je alleen inzoomt op die opvallende stijging en daling. Stel dat ik vandaag elke minuut met een dobbelsteen gooi. Uiteindelijk heb ik dan een tijdreeks van 1440 worpen. Wellicht gooi ik wel ergens vandaag vijf keer op rij een zes. Als je daarop inzoomt, klinkt dat extreem onwaarschijnlijk: de kans om vijf keer op rij een zes te gooien is erg klein ($(\frac{1}{6})^5 = \frac{1}{7776}$). Die kleine kans zou je kunnen aangrijpen als bewijs dat de dobbelsteen niet zuiver is. Maar, in de context van 1440 opeenvolgende worpen, is het gooien van vijf zessen niet heel raar. Waarschijnlijk had je het evengoed raar gevonden als het niet vijf opeenvolgende zessen waren, maar vijf opeenvolgende enen, tweeën, ..., of vijven. De kans dat zoiets gebeurt, ergens op de dag, is al meer dan 50%.

Voorbeeld: verkeersdoden

Een treffend voorbeeld van het inzoomen op een (te) klein deel van de data haalde vorige maand de media. Op 2 mei jl. kwam het CBS met nieuwe cijfers over het aantal dodelijke verkeersslachtof-

fers: in 2016 waren dit er 629, in 2015 waren het er 621, in 2014 waren het er 570. Reden voor de media om met afschrikwekkende krantenkoppen te komen: ‘Aantal verkeersdoden blijft stijgen’ (*Hart van Nederland*), ‘Aantal verkeersslachtoffers stijgt opnieuw’ (*RTL nieuws*). Feitelijk gezien correcte koppen natuurlijk, maar wel misleidend. Verschillende lobby-instituten gebruikten dit nieuws om — voor hun gunstige — voorstellen te doen. Zo adviseerde de politie om meer geld naar de politie te sturen voor verkeerscontroles en wou Veilig Verkeer Nederland meer geld voor voorlichting over veilig verkeer in Nederland. Nu is er natuurlijk weinig mis in het investeren in betere verkeersveiligheid, maar kom dan wel met de juiste onderbouwing.

Gemiddeld vielen er de afgelopen tien jaar jaarlijks 660,2 doden op de weg, met een standaarddeviatie van 69,3. De score van 2016 zat dus wederom onder dat gemiddelde en de stijging van 8 doden, hoe tragisch ook, was maar een tiende van de standaarddeviatie.

De grafiek [3] zoomt nog verder uit en laat zien wat het verloop is van de verkeersslachtoffers vanaf 1950, gecorrigeerd voor de groei in de bevolking. Uit die grafiek is op geen enkele manier reden tot zorg voor nu te halen.

De veranderingen in de afgelopen twee jaar blijven *ruim* binnen de waardes die de afgelopen tien jaar gemeten zijn. Desondanks wist *de Volkskrant* (krantenbericht ‘Waarom het aantal verkeersdoden weer stijgt’) precies uit te leggen waar die stijging toch aan lag: te weinig controle, te veel smartphones en steeds meer bejaarden op e-bikes — verklaringen die gevonden werden door onder meer te praten met belanghebbenden. Dat is geen *statistiek*, dat zijn *lies* en *damn lies*.

De juiste conclusie had moeten zijn dat het aantal verkeersdoden al een jaar of tien stabiel is op een niveau wat zo’n factor 7 lager ligt dan in begin jaren zeventig.



Referenties

- 1 A. Agresti en B.A. Coull, Approximate is better than exact for interval estimation of binomial proportions, *The American Statistician* 52 (1988), 119–126.
- 2 P.F. Velleman, Truth, damn truth, and statistics, *Journal of Statistics Education* 16(2) (2008).
- 3 Figuur gemaakt door Datagraver.com, op basis van openbare data van het Centraal Bureau voor de Statistiek

M. Ram Murty

Department of Mathematics
Queen's University, Kingston, Canada
murty@mast.queensu.ca

Trip to the Proof

How I discovered Euclidean proofs

Mathematicians carefully communicate the how of their results, but they hardly ever go into the why. In this new column 'Trip to the Proof' mathematicians describe the discovery process without going into the details of the proof. The first contribution is by Ram Murty, who holds a research chair in mathematics as well as an appointment in philosophy at Queen's University, Canada.

It was the summer of 1975 when I was entering the final year of my undergraduate studies at Carleton University in Ottawa, Canada, that I wandered into the library in search of a topic to research for my Bachelor's thesis. Browsing through some old volumes of the *American Mathematical Monthly*, I chanced upon an interesting article written by Bateman and Low showing that there are infinitely many primes in every coprime arithmetic progression (mod 24) using only basic properties of polynomials and nothing deeper than the law of quadratic reciprocity. Of course, Dirichlet had proved in a series of papers written between 1837 and 1840 that there are infinitely many primes in any coprime arithmetic progression using analytic and arithmetic methods including his deep class number formula. By contrast, the Bateman and Low paper [1] followed the line of attack initiated by Euclid in 300 BCE and they seemed to suggest at the end

of the paper that such 'Euclidean proofs' exist only when the residue class has order 1 or 2. I was intrigued by this and wrote to Professor Bateman to ask how one would prove such a statement. He responded by saying that he had no formal proof but that all the examples known satisfied this criterion. So I took this up for my Bachelor's thesis and tried to make the problem precise.

All of us are familiar with Euclid's elementary proof of the infinitude of primes. It proceeds by contradiction. Assume that there are only finitely many, say $p_1, \dots, p_r$. Then the number $P = p_1 \cdots p_r + 1$ is a number coprime to all of the primes $p_1, \dots, p_r$. At the same time it is larger than 1 and so must be divisible by a prime which is not in our list, which is a contradiction. Many excellent books on elementary number theory often extend this argument to show infinitude of primes congruent to 1 or 3 (mod 4). For example, if there are only fi-

nitely many primes congruent to 3 (mod 4), say $p_1, \dots, p_r$ then consider $P = 4p_1 \cdots p_r - 1$. This number being odd and being coprime to $p_1, \dots, p_r$ must have prime divisors either congruent to 1 or 3 (mod 4). But not all its prime divisors can be 1 (mod 4) for otherwise, the number itself would be 1 (mod 4), which it is not. So it must have a prime divisor congruent to 3 (mod 4) not in our list. This contradiction shows there are infinitely many primes congruent to 3 (mod 4).

A small variation in this argument can show the infinitude of primes congruent to 1 (mod 4). Indeed, as before suppose there are only finitely many, say $p_1, \dots, p_r$. Consider $N = 4(p_1 \cdots p_r)^2 + 1$ which is coprime to all of the primes $p_1, \dots, p_r$. If p is any prime divisor of N , then p is different from $p_1, \dots, p_r$ and -1 is a quadratic residue (mod p). But only primes congruent to 1 (mod 4) have -1 as a quadratic residue so that $p \equiv 1 \pmod{4}$.

Both of these proofs are in the spirit of Euclid and so my question was how far one could push this argument and give a 'Euclidean proof' of Dirichlet's theorem. I was 22 years old at that time and I can vividly recall the great delight I felt when



Ram Murty with Dinesh Thakur and Dipendra Prasad (Boston, 1983)



Ram Murty with Dinesh Thakur and Dipendra Prasad (TIFR, Mumbai, 2015)

I asked the question. Bateman's reply to my letter only encouraged me to make my question as precise as possible and to answer it the best I could. I believe that there are already several important features of the research experience evident in this narration. As I have taught my students in later years, research is really the art of asking 'good questions'. What is a 'good question'? This is difficult to define. However, the question should not be too easy or too difficult, but must be just right so as to stimulate some progress in the direction of the answer. Fortunately, this problem was just right and it took me to the frontiers of modern research.

There are other aspects of research that are underlined by my story. Browsing plays an important part in research. In my case, browsing old journals in the library was an exciting experience and I stumbled upon an article that I could dive deeper into. Moreover, there was some literature already in place that I could consult for a hint of how to proceed. For instance, Bateman seemed to imply that all the proofs known to him suggested such a proof can only be given if the residue class had order 1 or 2 but could not give a proof of this assertion. In his paper, there was a reference to a 1912 paper of Schur [5] that showed using cyclotomic polynomials that if k is a natural number and $a \pmod k$ is a residue class such that $a^2 \equiv 1 \pmod k$, then one can construct a polynomial $f(x)$ with integer coefficients such that any prime divisor p of $f(n)$ is congruent to either 1 or $a \pmod k$. Schur's paper was written in German and was about ten pages long. Though I had a year long course in German in high school, I was not fluent in it. However, the paper was sufficiently short that I could sit with a dictionary and translate it well enough to reproduce Schur's proof in my own words and make it the first chapter of my Bachelor's thesis.

To give some idea to the reader of Schur's argument, it may be instructive to illustrate how one would give a 'Euclidean proof' for the infinitude of primes $\equiv 1 \pmod k$

for any natural number k . Indeed, if $\Phi_k(x)$ is the k -th cyclotomic polynomial, then

$$x^k - 1 = \prod_{d|k} \Phi_d(x).$$

Using this factorization, it is relatively easy to show that if a prime p divides $\Phi_k(n)$ then either $p|k$ or $p \equiv 1 \pmod k$. From this fact, one can cheerfully construct the desired proof. Schur's argument for other arithmetic progressions $a \pmod k$ for which $a^2 \equiv 1 \pmod k$ uses elementary Galois theory and was a nice challenge for me to apply my theoretical knowledge from my third year course in my fourth year Bachelor's thesis.

But the real hurdle was in showing the converse. That is, if such a 'Euclidean proof' exists using a 'Euclidean polynomial', then does it follow that $a^2 \equiv 1 \pmod k$? What do we mean by a 'Euclidean polynomial'? This had to be made precise. To answer this, my study took me deeper into class field theory. A theorem of Bauer states that given any polynomial $f(x)$ with integer coefficients there are infinitely many primes p for which $f(x) \equiv 0 \pmod p$ has a solution and $p \equiv 1 \pmod k$ for any given k . So, if we want to give a 'Euclidean proof' for the progression $a \pmod k$ the best we can hope for is to find a polynomial $f(x)$ such that whenever $f(x) \equiv 0 \pmod p$ has a solution, then either $p \equiv 1$ or $a \pmod k$. If $a^2 \not\equiv 1 \pmod k$, I could use the Chebotarev density theorem along with some elementary Galois theory to show the desired polynomial doesn't exist. It would take us too far afield to describe the Chebotarev density theorem. Suffice it to say that it is one of the crowning achievements of twentieth century number theory and forms a chapter in class field theory. It can be seen as a grand generalization of the prime number theorem and Dirichlet's theorem on the infinitude of primes in arithmetic progressions.

When I completed my undergraduate thesis, I had no guidance about publishing my new theorem. So the result remained unpublished for a long time. While in graduate school at MIT, I mentioned it to my

doctoral advisor Harold Stark who encouraged me to publish it, but I kept putting it off since my immediate work demanded more attention. I received further encouragement from Nesmith Ankeny and Sarvadaman Chowla but still didn't write up the result as a paper. It was only when I met Bateman at a conference that I decided to do it since he thought it was worth publishing. By that time, the year was 1987. That was the year that marked the centenary of Ramanujan's birth and many journals were asking for papers for a volume dedicated to his work. I received many such requests which were coming in faster than I could come up with new results. It was at that time I turned to the theorem from my Bachelor's thesis, and submitted it to the Journal of Madras University [3] and it appeared there in 1988. Sadly, this journal was not very accessible then and I doubt it is accessible even now. Bateman was happy I finally published the proof and referenced it in his 2004 book with Harold Diamond but still complained it was not widely available (see p. 236 of [2]). In 2006, I had to supervise an undergraduate student as part of his summer research fellowship. So I gave him the task of extending Euclidean proofs to proving cases of the Chebotarev density theorem. This we did and finally published the generalization in a more accessible journal [4].

Perhaps the last chapter of this story is instructive. Often, we do not know the value of our own work. Without proper guidance, we may downplay the significance of our contribution. As advice to a young scientist, all I can say is that we should thoroughly investigate as best as we can and then publish our results, however modest they may be. This is the way science advances, not by giant leaps, but through small steps taken by many, many diligent people. $\diamond$

Acknowledgements

I thank Kumar Murty and Akshaa Vatswani for their helpful comments on an earlier version of this article.

References

1. P. Bateman and M. E. Low, Prime numbers in arithmetic progressions with difference 24, *American Math. Monthly*, 72 (1965), 139–143.
2. P. Bateman and H. Diamond, *Analytic Number Theory, An introductory course*, World Scientific, 2004.
3. M. Ram Murty, Primes in certain arithmetic progressions, *J. Madras Univ.* 51 (1988), 161–169.
4. M. Ram Murty and Nithum Thain, Prime numbers in certain arithmetic progressions, *Fonctiones et Approximatio* 35 (2006), 249–259.
5. I. Schur, Über die existenz unendlich vieler primzahlen in einiger speziellen arithmetischen progressionen, *Sitzungsberichte der Berliner Math. Gesellschaft* 11 (1912), 40–50.

Rob van Oord

Waddinxveen
robvanoord@tiscali.nl

Evenement 23e Nationale Wiskunde Dagen

Hoe vaak is oneindig?

Op vrijdag 3 februari en zaterdag 4 februari vonden in Noordwijkerhout voor de 23ste keer de Nationale Wiskunde Dagen plaats. Twee dagen waarop wiskundeleraren en andere belangstellenden naar wiskunde kijken en luisteren, maar er vooral ook zelf mee aan de slag gaan. Een persoonlijke impressie van Rob van Oord, als gepensioneerd docent nog altijd actief als invalkracht.

Blij en met een doos vol spullen ga ik op weg naar Noordwijkerhout. Dit keer mag ik met een oud-collega meerijden. Van de organisatie mag ik tot in lengte van dagen naar de NWD. Oneindig vaak als ik wil. Ik voel me vereerd en heb zin in de vol ingetekende workshop die ik samen met Rutger ga geven. Deelnemers uitdagen en inspireren, dat gaan we doen.

Sierborden

Professor Henk van der Vorst opende de 23ste NWD met een show van de passie die hij bij zijn emeritaat heeft opgevat, litho's ontwerpen en afdrukken. Omdat het

maken van spiegelbeeld-afdrukken van litho's niet mogelijk is, gebruikt Henk een zelfde litho door hem telkens een kwartslag te draaien. Daarna drukt hij volgende versies in andere kleuren eroverheen. Door er dan zestien te combineren krijg je schitterende tableaux. Zie Figuur 1.

Vervolgens heeft Henk banen van de basispatronen op een cirkelband getransformeerd. Tot slot werden deze banen naar binnen toe 'oneindig' vaak verkleind herhaald. Hierdoor lijken de cirkelvormige eindversies op plaatjes van Coxeter en Escher. Henk liet de op deze manier gevonden afbeeldingen op sierborden drukken. Alle

sprekers kregen één van deze borden als dank voor hun inzet. Zie Figuur 2. Ook de poster van de NWD is een product van Henk.

Wilhelmus

In een zinderend spannende presentatie legt Mike Kestemont uit dat met gebruikmaking van wiskundige vergelijkingsmethodes het Wilhelmus hoogstwaarschijnlijk niet door Marnix van St. Aldegonde is geschreven. Aan de hand van een database van getelde functiewoorden in teksten kan worden bewoerd dat ons volkslied het meest overeenkomt met geschriften van Petrus Datheen. 'Blijf ik tot in den dood', is dat ook tot in het oneindige?

Sofia Kovalevskaya

Luuk Hoevenaars nam ons in zijn boeiende lezing mee naar het leven van Sofia Kovalevskaya (1850–1891). Deze dame van Russische komaf viel Weierstrass op toen zij in Berlijn bij hem een promotie deed. Wellicht is ze geïnspireerd door het behang in haar kamer, dat bestond uit bladzijden van een boek van de wiskundige Ostrogradsky, over differentiaal- en integraalrekening. Een hint voor collega's die op het punt staan de kamer van hun dochter te gaan behangen. Maar een witte wand waarop je doorlopend wiskundige teksten laat projecteren helpt misschien ook.

Ze heeft zelfs drie proefschriften geschreven, eentje over de uniciteit van analytische partiële differentiaalvergelijkingen die aan voorwaarden moeten voldoen die



Figuur 1 Basistableau van 16 tegels.



Figuur 2 Bord van Henk van der Vorst.

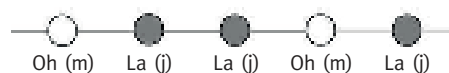
al eerder door Cauchy geformuleerd zijn. Voor haar latere werk over de mechanische beweging van een tol kreeg ze de prestigieuze prijs van de Franse academie van wetenschappen, de 'Prix Bordin'. De oplossingen van dit probleem convergeren met een Taylorreeks naar een limiet als x naar oneindig gaat. Hoe ver moet je daarin gaan?

Zij ontdekte ook een tegenvoorbeeld van de bewering van Weierstrass dat elke hogere-orde partiële differentiaalvergelijking een particuliere oplossing heeft. De oplossing van de zogeheten temperatuurstaaft heeft een term die divergent is. De staaft zal dus als het ware ontploffen.

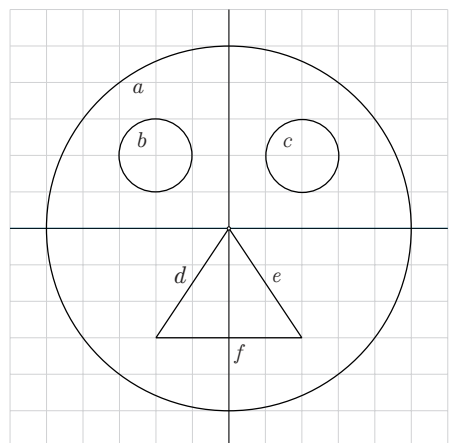
Na een ongelukkig huwelijk kreeg zij na de zelfmoord van haar man een aanstelling in Zweden aan de universiteit van Stockholm. Door een noodlottig voorval kreeg zij bij terugkeer van een vakantie de griep, waaraan ze stierf op 41-jarige leeftijd.

Oh-La-La, een lachend gezicht

In de tweede ronde moest ik zelf aan de bak. In deze ronde draaiden allemaal workshops waar de deelnemers zelf aan de slag konden. Ook Rutger Kock en ik daagden de deelnemers uit om zelf actief te worden. Van een som uit het boek naar een leuke les, hoe doe je dat? We begonnen met zingen waarmee je in je les machten van twee kunt inleiden. In Figuur 3 staat de eerste regel van de partituur. Bij een open rondje zingen de meisjes Oh, bij een dicht rondje zingen de jongens tegelijk La. Ik geef het tempo aan met een stokje. Met al die Oh's (meisjes) en La's (jongens) kwam de stem-



Figuur 3 Eerste regel van de partituur.



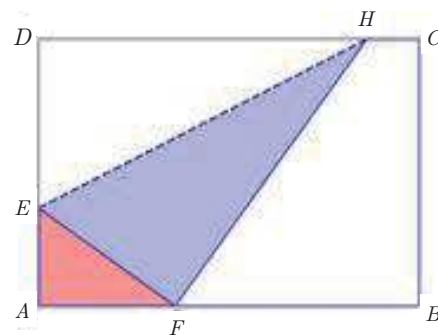
Figuur 4 Parametriseren van een gezicht.

ming er al goed in. Er worden vijf regels gezongen. (Daarna krijgen de leerlingen de opdracht om een zo lang mogelijke partituur van regels met vijf noten te maken, waarbij alle regels van elkaar verschillend zijn.)

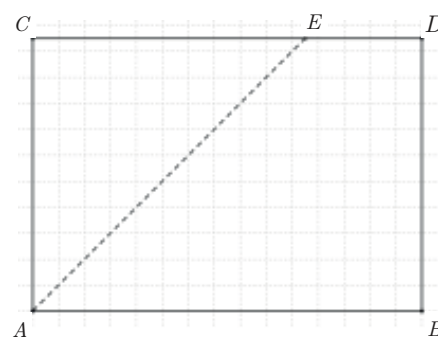
Vervolgens legde Rutger uit hoe hij zijn klas had uitgedaagd om met parametriseren een gezicht op het scherm te maken. Als bonus moest het gezicht lachend gemaakt worden. Hierbij moet je goed letten op het domein. Het domein van een cirkel ligt min of meer vast met $[0, 2\pi]$. Daar moeten de lijnstukjes en cirkelbogen op worden aangepast. Een mooie wiskundige denkactiviteit. Zie Figuur 4.

Driehoeken en ellipsen vouwen

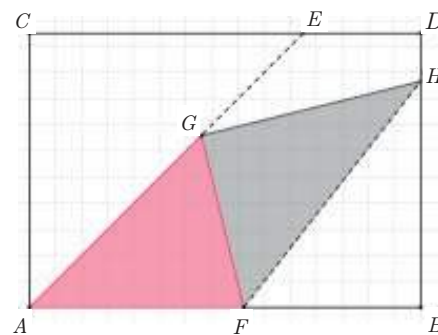
Nu volgt een voorbeeld van hoe ik bij een som uit het boek een leuke les maak. Ik laat het verhaal bij de opgave eerst zelf beleven. Er moet een vouw in een blaadje gemaakt worden waardoor er een driehoek ontstaat. Ik laat de klas dan willekeurige (drie)hoeken omvouden. Hoekpunt D wordt naar F op zijde AB gevouwen. Zie Figuur 5. Daarna moeten ze door opmeten van de zijden de oppervlakte van een driehoek, in dit geval driehoek AFE , berekenen. Wie de grootste oppervlakte heeft gevonden krijgt wat lekkers. Je ziet dan bij de gegeven antwoorden (wie heeft een nog grotere oppervlakte?) ook meteen wie de factor $\frac{1}{2}$ is vergeten. Dat antwoord is dan ongeveer 2 keer zo groot als de andere. Jammer, maar je hebt dan niet gewonnen. Omdat blijkt dat er allemaal verschillende antwoorden tevoorschijn zijn gekomen, ga ik er met de klas dieper op in. Het lijkt wel of er een grootste is. Waar denk je dan aan? Welke vraag zou je kunnen stellen? Dan zet ik ze, liefst in groepjes, aan het werk. Ze zullen zelf een onbekende zijde x moeten stellen. In het boek wordt al aangegeven welke zijde je x moet stellen. Dan is het denkwerk al gedaan. Bovendien zijn er verschillende zijden die je x kunt stellen die allemaal wel tot hetzelfde antwoord leiden. Leuk om te zien dat leerlingen ook op verschillende manieren het antwoord vinden. Als je uitgaat van een blaadje van 30 bij 21 cm (A4-formaat) dan is de oppervlakte van driehoek AEF maximaal als $AE = 7$ cm. Ik daag de lezer uit dit te verifiëren. Naast de opgaven uit het boek kwamen er ook onnoemelijk veel zelf bedachte voorbeelden van vouwsels op tafel, vergelijkbaar met de opgave uit het boek. (Zie www.uu.nl/



Figuur 5 Getal & Ruimte vwo B deel 4, opgave A28, p.118.



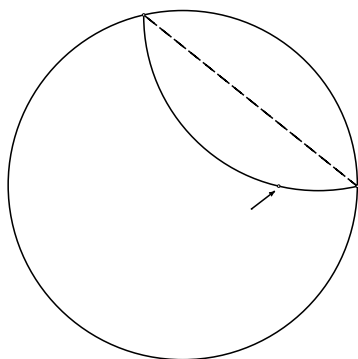
Figuur 6 Bissectrice AE van $\angle A$.



Figuur 7 B naar D op AE vouwen.

onderwijs/nationale-wiskunde-dagen, Archief, Slides/handouts. Ik ben bereid om bij secties die dat willen langs te komen en samen aan de slag te gaan om een leuke les bij opgaven uit het boek te maken.)

Bij de opgave 'driehoek naar $y = x$ ' wordt het hoekpunt rechtsonder naar de tevoren gevouwen bissectrice (diagonale vouw) van het hoekpunt linksonder gevouwen. Zie Figuur 6 en 7. Onder de omgevouwen onderkant zie je een driehoek (AFG) ontstaan met de gevouwen bissectrice en de onderkant van het blaadje. Zie Figuur 7. Ga weer uit van de afmetingen 30 bij 21 cm (A4-formaat). Hoe zou je door meten de oppervlakte kunnen berekenen? Stel een formule op van de oppervlakte van de (roze) driehoek AFG . Bereken de maximale oppervlakte van de op deze manier



Figuur 8 Een ellips vouwen.

verkregen driehoek. Aan de lezer om eerst eens zelf te gaan vouwen en de maximale oppervlakte te vinden. Het antwoord kan als volgt gaan. Stel $AF = x$. Dan is $BF = FG = 30 - x$. Neem AG als basis van driehoek AFG , dan is de hoogte de loodlijn uit F op AG is $x/\sqrt{2}$. Je kunt AG uitdrukken in x met behulp van de cosinusregel:

$$FG^2 = AF^2 + AG^2 - 2AF \cdot AG \cdot \cos(\angle GAF);$$

$\angle GAF = 45^\circ$, dus krijg je

$$(30 - x)^2 = x^2 + AG^2 - 2xAG \cdot \frac{1}{2}\sqrt{2}$$

oftewel

$$AG^2 - x\sqrt{2}AG + 60x - 900 = 0$$

en met de abc-formule is nu

$$AG = \frac{1}{2}(x\sqrt{2} + \sqrt{2x^2 - 240x + 3600});$$

de oppervlakte van $\triangle AFG$ is nu

$$\frac{1}{2} \cdot \frac{x}{\sqrt{2}} \cdot \frac{1}{2}(x\sqrt{2} + \sqrt{2x^2 - 240x + 3600}).$$

De afgeleide nul stellen levert een onpretelijke vergelijking op. CALC MAX geeft $x = 15$ (dus precies als je op het midden van de onderkant zit); $\max_{\text{opp}} = 112,5$. Wie kan het berekenen van de waarde van x waarbij de oppervlakte maximaal is, exact oplossen?

Behalve driehoeken werden er ook ellipsen 'gevouwen'. Als je oneindig vaak de rand van een cirkelvormig blaadje naar een gegeven stip (zie pijltje in Figuur 8) binnen de cirkel vouwt, dan ontstaat er binnen de cirkel een vlakdeel waar geen vouwen te zien zijn. Dit vlakdeel lijkt een ellips te zijn. Dit oneindig vouwen kun je beperken tot 20 tot 30 keer. De vraag is dan wat de vouwlijnen met de ellips te maken hebben. Kun je ook op elke vouwlijn het punt van de ellips construeren? Kun je ook de definitie van de ellips afleiden waarbij de som van de afstanden tot de brandpunten constant

is (het tekenen van een ellips met twee punaises en een touwtje)? Als het goed is kun je snappen dat het gegeven stipje (F) een brandpunt van de ellips is en dat het middelpunt M van de gegeven cirkel het tweede brandpunt van de ellips is en dat de straal van de cirkel precies de lengte van het touwtje is. Allemaal vragen die je met de klas samen kunt proberen te beantwoorden. Als je bedenkt dat het vouwen van de cirkelrand in feite een spiegeling is van een cirkelboog, dan kun je veel vragen beantwoorden en snappen hoe het zit bij een ellips. Neem een van de vouwen in het vizier en teken die met potlood over. Geef op de omgevouwen cirkelboog aan (stip G) waar die op het stipje F komt. Vouw terug. G ligt nu op de cirkelrand. De vouw AB is de middelloodlijn van FG . Teken nu de straal MG . Het snijpunt S van MG en de vouwlijn AB ligt nu op de ellips met brandpunten F en M . Immers $SF = SG$ (middelloodlijn) en $MS + SG = \text{straal}$, dus $MS + SF$ ook.

Getallentrucjes en Möbiusharten

Het avondprogramma werd verzorgd door Albrecht Beutenspacher. Hij is de directeur van het Mathatikum in Giessen (zie www.mathematikum.de). Dit museum trekt sinds de opening in 2002 jaarlijks vele bezoekers,



Figuur 10 Möbiusharten.

jong en oud. Het is een interactief museum waarin allerlei spelletjes en puzzels gedaan kunnen worden met wiskundige principes en verrassingen. In enkele ruimtes waren ook een aantal ervan tentoongesteld. Eén ervan is een parabool waarmee je kunt vermenigvuldigen. Verbind de punten van de parabool $y = x^2$ boven $x = -a$ en $x = b$. Het antwoord van $a \cdot b$ vind je dan op de y -as. Verklaring: de helling van de lijn AB is $(b^2 - a^2)/(a + b) = b - a$. De lijn $y = (b - a)(x - b) + b^2$ heeft helling $b - a$ en gaat door (b, b^2) . $x = 0$ geeft dan $y = ab$. Grappig, maar waar.

Hij maakte indruk met een getallentrucje waarmee je zonder gebruik van een rekenmachine eenvoudig twee grote getallen kunt vermenigvuldigen. Bijvoorbeeld 996×885 doe je als volgt: $996 = 1000 - 4$, $885 - 4 = 881$; de eerste 3 cijfers van het antwoord zijn nu 881, $885 = 1000 - 115$, doe nu $4 \times 115 = 460$, dit zijn de laatste 3 cijfers van het antwoord. Reken maar na: $996 \times 885 = 881460$. Hoe werkt de truc? Even uitgezocht. $x = 996$ geeft $1000 - x = 4$, $y = 885$ geeft $1000 - y = 115$. Dan is $y - (1000 - x) = x + y - 1000$ (dit is die 881); dus

$$\begin{aligned} (y - (1000 - x)) \cdot 1000 + (1000 - x)(1000 - y) \\ = (x + y - 1000) \cdot 1000 + 1000000 \\ - (x + y) \cdot 1000 + 1000000 + x \cdot y = x \cdot y. \end{aligned}$$

Dit is dan $881 \times 1000 + 4 \times 115 = 881460$.

Het meest interessante trucje was het plakken en doormidden knippen van twee dwars op elkaar geplakte tegengesteld gedraaide Möbiusbanden. Je krijgt dan twee in elkaar gestrengelde harten. 's Nachts op mijn kamer meteen maar uitgeprobeerd. Gelukt! Zie Figuur 10. Leuk om met Valentijnsdag in de les te doen.

TZAAR en Ramanujan

Voordat ik mij op de dansvloer waag probeer ik altijd een van de (nieuwe) spellen uit die elk jaar klaarliggen in de hal. Dit keer speelde ik een paar potjes TZAAR met Peter Donkelaar, een van de vrienden die ik ken van de staatsexamens. Het is een zogenaamd abstract gezelschapsspel voor 2 personen. Het is de bedoeling dat je als eerste van de tegenstander alle *tzaren*, *tzarara's* of *totts* van het veld hebt geslagen. Dit zijn allemaal ronde schijven met 0, 1 of 2 ringen. Het lijkt op een veredeld dammen waarbij je naar hartenlust mag stapelen 'tot in het oneindige'. Zie Figuur 11.

's Avonds werd de film *The man who knew Infinity*, over het leven van Srinivasa



Figuur 11 TZAAR.

Ramanujan, getoond. In de krant las ik er niet zulke goede recensies over. Maar collega's die ik sprak die hem gezien hadden vonden hem best wel indrukwekkend.

Spinkromme en eikromme

Voor de ochtendlezing op zaterdag ging ik naar Martin Kindt. Op 27 januari werd Martin aan het eind van een symposium ter gelegenheid van zijn 80ste verjaardag benoemd tot Officier in de Orde van Oranje Nassau. Zo de koning het heeft behaagd. Ik ben al vele jaren fan van Martin. Ook vandaag verraste hij ons weer met een mooi verhaal over de krommen van Dürer.

Uit een dik boek in het Duits in Gothische letters, een leerboek voor kunste-

naars over de drie dimensies en perspectieftekeningen, heeft Martin met de vertaling in het Engels ernaast enkele krommen gehaald en aan ons uitgelegd. De slakkenspiraal, de Archimedische spiraal en de helix (trappenspiraal) werden getoond en uitgelegd. De limaçon van Pascal werd al door Dürer geconstrueerd als een 'spinkromme' (1525). Hij tekende de hulplijntjes van de geconstrueerde punten er ook bij. Een straal met bijbehorende stukjes raaklijn. Op die manier lijkt het geheel op een spin met pootjes. Met $x = 3 \sin(t) - 2 \sin(2t)$ en $y = 3 \cos(t) - 2 \cos(2t)$ krijg je deze kromme op je scherm. Zie Figuur 12.

In de voor Martin typerende stijl, rustig en bescheiden, liet hij ons zien hoe Dürer bewees dat de 'eikromme' die je krijgt bij het doorsnijden van een kegel ook echt een ellips is. Al is het bewijs van Dandelin met de bollen in een kegel die onder en boven aan het doorsnijdingsvlak raken natuurlijk van een andere orde en eenvoud. Als slot liet Martin zien dat met het folium van Dürer de driedeling van een hoek kan worden gedaan. $x = \cos(\frac{1}{2}t) \cdot \cos(t)$ en $y = \cos(\frac{1}{2}t) \cdot \sin(t)$, dit geeft $r = \sqrt{x^2 + y^2} = \cos(\frac{1}{2}t)$. Zie Figuur 13. Dürer was niet alleen een begenadigd

schilder, maar had ook veel wiskundige kennis in huis. Dat is nu wel duidelijk.

