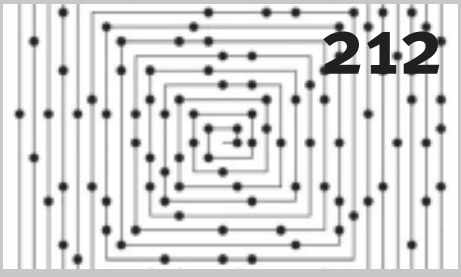
Inhoud | Contents

Artikelen | Features

Rubrieken | Departments

Uitgelicht



Op het KWG Wintersymposium 2021 spraken Lola Thompson en Pieter Moree beiden over priemsprongen.

```
theorem (n : ℕ) : ∃ p > n, p.prime :=
begin
  let N := n! + 1,
  let p := nat.min_fac N,
  have : n! > 0 := by library_search,
  have : N > 1 := by library_search,
  have : N ≠ 1 := by library_search,
  have : p.prime := by library_search,
  have : p > n,
  { by_contra' : p ≤ n,
    have : ¬p | 1 := by library_search,
```

231

Johan Commelin beschrijft wat het Liquid Tensor Ecperiment inhoudt.

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

Hoofdredactie
Raf Bocklandt (r.r.j.bocklandt@uva.nl)
Robbert Fokkink (r.j.fokkink@tudelft.nl)

Eindredactie/Bladmanager
Fred Drissen (fred@nieuwarchief.nl)

Redactie
Francesca Arici (UL), Viktor Blåsjö (UU), Hans Cuypers (TU/e), Teun Koetsier (VU), Nikki Levering (UvA), Daan Mulder, Nicolaos Starreveld (UvA), Clara Stegehuis (UT), Hans Sterk (TU/e), Mark Timmer (UT)

Problemenrubriek (problems@nieuwarchief.nl)
Onno Berrevoets en Daan van Gent

Bureauredactie
Anne van Grinsven

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 beoefenaren van de wiskunde. In 1778 opgericht onder de zinspreuk: 'Een onvermoeide arbeid komt alles te boven' is het 's werelds oudste nationale wiskundegenootschap. Leden ontvangen het Nieuw Archief voor Wiskunde als onderdeel van hun lidmaatschap.

Bestuur
Barry Koren (TU/e, voorzitter), Wioletta Ruszel (TUD, penningmeester), Willem Jan Palenstijn (CWI, secretaris), Danny Beckers (VU), Rogier Bos (UU), Marie-Colette van Lieshout (CWI), Michael Müger (RU), Alef Sterk (RUG), Jan Wiegerinck (UvA).

Secretariaat
Koninklijk Wiskundig Genootschap, CWI
Postbus 94079, 1090 GB Amsterdam
wiskgenoot@wiskgenoot.nl

Ledenadministratie KWG / Abonnementen
admin@wiskgenoot.nl, tel. 020-5924008
Wijzigingen of opzegging kunt u ook doorgeven door in te loggen op www.wiskgenoot.nl.

Contributie
Tarieven per jaar (bij betaling per automatische incasso krijgt u € 2,50 korting):
– gewoon lid: € 97,50
– reciprociteitslid: € 77,50
– gepensioneerden en werklozen: € 52,50
– aio's, oio's, studenten: € 42,50 (max. 4 jaar)
– lid zonder Nieuw Archief: € 57,50
Studenten en pas afgestudeerden kunnen een jaar lang gratis lid worden.
Voor verzending van het Nieuw Archief naar het buitenland wordt een portotoeslag van € 10 in rekening gebracht.
Instituten in Nederland en buitenland kunnen zich abonneren op het Nieuw Archief voor Wiskunde voor € 105 (Nederland), € 115 (Europa) of € 117,50 (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 € 77,50 instead of the full membership fee of € 97,50 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@cwi.nl

Informatie voor auteurs

Kopij
Kopij dient per e-mail te worden aangeboden aan kopij@nieuwarchief.nl. Voor meer informatie en auteursinstructies zie www.nieuwarchief.nl.

Volgende nummers

nummer	*maand verschijnen*	*deadline kopij*
23(1)	maart 2022	verstreken
23(2)	juni 2022	01-02-2022
23(3)	september 2022	01-05-2022
23(4)	december 2022	01-08-2022

Instituuts- en bedrijfsleden

De publicaties van het KWG worden mede mogelijk gemaakt door de bijdragen van de volgende instituten en bedrijven.

Centrum Wiskunde & Informatica
Universiteit van Amsterdam
Vrije Universiteit Amsterdam
Rijksuniversiteit Groningen
Universiteit Leiden
Radboud Universiteit Nijmegen
Universiteit Utrecht
Technische Universiteit Delft
Technische Universiteit Eindhoven
Universiteit Twente

Elsevier
ORTEC

Op het omslag

De meer dan honderd jaar oude stalen spoorbrug in Lethbridge (Alberta) over de Oldman River is in zijn soort de langste ter wereld. Meer over stangenconstructies is te lezen in het verslag van de Vakantiecursus die dit jaar 75 bestond en als thema 'Stangenmeetkunde' had, zie pagina 209.

Onverwachte implicaties

"Heb je wel gedacht aan de gevolgen?" vroeg mijn vrouw. Daar was ik inderdaad mee bezig. Mijn oudste dochter is dit jaar gestart in de middelbare school en had haar eerste toets wiskunde achter de rug. Een van de onderwerpen op het menu was de introductie van een aantal wiskundige symbolen, waaronder de implicatiepijl. Om dit te testen kreeg ze op de toets de volgende vraag.

Vul aan: $3|x$ en $5|x \Rightarrow \cdots$

Een duidelijke vraag met een voor de hand liggend antwoord, ware het niet dat mijn dochter '$1|x$' had ingevuld. Technisch gezien correct, maar helaas volgens de juf geen punten waard. "Moeten we daar niet iets over zeggen", opperde ik. Maar ja, is het wel verstandig om in de eerste maanden op een nieuwe school al een reputatie op te bouwen als wiskundige wijsneus?

Terwijl dit dilemma voor me opdook, dwaalden mijn gedachten af. Voor Nieuw Archief was er namelijk net een bijdrage binnengekomen over *automated proof checking*. In dat artikel, dat u in dit nummer kan lezen, vertelt Johan Commelin over het Liquid Tensor Project. Dit project is opgezet om een stelling van Peter Scholze te checken met behulp van het software-pakket Lean. De reden hiervoor is dat Scholze zichzelf niet honderd procent zeker voelt over zijn bewijs, en er eigenlijk niemand anders voldoende overzicht heeft op hoe alle puzzelstukjes precies in elkaar vallen.

Lean is een programmeertaal waarin je bewijzen kan formaliseren en checken. Als het Liquid Tensor Project erin slaagt het bewijs te implementeren, dan biedt het resultaat van Scholze heel wat toepassingen in verschillende vakgebieden uit de topologie, analyse en algebraïsche meetkunde. Maar hoe moeilijk zou zo'n implementatie zijn? Om de proef op de som te nemen, bedacht ik dat ik zelf iets in Lean zou kunnen programmeren. Ik zou bijvoorbeeld het antwoord van mijn dochter en dat van de juf kunnen checken in Lean. Mijn vermoeden was dat dat van mijn dochter zonder problemen zou passeren maar dat van de juf niet omdat dat immers impliciet gebruikmaakt van de Chinese reststelling.

Aan de slag dus. Ik opende een online emulator met tutorial en begon me de syntax van deze computertaal eigen te maken. Dat bleek niet zo evident en enkele uren later was ik nog niet veel verder geraakt dan een bewijs dat de som van twee even getallen even is. Mijn bewondering voor Johan en zijn collega's steeg met de minuut.

"Ben je er al uit?" vroeg mijn vrouw. "Nee", antwoordde ik, "en dat zal nog wel even duren…."

Raf Bocklandt, hoofdredacteur
Korteweg-de Vries Instituut, Universiteit van Amsterdam

Agenda

| Upcoming Events

december 2021

9 december 2021
❑ **Workshop: OR in Waste Management**
Online workshop, georganiseerd door Remy Spliet (Erasmus Universiteit) en Sanne Wøhlk (Aarhus University).
plaats *online*
info *econ.au.dk*

13–17 december 2021
❑ **The Future of Mendelian Randomization Studies 2021**
Lorentz workshop, mede georganiseerd door Sonja Swanson (Erasmus MC).
plaats *online*
info *lorentzcenter.nl*

januari 2022

15 januari 2022
❑ **Wintersymposium KWG**
Jaarlijks symposium van het KWG. Dit jaar is het thema 'Zwarte gaten' met lezingen van Tanja Hinderer (UU), Klaas Landsman (RU), Jeroen van Dongen (UvA) en Simon Portegies Zwart (UL).
plaats *Academiegebouw, Utrecht*
info *wiskgenoot.nl*

17–19 januari 2022
❑ **LNMB-conferentie**
Conferentie over de wiskunde van besliskunde georganiseerd door het Landelijk Netwerk Mathematische Besliskunde (LNMB).
plaats *Congrescentrum De Werelt, Lunteren*
info *lnmb.nl*

17–27 januari 2022
❑ **Eerste ronde Nederlandse Wiskunde Olympiade**
De eerste ronde van de jaarlijkse landelijke wiskundewedstrijd voor leerlingen uit de onderbouw van het havo en het vwo.
plaats *op eigen school*
info *wiskundeolympiade.nl*

20–21 januari 2022
❑ **40e Panama-conferentie**
Conferentie met jubileumthema '40 x Panama: verleden, heden en toekomst'.
plaats *Zeist*
info *panamaconferentie.sites.uu.nl*

24–26 januari 2022
❑ **Winter School Mathematical Finance**
Winterschool over financiële wiskunde met onder andere minicursussen van Jan Obloj (Oxford) en Gilles Pagès (Paris Diderot).
plaats *Congrescentrum De Werelt, Lunteren*
info *staff.fnwi.uva.nl/p.j.c.spreij/winterschool/winterschool.html*

24–28 januari 2022
❑ **Study Group Mathematics with Industry**
Jaarlijkse studiegroep waarin wiskunde en industrie samen problemen oplossen, dit jaar georganiseerd door Universiteit Twente.
plaats *Universiteit Twente*
info *swi-wiskunde.nl*

28–29 januari 2022
❑ **Nationale Wiskunde Dagen**
28ste editie van de tweedaagse conferentie voor wiskundeleraren.
plaats *Noordwijkerhout*
info *uu.nl/onderwijs/nationale-wiskunde-dagen*

31 januari – 4 februari 2022
❑ **Post-Quantum Cryptography for Embedded Systems**
Lorentz workshop, mede georganiseerd door Tanja Lange, Andreas Hülsing (TU/e) en Simona Samardjiska (RU).
plaats *Lorentz Center@Oort, Leiden*
info *lorentzcenter.nl*

februari 2022

16 februari 2022
❑ **OnderbouwWiskundeDag**
Competitie voor leerlingen uit 3 havo/vwo. In teams wordt gedurende een dag aan een grote wiskundige (denk)opdracht gewerkt, waarin probleemoplossen centraal staat.
plaats *eigen school*
info *wiskundeinteams.sites.uu.nl*

Suggesties voor deze agenda zijn welkom.
Redacteur: Nikki Levering
agenda@nieuwarchief.nl

28 februari – 4 maart 2022

❑ **Machine-Checked Mathematics**

Lorentz workshop, mede georganiseerd door Sander Dahmen en Robert Lewis (VU).

plaats *Lorentz Center@Oort, Leiden*

info *lorentzcenter.nl*

maart 2022

9 maart 2022

❑ **Rekenconferentie Kennispunt taal en rekenen MBO**

Rekenconferentie met als doel het kennisdelen rondom rekenen in het algemeen en de invoering van de nieuwe rekeneisen.

plaats *nog te bepalen*

info *elbd.sites.uu.nl*

11 maart 2022

❑ **Tweede ronde Nederlandse Wiskunde Olympiade**

De tweede ronde van de Nederlandse Wiskunde Olympiade speelt zich af op de universiteiten.

plaats *universiteiten van Nederland*

info *wiskundeolympiade.nl*

11 maart 2022

❑ **Onderwijs meets onderzoek**

Symposium waarbij wiskundedocenten en onderzoekers in wiskunde educatie kijken naar de vraag wat educatie zelf en het onderzoek naar educatie voor elkaar kunnen betekenen.

plaats *Domstad, Utrecht*

info *nvvw.nl*

17 maart 2022

❑ **W4 Kangoeroe**

WereldWijdeWiskundeWedstrijd voor basis- en middelbare scholieren.

plaats *op eigen scholen*

info *w4kangoeroe.nl*

18 maart 2022

❑ **Finaleweekend Wiskunde A-lympiade**

Teams uit Nederland, Duitsland, Denemarken, Kroatië en Japan werken aan een opdracht tijdens een tweedaags verblijf op de Veluwe.

plaats *Garderen*

info *wiskundeinteams.sites.uu.nl*

24 maart 2022

❑ **Prijsuitreiking Wiskunde B-dag 2021**

Feestelijke bekendmaking top 10 deelnemende teams Wiskunde B-dag.

plaats *Academiegebouw, Utrecht*

info *wiskundeinteams.sites.uu.nl*

25 maart 2022

❑ **Nationale Rekencoördinator Dag**

Dag voor rekencoördinatoren en leerkrachten, waarop het rekenonderwijs van de basisschool centraal staat.

plaats *Utrecht*

info *nrcd.sites.uu.nl*

30 maart 2022

❑ **Grote Rekendag**

Dag voor alle basisscholen in Nederland en Vlaanderen (groep 1 t/m 8) die helemaal in het teken staat van rekenen.

plaats *basisscholen Nederland en Vlaanderen*

info *groterekendag.nl*

april 2022

6–12 april 2022

❑ **European Girls' Mathematical Olympiad**

Europese wiskundewedstrijd speciaal voor meisjes.

plaats *Eger, Hongarije*

info *egmo.org*

8 april 2022

❑ **NVORWO Jaarvergadering en Studiedag**

Jaarvergadering van de Nederlandse Vereniging tot Ontwikkeling van het Reken/Wiskunde Onderwijs (NVORWO).

plaats *nog te bepalen*

info *elbd.sites.uu.nl*

11–14 april 2022

❑ **International Conference on Multilevel Analysis**

Tweejaarlijks congres, met lezingen van George Leckie (University of Bristol) en Terrence D. Jorgensen (UvA).

plaats *Utrecht*

info *multilevel.fss.uu.nl*

mei 2022

13 mei 2022

❑ **ELWIeR-Ecent Conferentie en Symposium**

Conferentie met als thema het Bèta-onderwijs in Nederland van 1971–2021–2071. Dit jaar zal aansluitend het symposium '100 jaar bèta-didactiek' worden georganiseerd.

plaats *nog te bepalen*

info *uu.nl*

30 mei – 3 juni 2022

❑ **Noncommutative Geometry Along the North Sea 2022**

Lorentz workshop, mede georganiseerd door Bram Mesland (UL) en Walter Daniel van Suijlekom (RU).

plaats *Lorentz Center@Snellius, Leiden*

info *lorentzcenter.nl*

30 mei – 3 juni 2022

❑ **Benchmarked: Optimization Meets Machine Learning 2022**

Lorentz workshop, mede georganiseerd door Joaquin Vanschoren (TU/e) en Mike Preuss (UL).

plaats *Lorentz Center@Oort, Leiden*

info *lorentzcenter.nl*

juli 2022

4–8 juli 2022

❑ **Current Debates in Forensic Statistics 2022**

Lorentz workshop, mede georganiseerd door Ronald Meester (VU), Klaas Slooten (VU, NFI) en Anne Ruth Mackor (RUG).

plaats *Lorentz Center@Oort, Leiden*

info *lorentzcenter.nl*

6–16 juli 2022

❑ **International Mathematical Olympiad (IMO)**

Internationale wiskundecompetitie voor middelbare scholieren, dit jaar in Noorwegen.

plaats *Oslo, Noorwegen*

info *imo2022.org*

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: Nikki Levering

nieuws@nieuwarchief.nl

Constance van Eeden overleden

Constance van Eeden (Delft, 1927), wereldberoemd onderzoeker in de verdelingsvrije statistiek en besliskunde, is op 21 september jongstleden overleden. Van Eeden was een van de eerste vrouwelijke wetenschappers van het Mathematisch Centrum in Amsterdam (nu CWI), waar zij met David van Dantzig en Jan Hemelrijk werkte. Zij was tevens de eerste vrouw in Nederland die promoveerde in de statistiek (cum laude, 1958), en zou 29 jaar lang ook de enige blijven. Van Eeden heeft vele jaren in Canada gewerkt, en speelde een grote rol in de ontwikkeling van de statistiek in Franstalig Canada. In 1990 ontving zij dan ook de Gold Medal van de Statistical Society of Canada, en in 2011 het erelidmaatschap van dit genootschap. Verder was Van Eeden ook Fellow van de American Statistical Association en Fellow van het Institute of Mathematical Statistics, die haar in 1999 de Henri Willem Methorst Medal toekende. Ter ere van Van Eeden heeft het CWI het Constance van Eeden PhD Fellowship-programma opgezet voor getalenteerde vrouwelijke PhD-studenten, welke elke twee jaar zal worden toegekend. *cwi.nl, vvsor.nl*

Foto: Peter Macdonald

Constance van Eeden

Wil Schilders nieuwe president ICIAM

Prof. dr. Wil Schilders (TU/e) is gekozen als volgende president van The International Council for Industrial and Applied Mathematics (ICIAM). Op 30 september is zijn termijn als President-Elect begonnen. De positie van President zal Schilders vanaf 2023 op zich nemen. ICIAM is een wereldwijde organisatie die zich inzet voor de vooruitgang van wiskundige toepassingen over de hele wereld. Zij organiseert ook elke vier jaar het International Congress on Industrial and Applied Mathematics, met meer dan 4000 deelnemers. Tijdens dit congres worden onder andere de prestigieuze Lagrange-, Maxwell- en Collatz-prijzen uitgereikt.

Schilders was eerder al President van het European Consortium for Mathematics in Industry, en is ook een van de oprichters en de huidige President van EU-MATHS-IN. Daarnaast is Schilders momenteel ook directeur van Platform Wiskunde Nederland.

platformwiskunde.nl, tue.nl

Maximale score bij Nederlandse Wiskunde Olympiade

Casper Madlener, een zesdeklasser uit Hoofddorp, heeft de Nederlandse Wiskunde Olympiade gewonnen. Hij behaalde als enige in alle drie de rondes alle punten en had zo een perfecte score. In de categorie 'Klas 5' ging Hylke Hoogeveen uit Odijk met de winst aan de haal, in de categorie 'Klas 4 en lager' was de winst voor Allie Zong uit Veldhoven. Zowel Casper, Hylke als Allie was in een van de voorgaande edities van de Olympiade ook prijswinnaar. Daarnaast heeft Hylke afgelopen schooljaar een bronzen medaille gewonnen bij de Internationale Wiskunde Olympiade, en Allie een bronzen medaille bij de European Girls' Mathematical Olympiad. De drie winnaars zullen nu, samen met de rest van de top-5 scholieren per categorie en veertien veelbelovende deelnemers van de Olympiade, een uitdagend trainingsprogramma volgen ter voorbereiding op de selectietoetsen die bepalen wie Nederland mag vertegenwoordigen op internationale Olympiades. *wiskundeolympiade.nl*

Daniel Gomon schrijft beste Masterscriptie Toegepaste Wiskunde

Tijdens de eerste editie van het Dutch Mathematics Community event afgelopen september is de Best Thesis in Applied Math Award 2021 uitgereikt aan Daniel Gomon (UL). In zijn scriptie, getiteld *Continuous time control charts: generalizations and an application to the Dutch Arthroplasty Register (LROI)*, analyseert en ontwikkelt Daniel verschillende methoden voor het vroeg identificeren van kwaliteitsproblemen bij transplantatiechirurgie. Zijn methoden, die problemen vijftien maanden eerder kunnen herkennen, zullen door de Landelijke Registratie Orthopedische Implantaten geïmplementeerd worden. Naast Daniel waren er twee andere finalisten. Irene Kuin (UT) schreef een masterscriptie over het optimaal roosteren van rechtszaken. De door haar ontwikkelde methoden zijn veelbelovend, en er zijn dan ook twee PhD-posities gecreëerd om dit onderzoek verder uit te breiden. Maaike Vollebergh (TUD) heeft in haar scriptie gekeken naar de planning van de Nederlandse Spoorwegen. Zij heeft aangetoond dat deze planning niet optimaal is, en heeft zelf dan ook een nieuwe en flexibele methode geïntroduceerd die deze planning kan verbeteren. *platformwiskunde.nl*

IMU viert 100-jarig bestaan

De International Mathematical Union (IMU) heeft afgelopen september haar 100-jarig bestaan gevierd met de conferentie 'Mathematics without borders'. De viering vond plaats op haar 101ste verjaardag, gezien deze vorig jaar vanwege coronarestricties niet door kon gaan. De conferentie had een hybride vorm, zodat geïnteresseerden van over de hele wereld deel konden nemen, waarbij het offline gedeelte plaatsvond op het Palais Universitaire in Straatsburg, Frankrijk, daar waar het in 1920 ook allemaal begon.

Het doel van de IMU is om wiskundige samenwerking te promoten, en de IMU ondersteunt dan ook alle internationale activiteiten die bijdragen aan de ontwikkeling van wiskunde. Vroeger was dit anders: bij de oprichting, in de nasleep van de Eerste Wereldoorlog, werden de landen die als de verliezers van deze oorlog werden beschouwd buitengesloten van het wetenschapsveld. Dit leidde tot weinig succes, en in 1932 werd de stekker eruit getrokken. De huidige opzet van de IMU dateert uit 1952, tot stand gekomen onder leiding van de Amerikaan Marshall Stone. Tegenwoordig zijn meer dan 90 landen lid van de IMU, en wordt onder andere samengewerkt met het Committee for Women in Mathematics om de genderkloof te verkleinen, en met het Committee for Developing Countries om wiskunde in ontwikkelingslanden te ondersteunen. Iedere vier jaar organiseert de IMU het International Congress of Mathematicians (ICM), de grootste conferentie binnen het vakgebied wiskunde, waar de Fieldsmedaille wordt uitgereikt. De komende ICM zal in 2022 plaatsvinden in St. Petersburg, Rusland, waar ook een nieuwe medaille zal worden uitgereikt. Deze medaille is vernoemd naar Russisch wiskundige Olga Aleksandrovna Ladyzhenskaya, die volgend jaar de leeftijd van 100 zou hebben bereikt. De prijs eert werk in de wiskundige fysica, en zal de eerste IMU-prijs zijn die vernoemd is naar een vrouw. *Marianne Freiberger, Rachel Thomas, plus.maths.org*

Koninklijke Onderscheiding Ton Koonen

Voorafgaand aan zijn afscheidsrede, tijdens het symposium 'Optical Networks', heeft professor Ton Koonen een Koninklijke Onderscheiding ontvangen in de graad van Ridder in de Orde van de Nederlandse Leeuw. Koonen was twintig jaar lang werkzaam aan de Technische Universiteit Eindhoven, waar hij naast het hoogleraarschap de functie van vice-decaan binnen de Faculteit Electrical Engineering bekleedde. Daarnaast was Koonen ook wetenschappelijk directeur van het Institute for Photonic Integration. Koonen is van grote invloed geweest op de wereldwijde ontwikkeling van de breedbandtechnologie en heeft zich internationaal onderscheiden met onderzoek naar breedband-glasvezel en aansluitnetwerken. Zijn onderzoek heeft tot vele innovaties geleid die erop gericht zijn meer uit de potentie van het gebruik van glasvezel te halen. Vanwege de impact en kwaliteit van zijn werk heeft Koonen eerder onderscheidingen als Bell Labs Fellow, OSA Fellow en IEEE Fellow ontvangen. *networkpages.nl, tue.nl*

Foto: PhotOdette

Ton Koonen met zijn vrouw Annemie

Functie Plimpton 322 ontdekt

Plimpton 322 is een gebroken kleitablet, bezaaid met markeringen in spijkerschrift. Het tablet stamt uit de periode van het oude Babylonië, een gemeenschap die tussen 2500 en 500 v. Chr. in

Mesopotamië leefde. Daniel Mansfield van de Universiteit van New South Wales, Sydney, houdt zich al jaren bezig met een studie naar Plimpton 322. Samen met N.J. Wildberger, onderzoeker aan dezelfde universiteit, ontcijferde hij een aantal jaar geleden de tekst van het tablet. Ze ontdekten dat er pythagorese drietallen opstaan, wat Plimpton 322 de oudste bekende trigonometrische tabel ter wereld maakt. Lange tijd was het onduidelijk waar de Babyloniërs deze drietallen voor gebruikten. Mansfield denkt dat antwoord nu echter gevonden te hebben, hierbij geholpen door een tweede kleitablet, de Si.427. Dit tablet is in 1894 opgegraven in Irak, en zou door een landmeter zijn gebruikt om de grond in eerlijke stukken te delen door het op te splitsen in rechthoeken. Het kleitablet staat dan ook vol met verschillende rechthoekige driehoeken en rechthoeken. Opvallend is dat deze rechthoeken perfect zijn, wat Mansfield wijdt aan gebruik van pythagorese drietallen. Zijn vermoeden is dan ook dat het systematisch onderzoek naar deze drietallen, zoals op het Plimpton 322 tablet is weergegeven, aangezet is door de moeilijkheden van de landmeters in het oude Babylonië. Zijn bevindingen zijn gepubliceerd in 'Plimpton 322: A Study of Rectangles' in *Foundations of Science*. *newscientist.nl*

Foto: UNSW Sydney

Christiaan Huygensprijs voor Didier Nibbering

Sinds 1998 wordt door de KNAW jaarlijks de Christiaan Huygens Wetenschapsprijs uitgereikt. Deze prijs bekroont een jonge onderzoeker die met het proefschrift een innovatieve bijdrage in zijn/haar vakgebied levert. Elk jaar staat er een ander vakgebied centraal, en in 2021 is dat wiskunde (in het bijzonder actuariaat en econometrie). Uit drie nominaties werd door de jury het proefschrift *The Gains from Dimensionality* van Didier Nibbering, geschreven aan de Erasmus Universiteit Rotterdam, tot winnaar uitgeroepen. De jury looft de actualiteit van de behandelende onderwerpen, en de relevantie en interessante toepassingen die Nibbering laat zien. *eur.nl, christiaanhuygensprijs.nl*

Van Wijngaarden Award voor Susan A. Murphy

Iedere vijf jaar reikt het CWI de Van Wijngaarden Awards uit aan een wiskundige en een computerwetenschapper die speciale bijdragen hebben geleverd aan hun vakgebied. De awards zijn vernoemd naar wiskundige Adriaan van Wijngaarden, die beschouwd wordt als een van de grondleggers van de computerwetenschap in Nederland. Van Wijngaarden was bijna twintig jaar lang directeur van de voorloper van het CWI, het Mathematisch Centrum.

Dit jaar werden de awards voor de vierde keer uitgereikt. In de categorie computerwetenschappen ging de award naar Professor Marta Kwiatkowska van de Universiteit van Oxford. In de categorie wiskunde is De Van Wijngaarden Award 2021 ontvangen door professor Susan A. Murphy van de Harvard-universiteit. Haar onderzoek focust zich op het verbeteren van sequentiële en geïndividualiseerde beslissingen in de gezondheidszorg. Ze leidde de ontwikkeling van een nieuw type sequentiële proef die nu wordt ingezet in meerdere medische gebieden, waaronder de behandeling van verschillende chronische ziekten en verslavingsstoornissen. Eerder ontving Murphy al een MacArthur Fellowship en de Royal Statistical Society Guy Medal in Silver. Murphy was President van het Institute of Mathematical Statistics en de Bernoulli Society for Mathematical Statistics and Probability. *cwi.nl*

Koninklijk Wiskundig Genootschap

❑ **Wijziging statuten**

Op de Algemene Ledenvergadering van 6 april 2021 is een commissie ingesteld om naar de vigerende statuten te kijken. De commissie heeft een eventuele lichte herziening van de statuten voorgesteld, maar is van mening dat deze herziening niet noodzakelijk is en dat sommige afspraken beter in een gemakkelijker aan te passen huishoudelijk reglement kunnen worden vastgelegd. Zie wiskgenoot.nl voor meer informatie en waar de documenten te vinden zijn. Reageren op het voorstel of zelf wijzigingen voorstellen kan tot 5 januari 2022.

❑ **KWG Wintersymposium 2022**

Het jaarlijkse Wintersymposium voor docenten en andere geïnteresseerden vindt plaats op zaterdag 15 januari 2022 in het Academiegebouw in Utrecht. Het thema is 'Zwarte gaten'. Voor meer informatie en het programma zie wiskgenoot.nl.

❑ **Symposium Ietje Paalman-de Miranda**

Op 18 juni 2022 zal in de aula van de Universiteit van Amsterdam een eendaags symposium worden georganiseerd ter nagedachtenis van professor Aïda Paalman-de Miranda. Gedurende haar carrière was zij een inspirerende wetenschapper met hart voor onderwijs en zeer betrokken bij de begeleiding van studenten. Zij overleed in 2020 op 84-jarige leeftijd. Haar bijzondere verhaal verbindt de wiskundige gemeenschap en de Surinaamse gemeenschap. Het symposium zal ook digitaal te volgen zijn in Nederland en Suriname. Deelname is gratis. Meer informatie volgt op wiskgenoot.nl.

Recent verschenen:

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

Special Issue to the memory of T.A. Springer, Gunther Cornelissen en Eric Opdam (eds.), Volume 32, Issue 6, 2021.

Special Issue to the memory of T.A. Springer, Gunther Cornelissen en Eric Opdam (eds.), Volume 32, Issue 5, 2021.

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

Zebra 63. Doortrapte Getallen, Charlene Kalle en Irene Verstraten, € 10, 2021.

Zebra 62. Vormen en Verhoudingen in de Architectuur, Jacques Jansen en Karen de Kort, € 10, 2021.

Zebra 61. De driehoek van Pascal, Rob Bosch en Pieter Miedema, € 10, 2021.

Wil Schilders
Platform Wiskunde Nederland
w.h.a.schilders@tue.nl

Jeroen Spandaw
Delft Institute of Applied Mathematics
TU Delft
j.g.spandaw@tudelft.nl

Kees Temme
Bètapartners
kees.temme@uva.nl

Benne de Weger
Faculteit Wiskunde en Informatica
Technische Universiteit Eindhoven
b.m.m.d.weger@tue.nl

Evenement Vakantiecursus 2021

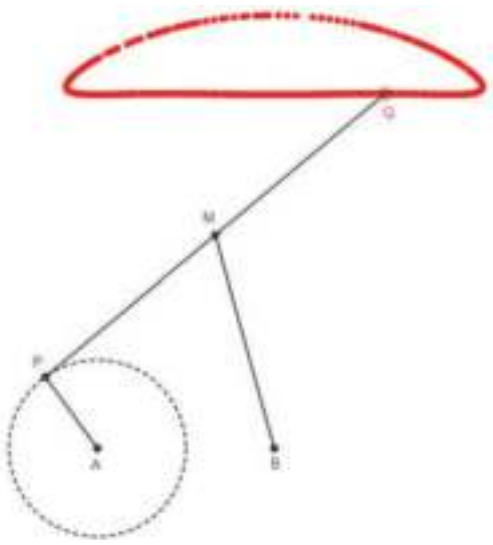
75 jaar Vakantiecursus voor wiskundeleraren

Jaarlijks wordt aan het einde van de zomervakantie de Vakantiecursus (VC) voor wiskundeleraren georganiseerd. De VC 2021, recent gehouden in Amsterdam en Eindhoven, had een feestelijk tintje, aangezien het 75 jaar geleden was dat de eerste Vakantiecursus werd gehouden aan het in 1946 opgerichte Mathematisch Centrum, tegenwoordig het Centrum Wiskunde & Informatica (CWI). Een verslag van de programmacommissie.

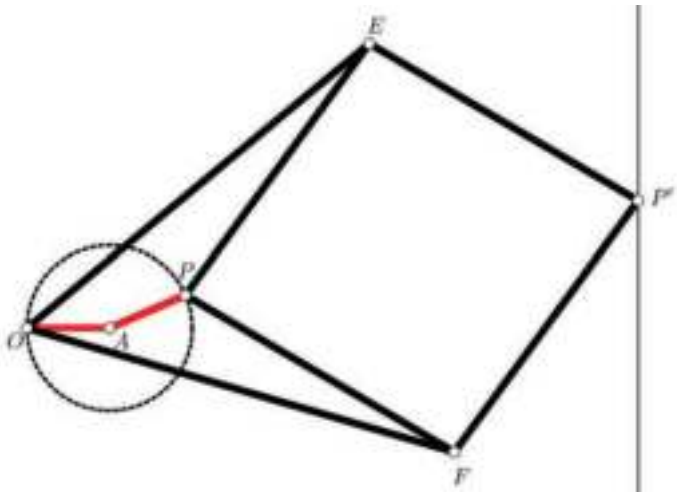
De eerste vakantiecursus wordt in het jaarverslag 1946 van het Mathematisch Centrum als volgt vermeld (in enigszins oud Nederlands): "Op 29 en 31 Oct. '46 werd onder auspiciën van het M.C. een druk bezochte en uitstekend geslaagde vacantiecursus gehouden voor wiskundeleeraren in Nederland. Op 29 October stond de wiskunde, op 31 October de didactiek van de wiskunde op de voorgrond. De sprekers waren: Prof. Dr. O. Bottema, 'De prismoide', Dr. A. Heyting, 'Punten in het oneindige', Mr. J. v. IJzeren, 'Abstracte Meetkunde en haar betekenis voor de Schoolmeetkunde', Dr. H. D. Kloosterman, 'Ontbinding in factoren', Dr. G. Wielenga, 'Is wiskunde-onderwijs voor alpha's noodzakelijk?', Dr. J. de Groot, 'Het scheppend vermogen van den wiskundige' en Dr. N. L. H. Bunt, 'Moeilijkheden van leerlingen bij het beginnend onderwijs in de meetkunde'. Aan het einde van de vacantiecursus werden diverse zaken besproken die het wiskunde-onderwijs in Nederland betroffen. Een Commissie werd ingesteld, die het M.C. over de verder te organiseren vakantiecursussen van advies zou dienen. Hierin namen zitting een vertegenwoordiger van de Inspecteurs van het V.H. en M.O. benevens vertegenwoordigers van de lerarenverenigingen Wimecos en Liwenagel. Ook werd naar aanleiding van 'wenschen' die tijdens de cursus naar voren gekomen waren ingesteld: een colloquium over moderne Algebra, een dispuut over de didactiek van de wiskunde, beiden hoofdzakelijk bedoeld voor de leeraren uit Amsterdam en omgeving, terwijl tevens vanwege het M.C. een cursus over Getallenleer werd toegezegd te geven door de heeren v.d. Corput en Koksma. (Colloquium, dispuut en cursus zijn in 1947 gestart en verheugen zich in blijvende belangstelling)."