Bewegende '3D'-plaatjes

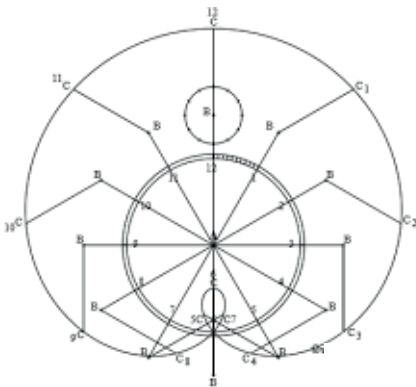
De laatste blokkezing die ik bijwoonde was van Jos Leys (www.josleys.com). Sinds 1980 bij de intrede van de eerste computers is Jos gefascineerd door plaatjes op het scherm. Immer nog maakt hij met behulp van eenvoudige formules met complexe getallen de mooiste bewegende '3D'-plaatjes van bijvoorbeeld Mandelbrotverzamelingen. Je kunt zien wat er gebeurt als je oneindig vaak inzoomt. Net als het Droste-effect waar bij het inzoomen ook nog eens gedraaid wordt. Jos gebruikt matrixtransformaties en groepentheorie om complexe vlakken af te beelden. Hij noemde onder andere werk van Bernard Maskit over de Schottky-groep als speciale Kleinse groep. Net als bij Henk van der Vorst worden stroken tot cirkels gemaakt en cirkels tot bollen. Met de duizelingwekkende beelden en een gevoel van bewondering, van zou ik dat ook ooit kunnen, verlaat ik de zaal.

Valselijk gebruik van statistiek

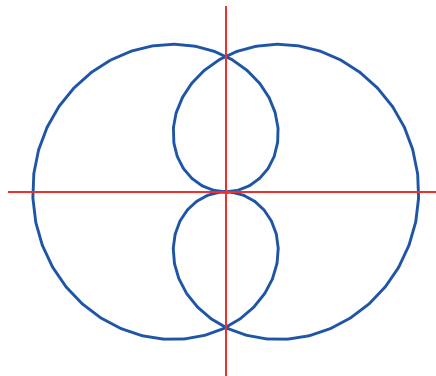
De slotlezing van Davy Paindaveine over de rangschikking van films vond ik wat te langdradig. De clou was al gauw duidelijk. Als je maar vaak genoeg een film een hoge waardering geeft dan gaan meer mensen die ook zien waardoor hij ook weer hoger gewaardeerd wordt. Op zich een mooi voorbeeld van het valselijk gebruik van statistiek. De rol van de mediaan en het gemiddelde werd pijnlijk duidelijk. Hoe een uitschieter naar oneindig voor een totale foute rangschikking kan leiden.

Voldaan naar huis

Na de lunch vertrok ik met een half lege big shopper, maar wel gevuld met mooie aandenkens aan deze NWD, voldaan naar huis.



Figuur 12 Spinkromme van Dürer.



Figuur 13 Folium van Dürer.

Jan Draisma

Mathematisches Institut, Universität Bern, en
Technische Universiteit Eindhoven
jan.draisma@math.unibe.ch

De oplossing

Tegenvoorbeelden voor het Helton–Nievermoeden

Het Helton–Nievermoeden zegt dat elke convexe, semialgebraïsche verzameling semidefinit representeerbaar is. In december 2016 is dit vermoeden op spectaculaire wijze met tegenvoorbeelden weerlegd door de Duitse wiskundige Claus Scheiderer. In dit artikel beschrijft Jan Draisma de achtergronden van het vermoeden en de tegenvoorbeelden van Scheiderer.

Polyeders

Sinds het begintijdperk van de wiskundige optimalisering is een centrale rol weggelegd voor *polyeders*: deelverzamelingen van $\mathbb{R}^n$ van de vorm

$$P := \{x \mid Ax \geq b\} \quad (1)$$

waarin A een $m \times n$ -matrix is, $b \in \mathbb{R}^m$ en waarin de ongelijkheid betekent dat $\sum_{j=1}^n a_{ij}x_j \geq b_i$ voor alle $i = 1, \dots, m$.

Het maximaliseren van een lineaire functie over zo'n polyeder kan efficiënt met behulp van inwendige-puntmethoden. De klasse van polyeders is gesloten onder doorsnedes — zet de ongelijkheden onder elkaar — en ook onder lineaire projecties; een algorithmisch bewijs voor dat laatste is *Fourier–Motzkineliminatie*.

Convexe semialgebraïsche verzamelingen

Maar lang niet alle optimaliseringsproblemen zijn recht en hoekig. Veel algemener zouden we een polynomiale functie f willen maximaliseren over een *semialgebraïsche* verzameling $U \subseteq \mathbb{R}^n$, dat wil zeggen een verzameling beschreven door een eindige (syntactisch correcte) formule opgebouwd

uit de coördinaten x_i , reële constanten, de operaties $+$ en $\cdot$ en de symbolen $\geq$, AND, OR and NOT. Door een extra variabele x_{n+1} in te voeren en aan de beschrijving van U de conditie $x_{n+1} = f(x_1, \dots, x_n)$ toe te voegen, mogen we aannemen dat f lineair is. Dan is het maximum van f over U , als het bestaat, gelijk aan het maximum van f over het convexe omhulsel van U . Tarski's quantoreneliminatie impliceert dat dat con-

vexe omhulsel weer een semialgebraïsche verzameling is. Dit leidt tot de volgende centrale vraag:

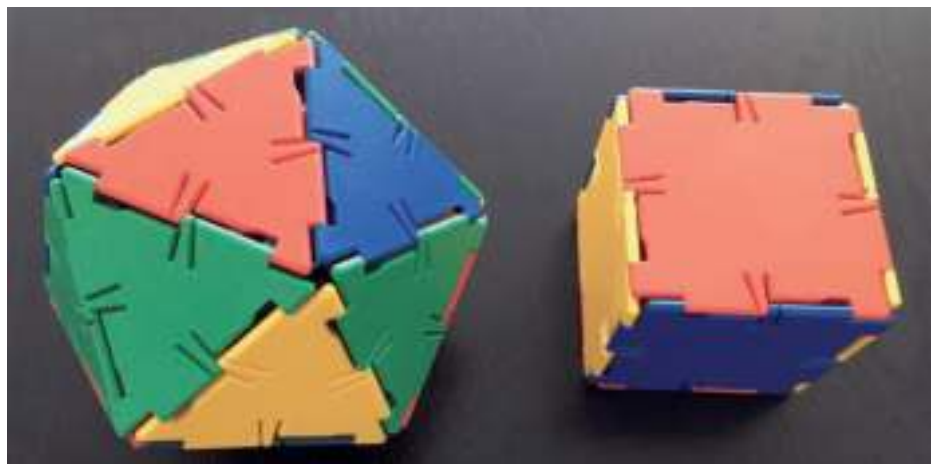
Vraag: Bestaat er een uniforme beschrijving voor convexe, semialgebraïsche verzamelingen?

Spectraëders en hun projecties

Even terug naar polyeders. De polyeder P in (1) is het beeld van de polyeder

$$Q := \{(y, z, s) \in \mathbb{R}^n \times \mathbb{R}^n \times \mathbb{R}^m \mid A(y - z) = b + s \text{ en } y, z, s \geq 0\}$$

onder de projectie $(y, z, s) \mapsto y - z$. Met deze truc kan dus elke polyeder P gezien wor-

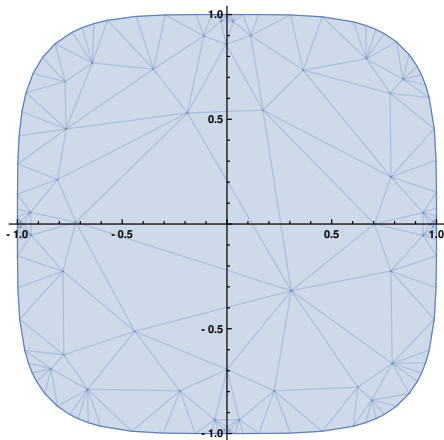


Figuur 1 Twee bekende polyeders.

den als het beeld onder een lineaire projectie van de doorsnede van een geschikte affien-lineaire deelruimte V (hier gegeven door $A(y-z) = b+s$) in een zekere $\mathbb{R}^p$ met het positieve orthant $\mathbb{R}_{\geq 0}^p$. Om ook ronde convexe verzamelingen te kunnen beschrijven, ligt het voor de hand om $\mathbb{R}_{\geq 0}^p$ te vervangen door een goed begrepen andere convexe kegel. Een van de meest bestudeerde kegels is de volgende: vervang $\mathbb{R}^p$ door de vectorruimte van symmetrische $p \times p$ -matrices, en vervang $\mathbb{R}_{\geq 0}^p$ door de kegel C_p van positief semidefiniete matrices, dat wil zeggen symmetrische matrices met alleen maar niet-negatieve eigenwaarden. Een doorsnede van C_p met een affien-lineaire deelruimte heet een *spectraëder*. In tegenstelling tot polyeders blijkt de klasse van spectraëders niet gesloten onder lineaire projecties. Een verzameling in $\mathbb{R}^n$ die het beeld is van een spectraëder onder een lineaire projectie, heet *semidefinit representeerbaar*. Inwendige-puntmethoden blijken ook te werken voor zulke verzamelingen — al is het voor praktische optimaliseringstoepassingen wel belangrijk dat de semidefiniete representatie niet al te groot is! Door $\mathbb{R}^p$ via diagonaalmatrices in te bedden in $\mathbb{R}^{p \times p}$ vinden we trouwens dat elke polyeder semidefinit representeerbaar is.

Het Helton–Nievermoeden

Semidefinit representeerbare verzamelingen zijn semialgebraïsch en convex. In 2006 vroeg Nemirovski in zijn plenaire voordracht op het International Congress of Mathematicians of het omgekeerde ook waar is [4]. Helton en Nie gaven in [1] voldoende voorwaarden voor semidefiniete representeerbaarheid, en vermoedden dat



Figuur 2 Oplossingen van $x^4 + y^4 \leq 1$.

het antwoord op Nemirovski's vraag ja zou moeten zijn:

Het Helton–Nievermoeden. *Elke convexe, semialgebraïsche verzameling is semidefinit representeerbaar.*

Voorbeeld met Lasserres hiërarchie

Het gebied $U := \{(x, y) \in \mathbb{R}^2 \mid x^4 + y^4 \leq 1\}$ is convex en semialgebraïsch. Lezers van mijn leeftijd en ouder zullen er de vorm van een ouderwets televisiescherm in herkennen. Dit gebied blijkt inderdaad de projectie van een spectraëder. In plaats van een zo efficiënt mogelijke presentatie, is hier een presentatie die automatisch uit een constructie van Lasserre komt rollen: als de symmetrische matrix

$$A = \begin{bmatrix} 1 & a & b & c & e \\ a & c & d & h & j \\ b & d & e & i & k \\ c & h & i & l & n \\ e & j & k & n & p \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{array}{l} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 - (l+p) \end{array}$$

positief semidefinit is, dan hebben al haar hoofddeelmatrices niet-negatieve determinant. En dus geldt achtereenvolgens, door naar geschikte 2×2 -hoofddeelmatrices te kijken, $c \geq a^2$, $l \geq c^2 \geq a^4$, $e \geq b^2$ en $p \geq e^2 \geq b^4$. Ten slotte geeft de component rechtsonder dat $0 \leq 1 - (l+p) \leq 1 - (a^4 + b^4)$. Dus als we bovenstaande geparametriseerde affiene ruimte snijden met C_6 , dan ligt het beeld van die doorsnede onder projectie op het (a, b) -vlak in U . Omgekeerd, als $(x, y) \in U$, dan definiëren we de rijvector $u := [1 \ x \ y \ x^2 \ y^2 \ 0]$ en is de matrix

$$u^T u + \text{diag}(0, 0, 0, 0, 0, 1 - (x^4 + y^4)) = \begin{bmatrix} 1 & x & y & x^2 & y^2 & 0 \\ x & x^2 & xy & x^3 & xy^2 & 0 \\ y & xy & y^2 & x^2y & y^3 & 0 \\ x^2 & x^3 & x^2y & x^4 & x^2y^2 & 0 \\ y^2 & xy^2 & y^3 & x^2y^2 & y^4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 - (x^4 + y^4) \end{bmatrix}$$

positief semidefinit en van de vorm hierboven. Dus is U de projectie van een spectraëder. Lasserre introduceerde in [3] een algemene methode om convexe semialgebraïsche verzamelingen U steeds beter te benaderen met projecties van spectraëdra, op een zodanige manier dat — in ieder geval voor *compacte* U — die projecties convergeren naar U . Maar die methode geeft in het algemeen niet na eindig veel stappen een exacte beschrijving van U .

Overigens is het convexe omhulsel van een compacte semialgebraïsche *kromme*, ingebed in $\mathbb{R}^n$ — zoals hier de kromme met vergelijking $x^4 + y^4 = 1$ in $\mathbb{R}^2$ — altijd semidefinit representeerbaar [6]. In datzelfde artikel wordt daaruit het Helton–Nievermoeden voor $\mathbb{R}^2$ afgeleid.

Orbitopen

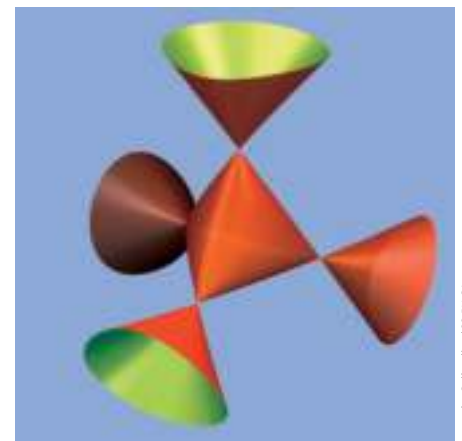
Orbitopen zijn convexe, compacte, semialgebraïsche verzamelingen die als volgt ontstaan. Neem een compacte topologische groep G , een continue representatie van G op een eindig-dimensionale reële vectorruimte V en een element $v \in V$. Dan is het convexe omhulsel U van de baan Gv van v semialgebraïsch, en het heet een orbitopen [5] — een samentrekking van *orbit* (baan) en *polytoop* (begrensde polyeder). De polyedra van Figuur 1 zijn voorbeelden van orbitopen.

Voor een rond voorbeeld nemen we $G = O_n$, de groep van orthogonale matrices die werkt op $V = \mathbb{R}^n$ door middel van matrix-vectorvermenigvuldiging. Dan is het orbitopen van $v \in V$ een bol van straal $\|v\|$. Dit orbitopen is zelf een spectraëder: nemen we voor het gemak $\|v\| = 1$, dan bestaat de bol uit alle vectoren $(x_1, \dots, x_n)$ waarvoor de matrix

$$\begin{bmatrix} 1+x_1 & x_2 & \cdots & x_n \\ x_2 & 1-x_1 & & \\ \vdots & & \ddots & \\ x_n & & & 1-x_1 \end{bmatrix}$$

(met nullen op de lege plekken) positief semidefinit is.

Een interessanter voorbeeld krijgen we met dezelfde $G = O_n$ en met V de ruimte van symmetrische $n \times n$ -matrices, waarop G werkt via $(g, A) \mapsto gAg^T$. Elke



Figuur 3 Cayley's derdegraads oppervlak.

baan bevat een unieke diagonaalmatrix $D := \text{diag}(\lambda_1, \dots, \lambda_n)$ waarbij $\lambda_1 \geq \dots \geq \lambda_n$. Het convexe omhulsel van de baan van D blijkt te bestaan uit alle symmetrische matrices A met eigenwaarden $\mu_1, \dots, \mu_n$ zo dat voor alle $k = 1, \dots, n-1$ de ongelijkheid $\sum_{i=1}^k \lambda_i \geq \sum_{i \in I} \mu_i$ geldt voor alle $I \subseteq \{1, \dots, n\}$ van kardinaliteit k en zo dat $\sum_{i=1}^n \lambda_i = \sum_{i=1}^n \mu_i$ — dat volgt uit de klassieke Schur–Hornstelling. Maak nu bij een algemene symmetrische matrix $A \in \mathbb{R}^{n \times n}$ de lineaire afbeelding A_k van het alternerend product $\wedge^k \mathbb{R}^n$ naar zichzelf gedefinieerd door

$$\begin{aligned} A_k(v_1 \wedge \dots \wedge v_k) \\ = \sum_{i=1}^k v_1 \wedge \dots \wedge v_{i-1} \wedge A v_i \wedge v_{i+1} \wedge \dots \wedge v_n. \end{aligned}$$

Dan is de conditie op de eigenwaarden μ_i van A equivalent met de eigenschap dat $(\sum_{i=1}^k \lambda_i)I - A_k$ positief semidefinit is voor elke $k = 1, \dots, n-1$. Dus deze A 's vormen een spectraëder.

In [5] werd de vraag geopperd of elk orbitoep een projectie van een spectraëder is — een speciaal geval dus van het Helton–Nievermoeden. De opgeblazen tetraëder in het midden van Cayley's derdegraads oppervlak (zie Figuur 3) wordt daar aangevoerd als ander voorbeeld van een orbitoep dat zelf al een spectraëder is.

Scheiderers tegenvoorbeelden

Veel convexe semialgebraïsche verzamelingen zijn dus inderdaad semidefinit representeerbaar. Maar in december 2016 weerlegde de Duitse wiskundige Claus Scheiderer uit Konstanz op spectaculaire

wijze het Helton–Nievermoeden, door te laten zien dat heel veel convexe semialgebraïsche verzamelingen in $\mathbb{R}^n$ *geen* projectie van enige spectraëder zijn [7]:

Stelling. *Voor elke semialgebraïsche verzameling $U \subseteq \mathbb{R}^n$ van dimensie tenminste twee bestaat er een polynomiale afbeelding $\phi: \mathbb{R}^n \rightarrow \mathbb{R}^m$ zo dat de afsluiting van het convexe omhulsel van $\phi(U)$ niet semidefinit representeerbaar is.*

Nu zou men kunnen denken, dat op deze manier slechts heel exotische niet semidefinit representeerbare convexe semialgebraïsche verzamelingen geconstrueerd kunnen worden. Maar niets is minder waar. Een concreet voorbeeld aan het einde van Scheiderers artikel is zelfs een orbitoep: laat O_n werken op de d -de symmetrische macht $S^d \mathbb{R}^n$ van $\mathbb{R}^n$ door $(g, v_1 \dots v_d) \mapsto (gv_1) \dots (gv_d)$. Deze vectorruimte heeft dimensie $\binom{n+d-1}{d}$, het aantal monomen in n variabelen van graad precies d .

Stelling. *Als $n, d \geq 4$ met d even, dan is het Veronese orbitoep, het convexe omhulsel van de baan $O_n v^d$ voor een willekeurige $v \in \mathbb{R}^n \setminus \{0\}$, niet semidefinit representeerbaar.*

Dit orbitoep hangt nauw samen met vragen die teruggaan tot werk van Hilbert. Elementen van $S^d \mathbb{R}^n$ kunnen worden opgevat als homogene polynomen van graad d in n variabelen. Neem aan dat d even is. De polynomen in $S^d \mathbb{R}^n$ die geschreven kunnen worden als som van



Claus Scheiderer

kwadraten van polynomen van graad $d/2$ vormen een convexe, gesloten kegel $\Sigma_{n,d}$. Deze kegel is bevat in de convexe kegel $P_{n,d} \subseteq S^d \mathbb{R}^n$ van polynomen die overal op $\mathbb{R}^n$ niet-negatieve waarden aannemen. Hilbert liet al zien dat $\Sigma_{n,d} \subsetneq P_{n,d}$ behalve voor $d = 2$ of $n \leq 2$ of $(n, d) = (3, 4)$ [2]. Scheiderer bewijst dat $P_{n,d}$ *geen* semidefinit representatie heeft, behalve in deze uitzonderingsgevallen.

Met Scheiderers werk komt er een abrupt einde aan de hoop dat alle convexe semialgebraïsche verzamelingen semidefinit representeerbaar zouden kunnen zijn. Maar er blijven nog allerlei spannende vragen open, zoals: wat is de laagste dimensie van zo'n tegenvoorbeeld? Misschien drie? ☹

Referenties

- 1 J. William Helton en Jiawang Nie, Sufficient and necessary conditions for semidefinite representability of convex hulls and sets, *SIAM J. Optim.* 20(2) (2009), 759–791.
- 2 D. Hilbert, Über die Darstellung definiter Formen als Summe von Formenquadraten, *Math. Ann.* 32 (1888), 342–350.
- 3 Jean B. Lasserre, Convex sets with semidefinite representation, *Math. Program.* 120(2(A)) (2009), 457–477.
- 4 Arkadi Nemirovski, Advances in convex optimization: conic programming, in *Proceedings of the International Congress of Mathematicians (ICM)*, Madrid, Spain, August 22–30, 2006, Plenary Lectures and Ceremonies, Volume I, European Mathematical Society, 2007, pages 413–444.
- 5 Raman Sanyal, Frank Sottile en Bernd Sturmfels, Orbitopes, *Mathematika* 57(2) (2011), 275–314.
- 6 Claus Scheiderer, Semidefinite representation for convex hulls of real algebraic curves, Preprint, 2012, arXiv:1208.3865.
- 7 Claus Scheiderer, Semidefinitely representable convex sets, Preprint, 2016, arXiv:1612.07048.

Frits Beukers

Mathematisch Instituut
Universiteit Utrecht
f.beukers@uu.nl

Rob Bisseling

Mathematisch Instituut
Universiteit Utrecht
r.h.bisseling@uu.nl

Evenement 53ste Nederlands Mathematisch Congres (NMC 2017)

Een congres door jong en oud

Op 11 en 12 april 2017 kwamen 226 deelnemers bijeen in het splinternieuwe Koningsbergergebouw van de Universiteit Utrecht voor het 53ste Nederlands Mathematisch Congres, georganiseerd onder auspiciën van het KWG. Frits Beukers en Rob Bisseling van het plaatselijke organisatiecomité doen verslag.

Het congres werd geopend door rector-magnificus Bert van der Zwaan die op energieke wijze het programma introduceerde, het belang en de voorbeeldfunctie van Mastermath benadrukte, en ook zijn waardering uitsprak voor de Utrechtse wiskunde.

Rondom het lezingenprogramma was er de gelegenheid de tentoonstelling 'Women in Mathematics' te bekijken met foto's gemaakt door Noel Tovia Matoff en interviews door Sylvie Paycha en Sara Azzali. Stands waren er van KWG, Epsilon uitgaven, Puzzlingworld, European Women of Mathematics, Ortec, de Nederlandse Vereniging van Wiskundeleraren, Pythagoras, Kangoeroe, Vierkant voor Wiskunde, Optische Fenomenen en Noordhoff. Er was ook een postersessie met vijf deelnemers, een klein aantal dat hopelijk groeit in de toekomst bij volgende NMC's. Het congresdiner in de fraaie ambiance van de aula van het Utrechtse Academieggebouw op dinsdagavond 11 april werd goed bezocht door ruim tachtig deelnemers.

De lokale organisatie was in handen van Rob Bisseling, Carolin Kreisbeck en Johan van de Leur. Het lezingenprogramma werd samengesteld door een wetenschappelijke commissie onder voorzitterschap van Frits Beukers.

Openingsvoordracht

Openings spreker was Henry Cohn, werkzaam by Microsoft Research, New England en MIT. Zijn voordracht ging over de recente spectaculaire resultaten over bolpakkingen. Stel je wilt massieve bollen van dezelfde grootte, zo dicht mogelijk samenvakken in de n -dimensionale ruimte. Wat is het grootst mogelijke bezettingspercentage? Voor $n = 2$ hebben we de honingraatstructuur en voor $n = 3$ de sinaasappelstapel van de groenteboer. Het bewijs van de optimaliteit van deze laatste pakking is een technisch hoogstandje van Tom Hales. De dimensies 8 en 24 zijn speciaal vanwege het bestaan van het E_8 - en het Leech-rooster. Heel recent bleek het mogelijk het bolpakkingprobleem voor deze dimensies op te lossen. Henry Cohn is een van de grote namen in deze ontwikkeling en is co-auteur van het bewijs voor $n = 24$. In een even mooie als toegankelijke voordracht legde Cohn ons de basisprincipes van het pakkingprobleem uit en ging vervolgens over naar het geval $n = 8$. Het gevaar van bolpakkingstheorie is dat het heel snel technisch dreigt te worden, zie bijvoorbeeld het bewijs van Hales voor $n = 3$. Het verhaal over $n = 8$ (en ook van $n = 24$) heeft een verrassende en wiskundig mooie wending door het verschijnen van modulaire vormen. Deze zijn het

werkpaard van de moderne getaltheorie. De voordracht was prachtig, zowel de presentatie als de geboden wiskunde. Een van de beste voordrachten van de afgelopen jaren.

Brouwermedaille

De Brouwermedaille wordt elke drie jaar door het KWG uitgereikt aan een vooraanstaand wiskundige en is de belangrijkste Nederlandse wiskundeprijs. Dit jaar was het te bekronen vakgebied de getaltheorie, en een jury bestaande uit Hendrik Lenstra (voorzitter), Gunther Cornelissen, Jan-Hendrik Evertse, Lenny Taelman en Jaap Top besloot deze onderscheiding toe te kennen aan Kenneth Ribet, werkzaam aan de



Kenneth Ribet geeft de Brouwerlezing

University of California, Berkeley. Hij is een van de grote namen op het gebied van de moderne getaltheorie, met name algebraïsche getaltheorie en modulaire vormen. Dankzij Ribet werd duidelijk dat de correctheid van het Shimura–Taniyama–Weil-vermoeden voor modulaire vormen de laatste stelling van Fermat impliceert. En dat is ook de manier waarop Wiles uiteindelijk zijn bewijs leverde. In aanwezigheid van zijn echtgenote Lisa Goldberg (zelf statisticus) en zijn twee dochters, Brouwer-biograaf Dirk van Dalen, de juryvoorzitter en vele anderen in een volgepakte Cosmoszaal, gaf Kenneth Ribet een zeer toegankelijke voordracht rondom de laatste stelling van Fermat. Hij bewees op het krijtbord dat de vergelijking $a^n + b^n = c^n$ geen geheeltallige oplossing heeft voor $n = 4$, en gaf veel historische context, ook uit zijn persoonlijke ervaringen puttend. Na Ribets voordracht sprak Hendrik Lenstra op zijn eigen, onnavolgbare humoristische wijze een laudatio uit, en overhandigde KWG-voorzitter Erik van den Ban de medaille aan Ribet. De laudatio en een interview met Ribet vindt u afgedrukt na dit verslag.

Openingsvoordracht tweede dag

De tweede dag van het NMC begon met een plenaire lezing van Konstantin Mischaikow (Rutgers University) die voor elk wat wils bracht met ingrediënten uit vele deelgebieden van de wiskunde: mathematische biologie, grafentheorie, combinatoriek, parallelle algoritmen en dynamische systemen. Mischaikow modelleert het genregulatiernetwerk van de malariaverwekker *Plasmodium falciparum* via dynamisch veranderende gerichte grafen en laat hierop computationele homologie-algoritmen los. Een implementatie is beschikbaar als open-source software DSGRN, Dynamic Signatures for Genetic Regulatory Networks.

Slotvoordracht

De slotspreker was Jos Leys, geen wiskundige, zoals hij zelf benadrukt. Hij is gepensioneerd ingenieur die in de chemie heeft gewerkt. Hij heeft echter wiskundige roem verworven door zijn schitterende galerijen van wiskundige visualisaties. Het filmpje bij de entree van het congres was een eenvoudig voorbeeld daarvan. Hij is een van de auteurs van de film *Dimensions*, die gaat van elementaire meetkunde, naar vierdimensionale polytopen en ten slotte Hopf-vezelingen. Recent is hij co-auteur

van de nieuwe film *Chaos*, die in dertien delen een uitleg geeft over dynamische systemen, vreemde attractoren en chaos. Beide films kunnen op zijn website gevonden worden (gewoon Jos Leys googelen).

De voordracht begon met een demonstratie van de bekende Mandelbrotverzameling, maar ook met driedimensionale versies ervan. Dit resulteerde in een bizarre galerij van driedimensionale landschappen. Een ander onderwerp was de visualisatie van limietverzamelingen van Kleinse groepen. Dit zijn discrete ondergroepen van $SL(2, \mathbb{C})$, die een uitzonderlijk rijke structuur hebben. Leys vertelde ons zijn problemen om op deze limietfiguren in te zoomen, maar kwam vervolgens met een aantal trucs om dit toch voor elkaar te krijgen. Niet slecht voor een niet-wiskundige.

Semiplenaire sprekers

Nelly Litvak (Universiteit Twente) gaf een overzicht van centraliteitsmaten in netwerken, zoals Googles PageRank voor het wereldwijde web. Ook presenteerde ze een tweefasen-algoritme dat haar in staat stelt snel de invloedrijkste Twittergebruikers te identificeren met slechts een beperkt aantal informatieverzoeken, typisch één per minuut, zoals toegestaan door sociale netwerken. Een algoritme met vermoedelijk grote commerciële potentie.

Afgelopen jaar heeft Dion Gijswijt (TU Delft) al enige furore gemaakt door het zogenaamde ‘Cap Set’-probleem op te lossen, samen met en onafhankelijk van Jordan Ellenberg. Het resultaat is een gemeenschappelijke publicatie in *Annals of Math*. In het vorige nummer van het Nieuw Archief is een artikel over dit werk te vinden en de toehoorders konden dus goed voorbereid naar de voordracht komen. Maar ook voor degenen die het artikel nog niet gelezen hadden, wist de spreker wel helemaal duidelijk te maken waar het probleem over ging en wat de oplossing was. Kort gezegd, een combinatorisch probleem, waarmee men al jaren vast zat, kan worden opgelost door gebruik te maken van een polynoomconstructie en eigenschappen van polynoomvermenigvuldiging modulo p . Zeer verrassend en indrukwekkend.

Natasha Maurits (Universitair Medisch Centrum Groningen) gaf een TED-achtige presentatie (zie ook haar YouTube filmpje *Patients in numbers*) waarin ze vertelde over toepassingen van wiskunde in de neurologie. Moderne tracking methoden



Nelly Litvak bespreekt een algoritme om snel de top-100 van meest gevolgde Twitteraars te vinden.

met sensors bevestigd aan hand en arm leveren de data van een beweging van de patient aan de computer, bij een standaardtest zoals de hand naar de neus brengen. Een machine learning-algoritme kan vervolgens het afgelegde traject classificeren naar symptomen van een neurologische aandoening zoals de ziekte van Parkinson.

Bob Rinks semiplenaire lezing (met prachtige figuren gemaakt in TikZ) behandelde het probleem van synchronisatie in netwerken van gekoppelde niet-lineaire dynamische systemen. Een voorbeeld is het collectief gedrag van vogelzwermen en het simultaan afvuren van neuronen in de hersenen. Bobs aanpak van dit probleem is gebaseerd op de notie van graaffectiviteit.

Lezing Jaap Korevaar

Jaap Korevaar en Fred van der Blij zijn dit jaar precies 75 jaar lid van het KWG en dit werd op een speciale manier gevierd. De gezondheid van Fred van der Blij stond niet toe aanwezig te zijn op het NMC 2017, maar hij werd in het voorafgaande week-einde thuis verrast met een bloemstuk namens het KWG. Jaap Korevaar gaf acte de présence en was uitgenodigd terug te kijken op zijn lange carrière. Hij deed dit door een moderne beamerpresentatie te geven, ondersteund door een student die vrijwel ongemerkt telkens een signaal kreeg door te klikken naar de volgende slide.

Jaap, geboren in 1923, studeerde tijdens de oorlogsjaren, deed tentamens bij docenten thuis, en leende schaarse wiskundeboeken voor zover die beschikbaar waren



Foto: Karina Korevaar

Jaap Korevaar met stripboek na zijn lezing in gesprek met Ferdinand Verhulst.

om wiskunde uit te studeren. Na de oorlog bracht hij vele jaren door in de Verenigde Staten aan de universiteit van California in San Diego, en van Wisconsin in Madison, alvorens terug te keren naar Nederland, waar hij nu emeritus hoogleraar aan de UvA is. In zijn levendige verhaal doorspekt met anekdotes vertelde hij onder andere hoe een haperende kabelbaan tijdens een conferentie-excursie naar een bergtop zijn hele vakgebied dreigde weg te vagen. Het liep gelukkig goed af en Jaap nam voor de zekerheid toch maar het voetpad op de terugweg. Als dank voor zijn mooie historisch verhaal kreeg hij van de voorzitter van het KWG een passend cadeau, het stripboek *Ehrenfest!* uitgegeven door Museum Boerhaave. Een weergave van zijn voordracht vindt u verderop in dit nummer.

Minisymposia

In totaal zeven minisymposia met elk drie of vier sprekers waren onderdeel van het NMC: vier minisymposia georganiseerd door de clusters GQT, DIAMANT, NDNS+, en STAR, en verder een minisymposium over optimalisering, een minisymposium over scientific computing, en tot slot een minisymposium 'Computability, Complexity, and Randomness' van onderzoeksschool WONDER rondom de Stieltjesprijs 2015 voor het beste wiskundeproefschrift, gewonnen door Rutger Kuyper (University of Wisconsin, Madison).

Docentensymposium

Thema van deze middag was 'Achtergronden bij de nieuwe onderwerpen in

het wiskundeprogramma voor de tweede fase', georganiseerd door Michiel Doorman en Derk Pik. Er was een dertigtal deelnemers op de middag afgekomen. Het eerste deel bestond uit een drietal voordrachten. Eén over Sangaku-meetkunde door Jeroen Spandaw met wel een paar zeer uitdagende Sangaku's. Vervolgens Arthur Bakker over de dilemma's bij het geschikt maken van begrippen uit de statistiek voor het onderwijs. En ten slotte Quintijn Puite over logisch redeneren, een onderwerp uit wiskunde C. Het laatste deel bestond uit de uitreiking van de Pythagoras Profielwerkstuk Prijs. Daaraan vooraf gingen drie leerlingpresentaties van hun werkstuk, waarbij het publiek ondertussen ook was uitgebreid met aanhang van de leerlingen. Alle drie de presentaties waren van een verrassend hoog niveau. Toch kon er maar één de winnaar zijn en dat werd Tjeu Kayim over 'Error-correctie van QR-codes'.

Jaarvergadering KWG

Een dertigtal leden en het bestuur van het KWG vergaderden op 11 april tijdens de lunchpauze van het NMC, in een algemene ledenvergadering die geleid werd door KWG-voorzitter Erik van den Ban. Een belangrijke vraag die aan de orde kwam is het toekomstige formaat van het NMC, codenaam *NMC nieuwe stijl*, waarbij gemikt wordt op een conferentiecentrum als vaste locatie met 300 deelnemers, liefst in de periode rond Pasen. André Ran, voorzitter van de commissie NMC nieuwe stijl bracht verslag uit en vertelde dat zo'n NMC inderdaad mogelijk is, tegen een geringe verhoging van deelnemerkosten, waarbij dan wel zowel diner als een overnachting inbegrepen zouden zijn. De clusters zouden in deze opzet een grotere rol in de organisatie krijgen en hun jaarlijkse bijeenkomsten in het NMC onderbrengen.

Evaluatie Mastermath

Erik Koelink (Radboud Universiteit) presenteerde de bevindingen van een commissie bestaande uit Marieke Kranenburg, Cor Kraaikamp en hijzelf als voorzitter, die tot taak had het samenwerkingsverband Mastermath van Nederlandse masteropleidingen wiskunde te evalueren. Mastermath heeft in de afgelopen jaren een enorme groei doorgemaakt in het aantal deelnemende studenten en de vraag is hoe dit ook in de toekomst te accommoderen, via

een combinatie van centraal en decentraal gegeven colleges en werkcolleges. Er zal geëxperimenteerd worden met video-opnames van hoorcolleges. De commissie beschouwt Mastermath als een extra argument bij de werving van buitenlandse masterstudenten. Aanbevolen wordt de cursussen van Mastermath minstens twee jaar vooruit te plannen, zodat studenten bij het begin van hun master een volledig overzicht hebben over de hele studieperiode.

Bronstee PhD-prijs

Traditiegetrouw werd ook de PhD-prijs uitgereikt, een prijs voor de beste voordracht over hun werk door PhD-kandidaten. Deze werd gesponsord door Peter en Ghica van Emde Boas van Bronstee.com. Vijf PhD-kandidaten hielden een voordracht. Dat waren Maarten Derickx (Torsion points on elliptic curves over number fields), Ralph Klaasse (Constructing A -symplectic structures), Sanne Willems (Optimal scaling of ordinal data in survival analysis), Erik Visse (Explicit bounds on Brauer groups for Kummer surfaces) en Frans de Ruiter (Duality in two-stage linear and nonlinear adaptive robust optimization). De jury, onder leiding van Dirk Siersma, was onder de indruk van alle presentaties en onderzoeksresultaten. Op deze manier ontstond er een mooi en divers beeld van huidig promotieonderzoek in de wiskunde in Nederland. Uiteindelijk ging Ralph Klaasse er met de prijs vandoor. Hij bleek in staat om in korte tijd een abstract en diep onderwerp begrijpelijk te maken voor een wiskundig publiek, aldus de jury. ¶



Foto: Gilt Cavalcanti

Winnaar Ralph Klaasse van de Bronstee PhD-prijs

Hendrik Lenstra

*Mathematisch Instituut
Universiteit Leiden
hwl@math.leidenuniv.nl*

Event Award ceremony Brouwer Medal 2017

Laudation for Kenneth Ribet

At NMC 2017, on 11 April, the Brouwer Medal had been awarded to Kenneth Ribet for his contributions to number theory, in particular for the groundbreaking work in which he applies methods of algebraic geometry to number theoretical problems. This work later became of decisive importance for the proof of Fermat's Last Theorem.

This speech was pronounced at the event by Hendrik Lenstra, chairman of the Brouwer Medal Committee. An interview with Kenneth Ribet is published hereafter.

Ladies and gentlemen!

My name is Hendrik Lenstra, and I served as the chair of the 2017 Brouwer Medal Committee that was appointed by the Board of the Koninklijk Wiskundig Genootschap. The other members of the committee were Gunther Cornelissen, from Utrecht; Ronald Cramer, from the CWI in Amsterdam; Jan-Hendrik Evertse, from Leiden; Lenny Taelman, from the Universiteit van Amsterdam; and Jaap Top, from Groningen.

I wish to give account of the work done by the committee and the considerations that applied to the candidate that was selected. I have to warn you that there are limits on what I will be able to tell you. Many years ago I attended a laudation that was pronounced on an earlier Brouwer Medalist. The speaker enumerated many wonderful results that had been achieved by the candidate. And he concluded that 'therefore' the prize could *only* be awarded to this candidate. It struck me, at the time, that this was not a logical conclusion. Saying that 'only' one particular person deserves the prize, is a statement about all *other* candidates, and not about that particular person.

Not so long ago, during a reception following the Abel Prize ceremony in Oslo, King Harald of Norway asked the Abel Prize Committee how they had selected the prize winner. The answer of the committee was: Your Majesty, we considered all members of the entire world population, and we

eliminated them one by one, until only one person was left.

That is, essentially, also the way the Brouwer Medal Committee proceeded. So, if you want to hear more about this year's prize winner, I shouldn't say more about the work of the committee. But I do want to tell you which criteria we applied.

There are two official criteria. The first is that the candidate should be an 'internationally authoritative mathematician' in the area of number theory in the broad sense; number theory, because that is the area that the Board of the Koninklijk Wiskun-



Ken Ribet (left) receives the Brouwer Medal from Erik van den Ban, chairman of the Koninklijk Wiskundig Genootschap



Ken Ribet with his wife Lisa Goldberg

Photo: Gil Cavalcanti

dig Genootschap had selected for the 2017 Brouwer Medal. And the second criterion is that the candidate is able to give a lecture on his field that is of interest to a general mathematical audience.

There is a third, very informal criterion that the committee decided to apply, guided by the tradition of the Brouwer Medal. There are many prizes in mathematics, and they go to a relatively small number of excellent mathematicians. If you want your prize to be different from other prizes, then you should consider candidates whose work is more important than might appear from the number of prizes they have won. And that is what we did.

I want to mention two achievements of Ken Ribet in number theory that played an important role in the considerations of the committee.

The first is the Herbrand–Ribet theorem, which you just heard about in the

Brouwer Lecture. It dates from 1976, and it represented, at that time, a methodological breakthrough. It used, for the first time, techniques from algebraic geometry to solve an important problem in algebraic number theory. Suddenly all algebraic number theorists had to learn algebraic geometry. The paper has been enormously influential.

Ken's second achievement I want to mention is the epsilon conjecture, which he proved in 1986, and which is now called 'Ribet's level lowering theorem'. I will not attempt to explain what it says, but it played a key role in the proof of Fermat's Last Theorem, and did later develop into a standard tool for solving exponential diophantine equations. When you arrange the proof of Fermat's Last Theorem 'in its natural order', then Ken's result is the last one that you apply. So some commentator remarked that it was really Ken Ribet who

completed the proof of Fermat's Last Theorem, and not Andrew Wiles.

I like to mention a third achievement of Ken Ribet, not because it played a role in the committee's deliberations, but because, when I was Ken's colleague in Berkeley, I witnessed how it came about, and it gives you some insight into how Ken operates. (You may know that one mathematician in Berkeley got famous by doing his mathematics 'on the beaches of Rio', but that was not Ken.) One day, Ken found that he needed a certain statement about group representations, and he decided to ask one of our postdocs, who was a specialist in group theory. Now you should know that this postdoc had the habit of thanking God in his papers for leading him to the proofs of his theorems. I always felt that this was a rather frivolous thing to do, since I don't believe that God is a specialist in proofs; after all, He knows already what is true and what is not true, and He doesn't *need* proofs. And indeed, when the postdoc claimed he had solved Ken's problem, and gave a seminar lecture about it, it turned out that his solution was full of mistakes. After the lecture, we had a brief discussion about the problem, and Ken went back into his office. He started playing a computer game, I believe it is called 'Tetris'. It is a game in which little blocks fall down, and in my office, a few doors down the hall, I could almost hear them falling. After a while, Ken emerged from his office, and to my surprise he showed me the solution to his problem! It gave rise to a nice little paper, which has the peculiar property that its first half is written in French and the second half in English.

I trust you will agree that someone who beats God just by playing Tetris deserves nothing less than the Brouwer Medal. ☞

Gunther Cornelissen

Mathematical Institute
Utrecht University
g.cornelissen@uu.nl

Jan van Neerven

Delft Institute of Applied Mathematics
Delft University of Technology
j.m.a.m.vanneerven@tudelft.nl

Interview Kenneth Ribet, winner Brouwer Medal 2017

“No one had ever accused me of proving a theorem before”

On April 12th, 2017, Gunther Cornelissen and Jan van Neerven interviewed Ken Ribet at the occasion of him winning the Brouwer Medal 2017.

Professor Ribet, congratulations on winning the Brouwer Medal! We would like to ask you some questions about your scientific career and endeavours.

High school: the ‘maximum learning programme’

How was your high school education? You went to the same high school as Feynman (and Madoff, for that matter): the no-longer-existing Far Rockaway High School.

“I grew up in a part of New York City that is pretty far away from the centre. Students in New York City who were very oriented towards mathematics or science tended to apply to specialised high schools, like the Bronx High School of Science, Stuyvesant High School, or Brooklyn Tech. I didn’t want to spend hours every day on the bus or the subway, so there was one local high school, and that was my high school.

At that time, the educational system had not yet developed this idea that lots of resources should be spent on bringing

everyone up to the same level, but instead, they would identify specially talented students and put them in exceptionally strong

classes. I was in a programme that, believe it or not, was called the ‘maximum learning programme’. The students in this programme went from class to class together (this was called ‘block programming’), we got to know each other very well and we had among the best teachers in the high school, so I had a very good preparation in mathematics, science, English and social studies. Foreign languages were not block programmed because some people took French and some people took Spanish, but all of the core courses were block programmed.”

Then was it already clear before you entered high school that you had a ‘science-talent’?

“Well, the New York school system identified me as a ‘smart person’, but some of the students with me in the programme were talented in English, social studies or history. It was not focussed specifically on science.”

How was the mathematics education?

“It was great. First of all, I learnt a lot from the teachers, but we also had a math



Photo: Gil CavalCanti

Ken Ribet at the NMC 2017, holding the Brouwer Medal

team and I learnt a lot from the other students. There is one fellow who went on to do research mathematics, another became a specialist in mathematical problems and he published many books about that. We were always pushing each other to learn clever techniques to solve geometry and algebra problems. I learnt a little bit of calculus from these other students even before I had my first calculus course.”

Did you also take part in competitions, such as Math Olympiads?

“Math competitions weren’t so well organized in those days, but we did a few, and I was OK. I was not a big star but I would sometimes get an honourable mention.”

It is quite surprising that these kind of special schools already existed in those days. Nowadays it is rather common to offer special programmes to talented students. “My high school had something like 3000–4000 students, and this programme was just for a very small number, something like 50 students per year.”

What were the typical topics and what was the level?

“Just the standard high school topics, but during the summer of 1964, before my last year in high school I was in a summer

programme for science students at Brown University, which is actually the university I ended up attending and I was attracted to the university because I enjoyed that summer so much. We had three courses. One in computer programming where I learnt how to write programmes in original Fortran (typed into punch cards); another in calculus that was taught by an engineering professor, who had absolutely no interest in limit arguments and mathematical subtleties, but he taught us how to compute and it was great! That’s how you should learn calculus at first, through calculations, and I really liked that. Then there was a third course in material science—which coincidentally is the specialty of my older daughter—but in that course, I learnt absolutely nothing.

There was another thing that was somewhat special. We had a kind of ‘math talent class’, an additional math class, when I was in my last year of high school, where we did a lot of problems from a book from around 1891 called ‘Higher Algebra’ by Hall and Knight.¹ It was just full of tricky problems from the competitions in Cambridge University and I learnt a lot of strange mathematics; algebraic manipulations, discrete mathematics, all sorts of topics.”

In hindsight, has this benefited you?

“Oh, I am sure. I got very excited about math, and by the summer after I left high school, I really understood about epsilons and deltas for the first time, I found it really great. So I was full of enthusiasm and ready for university.

Godement used to say that in France, the students in the Lycée were just stuffed full of information and by the time they got to university, they knew quite a lot but they were very tired. In the USA, students learn much less, but when they get to college, they are really ready to learn. I think that was true for me. I was very excited about going to university, I was 17 years old and I was in great anticipation of what I would learn there from these professors, whom I considered to be humungous figures.”

But you enrolled in chemistry.

“That is not exactly correct. What happened is that I had a very strong high school chemistry teacher. When I was graduating from high school I thought: ‘You know, this chemistry is really great; may-

be I will major in chemistry.’ And over the summer, when I learnt about epsilons and deltas, I completely changed my mind and decided that mathematics was going to be my subject. In fact, by the time I got to university, I decided to abandon chemistry completely.”

Your story on epsilons and deltas is quite interesting. What is your opinion on the big calculus books that nowadays precede a decent class in analysis?

“I think the American system is fairly reasonable, that students learn calculus and then they take a separate course in real analysis and they learn what really goes on in calculus. The reason the books are so thick is simply that the publishers want to be able to sell to the largest number of universities and each university has some necessary conditions that have to be satisfied by a calculus book, so it tries to satisfy all of them. So you get these big books, it is a big juggernaut, with supplementary material, online homework, guide for the instructor, guide for the student, solution manual. All of this has to be prepared, so the whole thing is a very big project.”

Undergraduate years at Brown University: interacting with Ireland and Rosen

Then you went to Brown University. How was that?

“Oh, I loved it. Brown—where my younger daughter is a student now—is the same now as it was back then: there is lots of research, but there is a big focus on the undergraduates; on giving them lots of attention and lots of time and opportunities to learn different things. The professors in the Brown Math Department liked me and were willing to spend lots of time with me. The first course I took was a year-long course in linear algebra and multivariable calculus, but it was an honours course, so the linear algebra was abstract linear algebra, which I learnt for the first time and which I thought was absolutely beautiful.

I also liked multivariable calculus. We had a book called *Modern Multidimensional Calculus* by Monroe² and I never exactly knew what was going on, but I liked the fact that there was actually a formal definition of what a differential was, as a linear form on a tangent space. The book was full

Short biography of Kenneth A. Ribet

Kenneth Alan Ribet was born on 28 June 1948 and grew up in New York, where he attended a selective programme at Far Rockaway High School, before entering Brown University to study mathematics. He received his PhD from Harvard, directed by John Tate, in 1973. After some postdoc years at Princeton, he moved to Berkeley, where he has been a professor ever since.

He published about 60 papers and had around 25 graduate students, and was an editor of many journals and book series, including the acclaimed *Springer Graduate Texts* series.

He is a member of the U.S. National Academy of Science, and has received the Fermat Prize in 1989, and, this year, the Brouwer Medal of the Royal Dutch Mathematical Society. Since 2017, he serves as President of the American Mathematical Society.



Ken Ribet delivering the Brouwer lecture at NMC 2017

Photo: GIL Cavallanti

of Greek letters and the idea was that by thinking abstractly, you would gain more information. But I am not sure that really worked."

Does the interest of Brown faculty on undergraduates mean more individual tutoring, or group tutorials?

"It just means more availability and less rushing to the next seminar or conference."

What was your first encounter with number theory?

"In my second year I took my first abstract algebra course, which I also loved. By chance, just by walking in the math department, in the mail room I met a professor who started interrogating me. 'What are you studying, what are you doing, what did you just learn?' I said I was in this abstract algebra course, so he asked: 'What is an example of a cyclic Galois group?' So I said, you take an extension of finite fields, but he said: 'No, no, I want number fields, characteristic zero.' I think I might have come up with an example in-

volving cyclotomic fields. This was my first encounter with Kenneth Ireland. He turned to me and said 'Read this' and handed me André Weil's paper on number of solutions of equations over finite fields,³ which was basically where he made the Weil conjectures. Except he was unwilling to say it in print, because he was worried that he might be wrong. He wrote this article and went around lecturing about it, and in public, orally, he would explain what he really had in mind, but not in the article. The article is completely explicit, calculating numbers, using Gauss sums and Jacobi sums. The article expresses each idea in several different ways. I could follow it all line by line. It seemed pretty interesting and I liked the fact that this Brown professor was interested in me. Then he gave me another paper, the sequel, called 'Jacobi sums as Größencharaktere' by Weil.⁴ I read it and sort of understood it. But then there was all this number theory, and I took a course in number theory and that got me interested in arithmetic."

So you are not like Andrew Wiles, who in the famous BBC-documentary⁵ states that even as little kid he already came across the Fermat Conjecture and he wanted to solve that.

"I was not motivated by and had absolutely no ambition to solve a great problem or to be a great mathematician, but my ambition, locally, was to be like the professors that I had in math classes. I really liked them, I respected them, I thought they were doing something worthy. This was the time of the Vietnam war, where a lot of people that I knew in business, like my parents' friends, were doing things that were tangentially related to the war effort and they were seeking profit. And these people at university were more like monks, very serene and motivated by the love of knowledge. They seemed to me to be really people to emulate."

Was this in particular true for the mathematics professors, or was it more general?

"Well, I liked the academic atmosphere in general, but the math professors were the

ones that I saw and they were very much unlike the adults I saw when I grew up, who were in business. My first professor, Frank Moore Stewart, who taught me linear algebra and multivariable calculus, looked like some farmer, but he was in pursuit of knowledge and he had spent a great deal of time with one of the historically black colleges in the South. Brown University had a partnership with Tougaloo College in Mississippi, which I had never heard of before I went to Brown. There was an exchange program, where a few Brown students who go to Mississippi and a few Mississippi students would go to Brown, and some faculty members would go to the other university. This guy had spent some time teaching at Mississippi and he was deeply committed to equality and pacifism. I was very impressed and I had never met anyone like that before coming to university."

Graduate years at Harvard: interacting with Tate and Serre; the Antwerp conference

Then you went to Harvard.

"The two professors that mentored me, Michael Rosen and Kenneth Ireland,⁶ just told me what to do. 'This is your subject. You are going to study arithmetic geometry. Apply to these universities: Harvard, Princeton, Brandeis and Chicago.' So I applied to these four universities, and I guess they planned to write me very good letters of recommendation, and I got into all four. I reported back that I got these four envelopes back and they are offering me admission and they said to me: 'Go to Harvard and work with Tate', and that was it. So I said: 'OK.'"

I showed up at Harvard in September 1969 and I knocked on John Tate's door and I said: 'I am Ken Ribet, your new student.' He seemed rather taken aback by this, but he never said anything negative, he said: 'OK.'"

Had you already done your qualifying exams?

"Oh, that was a real embarrassment. Namely, at the end of my first year at Harvard, there were written exams everyone had to take and this was at a time when the whole university was barely hanging together. There were people on strike, the USA was bombing Cambodia, people demonstrating in the streets and classes being closed down. There was a big anti-war effort and

anti-authority sentiment. The exams were two sessions of three hours each, and I came into the exams, dashed off answers on paper and left after half an hour; two times. It is clear that my answers were lacking in detail. Apparently, the Harvard faculty wanted to fail me, because grading by the strict criteria, I didn't have a passing score, but Tate intervened and said that this guy is really good and you can see from his answers that he knows what is going on, so we'll pass him.

I spent the next two years taking all kinds of courses, from Tate and John Coates. It seems there was an endless supply of visitors: Swinnerton-Dyer gave a course on modular forms, and Birch would come sometimes, and Serre must have been there, although I don't remember that. I learnt a lot. Finally, I came into Tate's office in my third year, and I asked when to start research; I had no idea how to do it. Tate said 'What are you doing?' and I said I was in this course, and this course, et cetera, and he said: 'Maybe you should go to fewer courses and work on this problem.' He gave me some problem that involved the Birch-Swinnerton-Dyer conjecture and elliptic curves with complex multiplication. I couldn't figure out what he had in mind, it just didn't make any sense to me. I came back to him and said that I didn't like this problem. You imagine most advisors are barely willing to give a student one problem, but Tate just gave me another problem. He and I were reading a paper of Serre on the Galois action on division points of elliptic curves. We had a seminar where we were working through the manuscript line by line and taking turns giving lectures. I understood the paper pretty well, so Tate said: 'Why don't you do certain abelian varieties?' (later called 'of GL_2 -type'), as an encore. I said that sounds like a good thing and I started working and learnt something by mimicking some arguments in Serre's book on Abelian ℓ -adic representations and elliptic curves.⁷ I thought I was doing a computation, and I came to Tate and told him what I had computed and he said: 'Well, that's a very nice theorem.' No one had ever accused me of proving a theorem before. It was a transformative moment when I actually had been told that I had done some research, because I had no idea what research was or how you would go about doing it, so it was very empowering.

He told me to continue on, and I went to the Antwerp conference in 1972 where I met Serre.⁸ I told Serre what I was working on and what I had done so far. But as you can see from the Serre-Tate correspondence, Serre already knew about me; Tate had written to him. 'This kid Ribet is coming to Antwerp; be nice to him, he is very shy.' When I met Serre he was standing on his head, demonstrating J. Frank Adams's method of drinking beer while standing on your head. He had a big crowd of admirers around him and I didn't know when I could possibly ask him about my thesis, so I decided to just interrupt him with: 'Excuse me, professor Serre, I want to ask you some questions about abelian varieties.' Everybody who was there started laughing. But Serre asked me who I was, and when he remembered who I was, he started talking to me. He told me how to continue my thesis, what to do, and how it would work out. I actually found this very depressing, I was working on something, working, working, working, and Serre, in thirty seconds could see the entire sweep of what I was doing and tell me what to do next — literally while standing on his head. It was in some sense very discouraging. What am I ever going to do in mathematics and will anybody care about me when there are these other people who can do the thing ten times better and thirty times faster."

Postdoc at Princeton, interacting with Katz and work with Deligne

"Nonetheless, I continued writing my thesis, handed it in, and graduated.⁹ During the year when I wrote my thesis, which was my fourth year at Harvard, I really had the impression that no one would ever care about what I was writing and that I would get a job in some really obscure university, not in a major centre. When I applied for jobs, I wrote to about sixty universities, hoping that one of them would pay some attention to me. It was really quite a shock that in January of the year I was writing my thesis, very early in the hiring cycle, I got a phone call from Princeton offering me a job. It was the craziest thing that ever happened to me. Like everybody who came to Princeton as a postdoc — at the time my title was 'Lecturer', the phrase 'Postdoc' was not used yet in mathematics — I was terrified that the senior faculty would find out that they hired someone who was

completely stupid. Everybody had that fear. I showed up and my mentor was Nick Katz, who was wonderful and very supportive. He asked me some question that I was able to answer during my first year, and this is how I got into this collaboration with Deligne about totally real fields.”

What was it like to work with Deligne?

“I did not really work with Deligne. Katz told me you had to prove the irreducibility of some moduli space in characteristic p and Katz had already found in his Antwerp article that this amounted to the surjectivity of some Galois representation, which in the case of elliptic curves was proved by looking at the image of some inertia group around supersingular points; a method that did not work for higher-dimensional abelian varieties. Katz just asked me a very narrow question about some Galois representation, where he translated all the difficulties into one place where I was supposed to be knowledgeable, and asked: ‘How do you prove it has a big image?’ I said, the way we usually do this is using Frobenius elements, and I made some argument using Honda-Tate theory showing that the Frobenius elements fill the thing up, so I solved the problem and did it literally overnight. Katz said ‘Holy cow, this is the missing piece!’ and asked me to write to Deligne, who replied that now we could write a joint paper. He already had a manuscript, a letter to Serre, outlining what to do, but with this missing piece. Working with Deligne meant that I had to understand this manuscript. So I went to Paris and spent the first year there (1975–1976) at the IHES and mostly during that year I tried to understand the manuscript. I saw Deligne every day but I didn’t talk to him all that often, since I didn’t have all that much to say. My main contribution to that paper was the irreducibility in characteristic p , and then there was another point, which had to do with powers of 2. The idea was that the p -adic L -function was integral (a p -adic power series), except that when $p = 2$ and you look at the Eisenstein series, the constant term is an L -value divided by 2^n where n is the degree. It would be very natural to think that L -values for the 2-adic L -function were divisible by 2^n , but after appropriate symmetrisation, Deligne could prove in complete generality only that they were divisible by 2^{n-1} and had some general situations where he knew they were

divisible by 2^n and a whole class where he couldn’t decide. He did one calculation for one totally real quadratic field, where he saw it wasn’t divisible by 2^n (by 4 in that case) and he wondered what happened in general. I did a few more examples and gave a lecture about it at Orsay. Hendrik Lenstra immediately saw what the answer was supposed to be. Getting that hint from Lenstra, I worked and worked and worked and compared Eisenstein series and theta series and actually proved that the surmise of Lenstra was correct. So my second significant contribution to that joint paper had to do with powers of 2 in the 2-adic L -function. So I did two different things for that article.”

Antwerp again, and Grothendieck

The Antwerp conference was organised by Willem Kuyk, the mathematical great-grandfather of one of us, a Dutch mathematician that had gone to Belgium to found the mathematics department at Antwerp. On the web page of William Stein, we found an interesting conference picture¹⁰, in which you identified many participants and to which you contributed a little note about the alcohol consumption at that conference.

“There was wine served at lunch and dinner. I often sat with Bombieri who used the following ploy: as we sat down, we would pour out the first bottle; so we had an empty bottle and we got a second bottle,

and then that would get you started. There was also a lot of drinking in the evening after dinner, with beer and wine and ping-pong. The food and wine at that conference were just excellent.”

This gregariousness seems very much in line with the reputation of the algebra group at Antwerp.

“At the time I was still a graduate student. What I also remember from the conference was that after every talk, students would gather around Nick Katz in front of the building. He would explain to them what the lecture was really about. The most elementary lectures I would understand but the more advanced things required some help. Listening to Katz was just great.”

Was this the conference where Grothendieck refused to attend because of the conference being funded by NATO?

“Somehow I managed to miss the first day of the conference by mis-timing some trains. I came to Europe a week or two before the conference and travelled with some friends, and the morning the conference began I was in Switzerland.

At the first day proceedings, Grothendieck was making a big stink, protesting and interrupting. The second day, when I came, Grothendieck was sitting in front of the building where the lectures were held, with a huge bouquet of helium filled balloons. I knew who Grothendieck was because he came to Harvard when I was



Conference photo from the Antwerp conference, 1972

a graduate student, but I don't think he recognised me. So the only direct conversation I ever had with Grothendieck was that I went up to him and asked him: 'Excuse me, why are you sitting here with balloons?' He looked at me and said: 'Because they are nice.' That was the only sentence he ever spoke directly to me.

No, I take it back. He spoke other sentences to me, because when I was at Harvard, he was already on his 'Survival' kick. When visiting universities, he would lecture in mathematics only if he was allowed to give a general lecture about the evils of doing mathematics. I went to both his algebraic geometry lecture, which was on the definition of étale cohomology, and in the evening to his public lecture, as did all math graduate students, and he was going on that we should go till the soil and not waste our time doing mathematics. I asked: 'Excuse me, I have spent three years now learning higher mathematics, including arithmetical algebraic geometry. I think I am pretty good at it and that I would be able to make a contribution, whereas if I go and till the soil as a gardener, I won't be any better than any other person, probably a lot worse. What do you say to that?' He gave an answer, but speaking to the public. I don't think his answer was all that satisfactory."

Reaching out to young people

The NAW would like to reach more young people. As President of the AMS, which suggestions do you have?

"The new editor of the *Notices of the AMS*, Frank Morgan, has devoted a tremendous amount of energy to the journal. He has worked to make the articles shorter and more visually appealing. In particular, articles tend to have short bibliographies — or none at all. He has worked to move routine material out of the *Notices* on the grounds that it can be found easily online. Frank has edited many of the submissions quite heavily; the practice of editing submissions is common in the literary world but rare in the mathematical community.

When I was a student, graduate students would be members for free; graduate schools would nominate them. Then it was very natural to continue once they had a real job. The real benefit was that I would get my own copies of the *Notices*

and the *Bulletin*. I could take them home and read them. Nowadays the University is subscribed to these publications as institutional members. That means that when you are at the university, you can read all these publications on your laptop or tablet. A benefit of electronic copies is that you can do searches. Young people are less and less married to physical copies. You can decide not to be a member and still have the electronic versions available through the university. So basically the problem which the AMS is attempting to counter is the attitude that young people might have of 'what's in it for me?' When I was a young faculty member I joined the society because everyone did, it was the thing to do. When I came to Berkeley I also joined the Faculty Club. Once you pay dues to become a member of the club, you get a discount on your purchases. But many will say that it is not worth it. Mathematicians are very good at calculating the benefits!"

What are the main challenges that the AMS is facing?

"Many challenges have been identified in the strategic plan, but an obvious one is to make sure that its electronic products are still relevant in an age when Google does everything for free. For instance MathSciNet, the online review service for mathematical research papers, is constantly adding more capabilities. Certainly it is very important to the Society to make sure that MathSciNet stays ahead. People often don't realise everything the Society is offering, such as the remote access button in MathSciNet which is unknown to most users. We do regular surveys among our members who then request all sorts of features that we already have."

You have said elsewhere that the importance of printed journals is declining.

"Fields Medallist Timothy Gowers will tell you that the future of publishing in journals is overlay journals: you publish on arXiv and all the journal does is to anoint certain of these articles. That's it, very little work needs to be done. An argument can be made that commercial publishers, including one in this country, are exploiting the mathematical community by extracting a huge profit from a product that is basically powered by free labour from the mathematical community. Overlay journals are one extreme, commercial publishers

Three theorems of Ken Ribet

A central role in Ribet's work is played by so-called 'Galois representations', a way to look at extensions of number fields through the eyes of representation theorists, connecting them to algebraic geometry through automorphic forms and Shimura varieties.

Ribet rose to fame when he published what is now known as the 'Herbrand–Ribet' theorem¹¹, a result on class groups of cyclotomic fields that was spectacular not just as a statement, but also from the point of view of the *methods* that he used; a whole new generation of number theorists copied successfully his algebro-geometric ideas to solve purely number theoretical problems, and the paper made a lasting impact on the field of Iwasawa theory.

Ribet proved the ε -conjecture¹², effectively implying that, through a method of Frey, proving the Taniyama–Shimura conjecture would solve Fermat's Last Theorem (which Andrew Wiles subsequently did).

In a famous work with Deligne¹³, he showed congruences between special values of L -series of real quadratic fields (known to be rational by work of Siegel), implying the existence of p -adic L -functions, which seemed very inaccessible at that time. Again, the method of Deligne and Ribet changed the landscape on how to approach such questions: suddenly, analytic statements were approached through modern algebraic geometry and a very detailed study of moduli spaces.

the other, and many people think that the Societies are a good compromise: they are non-profit organisations and they are really serving the mathematical community. The AMS has a Gold Open Access version of its Transactions and Proceedings journals and charges \$2000 per article. That is what it actually costs to take an article and process it. There are all sorts of arguments as to whether or not these are real costs. The AMS makes money on some of its publishing activities, but this money is turned back to the mathematical community through the many services that the AMS provides to the profession. At the end of every year the balance should be even."