Het was een mooi initiatief dat sindsdien jaarlijks wordt herhaald. Tot en met 2010 werd de Vakantiecursus georganiseerd door het MC/CWI, vanaf 2011 nam het in 2010 opgerichte Platform Wiskunde Nederland (PWN) de organisatie ter hand. Momenteel werkt Erik-Jan van Gelderen (VU), onder supervisie van Gerard Alberts, aan een masterscriptie waarin de historie van de Vakantiecursus in detail wordt besproken: alle programmacomité's in de loop der jaren, alsmede alle sprekers, de bijbehorende titels en meer. Op de website van PWN is de recente historie te vinden, met de syllabi vanaf 1983.

Elk jaar bepaalt het programmacomité het onderwerp en krijgt de Vakantiecursus een pakkende titel, zoals 'Wiskunde in je broekzak: cryptografie in het dagelijks leven' (2018), 'Dit is triviaal' (2015), 'Tel uit je winst – wiskunde in geld en spelen' (2009) en 'Is wiskunde nog wel mensenwerk?' (2000). Tot en met 2017 waren er vaak 6 à 8 sprekers, zodat de cursus een wat caleidoscopisch karakter had. In 2018 werd besloten om het over een andere boeg te gooien door één hoofdspreker uit te nodigen, expert op een bepaald terrein. De hoofdspreker vraagt vervolgens nog één of twee gastsprekers. Dit nieuwe format valt erg in de smaak van de deelnemers, omdat de stof eenvoudiger te volgen is en er meer continuïteit is in de besproken lesstof. Vereiste is wel om dan uitstekende sprekers te zoeken die bereid zijn behoorlijk wat tijd te steken in de voorbereiding van de cursus. In 2018 trapte Benne de Weger af met cryptografie, waarbij medewerkers van het Cryptomuseum een originele Enigma-machine meenamen met een waarde van meer dan 100 000 euro! In 2019 was Sjoerd Verduyn Lunel, toentertijd voorzitter van PWN, hoofdspreker rondom het thema 'deep learning', terwijl in 2020 Frank Thuijsman van de Universiteit Maastricht sprak over speltheorie.



Figuur 1 Lambda-constructie van Tsjebysjov.



Figuur 2 Een Peaucellier–Lipkin inversor. De zes zwarte stangen vormen een ruit $PFP'E$ en een vlieger $OFP'E$. Het punt O ligt vast. Als P beweegt over een cirkel die O bevat dan beweegt P' over een rechte lijn!

Editie 2021

Voor de speciale feestelijke editie in 2021 vonden we Rainer Kaenders van het Hausdorff Center for Mathematics in Bonn bereid om de cursus voor te bereiden omtrent zijn grote hobby, de stangenmeetkunde. Rainer spreekt uitstekend Nederlands, hij deed van 1993 tot 1997 promotieonderzoek aan de Radboud Universiteit onder supervisie van Joseph Steenbrink, was in 1997–1998 postdoc aan de Universiteit Utrecht en had in de periode van 2000 tot 2007 diverse posities in Nijmegen en Delft. Rainer verraste ons en het publiek met allerlei prachtige constructies en stellingen omtrent de stangenmeetkunde. Het is een gebied waarin bekende wiskundigen als Tsjebysjov ook bijdragen hebben geleverd met onder andere zijn befaamde lambda-constructie (zie Figuur 1).

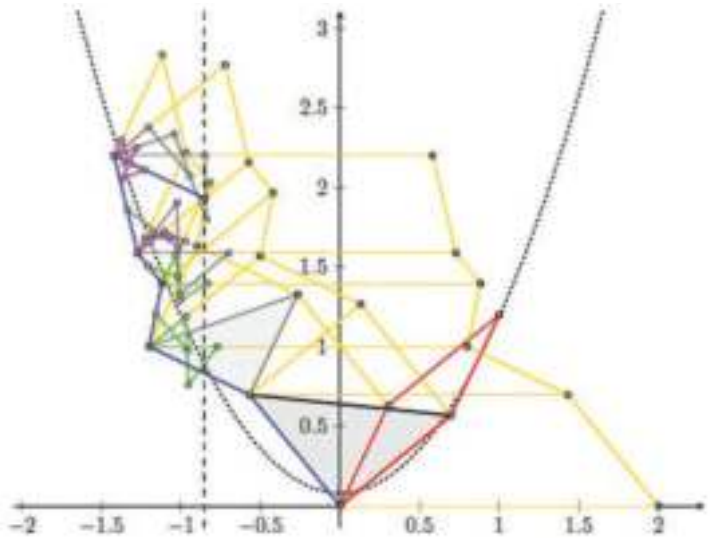
Centraal thema in de cursus was de vraag: "Hoe teken je een rechte lijn", natuurlijk met behulp van stangenconstructies. Dit blijkt een vraagstelling te zijn waar veel onderzoekers zich mee bezig hebben gehouden, onder anderen James Watt met zijn stoommachines. Aanvankelijk dachten sommigen dat ze een constructie gevonden hadden waarmee een rechte lijn getekend kon worden, maar bleek bij nader inzien, dat de gecreëerde kromme geen rechte lijn was. Dit is ook te zien door de constructie in GeoGebra na te tekenen en vervolgens op de kromme in te zoomen. Gerrit Veldkamp van de TU Eindhoven schreef een prachtig boek over de materie, waarin hij gedetailleerde berekeningen presenteerde die de afwijking in algebraïsche vorm lieten zien, gerelateerd aan de bekende Tjsebysjov-polynomen. Een van de belangrijkste bijdragen rondom deze vraagstelling kwam van de Fransman Peaucellier en de Litouwer Lipkin, die er uiteindelijk in slaagden een constructie te maken waarin daadwerkelijk een rechte lijn wordt getekend (zie Figuur 2).

Verrassend genoeg blijkt het zoeken naar stangenconstructies die een rechte lijn produceren, te maken te hebben met de befaamde 'strandbeesten' van kunstenaar Theo Jansen. Laatstgenoemde was dan ook uitgenodigd als laatste spreker. Hij toonde een filmpje van de ontwikkeling van strandbeesten vanaf 1990 en legde uit hoe hij de constructie met behulp van een Atari-computer in 1990–1991 had vervolmaakt door de optimale parameters te berekenen in de gebruikte stangenconstructie.

Voor wiskundigen was een cruciale vraag of stangenconstructies gebruikt kunnen worden om een willekeurige algebraische kromme te tekenen. Het antwoord daarop blijkt bevestigend. Dit was al in 1875 bewezen door Kempe in het beroemd geworden artikel 'On a General Method of describing Plane Curves of the nth degree by Linkwork'. Dat de bijbehorende stangenconstructies al spoedig zeer ingewik-

Rainer Kaenders met een stangenconstructie

Teun Koetsier over 'De magie van de beweging'



Figuur 3 GeoGebra-afbeelding van constructie om parabool te tekenen.

keld worden, werd gedemonstreerd door Rainer, die voor een parabool liet zien hoe een stangenconstructie afgeleid kon worden. De animatie vervaardigd met GeoGebra was indrukwekkend en had hem vele uren achter het scherm gekost. Maar de deelnemers waren zeer onder de indruk!

De gepresenteerde stof is op verschillende niveaus in het voortgezet onderwijs te gebruiken. Leerlingen kunnen concreet met stangetjes aan de slag. Ze kunnen in GeoGebra constructies (na)bouwen en bestuderen. Ze kunnen redeneren over de constructies met behulp van synthetische (coördinaatvrije) meetkunde, waarbij ook zinvolle en interessante algebra en goniometrie aan de orde kunnen komen, of ze kunnen hun tanden stukbijten op rekenpartijen in het reële coördinatenvlak. Het is zelfs mogelijk om een hoger abstractieniveau als 'de topologie van een configuratieruimte' toegankelijk te maken, zoals Rainer mooi demonstreerde met GeoGebraplaatjes (zie Figuur 3) en zwembanden. Voor meer toelichting verwijzen we naar het artikel 'Wiskunde ontdekken met GeoGebra' (werktitel) dat begin 2022 in *Euclides* verschijnt.

Op de vrijdagavond was Teun Koetsier (emeritus VU) gastspreker, met een mooie en zeer interessante lezing over 'De magie van de beweging' waarin de stangenconstructies in een historisch kader geplaatst werden. Hij kwam met prachtige voorbeelden van vraagstukken die uit de technische ontwikkelingen tijdens de industrialisatie zijn voortgekomen en waarmee enkele van de beste wiskundigen van hun tijd, zoals bijvoorbeeld Tjsebysjov, Sylvester, Kempe en Poincaré, aan de slag zijn gegaan.

Al met al was deze feestelijke editie er een om in te lijsten. Een interessant thema met zeer verrassende resultaten, uitstekende sprekers en een mooie afsluiting door kunstenaar Theo Jansen. In Eindhoven was ook kunstenaar Ivo Schoofs aanwezig die voor het jaarlijkse Glow-evenement in lichtstad Eindhoven een prachtig kunstwerk had gemaakt gebaseerd op de Peaucellier–Lipkin-constructie.

De gastvrijheid en catering in Amsterdam alsmede Eindhoven werd ook weer zeer op prijs gesteld. In Eindhoven vindt de Vakantiecursus sinds 2020 plaats in het Academisch Genootschap Eindhoven (AGE) aan de Parklaan. Met dank aan het prachtige zomerweer kon er vrijdag buiten gedineerd worden en werden de pauzes door veel deelnemers aangegrepen om even van de zon te genieten en samen te discussiëren over de besproken stof.

Oproep

Er zijn veel vaste deelnemers aan de Vakantiecursus, maar gelukkig zien we ook elk jaar nieuwe deelnemers. Vooral ook voor jongere leraren (<50 jaar) is de Vakantiecursus ideaal om even "bij te tanken" en samen met collega's te discussieren over onderwerpen die, zoals Rainers stangenconstructies, mogelijk ook in de klas kunnen worden behandeld. Graag suggereren we dan ook om eens te overwegen een cursus bij te wonen. Elk thema is interessant, de sprekers zijn uitstekend en men leert er altijd van alles van. Ook voor niet-leraren is de cursus interessant, om in een aangename setting eens wat te leren over onderwerpen waar men weinig of niets van af weet. Ons vak wiskunde bevat zoveel prachtige resultaten, soms zeer onvermoed zoals weer eens werd aangetoond in de editie van 2021. De Vakantiecursus staat dan ook zeker open voor anderen dan leraren. Daarnaast kan men dan ook eens van gedachten wisselen met vaak zeer ervaren wiskundeleraren over het onderwijs in het VO.

Theo Jansen demonstreert een mini-versie van een strandbeest

Kunstwerk van Ivo Schoofs tijdens het Glow-evenement in Eindhoven

Lola Thompson
Mathematical Institute
Utrecht University
l.thompson@uu.nl

Research

(Mind the) gaps between primes

The question of whether there are infinitely many pairs of 'twin primes' (primes that differ by 2) has puzzled mathematicians for hundreds, if not thousands, of years. Until recently, it was not even known whether there are infinitely many pairs of primes that differ by a finite number. In 2013, Yitang Zhang stunned the mathematics community by proving that there are infinitely many pairs of primes that differ by at most 70 000 000. While 70 000 000 is still quite far from 2, Zhang's work has inspired a flurry of activity on this problem, leading to many other interesting results in number theory. This expository article is based on a talk that Lola Thompson gave with the same title at the Winter Symposium of the Koninklijk Wiskundig Genootschap (Royal Dutch Mathematical Society) on 9 January 2021. The other speaker was Pieter Moree, who also has an article in this issue.

Patterns in the prime numbers?

Prime numbers have long been a source of fascination. Just as some people would look to the skies and wonder about the stars, others would look at lists of whole numbers and wonder about the primes: that is, those numbers greater than 1 that are only divisible by 1 and themselves. Like DNA in biological organisms, primes can be viewed as the 'building blocks' of the integers. Every positive integer greater than 1 can be expressed uniquely as a product of primes. In other words, the prime factorization of an integer completely specifies that integer.

Some would say that the primes behave erratically, seeming to appear at random places, while others would say that they display a surprising amount of symmetry.

For example, in Figure 1 the positive whole numbers are arranged in a spiral, starting with 1 at the center. There is a black dot at each prime that appears on the line. Remarkably, the black dots appear to arrange themselves along diagonal lines. Perhaps there is a certain rhythm of the primes after all!

Looking at the primes naturally leads one to look for patterns. However, one has to be a bit careful when looking for patterns in the primes. In 1650, Fermat famously conjectured that all numbers of the form $2^{2^n}+1$ (where $n=0,1,2,3,4,\ldots$) are prime. He based his conjecture on the fact that the pattern holds for $n=0,\ldots,4$, and that was as far as he could compute by hand. However, in 1732, Euler showed that Fermat's conjecture fails when $n=5$. As of 2010, it is known that $2^{2^n}+1$ is composite for $5\leq n\leq 32$. Some mathematicians have even conjectured that $2^{2^n}+1$ is composite for all $n\geq 5$! If they are correct, then Fermat could not have been more wrong! In short, just because the smaller primes seem to display certain patterns, one cannot extrapolate that these patterns hold in general. One needs to prove, rigorously, that these patterns hold continue past the small data points that humans are able to compute. The fact that the primes appear to land along the diagonals in the spiral above is also a phenomenon that dissi-

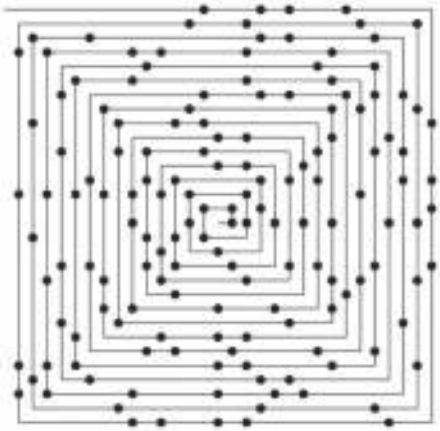


Figure 1 Prime spiral, by Eric W. Weisstein [15].

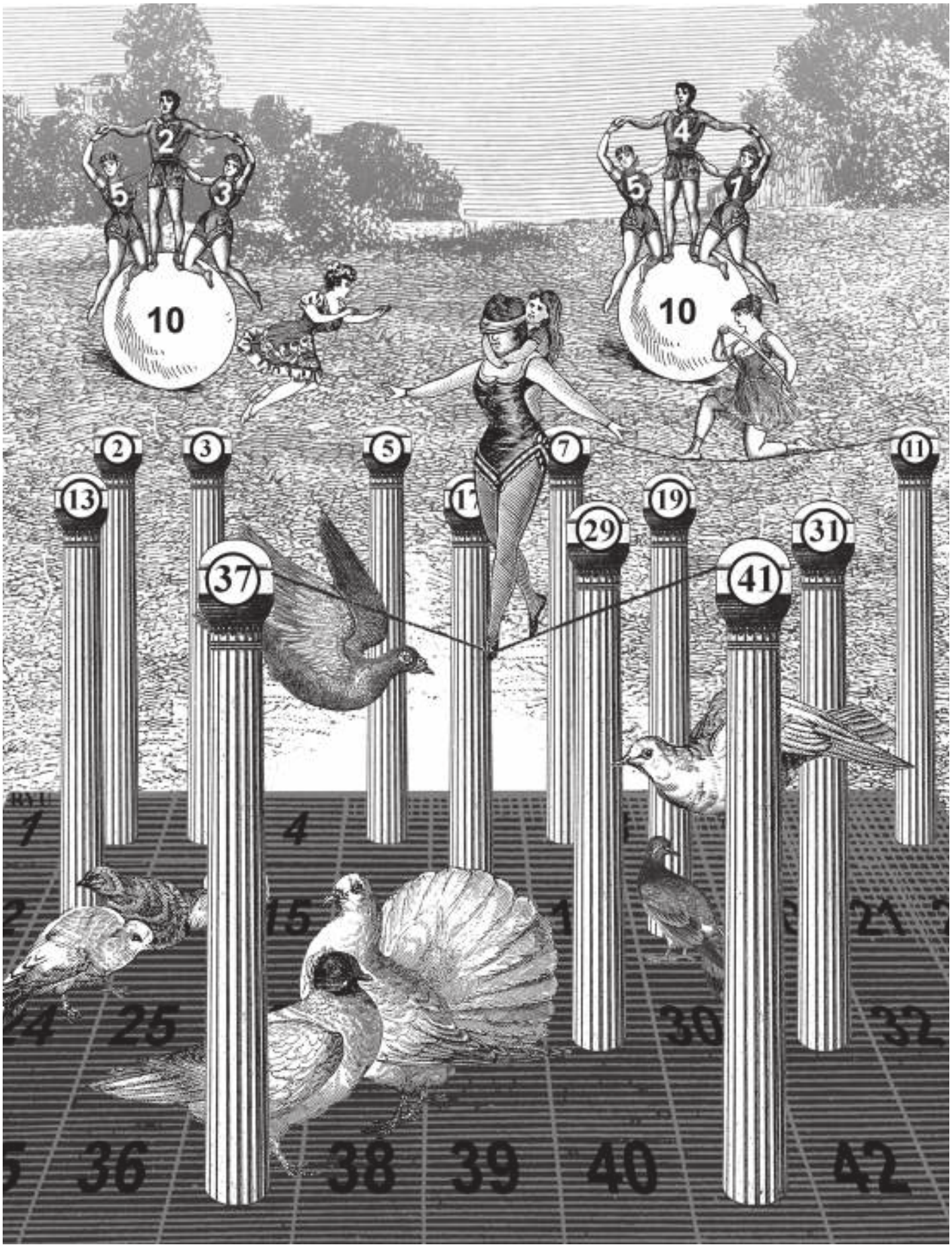


Illustration: Ryu Tajiri

1	**2**	**3**	4	**5**	6
7	8	9	10	**11**	12
13	14	15	16	**17**	18
19	20	21	22	**23**	24
25	26	27	28	**29**	30
31	32	33	34	35	36
37	38	39	40	**41**	42
43	44	45	46	**47**	48
49	50	51	52	**53**	54

Table 1

pates as you zoom out, though there is a good reason for it.

As another cautionary tale, consider the positive whole numbers in Table 1. The casual observer might notice that all of the primes (except 2) seem to fall in columns '1' and '5'. Unlike the previous example, this pattern actually holds in general. One could prove that all primes greater than 2 fall into columns '1' and '5' if an infinite table were constructed in the same manner. Unfortunately, this is not a deep observation. Notice that, every entry in column '1' can be written in the form $6n+1$, where $n=0,1,2,\ldots$. Similarly, column 2 corresponds to the numbers of the form $6n+2$, and the other whole numbers can be written in the form $6n+3$, $6n+4$, $6n+5$, or $6n$. Notice that $6n+2=2(3n+1)$. This means that $6n+2$ can always be factored into a product of two numbers that are between 1 and $6n+2$, so it cannot be prime. Similar logic shows that $6n+3$ and $6n+4$ also cannot be prime. Moreover, $6n$ is clearly not prime since it is a product of 6 and another number. As a result, the only columns that could possibly contain prime numbers are columns '1' and '5' above. The fact that we have convinced ourselves that the pattern in the table is true in only a few sentences shows that this pattern is pretty trivial.

In this article, we will focus on some patterns in the primes that are both provably true and nontrivial.

Prime number theory

How many primes are there? It turns out that there are infinitely many of them. The first few prime numbers are relatively close together: $2,3,5,7,\ldots$. However, as you zoom out further, the primes seem to spread out. Indeed, there are four prime numbers between 1 and 10, in other words 40% of the first ten positive numbers are prime. However, only 25% of the first one hundred numbers turn out to be prime, and the percentage appears to get worse as you look at larger and larger intervals. One can see this phenomenon illustrated in the following Table 2.

One might look at this table and wonder, in the long run, what percentage of the positive whole numbers are prime. Perhaps surprisingly, as you make the table infinitely large, the percentage will approach 0%! In other words, there are infinitely many primes, but they are extremely rare within the set of positive whole numbers. The primes are so rare that, if you put all positive whole numbers into a paper bag and draw one number out at random, you would have a 0% chance of selecting a prime!

10	4	40%
100	25	25%
1 000	168	16.8%
10 000	1 229	12.29%
100 000	9 592	9.592%
1 000 000	78 498	7.85%
10 000 000	664 579	6.65%
100 000 000	5 761 455	5.70%
1 000 000 000	50 847 534	5.09%
10 000 000 000	455 052 511	4.55%
100 000 000 000	4 118 054 813	4.12%
1 000 000 000 000	37 607 912 018	3.77%

Table 2 Percentage of numbers that are prime.

Twin primes

One pattern that does seem promising in the exploration of prime numbers is the incidence of *twin primes*: primes that differ by 2. The following are pairs of twin primes: $(3,5)$, $(5,7)$, $(11,13)$,... Some very large pairs of twin primes have been found! For example, the numbers

$$(3756801695685\cdot 2^{666669}-1$$
$$3756801695685\cdot 2^{666669}+1)$$

are both prime and they only differ by 2, making them a twin prime pair. However, it is not yet known whether there are infinitely many such pairs. Determining whether there are infinitely many pairs of twin primes is one of many famous unsolved problems in number theory.

More generally, one could ask if there are infinitely many pairs of primes that differ by any positive integer h that you like. This question can be answered very easily when h is odd. Since there is only one even prime number, namely 2, then we only get odd differences between primes when the smaller prime is 2. As a result, gaps of size h for odd h can appear at most once. The situation where h is even appears to be a lot more interesting. In the special case where $h=2$, these are the pairs of twin primes that we considered above. However, we could also look at primes that differ by 4 or 6 or 8 or...

We refer to differences between consecutive primes as 'gaps' between primes. It has been conjectured that all even gaps between primes occur infinitely often:

Conjecture 1 (de Polignac, 1849). *For even integers h, there are infinitely many pairs of primes $p,p+h$.*

This is the first known appearance of the so-called 'twin primes conjecture' that appears in the literature. While the statement seems simple enough, it is astonishingly difficult to prove. In fact, up until recently, one could not even show that any particular integer appears infinitely often as a gap between primes! We still do not know of a single example of a prime gap that occurs infinitely often. However, as we will see below, it has been shown (as of 2013) that at least one finite number appears infinitely often as a gap between primes.

The GPY approach

In 2003, Dan Goldston and Cem Yıldırım announced a proof that there are infinite-

ly many pairs of primes that differ by at most 12. In other words, they claimed that they could prove that one of the numbers 2, 4, 6, 8, 10 or 12 appears infinitely often as a gap between primes. This announcement was met with a great deal of excitement. After all, it would be the first time that anyone could prove that a finite number appears infinitely often as a gap between primes! Unfortunately, their work was quickly discredited by Granville and Soundararajan, who found a fatal flaw in their argument. While Goldston and Yıldırım were unable to salvage the original result, they were able to join forces with another author, János Pintz, to obtain a *conditional* result. A conditional result is one that depends on the validity of a different unsolved conjecture. In their case, they proved:

Theorem 1 (Goldston, Pintz and Yıldırım, 2005). *If a certain unsolved conjecture is true, then there are infinitely many pairs of primes that differ by at most* 16.

(The unsolved conjecture is called the Elliot–Halberstam Conjecture.) On the surface, this only looks a bit worse than what they initially announced. After all, it would just mean that one of the numbers 2, 4, 6, 8, 10, 12, 14 or 16 appears infinitely often as a gap between primes. However, the famous unsolved conjecture that they assumed is also likely to be very difficult to prove. For that reason, the result is somewhat less satisfying than if it were an *unconditional* proof.

For several years, the general consensus in the number theory community was that Goldston, Pintz and Yıldırım had pushed the existing mathematical tools as far as possible. In other words, it would take a whole new set of tools in order to prove that there are infinitely many pairs of primes with a finite number appearing as a gap between them. Then, out of nowhere, a relatively unknown mathematician named Yitang Zhang announced that he had done what had long eluded number theorists: he had shown that there are infinitely many pairs of primes that differ by at most 70 000 000. By the pigeonhole principle this means that there must be some finite (even) number between 2 and 70 000 000 that appears infinitely often as a gap between primes! (The pigeonhole principle says that if you have $n+1$ pigeons that you want to stuff into n holes, there must be at least one hole containing two pigeons. Moreover, if you have infinitely many pigeons that you want to stuff into finitely many holes, then there must be a hole with an infinite number of pigeons. In our example, the "pigeons' are gaps between pairs of primes and the 'holes' are the even numbers between 2 and 70 000 000.

Zhang's approach

How did Zhang manage to overcome the difficulties that Goldston, Pintz and Yıldırım encountered?

When his result was announced, he seemed like an unlikely superhero. After earning his PhD, he was unable to secure an academic position. Instead, he spent five years doing a series of odd jobs (Sandwich Artist at a Subway restaurant, motel employee in Kentucky, delivery worker in a New York City restaurant) before taking an adjunct position at the University of New Hampshire. Prior to his seminal paper on gaps between primes, he had only written two other papers, including his PhD thesis which was never published. He was already in his late 50's when he made his groundbreaking discovery. Perhaps working outside of the traditional academic system is what gave him the freedom to follow his convictions. He believed that, rather than needing to develop a whole new set of tools, he could simply relax some conditions in Goldston, Pintz and Yıldırım's work in order to overcome the barrier that prevented them from obtaining an unconditional result.

The barrier in Goldston, Pintz and Yıldırım's paper had to do with how 'uniformly distributed' the primes are. In order to understand what is meant by this, we will need to take a step back and discuss *modular arithmetic*. Simply put, modular arithmetic is something that we do every day when we tell time on an analogue clock. For example, when the digital clock says that it is 13:00, we mentally convert it to the time on the old analogue clock and say that it is 1 PM. Similarly, 14:00 corresponds to 2 PM, 15:00 corresponds to 3 PM, et cetera.

Instead of creating clock faces with twelve numbers, we can create clock faces with any quantity of numbers that we like. We could make a clock with only three numbers, or we could make a clock with thirteen numbers. For various reasons, number theorists like to work with clocks that have a prime number of numbers.

In the example shown in Figure 2, we see that the numbers keep wrapping around the clock. Since 7 behaves like midnight in this clock, it means that 8 corresponds to 1, and 9 corresponds to 2,... but we can also imagine traveling around the clock in a counterclockwise fashion and have a notion of negative numbers on our clock. We say that the numbers on a clock with

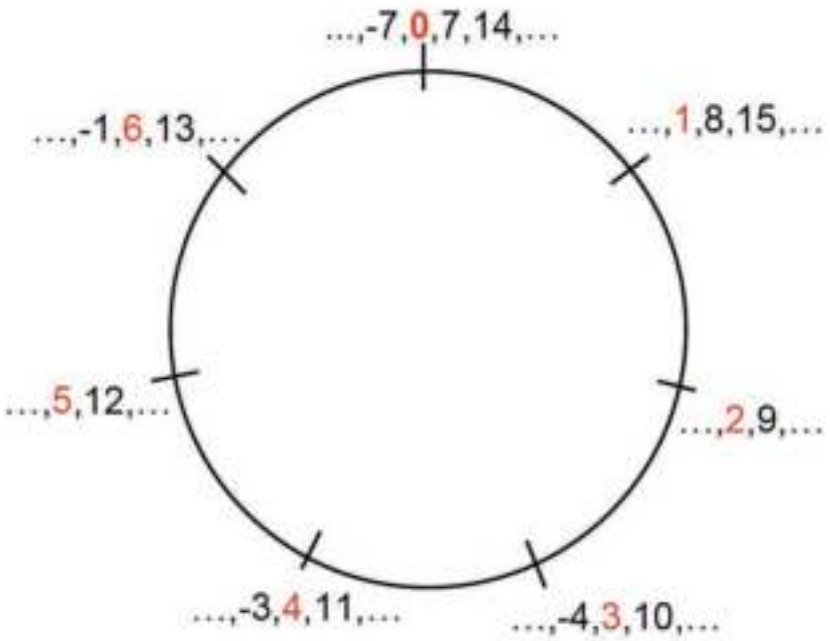


Figure 2 Modulo 7 clock by Richard Taylor [14].

7 values are integers (mod 7). When two numbers are equivalent to one another on the clock with 7 numbers, we say that they are congruent (mod 7). For example, we just saw that $8 \equiv 1 \pmod 7$. The picture also shows us that $-1 \equiv 6 \pmod 7$. When two numbers are equivalent in this clock arithmetic, we say that they fall into the same *residue class*.

In order to prove an unconditional version of their result, Goldston, Pintz and Yıldırım (GPY) would have needed to show that the primes are reasonably 'well-distributed' among the residue classes (mod q) for all positive integers q up to a certain point. As an example, the primes are 'well-distributed' $(\mathrm{mod}\ 7)$ if there is an equal proportion of primes in each possible residue class (it turns out that primes other than 7 cannot be congruent to $0 \pmod 7$ since this would imply that they are divisible by 7 and we know that primes have no divisors besides 1 and themselves). This leaves six possible residue classes that the primes can fall into, namely they can be congruent to any of the numbers between 1 and $6 \pmod 7$. So, being reasonably well-distributed would mean that about $1/6$ of the primes are congruent to $1 \pmod 7$, roughly $1/6$ are congruent to $2 \pmod 7$, et cetera. It has been proven that this is true when the size of the clock is relatively small. However, when looking over a range of numbers $[1,N]$, the GPY proof relies on the assumption that the primes are reasonably well distributed modulo q when q is just a tiny bit larger than $N^{1/2}$. It turns out that the primes are well-distributed for q smaller than $N^{1/2}$; nevertheless, one cannot prove unconditionally that the same phenomenon occurs for $q > N^{1/2}$. To get past this issue, Zhang put some extra restrictions on the values of q that he looked at, but was able to show that for integers q with these restrictions, he could prove that the primes were reasonably well-distributed, even when q is a bit larger than $N^{1/2}$. In spite of these extra restrictions on q, it was enough to push the GPY machinery through and obtain the following unconditional result:

Theorem 2 (Zhang, May 2013). *There are infinitely many pairs of primes that are at most* $70\,000\,000$ *apart.*

At long last, the world had confirmation that there is a finite number that appears infinitely often as a gap between primes!

Maynard and Tao's approach

When hearing about twin primes, students often ask about the next logical case: can there be infinitely many triples of primes? Here, the answer depends on what is meant by a 'triple of primes'. If one looks at triples of the form $(p, p+2, p+4)$ and asks whether they can be prime infinitely often, the answer is, unfortunately, 'no'. The reason that this cannot happen is because one of the numbers p, $p+2$, and $p+4$ must always be divisible by 3. As an exercise, you can use clock arithmetic to check this for yourself! (Hint: Consider three cases: $p \equiv 1 \pmod 3$, $p \equiv 2 \pmod 3$, and $p \equiv 0 \pmod 3$, and then see what this tells you about $p+2$ and $p+4$ in each case.)

In order to exclude the cases of tuples whose entries *cannot* all be prime, we define the notion of an admissible k-tuple:

Definition 1. We say that a k-tuple $(h_1, \ldots, h_k)$ of nonnegative integers is *admissible* if it doesn't cover all of the possible residue classes $(\mathrm{mod}\ p)$ for any prime p.

For example, $(0,2,6,8,12)$ is an admissible 5-tuple. We can see this by checking to make sure that, for every prime p, there are always some residue classes $(\mathrm{mod}\ p)$ that are not covered by this tuple. Notice that none of the terms in the 5-tuple are congruent to $1 \pmod 2$, so the residue 1 is not covered. Similarly, all of the numbers in the 5-tuple are congruent to 2 and $0 \pmod 3$, so the residue 1 remains uncovered. One can check this for all small prime clock sizes and then, once you have more possible residue classes than terms in the tuple, it is clear that there will always be some residue classes that are not covered (in this example, it is sufficient to check through $p = 5$, since after that there will be more than 5 residue classes $(\mathrm{mod}\ p)$).

Now that we have excluded the impossible prime tuples by establishing an admissibility criterion, we can state a nice generalization of gaps between pairs of primes:

Conjecture 2 (Hardy-Littlewood prime k-tuples). *Let* $\mathcal{H} = (h_1, \ldots, h_k)$ *be admissible. Then there are infinitely many integers* n *such that all of* $n + h_1$ *are prime.*

Unfortunately, this is even more difficult to prove, and it remains a conjecture. However, progress in this direction was made a mere six months after Zhang's paper on gaps between primes appeared on the arXiv. James Maynard [7] and Terence Tao independently showed that one could obtain k-tuples that include a certain number of primes infinitely often. Namely, they proved:

Theorem 3 (Maynard-Tao, November 2013). *Let* $m \geq 2$. *For any admissible* k*-tuple* $(h_1, \ldots, h_k)$ *with* k *sufficiently large (relative to the size of* m*), there are infinitely many* n *such that at least* m *of* $n + h_1, \ldots, n + h_k$ *are prime.*

Notice that one cannot tell which of the m numbers in $n + h_1$ wind up being prime. However, this result is already stronger than what Zhang showed, since the $k = 1$ case implies that there are bounded gaps between pairs of primes. The astounding part is that Maynard and Tao used an approach that was completely different from that used by Zhang. Rather than relaxing the conditions on q and showing that the primes are reasonably well-distributed in a slightly broader range, they developed a powerful new method that has already revealed itself to be useful in a broad array of applications.

The method used by Maynard and Tao requires using a mathematical tool called a sieve. Just like a collander is used to separate pasta from water, or a plastic sieve is used on the beach to separate sea shells from sand, a mathematical sieve is used to separate numbers with a property that we desire from numbers without that property. Maynard and Tao pre-sieved the set of positive integers, creating a sample space that consisted only of those that are likely to be prime and closer together than average. Then they were able to show that the weighted average of the number of primes among $n + h_1, \ldots, n + h_k$ over the sample space that they constructed is sufficiently large that there must be a certain number of primes in the tuple.

Polymath improvements

Recall that Zhang's original result showed that there are infinitely many pairs of primes that differ by at most $70\,000\,000$. Almost immediately, various mathematicians set out to whittle that number down. Tao had the brilliant idea of crowdsourcing this work, spreading the tasks over dozens of

mathematicians in order to speed up the process. This became known as the polymath project, more specifically Polymath 8, since it was the eighth crowdsourced project to come from this initiative. Using Zhang's approach, Polymath 8 was able to bring the gap size of at most $70\,000\,000$ all the way down to at most 4680. Using the approach of Maynard and Tao, Polymath 8 [11] was able to obtain further improvements. The current state-of-the-art is as follows:

Theorem 4 (D.H.J. Polymath, 2014). *There are infinitely many pairs of primes that are at most* 246 *apart.*

In other words, by the pigeonhole principle, we know that at least one even number between 2 and 246 appears infinitely often as a gap between primes! Moreover, if one is willing to assume an unsolved conjecture (The Elliot–Halberstam Conjecture), Polymath 8 has obtained the conditional result that at least one of the numbers 2, 4, or 6 must appear infinitely often as a gap between primes!

Applications of the Maynard–Tao machinery
In this section, we discuss just a few of the many applications of Maynard and Tao's work on small gaps between primes. The main focus will be on the author's own work, since one of the aims of the Winter Symposium of the Royal Dutch Mathematical Society was to highlight the research of mathematicians working in the Netherlands. In reality, there are many interesting applications of the Maynard–Tao approach, far too many to list here. For a more comprehensive guide, see, for example, the excellent article by Andrew Granville [5].