New developments in number theory

Let's talk about recent developments in the field. Is there something that gets you really excited? If you would have two years to study only something mathematical, what would it be?

"Well, it would clearly be perfectoid spaces."¹⁴

I actually wrote that down as next subject! Two of our Utrecht students attended the Arizona Winter School about that, I guess you were not there?

"No, but their inventor Peter Scholze was in Berkeley for a semester fairly recently and he gave a course. I have tried to follow the beginning of the course and I was just completely blown away by (1) the beauty of the subject and (2) the amazing command of an entire landscape that he has. He was lecturing to many people who were experts in different corners, like (ϕ, Γ) -modules and different ways of expressing Galois representations in somewhat concrete terms and Scholze understands all of this in his new framework in some illuminating way that completely surprised the original perpetrators of the subject, who were sitting in the audience shaking their heads. Obviously, as you see from the joint work of Scholze and Jared Weinstein,¹⁵ when you take modular curves and you add lots of p -power level, in the end you are dealing with a perfectoid space, and these recent developments where you associate Galois representations to $\text{mod-}p$

cohomology classes are just mind-blowing. Certainly, if I were starting out and could sit for two years and think about nothing but learning a new subject, that would have to be it."

Then being president of the AMS is not the best strategy, is it? Do you still have time for research?

"You know, I have done lots of different things in my life and the AMS is very interesting, learning about the society and anticipating in its activities and this is some way in which I grow, even if it is not learning perfectoid spaces. One of the things with being president is that I teach only half as much, and even when I am teaching and I have to go away for an AMS activity, a graduate student is there ready to replace me; this is part of the agreement between my university and the AMS."

Chances are that you will meet the President of the United States?

"Every year there is a ceremony for the National Medals of Science. Presumably I get invited if a mathematician wins. If I would find myself in a room with Donald Trump, I would try to have an affable conversation without much substance. I would tell him that I admire his Twitter style and would ask him if he is having a good time. I probably wouldn't have more than three minutes to talk to him!"

Professor Ribet, thank you very much for the interview!

During the interview, we asked Ken Ribet to describe how the AMS reaches out to young people (a continuing point of interest, also for KWG and NAW), and this is the answer that the executive director of the AMS, Dr. Catherine Roberts, later provided by email:

"There are many ways that the American Mathematical Society supports young people interested in Mathematics. Frank Morgan has devoted a tremendous amount of energy in transforming the *Notices of the AMS*. I think his attention to short, interesting articles with lots of illustrations and his addition of 'Lecture Samplers' and the 'Graduate Student Section' make this publication, freely available online, more interesting and accessible to students. Our members have established the Epsilon Fund, which supports many math programs and summer math camps for high school students. We provide travel funds to students interested in attending our conferences. Last year, at the Joint Mathematical Meeting, we ran Mathemati-Con jointly with the Mathematical Association of America. This event was free and open to families and celebrated mathematics with engaging presentations as well as the national finals of our popular quiz program, *Who Wants to be a Mathematician?* These are just a few of the programs I can think of that might be of interest to young people, and I encourage those interested in mathematics to explore our website at www.ams.org."

Notes and references

- 1 H.S. Hall and S.R. Knight, *Higher Algebra 1887*, Macmillan and Co. (Free copy easily found online.)
- 2 M. Monroe, *Modern Multidimensional Calculus*, Wiley, 1963.
- 3 A. Weil, Numbers of solutions of equations in finite fields, *Bull. A. M. S.* 55(5) (1949), 497–508.
- 4 A. Weil, Jacobi sums as 'Größencharaktere', *Trans. A. M. S.* 3 (1952), 487–495.
- 5 *Fermat's Last Theorem*, BBC Horizon Documentary by Simon Singh, 1995–1996; also a book by Simon Singh first published by Fourth Estate.
- 6 Known, amongst others, for their book *A Classical Introduction to Modern Number Theory*, Springer GTM 84.
- 7 J.-P. Serre, Abelian L -adic representations and elliptic curves, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W.A. Benjamin, 1968.
- 8 Modular functions of one variable. I–IV, *Proceedings of the International Summer School, University of Antwerp, RUCA, July 17–August 3, 1972*, edited by Willem Kuyk, Lecture Notes in Mathematics, Vol. 320, 349, 350, 476, Springer, 1973–1975.
- 9 K.A. Ribet, *Galois Action on Division-points of Abelian Varieties with Many Real Multiplications*, PhD thesis, Harvard, 1973.
- 10 http://wstein.org/antwerp_photo.
- 11 K.A. Ribet, A modular construction of unramified p -extensions of $\mathbf{Q}(\mu_p)$, *Invent. Math.* 34(3) (1976), 151–162.
- 12 K.A. Ribet, On modular representations of $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, *Invent. Math.* 100(2) (1990), 431–476.
- 13 P. Deligne, Pierre and K.A. Ribet, Values of abelian L -functions at negative integers over totally real fields, *Invent. Math.* 59(3) (1980), 227–286.
- 14 Introduced by Peter Scholze. See, for example: B. Bhatt, What is... a perfectoid space? *Notices of the A. M. S.* 61(9) (2014), 1082–1084.
- 15 P. Scholze and J. Weinstein, Moduli of p -divisible groups, *Cambridge J. Math.* 1(2) (2013), 145–237.

Jaap Korevaar

Korteweg de Vries Instituut voor Wiskunde
Universiteit van Amsterdam
j.korevaar@uva.nl

Evenement Voordracht op NMC 2017 ter ere van 75-jarig lidmaatschap KWG

Wie en wat mij geholpen heeft om wiskundige te worden

Tijdens het Nederlands Mathematisch Congres van 11 en 12 april is op speciale manier gevierd dat Jaap Korevaar en Fred van der Blij dit jaar precies 75 jaar lid zijn van het Wiskundig Genootschap. Jaap Korevaar is uitgenodigd terug te kijken op zijn lange carrière. Fred van der Blij, wiens gezondheid het niet toeliet aanwezig te zijn op het NMC, is thuis in het zonnetje gezet door het KWG.

Cornelis Visser (1910–2001)

Ik begin met Visser, die in de tweede tot en met de vierde klas (1936–39) mijn wiskundeleraar was op de hbs in Dordrecht. Hij was gepromoveerd bij Julius Wolff (1882–1945) in Utrecht en kwam in 1936 terug van een vruchtbaar postdocjaar aan Harvard en Princeton (vergelijk Kortram [34]). Ik was een lastige leerling, vroeg bij alles: “Waarom?” Maar dat vond hij niet erg en na een stroef begin ging het heel goed. Het is door Visser dat ik wiskunde ben gaan studeren. Maar waarom wil je naar Leiden en niet naar Utrecht, vroeg hij. Wel, zei ik, Leiden

is toch de oudste en beste universiteit van Nederland? Nou ja, zei Visser, ze hebben daar in elk geval Kloosterman, en die is wel goed! (Kloosterman zou vooral bekend worden door zijn artikelen [17] in de *Annals of Mathematics* van 1946. Zie ook de Bruijn [3].) Visser zou na de oorlog hoogleraar worden in Delft, en daarna in Leiden.

H.D. Kloosterman (1900–1968)

Ik ging dus in september 1940 naar Leiden, waar ik meteen bevriend werd met Fred van der Blij en met natuurkundestudent Hans Tolhoek. We genoten van het colle-

ge differentiaal- en integraalrekening van lector Kloosterman, dat na Kerstmis over moest gaan in exacte analyse. Eigenwijs als Fred en ik waren gingen we ook naar zijn caputcollege getaltheorie voor ouderejaars, dat we redelijk goed konden volgen. Kloosterman was een buitengewoon heldere docent. Geen woord te weinig, naar ook niks te veel. Hij begon zijn college altijd links boven op het bord te schrijven en eindigde na een uur keurig rechts beneden. Hij had ook een heel speciaal gevoel voor humor. Je kon de collegezaal voor of achter binnenkomen. Op de eerste dag deed Kloosterman, die altijd aan de voorkant binnenkwam, demonstratief de achterste deur dicht, met de woorden: “Ik doe deze deur één keer per jaar dicht; in het vervolg doet de *laatste* student die binnenkomt hem dicht.”



Cornelis Visser



Fred van der Blij



H.D. Kloosterman

Maar de universiteit werd op last van de Duitse bezetter *gesloten*, na het protest tegen het ontslag van de Joodse hoogleraren en de rede van Cleveringa op 26 november 1940. Leiden zou in de oorlog niet meer open gaan. (De oude meetkundige Prof. W. van der Woude (1876–1974) speelde daarbij een belangrijke rol. Hij werd Rector en gaf eind 1941 niet toe aan de eisen van de bezetter voor heropening.)

Studenten konden thuis studeren uit dictaten van ouderejaars, en (althans tot eind 1941) tentamen doen bij docenten aan huis. Ik begon ijverig te studeren uit het dictaat van Kloostermans tweejarige college analyse dat ik netjes overschreef. Fred van der Blij en ik kochten daarnaast enkele boeken: Pólya en Szegő's *Aufgaben und Lehrsätze aus der Analysis*, en de mooie kleine boekjes van Knopp over functietheorie uit de *Sammlung Götschen*. Ik bestudeerde verder het boek van Knopp, *Unendliche Reihen*, dat ik tweedehands had kunnen kopen. In 1941 en ook daarna kwam ik geregeld bij Visser thuis. Hij informeerde dan hoe het met de studie ging, en hij leende mij het boek van Schuh over 'Het getalbegrip'.

Tauberstellingen

In Kloostermans dictaat werd al gauw de continuïteitsstelling van Abel bewezen: Als een reeks $\sum a_n$ convergeert, met som A , dan zal de somfunctie van de machtreeks

$$f(x) = \sum a_n x^n, \quad 0 \leq x < 1,$$

limiet A hebben voor $x \nearrow 1$. Maar kun je dat ook omkeren? Niet zonder meer, denk aan de reeks $1 - 1 + 1 - 1 + \dots$ en

$$1 - x + x^2 - x^3 + \dots = \frac{1}{1+x}.$$

Je hebt een extra voorwaarde nodig voor een omkering van Abels stelling. In 1897 bewees de Oostenrijkse wiskundige Arnold Tauber (1866–1942) dat de nevenvoorwaarde $na_n \rightarrow 0$ voldoende is voor convergentie $\sum a_n = A$, zie [46]. (Na zijn habilitatie werkte Tauber als verzekeringswiskundige. In 1900 werd hij hoogleraar, eerst aan de Technische Hogeschool in Wenen, later aan de Universiteit. Helaas zou hij (net als Wolff) omkomen in een concentratiekamp.) In Kloostermans dictaat stond vervolgens dat de zwakkere nevenvoorwaarde ' na_n begrensd' voldoende is voor omkering van Abels stelling. Dat was in 1911 bewezen door J.E. Littlewood (1885–1977), zie



J.E. Littlewood

[35]. Het was een vermoeden geweest van G.H. Hardy (1877–1947) en werd het begin van een lange en ongewoon vruchtbare samenwerking. Hardy en Littlewood introduceerden de naam Tauberstellingen en zouden er samen heel veel bewijzen, zie bijvoorbeeld [11,12] en hun stelling over Lambertreeksen verderop in dit artikel. Hun bewijzen met herhaalde differentiatie waren wel erg ingewikkeld. Voor het geval van machtreeksen zou J. Karamata (1902–1967) in 1930 een veel eenvoudiger bewijs geven [15], dat gebruik maakte van uniforme approximatie met veeltermen.

In 1941 vroeg ik aan Visser hoe je Tauberstellingen kon bewijzen. Hij wist blijkbaar veel over zulke stellingen en stelde voor dat ik kon proberen om een makkelijkere omkeerstelling te bewijzen. Wanneer $\sum a_n$ convergeert met som A , dan hebben de gemiddelden van de partiële sommen s_k , namelijk

$$\frac{s_0 + s_1 + s_2 + \dots + s_{n-1}}{n},$$

ook limiet A als $n \rightarrow \infty$. Probeer te bewijzen dat *hier* de nevenvoorwaarde ' na_n begrensd' voldoende is voor omkering. Dat kon ik; het bleek later een stelling te zijn van Hardy [10] uit 1910. (Nog later zou ik er achter komen dat Kloosterman in 1940 [16] een heel mooi bewijs had gegeven voor Hardy's stelling, met behulp van een discrete Taylor-formule.)

Bij een later bezoek vertelde Visser dat hij bezig was met een nieuwe aanpak van Wieners algemene Taubertheorie [49] uit 1932.

WG, collectie Blumenthal

In Januari 1942 mochten de Leidse studenten elders verder studeren. Fred van der Blij en ik (en Hans Tolhoek) gingen naar Utrecht, waar ik eind 1942 kandidaatsexamen deed. (Fred had dat eind 1941 nog net in Leiden kunnen doen.) We werden lid van het Wiskundig Genootschap en genoten van de *Wiskundige Opgaven* die het Genootschap publiceerde. We wedijverden met elkaar wie de meeste kon oplossen. In die tijd werd ik ook bevriend met een andere trouwe oplosser, de iets oudere N.G. (Dick) de Bruijn (1918–2012). Goede oplossingen konden gepubliceerd worden in het tijdschrift *Wiskundige Opgaven met de Oplossingen*. De verdienstelijke redacteur was prof. H. Bremekamp (1880–1963) in Delft; vergelijk ook Timman [47]. In 1943 volgde ik Dick de Bruijn als assistent aan de TH Delft; na zijn promotie ging Dick naar het Philips NatLab. In Delft kwam ik er achter dat prof. Bremekamp 'verre familie' was: zijn vrouw was een nicht van mijn opa Wepster, die over Bremekamp sprak als 'mijn neef Henkie'.

In Delft maakte ik kennis met de belangrijke collectie overdrukken van Otto Blumenthal (1876–1944), die lang Hilberts medewerker was geweest bij de *Mathematische Annalen*. Blumenthal was kort voor de oorlog naar Nederland uitgeweken, met zijn uitgebreide bibliotheek; hij had onder andere contact met prof. Jan Burgers in Delft. (Maar hij zou helaas toch omkomen in een concentratiekamp.)

In de 'collectie Blumenthal' heb ik Bochners vereenvoudigde behandeling van Wienertheorie gevonden [2]. Daar heb ik ook kennis gemaakt met de representatiestellingen van F. Riesz (1880–1956) voor continue lineaire functionalen, vergelijk [42]. Ik begon toen naarstig te zoeken naar een elementair bewijs voor de priemgetalstelling. Zoals bekend zegt die dat het aantal priemgetallen

$$2, 3, 5, 7, 11, 13, 17, 19, \dots \leq x$$

vergelijkbaar is met $x/\log x$. (Voor een afleiding zie verderop.) Ik gebruikte het werk van Riesz om elementair Tauberstellingen te bewijzen voor Lambertreeksen. Zoals ik al eerder schreef hadden Hardy en Littlewood een belangrijke Tauberstelling bewezen voor Lambertreeksen. Om zulke reeksen te vergelijken met machtreeksen vervangt men x (met $0 < x < 1$) en $x \nearrow 1$ door e^{-t} (met $\infty > t > 0$) en $t \searrow 0$. Dan schrijft

men de Lambertreeks als

$$F(t) = \sum a_n \frac{nt}{e^{nt} - 1}.$$

Hardy en Littlewood [13] hadden in 1921 bewezen dat uit $F(t) \setminus A$ en ‘ na_n begrensd’ volgt dat $\sum a_n = A$. Voor hun bewijs hadden zij echter de priemgetalstelling nodig (of zelfs een klein beetje meer). Deze onbevredigende situatie zou mede aanleiding zijn voor Norbert Wiener (1894–1964) om zijn algemene Taubertheorie [49] te ontwikkelen voor Fourierintegralen. Mijn eenvoudigere Tauberstellingen waren jammer genoeg niet sterk genoeg voor een bewijs van de priemgetalstelling! (Veel later zou ik verschillende bewijzen geven, zie bijvoorbeeld [29] (gebaseerd op Newman [40]) en mijn boek [30].) De TH Delft sloot in de lente van 1944 en nu liepen studenten en assistenten het risico opgepakt te worden voor ‘Arbeitseinsatz’ in Duitsland. Toen ik uit Delft thuis kwam stond er al gauw politie voor de deur. Gelukkig had mijn vader een tip gekregen en was ik ondergedoken. Na de zomer kon ik terug naar huis, maar ook daar moest ik mij verborgen houden.

Mijn eerste artikel

Mijn eerste artikel [18] was gebaseerd op een voetnoot in het boek van G. Doetsch over de Laplace-transformatie [6]. Ik heb dat eind 1943 geschreven aan de keukentafel, toen nog de enige warme plek in huis. Het verscheen in het Nederlands, want je mocht niet in een vreemde taal publiceren (behalve Duits).

In functietheorie, of complexe analyse, zijn de belangrijke functies de analytische. Zo’n functie $f(z)$ van de complexe veranderlijke $z = x + iy$ wordt lokaal gegeven door een convergente machtreeks

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n, \quad |z - z_0| < R.$$

Bijvoorbeeld

$$\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n, \quad |z| < 1.$$

Er ligt *altijd* een singulier punt op de convergentiecircel, de grootste cirkel om z_0 waarbinnen de machtreeks convergeert. Dat is een punt z_1 zo dat $f(z)$ op geen enkele omgeving analytisch is. Als $f(z)$ analytisch is in het hele vlak spreekt men van een *gehele functie*.

Sommige belangrijke analytische functies kunnen gegeven worden door een Dirichlet reeks,

$$g(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}, \quad s = \sigma + i\tau, \quad \sigma > \alpha.$$

De eenvoudigste en belangrijkste Dirichletreeks

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots, \quad \sigma > 1,$$

definieert de Riemann-zetafunctie $\zeta(s)$ in het halfvlak $\sigma > 1$. De som van de reeks kan analytisch voortgezet worden tot het hele complexe vlak, met uitzondering van het singuliere punt $s = 1$, waar de functie zich gedraagt als $1/(s-1)$. Er kan dus een singulier punt liggen op de rand van het convergentiegebied, maar dat *hoeft niet*, zie

$$\begin{aligned} \eta(s) &= 1 - 2^{-s} + 3^{-s} - \dots, \quad \sigma > 0 \\ &= (1 - 2^{1-s})(1 + 2^{-s} + 3^{-s} + \dots) \\ &= (1 - 2^{1-s})\zeta(s). \end{aligned}$$

(De singulariteit van $\zeta(s)$ wordt opgeheven door de factor $1 - 2^{1-s}$.) Hierin verschilt een Dirichletreeks van een machtreeks. Doetsch had geschreven dat er over het analoge verschijnsel voor de nauw verwante Laplace-integralen nog niet gepubliceerd was.

De functie $\eta(s)$ is een gehele functie. Mijn eerste artikel [18] ging over gehele functies die voorgesteld kunnen worden door een niet overal convergente Laplace-integraal. Of in Mellin-vorm:

$$g(s) = \int_1^{\infty} f(x)x^{-s-1}dx.$$

De reeks voor $\zeta(s)$ kan uitgedrukt worden door een Mellin-integraal met de ‘entier-functie’ $[x]$:

$$\begin{aligned} \zeta(s) &= \int_1^{\infty} x^{-s} d[x] = - \int_1^{\infty} [x] dx^{-s} \\ &= s \int_1^{\infty} [x] x^{-s-1} dx. \end{aligned}$$

Voor Mellin-integralen $g(s)$ bewees ik:

Stelling 1. *Zij $f(x)$ begrensd voor $x \geq 1$, periodiek met periode 1 en met gemiddelde 0 over een periode. Dan kan $g(s)$ voortgezet worden tot een gehele functie.*

Het bewijs gaat stap voor stap met herhaalde partiële integratie, waarbij men elke keer een primitieve gebruikt met gemiddelde 0. Toegepast op $f(x) = [x] - x + \frac{1}{2}$ construeert men zo de analytische voortzetting van de zetafunctie. Vergelijk ook het leuke

boekje van Roland van der Veen en mijn Amsterdamse collega Jan van de Craats [48].

Mathematisch Centrum, dissertatie

In 1947 werden Fred van der Blij en ik wetenschappelijk medewerkers aan het pas opgerichte Mathematisch Centrum, in de praktijk manusjes-van-alles. Behalve onderzoek doen en avondcursussen geven moesten we onder andere helpen om de bibliotheek op te zetten. Onder de binnenkomende literatuur vond ik in 1948 een interessant boekje van Obrechhoff [41] in de Actualités Scientifiques et Industrielles. Dat behandelde oude resultaten van Laguerre en nieuwere van Pólya (1887–1985) over benadering van gehele functies door polynomen, waarvan de nulpunten reëel zijn of in een hoek liggen met opening $< \pi$. Obrechhoff zelf bewees een vermoeden van Pólya voor het geval de nulpunten in een halfvlak liggen. Ik vroeg algemener wat men kan zeggen als de nulpunten van de benaderende polynomen in een willekeurige onbegrensde verzameling R liggen. Noem zulke polynomen R -polynomen en de limieten R -functies. Mijn algemene stellingen zouden in 1949 het beste deel van mijn dissertatie [20] vormen, vergelijk [21]. Van essentieel belang bleken de richtingen waarin R en zijn machten $R^k = \{z^k, z \in R\}$ naar oneindig gaan. Noem R regulier als die asymptotische richtingen voor geen enkele $k = 1, 2, \dots$ in een halfvlak liggen. Voor reguliere R zijn *alle* gehele functies met nulpunten in R approximeerbaar. Voor



G. Pólya

niet-reguliere R kijkt men naar de eerste R^k waarvoor de asymptotische richtingen in een halfvlak liggen, enzovoort. Vergelijk ook [23].

Dit soort werk zou uiteindelijk ook leiden tot een artikel over approximatie op begrensde, enkelvoudig samenhangende, gebieden G door polynomen waarvan de nulpunten op de rand liggen. Alle analytische functies op G bleken zo benaderbaar, zie mijn *Annals*-artikel [26].

Fred was al in 1947 gepromoveerd. Hij verliet het Mathematisch Centrum in 1948, was een poosje leraar en werd in 1953 medewerker aan de Universiteit Utrecht. Hij werd daar in 1955 hoogleraar en zou later ook enige jaren rector zijn.

Contacten met Paul Erdős

Het meest heb ik wel geleerd van contacten met Paul Erdős (1913–1996), te beginnen aan het Mathematisch Centrum in 1948. Daar sprak hij over zijn elementaire bewijs van de priemgetalstelling [7] (ten dele gevonden samen met Atle Selberg [45]). Elementair betekent hier: zonder gebruik van complexe analyse en de zeta-functie. Zijn voordracht zou resulteren in de eerste publicatie over het elementaire bewijs, namelijk door van der Corput [5]. Erdős ging met mij praten omdat ik een aanvulling had gepubliceerd [19] op een artikel van Clarkson en hemzelf [4], over benadering op $[0, 1]$ met lineaire combinaties van machten $x^{n_1}, x^{n_2}, \dots$ (Ons probleem was overigens in de oorlog al opgelost door Laurent Schwartz in zijn dissertatie [43], maar die kende ik niet op tijd.) Erdős wilde nu mijn commentaar op het moeilijke bewijs van zijn niet-lineaire Tauberstelling [8], die uitging van een abstracte vorm van de zogenaamde fundamentele relatie van Selberg. Maar ik kon zijn ingewikkelde bewijs, waarvan de presentatie uren in beslag nam, toen nog niet volgen!

Ik zou Erdős vele malen ontmoeten, op diverse plaatsen: Purdue University, Delft, diverse conferenties, UC San Diego, en ten slotte in Jeruzalem, toen hij daar in 1984 een Wolfprijs kreeg! (Slim als altijd ried Erdős meteen waarom ik daar ook was.)

Restschattingen

Aan Purdue zou Erdős mij in 1950 wijzen op het belang van goede restschattingen in Tauberstellingen. Bijvoorbeeld, als

$$|\sum a_n x^n - A| \leq B(1-x) \quad \text{voor } 0 \leq x < 1$$



Paul Erdős

en $|na_n| \leq C$, wat kun je dan zeggen over de resten $|s_n - A|$? Hij deed een suggestie om nuttige voorbeelden te construeren, en na enige tijd vond ik voor dit geval de optimale restschatting

$$|s_n - A| \leq C/\log n,$$

zie [22]. Het was teleurstellend dat de rest niet kleiner hoefde te worden. (Later bleek dat Geza Freud al eer wist dat $s_n - A = O(1/\log n)$. Turan had die bovengrens eerst niet willen publiceren omdat hij dacht dat hij veel te zwak was! Zie Freud [9].)

Tussen haakjes: in april 1952 zou Erdős bij mij en mijn vrouw Jopie logeren in Delft, net een week voor de geboorte van onze oudste dochter Wilma. We moesten hem vragen ergens anders heen te gaan. Hij begreep dat eerst niet goed, maar het bleek geen probleem. Zijn natuurkundige vriendin Jo Brunings uit Rochester (oorspronkelijk uit Rijswijk), die hem naar al zijn afspraken reed, zorgde voor ander onderdak.

Naast zeer algemene resultaten voor machtreksen zou ik al snel optimale restschattingen vinden voor andere soorten reksen. Met hulp van mijn vroegere mentor Kloosterman kon al dit werk snel gepubliceerd worden in de *Proceedings* van de KNAW. Dat was belangrijk omdat ik, inmiddels assistant professor aan de Universiteit van Wisconsin (1953–1964), onder druk stond om te publiceren teneinde daar een vaste baan te krijgen. Overigens werd goed lesgeven in Madison ook belangrijk gevonden.

Ik zou over mijn Tauberstellingen spreken tijdens een ‘Summer of Analysis’ aan de Universiteit van Chicago (georganiseerd door Zygmund) in 1956. Daar ontmoette ik Littlewood voor het eerst; het was zijn eerste bezoek aan de Verenigde Staten. Hij zou later een jaar in Madison doorbrengen en ik zou hem ook ontmoeten aan Trinity College in Cambridge.

Als een terzijde vermeld ik dat mijn restschattingen-artikel [24] uit 1954 impliciet het antwoord bevatte op een leuke vraag die Donald Newman in 1960 zou stellen: Voor welke exponenten k_n benadert de functie

$$f(x) = \sum_{n=0}^{\infty} (-1)^n x^{k_n}$$

de limiet $\frac{1}{2}$ voor $x \nearrow 1$ zo snel mogelijk? (Het antwoord is $k_n = n^2$. Zie [39] en mijn opmerking in *Mathematical Reviews* 0117474.)

Intermezzo over Wienertheorie

Ik noem alleen de nuttige stelling van Wiener en zijn leerling S. Ikehara [14] uit 1931.

Stelling 2. Zij de reeks

$$g(s) = \sum \frac{b_n}{n^s} \quad \text{met } b_n \geq 0$$

convergent voor $s = \sigma + i\tau$ als $\sigma > 1$, en stel dat

$$h(s) = g(s) - \frac{B}{s-1}$$

continue randwaarden heeft als $\sigma \searrow 1$. Voor $S(x) = \sum_{n \leq x} b_n$ geldt dan

$$\lim_{x \rightarrow \infty} \frac{S(x)}{x} = B.$$

(Later zou ik een bewijs geven met complexe analyse [32].)

Toegepast op de reeks

$$\sum_{p \text{ priem}} \frac{\log p}{p^s},$$

of op

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum \frac{\Lambda(n)}{n^s} = \sum \frac{\log p}{p^s} + \sum \frac{\log p}{p^{2s}} + \dots$$

geeft de stelling onmiddellijk de priemgetalstelling. Want er is dan een pool $1/(s-1)$ in het punt $s = 1$. Men hoeft verder alleen maar te weten dat $\zeta(s)$ geen nulpunten heeft op de lijn $\{\sigma = 1\}$. De conclusie is dat

$$\lim_{x \rightarrow \infty} \frac{1}{x} \sum_{p \leq x, p \text{ priem}} \log p = 1.$$

Nu ligt $\log p$ voor $x^{1-\varepsilon} \leq p \leq x$ dichtbij $\log x$. Met de notatie $\pi(x)$ voor het aantal priemgetallen $p \leq x$ vindt men dan dat

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1.$$

In woorden: $\pi(x)$ is asymptotisch gelijk aan $x/\log x$.

Contacten met Laurent Schwartz, distributies

Mijn vriend Hans Tolhoek en ik kwamen al vroeg gegeneraliseerde functies tegen zoals de 'deltafunctie', vergelijk het boek van Lützen [36] over de prehistorie van distributies. Maar ik dank bijna al mijn echte kennis over distributies aan Laurent Schwartz (1915–2002). Op het ICM Congres in Cambridge, Massachusetts 1950 luisterde ik naar zijn voordracht (en die van Hermann Weyl) in verband met zijn Fieldsmedaille. (Mijn vrouw Jopie en ik genoten ook van het optreden van Tom Lehrer in het Harvard Theater.) Aan Purdue University organiseerden Michael Golomb, Merrill Shanks en ik daarna enthousiast een werkgroep over distributies. Het eerste boek van Schwartz was net verschenen [44]. We vonden daarin het gebruik van de topologische vectorruimten van Dieudonné en Schwartz best lastig. Ik begon al gauw te zoeken naar een meer elementaire aanpak. Onder druk publiceerde ik echter te haastig over een elementaire theorie, zie [25]. Later zou ik een meer elegante aanpak bedenken met completering. Zo'n constructie werkt zowel voor de invoering van reële getallen, als voor Lebesgue-integreerbare functies en ook distributies! Zie beneden en mijn latere boeken [28, 33]. (Met distributies kon ik de voorwaarde van continue randwaarden in de Wiener-Ikehara stelling uit Stelling 2 omzetten in een nodige en voldoende voorwaarde, vergelijk [31] en ook [27].)

Polen zomer 1966

Ik ga het nu eerst hebben over een grote conferentie over gegeneraliseerde functies of distributies in Polen, georganiseerd door J.G. Mikusinski (1913–1987). Hij was bekend om zijn elementaire (minder algemene) distributietheorie, vergelijk [37, 38]. De bijeenkomst werd bijgewoond door veel prominente experts: Laurent Schwartz, Sergei Sobolev, George Temple en Jean Dieu-



Laurent Schwartz

donné (een van de grondleggers van de invloedrijke Bourbakigroep in Frankrijk). Mijn oude vriend Wim Luxemburg en mijn vrouw Jopie waren er ook. De conferentie begon in Katowice, waar Mikusinski zijn vaste baan had. Later verhuisde de bijeenkomst naar een wintersportgebied in het zuidoosten van Polen (Kluskowce?). Deelnemers en begeleidende personen werden per bus vervoerd en we kregen een lunchpakket mee. Rond de middag stopten we onverwachts bij de ingang van het concentratiekamp Auschwitz. Dat was schrikken; de confrontatie met de Holocaust was heftig. Enkele deelnemers weigerden het kamp binnen te gaan.

In de middag gingen we verder naar onze eindbestemming waar de conferentie werd voortgezet. Daar werden we al gauw getraakteerd op een excursie naar de bergen. Een gammele stoeltjeslift vervoerde ons over een flinke afstand, min of meer horizontaal, over een ruig landschap. Laurent Schwartz zat in het stoeltje voor mij en Sobolev net achter me. Toen de lift abrupt stopte en hevig begon te schommelen boven een ravijn, riep Schwartz naar Sobolev: als we nu neerstorten is dat het einde van distributietheorie! Na een poosje ging de lift verder naar een picnicplaats. Daar besloten Schwartz, mijn vrouw Jopie en ik om te voet terug te gaan.

In 1972 kon ik Dieudonné uitnodigen voor een semester als gasthoogleraar aan UC San Diego (ik was toen Department Chair). En in 1983 zou ik Schwartz nog ontmoeten bij zijn afscheid van de École Polytechnique in Palaiseau bij Parijs.

Completering, distributies

In een vectorruimte X met een geschikt convergentiebegrip beschouwen we Cauchyrijen $\{u_k\}$, $\{v_k\}$, enzovoort, dus

$$u_j - u_k \rightarrow 0 \text{ in } X \text{ wanneer } j, k \rightarrow \infty, \text{ enz.}$$

Sommige Cauchyrijen zullen in X convergeren, andere niet. Cauchyrijen $\{u_k\}$ en $\{u'_k\}$ heten *equivalent* als $u_k - u'_k \rightarrow 0$ voor $k \rightarrow \infty$. De equivalentieklassen U enzovoort van Cauchyrijen $\{u_k\}$, $\{u'_k\}$, ..., enzovoort, met voor de hand liggende definities voor diverse operaties, vormen de 'completering' $\overline{X}$ van X . Als een element U uit convergente rijen $\{u_k\}$ enzovoort bestaat wordt het geïdentificeerd met de limiet u van die rijen in X . Onder geschikte voorwaarden zal de nieuwe ruimte $\overline{X}$ inderdaad volledig zijn.