Prime gaps between polynomials
Just like the primes were the building blocks of the integers, we could also look at building blocks of polynomials: these are called *irreducible polynomials* and they are polynomials that cannot be factored any further. For example, we can factor the polynomial $x^3-1=(x-1)(x^2+x+1)$. As hard as we try, we cannot factor $x-1$ or x^2+x+1 into smaller polynomials. As a result, $x-1$ and x^2+x+1 are irreducible polynomials. In fact, $x-1$ and x^2+x+1 are examples of *cyclotomic polynomials*, which you can learn more about by reading Pieter Moree's article [8] in this issue.)

As one might imagine, there are many parallels between prime numbers and prime polynomials. In fact, there is a whole area of number theory research dedicated to understanding which results about prime numbers still hold for prime polynomials. Thus, it is natural to consider whether we can translate the results of Maynard and Tao about gaps between prime numbers and obtain analogous results for polynomials.

Just like we could reduce integers $(\mathrm{mod}\ p)$, where p is a prime number, we can also do this with polynomials.

Example: The polynomial $4x^2+5x+1$ is irreducible. However, if we reduce it $(\mathrm{mod}\ 3)$ then it factors as follows:

$$\begin{aligned}4x^2+5x+1 &\equiv x^2+2x+1\,(\mathrm{mod}\ 3)\\ &\equiv (x+1)^2\,(\mathrm{mod}\ 3).\end{aligned}$$

Let $\mathbb{Z}_p[x]$ denote the set of polynomials $(\mathrm{mod}\ p)$. The first to prove a 'bounded gaps' result for prime polynomials was Chris Hall, who showed in his PhD thesis [6] that any of the numbers $1,\ldots,p-1$ can occur as gaps between prime polynomials in $\mathbb{Z}_p[x]$ infinitely often, provided that p is greater than 3. The case where $p=3$ turned out to be trickier. However, two years later, Paul Pollack showed in his PhD thesis [9] that the result also holds when $p=3$. Combining their results yields the following theorem that holds for all $p\geq 3$:

Theorem 5 (Hall, 2006; Pollack, 2008). *If* $p\geq 3$*, then any* $a\in\mathbb{Z}_p$ *(excluding* $a=0$*) occurs infinitely often as a gap between irreducible polynomials.*

Notice that this is a much stronger result than anything that we can say about gaps between prime numbers. For example, this result implies that there are infinitely many pairs of prime polynomials that differ by 2. If we could prove that for prime integers, we would solve the famous twin primes conjecture! Indeed, it is often easier to prove the polynomial analogues of famously difficult problems about prime numbers.

After the paper of Maynard [7] appeared on the arXiv, Hall and Pollack teamed up with a few others who were interested in studying the methods of Maynard and Tao. This is where the author of the present article enters the picture. Along with Abel Castillo, Chris Hall, Robert Lemke Oliver, and Paul Pollack, we showed [2]:

Theorem 6 (Castillo, Hall, Lemke Oliver, Pollack and Thompson, 2014). *Let* $m\geq 2$*. For any admissible* k*-tuple* $(h_1,\ldots,h_k)$ *of polynomials in* $\mathbb{Z}_p[x]$ *with* k *'sufficiently large', there are infinitely many* $f\in\mathbb{Z}_p[x]$ *such that at least* m *of* $f+h_1,\ldots,f+h_k$ *are irreducible.*

This improves on the original work of Hall and Pollack in several ways. First, our 'gaps' need not be prime integers: in fact, we also can prove that our result holds when f is any monomial. Second, the proofs of Hall and Pollack are constructive, and the examples of pairs of prime polynomials that differ by a specific integer jump up in degrees very quickly. In other words, their method produces a relatively sparse set of examples of prime polynomials with bounded gaps between them. In contrast, our prime polynomial pairs occur in many degrees. In fact, we can even show that, for sufficiently large degrees, any positive proportion of elements of $\mathbb{Z}_p[x]$ of bounded degree can occur as a gap between prime polynomials!

This work has recently been extended by Sawin and Shusterman in [12], who prove a number of prime polynomial analogues of problems that remain open for prime integers.

Digit sums
One perhaps surprising application of the proof method of Maynard and Tao has to do with digit sums. Notice that, if we take the sum of the digits of 523, we obtain $5+2+3=10$. Similarly, if we sum the digits of 541, then we get $5+4+1=10$. It turns out that 523 and 541 are consecutive primes. It is natural to wonder whether there are other pairs of consecutive primes with the same digit sum in base 10. As always, there are a number of ways to generalize this question. One could look at triples of consecutive primes that have the same digit sum, or quadruples, or quintuples,... Moreover one could consider digit sums in other bases, rather than just looking at base-10 digit sums (as in the example above). From now on, let $s_g(n)$ denote the sum of the base-g digits of n.

In 1961, Sierpiński posed the question: "Are there arbitrarily long runs of consecutive primes p on which $s_g(p)$ is constant?" He also considered the related questions of whether one could find arbitrarily long runs of consecutive primes on which the digit sum is always increasing (or always

decreasing). He showed [13] that he could find increasing pairs of digit sums, i.e., $s_{10}(p_n) < s_{10}(p_{n+1})$, infinitely often. The following year, Erdős showed that one can also find decreasing pairs of digit sums infinitely often. In 1968, Sierpiński went a step further, showing that if an unsolved conjecture (Dickson's prime k-tuples conjecture) is assumed, then one can obtain decreasing triples of consecutive primes infinitely often, i.e., $s_{10}(p_n) > s_{10}(p_{n+1}) > s_{10}(p_{n+2})$. Some time later, in an unpublished claim, Schinzel announced that, assuming a different unsolved conjecture (Schinzel's Hypothesis H), one can show that there are arbitrarily long runs of consecutive primes on which the digit sums are increasing, and similarly there are arbitrarily long runs of consecutive primes on which the digit sums are decreasing.

In late 2013, my co-author and I became aware that the methods developed by Maynard and Tao were being used to prove a number of results on runs of consecutive primes. The first such paper was written by Banks, Freiberg and Turnage-Butterbaugh [1] within the same month that Maynard's paper appeared on the arXiv. We realized that it would be possible to use these new methods to generalize the results of Sierpinski, Erdős and Schinzel. In particular, we showed [10]:

Theorem 7 (Pollack and Thompson, 2014). *For any base g, there are arbitrarily long runs of consecutive primes p on which $s_g(p)$ is constant/increasing/decreasing.*

Note that we generalize the prior work on digit sums on consecutive primes in a number of ways. First, our results hold for digits sums in any base (i.e., we are not limited to base 10). Moreover, our results do not depend on the validity of any unsolved conjectures — they are unconditional! The proof method goes beyond the scope of this expository article, but it is worth briefly mentioning that it combines the proof method of Maynard–Tao with a deep result of Drmota, Mauduit and Rivat [3].

Acknowledgements
The author would like to thank the Koninklijk Wiskundig Genootschap (Royal Dutch Mathematical Society) for inviting her to speak at their Winter Symposium. She would also like to express her gratitude to Pieter Moree, who proofread this manuscript prior to publication.

References

1 W.D. Banks, T. Freiberg and C.L. Turnage-Butterbaugh, Consecutive primes in tuples, *Acta Arith.* 167 (2015), 261–266.
2 A. Castillo, C. Hall, R. Lemke Oliver, P. Pollack and L. Thompson, Bounded gaps between primes in number fields and function fields, *Proc. Amer. Math. Soc.* 143 (2015), 2841–2856.
3 M. Drmota, C. Mauduit and J. Rivat, Primes with an average sum of digits, *Compos. Math.* 145 (2009), 271–292.
4 D.A. Goldston, J. Pintz and C.Y. Yıldırım, Primes in tuples. I, *Ann. of Math.* 170 (2009), 819–862.
5 A. Granville, Primes in intervals of bounded length, *Bull. Amer. Math. Soc.* 52(2) (2015), 171–222.
6 C. Hall. L-functions of twisted Legendre curves. *J. Number Theory* 119(1) (2006), 128–147.
7 J. Maynard, Small gaps between primes, *Ann. of Math.* 181 (2015), 1–31.
8 P. Moree, Prime gaps and cyclotomic polynomials, *Nieuw Archief voor Wiskunde* 5/22 (2021), 219–225, this issue.
9 P. Pollack, An explicit approach to Hypothesis H for polynomials over a finite field, *Anatomy of Integers*, CRM Proc. Lecture Notes 46 (2008), 259–273.
10 P. Pollack and L. Thompson, Arithmetic functions at consecutive shifted primes, *Int. J. Number Theory* 11(5) (2015), 1477–1498.
11 D.H.J. Polymath, Variants of the Selberg sieve, and bounded intervals containing many primes, *Res. Math. Sci.* 1(1) (2014), 1–83.
12 W. Sawin and M. Shusterman, On the Chowla and twin primes conjectures over $\mathbb{F}_q[T]$, arXiv:1808.04001.
13 W. Sierpinski, Sur la somme des chiffres de nombres premiers, *Rend. Circ. Mat. Palermo (2)* 10 (1961), 229–232.
14 R. Taylor, Modular arithmetic: Driven by inherent beauty and human curiosity, from The Institute Letter Summer 2012, https://www.ias.edu/ideas/2012/taylor-modular-arithmetic.
15 E.W. Weisstein, Prime spiral, from MathWorld – A Wolfram Web Resource, https://mathworld.wolfram.com/PrimeSpiral.html.
16 Y. Zhang, Bounded gaps between primes, *Ann. of Math.* 179 (2014), 1121–1174.

Pieter Moree
Max Planck Institute for Mathematics
Bonn
moree@mpim-bonn.mpg.de

Research

Prime gaps and cyclotomic polynomials

Pieter Moree was a speaker at the Winter Symposium of the Royal Dutch Mathematical Society on 9 January 2021. He discussed his recent research paper [26] with Kosyak, Sofos and Zhang on finding cyclotomic polynomials with prescribed maximum coefficient and its connections with prime number theory. The other speaker was Lola Thompson, her talk also involved prime numbers. Her write-up [46] requires fewer prerequisites than this one.

Cyclotomic polynomials: basics

It is clear that $X^2-1=(X-1)(X+1)$, $X^3-1=(X-1)(X^2+X+1)$ and $X^4-1=(X-1)(X+1)(X^2+1)$. Over the rationals none of the factors can be factorized further and the expressions give the factorization into *irreducibles*. However, it is not so obvious how to factorize X^n-1 for an *arbitrary* integer $n\geq 1$ into *irreducibles* over the rationals in a systematic way.

Over the *complex numbers* the answer is easy:

$$X^n-1=\prod_{m=1}^{n}\big(X-e^{\frac{2\pi i m}{n}}\big). \tag{1}$$

The roots are the n-th roots of unity and these divide the circle into equal parts. The word *cyclotomy* comes from ancient Greek and literally means circle-cutting. A root of unity ζ is said to be a *primitive* n-th root of unity if it satisfies $\zeta^n=1$, but not $\zeta^d=1$ for any $1\leq d<n$. For any two integers n and d by the Euclidean algorithm we can find integers a and b such that $an+bd=\gcd(n,d)$, where $\gcd$ is a shorthand for *greatest common divisor*. Thus if $\zeta^n=1$ and $\zeta^d=1$, it follows that $\zeta^{\gcd(n,d)}=1$. Therefore, in order to check that ζ is a primitive n-th root of unity, it suffices to check that $\zeta^n=1$ and $\zeta^d\neq 1$ for every proper divisor d of n. By a similar argument one deduces that if ζ is a primitive n-th root of unity, then ζ^j is of order $n/\gcd(j,n)$. It follows that all the primitive n-th roots of unity are of the form ζ^j, with $1\leq j\leq n$ and $\gcd(j,n)=1$. There are precisely $\varphi(n)$ primitive n-th roots of unity, where φ is the *Euler totient function*, which is defined as

$$\varphi(n)=\sum_{\substack{j=1\\(j,n)=1}}^{n}1.$$

An obvious primitive n-th root of unity is $e^{2\pi i/n}$.

The n-th *cyclotomic polynomial* can be defined as

$$\Phi_n(X)=\prod_{\substack{j=1\\(j,n)=1}}^{n}\big(X-e^{\frac{2\pi i j}{n}}\big). \tag{2}$$

It thus has precisely the n-th order primitive roots of unity as its simple roots. (Note that of all Greek letters Φ looks the most like a cut circle.) The degree of $\Phi_n(X)$ is $\varphi(n)$ and we have $\Phi_n(x)=X^{\varphi(n)}+\cdots$.

By reducing the fractions m/n in (1) (e.g., $4/6=2/3$), we see that for each divisor d of n there are $\varphi(d)$ reduced fractions with denominator d. These correspond to roots of unity of order d. We thus infer from (1) and (2) that

$$X^n-1=\prod_{d\,|\,n}\Phi_d(X). \tag{3}$$

Setting $n=1$ we get $\Phi_1(X)=X-1$. In case $n=p$ is a prime, we obtain

$$\Phi_p(X)=X^{p-1}+X^{p-2}+\cdots+X+1.$$

It can be shown that all cyclotomic polynomials have integer coefficients and are irreducible, and so (3) gives the factorization of X^n-1 into irreducibles over the rationals. Indeed, many famous mathematicians gave proofs of the irreducibility of the cyclotomic polynomials (Gauss, Kronecker, Eisenstein, Dedekind, Landau, Schur,...). For some of these proofs, see Weintraub [48]. The (very short) proof of Schur was even set to rhyme! (Cremer [14, pp. 39–41]).

Write

$$\Phi_n(x)=\sum_{j=0}^{\varphi(n)}a_n(j)\,x^j. \tag{4}$$

For $j>\varphi(n)$ we put $a_n(j)=0$. We define

$$A(n)=\max_{k\geq 0}\big|a_n(k)\big|,\quad A\{n\}=\{a_n(k)\colon k\geq 0\},$$

and call $A(n)$ the *height* of Φ_n. Note that, for example, $A\{105\}=\{-2,-1,0,1\}$, see Table 1. Our interest is in the possible heights $A(n)$ and extrema of $A\{n\}$ as n runs over the integers.

The cyclotomic coefficients $a_n(j)$ are usually very small. Indeed, in the nineteenth century mathematicians even thought that they are always 0 or ± 1. The first counterexample to this claim occurs at $n=105$; we have $a_{105}(41)=a_{105}(7)=-2$. Issai Schur in a letter to Edmund Landau proved that every negative even number occurs as a coefficient of some cyclotomic polynomial. Emma Lehmer [29] reproduced Schur's argument, which is easily adapted to show that *every* integer is assumed as value of a cyclotomic coefficient [44]. For the best result to date in this direction see Fintzen [17] (found during her Max Planck Institut für Mathematik (MPIM) internship).

n	$\Phi_n(x)$
5	$x^4+x^3+x^2+x+1$
12	x^4-x^2+1
15	$x^8-x^7+x^5-x^4+x^3-x+1$
16	x^8+1
60	$x^{16}+x^{14}-x^{10}-x^8-x^6+x^2+1$
105	$x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-2x^{41}-x^{40}-x^{39}+\cdots+1$
210	$x^{48}-x^{47}+x^{46}+x^{43}-x^{42}+2x^{41}-x^{40}+x^{39}+\cdots+1$
240	$x^{64}+x^{56}-x^{40}-x^{32}-x^{24}+x^8+1$

Table 1 Some cyclotomic polynomials.

Nowadays computations can be extended enormously far beyond $n=105$, cf. Figure 1. These and analytic number theoretical considerations show clearly that the complexity of the coefficients is a function of the number of distinct odd prime factors of n, much rather than the size of n. Complex patterns arise (see Figure 1) and a lot of mysteries remain.

Which maximum coefficients do occur?

The very innocent looking question we consider here is the following.

Question 1. Which integers occur as a maximum coefficient of some cyclotomic polynomial?

For example, Φ_{210} has 2 as a maximum coefficient. We propose the following conjecture.

Conjecture 1. *Every natural number occurs as the maximum coefficient of some cyclotomic polynomial.*

The rest of the paper discusses the progress we made on establishing this conjecture. Surprisingly, a big role in this is played by deep work done by many number theorists on the distribution of gaps between primes. Last but not least, everything hinges on a construction found by Eugenia Roşu [38] during a 2010 MPIM internship, improving on an earlier construction due to Yves Gallot and myself [21].

Prime gaps

Elementary material, generalities

For millenia now (some!) humans have been fascinated by prime numbers and their distribution. Recall that *prime numbers* are numbers >1 only divisible by themselves and 1 (it turns out that it is much better to consider 1 itself not as a prime number). It is usually attributed to Euclid (circa 300 BCE) that he proved there are infinitely many primes. Several formulas producing infinitely many primes are known, but they turn out to be practically useless. A famous example is a result of Mills, which asserts the existence of a real number $A>1$ with the property that A^{3^n} rounded down to the nearest integer is prime for each natural number n. This first 'defeat' forces us to take a step back and ask less precise questions such as to estimate the *prime counting function* $\pi(x)$, which counts the number of primes p not exceeding x; that is $\pi(x)=\sum_{p\le x}1$. In the course of answering this, the *stochastic* nature of the prime numbers will become apparent. The notion of an error term will also be involved. If $|f(x)|\le Bg(x)$, for some positive constant B and all values of $x\ge 1$, we write this compactly as $f(x)=O(g(x))$. This notation was introduced by Bachmann in 1894 and popularized by Landau and is generally named *Landau's Big O notation*. Edmund Landau (1877–1938) was the first to put prime number theory as a separate field on the mathematical map and wrote a bulky standard work [28] on it. Two non-Germans mathematicians, who studied the original German version, were surprised to learn about a very strong mathematician called Verfasser they had never heard of ('Verfasser' means 'author'...).

The first mathematicians to investigate the growth of $\pi(x)$ had of course to start with collecting data to get some intuition for what is going on. They did this by painfully setting up tables of consecutive prime numbers. The most famous of these computers was Carl-Friedrich Gauss. In 1791, when he was 14 years old, he noticed that as one gets to larger and larger numbers the primes thin out, but that locally their distribution appears to be quite erratic. He based himself on a prime number table contained in a booklet with tables of logarithms he had received as a prize, and went on to conjecture that the "probability that an arbitrary integer n is actually a prime number should equal $1/\log n$." Thus Gauss conjectured the following approximations:

$$\pi(x)\approx\sum_{2\le n\le x}\frac{1}{\log n}\approx \mathrm{Li}(x),$$

where

$$\mathrm{Li}(x)=\int_2^x\frac{dt}{\log t},$$

denotes the *logarithmic integral*. By partial integration one sees that $\mathrm{Li}(x)\sim x/\log x$, where by $A(x)\sim B(x)$ we mean that

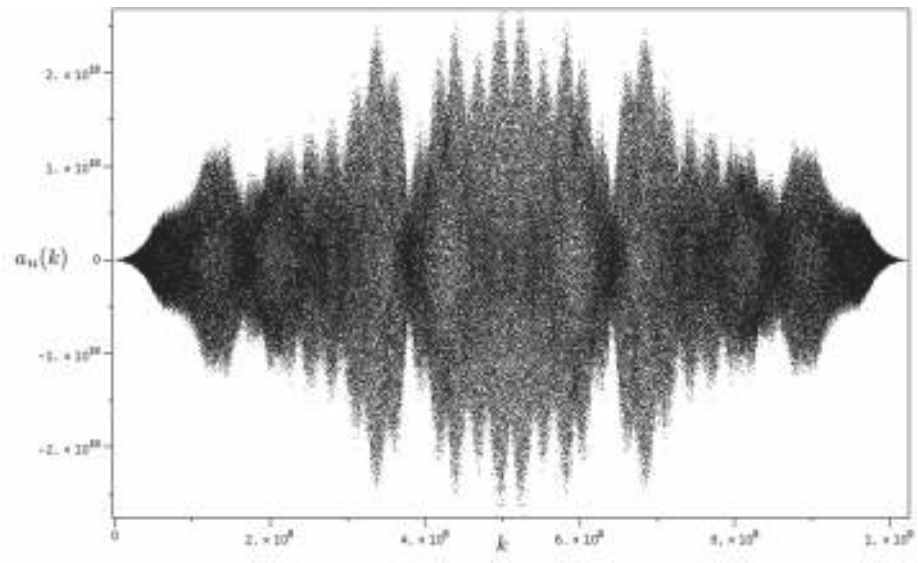


Figure 1 Coefficients of the n-th cyclotomic polynomial for $n=3234846615=3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23\cdot29$, cf. [2].

$\lim_{x\to\infty} A(x)/B(x) = 1$. Thus Gauss's heuristic leads to the conjecture that

$$\pi(x) \sim \frac{x}{\log x}.$$

This was proved much later, in 1896, by Hadamard and independently by de La Vallée Poussin and is now called the *Prime Number Theorem* (PNT). Both of them were divinely rewarded for doing so and became immortal. Well, almost — they lived to be near centenarians...

If the *Riemann Hypothesis* (RH) were true, it would imply that

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x). \qquad (5)$$

The RH is one of the Millennium Problems and will not be discussed further here. Its intimate connection with the distribution of prime numbers is discussed in an introductory way in [37].

Prime number questions fall into two main categories: *global problems* and *local problems*. The former concerns asymptotic formulae, sums, estimations and the like of $\pi(x)$ and related functions (of which the PNT is an example), while local problems involve questions dealing with the individual primes. Our focus here will be on large differences between primes (a local property) and their applications.

We let p_n denote the n-th prime number and put $d_n := p_{n+1} - p_n$. For example, the first few prime numbers are $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ which means that the first few prime gaps are $d_1 = 1$, $d_2 = 2$, and $d_3 = 2$. Note that $\sum_{k=1}^{n}(p_{k+1} - p_k) = p_{n+1} - 2$. By an equivalent form of the PNT the n-th prime number p_n asymptotically grows as $n\log n$. (This is plausible as by the PNT the number of primes not exceeding $n\log n$ is asymptotically equal to $n\log n/(\log(n\log n)$, that is to n.) Thus on average the prime gap is $\log n$, which behaves as $\log p_n$. A natural question is then how often d_n is behaving far from average. E.g., looking at the d_n one might suspect that infinitely often $d_n = 2$. This happens when both p_n and p_{n+1} are primes (they then form a *twin prime pair*) and the Twin Prime Conjecture states that there are infinitely many twin prime pairs. Similarly it is suspected that, given any even number $2k$, infinitely often $d_n = 2k$. Proving results in this direction is extremely hard. If one focuses on rather bigger gaps, life is a bit easier. For example, Helmut Maier [31] showed that $p_{n+1} - p_n \le (\log p_n)/4$ for infinitely many n. There are a lot of interesting things to say further on small gaps and some spectacular recent developments to report on, see, e.g., the recent book by Broughan [10]. However, since this topic is dealt with in the companion article by Lola Thompson [46], we will not discuss it further here.

Our focus will be on large prime gaps. One does not need the PNT to see that there are arbitrarily large prime gaps, i.e. arbitrarily large stretches of composite integers. Namely, for every $N > 1$ there exists a string of at least N consecutive composite integers. An example is given by the string $(N+1)!+2, (N+1)!+3, \ldots, (N+1)!+N+1$. Experimentally gaps of size N have been found between numbers much smaller than $(N+1)!+N+1$. Rankin [40] proved in 1938 that there exists a positive constant c such that, for infinitely many n, we have

$$p_{n+1} - p_n \ge c\log p_n \frac{(\log\log p_n)(\log\log\log\log p_n)}{(\log\log\log p_n)^2}.$$

This improved on work of Westzynthius (1931) who showed that the sequence $(p_{n+1} - p_n)/\log p_n$ is unbounded. In his final paper on this topic Rankin showed that one can take c to be any number smaller than e^{γ}, where $\gamma = 0{,}5772156649\ldots$ is *Euler's constant*. This had been shown already in 1935 by Pál Erdős [16]. Indeed, Erdős who had the habit of offering prizes for solving various open problems, offered $10\,000$ dollar to anyone who could prove that c can be replaced by any arbitrarily large constant. In 2016, twenty years after Erdős passed away, this conjecture was independently established by Ford, Green, Konyagin and Tao [18] and Maynard [33]. The group of four authors and Maynard received each 5000 dollar from Ron Graham, a close friend of Erdős.

The function $\log\log x$ walks off to infinity in such a gentle way that one does not notice it. For example, the reciprocal prime sum $\sum_{p\le x} 1/p$ behaves in that way. It comes perhaps as a surprise (or shock!) to the reader that if we sum the reciprocals of all different primes any human eye has ever looked at, the number comes to be out less than ... 4! The fact that making conjectures in analytic prime number theory is a notoriously dangerous endeavour is related to this. The danger lies in the fact that computers can barely spot $\log\log$ terms and are certainly blind to the $\log\log\log$ terms that frequently occur. It is there that the log log log devil is in his element. The presence of such terms can result in the conjecture being false on very thin subsequences. A famous example is the conjecture that $\pi(x) < \mathrm{Li}(x)$. It is false, but true up to gigantic values of x. Littlewood proved that $\pi(x)$ and $\mathrm{Li}(x)$ carry out an eternal dance around each other. This is now a classic result, but falls a bit short of proving RH (on the suggestion of his tutor Littlewood tried to prove RH during his postdoctoral studies!). Further examples of log log log devil teases are discussed in my article [36].

Large prime gaps

There is a whole range of conjectures on gaps between consecutive primes; from more careful to high-risk. The most famous one is Legendre's and claims that there is a prime in $(m^2, (m+1)^2)$ for every natural number m. This is a conjecture that is on the safer side, but for example Firoozbakht's conjecture that $p_n^{1/n}$ is a strictly decreasing function of n is 'trés risqué'. It implies that $d_n < (\log p_n)^2 - \log p_n + 1$ for all n sufficiently large (see Sun [43]), contradicting a heuristic model suggesting that, given any $\epsilon > 0$, there are infinitely many n such that $d_n > (2e^{-\gamma} - \epsilon)(\log p_n)^2$; see Banks, Ford and Tao [4]. Cramér in 1936 conjectured that $d_n = O((\log p_n)^2)$. Piltz in 1884 conjectured more modestly that $d_n = O(p_n^{\epsilon})$ for every $\epsilon > 0$. The first to *prove* that $d_n = O(p_n^{\theta})$ for some $\theta < 1$ was Hoheisel in 1930. He took $\theta = 1 - \frac{1}{33000} + \epsilon$. Well-known to number theorists is Huxley's [24] result from 1972 showing that one can take $\theta = \frac{7}{12} + \epsilon$. Baker et al. [3] showed that $d_n = O(p_n^{0.525})$, which is not much weaker than what one can prove assuming RH. Under RH it is an easy consequence of (3.1) that $d_n = O(\sqrt{p_n}(\log p_n)^2)$. Cramér [13] improved on this by showing in 1920 that $d_n = O(\sqrt{p_n}\log p_n)$ under RH. More explicitly, Carneiro et al. [11] established under RH that $d_n \le \frac{22}{25}\sqrt{p_n}\log p_n$ for every $p_n > 3$.

We will be especially interested in the following conjecture, which is in the same league as Legendre's conjecture.

Conjecture 2 (Andrica's conjecture). *For $n \ge 1$, $p_{n+1} - p_n < \sqrt{p_n} + \sqrt{p_{n+1}}$, or equivalently $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$, or equivalently $p_{n+1} - p_n < 2\sqrt{p_n} + 1$.*

Andrica's Conjecture is currently out of reach as we have just seen (even under RH). The next best thing one can then hope for is to prove that there are not too many n for which the inequality fails (more on that later).

Many mathematicians take it that an unproven assertion can only be called conjecture if there are overwhelming reasons for its truth. From this perspective it seems fair to say that this does not apply to any of the conjectures in this section. Some log log log devil (or any of its kin) might well be lurking somewhere...

The size of large prime gaps

Estimating the size of large prime gaps by establishing a small exponent α in

$$\sum_{\substack{p_n \le x \\ p_{n+1}-p_n \ge \sqrt{p_n}}} (p_{n+1}-p_n) = O(x^{\alpha}) \qquad (6)$$

is a sport. The current record is due to Heath-Brown [23], who established $\alpha = 3/5+\epsilon$, with ϵ any positive number. This result is very relevant for us, as we will see in the sequel. I include the table with 'exponent hunters', as it strongly suggests how much effort it often takes in prime number theory to achieve seemingly small improvements (see Table 2).

More on cyclotomic polynomials

From (1.3) it can be deduced by so-called Möbius inversion that

$$\Phi_n(X) = \prod_{d \mid n} (X^d-1)^{\mu(n/d)}, \qquad (7)$$

where the product is over all positive divisors d of n and μ is the *Möbius function* defined by $\mu(n) = (-1)^t$ if n is a square-free positive integer having t prime factors, and $\mu(n) = 0$ if n has a repeated prime factor.

exponent	author	year
0.9666	D. Wolke	1975
0.8674	R.J. Cook	1979
0.8243	M.N. Huxley	1980
0.8083	A. Ivić	1981
0.8055	R.J. Cook	1981
0.7501	D.R. Heath-Brown	1979
0.6944	A.S. Peck	1998
0.6666	K. Matomäki	2007
0.6001	D.R. Heath-Brown	2019

Table 2 Record exponents α in (6) over time.

Let p be a prime and n a positive integer. Then from (7) the following properties are easily deduced

1. $\Phi_{pn}(X) = \Phi_n(X^p)$ if p divides n;
2. $\Phi_{2n}(X) = (-1)^{\varphi(n)}\Phi_n(-X)$ if n is odd;
3. $\Phi_n(X) = X^{\varphi(n)}\Phi_n(1/X)$, that is, Φ_n is *self-reciprocal* if $n > 1$.

For example, using the first property we infer that $\Phi_{16}(X) = \Phi_2(X^8) = X^8+1$.

It is a classical result that if n has at most two distinct odd prime factors, then $A(n) = 1$, cf. Lam and Leung [27]. The first non-trivial case arises where n has precisely three distinct odd prime divisors and thus is of the form $n = p^e q^f r^g$, with $2 < p < q < r$ prime numbers. By repeatedly invoking the first property above we have $A\{p^e q^f r^g\} = A\{pqr\}$, and hence it suffices to consider only the case where $e = f = g = 1$ and so $n = pqr$. This motivates the following definition.

Definition 1. A cyclotomic polynomial Φ_n is said to be *ternary* if $n = pqr$, with $2 < p < q < r$ primes. In this case we call the integer n *ternary*.

An important subclass of these polynomials where we have even more control are the *optimal* ternary cyclotomic polynomials.

Definition 2. A ternary cyclotomic polynomial Φ_{pqr} is said to be *optimal* if its coefficients assume $p+1$ different values, that is $A\{pqr\}$ has cardinality $p+1$.

The usage of the word optimal comes from the fact that $p+1$ is the maximum number of distinct coefficients that can occur.

A special property of ternary cyclotomic polynomials is that consecutive coefficients differ by at most one (proven in [20]). Here an example:

$$\begin{aligned}\Phi_{11\cdot 13\cdot 17}(X) &= \cdots - X^{672} - 2X^{673} - 2X^{674} - 2X^{675} \\ &\quad - 3X^{676} - 4X^{677} - 3X^{678} \cdots\end{aligned}$$

It follows that $A\{n\}$ consists of consecutive integers if n is ternary (this is not true in general!). For example, $A\{11\cdot 13\cdot 17\} = \{-4,-3,\ldots,1,2,3\}$, as can be read off from Table 5. In the ternary case the behaviour of the coefficients is both non-trivial, but also understood so well, that we can use this to our benefit. This is not the case if n has four or more distinct odd prime factors. For optimal ternary cyclotomic polynomials the situation is even more under control, since if we know that $a_{pqr}(k_1) = b$ and $a_{pqr}(k_2) = a$, with $b-a = p$, then b must be the maximal coefficient and a the minimal one.

The family Φ_{pqr} with p fixed

In this subsection we briefly discuss other research on ternary coefficients.

The height $A(n)$ is unbounded if n ranges over the ternary integers. However, if we restrict to ternary n having a prescribed smallest prime factor $P(n) = p$, we get a bounded quantity $M(p)$. The definition of $M(p)$ can be stated more explicitly as

$$M(p) = \max\{A(pqr) : 2 < p < q < r\},$$

where p is a fixed odd prime and q,r range over the primes satisfying $r > q > p$. As the definition of $M(p)$ involves infinitely many cyclotomic polynomials, it is not clear whether there exists a finite procedure to determine it. Duda [15], during his internship at MPIM, provided such a procedure. It reduces the computation of $M(p)$ to the determination of the maximum value of $A(n)$, with n running through a *finite* set of ternary integers pqr. As the n involved are huge, the procedure is unfortunately not practical. It is a major open problem to find a *practical* procedure leading to explicit values of $M(p)$.

In 1971, Möller [35] gave a construction showing that $M(p) \ge (p+1)/2$ for $p > 5$. On the other hand, in 1968, Sister Marion Beiter [5] had conjectured that $M(p) \le (p+1)/2$ and shown that $M(3) = 2$ [7], which on combining leads to the conjecture that $M(p) = (p+1)/2$ for $p > 2$. The bound of Möller together with Beiter's [6] bound $M(5) \le 3$ shows that $M(5) = 3$. Zhao and Zhang [49] showed that $M(7) = 4$. Thus Beiter's conjecture holds true for $p \le 7$. Gallot and Moree [21] showed that Beiter's conjecture is false for every $p \ge 11$. Moreover, they showed that for every $\epsilon > 0$ we have $M(p) \ge (\frac{2}{3}-\epsilon)p$ and conjectured that always $M(p) \le 2p/3$, dubbing this conjecture the 'corrected Sister Beiter conjecture' (see Table 3).

The true behavior of $M(p)$ is much more complicated than suggested by Beiter's conjecture. For one, it is related to the distribution of inverses modulo primes p. Given any integer a coprime to p, any integer b with $ab \equiv 1 \pmod p$ is its *modular*

p	3	5	7	11	13	17	19	23	29	31	37	41
$(p+1)/2$	2	3	4	6	7	9	10	12	15	16	18	21
$M(p)\geq$	2	3	4	7	8	10	12	14	18	19	22	26
$[2p/3]$	2	3	4	7	8	11	12	15	19	20	24	27

Table 3 Some numerical evidence for the corrected Sister Beiter conjecture.

inverse. The collection of points (a,b) with $0<a,b<p$ is called the *modular hyperbola*; for a survey see Shparlinski [42]. The distribution of points on the modular hyperbola is traditionally investigated using the *Kloosterman sum* $K(a,b;p)$, which is defined as

$$K(a,b;p)=\sum_{1\leq x\leq p-1} e^{2\pi i(ax+b\bar{x})/p},$$

with $\bar{x}$ any modular inverse of x modulo p. (As an aside we note that the Dutch word kloosterman means 'cloister man' and thus the cloister man sums can be used to investigate a conjecture of a nun. Honi soit qui mal y pense! Reader beware: too intense study of these sums and their applications can lead to 'Kloostermania' [34].) By a fundamental result of Weil we have $|K(a,b;p)|\leq 2\sqrt{p}$, which can be used to show that $M(p)>2p/3-3p^{3/4}\log p$ (see Cobeli et al. [12]).

In Figure 2 we display part of the modular hyperbola mod 241 that is relevant in constructing a sharp lower bound for $M(241)$ in the work of Gallot and myself. It gives integer pairs (a,b) with $1\leq a,b\leq 240$ in certain triangles with $ab\equiv 1 (\mathrm{mod}\ 241)$. For a detailed analysis of this construction, see Cobeli et al. [12].

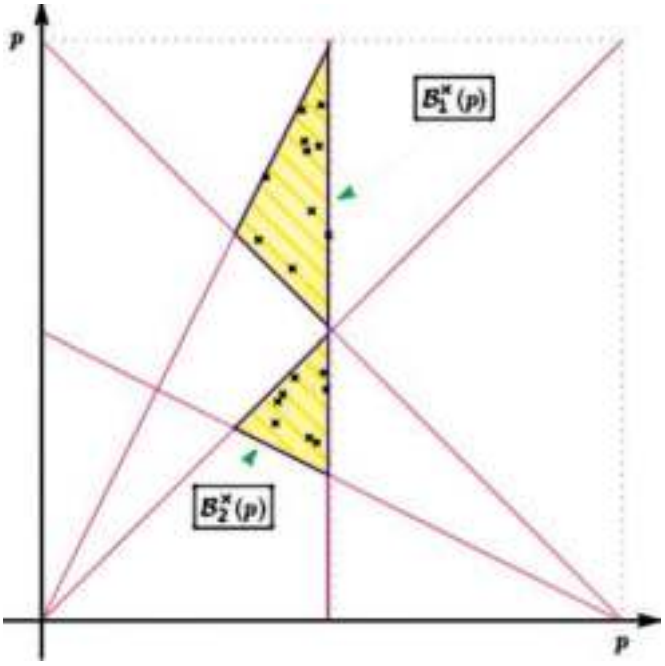


Figure 2 $M(241)$ estimation relevant part of modular hyperbola $\mathrm{mod}\ 241$.

Our results on the maximum coefficient

In this section I finally return to Question 1 and discuss the recent progress made on it in my paper with Kosyak, Sofos and Zhang [26]. It relies on a construction found by my former intern Eugenia Roşu (using only paper!). For certain primes p it improves on an earlier construction by Gallot and myself (found using paper... and computer). The original formulation is quite lengthy, however for us the following watered down version will do.

Theorem 1 (Moree and Roşu [38]). *Let $m\geq 0$ be an arbitrary integer and $p\geq 4m^2+2m+3$ be any prime. Then there exist primes q_1, r_1, q_2, r_2 such that $\Phi_{pq_1r_1}$ and $\Phi_{pq_1r_1}$ have maximum coefficient $(p-1)/2-m$, respectively $(p+1)/2+m$.*

This shows that the set of cyclotomic maximum coefficients we can obtain certainly contains

$$\begin{aligned}\mathcal{R}:=&\left\{\frac{p-1}{2}-m\colon p \text{ is a prime},\right.\\ &\left. m\geq 0, 4m^2+2m+3\leq p\right\}\\ \cup&\left\{\frac{p-1}{2}+m\colon p \text{ is a prime},\right.\\ &\left. m\geq 0, 4m^2+2m+3\leq p\right\}.\end{aligned}$$

We conjecture that this set equals the set of all natural numbers, thus implying that each natural number can arise as maximum coefficient of some cyclotomic polynomial. Roughly speaking $\mathcal{R}$ is a union of integers in intervals of the form $((p-1)/2-\sqrt{p}/2, (p-1)/2+\sqrt{p}/2)$, and thus if the gaps between successive primes are *always* sufficiently small, all natural integers will be covered. Working out the technicalities one arrives at the following result.

Theorem 2. *If $p_{n+1}-p_n<\sqrt{p_n}+\sqrt{p_{n+1}}$ holds for $p_n\leq 2h$, then the integers $1,2,\ldots,h$ are in $\mathcal{R}$. Andrica's conjecture, Conjecture 2, implies that every natural number occurs as the maximum coefficient of some ternary cyclotomic polynomial.*

A lot of numerical work on large gaps has been done (see the website [39]). This can be used to infer that the inequality in Theorem 2 holds for $p_n\leq 2\cdot 2^{63}\approx 1.8\cdot 10^{19}$, leading to the following corollary.

Corollary 1. *Every integer up to $9\cdot 10^{18}$ occurs as the maximal coefficient of some ternary cyclotomic polynomial.*

If holes in the set $\mathcal{R}$ appear, it is when $p_{n+1}-p_n\geq\sqrt{p_n}+\sqrt{p_{n+1}}$. The number of natural numbers up to x that are not in $\mathcal{R}$ (if any), is close to

$$\begin{aligned}&\sum_{\substack{p_n\leq 2x\\ d_n\geq\sqrt{p_n}+\sqrt{p_{n+1}}}}(d_n-\sqrt{p_n}-\sqrt{p_{n+1}})\\ &\leq \sum_{\substack{p_n\leq 2x\\ d_n\geq\sqrt{p_n}+\sqrt{p_{n+1}}}} d_n \leq \sum_{\substack{p_n\leq 2x\\ d_n\geq\sqrt{p_n}}} d_n.\end{aligned}$$

Now the reader might be reminded of (6). An easy climb on the shoulders of giants in analytic number theory then leads to the following result.

Theorem 3. *For any fixed $\epsilon>0$, there exists a constant C_ϵ such that the number of positive integers $\leq x$ that do not occur as a height of a ternary cyclotomic polynomial is at most $C_\epsilon x^{3/5+\epsilon}$. Under the Riemann Hypothesis this number is at most $C_\epsilon x^{1/2+\epsilon}$.*

A different approach

Let $h>1$ be odd. If there exists a prime $p\geq 2h-1$ such that $q:=1+(h-1)p$ is a prime too, then for some prime $r>q$ it can be shown that Φ_{pqr} has maximum coefficient h. This is a consequence of work of Gallot, Moree and Wilms [22] and involves ternary cyclotomic polynomials that are not optimal. For some choices of h,p and q see Table 4.

Conjecture 3. *Let $h>1$ be any odd integer. There exists a prime $p\geq 2h-1$, such that $1+(h-1)p$ is a prime too.*

This conjecture is a consequence of the widely believed Bateman–Horn conjecture [1], which implies that, given an arbitrary odd integer $h>1$, there are *infinitely* many primes p such that $1+(h-1)p$ is a prime too.

Theorem 4. *If Conjecture 3 holds true, then every positive odd natural number occurs as maximal coefficient of some ternary cyclotomic polynomial. Unconditionally a positive fraction of all odd natural numbers occur as maxima.*

Our proof of the second assertion makes use of deep work of Bombieri, Friedlander and Iwaniec [8] on the level of distribution of primes in arithmetic progressions with fixed residue and varying moduli. Although the unconditional statement in Theorem 4 is surpassed by the unconditional statement in Theorem 3, the proof of Theorem 4 is, in a way, 'orthogonal' to the one of Theorem 3; it thus has the potential of working for variations of the problem where the method behind Theorem 3 would fail. Interestingly, like our prime gap criterion, it rests on a variation of a certain very well studied problem involving prime numbers. Both prime number questions are, however, quite different. In [26] we also obtain the same type of results as described in the previous section for the minimum coefficient and for the height. In case of the height a conjecture slightly stronger than Andrica's enters the game.

h	p	q
3	5	11
5	13	53
55	139	7507
117	263	30509
219	449	997883

Table 4 Smallest choice of $p\geq 2h-1$ with $q:=1+(h-1)p$ prime.

height	p	q	r	k	sign	diff.
1	3	7	11	0	+	2
2	3	5	7	7	−	**3**
3	5	7	11	119	−	**5**
4	11	13	17	677	−	7
5	11	13	19	1008	−	9
6	13	23	29	2499	−	10
7	17	19	53	6013	+	14
8	17	31	37	5596	−	14
9	17	47	53	14538	−	**17**
10	17	29	41	4801	−	**17**

Table 5 Minimal ternary examples with prescribed height.

Conjecture 4. *Every natural number occurs as the height of some cyclotomic polynomial.*

We demonstrate this in Table 5, which gives the minimum ternary integer $n=pqr$ with $p<q<r$ such that Φ_n has height m for the numbers $m=1,\ldots,10$. The integer k has the property that $a_{pqr}(k)=\pm m$, with the sign coming from the sixth column. The seventh column records the difference between the largest and smallest coefficient and is in bold if this is optimal, that is, if the difference equals p (compare Definition 2). See [26] for the continuation of the table up to $m=40$.

Prime differences make their appearance since in our approach we work with ternary cyclotomic polynomials. One would want to work with Φ_n with n having at least

With Bogdan Petrenko and MPIM interns Oana-Maria Camburu, Jessica Fintzen and Eugenia Roşu (from left to right).

four prime factors; however, this leads to a loss of control over the behaviour of the coefficients in general and the maximum, minimum and height in particular. Prime number properties play a true role if one asks for the possible heights $A(n)$ and extrema of $A\{n\}$ with n restricted to ternary integers.

Further reading

For a popular account on prime gaps in Dutch see one of the chapters in Van den Brandhof [47], who speaks of them as 'Priemwoestijnen' (prime deserts). Ribenboim's book [41] gives a wealth of results on prime numbers and their distribution. It can be thought of as a number-theoretical version of the Guinness Book of Records. Also some of the underlying mathematics is explained. For a computational history of prime numbers and Riemann zeros see [37]. The truly courageous might have a go at the monumental book of Landau [28].

Acknowledgment

I would like to thank Alexandru Ciolan, Kate Kattegat, Alexandre Kosyak and Lola Thompson for proofreading earlier versions, and Igor Shparlinski for a mathematical comment. Figure 2 was provided by Cristian Cobeli. The part of the Table 2 up to 1981 is taken from Ivić [25, p. 350], who also gives a proof of the 1979 result of Heath-Brown. Table 3 was computed by Yves Gallot, and Table 5 by Bin Zhang.

Since 2005 I have regularly guided budding mathematicians for one month internships. I dedicate this article to them for their youthful enthusiasm, energy, fresh outlook at life and mathematical creativity.

References

1 S.L. Aletheia-Zomlefer, L. Fukshansky and S.R. Garcia, The Bateman-Horn conjecture: heuristics, history and applications, *Expos. Math.* 38 (2020), 430–479.

2 A. Arnold and M. Monagan, http://www.cecm.sfu.ca/~ada26/cyclotomic/.

3 R.C. Baker, G. Harman and J. Pintz, The difference between consecutive primes. II, *Proc. London Math. Soc. (3)* 83 (2001), 532–562.

4 W. Banks, K. Ford and T. Tao, Large prime gaps and probabilistic models, arXiv:1908.08613.

5 M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$, *Amer. Math. Monthly* 75 (1968), 370–372.

6 M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}. II, *Duke Math. J.* 38 (1971), 591–594.

7 M. Beiter, Coefficients of the cyclotomic polynomial $F_{3qr}(x)$, *Fibonacci Quart.* 16 (1978), 302–306.

8 E. Bombieri, J.B. Friedlander and H. Iwaniec, Primes in arithmetic progressions to large moduli. II, *J. Math. Ann.* 277 (1987), 361–393.

9 K. Broughan, *Equivalents of the Riemann Hypothesis*, Vol. 2, Analytic equivalents, Encyclopedia of Mathematics and its Applications 165**,** Cambridge University Press, 2017.

10 K. Broughan, *Bounded Gaps between Primes: The Epic Breakthroughs of the Early 21st Century,* Cambridge University Press, 2021.

11 E. Carneiro, M.B. Milinovich and K. Soundararajan, Fourier optimization and prime gaps, *Comment. Math. Helv.* 94 (2019), 533–568.

12 C. Cobeli, Y. Gallot, P. Moree and A. Zaharescu, Sister Beiter and Kloosterman: a tale of cyclotomic coefficients and modular inverses, *Indag. Math.* 24 (2013), 915–929.

13 H. Cramér, Some theorems concerning prime numbers, *Arkiv f. Math. Astr. Fys.* 15 (1920), 1–33. [*Collected Works* 1, Springer, 1994, pp. 85–91.]

14 H. Cremer, *Carmina mathematica und andere poetische Jugendsünden*, 7. Aufl., Verlag J. A. Mayer, 1982.

15 D. Duda, The maximal coefficient of ternary cyclotomic polynomials with one free prime, *Int. J. Number Theory* 10 (2014), 1067–1080.

16 P. Erdős, On the difference of consecutive primes, *Quart. J. of Math.* 6 (1935), 124–128.

17 J. Fintzen, Cyclotomic polynomial coefficients $a(n,k)$ with n and k in prescribed residue classes, *J. Number Theory* 131 (2011), 1852–1863.

18 K. Ford, B. Green, S. Konyagin and T. Tao, Large gaps between consecutive prime numbers, *Ann. of Math. (2)* 183 (2016), 935–974.

19 K. Ford, B. Green, S. Konyagin, J. Maynard and T. Tao, Long gaps between primes, *J. Amer. Math. Soc.* 31 (2018), 65–105.

20 Y. Gallot and P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, *J. Ramanujan Math. Soc.* 24 (2009), 235–248.

21 Y. Gallot and P. Moree, Ternary cyclotomic polynomials having a large coefficient, *J. Reine Angew. Math.* 632 (2009), 105–125.

22 Y. Gallot, P. Moree and R. Wilms, The family of ternary cyclotomic polynomials with one free prime, *Involve* 4 (2011), 317–341.

23 D.R. Heath-Brown, The differences between consecutive primes. V, *Int. Math. Res. Not. IMRN,* to appear, Doi: 10.1093/imrn/rnz295.

24 M.N. Huxley, On the difference between consecutive primes, *Invent. Math.* 15 (1972), 164–170.

25 A. Ivić, *The Riemann Zeta-Function*, Wiley, 1985.

26 A. Kosyak, P. Moree, E. Sofos and B. Zhang, Cyclotomic polynomials with prescribed height and prime number theory, *Mathematika* 67 (2021), 214–234.

27 T.Y. Lam and K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, *Amer. Math. Monthly* 103 (1996), 562–564.

28 E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, 2 Bände, with an appendix by P.T. Bateman, Chelsea Publishing, 1953, 2nd ed.

29 E. Lehmer, On the magnitude of the coefficients of the cyclotomic polynomials, *Bull. Amer. Math. Soc.* 42 (1936), 389–392.

30 H. Maier, Primes in short intervals, *Michigan Math. J.* 32 (1985), 221–225.

31 H. Maier, Small differences between prime numbers, *Michigan Math. J.* 35 (1988), 323–344.

32 J. Maynard, Small gaps between primes, *Ann. of Math.* 181 (2015), 131.

33 J. Maynard, Large gaps between primes, *Ann. of Math.* 183 (2016), 915–933.

34 P. Michel, Some recent applications of Kloostermania, *Physics and Number Theory*, IRMA Lect. Math. Theor. Phys. 10, European Mathematical Society, 2006, pp. 225–251.

35 H. Möller, Über die Koeffizienten des $n$ten Kreisteilungspolynoms, *Math. Z.* 119 (1971), 33–40.

36 P. Moree, Irregular behaviour of class numbers and Euler-Kronecker constants of cyclotomic fields: the log log log devil at play, in J. Pintz and M.Th. Rassias, eds., *Irregularities in the Distribution of Prime Numbers – Research Inspired by Maier's Matrix Method*, Springer, 2018, pp. 143–163.

37 P. Moree, I. Petrykiewicz and A. Sedunova, A computational history of prime numbers and Riemann zeros, arXiv:1810.05244.

38 P. Moree and E. Roşu, Non-Beiter ternary cyclotomic polynomials with an optimally large set of coefficients, *Int. J. Number Theory* 8 (2012), 1883–1902.

39 T.R. Nicely, First occurrence prime gaps, http://www.trnicely.net/gaps/gaplist.html.

40 R.A. Rankin, The difference between consecutive prime numbers, *J. London Math. Soc.* 11 (1936), 242–245.

41 P. Ribenboim, *The Book of Prime Number Records*, Springer, 1989, 2nd ed.

42 I. Shparlinski, Modular hyperbolas, *Jpn. J. Math.* 7 (2012), 235–294.

43 Z.W. Sun, On a sequence involving sums of primes, *Bull. Aust. Math. Soc.* 88 (2013), 197–205.

44 J. Suzuki, On coefficients of cyclotomic polynomials, *Proc. Japan Acad. Ser. A Math. Sci.* 63 (1987), 279–280.

45 R. Thangadurai, On the coefficients of cyclotomic polynomials, *Cyclotomic Fields and Related Topics* (Pune, 1999), 311–322.

46 L. Thompson, (Mind the) gaps between primes, *Nieuw Archief voor Wiskunde* 5/22 (2021), 212–218, this issue.

47 A. van den Brandhof, *Priemwoestijnen*, Uitgever Prometheus, 2018.

48 S. Weintraub, Several proofs of the irreducibility of the cyclotomic polynomials, *Amer. Math. Monthly* 120 (2013), 537–545.

49 J. Zhao and X. Zhang, Coefficients of ternary cyclotomic polynomials, *J. Number Theory* 130 (2010), 2223–2237.

Jan van Neerven
Faculty EEMCS
TU Delft
j.m.a.m.vanneerven@tudelft.nl

News **Koninklijk Wiskundig Genootschap**

Indagationes Mathematicae: A status report

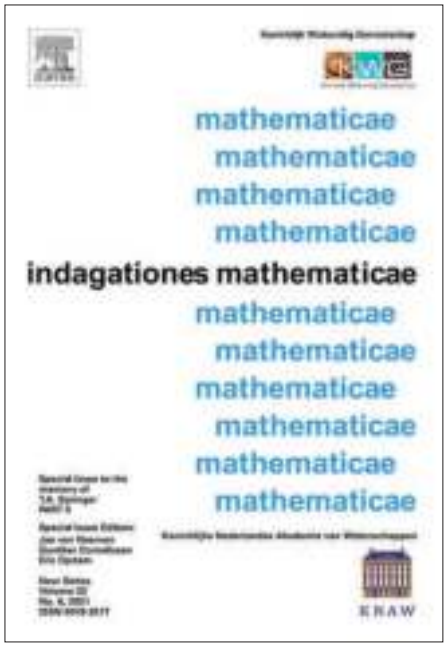
Indagationes Mathematicae is the international peer reviewed mathematics journal of the KWG. The Editor-in-Chief Jan van Neerven describes this article some recent changes in the editorial process and policies, and reports on the journal's present performance.

Formerly published by the Royal Netherlands Academy of Arts and Sciences (KNAW), *Indagationes Mathematicae* has been transferred in 2010 to the Royal Dutch Mathematical Society (KWG) [1], which is now in charge of its editorial policies. A history of the journal has been written by Jaap Korevaar and Rob Tijdeman [2]. Indagationes's aims and scope (see [8]) include

> "...the publication of original mathematical research papers of high quality and of interest to a large segment of the mathematics community."

Review papers of high quality are welcomed as well. Indagationes publishes six issues per year of approximately 200–250 pages each, some of them being Special Issues dedicated to important events in the Dutch mathematics community (see the box below). Around 250–300 submissions are received yearly, of which approximately 25% gets accepted; this figure includes regular and Special Issues.

On behalf of the KWG, the journal is published by Elsevier, which pays royalties to the KWG based on page views and downloads.



Recent and upcoming Specials Issues

Special Issue dedicated to the memory of J.W. Cohen (expected 2022)
Editors: Onno Boxma and Michel Mandjes

Special issue to the memory of T.A. Springer (3 issues, 2021–22)
Editors: Gunther Cornelissen, Eric Opdam

Special Issue in memory of Hans Duistermaat (2021)
Editors: Gunther Cornelissen, Jan van Neerven

Special Issue dedicated to the memory of Wim Luxemburg (2020)
Editors: Peter G. Dodds, Ben de Pagter, Anton R. Schep

Aperiodic Patterns in Crystals, Numbers, and Tiles (2018)
Editors: Carlo Carminati, Alex Clark, Robbert Fokkink, Cor Kraaikamp, Tom Schmidt, Rob Tijdeman

L.E.J. Brouwer, 50 years later (2 issues, 2017–18)
Editors: Dirk van Dalen, Geurt Jongbloed, Jan Willem Klop, Jan van Mill

Special Issue on Automatic Sequences, Number Theory, and Aperiodic Order (2017)
Editors: Valérie Berthé, Frits Beukers, Alex Clark, Robbert Fokkink, Cor Kraaikamp

Policy and Editorial Board

The editorial board has been rejuvenated, internationalised, diversified and restructured (see the box below). To begin with the latter, four 'Editors' (covering Geometry & Number Theory, Algebra & Discrete Mathematics, Probability & Statistics, and Analysis) have been appointed to serve as intermediates between the Editor in Chief and the board of approximately 25 Associate Editors. Their task is to screen incoming submissions for mathematical quality and relevance, and hand over the strong papers to one of the Associate Editors for the actual handling. By default two referee reports are solicited.

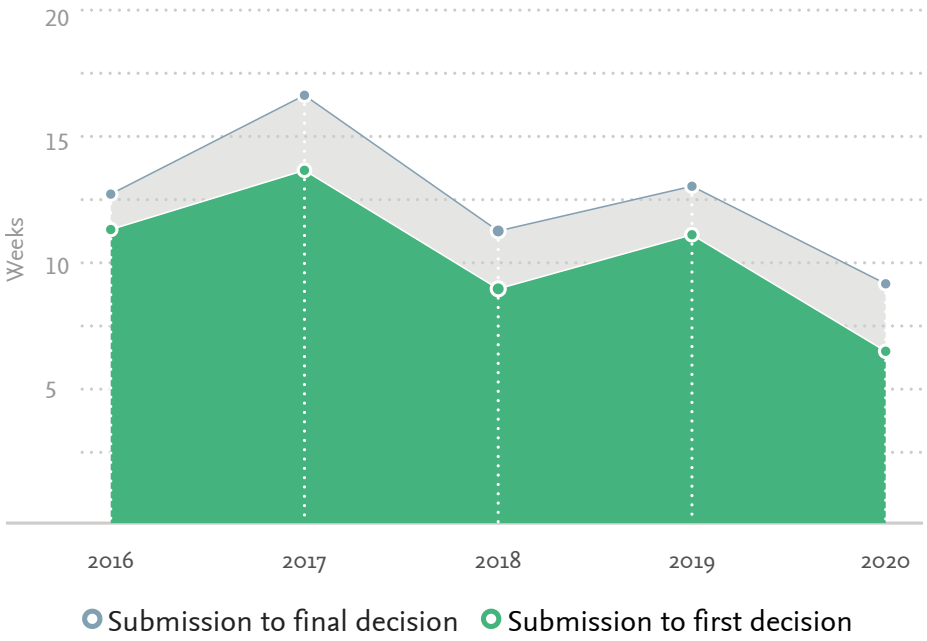


Figure 1 Review speed Indagationes Mathematicae [6].

With the appointment of fifteen new (mostly mid-career) Associate Editors, the editorial board is dynamic and relatively young. With an average submission-to-acceptance time of *6.8 weeks* and online publication time of *1 week* in 2020, papers get published comparatively fast (see Figure 1. Submissions whose lengths do not exceed fifteen pages enter a newly created *fast track* guaranteeing the authors a handling time of at most six months. Editors are appointed for a 4-year term.

Open Access and arXiv

Indagationes Mathematicae is a so-called 'Hybrid Open Access journal'. As such it is included in Elsevier's transformative agreements, which guarantee that papers submitted by corresponding authors affiliated with member institutions of participating organisations get published in Gold Open Access free of charge. All institutions hosting a mathematics department in the Netherlands and in many European countries fall under these agreements. In particular any paper submitted by a corresponding author at a Dutch university will be published in Gold Open Access free of charge. A complete list of participating organisations can be found on the website [7].

As of 2019, it was decided to only handle papers posted on the preprint server arXiv prior to submission. Providing the arXiv identifier is part of the submission procedure and submissions not complying with this requirement receive a desk reject. Effectively, this makes the journal into a Green Open Access journal. As it turned out, this policy had the further beneficial advantage of considerably decreasing the number of low-quality submissions — a problem that most general mathematics journal face. Statistical research carried out prior to the installation of this policy had revealed that nearly 100% of the pre-2019 submissions that were not posted on arXiv had been re-

METRICS

YEAR	CITESCORE	CITESCORE PERCENTILE	CITATIONS	DOCUMENTS
2020	1.7	69	528	319
2019	1.6	69	521	335
2018	1.2	61	409	335
2017	1.0	50	316	312
2016	0.8	42	219	263

Figure 2 Various metrics over the past 5 years [4].

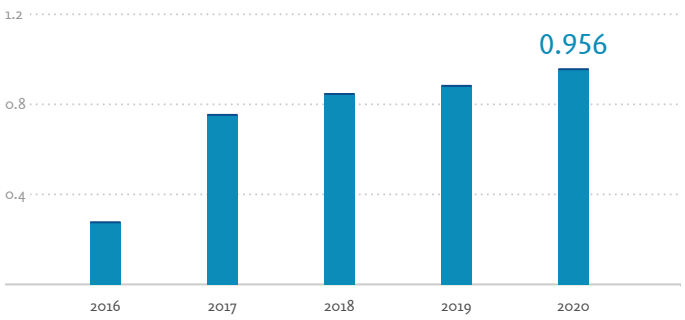


Figure 3 Impact factor over the past 5 years [5].

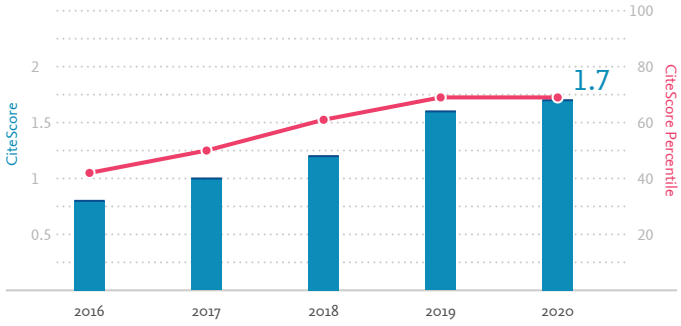


Figure 4 CiteScore over the past 5 years [4].

jected. The total volume of submissions has gone down by an estimated 25% due to this policy, but there has been no adverse effect on the volume of strong papers.

Special issues

Since 2011, 17 Special Issues have been published and several others are in various stages of planning. The most recent Special Issues are listed in the box on the first page. The full list is available on the journal's website [8] and include issues in memory of L. E. J. Brouwer (50 years later), Wim Luxemburg (memorial issue), Hans Duistermaat (10 years later), and Tonny Springer (10 years later). Articles for Special Issues are solicited by a guest editorial board on the basis of invitation-only. Ideas for future SI's are always welcome.

Stats

Some metrics about the journal's performance are presented in Figure 2. The current journal's Impact Factor (the number of times an average paper in the journal is cited during the preceding two years) equals 0.956, representing an increase by 0.596 in the last five years, see Figure 3. The current CiteScore (the average citations in the past four years (2017–2020) received per article) equals 1.7, an increase by 0.76 in the last five years, see Figure 4. (Elsevier uses the Clarivate metrics, https://clarivate.com).

Journal	Impact Factor
Ann. Mat. Pura Appl.	0.969
Ann. Instit. Poincaré	0.968
Kyoto J. Math.	0.964
Math. Z.	0.964
Indag. Math.	**0.956**
J. Math. Soc. Japan	0.949
Period. Math. Hungar.	0.940
Israel J. Math.	0.907
Ark. Mat.	0.896

Table 1 Journals with comparable impact factor [3].

Indagationes currently ranks among the Q2 (second quartile) journals. Although it is in good company (see Table 1), the long-term aim is to make it into the Q1 quartile: it is not uncommon that grant agencies impose an obligation to publish in Q1 journals only.

Submit a paper!

Despite good performance, speedy handling, and upward trends, the number of submissions from our own community remains very low: in the regular issues of both 2019 and in 2020, only around five papers have appeared with a Netherlands-based corresponding author, an average of one per issue. I close with expressing the hope that you, reader, after having read this article, will submit a paper to *Indagationes Mathematicae*.

References

1 Henk Broer, Indagationes Mathematicae, *Nieuw Archief voor Wiskunde* 5/12(4) (2011), 234.
2 Jaap Korevaar and Rob Tijdeman, De geschiedenis van Indagationes Mathematicae, *Nieuw Archief voor Wiskunde* 5/14(1) (2013), 66–72.
3 https://impactfactorforjournal.com/jcr-2021.
4 https://journalinsights.elsevier.com/journals/0019-3577/citescore.
5 https://journalinsights.elsevier.com/journals/0019-3577/impact_factor.
6 https://journalinsights.elsevier.com/journals/0019-3577/review_speed.
7 https://www.elsevier.com/open-access/agreements.
8 https://www.journals.elsevier.com/indagationes-mathematicae.

Daan Mulder
promovendus AMOLF, Amsterdam
mulderdaan@live.nl

Het keerpunt van Durk Jan de Bruin

Ze hebben in het onderwijs meer geduld met je dan in het bedrijfsleven

Tussen de studenten met wie ik de lerarenopleiding volgde, was Durk Jan de Bruin een opvallende verschijning: al grijs, dat wel, maar minstens zo energiek als de twintigers met wie hij had besloten de collegebanken te delen. Voordat hij als leraar begon, zo bleek uit het voorstelrondje, had De Bruin als internetondernemer Startpagina.nl opgericht.

Hoe was je zelf als middelbare scholier?
"Eerlijk gezegd: ik had een goede Citotoets, en ben begonnen in 1 vwo, maar ik ben na één jaar gecrasht en kwam op de mavo terecht. Ik heb geen havo gezien. Het was me altijd komen aanwaaien, en nu moest ik ineens mijn best doen. Misschien maakte het ook wel uit dat ik een autistisch broertje heb. Mijn moeder was veel met hem bezig, en mijn vader was veel aan het werk. Ik had eigenlijk weinig begeleiding van mijn ouders, die hebben mij op school lekker laten klooien zonder ooit gevraagd te hebben of mijn huiswerk al af was. Zelf was ik ook helemaal niet met school bezig. Ik zat bij de Anthony Fokkerclub, en dat vond ik geweldig: van balsahout modelbouwvliegtuigjes maken.

In 3 mavo heb ik mijn eerste bedrijf opgericht. Ik zat bij een fotoclub en daar fotografeerde ik de schoolboeken, die ik dan heel klein afdrukte en verkocht als spiekbriefjes. Dat was een goudmijn, totdat er iemand betrapt werd. Dat was toevallig een meisje met rijke ouders, en het management van de school verdacht haar ouders ervan dat ze geholpen hadden en er geld in hadden gestoken. Hoe was ze anders aan die afdrukken gekomen? Tegenwoordig heb je overal printers, maar toen had je die niet. Het lullige was dat ik het briefje niet eens aan haar verkocht had: ik had het aan iemand anders verkocht en die had het weer doorverkocht. Ik was wel pissig: iemand gepakt met mijn briefje en ik ben niet eens betaald!"

Durk Jan de Bruin

Kom je uit een bèta-nest?
"Nul komma nul nul nul. Mijn vader was vice-president van een rechtbank. Hij is ook de oprichter van Amnesty International in Nederland, daar ben ik wel trots op. Mijn moeder was doctor in de Nederlandse letteren, en was lerares Nederlands. Allebei wisten ze niks van wiskunde, of techniek of scheikunde. Maar, wat mijn vader altijd zei, het slaat soms generaties over: mijn opa was weer onderdirecteur bij Philips, die was wel technisch. Als je ouders niks kunnen, word je als kind snel gevraagd een spijker in de muur te slaan om een schilderij op te hangen. Terwijl ik mijn vader nog nooit met gereedschap aan de gang heb gezien.

Na mijn middelbare school heb ik hts werktuigbouwkunde gedaan. Wat later ben ik bij de échte Fokker gaan werken, in de tekenkamer. Na een reorganisatie plaatsten ze mij bij de IT-afdeling, al wist ik helemaal niks van IT. Dat ga je maar leren, zeiden ze. Ik dacht: ik zit hier nu, laat ik er het beste van maken. Blijkbaar wil de kosmos dat ik nu deze weg ga bewandelen. Je kan het ook serendipiteit

noemen: dat je iets vindt waar je niet naar op zoek bent. Ik had geen universiteitsdiploma, mijn ouders allebei wel, dus ik wilde ook graag in hun voetsporen gaan treden.

De enige manier waarop ik op de universiteit informatica kon studeren was in Leiden, bij de wiskundefaculteit. Op dinsdag en donderdag ging ik uit mijn werk bij Fokker naar Leiden. Dat was van 1990 tot 1997.

In de tijd dat ik studeerde, en dat was ook een groot toeval, was het internet net in opmars. Via de universiteit leerde ik heel wat van internet, terwijl niemand in de gewone wereld nog wat van internet wist. Ik had voor mezelf een homepage gemaakt, djdebruin.com geloof ik, en wat websites voor de universiteit. Als afstudeeropdracht was ik met e-commerce bezig.

Toen heb ik Startpagina.nl opgericht, eigenlijk voor mijn vader als een soort hulppagina. Die pagina werd een enorm succes. Het groeide heel wiskundig, met een mooie trendlijn van meer en meer en meer bezoekers."

Had je enig idee hoe het zo groot werd?
"In het begin ben ik wel langs geweest in bibliotheken, om daar Startpagina.nl op de computers te zetten. En ook in computerwinkels: ik ging allemaal winkels langs en deed alsof ik een nieuwe computer wilde kopen. Ondertussen installeerde ik Startpagina.nl: 'Oh, mag ik die computer daar ook nog proberen?'

Zo begon het langzaam te lopen. Het was een jongensdroom die uitkwam, het werd gewoon de nummer 1 van Nederland. Startpagina.nl stond regelmatig in de krant, ik werd vaak gebeld.

Dat maakte het ook spannend: ik werd heel veel gekopieerd, er kwamen allemaal mensen die hetzelfde trucje gingen doen. Ik bleef druk bezig om mijn voorsprong te behouden. Met een bedrijf is het altijd spannend: dan gaat het weer omhoog, dan zakt het weer een beetje in. Je moet nooit, als je er goed voor staat, gaan roepen: ik ben zo goed en zo geweldig. Integendeel: je bent erop gericht te blijven verbeteren.

In 2000 heb ik het voor een enorm bedrag verkocht aan Sanoma, en toen hoefde ik plots niet meer te werken. Als je ineens een hoop geld hebt, kun je met een hengel langs de rivier gaan zitten, maar dat is ook weer niet uitdagend. De vraag blijft: wat doe je met je leven?

Toen heb ik een e-commerce-site opgericht, MijnWinkel.nl, of MyShop.com. Dat was een site waarmee je makkelijk een webwinkel kon maken. Mijn afstudeerproject van de universiteit ging daar ook over, en dat wilde ik realiseren. Dat is in Nederland best een succes geweest. ANWB, KLM, dat soort bedrijven zaten erbij. Ook dat heb ik verkocht. Ik was toch wel weer blij dat ik ervan af was. Dat klinkt misschien raar. Maar, als ik een internetbedrijf heb, dan kan ik niet zomaar op vakantie gaan. Ik ben er dan 24 uur per dag, 7 dagen in de week mee bezig."

En toen werd je leraar?
"Nou, ik was bijna een soort pensioen gaan houden: ik had Startpagina.nl verkocht, ik had MyShop.com verkocht. Maar er was een coach die in een persoonlijke ontwikkelingscursus tegen mij zei: jouw doel is leraar worden. En op een gegeven moment belde iemand op: 'Durk Jan, je moet meekomen, op het Haarlem College is er een open dag voor zij-instromers.' Dat vond ik leuk: al bleek dat ik met mijn opleiding geen zij-instroomtraject moest doen, maar de post-universitaire lerarenopleiding. Dan was ik in een jaar eerstegraads bevoegd. Ik ging googelen, en wat bleek: ik had nog drie dagen om me in te schrijven. Toen dacht ik: dit komt nu zo op mijn pad, blijkbaar moet dit zo.