Voor de invoering van *distributies* op $\mathbb{R}$ gaat men uit van rijen $\{u_k\}$, $\{v_k\}$, ... van continue of lokaal integreerbare functies. Convergentie is nu relatief tot testfuncties: oneindig differentieerbare functies ϕ met begrensde drager. Dus $u_k \rightarrow u$ in X wordt gedefinieerd door de eis dat

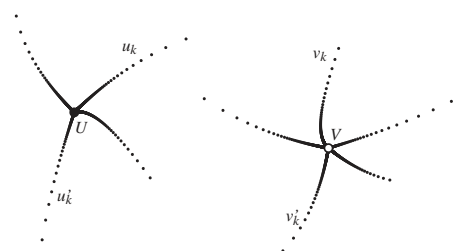
$$\int_{\mathbb{R}} u_k \phi \rightarrow \int_{\mathbb{R}} u \phi \text{ voor alle } \phi.$$

Nu is $\{u_k\}$ een Cauchyrij in X als $\int (u_j - u_k) \phi \rightarrow 0$ voor alle ϕ . Distributies op $\mathbb{R}$ zijn per definitie equivalentie-classes $U, V, \dots$ van zulke Cauchyrijen in X .

Voor primitieven $F = f^{(-1)}$ van lokaal integreerbare functies f voldoet de afgeleide $DF = f$ aan de relatie

$$\int_{\mathbb{R}} (DF) \phi = - \int_{\mathbb{R}} F \phi' \text{ voor alle } \phi.$$

Dezelfde formule wordt gebruikt om de afgeleide DU van een distributie U te definiëren: in elke equivalentieklasse zitten wel primitieve functies. Men bewijst vervolgens dat elke distributie lokaal gelijk is aan de afgeleide $D^k F$ van zekere orde k van een lokaal integreerbare functie F . De volledigheid van het stelsel distributies kan bewezen worden met behulp van Fourierreeksen, vergelijk [33]. In de completering $\overline{X}$ is de distributie V de limiet van zijn Cauchyrijen $\{v_k\}$.



Klassen van Cauchyrijen ('spiders')

Spiders

Mijn studenten aan UCSD verrasten mij rond 1973 met een leuke schets, die ik sterk ingekort weergeef.

The Gospel according to Professor Korevaar. In the beginning the earth was deso-

late and empty. But then The Lord created spiders. He made them of two kinds: spiders with a heart, and spiders with a hole. The first kind He called functions, and the second kind He named distributions. The two kinds lived well together and they had numerous offspring. Some of the offspring

had a heart, but most of them had just a hole. However, every spider with a hole had an ancestor with a heart! ☺

Dankbetuiging

Ik dank Tom Koornwinder voor de foto's van wiskundigen en Jan van de Craats voor de 'spiders'.

Referenties

- 1 F. van der Blij, *Theta Functions of Degree m*. PhD thesis, University of Leiden, 1947, 47 pp.
- 2 S. Bochner, Ein Satz von Landau und Ikehara. *Math. Z.* 37 (1933), 1–9.
- 3 N.G. de Bruijn, Levensbericht H.D. Kloosterman, *Jaarboek KNAW 1967–1968*, pp. 326–330.
- 4 J.A. Clarkson en P. Erdős, Approximation by polynomials, *Duke Math. J.* 10 (1943), 5–11.
- 5 J.G. van der Corput, Démonstration élémentaire du théorème sur la distribution des nombres premiers, *Scriptum*, No. 1, Math. Centrum Amsterdam, 1948, 32 pp.
- 6 G. Doetsch, *Theorie und Anwendung der Laplace-Transformation*, Springer, 1937, xiii + 436 pp.
- 7 P. Erdős, On a new method in elementary number theory which leads to an elementary proof of the prime number theorem, *Proc. Nat. Acad. Sci. U.S.A.* 35 (1949), 374–384.
- 8 P. Erdős, On a Tauberian theorem connected with the new proof of the prime number theorem, *J. Indian Math. Soc. (N.S.)* 13 (1949), 131–144.
- 9 G. Freud, Restglied eines Tauberschen Satzes, I, *Acta Math. Acad. Sci. Hung.* 2 (1951) (the paper actually appeared somewhat later), 299–308; II, *Acta Math. Acad. Sci. Hung.* 3 (1952/53), 299–307; III, *Acta Math. Acad. Sci. Hung.* 5 (1954), 275–288.
- 10 G.H. Hardy, Theorems relating to the summability and convergence of slowly oscillating series, *Proc. London Math. Soc. (2)* 8 (1910), 301–320.
- 11 G.H. Hardy en J.E. Littlewood, Tauberian theorems concerning series of positive terms, *Messenger of Math.* 42 (1913), 191–192.
- 12 G.H. Hardy en J.E. Littlewood, Tauberian theorems concerning power series and Dirichlet series whose coefficients are positive, *Proc. London Math. Soc. (2)* 13 (1914), 174–191.
- 13 G.H. Hardy en J.E. Littlewood, On a Tauberian theorem for Lambert's series, and some fundamental theorems in the analytic theory of numbers, *Proc. London Math. Soc. (2)* 19 (1921), 21–29.
- 14 S. Ikehara, An extension of Landau's theorem in the analytical theory of numbers, *J. Math. and Phys. M.I.T.* 10 (1931), 1–12.
- 15 J. Karamata, Über die Hardy–Littlewood'schen Umkehrungen des Abelschen Stetigkeitssatzes, *Math. Z.* 32 (1930), 319–320.
- 16 H.D. Kloosterman, On the convergence of series summable (C,r) and on the magnitude of the derivative of a function of a real variable, *J. London Math. Soc.* 15 (1940), 91–96.
- 17 H.D. Kloosterman, The behaviour of general theta functions under the modular group and the characters of binary modular congruence groups, I, II, *Ann. of Math. (2)* 47 (1946), 317–375, 376–447.
- 18 J. Korevaar, Some entire functions represented in a half-plane by Laplace integrals. (Dutch) *Mathematica B, Zutphen* 12 (1944), 107–114.
- 19 J. Korevaar, A characterization of the sub-manifold of $C[a,b]$ spanned by the sequence $\{x^{n_k}\}$. *Indag. Math.* 9 (1947), 360–368.
- 20 J. Korevaar, *Approximation and Interpolation Applied to Entire Functions*, PhD thesis, University of Leiden, 1949, viii+56 pp.
- 21 J. Korevaar, The zeros of approximating polynomials and the canonical representation of an entire function, *Duke Math. J.* 18 (1951), 573–592.
- 22 J. Korevaar, Best L^1 approximation and the remainder in Littlewood's theorem, *Indag. Math.* 15 (1953), 281–293.
- 23 J. Korevaar, Entire functions as limits of polynomials, *Duke Math. J.* 21 (1954), 533–548.
- 24 J. Korevaar, A very general form of Littlewood's theorem, *Indag. Math.* 16 (1954), 36–45.
- 25 J. Korevaar, Distributions defined (from the point of view of applied mathematics) by fundamental sequences, I, II, III, IV, V, *Indag. Math.* 17 (1955), 368–378, 379–389, 483–493, 494–503, 663–674.
- 26 J. Korevaar, Asymptotically neutral distributions of electrons and polynomial approximation, *Ann. of Math. (2)* 80 (1964), 403–410.
- 27 J. Korevaar, Distribution proof of Wiener's Tauberian theorem, *Proc. Amer. Math. Soc.* 16 (1965), 353–355.
- 28 J. Korevaar, *Mathematical Methods, Vol. 1: Linear Algebra, Normed Spaces, Distributions, Integration*, Academic Press, 1968, xi + 505 pp.
- 29 J. Korevaar, On Newman's quick way to the prime number theorem, *Math. Intelligencer* 4 (1982), 108–115.
- 30 J. Korevaar, *Tauberian Theory. A Century of Developments*, Grundlehren der Mathematischen Wissenschaften, Vol. 329, Springer, 2004, xvi+483 pp.
- 31 J. Korevaar, A Tauberian theorem for Laplace transforms with pseudofunction boundary behavior, Complex analysis and dynamical systems II, *Contemp. Math.*, No. 382, Israel Math. Conf. Proc., Amer. Math. Soc., Providence, RI, 2005, pp. 233–242.
- 32 J. Korevaar, The Wiener-Ikehara theorem by complex analysis, *Proc. Amer. Math. Soc.* 134 (2006), 1107–1116.
- 33 J. Korevaar, *Fourier Analysis and Related Topics*, Amsterdam, Spring 2011, Internet book, vi+320 pp.
- 34 R.A. Kortram, In memoriam Cornelis Visser. *Nieuw Arch. Wisk.* 5/2 (2001), 202–203.
- 35 J.E. Littlewood, The converse of Abel's theorem for power series, *Proc. London Math. Soc. (2)* 9 (1911), 434–448.
- 36 J. Lützen, *The Prehistory of the Theory of Distributions*, Studies in the History of Mathematics and Physical Sciences, No. 7, Springer, 1982. viii+232 pp.
- 37 J. Mikusiński, Une définition de distribution. *Bull. Acad. Polon. Sci. Cl. III* 3 (1955), 589–591.
- 38 J. Mikusiński and R. Sikorski, *The Elementary Theory of Distributions, I*, Rozprawy Mat., No. 12 (1957), 54 pp; II, Rozprawy Mat., No. 25, 1961, 47 pp.
- 39 D.J. Newman, $1 - 1 + 1 - 1 + \dots = 1/2$, *Proc. Amer. Math. Soc.* 11 (1960), 440–443.
- 40 D.J. Newman, Simple analytic proof of the prime number theorem, *Amer. Math. Monthly* 87 (1980), 693–696.
- 41 N. Obrechhoff, *Quelques classes de fonctions entières limites de polynômes et de fonctions méromorphes limites de fractions rationnelles*, Actualités Scientifiques et Industrielles, No. 891, Hermann et Cie, 1941, 47 pp.
- 42 F. Riesz, Sur les opérations continues linéaires, *C.R. Paris* 149 (1910), 974–977.
- 43 L. Schwartz, *Étude des sommes d'exponentielles réelles*, PhD thesis, Paris, 1943, 89 pp.
- 44 L. Schwartz, *Théorie des distributions. Tome I*, Actualités Sci. Ind., No. 1091, Hermann et Cie, 1950; *Tome II*, Actualités Sci. Ind., No. 1122, Hermann, 1951, 169 pp.
- 45 A. Selberg, An elementary proof of the prime-number theorem, *Ann. of Math. (2)* 50 (1949), 305–313.
- 46 A. Tauber, Ein Satz aus der Theorie der unendlichen Reihen, *Monatsh. Math. u. Phys.* 8 (1897), 273–277.
- 47 R. Timman, In memoriam Prof. Dr. H. Bremekamp, *Nieuw Arch. Wisk.* 3/11 (1963), 61–63.
- 48 R. van der Veen en J. van de Craats, *De Riemann-hypothese. Een miljoenenprobleem*, Epsilon Uitgaven, deel 69, 2011, vi+102 pp.
- 49 N. Wiener, Tauberian theorems, *Ann. of Math.* 33 (1932), 1–100.

Lisa Rougetet

*ATER en Mathématiques
Université Charles de Gaulle, Lille, France
lisa.rougetet@gmail.com*

Education

The use of games and their history to improve secondary school students' skills in mathematics reasoning and problem solving

This article resulted from the talk 'Machines designed to play Nim games: a possible (re) use in the modern mathematics curriculum?', presented by Lisa Rougetet at the Winter-symposium of the KWG in January 2017. This talk, and the underlying studies, have been motivated by the latest reform (September 2016) of the French high school education system, which has led to changes in the curricula.

In mathematics, a new theme entitled 'algorithmics and programming' aims at initiating pupils (7th–9th grades) to 'write, develop and run a simple program'. To achieve this, the curriculum offers several class activities centered on 'games in a maze, [...], Nim game and Tic-Tac-Toe'. Of course, these examples are only suggestions, and teachers are free to approach the new theme with other activities. In this article, we would like to explain how Nim game, and some variants, could enable secondary school students to investigate problems through a stimulating experimental approach that helps to develop mathematical reasoning. As the idea of introducing games in class to tackle algorithmics notions is brand new (and as it is just a suggestion for teachers), we don't have many concrete teaching outcomes to present. However, we report on experiments that had been led with pupils in out-of-school contexts, using Nim game.

The resources provided by the French government to set up the new 'algorithmics and programming' theme point out

that pupils should develop algorithmic thinking. The expected skills at the end of the 9th grade are:

- breaking down a problem: analyzing a complex problem, and dividing it into sub problems;
- recognizing patterns: looking for invariants and repetition;
- generalization and abstraction;
- designing algorithms.

To do so, one of the proposed activities, among others, is to program playful applications (mazes, pong, battleship, Nim, Tic-Tac-Toe). This idea raised the question of using Nim-like games¹ in mathematics teaching; what skills do they help to develop, could they be used in class to help pupils to acquire algorithmic thinking, or more generally, mathematical reasoning? To try to answer these questions, the present article will focus on the Nim game, which is one of the most famous combinatorial games. We will see, through the Nim game, that combinatorial games may play a role in learning the know-how

of mathematical activities² and that they offer research activities (in which students have to think for themselves and are, in a way, placed in the situation the mathematician faced when he was looking for the solution of the game for the first time) for students from high school to university. Knowing their history and the development of their mathematical theory is important to understand the epistemic approach that students face when they play the game and try to solve it.

Nim game rules and solution

The Nim game—as it was introduced for the first time in 1901—is a take away game: usually three (or more) rows of matches are set on a table; each row contains a different number of matches. Alternately, both players select one of the rows and remove as many matches as they want: one, two, ..., or even the whole row. The player who takes the last match(es) wins the game. An example of a possible initial position is shown in Figure 1. There are many different versions of Nim, called Nim-like games, depending on the initial number of rows and matches, and the rules according to which they can be removed.³

The strategy to win at Nim is as follows: first, for each row, the number of matches must be written in binary. Then, these bi-

nary numbers are placed in three horizontal lines so that the units are in the same vertical column. The sum of each column is calculated and if all of them are congruent to 0 mod 2, the position is called a *losing position*. Such positions should be reached at each move in order to win the game, because the opponent cannot reach another losing position in the next move.⁴ The general theory of Nim using the binary system can hardly be discovered by pupils, but the aforesaid properties of winning and losing positions, defined in a recursive manner, are often understood rather well, even if not totally assimilated.⁵

History of Nim and combinatorial game theory

The starting point of the history of combinatorial game theory is commonly dated to 1901, when the Nim game was first mentioned under this name in an article published in the *Annals of Mathematics* by Charles Leonard Bouton (1869–1922), a mathematician from Harvard.⁶ In this article, Bouton gives the complete mathematical solution to Nim. Bouton's article is considered as a cornerstone of the development of combinatorial game theory, because, unlike recreational mathematics books of the sixteenth, seventeenth and eighteenth centuries, it gives a solution to any possible initial position, no matter the number of rows and objects in each row.

After Bouton's article, combinatorial game theory was developed by other mathematicians and became a beautiful abstraction with John Conway's surreal numbers theory in 1976. Thanks to Conway's work, combinatorial games became a separate branch of mathematics and computer science. Nowadays, combinatorial game theory is a branch of mathematics, which links up mathematics (graph theory, set theory), computer science (game programming, artificial intelligence) and education.

Being familiar with the history and the mathematical development of Nim-like games has a double interest: on one hand, it provides material to set up interdisciplinary activities (required in the French new curriculum) that combine history, mathematics and computer science. On the other hand, playing Nim-like games in order to solve them (finding a winning strategy) places students in an epistemic approach through a singular experimental situation in which the required knowledge

will appear as the optimal solution to the problem.⁷ Looking for the best moves to play, in order to win the game at the end, coincides with the knowledge we want the pupils to acquire, i.e. winning and losing position, strategy, backward reasoning, et cetera (unlike other games that require the use of multiplication tables, for instance).

Didactical aspects of Nim-like games

Different kinds of knowledge are associated to combinatorial games⁸: non-institutional knowledge, which includes specific notions of combinatorial games such as winning and losing position, and winning strategies, and institutional knowledge, which consists of mathematical notions that can be found in the usual curriculum, for example integers properties, induction, recursion, et cetera. The latter aspect shows that the use of combinatorial games in class is appropriate for learning fundamental notions in mathematics through a playful situation.⁹ Playing and analyzing Nim-like games are also appropriate to develop algorithmic skills. First, to understand how a game can be won in a general case, one needs to analyze simpler

positions, i.e. positions that occur at the end of the game. For instance, when they play Nim, pupils quickly start to analyze whether (1, 1), (1, 2) or (1, 1, 1) are winning or losing positions. This requires to break down the initial problem, which is quite complex, into simpler sub problems. Then, they should try to generalize some configurations. For instance, once pupils have understood that (1, 1) and (2, 2) are losing positions, they can figure out that (n, n) is also a losing position, for any n . The same occurs with $(1, 1, n)$, which is a winning position for any n . These observations have been made on a group of twelve pupils (14–15 years old) in the context of a 'mathematical summer camp' organized by 'Plaisir Maths' in June 2016.¹⁰ Then, even if games differ in their design from one to another, the mechanisms implemented to develop winning strategies are the same, centered on the properties of winning and losing positions. Thus, they stimulate pattern recognition (to identify a configuration seen before) and abstraction (to understand the underlying strategy regardless of the form of the game).

Beyond these notions connected to combinatorial games properties, games such as Nim could be a good training to practice mental arithmetic and to develop abstract thinking (e.g. speculating about what the opponent will play to better counter him). They could be used to introduce enumeration (given a position, what are the possible moves?) and to illustrate graph theory through game trees, which represent the possible connections between the positions in the game. But, as we mentioned earlier, since the reform of the curriculum is brand new, the use of combinatorial games in class is still in its early stages, and we have no records on the actual teaching outcomes. Furthermore, teachers first need to train themselves on Nim game, its strategy, its theory (less known than Tic-Tac-Toe for example), and they can attend study days devoted on this kind of training (but not mandatory).

Furthermore, combinatorial games enable the creation of situations in which students tackle problems with an autonomous research activity through an experimental approach that combine three kinds of actions in problem solving: presenting new problems, experimenting–observing–confirming, and trying to prove the correctness of an approach.¹¹ Combinatorial



Figure 1 Example of an initial position of the Nim game: three rows containing respectively 7, 5 and 3 matches.

games perfectly constitute a mathematical activity, as they allow for many fundamental aspects of mathematical activities: discovery phases, conjectures, trial and error, reformulation, proof arguments, et cetera. It is interesting to submit a given position of a game to pupils and to ask them to determine its nature (winning or losing). They can put their ideas to the test and confirm or invalidate their hypothesis by playing directly.¹²

Besides, as games are often considered more enjoyable than plain mathematical tasks, pupils may be more focused on finding the winning strategy. Using counters in Nim-like games can help, for instance, to better picture the problem and enables a quick representation of a position at any moment of the activity. Action is an essential part of mathematics learning for it gives meaning to the mathematical activity through its experimental dimension.

Conclusion

Combinatorial games are well-suited for active learning, and improve pupils' personal relationship with mathematics. In this kind of playful activity, pupils' involvement is

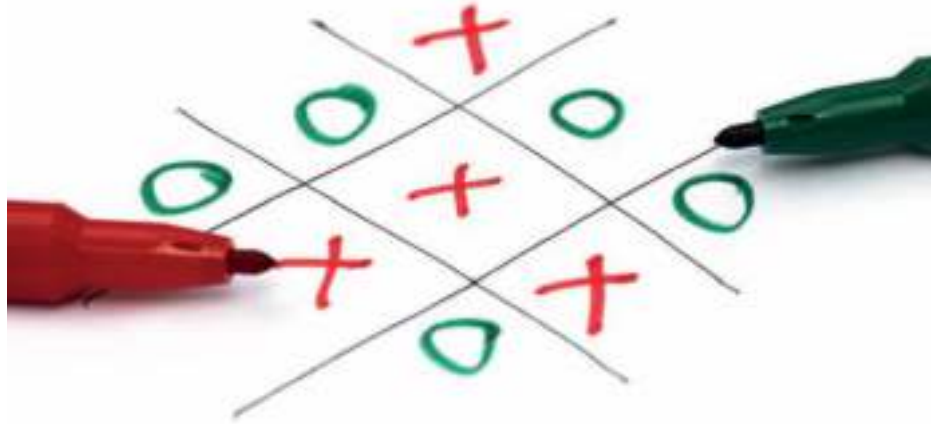


Figure 2 Tic-Tac-Toe is an example of a combinatorial game.

different, because it stimulates group work and communication, avoids them from getting discouraged, and can motivate pupils with learning difficulties: wanting to find how to win is a strong pedagogical lever. The game in itself is the environment the pupils act on and with, and the fact that it is fun helps them to learn mathematics. We

are confident that the strength of games for teaching makes them essential tools for mathematics education, because of the features they share with learning situations in which the student is involved; then he becomes actor of his learning and accepts the responsibility of the knowledge transfer. ☛

Notes

- 1 In general, *combinatorial* games can be used. In a combinatorial game, there are two players, playing alternately. Usually, there are a finite number of positions and the information is complete—which means both players know what is going on at any moment of the game. There are no chance moves such as rolling dice or shuffling card and generally the player who finds himself unable to play loses. *Tic-Tac-Toe*, *Connect Four* and *Checkers* are examples of combinatorial games. In a combinatorial game there is a strategy—a sequence of moves—that enables one player to win the game whatever his opponent plays. It means that, theoretically, it is possible to know the nature of any arbitrary position in the game (*losing* or *winning*) if we assume both players play optimally (in practice, the analysis is more complex, because of the high number of possible positions in most games).
- 2 With 'know-how' we mean the knowledge, methods and techniques that are the base of all mathematical activity, such as experimentations, doing a particular case study, modeling, construction of proofs and definitions, et cetera. See details in: X. Colipan, *Étude didactique des situations de recherche pour la classe concernant des jeux combinatoires de type Nim*, Doctoral thesis, Institut Fourier, Grenoble, France, 2014. Re-

- trieved from <https://tel.archives-ouvertes.fr/tel-01121726/>.
- 3 For instance, few years after Bouton, a Dutch mathematician named Willem Abraham Wythoff (1865–1939) published an article in the *Nieuw Archief voor Wiskunde*, presenting the following version of Nim: there are only two rows of matches, and at each turn players can remove any number of matches from one row only OR remove the same number of matches in both rows.
- 4 That is why the position is called a *losing position*: there exists a winning strategy for the player who has just played, and not for the next player to play. A position is a *winning position* if there exists a winning strategy for the next player to play.
- 5 For further details, see X. Colipan, 2014, p. 140, in the context of the geometrical Euclidean game.
- 6 Actually, things are not so definite: we have found earlier analyzes of combinatorial games in recreational mathematics books from the sixteenth century and thereafter. See, e.g. L. Rougetet, A Prehistory of Nim, in: M. Pitici (ed.), *Best Writing on Mathematics 2015*, Princeton University Press, 2016, pp. 207–214.
- 7 G. Brousseau, *Théorie des situations didactiques*, La Pensée Sauvage, 1998, p. 49.

- 8 X. Colipan, 2014, p. 36.
- 9 This approach is not new: the oldest analyzes of games—which we would qualify nowadays as combinatorial—have been found in recreational mathematics books in the sixteenth century. Their main purpose was to tickle curiosity, but also to use a playful dimension to obtain a mathematical result.
- 10 'Plaisir Maths' is a structure of mathematics popularization, which gather animators, teachers and researchers to create and organize playful and didactical mathematical projects.
- 11 N. Giroud, *Étude de la démarche expérimentale pour les situations de recherche pour la classe*, Doctoral thesis, Institut Fourier, Grenoble, France, 2011. Retrieved from <https://tel.archives-ouvertes.fr/tel-00649159>, p. 7.
- 12 As far as I know, Colipan and the group she worked with during her Ph.D. are the only ones, in France, who experimented combinatorial games in class and published didactical results on it. The federative structure 'Maths à Modeler' (whose aim is to propose workshops to the general public to discover fundamental computer sciences and mathematics) and 'Plaisir Maths' also use combinatorial games in their actions of scientific dissemination.

Jan Beuving

cabaretier, Zeist
janbeuving@gmail.com



Het keerpunt van Annelie Vink

Zonder wiskunde kom je er ook

Annelie Vink voltooide cum laude een master wiskunde aan de Universiteit Utrecht. Ze promoveerde vervolgens bij het RIVM en VUmc, en een mooie wetenschappelijke carrière gloorde. Maar ze gooide het roer om. Bijna letterlijk, want ze ging werken bij scheepsbouwer Royal IHC in Sliedrecht.

‘Momenteel blokkeert de toren van een pijpenlegschip het uitzicht van haar kantoor: ze had niet gelukkiger kunnen zijn.’ Deze zin gaat over jou, toch?
“Ha ha, ja!”

Het was de laatste zin van je Curriculum Vitae in je proefschrift. Ben je nog steeds zo gelukkig?

“Helemaal. Het is toch gaaf dat we zo’n groot schip kunnen bouwen? Dat zou je in je eentje nooit voor elkaar krijgen. Zo’n schip is echt buitenproportioneel, groot en extreem, daar word ik gelukkig van. Toen ik die zin opschreef, was ik ook zo gelukkig omdat ik in het laatste jaar van mijn promotietraject gericht gezocht heb naar wat ik wilde. Het liefst iets met grote machines, en het liefst in de scheepvaart. Als je dan zo’n schip vanuit je kantoor ziet, is het wel duidelijk dat het gelukt is. Het is in alle opzichten anders dan het RIVM. Als je daar naar buiten keek, zag je bos en konijntjes. Hier loop je in je pauze een rondje over de werf.”

Wat doe je bij IHC?

“Ik ben bezig met het uniformeren van bedrijfsprocessen. Binnen dat werk zijn drie pijlers: de software, de daadwerkelijke processen (wie doet wat in welke volgorde), en de data. En ik doe dat uni-

formeren specifiek bij de engineeringtak van het bedrijf. Engineering wordt steeds meer onze corebusiness. Het daadwerkelijke bouwen van de schepen gebeurt nog wel in Nederland, maar de verwachting is dat dat steeds meer in het buitenland zal plaatsvinden in landen zoals China, waar goedkoper gewerkt kan worden. Wij zijn vooral een *technology innovator*. Een



Annelie Vink

schip dat op een heel ingewikkelde plek een pijp moet leggen bijvoorbeeld, daar bieden wij een maatoplossing voor. En we zijn bezig met het ontwikkelen van schonere schepen, die niet meer op zware diesel varen, maar op LNG, *Liquified Natural Gas*.

Ik moet zorgen dat informatie zo efficiënt mogelijk wordt doorgegeven, en dat de engineers met wie ik samenwerk zich niet verliezen in details. Ik moet het overzicht houden in de puzzel van software, processen en data. Het zijn drie componenten die naadloos in elkaar moeten vouwen.”

Komt er nog (harde) wiskunde bij kijken?

“Nee. Wel moet ik heel procesmatig denken, en in dat opzicht lijkt het natuurlijk op een model bouwen. In een complexe omgeving waar heel veel voor mij onbekend is. Ik ben een buitenstaander, en stel dus onorthodoxe vragen. Dat werkt heel verhelderend; zo kunnen we scherp krijgen waarom we doen wat we doen. Maar ik zie geen formules meer. Héérlijk!”

Die laatste zin van je CV impliceert dat je minder gelukkig was in je promotietraject.

“Dat klopt. Maar echt ongelukkig was ik ook niet. Iedere promotie kent pieken en dalen. De eerste twee jaar leid je een heel saai bestaan. Er zijn nog weinig momenten waarop je echt iets bereikt. Je had wel collega’s, maar in je werk was je vaak alleen met je modellen.”

Waar ging je promotie over?

“Ik deed onderzoek naar de verwachte effecten van preventiemaatregelen tegen baarmoederhalskanker. Wat kunnen we op lange termijn verwachten van vaccinatie tegen het virus dat de veroorzaker is: HPV? Doet het vaccinatieprogramma wat we denken? We deden al een bevolkingsonderzoek vanaf 30 jaar, waarbij we tegenwoordig kijken of iemand een HPV-besmetting heeft. HPV is een soa, en kan zich dus makkelijk verspreiden. Maar daarnaast zijn we in 2009 begonnen met vaccineren van 12-jarigen tegen HPV. Die twee groepen gaan natuurlijk samenkomen: er komen straks mensen bij het bevolkingsonderzoek die gevaccineerd zijn. Hoe kunnen we het onderzoek het beste aan die mensen aanbieden? Je hebt modellen nodig om daar voorspellingen over te kunnen doen, en op basis daarvan konden wij bijvoorbeeld besluiten om de screeningsintervallen te verlengen.”

Dat is best verantwoordelijk werk.

“Ja. Ik moet wel zeggen: ik deed aanvullend onderzoek bij de beslissing om die screeningsintervallen te verlengen. Die was al genomen. Mijn resultaten waren een controle. Maar spannend is het natuurlijk wel. Je denkt wel eens: heb ik niet ergens een fout gemaakt? Ik heb er wel slapeloze nachten van gehad.”

Ik heb ook onderzoek gedaan naar hoe lang het duurt voor een HPV-besmetting uitmondt in baarmoederhalskanker. Gemiddeld rond de 25 jaar. Dat zijn cijfers die niet te observeren zijn, omdat het onethisch is om mensen te volgen tot dat punt. Er is namelijk een voorstadium van baarmoederhalskanker dat je goed kunt behandelen. Voor die voorspellingen zijn wiskundige modellen nodig. Die wiskunde zelf was ik nog niet zat, maar het gaf me niet genoeg energie.”

Ik hoor van veel wiskundigen die ik spreek dat hun promotie niet bepaald de gelukkigste tijd van hun leven was. Zou het niet anders in te richten zijn?

“Nou, jij spreekt voor deze rubriek een bevooroordeelde groep: mensen die daarna iets anders zijn gaan doen. Onderzoek gaat gewoon langzaam. Dat weet je nog niet als je 24 bent en je gaat promoveren. Wat bij mij trouwens ook mee-

speelde, was dat ik het gevoel had dat we de top van het HPV-onderzoek gehad hadden.”

Wilde je altijd al promoveren?

“Nee! Het tegenovergestelde! Promoveren was iets voor übernerds, dat was ik toch niet? Utrecht is vooral van de abstracte wiskunde. Ik zag het totaal niet voor me dat ik daartussen belanden zou. Die echte passie of vakidiotie had ik niet. Dat er ook promotie mogelijk was op grensgebieden, wiskunde en infectieziekten bijvoorbeeld, had ik niet gedacht.”

Wie heeft je dan toch overgehaald?

“Ik deed mijn afstudeeronderzoek al bij het RIVM, over het generatie-interval van infectieziekten. Hoeveel tijd zit er tussen de eerste ziektesymptomen van de besmetter en de besmette? Dat was voor het eerst in mijn wiskundestudie dat ik in aanraking kwam met data. Tijdens mijn afstuderen pas! Utrecht was zo theoretisch dat je de x_i -tjes nooit invulde.

In die tijd was er een keer een borrel — op de dag van de statistiek, hoe groot is die kans — en toen heeft mijn latere copromotor mij eerst genoeg bier gevoerd en vervolgens aan het denken gezet.

Hij daagde me vooral uit om de vacature die ze hadden nu eens echt serieus te nemen. Dat was voor mij wel het sein om na te denken: wat wil ik nou eigenlijk? De consultancy of een bank, dat leek me niks. Dit was wel iets waar ik over na kon denken. Toen heb ik het gedaan. Vaak begin ik gewoon aan dingen, en dan zie ik wel waar het uitkomt.”

Was je, met de kennis van nu, niet beter op je plek geweest op een technische universiteit?

“Misschien wel. Mijn keuze voor Utrecht was deels ingegeven door mijn wiskundedocent, en deels een sfeerkeuze. En: ik kon niet naar een TU, want ik had geen natuurkunde op de middelbare school. Ik had een Economie en Maatschappijprofiel, met wiskunde B1 en B2. Al die nerds die Natuur en Techniek gingen doen, daar zag ik me, als onzeker pubermeisje, totaal niet tussen zitten. Bovendien had ik een hekel aan biologie. Dat getrut met die plantjes en fotosynthese...”

En 8 jaar later studeerde je af op onderzoek naar infectieziekten!

“Ja, het kan raar lopen.”

Waarom wilde je wiskunde studeren?

“Ik heb het altijd heel leuk gevonden. Rekenen op de basisschool al. Dat er één antwoord was, en dat je dat ook kon controleren. Mijn brein werkt ook vooral op logica. Niet op geheugen.