Ik begon als informatica leraar-in-opleiding. In het begin heb ik zoveel fouten gemaakt; mijn begeleider moest soms ingrijpen om het weer stil te krijgen. Maar hij werd ziek, en toen kreeg ik de vraag: wil jij het doen? Na een week ben ik naar de afdelingsleider gegaan en heb ik gezegd: ik kan dit niet, ze breken de hele boel af. Er werd met vliegtuigjes gegooid, leerlingen zetten elkaars computer uit. Maar die afdelingsleider zei: maakt niet uit, ga maar lekker door. Ze hebben in het onderwijs meer geduld met je dan in het bedrijfsleven. Ik ben gaan zorgen dat het elke les een beetje beter ging. Ik zie het, nog steeds, bijna als een cursus persoonlijke ontwikkeling. Maar het is wel een cursus waarbij alles wat je niet goed doet, keihard afgestraft wordt.

Als ik nu op school geweest ben, is het alsof mijn vliegwiel harder is gaan draaien. Ik ben een groepsmens, ik floreer in de klas. Ook omdat ik het gevoel heb dat ik nuttig gevonden word. En er is gewoon zoveel vraag naar leraren. Ik ben nu 58, maar ze zitten aan alle kanten aan me te trekken. Dat is een heerlijk gevoel: ik ben nuttig! Ik ben niet te oud, of uitgerangeerd, of ingehaald door de jonkies. Ik zat daarvoor in een tijd waarin ik niks hoefde te doen, en toen was ik ineens weer keihard aan het studeren.

In mijn eerste jaar op de UvA zat ik veel met informatica- en wiskundedocenten samen. Er zat een jongen met dezelfde vooropleiding als ik juist bij wiskunde. Ik dacht: hé, als hij dat kan doen, waarom doe ik dat dan niet ook? Na mijn informaticajaar ben ik doorgegaan om ook mijn eerstegraads bevoegdheid voor wiskunde te halen: ik wilde doorstuderen. Ik wilde eigenlijk daarna ook nog de opleiding tot natuurkundeleraar doen, maar toen kwamen de vakdidactici van wiskunde en informatica naar me toe met de boodschap: we hebben eigenlijk iemand nodig op de UvA, als lerarenopleider. Dus ik ben nu leraren aan het opleiden én daarnaast ben ik nog les aan het geven op de middelbare school.

Nu vind ik het wel mooi dat ik als mavo-jongen voor wie wiskunde een heel slecht vak was — ik ging volgens mij over van 2 naar 3 mavo met een 'taak' voor wiskunde, wiskundehuiswerk voor in de zomervakantie — dat ik uiteindelijk universiteit gedaan heb, informatica en wiskunde geef op het vwo, nu ook op de universiteit met wiskunde te maken heb én het een prachtig vak vind. Dat vind ik een soort revanche op mezelf."

Meer lezen? Zie het boek *Van zolderkamer tot miljoenenbusiness* dat De Bruin met journalist Huib van der Stam schreef. Een ander project van De Bruin is mygoosebumpmoment.com, waar hij 'kippenvelmomenten' van over de hele wereld spaart.

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

Johan Commelin
Mathematisches Institut
Albert-Ludwigs-Universität Freiburg
jmc@math.uni-freiburg.de

Onderzoek

Liquid Tensor Experiment

Het *Liquid Tensor Experiment* betreft een project om de in 2019 door Dustin Clausen en Peter Scholze bewezen hoofdstelling van liquide vectorruimtes met behulp van een computer te verifiëren. In de achterliggende maanden heeft een team van wiskundigen dit project grotendeels afgerond. Johan Commelin vertelt in dit artikel wat het project inhoudt.

Op 5 November 2020 schreef Peter Scholze een blogpost [8,9] op de weblog van het Xenaproject van Kevin Buzzard. In deze blogpost poneerde hij een uitdaging om recent werk in de liquide wiskunde met behulp van een computer formeel te verifiëren. Een divers team wiskundigen, waaronder ikzelf, is deze uitdaging aangegaan.

Liquide wiskunde [6] is een deelgebied van gecondenseerde wiskunde [7], wat op zichzelf een nieuw vakgebied in de wiskunde is. Deze wiskunde is in de afgelopen jaren door Dustin Clausen en Peter Scholze ontwikkeld. Liquide wiskunde beoogt technieken uit de homologische algebra beschikbaar te maken in de functionaalanalyse. Ze baseert zich daarbij op een fundamentele stelling over de reële getallen, die met recht de hoofdstelling van de liquide wiskunde genoemd mag worden. Het bewijs van deze stelling is gecompliceerd en maakt gebruik van nieuwe technieken. Scholze schrijft hierover: "I spent much of 2019 obsessed with the proof of this theorem, almost getting crazy over it. In the end, we were able to get an argument pinned down on paper, but I think nobody else has dared to look at the details of this, and so I still have some small lingering doubts." [9]

Vanwege de fundamentele plaats van deze stelling in het werk van Clausen en Scholze en de mogelijke toepassingen die liquide wiskunde in de toekomst kan vinden binnen andere vakgebieden van de wiskunde, was er veel aan gelegen ook het laatste spoortje twijfel weg te nemen. In de woorden van Scholze: "I think this may be my most important theorem to date. (It does not really have any applications so far, but I'm sure this will change.) Better be sure it's correct…" [9] Computer-gecontroleerde bewijzen kunnen de zekerheid bieden die hier nodig is.

In dit artikel bespreek ik eerst wat computerbewijzen zijn. Vervolgens geef ik een zeer beknopte uitleg over liquide wiskunde. Dit hoofdstuk is vrij technisch, maar de details zijn niet essentieel voor de rest van het artikel. Ten slotte geef ik een overzicht van wat het Liquid Tensor Experiment heeft bereikt.

Liquid Tension Experiment

De naam van het project is een verwijzing naar de progressieve rockband *Liquid Tension Experiment*, waar Peter Scholze en ik beiden fan van zijn. Deze band bracht in 1998 en 1999 twee albums uit, waarna een radiostilte volgde van ruim twintig jaar.

Op 14 december 2020, minder dan tien dagen na het verschijnen van Scholze's eerste blogpost [9], kondigde de band op Twitter hun album *Liquid Tension Experiment 3* aan. Dit album verscheen in april 2021 en bevat onder andere een bonusnummer met de titel 'View from the Mountaintop'. Scholze schrijft in zijn tweede blogpost: "It feels like the main theorem is some high plateau with a wonderful view, but the way there leads through a large detour, to attack the mountain from the other side, where it is dark and slippery, and one has to climb up a certain steep wall; and no other pathways are seen left or right." [5] Nog enkele titels uit dit album die opvallend goed bij het Liquid Tensor Experiment passen, zijn: 'Beating the Odds', 'Liquid Evolution' en 'Solid Resolution Theory'.

Computerbewijzen

Het meeste wiskundige onderzoek wordt gedaan in de klassieke stijl: met een doos krijtjes bij het bord, of met pen en papier. Dit zijn beproefde hulpmiddelen om gedachten te ordenen, vast te leggen en te delen. In de laatste decennia zijn er echter ook speciale wiskundige computerprogramma's ontwikkeld. Naast de computeralgebra-pakketen die voor allerlei berekeningen geschikt zijn, zijn er ook programma's die in staat zijn om wiskundige definities, stellingen en bewijzen te lezen en te controleren. Daarvoor moet die wiskunde wel in een speciale wiskundige computertaal geschreven worden. De taal die we gekozen hebben voor het Liquid Tensor Experiment heet Lean.

Vogelvlucht door de geschiedenis

De Nederlandse wiskundige N.G. de Bruijn heeft na zijn fundamentele onderzoek in de analyse en getaltheorie een voortrekkersrol genomen in het onderzoek naar computerprogramma's die wiskundige bewijzen verifiëren. In Eindhoven ontwikkelde hij het programma *Automath* en in 1975 voltooide zijn student L.S. van Benthem Jutting de Automath-vertaling van Landau's *Foundations of Analysis*.

In de daaropvolgende decennia zijn vele andere systemen ontwikkeld, met hun eigen accenten en variaties. Sommige systemen (met name Mizar en Isabelle/ZF) zijn gebaseerd op verzamelingenleer, andere kiezen, geïnspireerd door de theorie van programmeertalen, voor type-theoretische fundamenten (Coq, Isabelle/HOL, Lean). Het

ene systeem kiest voor snelheid (Metamath), het andere legt de focus op leesbaarheid (Naproche). Voor een verdere vergelijking van al deze systemen verwijs ik graag naar het werk van Freek Wiedijk [11]. Naar mijn mening is de nieuwkomer Lean een zorgvuldig gebalanceerd systeem dat het best bruikbaar is voor wiskundigen.

In deze systemen zijn al meerdere noemenswaardige wiskundige resultaten geverifieerd: de priemgetalstelling, de vierkleurbaarheidsstelling, de Feit–Thompson-stelling (iedere eindige groep met oneven orde is oplosbaar), het bewijs van Hales van het Keplervermoeden, en de onafhankelijkheid van de continuümhypothese. Voor verdere informatie, zie [1, 2].

Lean

Lean is een functionele programmeertaal met speciale ondersteuning voor proposities en bewijzen. Het brein achter Lean is Leonardo de Moura, een onderzoeker van Microsoft Research [4]. Hij heeft Lean steeds verder ontwikkeld, en inmiddels met versie 4 een stabiele en bijzonder goed voor wiskunde bruikbare taal beschikbaar gesteld.

Om Lean (of een willekeurig andere wiskundige computertaal) te kunnen gebruiken, is ook een bibliotheek nodig van wiskundige stellingen en bewijzen, die vervolgens gebruikt kunnen worden als bouwsteen om complexere stellingen te formuleren en bewijzen te formaliseren. De wiskundige bibliotheek van Lean heet mathlib [10]. Rondom Lean en mathlib is een levendige gemeenschap van wiskundigen en informatici ontstaan [12]. In het jaar 2020 hebben ruim honderd mensen de inhoud van de mathlib-bibliotheek verdubbeld naar bijna 500 000 regels wiskundecode. De gemeenschap houdt ook een overzicht bij van de wiskunde die in een doorsnee bachelorcurriculum behandeld wordt en die in mathlib beschikbaar is [13].

Potentiële toepassingen van een digitale wiskundige bibliotheek

- Stellingen en bewijzen worden tot in de kleinste details gecontroleerd door de computer. Er kunnen daardoor geen foutjes in de bewijzen sluipen.
- Er kunnen specialistische zoekmachines gemaakt worden die onderzoekers helpen bij het vinden van resultaten. Voorbeelden hiervan zijn Sledgehammer voor Isabelle en `library_search` voor Lean.
- Computers kunnen zelf op zoek gaan naar bewijzen. Dit is een vakgebied dat volop in ontwikkeling is, en waar interessante resultaten worden geboekt. Voorlopig zal het nog wel even duren voordat wiskundigen hun baan kwijtraken aan computers, want de beste computerprogramma's kunnen nog niet tippen aan een eerstejaars wiskundestudent. Maar soms gaan ontwikkelingen sneller dan verwacht. Zo had niemand verwacht dat computers de wereldkampioen Go zouden verslaan toen dat in 2016 toch ineens gebeurde. Ook nu al kan de computer een heel nuttige bijdrage leveren door allerlei kleine tussenstapjes in te vullen en daarbij de wiskundige achter het toetsenbord wat werk uit handen te nemen.
- Wiskundige publicaties kunnen focussen op het uitleggen van intuïtie en de grote patronen, en kunnen voor de precieze details verwijzen naar deze computer-gecontroleerde bewijzen.

Oneindig veel priemgetallen in Lean

Bij wijze van voorbeeld geven we hier een Lean-bewijs van de aloude stelling van Euclides dat er oneindig veel priemgetallen zijn.

```
theorem (n : ℕ) : ∃ p > n, p.prime :=
begin
  let N := n! + 1,
  let p := nat.min_fac N, -- the minimal prime factor, if N ≠ 1
  have : n! > 0 := by library_search,
  have : N > 1 := by library_search,
  have : N ≠ 1 := by library_search,
  have : p.prime := by library_search,
  have : p > n,
  { by_contra' : p ≤ n,
    have : ¬p ∣ 1 := by library_search,
    have : p ∣ n! := by library_search,
    have : p ∣ N := by library_search,
    have : p ∣ 1 := by library_search,
    contradiction },
  finish,
end
```

Het bewijs is opgebroken in kleine stapjes. Lean is in staat om met behulp van een zoekactie door de bibliotheek te laten zien dat iedere tussenstap volgt uit de voorgaande claims.

Liquide wiskunde

Gecondenseerde wiskunde

Gecondenseerde wiskunde biedt een algebraïsch alternatief voor topologie. Vanuit een categorie-theoretisch oogpunt levert dit veel voordelen op. Zo is bijvoorbeeld de categorie van topologische abelse groepen geen abelse categorie: als $\mathbb{R}^\delta$ de verzameling van reële getallen met de discrete topologie aanduidt, dan is de identiteitsafbeelding $\mathbb{R}^\delta \to \mathbb{R}$ een continu homomorfisme met triviale kern en cokern, maar het is geen isomorfisme. Daarentegen is de categorie van gecondenseerde abelse groepen wel een abelse categorie met zeer goede eigenschappen. (Gecondenseerde verzamelingen/groepen/ringen worden 'geïmplementeerd' als schoven van verzamelingen/groepen/ringen voor de pro-étale Grothendiecktopologie op de categorie van pro-eindige verzamelingen. Voor dit artikel volstaat het om over gecondenseerde objecten na te denken als 'objecten met een topologisch sausje'.)

Abelse categorieën zijn van cruciaal belang in de homologische algebra, die op haar beurt een belangrijk gereedschap vormt in hedendaagse getaltheorie en algebraïsche meetkunde. Gecondenseerde wiskunde opent de gereedschapskist van de homologische algebra voor objecten die topologisch van aard zijn, zoals bijvoorbeeld topologische vectorruimtes over $\mathbb{R}$ of $\mathbb{C}$, maar ook over meer exotische lichamen zoals de p-adische getallen $\mathbb{Q}_p$. Voor een topologische ring R vormen gecondenseerde R-modulen in het algemeen een goed algebraïsch analogon van topologische R-modulen.

Om de volledige slagkracht van de homologische algebra te benutten, moet er echter ook een tensorproduct van gecondenseerde R-modulen zijn dat zich 'goed' gedraagt. Typisch is het wenselijk dat het tensorproduct van 'complete' objecten zelf ook 'compleet' is, en dit is voor het naïeve tensorproduct niet het geval. In de functionaalanalyse is het topologische tensorproduct een notoir lastig concept. Grothendieck heeft er zijn proefschrift [3] over geschreven, waarin hij nucleaire ruimtes introduceerde. Vergeleken met algemenere lokaal-convexe topologische vectorruimtes hebben nucleaire ruimtes als voordeel dat er een 'canoniek' tensorproduct van nucleaire ruimtes is.

Analytische ringen

Gecondenseerde wiskunde beantwoordt al deze subtiliteiten met het concept *analytische ring* [7, §7]. Een analytische ring $\mathcal{A}$ bestaat uit een onderliggende gecondenseerde ring $\underline{\mathcal{A}}$, samen met een axiomatische notie van 'vrije, complete' $\mathcal{A}$-modulen. Voor de resulterende notie van $\mathcal{A}$-modulen is er een goed 'gecompleteerd' tensorproduct. Men kan vervolgens aan iedere commutatieve ring R een 'discrete' analytische ringstructuur toekennen. Op natuurlijke wijze hebben p-adische ringen als $\mathbb{Z}_p$ en $\mathbb{Q}_p$ (en veel algemener *Huberringen*) een analytische ringstructuur die hun p-adische topologie weerspiegelt.

Analytische ringen stapelen een flinke dosis abstractie bovenop de toch al abstracte gecondenseerde wiskunde. Gelukkig is er een belangrijke stelling die grip geeft op de categorie van $\mathcal{A}$-modulen. Stelling 7.5 van [7] toont aan dat $\mathcal{A}$-modulen een volle deelcategorie vormen van de categorie van gecondenseerde $\underline{\mathcal{A}}$-modulen, die gesloten is onder alle limieten, colimieten en extensies. Vrij gezegd, betekent dit dat vrijwel iedere constructie van $\underline{\mathcal{A}}$-modulen die toegepast wordt op $\mathcal{A}$-modulen, zelf weer een $\mathcal{A}$-moduul oplevert.

De reële getallen

Voor discrete ringen en voor p-adische ringen bestaan er dus analytische ringstructuren. De hoofdstelling van liquide vectorruimtes [6, Stelling 6.5] toont aan dat ook de reële getallen een analytische ringstructuur toelaten die de gebruikelijke topologie op $\mathbb{R}$ weerspiegelt. Hierbij moet meteen worden opgemerkt dat deze liquide analytische ringstructuur afhangt van een reële parameter $0 < p \leq 1$, en dat er dus oneindig veel analytische ringstructuren op $\mathbb{R}$ bestaan. De modulen over deze analytische ringen noemen we p-liquide vectorruimtes. Iedere p-liquide vectorruimte is tevens p'-liquide, voor alle $0 < p' \leq p$.

Op een natuurlijke manier kunnen Banachruimtes en nucleaire Fréchetruimtes opgevat worden als p-liquide vectorruimtes, voor alle $0 < p \leq 1$. Vanwege bovengenoemde stelling 7.5 van [7] zijn dus ook alle producten, sommen, en algemener limieten, colimieten en extensies van dergelijke objecten opnieuw p-liquide vectorruimtes. Er zijn bijvoorbeeld extensies van Banachruimtes die zelf geen Banachruimte zijn, maar die dus wel p-liquide zijn.

Voor alle p is het p-liquide tensorproduct compatibel met het topologische tensorproduct van nucleaire vectorruimtes. Anderzijds is het p-liquide tensorproduct niet compatibel met de klassieke tensorproducten van Banachruimtes. Tevens is voor $p' < p$ het p'-liquide tensorproduct in het algemeen niet compatibel met het p-liquide tensorproduct.

Analytische meetkunde

In de algebraïsche meetkunde kent men aan iedere commutatieve ring A een affien schema toe, het spectrum $\mathrm{Spec}(A)$. Deze affiene schema's kunnen vervolgens aan elkaar gelijmd worden tot algemene schema's. Op analoge wijze kan men aan iedere commutatieve analytische ring $\mathcal{A}$ een analytisch spectrum $\mathrm{AnSpec}(A)$ toekennen. En deze analytische spectra kunnen vervolgens aan elkaar gelijmd worden tot *analytische ruimtes*.

Deze nieuwe meetkundige wereld generaliseert veel klassieke meetkundige concepten. Allereerst kan ieder schema opgevat worden als analytische ruimte, omdat elke ring een discrete analytische ringstructuur heeft. Daarnaast vormen ook objecten uit de p-adische meetkunde, zoals adische ruimtes (en in het bijzonder perfectoïde ruimtes) voorbeelden van analytische ruimtes. Ten slotte maakt de hoofdstelling van liquide vectorruimtes het mogelijk om ook meetkundige objecten over $\mathbb{R}$ en $\mathbb{C}$ als analytische ruimte op te vatten. Voorbeelden hiervan zijn differentieerbare variëteiten over $\mathbb{R}$, of holomorfe variëteiten over $\mathbb{C}$.

Clausen en Scholze laten zien dat deze nieuwe technieken leiden tot beknopte bewijzen van klassieke resultaten als coherente dualiteit voor schema's, Serredualiteit en eindigheid van coherente cohomologie voor compacte complexe variëteiten, en het vergelijkingsisomorfisme tussen algebraïsche en analytische De Rham-cohomologie. Voor al deze bewijzen geldt dat de complexiteit van het bewijs verpakt wordt in de machinerie van analytische ringen: het eigenlijke bewijs laat zich reduceren tot een eenvoudige berekening over $\mathbb{Z}$ of de eenheidsschijf in $\mathbb{C}$.

Dit ondersteunt de claim dat de hoofdstelling van liquide vectorruimtes een krachtige 'black box' is. Scholze schrijft: "With this theorem, the hope that the condensed formalism can be fruitfully applied to real functional analysis stands or falls. I think the theorem is of utmost foundational importance, so being 99.9% sure is not enough." [9]

Het experiment

De uitdaging van Scholze is om de volgende stelling met behulp van een computer te verifiëren.

Stelling (Clausen–Scholze). *Zijn* $0 < p' < p \leq 1$ *reële getallen, zij* S *een pro-eindige verzameling en zij* V *een* p*-Banach ruimte. Zij* $\mathcal{M}_{p'}(S)$ *de ruimte van* p'*-maten op* S*. Dan geldt*

$$\mathrm{Ext}^i_{\mathrm{Cond(Ab)}}(\mathcal{M}_{p'}(S), V) = 0$$

voor alle $i \geq 1$.

Het formalisatieproces van deze stelling hebben we in twee delen gesplitst. Het eerste deel betreft de zeer technische Stelling 9.4 van [6], en het tweede deel reduceert het einddoel tot deze Stelling 9.4.

Het eerste deel is tegen het einde van mei 2021 afgerond. Dit is ook het gedeelte van het bewijs waar Scholze nog lichte twijfels bij had. Het bewijs maakt gebruik van een variant op exacte complexen van genormeerde groepen, waarbij het belangrijk is om de norm van elementen goed te beheersen door allerlei geschikt gekozen constanten. Tijdens het formalisatieproces werden de gebruikelijke typefouten en onnauwkeurigheden gevonden, en af en toe moest een lemma een beetje worden aangepast. Scholze schrijft hierover in een tweede blogpost: "This was precisely the kind of oversight I was worried about when I asked for the formal verification. ... The proof walks a fine line, so if some argument needs constants that are quite a bit different from what I claimed, it might have collapsed." [5]

In grote lijnen is het bewijs van [6] gevolgd. Het team dat aan de formalisatie werkt, schrijft ook aan een 'informele' LaTeX-versie van het bewijs, met kruisverwijzingen naar de Lean-versie [14]. Deze *blueprint* is nog sterk aan verandering onderhevig, en zal in de komende maanden gepolijst worden.

De snelheid waarmee de eerste mijlpaal bereikt werd kwam voor velen als verrassing. Jordan Ellenberg schrijft: "I didn't grasp something like Lean would so quickly become authentically helpful at the frontiers of math." [16] Zelf had ik aanvankelijk ingeschat dat we ongeveer een jaar nodig zouden hebben voor de eerste mijlpaal.

Het tweede deel van het experiment is op moment van schrijven in volle gang. Onderdeel hiervan is het opzetten van de theorie van gecondenseerde abelse groepen. Het technische resultaat uit het eerste deel is een uitspraak over complexen van genormeerde groepen, waarbij gecondenseerde wiskunde geen directe rol speelt. Voor de vertaalslag naar de Ext-groepen van gecondenseerde abelse groepen die in bovengeciteerde stelling voorkomen, wordt in [6] gebruikgemaakt van een zogeheten Breen–Deligne-resolutie. Dit is een technisch resultaat in de homologische algebra, en het bewijs dat Breen–Deligne-resoluties bestaan maakt gebruik van homotopietheorie. In samenwerking met Scholze hebben we een gerelateerde techniek ontwikkeld die zowel eenvoudiger te bewijzen als ook eenvoudiger toe te passen is.

Het team

Begin 2021 is er rondom het project spontaan een team ontstaan dat bestaat uit wiskundigen en af en toe ondersteund wordt door informatici. De samenwerking wordt georganiseerd via de online Lean-chatroom [15]. De meeste teamleden hebben elkaar nog nooit in levende lijve ontmoet en kennen elkaar vanwege hun gemeenschappelijke interesse in Lean. Rondom de klok worden er bijdragen aan de code toegevoegd, vanuit Noord-Amerika, Europa en Australië. Peter Scholze heeft veelvuldig deelgenomen aan discussies in de chatroom om bewijzen toe te lichten of alternatieven te schetsen.

Op moment van schrijven bestaat het kernteam uit: Riccardo Brasca, Kevin Buzzard, Johan Commelin, Heather Macbeth, Patrick Massot, Bhavik Mehta, Scott Morrison, Filippo A. E. Nuccio, Damiano Testa en Adam Topaz. Verdere bijdragen en technische ondersteuning zijn geleverd door: Reid Barton, Alex J. Best, Mario Carneiro, Floris van Doorn, Gabriel Ebner, Rob Lewis, Yakov Pechersky, Ben Toner en Eric Wieser.

Bewijsassistent

Computerprogramma's als Lean worden soms ook wel *bewijsassistenten* genoemd. Over het algemeen is die assistentie voornamelijk toekomstmuziek, en voert pedante verificatie de boventoon. Tegelijk is er op specifieke punten wel degelijk assistentie mogelijk. Wanneer een theorie (in de zin van de logica) *beslisbaar* is, dan kan men een algoritme schrijven dat automatisch bewijzen of tegenvoorbeelden genereert voor uitspraken in die theorie. Bekende voorbeelden hiervan zijn de Euclidische meetkunde en de theorie van geordende abelse groepen.

Juist bij het Liquid Tensor Experiment is er ook op een andere manier sprake van assistentie. De kern van het bewijs is ingewikkeld. Zo ingewikkeld dat het erg moeilijk is het volledige bewijs in het 'werkgeheugen' van het brein te houden. (Het is goed mogelijk dat in de toekomst een eenvoudiger bewijs deze complicaties wegneemt.) Bij verschillende pogingen om het bewijs met pen en papier te doorgronden, liep ik vast op deze complexiteit. Iemand gaf mij de volgende vergelijking: Wanneer men een tekst wil begrijpen die geschreven is in een taal die men erg zwak beheerst, dan is het moeilijk om de tekst van begin tot einde door te lezen. Maar de eerste twee regels lukken vaak nog wel. En nadat die twee regels zorgvuldig vertaald worden naar de moedertaal, wordt de betekenis van de daaropvolgende regels ineens duidelijker.

Op dezelfde manier zijn we stap voor stap door het bewijs in [6] heen gekropen. Telkens hebben we een lemma, of een paar regels, vertaald naar Lean. Daarna werd vaak de volgende bewijsstap duidelijker, totdat uiteindelijk de volledige bewijsstructuur helder was. Scholze geeft aan dat dit proces ook voor hem verhelderend werkte: "During the formalization … this made me realize that actually the key thing happening is a reduction from a non-convex problem over the reals to a convex problem over the integers." [5]

Meer weten?

- Lean leren: https://leanprover-community.github.io/learn.html
- Zulip chatroom: https://leanprover.zulipchat.com
- LTE blueprint: https://leanprover-community.github.io/liquid

Referenties

1 Jeremy Avigad, The mechanization of mathematics, *Notices Amer. Math. Soc.* 65(6) (2018), 681–690.

2 Kevin Buzzard, Proving theorems with computers, *Notices Amer. Math. Soc.* 67(11) (2020), 1791–1799.

3 Alexandre Grothendieck, Produits tensoriels topologiques et espaces nucléaires, *Mem. Amer. Math. Soc.* 16 (1955), Chapter 1: 196 pp., Chapter 2: 140 pp.

4 Leonardo de Moura e.a., The Lean theorem prover (system description), in *International Conference on Automated Deduction*, Springer, 2015, pp. 378–388.

5 Peter Scholze, Half a year of the Liquid Tensor Experiment: Amazing developments, 2021, https://xenaproject.wordpress.com/2021/06/05/half-a-year-of-the-liquid-tensor-experiment-amazing-developments (bezocht op 05-10-2021).

6 Peter Scholze, Lectures on analytic geometry, 2019, www.math.uni-bonn.de/people/scholze/Analytic.pdf.

7 Peter Scholze, Lectures on condensed mathematics, 2019, www.math.uni-bonn.de/people/scholze/Condensed.pdf.

8 Peter Scholze, Liquid Tensor Experiment, *Experimental Mathematics* 0.0 (2021), 1–6.

9 Peter Scholze, Liquid Tensor Experiment, 2020, https://xenaproject.wordpress.com/2020/12/05/liquid-tensor-experiment (bezocht op 05-10-2021).

10 The mathlib community, The Lean mathematical library, in *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020, New Orleans, LA, January 20–21, 2020*, 2020, pp. 367–381.

11 https://www.cs.ru.nl/~freek.

12 https://leanprover-community.github.io.

13 https://leanprover-community.github.io/undergrad.html.

14 https://leanprover-community.github.io/liquid (work in progress).

15 https://leanprover.zulipchat.com.

16 https://twitter.com/JSEllenberg/status/1401177931800530948.

Clara Stegehuis
Faculteit EWI
Universiteit Twente
c.stegehuis@utwente.nl

Francesca Arici
Mathematisch Instituut
Universiteit Leiden
f.arici@math.leidenuniv.nl

Proof by example Portraits of women in Dutch mathematics

Palina Salanevich

In 'Proof by example', Clara Stegehuis and Francesca Arici portray women in Dutch mathematics. This edition portrays Palina Salanevich, assistant professor at Utrecht University. She investigates mathematical properties of signal processing problems that arise from optics, acoustics or speech recognition. In this interview she tells about her research and her motivation for mathematics.

How and when did you first get interested in mathematics?
"In school, I performed well in several subjects. But my mathematics teacher actually put in effort to give me some interesting extra mathematical problems, for example about logics. I liked this very much. From there I took the route which is quite standard in Belarus if you want to have access to extra math education: compete in math Olympiads. Once I made it to the national round, I was invited to a preparation retreat with all candidates. There I really felt like I fit well into this community. So I chose to study maths not only because I enjoyed it, but also because I really liked the people."

And how did you get into research from there?
"After my first year of university, I was invited to participate in a mathematical summer school. During this school, prominent mathematicians gave lectures on advanced math topics, and we also had opportunity to work together on research projects. I really enjoyed this much better compared to Olympiads: there was no time pressure, you can collaborate and you can apply much more creativity in these research problems. From there on, I always worked as a research assistant, until I finished my studies and continued in academia."


Palina Salanevich

So what is the research area you are working in now?
"In general, my research is in the area of signal processing and applied harmonic analysis. In many applications, *frames* are used to describe a signal. Frames are similar to the encodings of vectors in a basis of a vector space. But compared to a vector basis, frames allow for redundancy in the signal representation. This compensates for the loss of information caused by possible noise in the signal. In this way, frames form a stable, redundant way to encode signals.

One of the things my research focuses on is the *phase retrieval problem*, where we would like to reconstruct the original signal from measurements that are provided in the form of a frame. However, the measurements only provide the absolute values, or intensities, of the frame vectors, not the entire vectors. This problem actually arises in many applications. For example, in speech recognition, the frame vectors are usually so noisy that using them instead of their absolute

values can prevent correct signal reconstruction. So even though I am working in theoretical mathematics, the problems I am working on are very much inspired by real applications."

What are the main mathematical challenges in this problem?
"Mathematically, phase retrieval leads to optimization problems that are typically non-convex, and therefore difficult to solve and analyze. If you use non-convex optimization, you often get stuck in local optima, which you would like to avoid. In my research, I study the properties of the optimization problems arising from phase retrieval using probability theory and harmonic analysis. Can we prove that signal reconstruction is possible for a specific set of measurements? And if the measurements contain some noise, can we still reconstruct the original signal accurately?"

What is the most interesting problem you have been working on recently?
"Recently, I have been investigating signals on graphs. Typically, we assume that signals are measured over time with a certain step size. This gives an easy structure on which we can apply time shifts, Fourier transforms and more. However, in some applications, the underlying domain is more complicated. For example, you may have several correlated measurements at the same time. This creates an underlying graph structure. Take for example weather prediction: weather stations are placed in different locations, but the measurements at neighboring stations are dependent. Analyzing signals on such graphs is much more difficult, because the standard Fourier methods do not immediately work on graphs. The questions I have been working on are: 'Is there an uncertainty principle for signals on graphs? And how does this depend on the graph structure and its eigenvalues?' In general, an uncertainty principle tells that you can only predict the position and speed of a particle at the same time within a limited accuracy even with many measurements. Similarly, for signals the uncertainty principle gives a bound on how accurately you can localize a signal on the time domain and the frequency domain at the same time. But what would an uncertainty principle look like for measurements on graphs? Knowing this is for example important if you do not want to measure all data, but rather sample only some measurements to work with."

And is there a particular result you are you most proud of?
"Recently I have worked on *frame order statistics* — a property that illustrates how well frame vectors cover all directions in a particular space. Most research in my area assumes that all frame vectors are independently drawn from some convenient distribution. This assumption makes it easy to prove many properties using probability theory. In most applications however, this assumption is not realistic at all. In acoustics for example, signals are usually represented by perturbations of one single vector, so that the frame vectors are extremely dependent. In these situations, we really needed new mathematical techniques, as virtually all existing ones assume this independence. So I am very happy that I was able to show that frame-order statistics provide a key to still derive properties of the phase retrieval problem in more application-relevant settings."

What do you like most about doing research?
"I love the sense of discovery. These moments when you finish a proof, and everything falls together. They do not happen every day, but they are definitely worth it. But also, I really like the connectedness of the mathematical community. It is not competitive at all, and we all like to solve new mathematical problems with a community spirit."

And what do you like less about doing research?
"In my particular area, many problems look very simple on first sight: they can be formulated in simple terms. However, they actually lead to very complicated mathematical questions. So at conferences, you are often approached by others who are less familiar with the particular question. They then often offer me an 'easy solution' to my problem using a method they know of. Then I have to explain them why the method they have in mind has been tried before, but was not powerful enough. Of course, I do not mind explaining, but sometimes it can be a bit frustrating when other scientists seem to think that I am making my research much more complex than necessary."

Quinten A. Meertens
Centraal Bureau voor de Statistiek
Den Haag
qa.meertens@cbs.nl

Onderzoek

Vertekening door algoritmes die fouten maken

Wat als je algoritmes, die soms fouten maken, op een hele populatie loslaat en de uitkomsten optelt? Kun je daarmee betrouwbare statistische uitspraken doen over de populatie? Quinten Meertens deed vanuit de Universiteit van Amsterdam (econometrie) en de Universiteit Leiden (informatica) promotieonderzoek bij het CBS naar deze vragen en beschrijft hier de problemen en oplossingen die hij heeft ontdekt.

Binnen de officiële statistiek is men geïnteresseerd in aantallen en hoeveelheden. Actuele voorbeelden op wereldwijde schaal zijn het aantal coronabesmettingen, de hoeveelheid bos in de Amazone en de oppervlakte ijs op de poolkappen. Op nationale schaal kun je denken aan het aantal huizen met zonnepanelen, het aandeel cybercrime binnen alle misdrijven en het aantal innovatieve bedrijven in Nederland. De gemene deler van deze zes voorbeelden is dat ze tot stand komen door een geheel (een populatie mensen, huizen, bedrijven, et cetera) in groepen te verdelen en dan de omvang van de afzonderlijke groepen te bepalen.

Het toekennen van een object aan een groep noemen we ook wel classificeren. Dat classificeren gebeurt steeds vaker met behulp van algoritmes, daarom ook wel classificatiealgoritmes genoemd. Algoritmes zijn snel, maar niet foutloos. Fouten die algoritmes maken kunnen grote gevolgen hebben op het niveau van individuen. De toeslagenaffaire is daarvan een tragisch voorbeeld. Wij zijn echter benieuwd naar de gevolgen van dezelfde fouten op het niveau van groepen. Wat gebeurt er als je de uitkomsten van het algoritme dat is toegepast op een hele populatie bij elkaar optelt? Het blijkt dat er dan vrijwel altijd statistische vertekening optreedt, ook als het algoritme relatief weinig fouten maakt. Die vertekening wordt *misclassification bias* genoemd.

Een actueel voorbeeld

We introduceren het principe van misclassification bias eerst aan de hand van een actueel voorbeeld: het aantal coronabesmettingen in Nederland. Zoals bekend kun je je bij klachten laten testen op het coronavirus. Een PCR-test geeft dan aan of je al dan niet met het coronavirus bent besmet. Alle positieve PCR-tests in Nederland worden geteld en zo komen we tot het aantal coronabesmettingen in Nederland.

Het is echter bekend dat de PCR-test niet altijd juist is. Om allerlei redenen kan iemand die wel COVID-19 heeft toch een negatieve testuitslag ontvangen. We noemen dat een fout-negatieve testuitslag. Volgens het RIVM is de kans op dit type fout tussen de 2 en de 33 procent, zie [10]. Andersom kan een fout-positieve testuitslag ook voorkomen: de kans dat je zonder COVID-19 te hebben toch een positieve testuitslag ontvangt is tussen de $0{,}5$ en 4 procent, zie wederom [10].

Met deze foutkansen kunnen we een simpel rekenvoorbeeld uitwerken. Stel dat er in een week $100\,000$ mensen met corona-gerelateerde klachten zich laten testen en stel dat hiervan $10\,000$ mensen ook daadwerkelijk COVID-19 hebben. Wat is dan (naar verwachting) het aantal coronabesmettingen op basis van de uitslagen van de afgenomen PCR-tests die week?

Het antwoord hangt af van wat de precieze kans op fout-positieven en fout-negatieven is. Laten we voor dit voorbeeld eens kijken wat er in het meest extreme geval

gebeurt. Stel dat de kans op een fout-negatieve uitslag gelijk is aan de genoemde 2 procent en de kans op een fout-positieve uitslag gelijk is aan 4 procent. Dan zullen van de $10\,000$ met COVID-19 besmette mensen naar verwachting 9800 een positieve testuitslag ontvangen. Van de $90\,000$ mensen zonder COVID-19 zullen naar verwachting 3600 een positieve testuitslag ontvangen. Het totaal aantal besmettingen komt dan uit op $13\,400$, naar verwachting. Dat ligt 34 procent hoger dan de werkelijkheid. De misclassification bias is dan $+0{,}034$.

Merk op dat we met andere combinaties uit de twee genoemde intervallen van foutkansen ook heel andere uitkomsten kunnen aantreffen. Als we uitgaan van het andere extremum, 33 procent kans op fout-negatieven en $0{,}5$ procent kans op fout-positieven, dan vinden we 7150 positieve tests. De misclassification bias is nu $-0{,}0295$. Een mooie laatste combinatie is 9 procent kans op fout-negatieven en 1 procent kans op fout-positieven, wat ook binnen de genoemde intervallen past: dan komen we precies op $10\,000$ uit. De misclassification bias is dan 0.

Formele definitie

Voordat we oplossingen beschrijven om misclassification bias te verkleinen, introduceren we eerst de formele definitie van misclassification bias. Daartoe is de volgende notatie benodigd. We beschouwen een populatie I van omvang N. Voor nu beperken we ons tot binaire classificatie. Dat wil zeggen dat elk object $i \in I$ tot een van twee klassen behoort. We noteren de klasse van een object $i \in I$ met $s_i \in \{0,1\}$ (s staat voor stratum). We zijn geïnteresseerd in de zogenaamde *base rate* α, die gelijk is aan

$$\alpha = \frac{1}{N}\sum_{i=1}^{N} s_i.$$

In het voorbeeld over coronabesmettingen geldt dat $N = 100\,000$, dat $s_i = 1$ dan en slechts dan als persoon i besmet is met COVID-19 en dat $\alpha = 0{,}1$.

Zoals in het voorbeeld is de waarde van s_i niet bekend. We kunnen alleen een schatting of, in het geval van classificatiealgoritmen, een voorspelling maken van de waarde van s_i. Die schatting noteren we met $\hat{s}_i$. De geschatte base rate die we verkrijgen door de schattingen $\hat{s}_i$ te middelen noteren we met $\hat{\alpha}$. We beschouwen $\hat{s}_i$ als een stochastische variabele waarvan de verdeling afhangt van de werkelijke waarde s_i. De *(mis)classificatiekansen* p_{ab}, met $a,b \in \{0,1\}$, zijn gedefinieerd als

$$p_{ab} = \mathbb{P}(\hat{s}_i = b \mid s_i = a).$$

De kans op een fout-negatieve uitkomst wordt dus met p_{10} genoteerd. De kans op een fout-positieve uitkomst wordt met p_{01} genoteerd. De matrix $P = (p_{ab})$ noemen we de *misclassificatiematrix*. In deze matrix staat p_{11} linksboven, dus P is gelijk aan

$$P = \begin{pmatrix} p_{11} & p_{10} \\ p_{01} & p_{00} \end{pmatrix}.$$

Merk op dat waarden in elke rij van P optellen tot 1, waarmee de getransponeerde matrix P^T een stochastische matrix is.

Tot slot introduceren we nog de *base rate vector* $\boldsymbol{\alpha} = (\alpha, 1-\alpha)^T \in \mathbb{R}^2$. De vector $\hat{\boldsymbol{\alpha}} = (\hat{\alpha}, 1-\hat{\alpha})^T$ is de geschatte base rate vector. Nu geldt de gelijkheid

$$\mathbb{E}[\hat{\boldsymbol{\alpha}}] = P^T\boldsymbol{\alpha}.$$

Met dit resultaat en de bovenstaande notatie kunnen we misclassification bias formeel definiëren en uitdrukken.

Definitie. *Misclassification bias* is de vertekening van $\hat{\alpha}$ als schatter voor de base rate α en is gelijk aan

$$(p_{11} - 1)\,\alpha + (1 - p_{00})\,(1 - \alpha).$$

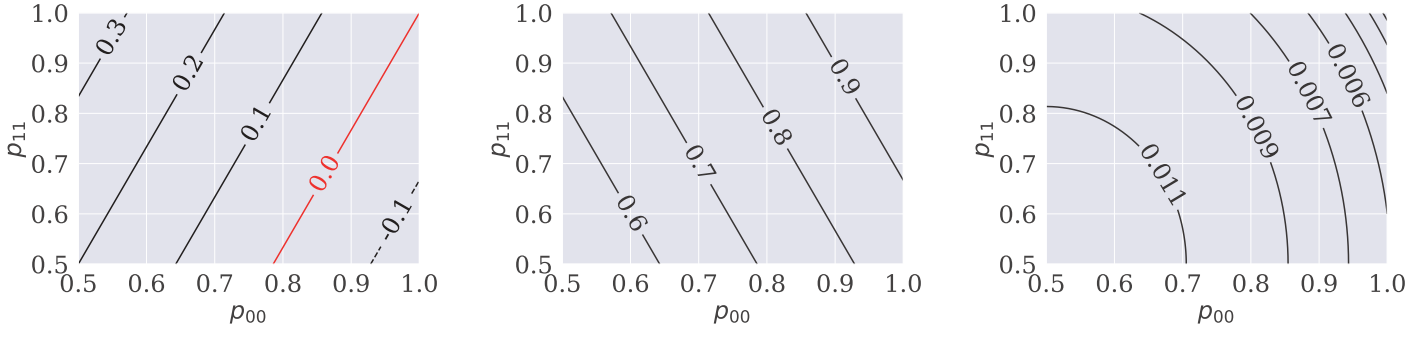
Het is nu eenvoudig in te zien dat de misclassification bias gelijk is aan 0 dan en slechts dan als (p_{00}, p_{11}) op de lijn tussen $(1-\alpha, \alpha)$ en $(1,1)$ ligt, zie de rode lijn in paneel (a) van Figuur 1.

Oplossingsrichtingen

Een classificatiealgoritme is, nadat de parameters zijn vastgesteld op basis van een zogenaamde 'training dataset', niets meer dan een deterministische functie van de kenmerkenruimte (feature space) naar, in ons geval, de verzameling $\{0,1\}$. We kunnen nu kiezen uit twee modellen om de fouten van dit algoritme te beschrijven.

In het eerste model beschouwen we de werkelijke klasse s_i als stochastisch, gegeven de uitkomst $\hat{s}_i$ van het algoritme. Dat wordt ook wel het *Berkson foutmodel* genoemd, geïntroduceerd in [1]. Dit is in de econometrie ook gebruikelijk: de onafhankelijke variabele wordt geschreven als een uitdrukking in de afhankelijke variabele plus een ruisterm. We zijn dan niet benieuwd naar de misclassificatiekansen p_{ab} van hierboven, maar naar de *calibratiekansen* c_{ab}, die gedefinieerd zijn als $c_{ab} = \mathbb{P}(s_i = b \mid \hat{s}_i = a)$. Samen vormen deze kansen de calibratiematrix $C = (c_{ab})$, met c_{11} linksboven.

In het tweede model beschouwen we de voorspelde klasse $\hat{s}_i$ gegeven de echte klasse s_i als stochastisch. Het idee daarachter komt uit de epidemiologie: de symptomen (als afhankelijke variabelen) worden bepaald door het al dan niet heb-



(a) Misclassification bias (b) Classification accuracy (c) Standaarddeviatie ($N = 2000$)

Figuur 1 Deze contourlijnen laten het verschil zien tussen (a) misclassification bias en (b) classification accuracy (dat wil zeggen: het percentage correct geclassificeerde objecten) voor base rate $\alpha = 0{,}3$ en variabele classificatiekansen p_{00} en p_{11}. Op de rode lijn in paneel (a) is de misclassification bias precies 0. De essentie van deze figuur is dat de richtingen van de contourlijnen in (a) en (b) tegengesteld zijn (en zelfs loodrecht op elkaar staan als $\alpha = 0{,}5$). Paneel (c) toont de standaarddeviatie van de schatter $\hat{\alpha}$ bij populatiegrootte $N = 2000$. Panelen (a) en (c) zijn overgenomen van [8].

ben van de ziekte (de binaire onafhankelijke variabelen), niet andersom. Dit tweede model wordt het *klassieke meetfoutmodel* genoemd, zie [2, p. 6].

Wij gaan uit van het laatste foutmodel, omdat het in de toepassingen waar we interesse in hebben het meest intuïtief is. In aanvulling op dat model nemen we aan dat de misclassificatiekansen voor elk object $i \in I$ gelijk zijn, gegeven de werkelijke klasse s_i van dat object. Bovendien nemen we aan dat de uitkomsten van het algoritme tussen de verschillende objecten stochastisch onafhankelijk van elkaar zijn.

Een gebruikelijke doelstelling binnen statistical learning is om classificatiealgoritmes te verbeteren. De kwaliteit van een algoritme wordt dan gemeten met bepaalde kwaliteitsmaten, zoals *precision*, *recall*, *accuracy* en vele andere. Minder fouten, oftewel het verhogen van p_{11} of p_{00} (of beide) zorgt ervoor dat elk van de gebruikelijke maten het algoritme beter beoordeelt. Het is dan ook tegenintuïtief dat dit niet automatisch betekent dat de misclassification bias kleiner wordt. Figuur 1 laat dit mooi zien. Stel bijvoorbeeld dat we met een classificatiealgoritme starten dat fouten maakt, maar α wel zuiver schat. Dat wil zeggen, we starten op de rode lijn in paneel (a). Als we nu het algoritme op zo'n manier verbeteren dat p_{00} gelijk blijft en p_{11} toeneemt, dan stijgt de accuracy (zie paneel (b)) en daalt de standaardafwijking (zie paneel (c)), maar *stijgt* de misclassification bias (zie daarvoor weer paneel (a)).

De uitdrukking voor misclassification bias zoals hierboven opgenomen kan gebruikt worden om aan te tonen dat een classificatiealgoritme de base rate α zuiver schat dan en slechts dan als precision en recall gelijk zijn. Het verwachte aantal fout-positieven is dan namelijk gelijk aan het verwachte aantal fout-negatieven. We zouden deze restrictie dus kunnen meenemen in het trainen van het algoritme, bijvoorbeeld door een maat te bedenken die naast het belonen van een hogere classification accuracy ook het verschil tussen precision en recall bestraft.

De oplossingsrichting die in mijn proefschrift *Misclassification Bias in Statistical Learning* wordt onderzocht is een heel andere, namelijk die uit de epidemiologie. Het idee is om het algoritme niet verder aan te passen, maar om na afloop voor vertekening te corrigeren. Simpel gezegd: we schatten α door $(P^T)^{-1}\hat{\alpha}$.

Dat lijkt een prachtige oplossing voor het probleem, maar er zit een addertje onder het gras. De misclassificatiematrix P is namelijk niet bekend en moet ook geschat worden. Helaas is de inverse van een geschatte matrix geen zuivere schatter van de inverse matrix. Bovendien kan de variantie zeer groot worden als de schatting van P op een klein aantal datapunten is gebaseerd. Om deze twee redenen bestuderen we alternatieve methoden uit de literatuur die na afloop voor vertekening corrigeren. We vergelijken de mean squared error (MSE) van de schatters die op deze correctiemethoden zijn gebaseerd en kunnen in verschillende situaties theoretisch bewijzen welke correctiemethode het beste is.

Correctiemethoden

De correctiemethoden zijn allemaal gebaseerd op schattingen van het aantal fouten dat het classificatiealgoritme maakt. We schatten dat aantal fouten met behulp van een zogenaamde testset, van grootte n. Van de objecten in deze (kleine) aselecte steekproef van de populatie achterhalen we de werkelijke klasse s_i, vaak door experts met domeinkennis in te zetten. We kunnen het classificatiealgoritme ook op deze testset loslaten om zo s_i en $\hat{s}_i$ te vergelijken. We komen zo tot tellingen n_{ab} ($a,b \in \{0,1\}$), het aantal objecten in de testset waarvoor geldt dat $s_i = a$ en $\hat{s}_i = b$. Zo komen we tot schattingen voor p_{ab}, namelijk $\hat{p}_{ab} = n_{ab}/(n_{a0} + n_{a1})$.

We bespreken hier twee correctiemethoden. De eerste methode is gebaseerd op het inverteren van de geschatte misclassificatiematrix. We noemen de verkregen schatter voor α de *misclassificatieschatter* en noteren deze schatter als $\hat{\alpha}_p$. Er geldt dat

$$\hat{\alpha}_p = \frac{\hat{\alpha} + \hat{p}_{00} - 1}{\hat{p}_{00} + \hat{p}_{11} - 1}.$$

De tweede methode is gebaseerd op het idee van de calibratiekansen c_{ab}, die we ook met behulp van de testset schatten, namelijk als $\hat{c}_{ab} = n_{ab}/(n_{0b} + n_{1b})$. We nemen het eerste element van de 2-vector $\hat{C}\hat{\alpha}$ als schatter voor α, oftewel

$$\hat{\alpha}_c = \hat{c}_{11}\alpha + \hat{c}_{10}(1-\alpha).$$

In [5] worden uitdrukkingen afgeleid voor de vertekening en variantie van de misclassificatieschatter en voor de calibratieschatter. Deze uitdrukkingen zijn benaderingen, nauwkeurig tot op orde $1/n^2$.

De winnaar

Het verschil tussen de MSE van de misclassificatieschatter en die van de calibratieschatter kan, tot op orde $1/n$ nauwkeurig, uitgedrukt worden als

$$\mathrm{MSE}[\hat{\alpha}_p] - \mathrm{MSE}[\hat{\alpha}_c] = \frac{T^2}{n(p_{00}+p_{11}-1)^2\beta(1-\beta)},$$

waarbij

$$T = (1-\alpha)p_{00}(1-p_{00}) + \alpha p_{11}(1-p_{11})$$

en

$$\beta = (1-\alpha)(1-p_{00}) + \alpha p_{11}.$$

Aangezien de bovenstaande uitdrukking altijd strikt positief is (want alleen gelijk aan 0 als $p_{00} = p_{11} = 1$, dat wil zeggen, als het algoritme nooit fouten maakt), komt de calibratieschatter $\hat{\alpha}_c$ altijd als winnaar uit de bus.

Een relevante uitzondering is wanneer een van de cruciale aannames wordt geschonden, namelijk de aanname dat de testset een aselecte steekproef is van de populatie. Vaak wordt een classificatiealgoritme namelijk eenmaal getraind en worden de foutkansen geschat op een aselecte steekproef als testset zoals eerder beschreven. Vervolgens wordt het algoritme voor een langere periode gebruikt zonder op een later tijdstip opnieuw de kwaliteit van het algoritme te bekijken. Wat hier essentieel is, is dat de base rate α over de tijd kan veranderen. Maar dan kan de eerder gebruikte testset niet meer als aselecte steekproef gezien worden van de populatie op dit latere tijdstip. En juist dit scenario is waarom het nauwkeurig schatten van α relevant is, denk wederom aan het voorbeeld over het aantal coronabesmettingen in Nederland. Het is interessant om dat aantal te schatten, juist omdat het over de tijd verandert.

Als we te maken hebben met een veranderende base rate α, zonder dat de foutkansen van het algoritme veranderen, dan spreken we van *prior probability shift*. Deze shift noteren we met δ. De uitdrukkingen van de MSE van $\hat{\alpha}_p$ en $\hat{\alpha}_c$ gaan dan afhangen van δ. In [7] laten we voor elk algoritme zien bij welke waarde van δ de eerdere conclusie verandert: voor δ voldoende groot zal de misclassificatieschatter een kleinere MSE hebben dan de calibratieschatter.

Een nog mooiere oplossing is om te allen tijde de twee correctiemethoden te combineren. Het idee is om op tijdstip $t = 0$

gebruik te maken van $\hat{\alpha}_c = \hat{\alpha}_c(0)$ en om op tijdstip $t > 0$ hier het verschil $\hat{\alpha}_p(t) - \hat{\alpha}_p(0)$ bij op te tellen. De eerste simulaties laten zien dat deze correctiemethode een kleinere MSE heeft dan zowel $\hat{\alpha}_c(t)$ als $\hat{\alpha}_p(t)$, voor alle $t > 0$ en elke waarde van δ, zie [4].

Toegepast op webwinkels

Binnen het CBS hebben we de misclassificatieschatter toegepast om een schatting te maken van de aankopen van Nederlandse consumenten bij buitenlandse webwinkels die binnen de EU zijn gevestigd, zie [6]. Dergelijke winkels zijn verplicht om in Nederland belasting af te dragen. Via de Belastingdienst zijn de aangiftes van dergelijke winkels beschikbaar binnen het CBS. (Het CBS hanteert strenge eisen omtrent privacy en statistische beveiliging opdat gepubliceerde cijfers nooit herleid kunnen worden tot individuele personen of bedrijven, zie ook [9].) Het probleem is dat veel andere buitenlandse bedrijven ook belastingaangifte doen en dat het onderscheid tussen webwinkels en andere bedrijven op basis van de beschikbare gegevens niet te maken is.

We hebben daarom een algoritme ontwikkeld dat automatisch de website van een bedrijf opzoekt met de naam van een bedrijf als uitgangspunt en vervolgens bepaalt of de gevonden website een webwinkel is. Voor een kleine aselecte steekproef hebben experts bepaald of een bedrijf al dan niet een webwinkel is. Dat is met name voor buitenlandse bedrijven met weinig omzet soms een behoorlijke klus. Met die informatie maken we een schatting van de misclassificatiekansen van het algoritme.

Vervolgens nemen we aan dat de misclassificatiekans onafhankelijk is van de hoogte van de omzet van een bedrijf. De schatting van de aankopen van Nederlandse consumenten bij buitenlandse webwinkels binnen de EU berekenen we dan door de geschatte 2-vector van omzetten op dezelfde manier te corrigeren voor misclassification bias als dat voor de geschatte base rate vector is gedaan.

Het resultaat van deze methodologie is, voor het jaar 2016, een uitkomst (met een geschatte standaardafwijking van 8 procent) die zes keer zo hoog is als eerdere schattingen op basis van consumentenenquêtes. De reden voor dit grote verschil is dat consumenten zich vaak niet realiseren dat ze iets bij een buitenlandse webwinkel bestellen, bijvoorbeeld omdat de website in het Nederlands is. Het grote effect van deze zogenaamde language bias kon nu met onze resultaten voor het eerst goed aangetoond worden.

Deze toepassing laat zien dat classificatiealgoritmes die niet perfect zijn toch goed binnen de officiële statistiek gebruikt kunnen worden, met uitstekende resultaten tot gevolg.

Vervolgonderzoek

Het gebruik van algoritmes om aantallen en hoeveelheden te schatten is een deelgebied van statistical learning dat *quantification learning* wordt genoemd. Er is weinig (maar toenemende) aandacht voor dit deelgebied dat verrassend veel toepassingen heeft in tal van uiteenlopende vakgebieden, van epidemiologie tot actuariaat en van remote sensing tot mariene biologie, zie [3]. En dus binnen de officiële statistiek. Binnen quantification learning worden drie typen correctiemethoden onderscheiden. Het eerste type, eerst tellen en dan corrigeren, hebben we hier besproken. Mijn proefschrift bevat het eerste theoretische bewijs over welke methode (binnen dit type) in welke situatie het beste is. Correctiemethoden van het tweede type maken gebruik van classificatiekansen, dat wil zeggen de continue uitkomsten van een algoritme die binnen het interval $[0,1]$ liggen. Methoden van het derde type slaan het classificeren helemaal over. Bij dit type wordt α direct geschat door de verdeling van de data binnen de kenmerkenruimte (feature space) tussen de training set en de rest van de populatie te vergelijken. Voor de methoden van het tweede en derde type zijn tot dusver al wat empirische resultaten bekend, maar nog geen theoretische resultaten. Daar zijn de komende jaren nog mooie stappen in te zetten.

Referenties

1 J. Berkson, Are there two regressions?, *Journal of the American Statistical Association,* 45(250) (1950), 164–180.

2 J.P. Buonaccorsi, *Measurement Error: Models, Methods, and Applications*, Chapman & Hall/CRC, 2010.

3 P. Gonzalez, A. Castaño, N.V. Chawla en J.J. del Coz, A review on quantification learning, *ACM Computing Surveys* 50(5) (2017), 74:1–74:40.

4 K. Kloos, A new generic method to improve machine learning applications in official statistics, *Statistical Journal of the IAOS* (2021), in pre-press, DOI: 10.3233/SJI-210885.

5 K. Kloos, Q.A. Meertens, S. Scholtus en J.D. Karch, Comparing correction methods to reduce misclassification bias, in L. Cao, W.A. Kosters en J. Lijffijt (eds.), *Proceedings of the 32nd Benelux Conference on Artificial Intelligence (BNAIC)*, Leiden, 2020, pp. 103–129.

6 Q.A. Meertens, C.G.H. Diks, H.J. van den Herik en F.W. Takes, A datadriven supply-side approach for estimating cross-border Internet purchases Within the European Union, *Journal of the Royal Statistical Society: Series A (Statistics in Society)* 183(1) (2020), 61–90.

7 Q.A. Meertens, C.G.H. Diks, H.J. van den Herik en F.W. Takes, Improving the output quality of official statistics based on machine learning algorithms, *Journal of Official Statistics* (2021), geaccepteerd voor publicatie.

8 S. Scholtus en A. van Delden, The accuracy of estimators based on a binary classier, Discussion Paper Nr. 202007, CBS, 2020.

9 https://www.cbs.nl/nl-nl/over-ons/organisatie/privacy.

10 https://www.rivm.nl/sites/default/files/2020-12/Toelichting%20betrouwbaarheid%20PCR.pdf.

Piet Groeneboom
Delft Institute of Applied Mathematics
TU Delft
p.groeneboom@tudelft.nl

Column Piet takes his chance

Chernoff's distribution and the bootstrap

Piet Groeneboom regularly writes a column on everyday statistical topics in this magazine.

Chernoff's distribution

In 1964 the remarkable paper [2] appeared, where Herman Chernoff derived the limit distribution of an estimator of the mode of a density. This distribution has become the 'normal distribution of non-standard asymptotics' in the sense that many estimators in the realm of (what is now called) non-standard asymptotics have this distribution as limit distribution. To the list of estimators with this limit distribution can recently be added the nonparametric maximum likelihood estimator of the distribution function of the incubation time of Covid-19, as discussed in [6].

The journal in which Herman Chernoff published his paper does not rank very highly in the list of journals in mathematical statistics, and I asked Herman Chernoff why he had sent his paper to this journal. He answered: "Well, they asked me to write a paper for them, and this is what I got." Which shows again that it is the author that counts, and not the prestige of the journal in which the author publishes (think of Grigori Perelman who published his results on arXiv).

Herman Chernoff

I looked for information on Chernoff's distribution in Wikipedia [11], but was shocked to see my own name three times in the references but no mention of Chernoff's paper [2]! And no, it wasn't me who wrote that entry! My only contributions to Wikipedia are about the Supreme Court during the German occupation, where my father played a role (see [12]) and about the statistical arguments in the Lucia de Berk court case (see [13]).

Now, to quote the Wikipedia article [11]: Chernoff's distribution, named after Herman Chernoff, is the probability distribution of the random variable

$$Z = \operatorname*{argmax}_{x \in \mathbb{R}} \{W(x) - x^2\}, \tag{1}$$

where W is a two-sided Wiener process (or two-sided Brownian motion), satisfying $W(0) = 0$. One of the pleasant properties of Brownian motion is that we can always use lots of symmetries; in this case one can immediately see that the random variable Z in (1) has the same distribution as the random variable.

$$U = \operatorname*{argmin}_{x \in \mathbb{R}} \{W(x) + x^2\}, \tag{2}$$

Moreover, further properties of Brownian motion imply that the location of the maximum (argmax) and the location of the minimum (argmin) are almost surely unique, and we therefore have (almost surely) well-defined random variables.

As mentioned in [6], for the model introduced there, the nonparametric maximum likelihood estimator $\hat{F}_n$ of the distribution function of the incubation time distribution function maximizes the log likelihood over all (cumulative) distribution functions F such that $F(x) = 0$ for $x < 0$:

$$\sum_{i=1}^{n} \log(F(S_i) - F(S_i - E_i)),$$

for a sample of size n, where S_i is the time of becoming symptomatic and E_i is the length of the exposure time of the ith person. It is proved in [7] that, if F_0 is the real distribution function of the incubation time and t is an interior point of the support of its density f_0, we have, under some conditions on the underlying distributions, denoting the convergence in distribution by $\xrightarrow{d}$, the following result for the maximum likelihood estimator (MLE) $\hat{F}_n$:

$$\lim_{n \to \infty} n^{1/3} \{\hat{F}_n(t) - F_0(t)\} \xrightarrow{d} cU, \tag{3}$$

where U is given by (2), for a constant $c > 0$, depending on the incubation time distribution and the distribution of the exposure times E_i. This means that, after rescaling, the limit distribution of

the maximum likelihood estimator is given by Chernoff's distribution (Theorem 4 in [7], where the dependence of the constant c on the underlying distributions is explicitly given).

A similar result was proved for a somewhat related model (the *interval censoring* model) 25 years ago in [3], and for the proof of (3) I had to go through similar steps again. The proof is quite complicated and I wish someone would come up with an easier one. The latest news on the analytical characterization of Chernoff's distribution is given in [8], where also references to earlier work can be found.

Bootstrap confidence intervals

In [6] an estimate of the (cumulative) distribution function of the incubation time of Covid-19 on the basis of data of 88 travelers from Wuhan was given by the MLE, but also by the smoothed maximum likelihood estimator (SMLE), given by:

$$\hat{F}_{nh}(t) = \int \mathbb{K}((t-y)/h)d\hat{F}_n(y), \tag{4}$$

where $h>0$ is the bandwidth, $\hat{F}_n$ the MLE of the distribution function, and $\mathbb{K}$ the integrated kernel

$$\mathbb{K}(x) = \int_{-\infty}^{x} K(u)\,du, \quad x\in\mathbb{R},$$

see (3) in [6]. Here K is a smooth symmetric kernel, symmetric around zero, with support $[-1,1]$, and h a bandwidth (which we choose here to be 4, on a scale of days).

So the SMLE is the convolution of the kernel $\mathbb{K}_h(\cdot) \stackrel{\text{def}}{=} \mathbb{K}(\cdot/h)$ with a discrete measure, given by the MLE $\hat{F}_n$.

Now, does the result (3) help us to derive the properties of (4)? One could say: a little bit. We do not really need to know that the limit distribution is Chernoff's distribution, because this 'fine behavior' of the MLE is washed away in the convolution with the kernel. On the other hand, once we know that this is the limit behaviour of the MLE, we know how to look for upper bounds we'll need in developing theory for the SMLE (4), in particular for constructing confidence intervals.

Today the standard method to achieve this is called the bootstrap. The bootstrap simulates the model we are using from the estimates themselves, in this case the MLE $\hat{F}_n$. The name 'bootstrap' comes from a version (American?) of the Baron von Münchhausen tales, where the baron pulls himself out of the swamp by his 'bootstrap' (in the copy I read as a child he pulls himself out of the mud by his hair).

However, one always has to prove that this will 'work', which means that one has to show that this procedure really reproduces the random behaviour one wants to simulate. In the present case it has for example been proved in [10] that the method *does not work* for the MLE in the analogous model of interval censoring if one tries to use the standard method for doing this, which is to resample with replacement from the data and to compute the estimates for these samples. In fact, the bootstrap has been proved to be *inconsistent* in this case. There is little doubt that the usual bootstrap will fail similarly for the MLE in the present model.

But one can in fact reproduce the convergence to Chernoff's distribution in (3) by using a different kind of bootstrap, as is suggested in [10]. In this version of the bootstrap one resamples from a smoothed version $\tilde{F}_n$ of the MLE, where $\tilde{F}_n$ has the property that $\forall u\in\mathbb{R}$:

$$\lim_{n\to\infty} n^{1/3}\{\tilde{F}_n(t+n^{-1/3}u) - \tilde{F}_n(t) - f_0(t)\,n^{-1/3}u\} = 0, \tag{5}$$

almost surely at points t in the interior of the support of the distribution, where f_0 is the density of the underlying incubation distribution (assumed to exist). In fact, the smoothed maximum likelihood estimator (SMLE) $\tilde{F}_{nh}$ has the desired property.

Although it is remarkable that we can indeed reproduce the 'Chernoffian behavior' by using this smooth bootstrap, one could (rightly) object to this method that if we assume that there exists an estimator having the property (5), we can do better and in fact use the SMLE $\tilde{F}_{n,h_n}$ as our estimator of the distribution function instead of the MLE. We then can prove:

$$n^{2/5}\{\tilde{F}_{n,h_n}(t) - F_0(t)\} \xrightarrow{d} N(\mu,\sigma^2),$$

if $h_n \sim kn^{-1/5}$, for $k>0$. That is, we have convergence to a normal distribution $N(\mu,\sigma^2)$, with mean μ and variance σ^2 specified in [7], at a faster rate than achieved by the nonparametric MLE in (3).

The construction of the 95% bootstrap confidence intervals in Figures 1 and 2 proceeded in the following way.

The (original) sample is $(E_1,S_1),\ldots,(E_n,S_n)$.
Sample $I_1^*,\ldots,I_n^*$ uniformly from $[0,E_1]$, …,$[0,E_n]$, respectively.
Sample $U_1^*,\ldots,U_n^*$ from the SMLE $\tilde{F}_{nh}$ of the incubation distribution function.
Let $S_i^* = I_i^* + U_i^*$. Then our bootstrap sample is:

$$(E_1,S_1^*),\ldots,(E_n,S_n^*).$$

Note that we keep the E_i fixed, relieving us from the duty of estimating its distribution.
Compute for each bootstrap sample either the MLE $\hat{F}_n^*$or the SMLE $\tilde{F}_{nh}^*$.

For Figure 1 all 1000 values $\hat{F}_n^*(t) - \int \mathbb{K}_h(t-y)\,d\hat{F}_n(y)$ were ordered and the percentiles $P_{0.025}(t)$ and $P_{0.975}(t)$ were determined. This gives the bootstrap intervals:

$$\big[\hat{F}_n(t) - P_{0.975}(t), \hat{F}_n(t) - P_{0.025}(t)\big].$$

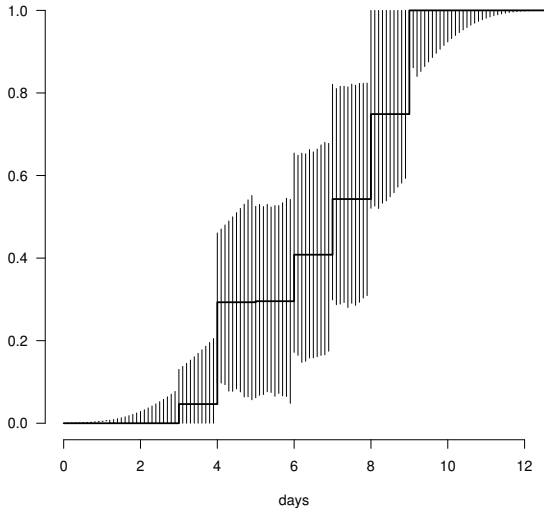


Figure 1 Estimate of the distribution function of the incubation time for the data in [1] by the MLE, with pointwise 95% bootstrap confidence intervals.

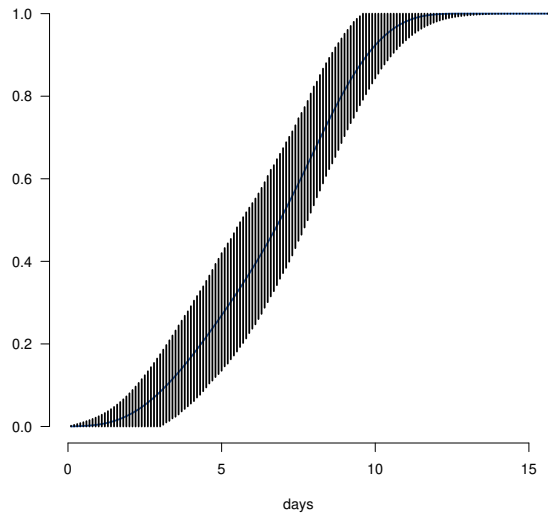


Figure 2 Estimate of the distribution function of the incubation time for the data in [1] by the SMLE, with pointwise 95% bootstrap confidence intervals.

For Figure 2 all 1000 values $\tilde{F}^*_{nh}(t) - \int \mathbb{K}_h(t-y)\,d\tilde{F}_{nh}(y)$ were ordered and the percentiles $\tilde{P}_{0.025}(t)$ and $\tilde{P}_{0.975}(t)$ were determined. Note that we do not subtract $\tilde{F}_{nh}(t)$ but instead subtract the convolution of the kernel $\mathbb{K}_h$ with $d\tilde{F}_{nh}$. This gives the bootstrap intervals:

$$[\tilde{F}_{nh}(t) - \tilde{P}_{0.975}(t), \tilde{F}_{nh}(t) - \tilde{P}_{0.025}(t)].$$

A similar procedure for the density estimates yields the confidence intervals in Figure 3.