Ik ben overigens heel blij met die abstracte opleiding hoor! Het heeft me ook het gevoel gegeven dat ik nu alles kan. En mijn promotie heeft me ook veel geleerd. Vooral een basisvertrouwen bij een probleem: nu begrijp ik het misschien nog niet, maar over een half jaar weet ik er alles van.”

Wat zijn je plannen voor de toekomst?

“Ik ga hier voorlopig niet weg. Ik raak snel verveeld, maar hier niet. Mijn weg ernaartoe was misschien niet de meest efficiënte, maar ik ben nu goed op mijn plek.”

Als de recorder al uitstaat, zegt Annelie ineens: “Wiskundigen kunnen best wel arrogant zijn, trouwens.”

Verklaar je nader?

“Misschien vooral tijdens hun studie. Niet de vakidioten, die zijn heel bescheiden. Het zijn de mensen zoals ik. Veel mensen zeggen dat ze vroeger slecht in wiskunde waren. Als je dat maar vaak genoeg hoort, denk je: ‘Ik doe iets wat anderen niet kunnen.’ Tien jaar geleden vond ik mezelf heel slim. Promoveren was vervolgens echt een oefening in nederigheid. Daar waren zoveel mensen die veel slimmer waren die geen wiskunde hadden gestudeerd.

Iets van die arrogantie zit in de hele wetenschap, overigens. Ik was gepromoveerd, kreeg een prijs voor jong onderzoeker van het jaar, en toen ging ik hierheen. Dat kwam me op verbaasde blikken te staan: ‘Waarom ga je weg? Dit is toch de beste plek waar je kunt zijn?’ Maar er is meer op de wereld. Zonder wiskunde kom je er ook.”

Goede suggesties voor een Nederlandse wiskundige met een keerpunt in zijn of haar carrière zijn welkom via keerpunt@nieuwarchief.nl.

Chris Peters

Department of Mathematics and Computer Science
Eindhoven University of Technology
c.a.m.peters@tue.nl

Obituary Wolf Barth (1942–2016)

Remembering a friend and colleague

On 30 December 2016 Wolf Barth passed away at the age of 74. Barth was born in Germany, where he lived most of his professional life. For a short but influential period (1972–1976) he held the Chair of Topology in Leiden. His former colleague Chris Peters looks back on his life and work.

If you have lately visited the exposition *Imaginary*¹, you have come across a nice picture of an algebraic surface with many nodes, the so-called *Barth sextic* (Figure 1) about which I will say more below. You may have wondered: “Who is this Barth?” In this article written on the occasion of his death last December I will sketch my relationship with him and I will elaborate on his significance for Dutch mathematics.

Wolf Barth was born on 20 October 1942 in Wernigerode and died on 30 December 2016 in Nürnberg. He studied mathematics and physics at the university of Erlangen and had followed R. Remmert (1930–2016) to Göttingen. Under Remmert’s auspices as well as that of K. Siegel’s successor H. Grauert (1930–2011) he got his doctorate in 1967. When Remmert in 1967 succeeded H. Behnke (1898–1979) in Münster, Barth followed him again and stayed there for two years. He came back in 1971 for his ‘Habilitation’, after having spent the academic year 1969/1970 at MIT, Cambridge, Massachusetts, as a visiting lecturer. He subsequently came as a professor to Leiden where he remained until 1976 when, at the age of 33, he accepted an offer from the university of Erlangen-Nürnberg, and stayed there until his retirement. Brought up in the Münster school of complex analysis of several complex variables, his first interests went into that direction. The mathematics he encountered at Leiden made him shift towards complex geometry, which would become his true love. At first this meant vector bundles; later his interest also turned to surfaces and their interplay with groups.

In Leiden

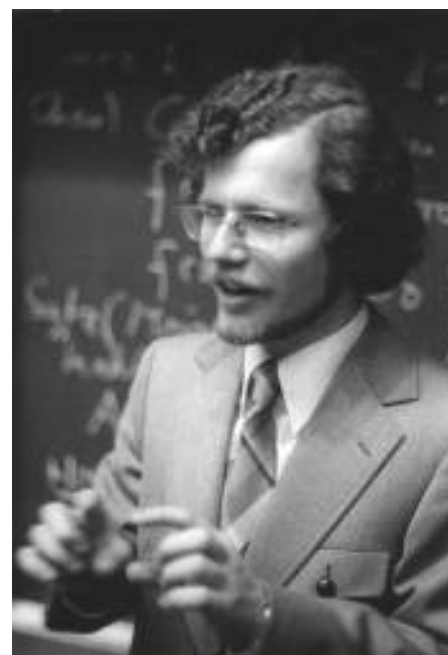
Between the years of 1970 and 1974 I was a graduate student of A. van de Ven (1931–2014). He had become professor of topology at Leiden in 1962. Wolf Barth came to Leiden to succeed W.T. van Est (1921–2002), a very amiable professor of geometry, whose inspiring lectures on algebraic topology I attended as a master student.²

Somehow van de Ven had been able to allure Barth, the most brilliant student of his friend and colleague R. Remmert, to come to Leiden as the successor of W.T. van Est. Maybe because here at the young age of 30 he was given a full professorship, a position that certainly trumped the one he had in Münster.³ Barth followed in the footsteps of van Est, teaching the course on mathematical physics the latter used to do. Barth was sensitive to his duties, real or imaginary, and as usual he took his assignment very seriously and produced immaculate lectures. In particular I recall his lectures on the representations of the Lorentz group, which I attended out of curiosity. It is a subject that runs the risk of becoming rather dry, but due to the presence of the mathematical physicist Peter Bongaarts, who posed a lot of questions, the lectures became quite animated. All in all it was a great success. However, maybe due to Barth’s usual high demands on himself, such an exchange with mathematical physics was never repeated in subsequent years.

Nowadays, one can hardly believe that one of the demands that came with a chair in the Netherlands consisted in deliver-

ing all lectures in Dutch. Barth took this very seriously and within a short time he spoke a perfect Dutch without any accent; he spoke it so well that some of my contemporaries originally thought of him as Dutch. It was the language we spoke between ourselves, even in later years when Wolf had long been residing in Germany, although in later years he complained that his Dutch had become so rusty he could no longer speak it.

Thanks to Barth I was introduced to modern techniques and encouraged to use them rather than being intimidated by them. One such was spectral sequences which had never appeared inside the walls of the Leiden mathematics department before, and which Barth had used to great success in his paper [1] on vanishing among coherent sheaves on projective spaces.



Wolf Barth

Even more importantly, he gave me a lot of support. When I was struggling with Jurriaan Simonis on the double point formula, being puzzled by a suggestion of my advisor, he very much urged me to keep on trying and not just give up and ask van de Ven for assistance. It paid off, Simonis and I finally figured it out and the paper [14] was well received and played a crucial role in the initial stages of my career. I also owe it to Wolf's direct support that I got hired back at Leiden after my post-doc at Harvard in 1974–1975 funded by a ZWO-stipend.⁴

As to be expected, Barth was influenced by his senior colleague and became involved with vector bundles and wrote several joint papers with him, the most influential being [12]. Also, the topic he gave to his first and only student⁵ in Leiden — Wilfred Hulsbergen — led to a new kind of bundles on projective spaces, subsequently named after the latter.

After his departure in 1976, Barth came back several times to Leiden. Barth's return to Leiden for the spring semester of 1990 stands out since he then took up an invitation for the prestigious Kloosterman Chair, a special chair for guest professorships named after the world-renowned number theorist.⁶ At that time he confided to me about the time when he was a professor in Leiden: "They were the best years of my life." He especially recalled with nostalgia how van de Ven and he worked in the former's cigar smoke filled office on the article [12], nicknamed the 'Babylonian vector bundles paper'.

Apart from these visits, Barth also stimulated exchanges between the Dutch and German geometry school.

Compact complex surfaces

Van de Ven had been thinking for some time to write a book on one of his favorite topics, complex surfaces, and suggested, it must have been around 1975, that Wolf and I would join him. After some thought we agreed, but it would take until 1984 before the resulting monograph [8] would come out. It is fair to consider Barth's participation to this project as his greatest contribution to Dutch related mathematics.

At the time of writing, technology was limited to electric typewriters with minimalist frills like the little round balls with special characters such as the Greek fonts. You really had to plan such an enormous project

carefully and discuss it at every stage for its coherence, since one did not want to bother the secretary with too many new versions.

First, there was the division of labour. Wolf wrote the sections on tools of complex analysis, which van de Ven then could use as black boxes in giving his specific proofs on surfaces, while my input was Hodge theory.

I should also add that I needed to act as a mediator, van de Ven and Barth did not always get along, both having strong opinions, and it came to my lot to present compromises. Wolf, for instance, did not approve of fancy notation, as that would only suggest difficulties where there were none. This was an important point in view of the poor technology we had at that time!

Much of the discussions took place in van de Ven's office, which — as noted before — was always filled with bluish smoke, as he was an inadvertent smoker of cigars. Although upon my entrance a window was quickly opened, it did not help much. The book was such a success (yes, we did make some money out of it) that a second edition [9] was commissioned. Below I occasionally return to this joint enterprise.

Back to Germany

Just after Wolf and Regina, his wife, left Leiden, my wife and I visited them in their flat in Erlangen. Some years later — the Barths had, like us, two children by then — our families met in Bubenreuth near Erlangen where they had built a house. On this occasion I got to know the people in the Erlangen mathematics department who just happened to have their annual outing. I was to see the Barths again in the spring of 1982. They graciously offered me to stay in their attic while Wolf and I were writing the sections on Enriques surfaces in the above mentioned book. It meant hard work at the department in the day, but in the evening beer and dinner at their place. We discussed mathematics and gossiped about our colleagues of course, but invariably other topics were touched upon such as the psychology of people, illustrated in his case by Westerns he loved to watch.

In the fall of 1982 I spent a couple of weeks in Warwick, during the festival of Algebraic Geometry arranged by Miles Reid. Then I started to delve deeper into the mysteries of Enriques surfaces and, together with Wolf, I was able to conclude this research which resulted in our paper [7].

By that time his work had become more concrete and geometrical than when he started as a student of Remmert. Several constructions for new vector bundles on projective spaces had been found by him, sometimes in connection with unexpected properties of special surfaces such as in [2] or, as in [6], written in collaboration with his first German student Klaus Hulek. For a timely report on this I refer to [3].

Oberwolfach

As most of my contemporary colleagues, I regularly went to one of the annual or bi-annual week-long seminars at the MFO (Mathematisches Forschungsinstitut Oberwolfach). Its themes ranged over all of mathematics.

Every other year in September the seminar 'Komplexe Analysis' took place. It was run from 1962 until 1980 by the trio Grauert–Remmert–Stein and, as the German title suggests, its theme had been complex analysis in the tradition of the Münster school. Although in the course of the years more and more complex geometry had entered, one could still be subjected to $\bar{\partial}$'s in the talks. But in 1982 a division took place into a more geometrically oriented seminar and one which continued in the old tradition. In the fall of 1982 Wolf Barth replaced K. Stein (1913–2000) and he would lead the geometry faction. He also saw to it that to a greater extent than before young upcoming people should be given opportunities to speak. He would be in charge until 1994 when J. P. Demailly, T. Peternell and K. Hulek took over.

Later years

After the conclusion of the first edition of the book, inevitably our contacts became less frequent and also our mathematical

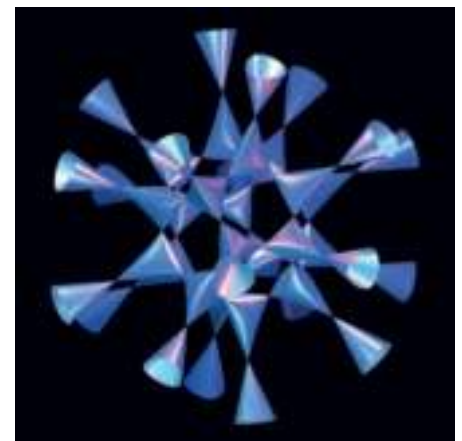


Figure 1 The Barth sextic.

interests diverged somewhat. I took on to Hodge theory while Wolf continued to work on concrete algebro-geometric objects; he has become especially known for the construction [4] of a projective surface of degree 6 having 65 nodes, 1 more than the maximum as asserted by Severi.⁷ See Figure 1. Apart from this I would also like to mention his articles with his students Th. Bauer [5], A. Sarti [1], and with S. Rams [10]. As the titles reveal, all these works are on very concrete geometric objects and their symmetries.

During the years 2000–2003 I met Wolf again regularly when preparing the second edition [9] of the book. He was still very much interested, but he wanted to be relieved of the responsibility of contributing new technical material, and instead van de Ven relegated it to the canonical choice, Klaus Hulek. We met mostly in the tower of the famous *Welfenschloß*, the mathematical institute of the home university of Hulek, Leibniz Universität Hannover. After that I did not see much of Wolf except a few times in Leiden during the meetings aptly named *Geometry in Autumn*, not only because they took place in the fall, but also hinting at the demise of geometry in Leiden after most geometers either had retired or left the country.

Notes

- 1 *Imaginary* is an international exposition; the Dutch edition started last year in Eindhoven, then went to (the University of) Twente, Amsterdam, Utrecht, and will end this year in Leiden.
- 2 Together with Alexander Rinnooy Kan we wrote a collection of exercises for van Est's course. In 1972 the latter accepted a chair at the University of Amsterdam where he remained until his retirement.

References

- 1 W. Barth, Transplanting cohomology classes in complex-projective space, *Amer. J. Math.* 92 (1970), 951–967.
- 2 W. Barth, Kummer surfaces associated with the Horrocks-Mumford bundle, *Journées de Géométrie Algébrique d'Angers, 1979/Algebraic Geometry, Angers, 1979*, Sijthoff & Noordhoff, 1980, pp. 29–48.
- 3 W. Barth, Report on vector bundles, *Proceedings of the International Congress of Mathematicians*, Vol. 1, 2 (Warsaw, 1983), PWN, 1984, pp. 783–789.
- 4 W. Barth, Two projective surfaces with many nodes, admitting the symmetries of the icosahedron, *J. Algebraic Geom.* 5 (1996), 173–186.
- 5 W. Barth and Th. Bauer, Smooth quartic sur-



Figure 2 Students of the last course taught by W. Barth, Erlangen, 2012.

Wolf would eventually divorce his wife Regina, and his life would take a new direction, although of course he always remained Wolf, maybe even more so — as illustrated by his conduct during his retirement party. Not only did he not bother to attend all the talks, but he did not even show up for the dinner that had been organized in his honor. Nobody, including the organizers, could come up with an explanation; I knew of course that in recent years his hesitation to show up at social events had only grown, but this I found to be carrying it to the extremes.

That something serious was amiss, I started to suspect when he declined an invitation to attend a memorial meeting for

van de Ven in Leiden in December 2015. He excused himself that he could not travel for an extended period in a train, but only after his death did I in retrospect realize the full implication.

People who did not know him well often were put off by his briskness in delivery and directness in his opinions. But if you learned to know him, you would discover his underlying kindness and loyalty behind his somewhat forbidding and undiplomatic exterior. He cared deeply for his students; they loved him in return as demonstrated in the picture (Figure 2) I took during his retirement talk. ☞

Disclaimer and Acknowledgements

This short obituary does not do full justice to the mathematical work of Wolf Barth that consists of more than fifty articles, many in collaboration. For this I refer to the obituary for the 'Jahresbericht der Deutschen Mathematiker Verein' that Thomas Bauer, Klaus Hulek, Sławomir Rams, Alessandra Sarti and Thomas Szemberg are writing.

I want to thank Ulf Persson and Hans Sterk for help with the redaction of this obituary; Klaus Hulek as well as Fabrizio Catanese corrected some faulty recollections. Finally, I want to express my thanks to Wilfred Hulsbergen and Alessandra Sarti for sharing their memories of Barth and the support and interest they showed.

- 3 He was 'Wissenschaftliche Rat und Professor', a position that does not exist anymore. In the Netherlands it would probably be equivalent to 'UD'.
- 4 The 'Stichting voor Zuiver Wetenschappelijk Onderzoek' was the predecessor of NWO.
- 5 Barth was also involved in my thesis and, even more so, in that of Hans Vogelaar, where he acted as a 'referent'. Vogelaar was officially a student of van de Ven.
- 6 W. Barth and K. Hulek, Projective models of Shioda modular surfaces, *Manuscripta Math.* 50 (1985), 73–132.
- 7 W. Barth and C. Peters, Automorphisms of Enriques surfaces, *Invent. Math.* 73 (1983), 383–411.
- 8 W. Barth, C. Peters and A. van de Ven, *Compact Complex Surfaces*, Ergebnisse der Math. No. 4, Springer, 1984.
- 9 W. Barth, K. Hulek, C. Peters and A. van de Ven, *Compact Complex Surfaces*, second edition, Ergebnisse der Math. No. 4, Springer, 2004.
- 10 W. Barth and S. Rams, Equations of low-degree projective surfaces with three-divisible

- 6 See www.math.leidenuniv.nl/nl/kloosterman for details on Kloosterman (1900–1968).
- 7 The 'true' maximum is indeed 65 as shown by Jaffe and Ruberman [13].
- 8 D. B. Jaffe and D. Ruberman, A sextic surface cannot have 66 nodes, *J. Algebraic Geom.* 6 (1997), 151–168.
- 9 C.A.M. Peters and J. Simonis, A secant formula, *Quart. J. Math. Oxford Ser. (2)* 27(106) (1976), 181–189.
- 10 W. Barth and A. Sarti, Polyhedral groups and pencils of K_3 -surfaces with maximal Picard number, *Asian J. Math.* 7(4) (2003), 519–538.
- 11 W. Barth and A. van de Ven, A decomposability criterion for algebraic 2-bundles on projective spaces, *Invent. Math.* 25 (1974), 91–106.
- 12 D. B. Jaffe and D. Ruberman, A sextic surface cannot have 66 nodes, *J. Algebraic Geom.* 6 (1997), 151–168.
- 13 C.A.M. Peters and J. Simonis, A secant formula, *Quart. J. Math. Oxford Ser. (2)* 27(106) (1976), 181–189.
- 14 W. Barth and A. van de Ven, A decomposability criterion for algebraic 2-bundles on projective spaces, *Invent. Math.* 25 (1974), 91–106.



Fokko Jan Dijksterhuis

Science, Technology and Policy Studies (STePS)

Universiteit Twente

f.j.dijksterhuis@utwente.nl

Vakantiecursus

Krommen pletten: kegelsneden in de Gouden Eeuw

Op de vakantiecursus 2015 van het Platform Wiskunde Nederland sprak Fokko Jan Dijksterhuis over de geboorte van de analytische meetkunde in Nederland in de Gouden Eeuw. Dit artikel is een weergave van zijn voordracht. Hij vertelt hoe Frans van Schooten de nieuwe meetkunde aan de praktijk koppelde door het tekenen van kegelsneden.

In 1646 publiceerde Frans van Schooten de Jongere (1615–1660) zijn eerste boek: *Organica Conicarum Sectionum in Plano Descriptione, tractatus* (Verhandeling over de mechanische beschrijving van kegelsneden in het platte vlak). Het kan beschouwd worden als een soort sollicitatiebrief waarin hij zijn wiskundige bekwaamheid tentoonspreidde. Van Schooten was kandidaat om zijn vader Frans van Schooten de Oudere (1581–1645) op te volgen als hoogleraar ‘Duytsche Mathematique’ in Leiden. Dit was een driejarige opleiding aan de Universiteit Leiden ten behoeve van vestingbouwers, landmeters en andere mensen uit de praktijk. Wiskunde werd onderwezen in de landstaal — Duytsch, dat wil zeggen Nederlands — en niet in het Latijn zoals gebruikelijk in de academie. Niet alleen de taal was aangepast, ook de inhoud van het programma was praktisch georiënteerd.¹ Frans jr. had zijn vader al regelmatig geassisteerd en vervangen en uiteindelijk werd hij inderdaad benoemd als de nieuwe hoogleraar. De *Organica* was niet in het Nederlands geschreven en ging over een onderwerp dat geen onderdeel van de ‘Duytsche Mathematique’ was. Desondanks was het een heel passende proeve van bekwaamheid voor deze positie. Van Schooten liet zien dat hij zeer kundig was in de wiskunde, maar bovendien wist hoe je die vertaalde naar de praktijk.

Mechanische beschrijving van kegelsneden in het vlak, aldus de titel. Aangevuld met: bruikbaar voor meetkundigen, optici, en in het bijzonder voor gnomoni-

ci en mechanici. (Dat laatste wil zeggen: bouwers van zonnewijzers en werktuigen.) Wat moeten we ons bij een mechanische beschrijving van kegelsneden in een vlak voorstellen? Kegelsneden waren een klassiek onderwerp uit de wiskunde, maar Van Schooten behandelde het op een nieuwe manier. Gelukkig vertaalde hij zijn boekje een jaar of tien later naar het Nederlands: *Tuych-werckelijcke beschrijving der kegelsneden op een vlack*. Het was onderdeel van: Francisci van Schooten, *Mathematische oeffeningen, begrepen in vijf boecken* (Leiden, 1660).² Zo kunnen we op ons gemak lezen wat er nieuw aan zijn aanpak was en waarom hij die verkoos. Nadat hij uitgelegd had hoe nuttig het tekenen van parabolen, ellipsen, en hyperbolen was voor zaken als lenzenslijpen, tuinaanleg, ornamenten, en zonnewijzers, vervolgde Van Schooten:

Wantse, indien het beschrijven der Kegel-sneden op een vlak tot so veelderhande dingen se kan kint, wat wonderlijck, dat is bevoordene van de leering der Kegel-sneden de nefeelijcke Maetschap van conin af haer so hebben bevlische, en datter doorgaen, en bysonder in dese eeuw, een nieuwen aenwas by gekomen is! Doch het geen my wonder geeft, is, dat niemant tot noch toe (dat ik weet) dese moeyten op hem gesamen heeft, namentlijk, datter inmansel gevonden zy, die van de Tuych-werckelijcke beschrijving der Kegel-sneden heeft gehandelt, en delfve in yder voorsal besont.

Met andere woorden: Van Schooten verbaasde zich erover dat het tekenen van kegelsneden in het vlak nog nooit wiskundig behandeld was. De ‘mathematici’ hielden zich aan de klassieke definitie waarbij een kegelsnede voortgebracht wordt door — zoals het woord al zegt — een kegel met een plat vlak te snijden. Deze definitie ging terug op het hoofdwerk van de kegelsneden, de *Konika* van Apollonius van Perga (circa 262–190 v.Chr.). Deze

ruimtelijke constructie speelde geen rol bij het tekenen van ellipsen, hyperbolen, en parabolen in het platte vlak. Dat riep de vraag op in hoeverre die praktische aanpak wiskundig onderbouwd was. Van Schooten wilde in deze lacune voorzien.

Tuiniersellips

Een klassiek voorbeeld van zo’n vlakke voortbrenging is de tuiniersellips. Sla twee pinnen in de grond, leg er een dichtgeknoopt touw omheen, trek een kromme rondom de pinnen met de strakgetrokken lus. Van Schooten liet zien dat deze kromme daadwerkelijk een ellips was die voldeed aan de eigenschappen die Apollonius had afgeleid. Tamelijk triviaal: Stelling 52 van Boek 3 van de *Konika* zegt dat de som van de afstanden van een punt op de ellips tot de brandpunten constant is (zie Figuur 1).

Met deze tuiniersellips zijn we ook direct bij de kern van Van Schootens boek. Het is een voorbeeld van een ‘tuych-werckelijcke’ beschrijving. Er waren ook andere manieren om kegelsneden in het platte vlak voort te brengen, maar die veronderstelden veelal beheersing van de wiskunde. Een voorbeeld is de puntsgewijze constructie. De werktuigelijke voortbrenging daarentegen bestond uit één vloeiende beweging waarvoor alleen het juiste instrument nodig was.

In zijn boek introduceerde Van Schooten instrumenten waarmee mensen uit de praktijk zo’n aan-een-verknachte beweging (zie Figuur 2) tot stand konden brengen en toonde aan dat de resultaten wiskundig correct waren. Deze combinatie van praktisch vernuft en wiskundige grondigheid was precies wat men van een hoogleraar ‘Duytsche Mathematique’ mocht verwachten.

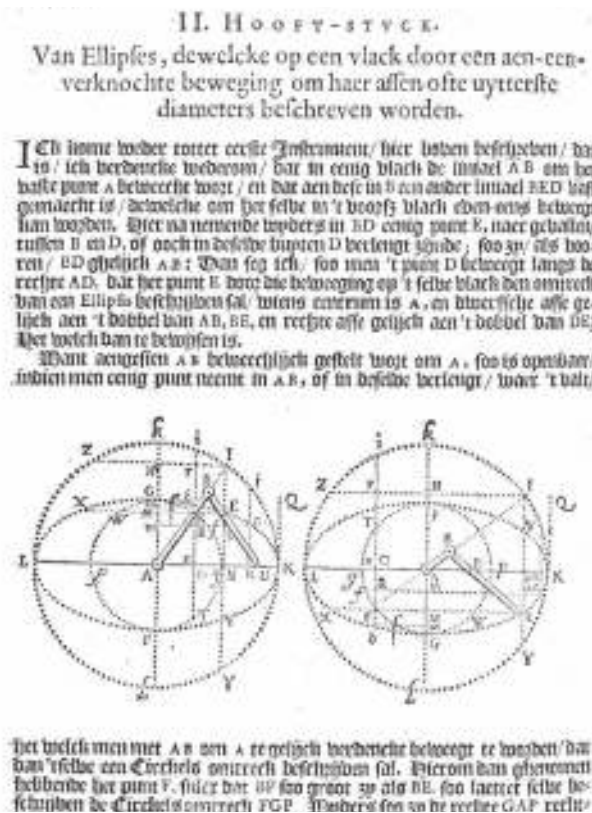
cirkel, of zoals in de constructies van Van Schooten die aangestuurd worden door een eenparige beweging. Waar het bij Descartes abstract-conceptueel bleef, maakte Van Schooten het concreet en praktisch. De mechanische bewegingen van zijn ellipsografen waren precies de continue beweging die Descartes bedoelde. Een kinematica van de meetkunde.

Geometria

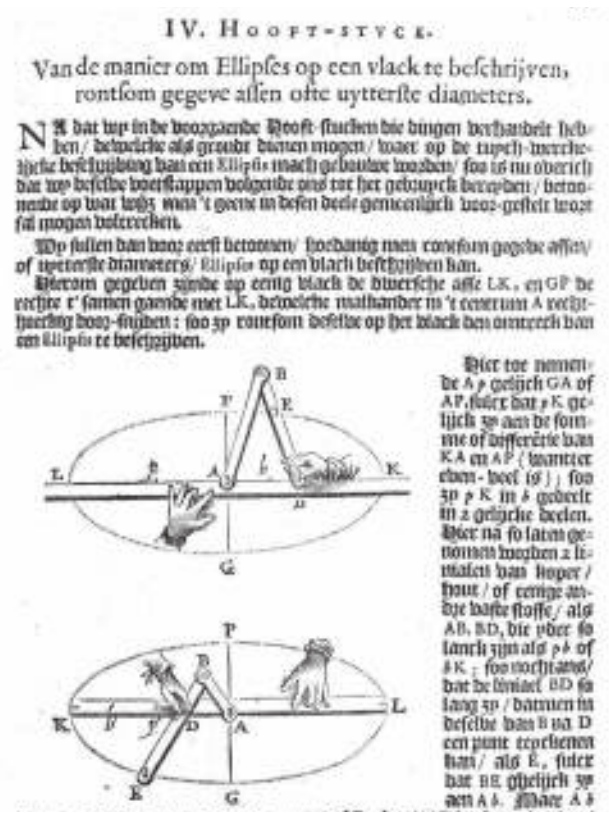
Met de *Organica* sloeg Van Schooten de brug tussen de 'geometria' van Euclides en Descartes enerzijds en de 'meetkunst' van landmeters en vestingbouwers anderzijds. Het was echter vooral een proeve van zijn bekwaamheid om les te geven aan de Duytsche Mathematique, geen lesboek. Alleen al vanwege het Latijn was het boek-

je niet geschikt voor de studenten van de ingenieursschool. Van Schooten trok er een ander type studenten mee: zonen van de goeude burgerij die belangstelling hadden voor de nieuwe wiskunde en wijsbegeerte van mensen als Descartes. Zoals Christiaan, de tweede zoon van Descartes' beschermheer Constantijn Huygens; Johannes Hudde, een Amsterdams patriciër; en Johan, zoon van het voorname Dordtse geslacht De Witt. In zijn 'privatissimae' bestudeerde Van Schooten met hen de *Géométrie* van Descartes, schreef toelichtingen en aanvullingen, hetgeen uiteindelijk uitmondde in zijn levenswerk: *Geometria, à Renato Des Cartes*. In 1649 gaf hij de eerste editie uit, in 1659–1660 verscheen de tweede, uitgebreid met tal van aanvullingen en annotaties.

Eén van de bijlagen van de *Geometria* was een beschouwing van één van zijn voorname studenten over kegelsneden. In *Elementa Curvarum Linearum* werkte Johan de Witt een analytische behandeling van kegelsneden uit.⁶ Hij zette hiermee het werk van zijn leermeester voort, en zette tegelijkertijd een stap verder. De platte voortbrenging was voor De Witt de grondslag van de analyse van krommen. Hij had geen last van de bescheidenheid van Van Schooten: "...achtte ik het volslagen in te gaan tegen de natuurlijke orde, die men in de wiskunde zoveel mogelijk in acht moet nemen, dat men de oorsprong van deze krommen zoekt in een ruimtelijk lichaam en deze vervolgens overbrengt naar het platte vlak." Hiermee hadden de klassieken afgedaan en waren de kegelsneden definitief geplet. ☛



Figuur 3 Begin van hoofdstuk II van de *Mathematische oefeningen*, p. 288.



Figuur 4 Begin van hoofdstuk IV van de *Mathematische oefeningen*, p. 299.

Noten en referenties

- 1 Zie ook F.J. Dijksterhuis, *The Golden Age of Mathematics: Stevin, Huygens and the Dutch Republic*, *Nieuw Archief voor Wiskunde* 5/9(2) (2008), 100–107.
- 2 Hierin is ook Christiaan Huygens' *Van Rekeningh in Spelen van Geluck* te vinden, de eerste publicatie op het gebied van kansrekening. De *Mathematische oefeningen* staan online bij <http://bc.library.uu.nl>.
- 3 F.J. Dijksterhuis. *Moving Around the Ellipse. Conic Sections in Leiden, 1620–1660*, in: Sven Dupré en Christoph Lüthy (eds.), *Silent Messengers: The Circulation of Material Objects of Knowledge in the Early Modern Low Countries*, Lit, 2011, pp. 89–124.
- 4 Henk Hietbrink heeft de constructies verzameld op www.fransvanschooten.nl en een GeoGebra-app geschreven om ermee te spelen.
- 5 Henk Bos, *Redefining Geometrical Exactness. Descartes' Transformation of the Early Modern Concept of Construction*, Springer, 2001.
- 6 Beide delen zijn vertaald en toegelicht door A.W. Grootendorst; Jan de Witt, *Elementa Curvarum Linearum. Liber Primus* (CWI, 1997); *Liber Secundus* (CWI, 2003).

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



Coarse-graining of Fokker–Planck equations

Upanshu Sharma

On 12 January 2017 Upanshu Sharma successfully defended his Ph.D. thesis *Coarse-graining of Fokker–Planck equations*, written under guidance of prof.dr. Mark Peletier (TU/e) and dr. M. Hong Duong (Warwick). He worked in the group CASA, a rich and vibrant environment, both academically and socially. He may be biased, but thinks that this vibrance is a reflection of the general outlook towards research in the Netherlands: informal, communicative and inclusive. Anyway, his years in Eindhoven were a great and fruitful experience and he absolutely enjoyed being a PhD student in the Netherlands.

When asked to tell about his research, Sharma first explains the title of his thesis: what has he been studying, and why? Next, he discusses how his results were obtained.

Coarse-graining

Coarse-graining is an umbrella term for procedures and techniques used to approximate a system by a simpler and lower dimensional one: a system is represented with fewer degrees of freedom than those actually present in the system. Most real-life applications and problems are fairly complex and higher dimensional, making their analysis difficult. As a result coarse-graining has gained tremendous importance in various fields of science. In particular, the questions raised and studied in Sharma's thesis were inspired from statistical mechanics, molecular dynamics and thermodynamics.