A comparison

We now try to throw more light on the difference between the nonparametric approach and the approach using distributions like the Weibul, log-normal, et cetera. for the incubation time distribution. We investigated, in a follow-up of a study presented by the medical statistician Ronald Geskus at a session of the Joint Statistical Meeting (JSM) August this year, how these methods behave in the estimation of the 95th percentile of the distribution. To this end we generated 1000 samples of size $n = 500$, using a Weibull distribution to generate the incubation time distribution.

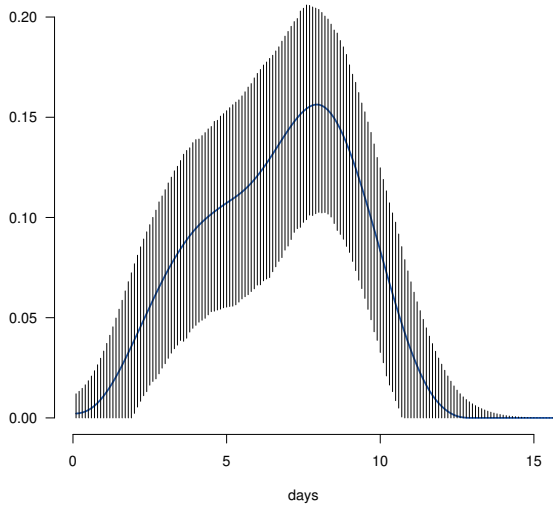


Figure 3 Estimate of the density of the incubation time for the data in [1], with pointwise 95% bootstrap confidence intervals.

This means that for each sample of size $n = 500$ we generated random variables $V_1, \ldots, V_n$, where each V_i had the Weibull distribution function

$$x \mapsto F_{\alpha,\beta}(x) \stackrel{\text{def}}{=} 1 - \exp\{-\beta x^{-\alpha}\}, \tag{6}$$

for $x \geq 0$ (zero otherwise), where $\alpha, \beta > 0$. In the simulations we took $\alpha = 3.03514$ and $\beta = 0.002619$ (these were values that came out of the study of travelers from Wuhan, discussed in [6]) for generating the samples. We also generated random variables $E_1, \ldots, E_n$ (exposure times), uniform on $[1,30]$, and for each i a variable $U_i \in [0, E_i]$ (infection time), uniform on $[0, E_i]$. This means that the sample on the basis of which the estimators of the incubation time distribution are computed consists of the pairs

$$(E_i, S_i) = (E_i, U_i + V_i), \quad i = 1, \ldots, n,$$

where S_i is the time of becoming symptomatic for the ith person, letting the exposure time have origin zero.

In the Weibull approach to the problem, we maximize for $\alpha, \beta > 0$:

$$\sum_{i=1}^{n} \log\{F_{\alpha,\beta}(S_i) - F_{\alpha,\beta}(S_i - E_i)\}, \tag{7}$$

where $F_{\alpha,\beta}$ is defined by (6). This gives a maximum likelihood estimate $F_{\hat{\alpha},\hat{\beta}}$ of the distribution function, where $(\hat{\alpha}, \hat{\beta})$ maximizes (7) over (α, β). The estimate of the 95th percentile is then defined by $F^{-1}_{\hat{\alpha},\hat{\beta}}(0.95)$, where $F^{-1}_{\hat{\alpha},\hat{\beta}}$ denotes the inverse function.

In the log-normal approach to the problem, we maximize for $\alpha \in \mathbb{R}$ and $\beta > 0$:

$$\sum_{i=1}^{n} \log\{G_{\alpha,\beta}(S_i) - G_{\alpha,\beta}(S_i - E_i)\}, \tag{8}$$

where $G_{\alpha,\beta}$ is defined by

$$G_{\alpha,\beta}(x) = \Phi((\log x - \alpha)/\beta), \tag{9}$$

for $x > 0$ (zero otherwise), where $\beta > 0$ and Φ is the standard normal distribution function. The estimate of the percentile is then given by $G^{-1}_{\hat{\alpha},\hat{\beta}}(0.95)$, where $(\hat{\alpha}, \hat{\beta})$ maximizes (8) over (α, β).

In the *nonparametric* maximum likelihood approach we simply maximize

$$\sum_{i=1}^{n} \log\{F(S_i) - F(S_i - E_i)\},$$

over *all* distribution functions F. This give the nonparametric MLE $\hat{F}_n$, from which we compute the SMLE $\tilde{F}_{nh}(t) = \int \mathbb{K}_h(t-y)\,d\hat{F}_n(y)$ and the estimate of the 95th percentile $\tilde{F}^{-1}_{nh}(0.95)$. The bandwidth h was chosen to be $h = 2$ here.

The results of this simulation for 1000 samples of size $n = 500$ are shown in the box plot Figure 4. The box plot is an invention of John Tukey, who started his mathematics career as a topologist: Tukey's lemma ("There is a maximal member of each non-void family of finite character") is one of the statements equivalent to the axiom of choice and the well-ordering principle listed in the famous book on topology [9] He is also known for his work on the Fast Fourier Transform (Cooley–Tukey FFT algorithm) and many other contributions to science. The box plot gives an image of the variability of the data, which in this case consist of the estimates of the 95th percentile of the incubation time distribution. The grey colored box ('interquartile box') is between the first and third quartile

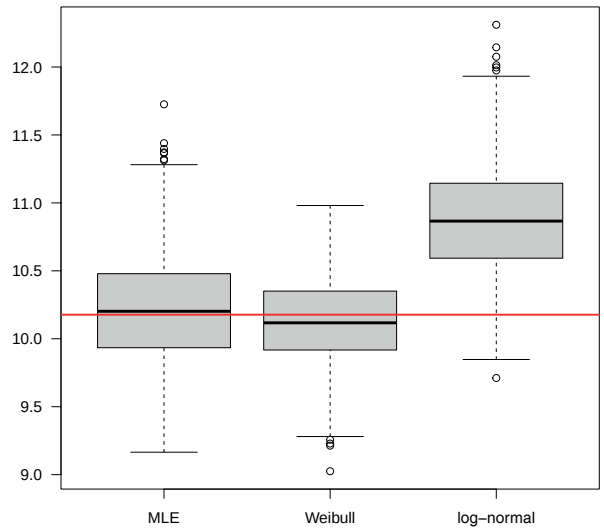


Figure 4 Box plot of 95th percentile estimates for the nonparametric, Weibull and log-normal maximum likelihood estimators for 1000 samples of size $n = 500$. The incubation time data are generated from a Weibull distribution.

of these 1000 estimates. The 'whiskers' are at a distance equal to 1.5 times the interquartile range from the boundaries of the interquartile box if there are outliers and otherwise at the smallest or largest observation. The outliers are further away than 1.5 times the interquartile range from the boundaries of the interquartile box. The black line segments in the boxes are at the position of the median. Finally, the red line denotes the value of $F^{-1}_{\alpha,\beta}(0.95) \approx 10.17716$ where $(\alpha, \beta) = (3.03514, 0.002619)$ (the values used to generate the Weibull incubation time distribution).

It can be seen that, since the incubation time data were generated from a Weibull distribution, the estimates of the quantiles assuming this distribution have indeed the smallest variation, but are slightly biased. But the nonparametric estimates, not making the assumption that the distribution is of the Weibull type, are also pretty good, whereas the estimates, assuming a log-normal distribution are completely off (in fact, these estimates are inconsistent, i.e., will not converge to the right value if the sample size tends to ∞), and indeed the model is 'misspecified' for these estimates. But the term 'misspecified' does not apply to the computations with the SMLE, since that estimate adapts to the underlying distribution and provides consistent estimates.

Some remarks of the statistician Richard Gill on this: One sees that the uncertainty about what interest us, is not much larger when one only uses the nonparametric SMLE than when one assumes that the incubation time distribution is Weibull (which is the correct distribution in this simulation setting), but much larger when one assumes log-normal. While there is absolutely no scientific (medical) reason to 'believe' Weibull, or to 'believe' log-normal. They lead to completely different statistical inferences, hence could lead to completely different policy recommendations. How to choose? We don't have to. We statisticians have figured out how to do it better, not making these assumptions.

Conclusion

In [6] the nonparametric maximum likelihood estimator $\hat{F}_n$ of the distribution function of the incubation time for Covid-19 was introduced, as an alternative to the parametric estimates used in this case, see, e.g., [1]. At that time it was still unknown what the local limit distribution of $\hat{F}_n$ (at a fixed point t) was. In the mean time it has been proved in [7] that, after rescaling, the limit distribution is Chernoff's distribution ((3) above), which was not exactly unexpected, but rather hard to prove.

It is argued above (and also in [5]) that one can probably better use smoothed nonparametric maximum estimates, of which Figures 2 and 3 give examples. Moreover, we can produce confidence intervals in a fully automatic way, using the smooth bootstrap, generating bootstrap samples from the SMLE. The ordinary bootstrap fails in producing valid confidence intervals via the MLE itself, as can be deduced from results in [10].

The methods discussed here provide an alternative for the parametric models which are usually applied in this context, estimating the incubation time distribution by, e.g., Weibull, gamma or log-normal distributions. The latter methods will not be able to catch finer aspects of the data, in contrast with, for example, the nonparametric density estimates. Moreover, they will only perform well if the underlying distribution is of the assumed type (Weibull, log-normal, et cetera) and otherwise will be inconsistent. On the other hand, the nonparametric methods will be consistent, irrespective of the underlying distribution.

All programs for generating the pictures in this column were written in C++ and are available as R scripts on [4].

References

1 Jantien A. Backer, Don Klinkenberg and Jacco Wallinga, Incubation period of 2019 novel coronavirus (2019-nCov) infections among travellers from Wuhan, China, 20–28 January 2020, *Euro Surveill.* 25 (2020).

2 H. Chernoff, Estimation of the mode, *Ann. Inst. Statist.* Math. 16 (1964), 31–41.

3 P. Groeneboom, Lectures on inverse problems, in *Lectures on Probability Theory and Statistics (Saint-Flour, 1994)*, Lecture Notes in Math., Vol. 1648, Springer, 1996, pp. 67–164.

4 Piet Groeneboom, Incubation time (2020), https://github.com/pietg/incubationtime.

5 Piet Groeneboom, Estimation of the incubation time distribution for COVID-19, *Statistica Neerlandica*, 2020.

6 Piet Groeneboom, Nederland in tijden van corona, *Nieuw Archief voor Wiskunde* 5/21 (2020), 181–184.

7 Piet Groeneboom, Nonparametric estimation of the incubation time distribution (2021), arXiv:2108.12606.

8 Piet Groeneboom, Steven Lalley and Nico Temme, Chernoff's distribution and differential equations of parabolic and Airy type, *J. Math. Anal. Appl.* 423(2) (2015), 1804–1824.

9 John L. Kelley, *General Topology*, D. Van Nostrand Company, 1955.

10 Bodhisattva Sen and Gongjun Xu, Model based bootstrap methods for interval censored data, *Comput. Statist. Data Anal.* 81 (2015), 121–129.

11 Wikipedia, Chernoff's distribution, https://en.wikipedia.org/wiki/Chernoff%27s_distribution, 2019.

12 Wikipedia, Supreme Court of The Netherlands in World War 2, https://en.wikipedia.org/wiki/Supreme_Court_of_the_Netherlands#Second_World_War, 2021.

13 Wikipedia, Lucia de Berk, https://en.wikipedia.org/wiki/Lucia_de_Berk, 2021.

Bert Zwaneveld
Science Department
Open Universiteit, Heerlen
zwane013@planet.nl

Dirk De Bock
Faculteit Economie en Bedrijfswetenschappen
KU Leuven
dirk.debock@kuleuven.be

History

Lucas Bunt's role in the development of statistics education

Lucas Bunt was a pioneer in the teaching of probability and statistics in Dutch secondary schools. As a teacher educator at Utrecht University, he and a group of teachers developed an experimental course which, from the mid-1950s on, became the reference textbook on this subject. Bunt's other — mostly international — activities are related to a curriculum reform movement initiated at the Royaumont Seminar in 1959, also known as the *New Math*. In the last years of his professional career, Bunt was a professor of mathematics at Arizona State University. In this article Bert Zwaneveld and Dirk De Bock describe the role of Lucas Bunt in the development of statistics education and highlight some developments in statistics education in the Netherlands 'after Bunt'.

The attention to statistics in Dutch secondary school mathematics arose in the early 1950s when a student text about statistics was developed by a group of mathematics teachers led by Lucas Bunt. The text was used in experiments in the last two years of secondary schools that prepared students for university studies in humanities. Bunt's reason to develop this text was a proposal made by *Liwenagel*, one of the two Dutch associations of teachers of mathematics at that time[1], to include statistics into the curriculum for these students. The proposal cannot be seen independently from a worldwide trend after World War II to include applications of mathematics into the secondary school curricula [10, 17]. During the 1950s the call for curriculum change was so strong that the OECD took the initiative to organize, in 1959, the Royaumont Seminar with representatives from different western countries to initiate the reform [8]. Bunt participated in 'Royaumont' and in many other international meetings related to this reform movement. Both in Royaumont as in subsequent meetings there was a great debate about the role of an axiomatic approach to secondary school mathematics.

Although Bunt's pioneering role in statistics education is well-known in the Netherlands, a proper scientific review of his work is still missing. Moreover, his acting at the international mathematics educational scene was not given appropriate attention so far, especially in the debates about a possible introduction of statistics at the secondary school level.

We present Bunt's role in the Dutch curriculum reform movement of the 1950s, more specifically, his activities related to the development of a statistics programme as a part of it. Based on written historical sources and a few oral testimonies of contemporaries, we first provide some elements of Bunt's professional career. We then report about his experiment with the teaching of statistics in secondary school classrooms and about the actions he took to ensure that his ideas became consolidated. Finally, we report what happened with statistics in Dutch secondary mathematics curricula 'after Bunt' and we present some conclusions.

Lucas Bunt

Lucas Nicolaas Hendrik Bunt (Figure 1) was born in 1905 in Edam, a small village north of Amsterdam. He studied mathematics at the University of Amsterdam where he also defended, in 1934, his PhD thesis, entitled *Bijdrage tot de theorie der convexe puntverzamelingen* ('Contribution to the theory of convex sets of points', see Figure 2).

Figure 1 Lucas Bunt (detail of a picture of the Wiskunde Werkgroep, 1948).


BIJDRAGE TOT DE THEORIE DER CONVEXE PUNTVERZAMELINGEN

PROEFSCHRIFT

LUCAS NICOLAAS HENDRIK BUNT

BIBLIOTHEEK
T.H. EINDHOVEN

MATHEMATISCH CENTRUM
Amsterdam

Figure 2 Title page of Bunt's PhD thesis (1934).

In the early 1930s, Bunt started his career as a mathematics teacher in Leeuwarden where he probably met his wife, a chemistry teacher at the same school. In the late 1940s Bunt became mathematics teacher trainer at the University of Groningen. From 1948 to 1969 he was appointed as a full-time mathematics teacher trainer at Utrecht University, a position that he combined with that in Groningen during several years. In 1968, immediately after the retirement of his wife, he and his family migrated to Arizona (US) where Bunt became a professor of mathematics at Arizona State University. We assume that Bunt had already developed strong professional ties with the US in the early 1960s to secure this appointment but could not verify this any further. Bunt died in 1984 in the US.

Figure 1 is a part of a larger picture made during a meeting of the *Wiskunde Werkgroep* ('Mathematics Working Group', see Figure 3), a group, chaired by Hans Freudenthal, that critically reflected on the existing secondary school curricula and developed proposals for new curricula [12]. Bunt was an active member of this group.

Besides Bunt's membership of the *Wiskunde Werkgroep* he also was active in the mathematics educational scene in the Netherlands after World War II. We shall later present some examples.

Bunt's international career already started in 1954. He then chaired section VII, Philosophy, History, and Education, during the International Congress of Mathematicians in Amsterdam. Bunt himself had two short contributions in this congress [11]. During the academic year 1956/57 Bunt and his family lived in Rio de Janeiro. On behalf of UNESCO, he was advisor to the Brazilian government about the reform of the secondary mathematics curriculum. Results of his stay in Brazil are a textbook on plane geometry and a Portuguese/Brazilian translation of his Dutch textbook on probability and statistics, which we further discuss in this chapter. In 1959, recommended by Hans Freudenthal to the Dutch Ministry of Education, Bunt was one of the three representatives for the Netherlands at the famous Royaumont Seminar and he co-edited the Seminar's Proceedings in cooperation with Howard F. Fehr [15]. In the late 1960s, Bunt translated and adapted, in cooperation with Harrie Broekman, a series of booklets that were developed by the *School Mathematics Study Group* in the US. This resulted in a six-volume programmed instruction course for Dutch secondary school students.

End 1950s, begin 1960s, Bunt was a member of the *Onderwijsraad* ('Educational Council'). The official task of this Council was, and still is, to advice the minister of education about politics and legislation related to education.

Bunt was primarily a mathematician who explained mathematics to a non-mathematically schooled audience. We report in more detail Bunt's activities in the Netherlands with statistics education. An important part of these activities was the co-authoring of the textbook *Statistiek voor het voorbereidend hoger en middelbaar onderwijs* ('Statistics for preparatory higher and secondary education') [2], intended for Dutch students, aged 16 to 18 years, who prepared themselves for university studies in social sciences, economics, geography, et cetera. Bunt conducted a teaching experiment with this textbook and he published a report of this experiment [3]. Without going into details we also mention that Bunt conducted a comparable experiment with the history of mathematics for the same target group of students. For this experiment he co-authored *Van Ahmes tot Euclides, hoofdstukken uit de geschiedenis van de wiskunde* ('From Ahmes to Euclid, chapters from the history of mathematics') [1]. In 1976 Bunt translated and revised *Van Ahmes tot Euclides* together with two American co-authors into *The Historical Roots of Elementary Mathematics* [6]. During the sixties, Bunt (co-)authored *An Introduction to Sets, Probability and Hypothesis Testing* (with Howard F. Fehr and George Grossman) (1964) and *Probability and Hypothesis Testing* (1968).

Figure 3 Participants of the conference of the Wiskunde Werkgroep on 13 and 14 November 1948; on the first row, left: Lucas Bunt, fifth from left: Hans Freudenthal (collection Fred Gofree).

First experiments with statistics education

Bunt took the initiative to develop an experimental text about statistics in some gymnasia A.[2] The text was initially mimeographed, in 1956 it was printed as a textbook [2]. As mentioned before, one of the reasons for Bunt to start with an experiment about the teaching of statistics was a proposal of a commission established by the organization of mathematics teachers *Liwenagel*, intended to study the opportunities and possibilities of "a re-organization of mathematics education in the A-streams of the gymnasia and the gymnasium sections of the lyceums[3]" [13, p. 49]. Bunt

was a member of that commission and, although it is not mentioned, likely the main author of the commission's report.

It is worth mentioning that Bunt did not develop the experimental text and the textbook on his own, although this was a common practice in the Netherlands at that time, but in cooperation with a team of teachers. In the Preface of the textbook Bunt wrote (translated from Dutch[4]):

> "...was an educational experiment in statistics, organized by the Department of Didactics of the Pedagogical Institute of the State University of Utrecht. The following teachers cooperated: Dr. Cath. Faber-Gouwentak, Barlaeus-Gymnasium, Amsterdam; Sr. E.A. de Jong, Rectrix [Headmistress] St. Theresia-Lyceum, Tilburg; D. Leujes, Grotius-Gymnasium, Delft; Dr. H. Mooy, Barlaeus-Gymnasium, Amsterdam; Dr. P.G.J. Vredenduin, Conrector [Vice Headmaster] Stedelijk [Municipal] Gymnasium, Arnhem." [2, p.v]

At that time in the Netherlands, statistics was not a part of the official curriculum that only included algebra and geometry, topics that were also part of the final exams, organized centrally by the government. However, based on an exceptional rule, the Inspection of Education could allow teachers to change parts of the exam programme. Such an exception was obtained for the statistics experiment.[5]

In 1957, Bunt published the report in which he describes and discusses the experiment with the student text that was used during the years 1951–1955 [3]. The reason why the textbook was published before this report was, as Bunt wrote in the textbook's Preface:

> "The recent proposals of the mathematics teachers associations *Wimecos* and *Liwenagel*[6] about the curriculum change for mathematics in the B-stream of the secondary schools, in which statistics is included as a new topic, made it desirable to make, as soon as possible, the text public." [2, p.v]

Bunt's report had two parts: part A includes the motivation and explanation about the selected topics, and the way they are treated; part B is the student text (it is not included in the printed version of the report).

We focus on some highlights of part A. Bunt motivated the reasons for choosing statistics as follows: to students in university disciplines such as economy, psychology and sociology, an extensive study of algebra is less useful than a well-balanced treatment of the first concepts and principles of statistics. Statistics in university turns out to be very difficult and uncommon to these students. Moreover, they have to learn it in a rather short period of time. Statistics in secondary school is not only useful for the aforementioned students, but for all citizens in modern society. By reducing the algebra content, Bunt found the necessary 35 classroom hours for his statistics course. After that, he justified the chosen topics. In the first experimental text, these topics were: frequency distribution, histogram, frequency curve, cumulative frequency, average, median, quartiles, range, mean deviation, standard deviation, quartile distance, permutations, variations (without repetitions), combinations, Pascal's triangle, Newton's binomial formula, some simple theorems from probability calculus, the binomial distribution for $p = 0.5$, the normal curve as a limit of the histogram of the binomial distribution (graphical, not with formulae). At the end of the course, some applications of the normal curve for calculating probabilities were presented. Linear regression and correlation were left out, because of being too time-consuming. Especially on the insistence of his cooperators, Bunt drastically changed the end by including a final chapter on hypothesis testing: estimating some characteristics of a population on the basis of a sample.

Figure 4 Bunt attending the public defense of the PhD thesis of his son Harry at the University of Amsterdam, 1981.

Bunt's approach to probability theory

Bunt deals extensively with the principles of probability calculus for which he presents an axiomatic approach. Probability is a function that assigns to an event a number in the interval $[0,1]$. He starts from the following two axioms: (1) If $p \rightarrow \neg q$, then $P(p \text{ or } q) = P(p) + P(q)$; (2) If p is the sure event, then $P(p) = 1$. From these axioms Bunt derives the complement and product rule. He illustrates these rules with examples about rolling dice. In the textbook, however, Bunt introduces the concept of probability differently. There he starts with the definition of Laplace: the probability of an event is the number of outcomes favorable for that event, divided by the total number of outcomes (under the condition of mutually exclusive and equally likely outcomes). After having dealt with the complement, the sum and the product rule, he introduces 'another' definition: if it turns out that in a large number of repetitions of an experiment, n, an event happens k times, then we are convinced that every time we repeat this experiment a sufficient number of times, this event will happen in $\frac{k}{n}$ part of this number. We then state that the probability of that event equals $\frac{k}{n}$. For probabilities derived from that 'new' definition, the complement, sum and product rule keep their validity.

A contrasting, radical axiomatic approach

We note that Bunt's approach contrasts sharply with that of his contemporary Gustave Choquet, then president of the *International Commission for the Study and Improvement of Mathematics Teaching* (CIEAEM), who proposed at its 9th meeting, specifically on the teaching of probability and statistics, a definition of probability based on the mathematical concept of measure (translated from French); Figure 5 illustrated Choquet's contribution:

> "In a set U, one chooses a family F of subsets E, to each of which we attach a number $m(E)$, called the measure of E. These subsets have the following properties: their union and their intersection are again part of F, even if the number of E's is infinite. In the case of probabilities, the set U has measure $m(U) = 1$. Each element of U represents a possible event: all favourable events constitute a subset E with measure $m(E)$. The probability of the favourable event is given by $m(E)/m(U)$." [7, pp.63–64]

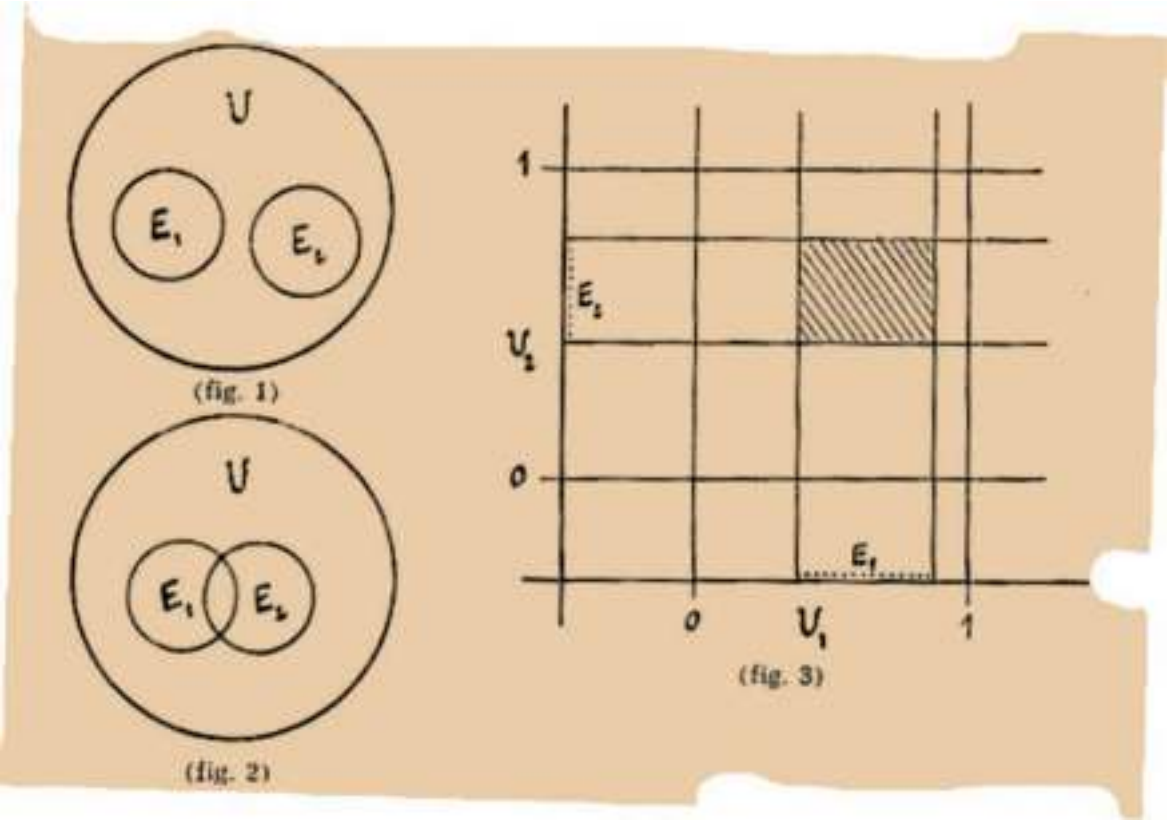


Figure 5 Illustration of Choquet's approach of probability.

The difference between Bunt's and Choquet's approaches illustrates the debate during the mid-1950s between the mathematics-didacticians and the mathematics-structuralists on how statistics should be introduced at the secondary school level. More generally, it illustrates the great debate about the role of an axiomatic approach to secondary school mathematics, as already shortly mentioned in the Introduction.

Bunt's approach to hypothesis testing

Because of its innovative character, we discuss in some detail how Bunt explained the concept and procedure of hypothesis testing. He wrote about this:

"On the basis of a sample of 10 marbles out of a box with 5000 white and 5000 red marbles the probabilities of $0, 1, 2, \ldots, 8, 9, 10$ red marbles in that sample are 0.001, 0.010, 0.044, 0.117, 0.205, 0.246, 0.205, 0.117, 0.044, 0.010, 0.001. It follows that in 1.1% of all samples of 10 marbles there are 0 or 1 red marbles, and even so, in 5.5%, there are 0, 1 or 2 red marbles. And, in 5.5% of all samples there are 8, 9 or 10 red marbles. And moreover, in 1.1% of all samples there are 9 or 10 red marbles. Now suppose that the fraction p of red marbles is unknown, and we take a sample of 10 marbles. We shall agree that if $p = 0.5$ and there are 0, 1, 9 or 10 red marbles in the sample, we shall reject the hypothesis $p = 0.5$. If the hypothesis $p = 0.5$ is right we have a risk of $1.1\% + 1.1\% = 2.2\%$ that we, in spite of this, reject the hypothesis. More precisely, there is a probability of 1.1% that we reject the hypothesis $p = 0.5$ on the strength of too small (or too large) a number of red marbles. Because, in this connection, we, for the time being, do not want to risk a greater probability than 2.5%, we stick to the mentioned agreement. This agreement, therefore, conforms to the following conditions: (a) if $p = 0.5$, we risk, both for too small and for too large a number of red marbles in the sample, a probability of not more than 2.5% that we reject the hypothesis $p = 0.5$; (b) both for too small and for too large a number of red marbles this probability lies as close to 2.5% as possible. When we reject the hypothesis $p = 0.5$, we say the hypothesis $p = 0.5$ is rejected with an unreliability of not more than 5%." [2, p. 12]

The fraction v is introduced as the number of red marbles divided by the number of marbles in the sample and its values which are or are not thought contradictory to $p = 0.5$ are represented by, respectively, dots and circles on an axis (Figure 6). Repeating this procedure for different values of p, one gets the two-dimensional scheme (Figure 7). By making the values of v and p 'continuous', one gets a graph on which the different boundary lines refer to different sample sizes (Figure 8). The textbook contains two of these, corresponding to unreliabilities of 5% and 10%, called by Bunt 'nomograms'. From these nomograms, the student can observe that the

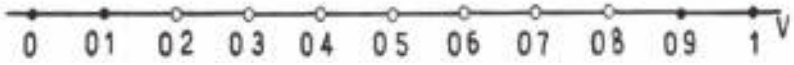


Figure 6 Axis representing values of v with dots, contradictory to $p = 0.5$, and circles, not contradictory

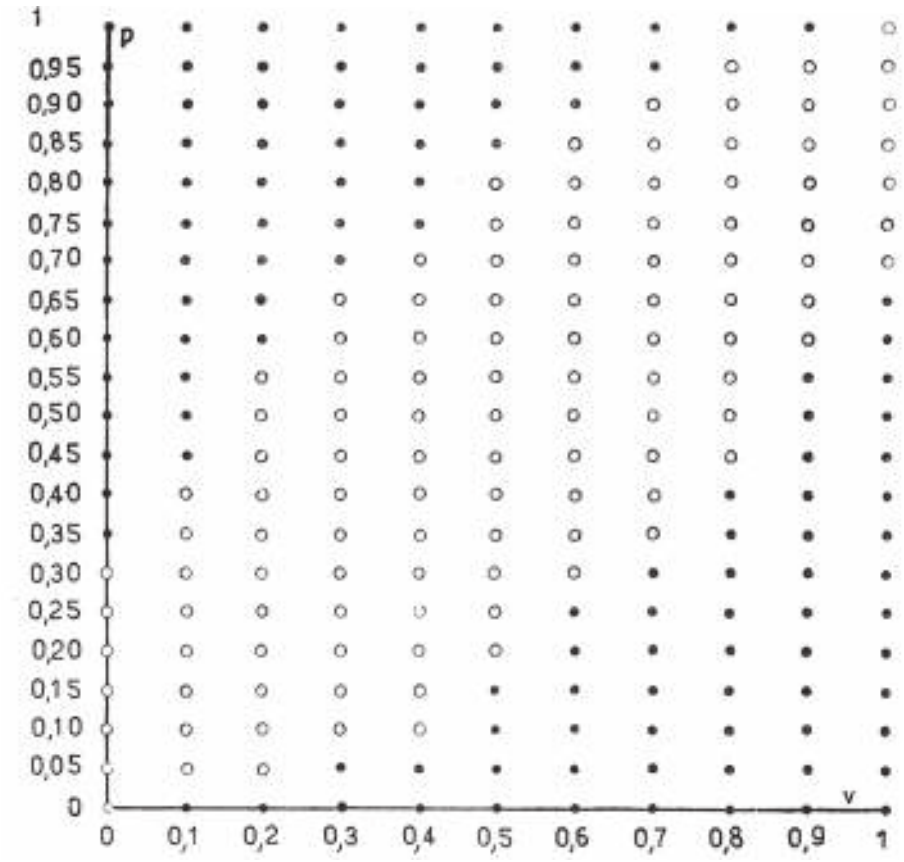


Figure 7 v-axes for different values of p.

probability of rejecting a false hypothesis increases with the sample size.

Consolidation and internationalization

In 1954–1955 a curricular commission of *Wimecos* published a report including a draft curriculum and central examination program for mathematics in HBS-B. Bunt had been a member of that commission representing the Dutch mathematics didacticians and mathematics teacher trainers. In the commission's report, it is stated that statistics had been important sources for the commission. The commission basically confirmed the conclusions of the report of *Liwenagel* [13], but now generalized to all students who prepared themselves for university studies. In 1958, the new curriculum was actually implemented, but, although it entailed a considerable change, statistics only became an optional subject for gymnasium A.

The fifth edition of Bunt's textbook [5] had a slightly different title, a consequence of the curriculum reform consolidated in 1968 by a new law for secondary education. The subtitle, 'Statistics for preparatory higher and secondary education', was changed into 'Statistics for preparatory scientific education'. This new curriculum reform was prepared and supervised by the *Commissie Modernisering Leerplan Wiskunde* (CMLW, 'Commission for Modernization of the Mathematics Curriculum'). The task of that commission was to prepare the mathematics curriculum reform in line with the ideas of Royaumont Seminar. Bunt was a member of the CMLW [16]. The commission was officially set up in June 1961 by the Ministry of Education, Arts and Science, but already in January 1961, Bunt had proposed to the Ministry to establish such commission. However, the Inspection of Education had given negative advice to the Ministry because the commission as proposed by Bunt was too small. In 1968 the new curriculum for mathematics, in which statistics played a clear role, was implemented in all schools for secondary education in the Netherlands: Bunt had

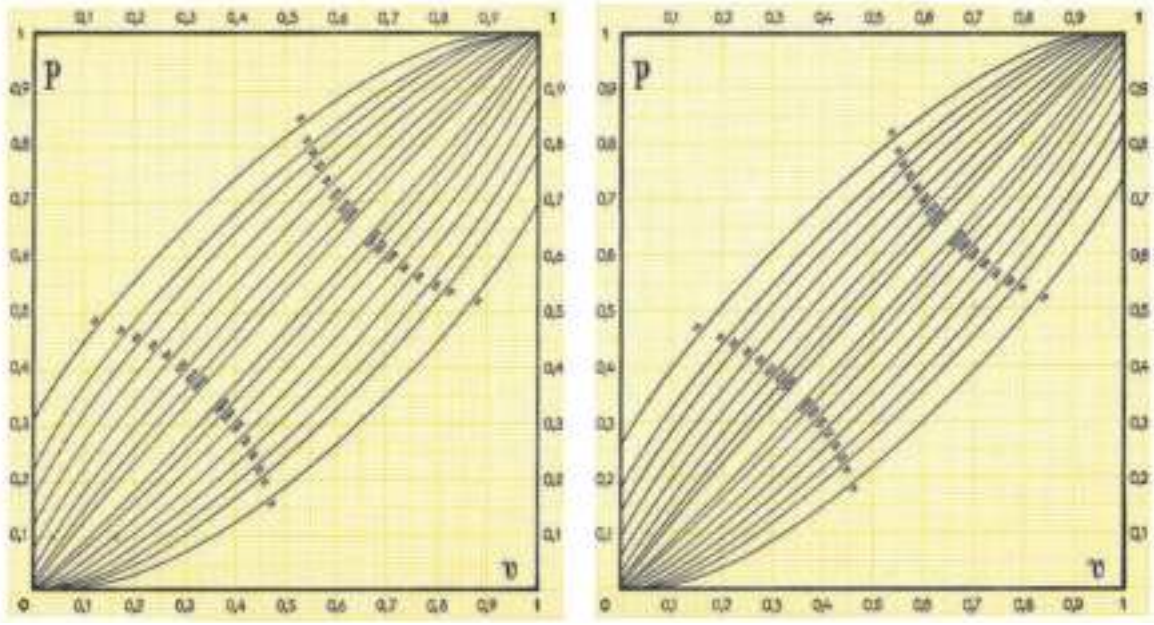


Figure 8 Nomograms for different sample sizes (left, the unreliability is 5%, right 10%).

achieved what he had started working on in 1951.