Fokker–Planck equations

The focus of his study was a class of evolution equations called the *Fokker–Planck* equations. These are partial differential equations which describe the collective behaviour of (infinitely many) microscopic particles which feel the effect of *deterministic* and *random* forces. As an example, Sharma describes a simple case where the position of each of these microscopic particles follows a Brownian motion, written informally as

$$\frac{dx}{dt} = \sqrt{2} \dot{B}_t.$$

Here $x(t)$ is the position of each individual particle at time t , which evolves randomly as modelled by the Brownian motion $\dot{B}_t$. Since each of the particles is moving randomly, the mean of the positions of these particles is also random. A very classical result then states that as the number of particles goes to infinity, this random mean converges to a *deterministic* macroscopic time-dependent density ρ which solves the well-known ‘diffusion equation’

$$\frac{\partial \rho}{\partial t} = \Delta \rho,$$

where Δ is the Laplace operator. (Formally the quantity considered

is the *empirical measure* instead of the mean.) The important point here is that the diffusion equation can be viewed as *arising from random particles*. Like the diffusion equation, many related linear and nonlinear equations share this feature and thus fall under the category of Fokker–Planck equations. It should be noted that Fokker–Planck equations are widely employed in both natural and social sciences.

Eliminating ‘uninteresting’ fast variables

Having discussed coarse-graining and Fokker–Planck equations, Sharma now links the two. Coarse-graining in the context of evolution equations typically arises in the presence of temporal and/or spatial *scale separation* which is indicated by the presence of a small or large parameter in the system. As a result of this parameter, the system has fast and slow variables. As the ratio of ‘fast’ to ‘slow’ increases, some form of averaging allows one to remove the fast variables, thereby producing a reduced dynamics on the slow variables. In other words, by coarse-graining, one eliminates the fast variables and keeps the coarse-grained variables with time or length scales much larger than typical particle scales.

A classical example helps to make these ideas more concrete: a randomly perturbed Hamiltonian system, which is for $\varepsilon = 0$ a classical Hamiltonian system. Consider the following random evolution of a particle in $\mathbb{R}^2$:

$$\frac{dX}{dt} = J\nabla H(x) + \sqrt{2\varepsilon} \dot{B}_t.$$

Here $X(t) \in \mathbb{R}^2$ is a variable in the phase space, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is the canonical symplectic matrix and $H: \mathbb{R}^2 \rightarrow \mathbb{R}$ is a Hamiltonian. As before, $\dot{B}_t$ is the Brownian motion. The small parameter $0 < \varepsilon \ll 1$ intuitively controls the amplitude of the noise. Repeating the same procedure as before, the random mean of infinitely many such particles converges to a deterministic macroscopic time-dependent density ρ which satisfies the following Fokker–Planck equation:

$$\frac{\partial \rho}{\partial t} = \operatorname{div}(\rho J \nabla H(x)) + \varepsilon \Delta \rho. \quad (1)$$

Here ρ can also be interpreted as the probability density function of the random variable X . The central question in this context is: “What is the behaviour of (1) in the limit of $\varepsilon \rightarrow 0$?” Under appropriate rescaling (which allows to see the effect of the noise), a scale separation arises in this system as $\varepsilon \rightarrow 0$: there is a faster Hamiltonian motion around the level sets and a slower diffusive motion from one level set to another. Following the discussion above, as this ratio of fast to slow increases it becomes possible to derive a simpler model.

In fact, this classical coarse-graining question has received wide attention in the dynamical systems and probability communities since it models a commonly encountered issue: the effect of noise in observation data in dynamical systems. Sharma does not give a solution to this problem here, but interested readers are welcome to have a look at his thesis for a solution to this simple, yet fascinating, question. Another interesting question from a numerical perspective would be to derive quantitative estimates which relate the behaviour in the limit $\varepsilon \rightarrow 0$ to the behaviour $\varepsilon > 0$.

Main results

While the Fokker–Planck equations in the examples above are linear, these equations can be nonlinear as well. An abstract Fokker–Planck equation can be written as

$$\partial_t \rho = (\mathcal{N}^\varepsilon) \rho, \quad (2)$$

where $\mathcal{N}$ is in general a nonlinear operator and $0 < \varepsilon \ll 1$ indicates the presence of scale separation in the system. The main results of Sharma’s thesis are towards addressing two facets of coarse-graining:

1. Qualitative coarse-graining: understand the behaviour of (2) as $\varepsilon \rightarrow 0$.
2. Quantitative coarse-graining: derive quantitative estimates for the solution of (2) for $\varepsilon > 0$.

While these questions are about the behaviour of the *macroscopic* Fokker–Planck equations, the crucial ingredient in the analysis, is the behaviour of the *microscopic* random particles underlying these equations. Specifically, Sharma uses the so-called ‘large deviations’ of the underlying stochastic process or random particles. Large deviations is a theory that analyses the rates of convergence of the underlying microscopic particles to the corresponding macroscopic equations. In addition to providing various insights, in the current context, the theory of large deviations can also be used to reformulate the Fokker–Planck equations as a solution to a *variational problem*. It turns out that this variational problem reveals the *geometrical structure* underlying the Fokker–Planck equations and also meshes well with coarse-graining questions. As a result this variational formulation of the Fokker–Planck equations is the central ingredient in Sharma’s thesis.

In light of this very fascinating and interesting micro–macro connection, the main message and novelty of Sharma’s thesis is that “studying underlying microscopic systems gives us structure and tools to understand Fokker–Planck equations”.

Significant moments

When asked about significant moments that had stood out for him, Sharma says that ironically the best period during his PhD time was also the hardest one: the last few months before the thesis submission. There was a palpable sense of pressure, which any PhD student will recognise. However, in his case this really helped since suddenly interesting ideas and connections kicked in. As a result he was doing some very interesting mathematics until the last day before his submission deadline, as opposed to the oft-heard dictum “All I do is write”. Additionally, the process of the thesis writing opened Sharma’s eyes to closely-related literature and helped him connect with some very interesting people. Hard but fun, the last few months were definitely his favourite.

In March, Sharma joined the École des Ponts ParisTech in France as a postdoc. Since Paris is a great city, both for mathematics and for life in general, he has really been looking forward to the experience. Hopefully he can continue to combine hard and fun work.

Ronald Meester

Afdeling Wiskunde
Vrije Universiteit Amsterdam
r.w.j.meester@vu.nl

Boekbespreking Ethan Canin: *Handboek van een twijfelaar*

De Malosz en de Abendroth: over wiskundig onderzoek in een roman

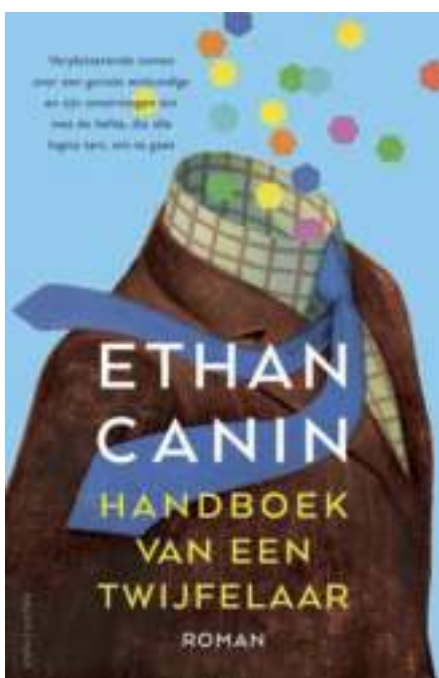
Bij Ambo|Anthos verscheen in januari een Nederlandse vertaling van *A Doubter's Almanac*, een roman van de Amerikaanse auteur Ethan Canin. Het *Handboek van een twijfelaar*, zoals het boek in het Nederlands heet, gaat over een geniaal wiskundige in de jaren zeventig die uitgroeit tot een legende door zijn onderzoek aan de universiteit van Berkeley. Ronald Meester, hoogleraar wiskunde aan de VU, bespreekt het boek.

Over wiskunde schrijven in een roman is een hachelijke onderneming. Over de inhoud van het vak kun je eigenlijk niets kwijt, dus hoe voorkom je dat het droogzwemmen blijft? Natuurlijk, wiskundigen zelf spreken nog wel eens tot de verbeelding, maar de clichés liggen altijd op de loer. Ik heb het gevoel dat wanneer het in de literatuur over wiskunde gaat, het vaker koketteren is dan dat er echt een poging gedaan wordt om er iets betekenisvol over te schrijven.

Maar met zijn laatste roman *Handboek van een twijfelaar* heeft Ethan Canin een poging gedaan om een roman te schrijven die zowel over de wereld van de wiskundige als over wiskundig onderzoek zelf gaat. En ik vind dat hij daar heel goed in geslaagd is. Niet dat het boek geen clichés bevat, maar Canin krijgt het voor elkaar om een boek te schrijven over wiskunde en de wereld van een wiskundige dat als roman ontroerend, meedogenloos en ge-

loofwaardig is, en als verhaal over wiskundig onderzoek behoorlijk realistisch. Sommige passages lijken mij alleen begrijpelijk voor wiskundigen, maar Canin heeft er heel goed voor gezorgd dat deze de loop van het verhaal niet verstoren. Ik vind zijn boek als roman heel geslaagd, met goed uitgewerkte karakters, verrassende wendingen, en prachtige dialogen. En bovendien denk ik niet dat ik eerder een roman heb gelezen waarin de wiskunde tegelijkertijd prominent en realistisch is. Ik denk dat deze roman door veel lezers van dit blad gewaardeerd zal worden.

Milo Andret is een bijzondere jongen, met een heel bijzonder wiskundig talent: hij is in staat om topologische en meetkundige constructies te visualiseren. Zijn toelatingsexamen voor een PhD-positie valt nogal op, en hij wordt de beschermeling van Borland, de bekendste wiskundige in de Verenigde Staten op dat moment, die heilig gelooft in zijn kunnen. Borland stuurt Milo in de richting van de topologie, en Milo, zeer ambitieus, neemt zich voor om het vermoeden van Malosz te gaan bewijzen, een zeer belangrijk en diepzinnig vermoeden. Dit vermoeden bestaat overigens niet echt, Canin heeft het verzonnen. Natuurlijk is het



Ethan Canin, *Handboek van een twijfelaar*, Ambo|Anthos uitgevers, 2017, 527 p. ISBN 978 90 263 34627, € 23,99.

niet mogelijk om in de roman uit te leggen wat het vermoeden precies zou behelzen (dat kan ook moeilijk als het niet bestaat), maar Canin weet dat knap te omzeilen. Hij geeft precies genoeg informatie om te begrijpen in welke richting we het moeten zoeken. Er zijn, natuurlijk, ook kapers op de kust. Andere wiskundigen, er worden er twee met name genoemd, die ook bezig zijn met hetzelfde vermoeden. Maar Andret is van mening dat zij niet zozeer oog hebben voor het vermoeden, als wel voor hun eigen carrière, en bewust stapje voor stapje kleine pasjes zetten, en elk pasje publiceren. Goed voor hun publicatielijst, maar Andret weet dat je er zo niet komt.

Hijzelf komt er uiteindelijk wel, en Canin probeert ons deelgenoot te maken van een doorbraak in zijn onderzoek, een moment waarop Andret inziet welke benadering mogelijk succes zou kunnen hebben. Andret realiseert zich op een gegeven moment dat dimensie een clou in zich draagt, en hij slaagt er uiteindelijk in om een bewijs te leveren. Dit bewijs van het vermoeden van Malosz levert Andret zijn PhD, een positie in Princeton, en een aantal jaren later ook de Fieldsmedaille op.

Maar inmiddels heeft Canin ook duidelijk gemaakt dat het karakter en de persoonlijkheid van Andret problematisch zijn. Hij heeft duidelijk autistische trekjes, woede-aanvallen, beledigt en schoffeert mensen, en is onvoorzichtig als het op vrouwen aankomt. Zijn wangedrag wordt door Princeton lang getolereerd, maar op een gegeven moment begint hij een affaire met de vrouw van een Nobelprijswinnaar. Ook dit gaat lang goed, totdat het uitkomt, en hij in een vlag van woede de Nobelprijswinnaar aanvalt. Dit leidt tot zijn ontslag, en daarna gaat het eigenlijk bergafwaarts met zijn leven.

Maar voordat het zover is, probeert Andret een ander vermoeden te kraken: het vermoeden van Abendroth. Opnieuw weten wij als lezer niet wat dit vermoeden precies behelst, maar we komen er wel achter dat er een belangrijke numerieke component in zit. Het verhaal speelt zich af in het begintijdperk van de digitalisering, en we zijn getuige van het feit dat Andret, al jaren bezeten van de Abendroth, zich volledig op het programmeren stort. In een werkelijk prachtige passage schetst Canin hoe er uiteindelijk, na weken en weken eindeloos debuggen, een getal verschijnt op het scherm. Een getal. Andret weet dat dit

de weg naar de oplossing is. Hij weet inmiddels ook dat hij concurrentie heeft van een veertienjarig wonderkind, Seth Kopter. Maar Andret heeft de modernste computer, en Kopter niet. Zijn leven bestaat, naast allerlei affaires, uit nog maar één ding: de Abendroth. Canin weet het neer te zetten als een bloedstollend gevecht tussen twee grote wiskundigen. Maar Andret verliest, op het nippertje. Kopter heeft weliswaar minder computerkracht tot zijn beschikking, maar gebruikt het veel efficiënter. Deze klap komt Milo Andret in zijn leven eigenlijk niet meer te boven: hij weet absoluut geen raad met het verlies.

Halverwege het boek verandert het perspectief, en gaat het verder in de ik-vorm, geschreven door de zoon van Andret. Tot op dat moment wisten we niet dat Andret een zoon had, of zelfs maar dat hij getrouwd was. Zoon Hans is zelf ook wiskundige, maar hij heeft voor het grote geld gekozen als handelaar in financiële producten. Hij zegt hierover zelf dat hij gecorrumpeerd is geraakt. Ook over deze tak van de wiskunde komen we langzaam maar zeker het een en ander te weten, en eigenlijk zijn we getuige van het begin van de financiële wiskunde. Ik zal hier niet alle gebeurtenissen uit dit tweede deel uit de doeken doen, er moet natuurlijk nog wel wat te lezen overblijven.

Maar de wiskunde komt ook in dit tweede deel volop aan bod. Niet zozeer vanuit het perspectief van het wiskundig onderzoek, als wel meer beschouwend wanneer Milo aan zijn zoon (en dochter Paulien) wiskundeonderwijs geeft. Zo leren we heel wat over Andrets kijk op het vakgebied. We horen hem bijvoorbeeld zeggen dat partiële integratie meer heuristiek dan wiskunde is en bovendien veel te voor de hand liggend om interessant te zijn. We horen over de tweestrijd tussen Newton en Leibniz, en ook de filosofie van de wiskunde komt aan de orde. Algebraïsche topologie krijgt er nog even van langs, en we maken ook kennis met het dedain dat Andret kennelijk heeft voor 'rekenen'.

Er wordt in het hele boek slechts één echte wiskundige opgave expliciet beschreven, namelijk een opgave die Hans op een wiskundewedstrijd moet oplossen. Hans vindt hem belachelijk makkelijk. Het antwoord wordt ook gegeven (met bewijs), maar ik kon de verleiding niet weerstaan de opgave zelf te proberen. Hij was te doen, maar belachelijk makkelijk...?

Hoewel het leven van Milo Andret na zijn ontslag uit Princeton nog slechts lijkt te bestaan uit een baantje als wiskundeleraar, drank, verslaving, en een mislukt huwelijk, weet Canin nog een heel bijzondere spanning in te bouwen. In een obscuur tijdschrift verschijnt een artikel van ene Benedek Fodor, een Hongaarse wiskundige die in een voetnoot schrijft: "Het is me niet ontgaan dat dit resultaat in strijd lijkt met een van de diepste en belangrijkste resultaten uit de topologie van de twintigste eeuw." Hij doelt hierbij op het bewijs van Andret van het Malosz-vermoeden. Hans ontvangt dit tijdschrift anoniem. Of het werk van deze Hongaarse wiskundige ook echt een weerlegging is, blijft onduidelijk. Ook onduidelijk (en spannend tot het eind) blijft of Andret zelf op de hoogte is. Onder tussen horen we kostelijke anekdotes over deze Hongaar, overduidelijk geïnspireerd door de figuur van Grigori Perelman.

Het leven van Milo Andret eindigt ontroerend. Hij wordt ernstig ziek, en in deze laatste maanden verzoent hij zich, voor zover hij daartoe in staat is, met zijn vrouw, met zijn gezin en met een liefde uit zijn jeugd. Een rivaal uit zijn PhD-tijd probeert hem nog te vernederen, met toespeeling op de gedachte dat Andret nooit iets gepresteerd heeft, omdat zijn bewijs van de Malosz op toeval zou hebben berust. Een fraai nieuw gezichtspunt, herkenbaar voor elke wiskundige. Soms gaat het inderdaad zo. Of dat voor de Malosz ook geldt, blijft natuurlijk in het ongewisse, en waarschijnlijk is er helemaal geen antwoord op de suggestie mogelijk. Wat is toeval?

Canin, nogmaals, levert een prestatie van formaat. Het enige minpuntje is het feit dat de titels van de hoofdstukken allemaal wiskundig zijn, en dat ik meestal geen relatie kon ontdekken tussen de titel en de inhoud. Dat was wat mij betreft niet nodig geweest. Ik vond de vertaling bij vlaggen misschien ook niet optimaal. Milo en Hans Andret hadden er een gewoonte van gemaakt om een gesprek te eindigen met "Fuck you dad", "Fuck you son". In de vertaling wordt dit "Val dood pap", "Val dood zoon". Niet helemaal adequaat, vind ik.

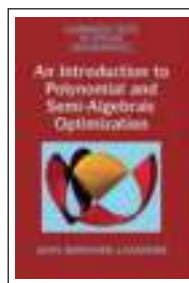
Lees *Handboek van een twijfelaar*, en word meegesleept door het genie Milo Andret, door allerlei herkenbare gebeurtenissen in de academische wereld van de wiskunde, en door het onvermogen van Milo Andret om een enigszins normaal leven te leiden.

Boekbesprekingen

| Book Reviews

Redactie: Hans Cuypers en Hans Sterk

Review Editors NAW - MF 7.092
 Faculteit Wiskunde & Informatica
 Technische Universiteit Eindhoven
 Postbus 513
 5600 MB Eindhoven
reviews@nieuwarchief.nl
www.win.tue.nl/wgreview



Jean Bernard Lasserre

An Introduction to Polynomial and Semi-Algebraic Optimization

Cambridge Texts in Applied Mathematics
 No. 52

Cambridge University Press, 2015

xii + 339 p., prijs £35.99

ISBN 9781107630697

Polynomial optimisation revolves around the problem of minimising a polynomial function over a set defined by polynomial inequalities. While this problem belongs to the well established field of nonlinear optimisation, the accent here is on finding the global minimum rather than a local minimum only. A new approach for polynomial optimisation was introduced around 2000, exploiting real algebraic properties of positive polynomials and classical results from moment theory. Jean Bernard Lasserre, a main driving force behind a whole wealth of developments in this very active research field, presents in this book a comprehensive introduction to this approach. The main objective is exposing hierarchies of tractable relaxations for the polynomial optimisation problem and discussing their properties, applications and extensions. The book is written at a level aiming to be accessible to students, engineers and non-expert researchers. It includes selected exercises and a guide to the software GloptiPoly implementing the method, and could be used as graduate text. As some of the foundational results are presented without proof the reader will need to refer to the existing literature in order to complete his/her understanding of this fascinating theory.

The book has three parts. Part I exposes relevant results from real algebraic geometry and moment theory. These are rooted in classical works by Hilbert, characterising when multivariate polynomials are sums of squares of polynomials, and by Stieltjes, characterising univariate sequences of moments of measures. The author reviews these and many recent results, giving sums-of-squares type representations for polynomials positive over basic closed semi-algebraic sets. He presents the general approach for designing hierarchies of convex relaxations, which give lower bounds converging to the global minimum of the polynomial optimisation problem. A key feature is a concrete optimality criterion (based on some rank stability condition for moment sequences) which permits to conclude that a given relaxation is exact and to compute global minimisers of the original problem. The author concludes Part I with a hierarchy of outer approximations for the cone of positive polynomials, based on the moment approach.

Part II is dedicated to the study of these hierarchies of convex relaxations for the polynomial optimisation problem. Depending on the type of positivity certificate that is used the relaxations boil down to linear or semidefinite programs, for which efficient numerical solvers exist. The author explains and analyses the advantages of the various approaches. He also draws an interesting parallel between the classical KKT conditions in continuous optimisation and the sums-of-squares certificates used in polynomial optimisation. The author goes on with addressing how to exploit sparsity or symmetry structure of the problem, how to extend the approach to the minimisation of rational or semi-algebraic func-

tions, and concludes with another use of the moment approach to get converging upper bounds that can be computed as general eigenvalue problems.

Part III presents several specialisations and extensions. In particular the author discusses properties for convex polynomial optimisation and how the approach can be applied to parametric polynomial optimisation, for finding convex under-estimators, and to problems whose feasibility region is defined by quantifiers. The book closes with a beautiful generalisation of the Löwner–John theorem, stating that for any degree d there is a unique homogeneous polynomial of degree d whose level set contains a given set K and has minimum volume. For degree 2 this level set is the celebrated minimum volume Löwner–John ellipsoid. *Monique Laurent*



Diane Maclagan, Bernd Sturmfels

Introduction to Tropical Geometry

Graduate Studies in Mathematics, Vol. 161

American Mathematical Society, 2015

363 p., prijs \$79.00

ISBN 9780821851982

Tropische meetkunde is een snel groeiend onderzoeksterrein op het snijvlak tussen polyedrale combinatoriek, algebraïsche meetkunde, rigide analytische meetkunde (Berkovichruimtes), computer-algebra en toepassingen. Het bijvoeglijk naamwoord *tropisch* is een hommage aan Imre Simon, een van oorsprong Hongaarse wiskundige in Brazilië, wiens werk aan toepassingen van de max-plus-semiring onderdeel is van de fundamenteën van het vak. Er zijn verschillende scholen in de tropische meetkunde, met verschillende interesses. Zo is Grigory Mikhalkin bekend geworden met zijn *correspondentiestelling* die het mogelijk maakt om bepaalde enumeratieve problemen uit de algebraïsche meetkunde van het volgende type in een zuiver combinatorische setting te beantwoorden: hoeveel vlakke krommen van graad d en geslacht g gaan door $3d + g - 1$ voorgeschreven punten in algemene ligging? Dat werk heeft veel navolging gevonden. Een uitstekende inleiding daartoe vormt nummer 35 uit de reeks *Oberwolfach Seminars: Tropical Algebraic Geometry* door Itenberg, Mikhalkin en Shustin.

Het boek van Maclagan en Sturmfels komt uit een andere hoek, meer gemotiveerd vanuit expliciete berekeningen. Het werd tijd dat de vele ontwikkelingen sinds begin deze eeuw in boekvorm verschenen! Het boek begint met een motiverend hoofdstuk, waarin verschillende, los van elkaar staande, gebieden beschreven worden waaruit tropische wiskunde is voortgekomen (*tropical islands*). Zo wordt een variant van Dijkstra's kortste-padalgoritme beschreven als tropische matrixvermenigvuldiging, komen tropische vlakke krommen en de correspondentiestelling kort aan bod, en passeren amoebes de revue. Een amoëbe krijg je uit een complexe algebraïsche variëteit ingebed in $\mathbb{C}^n$ door van alle coördinaten de logaritme van de absolute waarde te nemen. De amoëbe leeft dus in $\mathbb{R}^n$, en blijkt veel nuttige informatie over de variëteit te bevatten. Als je het grondtal t van de logaritme naar oneindig laat gaan, convergeert de amoëbe in Hausdorffzin naar een stuks-

gewijs lineair object — een polyedrale waaier, die de bijbehorende tropische variëteit heet. Algemener tropische variëteiten ontstaan door toe te staan dat t zelf voorkomt in de definiërende vergelijkingen — het gaat dan dus eigenlijk om eenparameterfamilies van variëteiten.

Na dit eerste, speelse hoofdstuk volgen twee hoofdstukken waarin de theorie van het *tropicaliseren* grondig opgebouwd wordt. Van deze twee is Hoofdstuk 3 zeer onderhoudend, maar dat bouwt voort op de ietwat droge theorie van Hoofdstuk 2. Ik raad lezers aan om eerst Hoofdstuk 3 te lezen en waar nodig terug te bladeren. De setting in Hoofdstuk 3 is die van een algebraïsche variëteit X ingebed in een algebraïsche torus $(K^*)^n$, waarin K een lichaam met een niet-Archimedische valuatie $v: K^* \rightarrow \mathbb{R}$ is. De tropicalisatie $\text{trop}(X) \subseteq \mathbb{R}^n$ van X wordt gedefinieerd in termen van *initiële idealen* van X — een generalisatie, uit Hoofdstuk 2, van Gröbnerbases naar een setting waarin de valuatie van K een rol speelt. Maar als K algebraïsch gesloten is en v surjectief, dan blijkt $\text{trop}(X)$ het beeld van X te zijn onder coördinaatsgewijs v toepassen. Deze *Fundamental Theorem* werd eerst door Kapranov beschreven voor het geval van hyperoppervlakken, maar voor het algemene geval zijn er verschillende foute bewijzen in de literatuur verschenen. Goed dus, dat er nu een tekstboek is waar een correct bewijs in staat. Verder wordt de Bieri–Groves-stelling bewezen, dat $\text{trop}(X)$ de drager is van een puur, eindig polyedraalcomplex van dimensie gelijk aan de Krulldimensie van X , en een stelling die zegt dat dit polyedraalcomplex gebalanceerd kan worden rond codimensie 1-polyeders. De moeilijkste stelling uit Hoofdstuk 3 zegt dat als X irreducibel is, $\text{trop}(X)$ op een sterke manier samenhangend is — het bewijs daarvan wordt echter uitgesteld tot Hoofdstuk 6.

Na Hoofdstuk 3 volgen weer twee speelse hoofdstukken met een keur aan voorbeelden waarin $\text{trop}(X)$ expliciet bepaald kan worden. Voor de Grassmannian van 2-dimensionale ruimtes van een n -dimensionale ruimte blijkt $\text{trop}(X)$ gelijk te zijn aan de parameter ruimte van alle metrische bomen met n bladeren. Het bewijs daarvan gebruikt combinatorische inzichten uit de wiskundige biologie; met name het zogenaamde *neighbour-joining algoritme*. Verder komen tropische lineaire ruimtes aan bod en hun verband met matroïden, tropische oppervlakken, tropische lineaire algebra, Hornuniformisatie en nog meer.

Hoofdstuk 6 ten slotte legt verbanden met torische meetkunde. De torus $(K^*)^n$ waar X in leeft kan op veel verschillende manieren (gedeeltelijk) gecompatificeerd worden tot een torische variëteit, en dat geeft corresponderende (gedeeltelijke) compactificaties van X en $\text{trop}(X)$. Die keuze wordt vastgelegd door een geschikte polyedrale waaier in $\mathbb{R}^n$ te kiezen. In het geval dat de valuatie v triviaal is (dat correspondeert met het nemen van de limiet van amoebes in de tweede paragraaf, zonder t als parameter toe te staan), is $\text{trop}(X)$ zelf de drager van een geschikte waaier, en ligt het dus voor de hand om zo'n waaier te nemen — X compactificeert als het ware zichzelf! Als voorbeeld wordt genoemd dat de Deligne–Mumford-compactificatie van de moduli ruimte van rationale krommen met n gemarkeerde punten op deze manier ontstaat uit een geschikte X . Verder wordt in dit hoofdstuk een alternatieve interpretatie van tropicalisatie behandeld, en eerdergenoemde stelling over samenhang bewezen.

Het boek bevat zowel voor studenten als wiskundige onderzoekers, en zowel voor hen die willen kennismaken met het vak als voor onderzoekers met meer achtergrondkennis, veel mooi

materiaal. Ik heb het boek gebruikt voor een mastervak aan de VU in Amsterdam, en stootte toen op een aantal onzorgvuldigheden. De auteurs hebben ondertussen op <http://www.ams.org/publications/authors/...books/postpub/gsm-161-errata.pdf> een lijst met errata staan.

Jan Draisma



Heinz Hanßmann

Functionaalanalyse

Epsilon Uitgaven, deel 81, 2015

xi + 245 p., prijs €28,00

ISBN 9789050411523

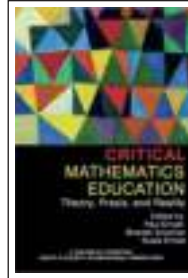
Deze uitgave in het Nederlands taalgebied vormt een rijke bron aan informatie over de gangbare onderwerpen die vallen onder de naam functionaalanalyse. Vanaf haar oorsprong rond 1900 met de Volterra-operator en integraalvergelijkingen tot de meer moderne insteek van analyse op oneindigdimensionale vectorruimten, vele onderwerpen passeren de revue. De focus ligt wel bij Banach- en Hilbertruimten en bij operatoren op deze ruimten. De omvang van het boek (het zijn college-aantekeningen bij een derdejaarsvak van de auteur aan de Universiteit Utrecht) behelst meer dan een college over dit onderwerp, in het voorwoord wordt hiervan ook gewag gemaakt. Tevens worden in een appendix geavanceerde onderwerpen (Sobolevruimten, zwakke topologieën, Von Neumann-algebra's, niet-lineaire functionaalanalyse) met een goede literatuurverwijzing genoemd. De referentielijst bij het totale boek is beperkt gehouden, geen probleem want de onderwerpen worden uitstekend aan de man gebracht. In die zin is het niet enkel een naslagwerk, maar is het ook zeer wel dienstbaar als (zelfstandig) studiemateriaal.

Het fundament onder functionaalanalyse wordt gelegd door de beroemde stellingen met de namen Hahn–Banach, Banach–Steinhaus (uniform boundedness principle) en Banach–Schauder (open mapping theorem). Waar op andere momenten (spectrum van een compacte operator) uitgebreide bewijzen worden geleverd, ontbreekt dat voor de stelling van Hahn–Banach. De schrijver verdedigt zich door te stellen dat met deze stelling “achteraf niets wordt gedaan”. Niet geheel terecht, want een (de) completering van een genormeerde ruimte wordt door hem geconstrueerd met hulp van die stelling. Veelvuldig legt de schrijver voor zijn keuzes verantwoording af, de vele verwijzingen maken het ‘doorlezen’ soms lastig, maar zijn voor het ‘doorstuderen’ plezierig. En verder trof ik in het boek (p. 1, p. 171) Cruyffiaanse uitspraken over nadelen die ook voordelen hebben, dit vind ik opmerkelijk bij het bedrijven van wiskunde (“Het nadeel dat de complexe scalaires niet geordend zijn wordt ruimschoots gecompenseerd door het voordeel dat elke vierkante matrix een complexe eigenwaarde heeft”). Om de welbekende ruimten van kwadratisch integreerbare functies te kunnen opvoeren wordt (terecht) voor de Lebesgue-integratietheorie naar de appendix verwezen.

Na enkele inleidende hoofdstukken over de topologie van metrische ruimten (inclusief de categoriestelling van Baire en de

contractiestelling van Banach), over de meetkunde van Hilbertruimten (inclusief de Stelling van Riesz), gaan hoofdstuk 6 tot en met 8 over begrensde, compacte en zelfgeadjungeerde operatoren. Hier vinden we dus de belangrijke spectraalstelling voor zelfgeadjungeerde compacte operatoren op een Hilbertruimte H . De auteur beziet in het vervolg zo’n operator als element van de Banachalgebra (C^* -algebra) van operatoren op H . De illustratie op de voorkant van het boek reflecteert naar deze zienswijze en de spectraalstelling. Overigens eindigt elk hoofdstuk met een gerichte literatuurbespreking en een collectie ‘Oefeningen’, circa dertig per hoofdstuk. Deze opgaven zijn van een zeer nuttige en niet-triviale soort, met soms een cryptische hint. In het laatste deel worden integraalvergelijkingen opgevoerd om bijvoorbeeld (via de compacte inverse Hamiltonoperator) de Schrödingervergelijking op te lossen. Het voorlaatste hoofdstuk behandelt Fredholm-operatoren, dat zijn begrensde operatoren S op een Banachruimte waarvoor $\text{index}(S) = \dim(\ker S) - \text{codim}(\text{im } S)$ een geheel getal is, of equivalent hiermee de inverteerbaarheid van de klasse van S in de Calkinalgebra van de Banachruimte. Het boek sluit af met een opdeling van het spectrum in een discreet deel, een continu deel en een rest. Na lezing van het boek heb ik alles weer op een rijtje staan voor wat de functionaalanalyse aangaat. De opgaven vormen een echte uitdaging, de literatuurverwijzing is adequaat (de ontstaansgeschiedenis daargelaten). Kortom, een mooi en degelijk handboek functionaalanalyse.

Gerard Jeurnink



Paul Ernest, Bharath Sriraman, Nuala Ernest (eds.)

Critical Mathematics Education Theory, Praxis, and Reality

Series: Cognition, Equity & Society: International Perspectives

Information Age Publishing, 2016

xii + 347 p., prijs \$39.09

ISBN 9781681232591

Voor ons ligt een boek uit de serie ‘Cognition, Equity, & Society: International Perspectives’. Dat betekent dat we te maken hebben met een boek dat de intentie heeft sociologische gedachten te presenteren met betrekking tot het onderwijs in de wiskunde. De attributen die aan de titel worden toegevoegd ‘Theory, Praxis, and Reality’, geven aan dat het boek zo mogelijk alle aspecten van het wiskundeonderwijs in de beschouwingen wil meenemen. Het boek bestaat uit 17 opstellen over het titelonderwerp, geschreven door een diversiteit van wiskundigen, pedagogen en docenten. De afgelopen dertig jaar is op het terrein van Critical Mathematics Education veel werk verzet. Vele conferenties zijn eraan gewijd, met name aan het epitheton ‘Critical’ dat prominent in de titel aanwezig is. In het vervolg van deze bespreking zal ik de afkortingen CME respectievelijk ME gebruiken voor Critical Mathematics Education, respectievelijk Mathematics Education.

Ondanks het vele werk dat inmiddels op het gebied van CME is verricht, zullen waarschijnlijk niet veel Nederlandse wiskundigen hiermee bekend zijn, daar het niet over het daadwerkelijk wiskundig metier gaat, maar over sociale achtergronden en over sociologische beschouwingen. De ‘grondaxioma’s’ van het gehele

boek worden nogal apodictisch neergezet: de wiskunde zou 'verheven' zijn en traditioneel worden gezien als de meest neutrale discipline die bestaat, het verst verwijderd van politieke en sociale discussies. Nu, zo'n dertig jaar later, zijn velen daarvan niet meer zo overtuigd en ook de CME-groep ontkent de stellingname dat wiskunde puur, objectief en waardenvrij zou zijn. Als argumenten wordt aangevoerd dat er duidelijke historische, maatschappelijke en politieke invloeden aan te wijzen zijn in de ontwikkelingsgang van de wiskunde, zowel in de toepassingen als in de vorming van concepten, methoden en bewijzen. Ook de leerprocessen binnen het wiskundeonderwijs (zowel vo, als ho en wo) zijn bepaald niet neutraal, getuige het feit dat de activiteiten binnen dat onderwijs onlosmakelijk verbonden zijn met het sociale en politieke leven. In algemene zin zijn dit in brede kring momenteel aanvaarde stellingen. Maar CME gaat een stap verder: het gaat dan over "openness, dialogicality, criticality towards received opinion, empowerment of the learner, and social/political engagement and citizenship are necessary dimensions of the teaching and learning of mathematics, if it is to contribute towards democracy and social justice". Daarbij is het ideaal dat daardoor het wiskundeonderwijs een bijdrage kan leveren aan het ontwikkelen van kritisch burgerschap, aan democratie, ja zelfs aan de wereldvrede. CME streeft naar gelijkheid en sociale rechtvaardigheid, zowel door research als door de alledaagse praktijk. Niemand zal de waarde van deze gedachten bestrijden, maar óf en h $\acute{o}$ e deze zijn te bereiken door ME/CME is natuurlijk een tweede. De 'founding fathers' van CME hebben deze gedachten al enkele decennia geleden verwoord, in het oog springt in dit verband de Braziliaanse emeritus hoogleraar Ubiratan D'Ambrosio (São Paulo). Met hem zijn er vele meer te noemen. Degene die de afgelopen dertig jaar zijn sporen op dit gebied heeft verdiend is de Deense emeritus hoogleraar Ole Skovsmose (Aalborg). Van beiden staat er een opstel in dit boek. De grondgedachten van CME hebben momenteel een behoorlijk verspreidingsgebied gekregen, zij het niet in alle uitgebreidheid en consequenties. Daarom is het goed dat dit boek is verschenen waarin het brede spectrum van CME naar voren wordt gebracht. De opstellen die in dit boek zijn opgenomen bevatten bijdragen op thema's als: de essentie van ME en CME, epistemologie en ethiek, ideologie, de hegemonie van de wiskunde, ethno-mathematics, socio-mathematics, real-life wiskunde, kapitalisme, globalisering, politiek, burgerschap en gelijkheid en dergelijke. "The outcome is a groundbreaking collection unified by a shared concern with critical perspectives of mathematics and education, and of the ways they impact on practice." Dit laatste aspect "impact on practice" blijft in de bijdragen vooralsnog tamelijk duister. Hier en daar wordt er wel aandacht aan geschonken, bijvoorbeeld door een verslag van een klasse-experiment, maar de praktische uitwerking blijft toch tamelijk rudimentair. Op schoolniveau kom je al gauw uit bij wiskunde A-achtige zaken. In het tertiair onderwijs zou je in dit verband moeten denken aan interfacultaire activiteiten en/of aan studium generale.

Kortom, een boek dat theoretisch nogal wat overhoop haalt, maar op de keper beschouwd weinig concrete handvaten geeft. Bovendien is het grondpostulaat dat de wiskunde op een verheven troon van ongenaakbare neutraliteit plaatst, niet meer de instelling van de gemiddelde wiskundige. Daarmee zeg ik niets ten nadele van de idealen van de CME-groep, integendeel, alleen w $\acute{e}$ l dat er nog heel wat moet gebeuren wil-

len we panklare ideeën hebben hoe een en ander in praktijk is te brengen. Het boek maakt niet duidelijk hoe we aan de beschreven idealen kunnen werken en tegelijkertijd een grondige training in wiskundige concepten en technieken kunnen geven. De grote diversiteit van de inhoud van de 17 bijdragen maken het ondoenlijk om een samenvattende beoordeling van ieder afzonderlijk opstel, respectievelijk van het gehele boek te geven. In ieder geval vormen de bijdragen tezamen een grondige inleiding op en samenvatting van CME. Een opsomming van de inhoud van het boek geeft in dit verband een goede indruk van het geheel:

'Mathematics: A Critical Rationality?', 'Ethnomathematics: A Response to the Changing Role of Mathematics in Society', 'Mathematics Education Ideologies and Globalization', 'Scripting the World in Mathematics and Its Ethical Implications', 'The Scope and Limits of Critical Mathematics Education', 'The Elephant in the Room: Equity, Social Class, and Mathematics', 'Connecting the Notion of Foreground in Critical Mathematics Education With the Theory of Habitus', 'The Hegemony of English Mathematics', 'School Curriculum and Different Mathematics Language Games: A Study at a Brazilian Agricultural Technical School', 'Ethnomathematics as a Human Right', 'Negotiating Critical Pedagogical Discourses Stories of Contexts', 'Mathematics and Agency', 'Critical Mathematics Education in the Context of "Real-Life Education"', 'The Role of Mathematics in Politics as an Issue for Mathematics Teaching', 'Investigating Critical Routes: The Politics of Mathematics Education and Citizenship in Capitalism', 'Are There Viable Connections Between Mathematics', 'Mathematical Proof and Democracy?', 'A Historical Analysis of Democracy in Mathematics and Mathematics Education in European Culture', 'Futures at Stake: Children's Identity Work in the Force Field of Social Valorization of School Mathematics'. *Wim Kleijne*



William P. Berlinghoff, Fernando Q. Gouvêa
vertaald door Desiree van den Bogaart en Jaenine Daems

Wortels van de Wiskunde **Een historisch overzicht voor leraren en anderen**

Epsilon Uitgaven, deel 84, 2016
x + 217 p., prijs €25,00
ISBN 9789050411561

Wortels van de Wiskunde is een voortreffelijk boek dat met veel zorg is vertaald door Desiree van den Bogaart en Jaenine Daems. Het bevat een beknopt maar helder overzicht van de geschiedenis van de wiskunde en daarnaast vijftientwintig schetsen. In die schetsen wordt de historische achtergrond van thema's als het getal nul, het rekenen met breuken, het getal π , de algebra, de kansrekening en dergelijke behandeld. De thema's zijn niet origineel maar de manier waarop het gebeurt is bijzonder geslaagd. De auteurs beschikken over de gave om ook minder overzichtelijke stukken geschiedenis van de wiskunde zoals die van de negatieve getallen en de goniometrie duidelijk en prettig op te schrijven. Het boek is zeer geschikt voor leraren en studenten, maar u kunt het zonder aarzelen aan een beroepswiskundige cadeau doen. Er is een uitgebreide literatuurlijst en de vertaalsters hebben daar een overzicht van de Nederlandse literatuur aan toegevoegd. *Teun Koetsier*

Recent verschenen publicaties. Als u een van deze boeken wilt bespreken of als u suggesties heeft voor andere boeken voor deze rubriek, laat dit dan per e-mail weten aan reviews@nieuwarchief.nl.



Remco van der Hofstad
**Random Graphs and Complex Networks
 Volume One**
 Cambridge University Press, 2017
 ISBN 9781107172876
www.cambridge.org/9781107172876



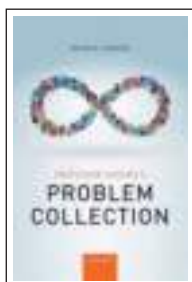
Steven J. Miller
The Probability Lifesaver
**All the Tools You Need to Understand
 Chance**
 Princeton University Press, 2017
 ISBN 9780691149554
press.princeton.edu/titles/11041.html



Abraham Arcavi, Paul Drijvers, Kaye Stacey
**The Learning and Teaching of Algebra
 Ideas, Insights and Activities**
 Routledge, 2017
 ISBN 9780415743723
www.routledge.com/9780415743723



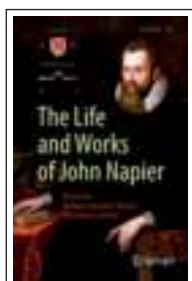
Michael Sewell
**Mathematics Masterclasses
 For Young People**
 Oxford University Press, 2017
 ISBN 9780198801214
oup.com/academic/product/9780198801214



Peter M. Higgins
Professor Higgins's Problem Collection
 Oxford University Press, 2017
 ISBN 9780198755470
oup.com/academic/product/9780198755470



Derek F. Holt, Sarah Rees, Claas E. Röver
Groups, Languages and Automata
 Cambridge University Press, 2017
 ISBN 9781316606520
www.cambridge.org/9781316606520



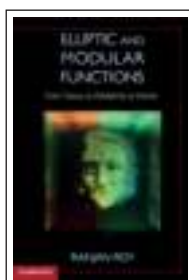
Brian Rice, Enrique Gonzalez-Velasco, Alexander Corrigan
The Life and Works of John Napier
 Springer, 2017
 ISBN 9783319532820
www.springer.com/9783319532813



Edward Barbeau
More Fallacies, Flaws, and Flimflam
 Cambridge University Press, 2017
 ISBN 9780883855805
www.cambridge.org/9780883855805



João P. Hespanha
**Noncooperative Game Theory
 An Introduction for Engineers and Computer
 Scientists**
 Princeton University Press, 2017
 ISBN 9780691175218
press.princeton.edu/titles/11047.html



Ranjan Roy
**Elliptic and Modular Functions from
 Gauss to Dedekind to Hecke**
 Cambridge University Press, 2017
 ISBN 9781107159389
www.cambridge.org/9781107159389

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. (To compete for the book token you should have a postal address in The Netherlands.)

Please send your submission by e-mail (LaTeX is preferred), including your name and address to problems@nieuwarchief.nl.

The deadline for solutions to the problems in this edition is 1 September 2017.

Problem A

Show that there are no infinite antichains for the partial order $\leq$ on $\mathbb{N}^k$ defined by $(x_1, x_2, \dots, x_k) \leq (y_1, y_2, \dots, y_k)$ iff $x_i \leq y_i$ for all i , $1 \leq i \leq k$.

Problem B

A sector is a portion of a disk enclosed by two radii and an arc. For each pair of radii, there are two complementary sectors. If the two complementary sectors have unequal area, then we say that the larger sector is the major sector.

Let S be a subset of the plane. We say that $x \in S$ is virtually isolated if x is the only element of S in a major sector of a disk centered on x . Suppose that all elements of S are virtually isolated. Prove that S is countable.



Problem C (proposed by Hendrik Lenstra)

Let n be a natural number > 1 . Suppose that for every prime $p < n$ we have that $p^n \equiv (p-1)^n + 1 \pmod{n^2}$. Prove that $n = 2$.

Edition 2016-4 We received solutions from Pieter de Groen, Alex Heinis and Toshihiro Shimizu.

Problem 2016-4/A (folklore)

For a finite sequence $s = (s_1, \dots, s_n)$ of positive integers, denote by $p(s)$ the number of ways to write s as a sum $s = \sum_{i=1}^n a_i e_i + \sum_{j=1}^{n-1} b_j (e_j + e_{j+1})$ with all a_i and b_j non-negative. Here e_i denotes the sequence of which the i -th term is 1 and of which all the other terms are 0. Show that there exists an integer $B > 1$ such that for any product F of (positive) Fibonacci numbers, there exists a finite sequence $s = (s_1, \dots, s_n)$ with all $s_i \in \{1, 2, \dots, B\}$ such that $p(s) = F$.

Solution We received solutions from Pieter de Groen, Alex Heinis and Toshihiro Shimizu. The book token goes to Pieter de Groen. The following solution is based on that of Alex Heinis.

Let $s = (s_1, \dots, s_m)$ be a finite sequence of positive integers. We say that s is *left safe* if $s_1 \geq s_2$, *right safe* if $s_m \geq s_{m-1}$, and *safe* if they are both left safe and right safe. Let $s = (s_1, \dots, s_m)$, $t = (t_1, \dots, t_n)$ be finite sequences of integers with $m, n \geq 1$. We define the *join* $s \vee t$ of s and t as the sequence $(s_1, \dots, s_{m-1}, s_m + t_1, t_2, \dots, t_n)$. Note that taking the join of sequences is associative.

Redactie:

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

Moreover, if $s = (s_1, \dots, s_m)$ is a finite sequence of positive integers, define

$$V(s) = \left\{ (a, b) \in \mathbb{Z}_{\geq 0}^n \times \mathbb{Z}_{\geq 0}^{n-1} : s = \sum_{i=1}^n a_i e_i + \sum_{j=1}^{n-1} b_j (e_j + e_{j+1}) \right\},$$

so that $\#V(s) = p(s)$, and define

$$W(s) = \left\{ b \in \mathbb{Z}_{\geq 0}^{n-1} : s \geq \sum_{j=1}^{n-1} b_j (e_j + e_{j+1}) \right\}$$

(where we take the usual partial order on the set of finite sequences of some fixed

$$b \mapsto \left(s - \sum_{j=1}^{n-1} b_j (e_j + e_{j+1}), b \right)$$

length). Then we have a bijection $V(s) \rightarrow W(s)$ given by $(a, b) \mapsto b$, with inverse , so also $\#W(s) = p(s)$. We will then show the following.

Lemma. *Let s be a right safe sequence, and let t be a left safe sequence. Then $p(s \vee t) = p(s)p(t)$.*

Proof. Write $s = (s_1, \dots, s_m)$ and $t = (t_1, \dots, t_n)$. Since for any $b \in W(s)$ and $c \in W(t)$, we have $s_m + t_1 \geq b_{m-1} + c_1$, concatenation of sequences defines a map $W(s) \times W(t) \rightarrow W(s \vee t)$. Since s is right safe, for any $d \in W(s \vee t)$, we have $s_m \geq s_{m-1} \geq d_{m-2} + d_{m-1} \geq d_{m-1}$, so we have a map $W(s \vee t) \rightarrow W(s)$ sending $(d_i)_{i=1}^{m+n-2}$ to $(d_i)_{i=1}^{m-1}$. By a similar argument, since t is left safe, we have a map $W(s \vee t) \rightarrow W(t)$ sending $(d_i)_{i=1}^{m+n-2}$ to $(d_{m-1+i})_{i=1}^{n-1}$, and therefore also a map $W(s \vee t) \rightarrow W(s) \times W(t)$, which by construction is the inverse of the concatenation map. Hence $p(s \vee t) = p(s)p(t)$. $\square$

Now we return to the problem. Let F_n be the n -th Fibonacci number, where we take as convention $F_0 = F_1 = 1$. Let $F = \prod_{i=1}^n F_{m_i}$ be a product of Fibonacci numbers. We may assume that each F_{m_i} is at least 2, that F_2 occurs at most twice (since $F_5 = 8$), and therefore that if $m_i = 2$, then $i = 1$ or $i = n$.

Let s_i denote the sequence of m_i ones; it is well-known then that $p(s_i) = F_{m_i}$ for all i . Then note that s_1 is right safe, that all s_i with $2 \leq i \leq n-1$ are of length at least 3 and safe, and that s_n is left safe. Moreover, as s_i has length 3 if $2 \leq i \leq n-1$, we see that $s_1 \vee \dots \vee s_i$ is right safe if $2 \leq i \leq n-1$. Hence inductively applying the lemma gives $p(s_1 \vee \dots \vee s_n) = \prod_{i=1}^n p(s_i) = F$, as required.

Problem 2016-4/B (folklore)

Let ℓ be a prime number. For any group homomorphism $f: A \rightarrow B$ between abelian groups and for any integer $n \geq 0$, denote by f_n the induced homomorphism $A/\ell^n A \rightarrow B/\ell^n B$. Let $(k_n)_{n=0}^\infty$ and $(c_n)_{n=0}^\infty$ be sequences of integers.

Show that there exist integers $N, a, b \geq 0$ and a group homomorphism $f: (\mathbb{Z}/\ell^N \mathbb{Z})^a \rightarrow (\mathbb{Z}/\ell^N \mathbb{Z})^b$ such that for all $n \geq 0$ we have $\#\ker f_n = \ell^{k_n}$ and $\#\operatorname{coker} f_n = \ell^{c_n}$ if and only if $k_0 = c_0 = 0$ and the sequences $(k_{n+1} - k_n)_{n=0}^\infty$ and $(c_{n+1} - c_n)_{n=0}^\infty$ are non-negative, non-increasing, eventually zero, and there is a constant C such that for all n such that $k_{n+1} - k_n$ and $c_{n+1} - c_n$ are not both zero, their difference is C .

(Recall that the *cokernel* $\operatorname{coker} f$ of a group homomorphism $f: A \rightarrow B$ between abelian groups is the quotient of B by the image of f .)

Solution We received a solution from Alex Heinis, who is also rewarded the book token for this problem. The second part of the following solution is similar to that of Alex Heinis. Write $A = (\mathbb{Z}/\ell^N \mathbb{Z})^a$ and $B = (\mathbb{Z}/\ell^N \mathbb{Z})^b$, and write $A_n = A/\ell^n A$ and $B_n = B/\ell^n B$. Moreover, for all $n \geq 0$, let $k_n = \frac{\log(\#\ker f_n)}{\log \ell}$. We show they satisfy the required properties.

For all $n \geq 0$, let $i_n = \frac{\log(\#\operatorname{im} f_n)}{\log \ell}$. Note that the quotient map $B \rightarrow B_n$ sends $\operatorname{im} f$ to $\operatorname{im} f_n$, and the induced map $\operatorname{im} f \rightarrow \operatorname{im} f_n$ is surjective with kernel $\operatorname{im} f \cap \ell^n B$. By the structure theorem for finitely generated abelian groups (and as $\operatorname{im} f$ is ℓ^N -torsion), there exist unique $t_1, \dots, t_N \geq 0$ such that $\operatorname{im} f \cong \bigoplus_{i=1}^N (\mathbb{Z}/\ell^i \mathbb{Z})^{t_i}$. Moreover, we have $\ell^n B = B[\ell^{N-n}]$ if $n \leq N$ and $\ell^n B = 0$ otherwise, so $\operatorname{im} f \cap \ell^n B = (\operatorname{im} f)[\ell^{N-n}]$ if $n \leq N$ and $\operatorname{im} f \cap \ell^n B = 0$ otherwise.

We deduce that

$$\begin{aligned} i_n &= \sum_{j=1}^N j t_j - \sum_{j=1}^N \min(j, N-n) t_j \\ &= \sum_{j=1}^N \max(j+n-N, 0) t_j = \sum_{j=N-n+1}^N (j+n-N) t_j, \end{aligned}$$

and that $i_n = \sum_{j=1}^N j t_j$ otherwise.

Therefore, for all $n \geq N$ we have $i_{n+1} - i_n = 0$. Moreover, note that $i_{n+1} - i_n = \sum_{j=N-n}^N t_j$ if $n < N$, so that $(i_{n+1} - i_n) - (i_n - i_{n-1}) = t_{N-n}$ for all $1 \leq n < N$.

First note that $k_0 = c_0 = 0$, and $k_n, c_n \geq 0$ for all $n \geq 0$ (as ℓ to that power is the order of a group). Now we use the isomorphisms $A_n / \ker f_n \rightarrow \text{im} f_n$ and $B_n / \text{im} f_n \rightarrow \text{coker} f_n$ to see that we have $k_n = \min(n, N) a - i_n$ and $c_n = \min(n, N) b - i_n$ for all n . Therefore:

– If $1 \leq n < N$, then

$$\begin{aligned} (k_{n+1} - k_n) - (k_n - k_{n-1}) &= (c_{n+1} - c_n) - (c_n - c_{n-1}) \\ &= (i_n - i_{n-1}) - (i_{n+1} - i_n) = -t_{N-n} \leq 0 \end{aligned}$$

– If $n \geq N$, then $k_{n+1} - k_n = c_{n+1} - c_n = 0$;

– Moreover, $k_N - k_{N-1} = a - i_N + i_{N-1} = a - \sum_{j=1}^N t_j$, and $c_N - c_{N-1} = b - \sum_{j=1}^N t_j$

As $\sum_{j=1}^N t_j$ is the minimum number of generators of $\text{im} f$ and A maps surjectively to $\text{im} f$, it follows that $k_N - k_{N-1} \geq 0$. As $\sum_{j=1}^N t_j$ is the dimension over $\mathbb{F}_\ell$ of $(\text{im} f)[\ell]$ and $(\text{im} f)[\ell] \subseteq B[\ell]$, it follows that $c_N - c_{N-1} \geq 0$. Therefore we see that $(k_{n+1} - k_n)_{n=0}^\infty$ and $(c_{n+1} - c_n)_{n=0}^\infty$ are non-increasing sequences that are eventually zero, hence they are non-negative as well.

Finally, note that for $n < N$, we have $(k_{n+1} - k_n) - (c_{n+1} - c_n) = a - b$, which shows that the sequences $(k_n)_{n=0}^\infty$ and $(c_n)_{n=0}^\infty$ satisfy the required conditions.

For the converse, suppose that $(k_n)_{n=0}^\infty$ and $(c_n)_{n=0}^\infty$ satisfy the conditions in the problem. Let N be the smallest integer $n \geq 0$ for which $k_{n+1} - k_n = c_{n+1} - c_n = 0$. Let for $0 \leq n < N$, $r_n = (k_n - k_{n-1}) - (k_{n+1} - k_n) = (c_n - c_{n-1}) - (c_{n+1} - c_n)$, which is non-negative as the sequences $(k_{n+1} - k_n)_{n=0}^\infty$ and $(c_{n+1} - c_n)_{n=0}^\infty$ are non-increasing. Moreover, let $s_k = k_N - k_{N-1}$ and let $s_c = c_N - c_{N-1}$. Consider the map

$$f : (\mathbb{Z}/\ell^N \mathbb{Z})^{s_k} \oplus \bigoplus_{n=1}^{N-1} (\mathbb{Z}/\ell^n \mathbb{Z})^{r_n} \rightarrow (\mathbb{Z}/\ell^N \mathbb{Z})^{s_c} \oplus \bigoplus_{n=1}^{N-1} (\mathbb{Z}/\ell^n \mathbb{Z})^{r_n}$$

of which the matrix in block form (with respect to the given splitting into summands) is the diagonal matrix with diagonal $(0_{s_c \times s_k}, \ell \cdot I_{r_1}, \ell^2 \cdot I_{r_2}, \dots, \ell^{N-1} \cdot I_{r_{N-1}})$.

A couple of observations: first note that if $n \geq N$, then $f_n = f$. Moreover, we note that for $n < N$, the induced map

$$f_n : (\mathbb{Z}/\ell^n \mathbb{Z})^{s_k} \oplus \bigoplus_{i=1}^{N-1} (\mathbb{Z}/\ell^i \mathbb{Z})^{r_i} \rightarrow (\mathbb{Z}/\ell^n \mathbb{Z})^{s_c} \oplus \bigoplus_{i=1}^{N-1} (\mathbb{Z}/\ell^i \mathbb{Z})^{r_i}$$

is given by the same matrix as the one defining f . And finally, we note that therefore $\ker f_n = \ker 0_{s_c \times s_k} \oplus \bigoplus_{i=1}^{N-1} \ker(\ell^i \cdot I_{r_i})$.

Let us show by induction on n that $\#\ker f_n = \ell^{k_n}$ and $\#\text{coker} f_n = \ell^{c_n}$ for all n . First of all, for $n = 0$, note that f_0 is the map $0 \rightarrow 0$, so $k_0 = c_0 = 0$. Now let $0 < n \leq N$, and suppose that $\#\ker f_{n-1} = \ell^{k_{n-1}}$ and $\#\text{coker} f_{n-1} = \ell^{c_{n-1}}$. Note that $\#\ker f_n = \ell^{n s_k + \sum_{i=1}^{N-1} \min(i, n) r_i}$ and that $\#\ker f_{n-1} = \ell^{(n-1) s_k + \sum_{i=1}^{N-1} \min(i, n-1) r_i}$. Therefore $\#\ker f_n / \#\ker f_{n-1} = \ell^{s_k + \sum_{i=n}^{N-1} r_i}$; by definition of s_k and the r_i , the exponent is by a telescoping sum equal to $k_n - k_{n-1}$. Hence $\#\ker f_n = \ell^{k_n - k_{n-1}} \#\ker f_{n-1} = \ell^{k_n}$. Similarly, we show that $\#\text{coker} f_n = \ell^{c_n}$.

Finally, we note that for $n > N$, we have $\#\ker f_n = \#\ker f_N = \ell^{k_N} = \ell^{k_n}$, as for all $i > N$, we have $k_{i+1} - k_i = 0$; and similarly, we have $\#\text{coker} f_n = \ell^{c_n}$.

Problem 2016-4/C (folklore)

Let R be the polynomial ring over $\mathbb{Z}$ with variables x_i, y_i, z_i for all $i \in \mathbb{Z}$. Let S be the polynomial ring over $\mathbb{Z}$ with variables t_i for all $i \in \mathbb{Z}$. Let $\tau : R \rightarrow R$ be the isomorphism of rings given by $x_i \mapsto x_{i+1}$, $y_i \mapsto y_{i+1}$ and $z_i \mapsto z_{i+1}$.

Consider the morphism $f: R \rightarrow S$ of rings given by $x_i \mapsto t_{i-1}t_it_{i+1}$, $y_i \mapsto t_i^3$ and $z_i \mapsto t_i^2$. Does there exist a finite number of elements $r_1, \dots, r_n \in R$ such that the kernel I of f is generated as an ideal in R by $\{\tau^i r_j; i \in \mathbb{Z}, j = 1, \dots, n\}$?

Solution We received no solutions for this problem. The answer is no.

We assume monomials to be monic. Moreover, we will abuse notation by setting $\tau: S \rightarrow S$ to be the automorphism of rings sending t_i to t_{i+1} for all $i \in \mathbb{Z}$. Let $M \subseteq R$ denote the set of monomials of R , and let $N \subseteq S$ denote the set of monomials of S . Then f maps M into N . Moreover, identifying (as groups) R with $\bigoplus_{m \in M} \mathbb{Z} \cdot m$ and S with $\bigoplus_{n \in N} \mathbb{Z} \cdot n$, we see that $f: R \rightarrow S$ is given by

$$\sum_{m \in M} x_m m \mapsto \sum_{n \in N} \left(\sum_{m \in f^{-1}(n)} x_m \right) n,$$

for x_m zero for all but finitely many $m \in M$. Finally, we note that for all $x \in R$, we have $f(\tau x) = \tau f(x)$.

Let, for $x = \sum_{m \in M} x_m m \in R$ and $n \in N$, the n -th homogeneous part be $x_n = \sum_{m \in f^{-1}(n)} x_m m$. Then note that $x \in I$, if and only if for all $n \in N$, we have $x_n \in I$, and $x = \sum_{n \in N} x_n$, where we note that x_n is zero for all but finitely many $n \in N$, as the same is true for the x_m for $m \in M$. So let us say that an element of the form $\sum_{m \in f^{-1}(n)} x_m m$ in R is *homogeneous with respect to n* .

Write $R_n = \bigoplus_{m \in f^{-1}(n)} \mathbb{Z} \cdot m$. Then note that $f|_{R_n}$ is injective if and only if $\#f^{-1}(n) \leq 1$. So consider the set $N' \subseteq N$ of $n \in N$ such that $\#f^{-1}(n) \geq 2$, where we take the partial order on N given by divisibility by an element of $f(M)$, i.e. $n \leq n'$ if there exists an $m \in M$ such that $nf(m) = n'$.

Define, for integers $k \geq 1$ and i , the monomial $n_{k,i} = t_i^3 t_{i+1} t_{i+2} \cdots t_{i+3k-1} t_{i+3k}^3$. We determine $f^{-1}(n_{k,i})$. Let $m \in f^{-1}(n_{k,i})$. Since n only has two exponents of at least 2, we see that the total y, z -degree of m is at most 2. Moreover, the degree of n is $3k+5$, so comparing degrees modulo 3, we see that m must be divisible by either $y_i z_{i+3k}$ or $y_{i+3k} z_i$. In the first case, write $m = m' y_i z_{i+3k}$, and note that $f(m') = t_{i+1} \cdots t_{i+3k}$. By induction on k , one can show that m' must be equal to $x_{i+2} x_{i+5} \cdots x_{i+3k-1}$, therefore m must be $m_{k,i,1} = x_{i+2} x_{i+5} \cdots x_{i+3k-1} y_i z_{i+3k}$. In the same way, one shows in the second case that m must be equal to $m_{k,i,2} = x_{i+1} x_{i+4} \cdots x_{i+3k-2} y_{i+3k} z_i$. Since both of them do map to $n_{k,i}$, we find that $f^{-1}(n_{k,i}) = \{m_{k,i,1}, m_{k,i,2}\}$. In particular, $n_{k,i} \in N'$, and $\ker f|_{R_{n_{k,i}}}$ is generated by $m_{k,i,1} - m_{k,i,2}$.

Moreover, $n_{k,i}$ is minimal in N' ; if $n \in N'$ divides $n_{k,i}$ in $f(M)$, then for $m_1, m_2, m' \in M$ such that $m_1 \neq m_2$, $f(m_1) = f(m_2) = n$ and $f(m_1)f(m') = f(m_2)f(m') = n_{k,i}$, we have $\{m_1 m', m_2 m'\} = \{m_{k,i,1}, m_{k,i,2}\}$. Since $\gcd(m_{k,i,1}, m_{k,i,2}) = 1$, it follows that $m' = 1$ and therefore that $n = n_{k,i}$.

Now we can prove our answer. Let G be any subset of $R - \{0\}$ such that I is generated by $\{\tau^a g; a \in \mathbb{Z}, g \in G\}$. We show that G is infinite. Let G' denote the set of non-zero homogeneous parts of elements of G , and note that G is finite if and only if G' is. Then I is also generated by $\{\tau^a g'; a \in \mathbb{Z}, g' \in G'\}$.

Note that for all $k \geq 1$, we have $m_{k,0,1} - m_{k,0,2} \in I$, and write $m_{k,0,1} - m_{k,0,2} = \sum_{a,g'} \alpha_{a,g'} \tau^a g'$, for some $\alpha_{a,b} \in R$ that are zero for all but finitely many pairs (a,b) ; we may assume that the $\alpha_{a,b}$ are homogeneous, by taking the $n_{k,0}$ -th homogeneous part of this identity if necessary. If (a,g') is such that $\alpha_{a,g'} \neq 0$, and if g' is homogeneous with respect to n , then $\tau^a n \in N'$ and $\tau^a n \leq n_{k,0}$, so by minimality of $n_{k,0}$ it follows that $\tau^a n = n_{k,0}$. Moreover, $\ker f|_{R_{n_{k,0}}}$ is generated by $m_{k,0,1} - m_{k,0,2}$, so $\tau^a g'$ is a non-zero integer multiple of $m_{k,i,1} - m_{k,i,2}$. It follows that for any $k \geq 1$ there exists $g'_k \in G'$ such that g'_k is a non-zero integer multiple of $\tau^a (m_{k,0,1} - m_{k,0,2})$ for some $a \in \mathbb{Z}$. Now τ preserves total degrees, so the total degree of g'_k is that of $m_{k,0,1}$ and $m_{k,0,2}$, which is $k+2$. In particular, G' contains elements of every total degree that is at least 3, so G' (and therefore G) is infinite, as desired.

Rectification

In the list of solvers of 2016-3/B, Rob van der Waall was missing, but should have been there. We apologise for this omission.