During the late 1950s and early 1960s, Bunt disseminated his ideas about the teaching of statistics. Already on 24 May 1959 he was invited to report on his experiment about the teaching of statistics at the annual meeting of the *Société Belge de Professeurs de Mathématiques* ('Belgian Association of Mathematics Teachers') and the *Société Belge de Statistique* ('Belgian Association of Statistics'), held in Brussels on 24 May 1959 [4]. The manner in which statistics became a part of the secondary-school curriculum in the Netherlands was also the topic of Bunt's paper at the Royaumont Seminar [15]. In the period after Royaumont, Bunt had the opportunity to participate actively in almost all meetings held in order to coordinate, monitor and refine the implementation of the Royaumont recommendations (Aarhus, 1960; Athens, 1963; Echternach, 1965).

Recent developments in the Netherlands

In 1968 the structure of secondary education in the Netherlands completely changed, and at the same time, also the mathematics curricula. According to the law for secondary education of 1968, two types of schools could prepare students to higher education: *Voorbereidend Wetenschappelijk Onderwijs* (VWO, six grades for students from age 12 to 18, 'Preparatory Scientific Education'), preparing for university studies, and *Hoger Algemeen Voortgezet Onderwijs* (HAVO, five grades for students from age 12 to 17, 'Higher General Continued Education'), preparing for education at *Hogescholen* ('Institutes for Higher Education'), nowadays called universities for applied sciences. The mathematics curricula for both school types were prepared by the CMLW. Begin 1970s the CMLW stopped activity, but there was a kind of successor: the *Instituut voor de Ontwikkeling van het Wiskunde Onderwijs* (IOWO, 'Institute for the Development of Mathematics Education') with Freudenthal as director, nowadays the Freudenthal Institute. This Institute had the supervision of the implementation of the new mathematics curricula. But maybe more important is that Realistic Mathematics Education (RME) was development there. Important characteristics of RME are: start mathematics education with concrete situations which are recognizable to the students, design the learning process of the students by guided re-invention of the mathematical concepts and methods, and emphasize that mathematics is human activity.

The curriculum of VWO included probability theory and statistics, that of HAVO only included descriptive statistics. These topics were intended to be taught in the last two years of these school types. We restrict ourselves to statistics education at VWO. Although Bunt's textbook was available, CMLW judged that it was better to not implement statistics immediately, but first to develop a new text and conduct an experiment with a restricted number of schools. The argument was that Bunt's textbook was only intended for students in the 'old' gymnasia A, whereas statistics now had become a compulsory subject for all students. A statistics developmental team started in 1970, first under the supervision of the CMLW, from 1971 under the supervision of the then started IOWO, the predecessor of the Freudenthal Institute.

After a first draft the team developed a textbook [14] including the following content: Introduction, Probability rules, Probability distributions, Hypothesis testing and reliability intervals, Parameters of a distribution, Use of the normal distribution. The Introduction included an example with a prognosis of the number of students of VWO that should follow science or mathematics at the university, based on data of the Dutch *Central Bureau of Statistics*. From that example, terms as sample, population, random, representative, testing — for instance with respect to the quality of the production of certain items — were introduced. In this textbook the students themselves started with a probability experiment. There was a box with 1000 small marbles, 600 red and 400 black. With a kind of spoon with 20 wholes, they drew a random sample of 20 marbles. This box with the 'spoon' was used to simulate various probability experiments.

Concluding remarks

The mathematician Lucas Bunt played a crucial role in promoting and developing materials for statistics education at the secondary level, in the Netherlands but also at the international level. Indeed, in the post-Royaumont era, probability and statistics were seen as valuable elements of a worldwide reform of the mathematics curricula. Although Bunt explained his approach in a rather classical way, starting

Bert Zwaneveld studied mathematics at the University of Amsterdam. He started his professional career as mathematics teacher in secondary education and mathematics teacher trainer. After these jobs he became mathematics course developer in the Computer Science Department of the Open Universiteit (of the Netherlands). At this university he got his PhD on a study how secondary and undergraduate students can structure their mathematical knowledge and skills, using knowledge graphs (mind maps) as a tool. At the beginning of this century he became professor in the professionalization of mathematics and informatics secondary teachers at the Open Universiteit. His current research interests are: teaching applications of mathematics and especially mathematical modelling, threshold concepts in undergraduate courses of mathematics and computer science, and the history of mathematics education, more especially in the field of applications, modelling and statistics.

Dirk De Bock is professor of mathematics in the Faculty of Economics and Business of the University of Leuven (Belgium). His major research interests are history of mathematics education, psychological aspects of teaching and learning mathematics, the role of mathematics in economics and finance, and financial literacy. His recent research in the field of history of mathematics education focused on the role of Belgian mathematicians and mathematics teachers in the international modern mathematics reform movement of the 1960s, and has led to the monograph [9]. Ongoing research projects include the study of New Math or modern mathematics from an international perspective.

with some probability axioms (in pure *New Math* style), the approach in his textbook was very pragmatic. Bunt did not emphasize 'theoretical aspects', accepted properties without proof and provided many clarifying examples. This pragmatic style enabled Bunt to explain the basic principles of hypothesis testing at the end of his course, in a limited number of lessons. Nowadays in the Netherlands and in several other countries, probability and statistics are included in the mathematics programmes, at least for some streams at the secondary level, but in the 1950s and 1960s, it was quite revolutionary to propose to teach these topics at that school level.

Because of his didactical work in general and more specifically on statistics, Bunt was important in Dutch mathematical education in the post-World War II period. Due to his participation in Royaumont and other international conferences, and his textbooks in English, Bunt may also have played some role in debates about the gradual introduction of statistical curricula for the secondary school level in other countries. However, this role has not yet been clarified and might be a topic for follow-up research.

Acknowledgments
The authors thank Bunt's son Harry for the biographical information about his father, Circe Mary Silva da Silva for her information about Bunt's activities in Brazil, Danny Beckers for the information about the start of the CMLW, Harrie Broekman for his information about Bunt in the years he was Bunt's colleague at Utrecht University, and Leo Rogers for his feedback on an earlier draft of this paper.

Notes

1 The other association of teachers of mathematics was Wimecos. Both associations, Liwenagel and Wimecos, were the predecessors of the Nederlandse Vereniging van Wiskundeleraren ('Dutch Association of Mathematics Teachers').

2 At that time, the gymnasia in the Netherlands had two study streams: The A-stream, preparing students for university studies such as languages, economics, psychology, sociology, history, and geography, and the B-stream, preparing students for university studies in mathematics, science and technology.

3 A lyceum was a school for secondary education with two sections: gymnasium and Hogere Burger School (HBS, 'Higher Citizens School'), similar to gymnasium but without Latin or Greek.

4 All translations were made by the authors.

5 The experiment with the teaching of the history of mathematics happened under the same exception rule.

6 At that time there were these two different Mathematics Teachers' Associations. In 1968 they merged and became the Nederlandse Vereniging van Wiskundeleraren ('Dutch Association of Mathematics Teachers').

References

1 Lucas H.N. Bunt, *Van Ahmes tot Euclides, hoofdstukken uit de geschiedenis van de wiskunde*, Wolters-Noordhof, 1954.

2 Lucas H.N. Bunt, *Statistiek voor het VHMO*, Wolters-Noordhoff, 1956.

3 Lucas H.N. Bunt, *Statistiek als onderwerp voor het gymnasium A: verslag van een proefneming*, Paedagogisch Instituut der Rijksuniversiteit te Utrecht, 1957.

4 Lucas H.N. Bunt, L'enseignement de la statistique dans les écoles secondaires des Pays-Bas, *Mathematica & Paedagogia* 17 (1959), 35–48.

5 Lucas H.N. Bunt, *Statistiek voor het VWO*, Wolters-Noordhoff, 1968.

6 Lucas N.H. Bunt, Phillip S. Jones and Jack D. Bedient, *The Historical Roots of Elementary Mathematics*, Prentice-Hall, 1976.

7 Lucienne Carleer, IX[e] rencontre internationale de professeurs de mathématiques, *Mathematica & Paedagogia* 7 (1955–1956), 63–66.

8 Dirk De Bock and Geert Vanpaemel, Modern Mathematics at the 1959 OEEC Seminar at Royaumont, in K. Bjarnadóttir, F. Furinghetti, J. Prytz and G. Schubring (Eds.), *"Dig where you stand" 3, Proceedings of the Third International Conference on the History of Mathematics Education*, Uppsala University, 2015, pp. 151–168.

9 Dirk De Bock and Geert Vanpaemel, *Rods, Sets and Arrows: The Rise and Fall of Modern Mathematics in Belgium*, Springer, 2019.

10 Dirk De Bock and Bert Zwaneveld, From Royaumont to Lyon: Applications and modelling during the sixties, in G.A. Stillman, G. Kaiser and C.E. Lampen (Eds.), *Mathematical Modelling Education and Sense-Making*, Springer, 2020, pp. 407–417.

11 Johan C.H. Gerretsen and Johannes De Groot, *Proceedings of the International Congress of Mathematicians*, North-Holland, 1954, Vol. 1, p. 12 (Bunt chaired section VII), pp. 545–546; Vol. 2, p. 416.

12 Saskia La Bastide-van Gemert, *All Positive Action Starts with Criticism. Hans Freudenthal and the Didactics of Mathematics*, Springer, 2015.

13 Liwenagel, Rapport van de commissie ter bestudering van een reorganisatie van het wiskundeonderwijs in de A-afdelingen van de gymnasia en de gymnasiale afdelingen der lycea, *Euclides* 26(2) (1950–1951), 49–55.

14 Bert Nijdam, Jan Van Daal, Jan Sloff, Jo Wouters, Ane Yntema (successor of Jo Wouters) and Bert Zwaneveld, *Statistiek en kansrekening voor het VWO*, IOWO, 1973.

15 OEEC, *New Thinking in School Mathematics*, OEEC, 1961.

16 Piet Vredenduin, Commissie Modernisering Leerplan Wiskunde, *Euclides* 37(5) (1962), 144–151.

17 Bert Zwaneveld and Dirk De Bock, Views on usefulness and applications during the sixties, in K. Bjarnadóttir, F. Furinghetti, J. Krüger, J. Prytz, G. Schubring, H.J. Smid (Eds.), *"Dig where you stand" 5, Proceedings of the Fifth International Conference on the History of Mathematics Education*, Freudenthal Institute, 2019, pp. 387–399.

Jan Karel Lenstra
voorzitter PWN-commissie Onderwijs
jkl@cwi.nl

Heleen van der Ree
beleidsmedewerker Nederlandse Vereniging van Wiskundeleraren
h.vanderree@nvvw.nl

Onderwijs

Op weg naar een nieuw curriculum voor de bovenbouw van havo en vwo

De Nederlandse Vereniging van Wiskundeleraren en het Platform Wiskunde Nederland hebben aanbevolen om de inrichting van het wiskundeonderwijs in de bovenbouw van havo en vwo te veranderen. Er worden drie groepen vervolgopleidingen onderscheiden met elk een eigen wiskundeprogramma, opgebouwd uit drie clusters van eindtermen. Jan Karel Lenstra (PWN) en Heleen van der Ree (NVvW) geven een beschrijving en onderbouwing van de voorgestelde structuur.

In 2015 zijn nieuwe examenprogramma's voor havo en vwo ingevoerd, ontwikkeld door de commissie Toekomst Wiskunde Onderwijs (cTWO). De commissie signaleerde in haar eindrapport [1] al een aantal knelpunten. Uiteraard zijn niet alle problemen in het onderwijs op te lossen door een wijziging in het curriculum. In deze notitie beschrijven wij hoe een herziening daar wel aan kan bijdragen.

Knelpunten in de bovenbouw

De NVvW en de PWN-commissie Onderwijs hebben een visiedocument opgesteld ten behoeve van het onderwijsvernieuwingsproject Curriculum.nu [4, 5]. Maarten Müller doet in het NAW van juni 2020 [3] verslag van de opbrengsten van dit project, die zich echter niet uitstrekken tot de bovenbouw van havo en vwo.

Het visiedocument gaat uit van de kernwaarden van de wiskunde in het voortgezet onderwijs, die aansluiten bij de drie centrale doelen van het onderwijs: *persoonlijke vorming, maatschappelijke toerusting* en *voorbereiding op vervolgopleiding en beroep*. In de onderbouw wordt een brede en stevige basis in de wiskunde gelegd, bestaande uit rekenen, algebra, analyse, meetkunde, kansrekening en statistiek. In de bovenbouw vindt dan profilering en differentiatie plaats op basis van de capaciteiten en voorkeuren van de leerlingen en de behoeftes van de vervolgopleidingen. Het document noemt vier knelpunten die zich in de huidige structuur in de bovenbouw van havo en vwo voordoen:

Eindrapport cTWO [1]

- de dubbelzinnige inrichting van wiskunde A, dat zowel maatschappij- als natuurprofielen moet bedienen;
- de kwetsbare positie van de kleine vakken wiskunde C en wiskunde D, waardoor een aantal scholen wiskunde D niet meer aanbiedt;
- het ontbreken van statistiek in wiskunde B;
- het havo-vak wiskunde B, dat door bijna geen enkele hbo-opleiding wordt geëist.

De commissie cTWO deed in 2012 al aanbevelingen tot veranderingen. Het leek haar "een goede zaak, de positie van wiskunde in de profielstructuur te heroverwegen. Daarbij kan gedacht worden aan één wiskundevak voor de maatschappijprofielen waarin het wiskunde A-programma geheel of grotendeels wordt samengevoegd met onderdelen uit het vernieuwde wiskunde C-programma. Denk daarbij bijvoorbeeld aan een uitbreidingsstructuur zoals die voor 2007 bestond. Daarnaast zou er dan één wiskundevak in de natuurprofielen moeten zijn dat bestaat uit een samenvoeging van de wiskunde B- en wiskunde D-programma's." [1, p. 25]

Een nieuwe inrichting van het wiskundeonderwijs kan direct bijdragen aan het

oplossen van de eerste drie knelpunten. Voor het vierde punt zal eerst onderzocht moeten worden of een andere invulling van het vak wiskunde B op de havo beter aan de behoefte van het hbo zou voldoen. Uitgangspunten voor de herinrichting zijn enerzijds de bestaande profielen binnen havo en vwo en anderzijds de behoefte aan wiskundekennis en -vaardigheden in het vervolgonderwijs.

Drie wiskundevakken

Wij onderscheiden drie groepen vervolgopleidingen.

1. *Culturele en sociale studies* en *studies in de gezondheidszorg* hebben informatieverwerking en onzekerheid en onderwerpen uit de discrete wiskunde nodig.
2. *Economische en toegepaste bètastudies* hebben daarnaast behoefte aan algebra, analyse en meetkunde.
3. *Fundamentelere bètastudies* en *technische studies* vragen om méér algebra, analyse en meetkunde.

Dit leidt tot een voorstel voor drie clusters van eindtermen:

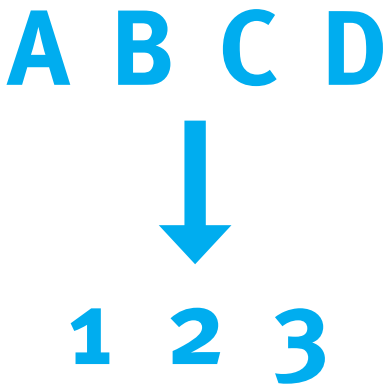
- Cluster IOD: informatieverwerking en onzekerheid (combinatoriek, kansrekening, schatten en toetsen, beschrijvende statistiek) en discrete wiskunde (grafen en netwerken).
- Cluster AAM: algebra, analyse en meetkunde.
- Cluster AAM+: verdieping in algebra, analyse en meetkunde en een compacte module kansrekening en statistiek.

Het ligt dan voor de hand om drie vakken in te voeren bedoeld als voorbereiding op de drie groepen vervolgopleidingen:

- Wiskunde 1: cluster IOD.
- Wiskunde 2: clusters IOD en AAM.
- Wiskunde 3: clusters AAM en AAM+.

De precieze invulling van de drie clusters valt buiten het kader van deze notitie en moet in een vervolgtraject worden uitgewerkt. Het is van belang dat er in ieder cluster aandacht is voor vaardigheden zoals modelleren, abstraheren en probleemoplossen en dat er inspiratie wordt geput uit terreinen zoals natuur en techniek, logistiek en finance, en duurzaamheid en klimaat.

Op welke manier draagt de voorgestelde herinrichting bij aan het oplossen van de vier genoemde knelpunten, waarbij ook



de centrale onderwijsdoelen in het oog worden gehouden?

De dubbelzinnige inrichting van wiskunde A. Wiskunde A kan momenteel in de profielen CM, EM en NG worden gekozen. Deze profielen bereiden voor op een scala aan vervolgopleidingen met sterk uiteenlopende eisen aan wiskundige voorkennis. Het vak heeft daarmee geen eenduidig doel. Ons voorstel brengt een duidelijke focus aan, gericht op vervolgopleidingen, waarbij leerlingen uit een M-profiel wiskunde 1 of 2 volgen en leerlingen uit een N-profiel wiskunde 3.

De kwetsbare positie van wiskunde C en wiskunde D. Met een herinrichting volgens ons voorstel komen belangrijke domeinen uit wiskunde D in het cluster AAM+ terecht. Wiskunde 3 wordt dan door alle leerlingen uit de N-profielen gevolgd en bovendien op iedere school aangeboden. Bèta- en technische studies zullen hier baat bij hebben, mits de toevoeging van kansrekening en statistiek niet ten koste gaat van de algebra, analyse en meetkunde.

Wiskunde C is oorspronkelijk toegesneden op een aantal vervolgopleidingen. Bij het samenstellen van het cluster IOD kan dat heroverwogen worden, met een grotere doelgroep voor ogen. Leerlingen die kiezen voor wiskunde 2 zijn wellicht organisatorisch te combineren met wiskunde 1. Wiskunde 1 wordt dus geen vak met weinig leerlingen.

Het ontbreken van statistiek in wiskunde B. Ons voorstel komt hieraan tegemoet. Dit is een belangrijke verbetering in het kader van maatschappelijke toerusting en bij de voorbereiding op bèta- en technische studies.

Het havo-vak wiskunde B. Op de havo is het moeilijk gebleken een voldoende divers en interessant aanbod aan wiskunde te creëren. De havo kent geen wiskunde C, weinig scholen bieden wiskunde D aan, en vrijwel geen vervolgopleiding eist wiskunde B.

Het brede instroombeleid van het hbo vindt zijn grond in de plicht studenten met een mbo-diploma toe te laten en de wens zoveel mogelijk studenten aan te trekken. Veel opleidingen worstelen daardoor met het wiskundeniveau van de instromende studenten. Het succes van iedere herinrichting van de wiskunde op de havo is afhankelijk van een herbezinning van het hbo op dit punt.

Toch kan een herinrichting en een weloverwogen samenstelling van de clusters IOD, AAM en AAM+ van eindtermen tot verbetering leiden. Doel is dat leerlingen, rekening houdend met hun capaciteiten, voorkeuren en vervolgopleiding, een keuze kunnen maken die bijdraagt aan hun persoonlijke vorming en hun voorbereiding op het vervolgonderwijs.

Aansluiting bij de aanbevelingen van cTWO

Dit voorstel sluit aan bij de insteek van cTWO [1]. Daaruit komt een beeld naar voren met twee soorten wiskunde in de bovenbouw, in de huidige termen wiskunde A+C en wiskunde B+D; de genoemde uitbreidingsstructuur houdt in dat sommige leerlingen een deelvak van de samenvoeging A+C volgen. Er zijn overeenkomsten met de voorgestelde structuur met drie wiskundevakken. Want ook al spreekt cTWO over het samenvoegen van bestaande vakken en zouden wiskunde 1, 2 en 3 op basis van de drie doelgroepen een nieuwe invulling krijgen, veel van de uiteindelijke inhoud van de clusters IOD, AAM en AAM+ zullen herkenbare domeinen uit wiskunde A, B, C en D blijken te zijn.

De aanbeveling van cTWO beperkt bovendien de rol van wiskunde A tot de M-profielen (eventueel met een deelvak voor profiel CM) en bestrijdt zo de dubbelzinnige inrichting op eenzelfde manier als wiskunde 2 dat zou doen. De samenvoeging van wiskunde B en D voor de N-profielen speelt een soortgelijke rol als wiskunde 3 zou doen. En het ontbreken van statistiek in wiskunde B wordt er ook mee verholpen.

Een voordeel van de benadering die cTWO voorstond, is dat de waardevolle elementen van het huidige wiskundeprogramma behouden blijven. Daar zal oog voor moeten zijn wanneer de drie groepen

vervolgopleidingen als uitgangspunt worden gekozen. Er zijn meer elementen uit de geschiedenis die wij bij een herinrichting in ogenschouw moeten nemen, bijvoorbeeld wat de overwegingen waren om van de structuur bestaande uit wiskunde A1,2 met deelvak A1 en wiskunde B1,2 met deelvak B1 af te stappen. Die paste uitstekend bij de inrichting in profielen. Wringt aansluiten bij het vervolgonderwijs met de vierledige profielstructuur?

Vervolgopleidingen

Een herinrichting van de wiskunde in de bovenbouw van havo en vwo dient hoe dan ook de bezwaren van de huidige structuur te ondervangen. Zij moet breed gedragen worden en de voorbereiding op vervolgopleiding en beroep maar ook de maatschappelijke toerusting en de persoonlijke vorming moeten ermee worden gediend. Het doel van de herinrichting is dat iedere leerling de wiskunde leert waar hij of zij iets aan heeft, die aansluit bij de belangstelling en die voorbereidt op de vervolgopleiding.

De voorbereiding op vervolgopleidingen lijkt een geschikt uitgangspunt. De PWN-commissie Onderwijs heeft in een reeks van 21 interviews met vervolgopleidingen geverifieerd of de voorgestelde herinrichting zal leiden tot een betere aansluiting tussen voortgezet en hoger onderwijs [6]. De gesprekspartners ontvingen

Onderzoeksrapport SLO [7]

het voorstel positief, al zullen de gevolgen op het hbo minder direct zijn, door oorzaken die buiten de wiskunde liggen.

Wij onderstrepen dat de door ons aangegeven koppeling tussen vervolgopleidingen en clusters van eindtermen slechts indicatief is. Het is aan de vervolgopleidingen om te bepalen welke eisen zij stellen. Uit de interviews blijkt dat er grote verschillen bestaan binnen dezelfde studie aan verschillende instellingen. Voorbeelden zijn de opleidingen informatica en ICT, vooral op het hbo, en de opleidingen economie en bedrijfskunde.

Ten slotte merken wij op dat het onderwijs in de wiskunde niet ophoudt bij havo en vwo. Studenten in de wiskunde, natuurkunde en econometrie leren de meeste wiskunde in de collegebanken. Disciplines waar het gebruik van de wiskunde op dit moment toeneemt, zoals de biologie en de rechtsgeleerdheid, zullen daaraan moeten wennen.

Hoe verder?

Het Ministerie van OCW heeft in ons voorstel aanleiding gevonden om het Nationaal Expertisecentrum Curriculumontwikkeling SLO opdracht te geven een uitgebreider onderzoek naar de knelpunten in het wiskundeonderwijs in de bovenbouw van havo en vwo uit te voeren. Dit onderzoek vond plaats onder docenten, vervolgopleidingen, leerlingen en schoolleiders en kwam gereed in juli 2021 [7]. Wij noemen ook de blogs die Petra Hendrikse (SLO) aan dit onderwerp wijdt [2]. Vervolgens heeft OCW SLO gevraagd om een advies aan de minister over de vakkenstructuur voor wiskunde in de bovenbouw van havo en vwo. Daartoe is in september 2021 een werkgroep ingesteld. De bevindingen van deze werkgroep kunnen leiden tot een aanpassing van de vakkenstructuur, waarna een vakvernieuwingscommissie aan de slag kan met het bepalen van de inhoud.

Referenties

1 Commissie Toekomst Wiskunde Onderwijs, *Denken & doen – wiskunde op havo en vwo per 2015*, eindrapport van de vernieuwingscommissie wiskunde cTWO, 2012.

2 Petra Hendrikse, Knelpunten uit het onderzoek naar de vakkenstructuur wiskunde h/v, blogreeks op SLO-website, https://www.slo.nl/sectoren/havo-vwo/wiskunde-havo-vwo/bovenbouw/knelpunten-onderzoek-vakkenstructuur, 2021.

3 Maarten Müller, Op weg naar een nieuw curriculum, *Nieuw Archief voor Wiskunde* 5/21(2) (2020), 129–133.

4 NVvW en PWN-Commissie Onderwijs, *Wiskunde in het voortgezet onderwijs*, 2018, https://www.platformwiskunde.nl/wp-content/uploads/2018/01/20180117-wiskunde-in-vo.pdf.

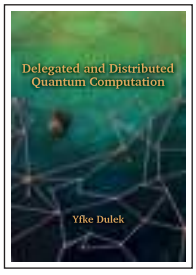
5 NVvW en PWN-Commissie Onderwijs, *Wiskunde in het voortgezet onderwijs: aandacht voor de bovenbouw van havo en vwo*, 2020, https://www.platformwiskunde.nl/wp-content/uploads/2020/01/20191031-W-vo-bb.pdf.

6 PWN-commissie Onderwijs, Aansluiting tussen voortgezet en hoger onderwijs, *Euclides* 95(7) (2020), 14–15.

7 SLO, *Uitkomsten onderzoek vakkenstructuur wiskunde havo-vwo bovenbouw*; https://www.slo.nl/@19152/uitkomsten-onderzoek-vakkenstructuur, 2021.

In de verdediging

| In defence



Delegated and Distributed Quantum Computation
Yfke Dulek

In January 2021 Yfke Dulek from the CWI and QuSoft, the Dutch research centre for quantum software, successfully defended her PhD thesis with the title *Delegated and Distributed Quantum Computation*. Yfke carried out her research under the supervision of dr. Christian Schaffner (UvA) and Prof. dr. Harry Buhrman (UvA).

In classical cryptography the goal is to develop methods to encrypt classical messages. Classical here refers to messages consisting of binary bits, the building block of classical information. Quantum computers perform computations using quantum bits, or qubits, and not classical bits. This means that quantum messages are inherently different from classical messages, while a classical message is usually modelled as a string of bits (0 or 1), a quantum message consists of qubits, which can be thought of as vectors $\varphi \in \mathbb{C}^2$ with norm 1, much richer objects that can be in one of infinitely many different states.

In her dissertation, Yfke explored the power and limitations of cryptography for quantum data. Can it help to securely delegate or distribute a quantum computation in a network of computers? Before diving into the quantum world and the details of Yfke's research, let's have a quick look at some important concepts from classical cryptography.

Absolute security

The quest for safe encryption methods dates to the ancient times, from the Scytale of the Spartans to the Ceasar cipher of the Romans. However, theoretically understanding how a safe encryption mechanism should be constructed is a much more recent endeavour. Auguste Kerckhoffs observed in 1883 that a proper secret key is crucial to a successful cryptographic protocol. Simply said, he postulated that an encryption should stay secure, even if everything about the encryption protocol, except of the secret key, is accessible to the public. Kerckhoffs's principle has been essential to shaping cryptography as we know it today.

In 1948 Claude Shannon published his article 'A mathematical theory of communication' which gave birth to the field of information theory. In his article Shannon formalized the notion of information content of a message, and showed that information can be quantified using bits which could be studied mathematically. To properly hide a message from adversaries, one has to ensure that there is no information about the message present in the *ciphertext*, the text that is obtained after encrypting the message. At the same time, a receiver that knows the secret key should of course be able to retrieve all the information about the message. Shannon showed that the only way to simultaneously achieve these properties is to use a secret key of the same length as the message.

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: Nicolaos Starreveld
FNWI, Universiteit van Amsterdam
Postbus 94214
1090 GE Amsterdam
verdediging@nieuwarchief.nl

The canonical example of an information-theoretically secure encryption scheme is the one-time pad. Encrypting an n-bit message $x \in \{0,1\}^n$ with the one-time pad requires an n-bit secret key $k \in \{0,1\}^n$. The ciphertext $c \in \{0,1\}^n$ is defined by simply taking the bitwise XOR between the message and the key: $c_i = x_i \oplus k_i$ for every $1 \leq i \leq n$. If the key is chosen uniformly at random, one can prove that the message x and ciphertext c share no information: the one-time pad provides perfect information-theoretic security.

Absolute security may not be desirable

The one-time pad described above offers absolute security but in practical applications it may not be desirable. For every encrypted message that has to be communicated, a secret key of the same length should also be communicated. This renders the one-time pad rather inefficient. Hence we see that a balance between security and efficiency is desirable.

Public-key cryptography, where messages are encrypted using a key that is publicly known, and are decrypted with a private key which is known only to the decrypting party, reduces the amount of information that needs to be communicated. This is achieved by slightly relaxing what it means to keep a message secret: instead of requiring that the ciphertext contains no information about the message, it is only required that the information is hard to retrieve. This idea is usually formalized by stating that if one is able to recover the message from the ciphertext, then one is also able to solve a specified mathematical problem. Examples of such problems that are used in cryptographic systems are integer factorization or discrete logarithms of elliptic curves. Under the assumption that this mathematical problem is hard to solve, it should be practically impossible to break the encryption. This provides both efficiency for the user and computational intractability for the attacker. The same ideas hold also in the world of quantum computers for the encryption of quantum messages. Cryptographic systems are based on problems which are believed not to be easily solvable by a quantum computer.

The quantum shield

As described above, classical encryption protocols rely on mathematical problems that are believed to be difficult to solve. Quantum encryption protocols rely on the same idea, but the important question is whether mathematical problems that are classically difficult are also quantumly difficult. In any case, this does not hold for integer factorization. In 1994 Peter Shor discovered a quantum algorithm that can solve prime factorization in polynomial time. At the same time, it is still not known whether there is a classical algorithm that can solve prime factorization for large numbers in polynomial time. Hence encryption algorithms that rely on prime factorization are not secure against an attack from a quantum computer.

A notable example of an information-theoretically secure quantum protocol is the quantum one-time pad, which securely encrypts quantum messages. Similarly to the classical one-time pad, the secret key for the quantum one-time pad is fairly large: to encrypt a message consisting of n qubits, one needs a secret key of length $2n$. The crucial fact that makes the quantum one-time pad a useful tool, however, is the fact that the secret key can consist of classical bits! Since qubits are very sensitive and unstable, using classical keys makes life much easier, even if their length is twice the length of the quantum message.

Photo: MFO, Konrad Jacobs

Claude Shannon

Peter Shor

To understand how the quantum one-time pad works we need a little bit of linear algebra. Operations on qubits are in general described by unitary operators. The most basic unitary operators used in quantum computing are described by the Pauli group, which is the matrix group generated by the two elements

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

which represent a 'bit flip' (swapping the two entries of a qubit vector φ) and 'phase flip' (changing the sign of the second entry relative to the first), respectively. For actual interesting quantum computations, more operators outside of the Pauli group are required: in particular, we need an operator to create quantum superpositions (redistributing weight between the two entries of φ), one to create quantum entanglement (correlating the entries of φ with those of another qubit vector), and one that is capable of performing more complex logical operations akin to 'and' and 'or' gates on a classical computer. However, despite the limited computational power of the Pauli group, it turns out to be sufficient for completely hiding the information in a qubit.

For a single-qubit state φ the quantum one-time pad works as follows. The key generation selects two bits a, b each uniformly at random from $\{0,1\}$. Encryption and decryption correspond to applying the Pauli operator $X^a Z^b$. The encrypted state is thus $X^a Z^b \varphi$. An adversary who has possession over this encrypted quantum state, but does not know the secret key (a,b), has no information about the state φ. The adversary observes a fully mixed state, which is obtained by averaging over the four possible values of (a,b). This idea can be extended to n qubits. In this case the encryption is given by the average over all unitary operators in the n-qubit Pauli group, which is the n-fold tensor product of one-qubit Pauli groups.

Distributing and delegating qubits

In her research Yfke focussed on another complication that emerges due to the nature of quantum computers. Functional quantum computers are very sensitive and delicate machines, which means that when they will become available for open public use, they will likely be in possession of large institutions, either companies or universities, that can guarantee for their proper functioning. Users can then log on and use the quantum computer for their needs. This means that quantum computations will most likely be distributed amongst

multiple parties, or delegated to a party that has possession of a quantum computer. It is thus important that quantum encryption protocols take distribution and delegation of information into consideration. In her PhD Yfke explored the possibilities, and impossibilities, of various cryptographic primitives, the building blocks of encryption protocols, for delegated and distributed quantum computation. Specifically, Yfke considered three quantum-cryptographic primitives, namely quantum homomorphic encryption, multi-party quantum computation, and quantum obfuscation.

Fully homomorphic encryption

The discovery of fully homomorphic encryption (FHE) in classical cryptography in 2009 is widely considered to be one of the major breakthroughs of the field. Unlike standard encryption, FHE makes it possible for parties that do not hold the decryption key to perform computations on encrypted data. In this method encrypting a message corresponds to applying an homomorphism on the plaintexts, mapping them into the ciphertext. Decryption corresponds to inverting the homomorphism. Moreover, as the name suggests, performing operations in the plaintext space should be preserved after applying such a homomorphism. This property allows parties to perform computations on the encrypted data. The same idea applies also in quantum cryptography, but now operations are applied on qubits. In quantum homomorphic encryption (QHE), quantum input data is encrypted in such a way that a server can carry out arbitrary quantum computations on the encrypted data, without interacting with the encrypting party.

In her research, Yfke worked with a hybrid classical-quantum construction, based on a very natural idea: to encrypt a quantum message under the quantum one-time pad, and to encrypt the (classical) keys to the quantum one-time pad under classical FHE, attaching the ciphertexts to the quantum ciphertext. The construction of quantum homomorphic encryption raises an important question: do the numerous classical applications of FHE have suitable quantum analogues? As it turns out, most of the classical applications require an additional property which is simple classically, but nontrivial quantumly. That property is *verification*: the ability of the user to check that the final ciphertext produced by the server is indeed the result of a particular computation, homomorphically applied to the initial user-generated ciphertext. In the classical case, this is a simple matter: the server makes a copy of each intermediate computation step, and provides the user with all these copies. In the quantum case, such a 'transcript' or 'log' appears to violate no-cloning.

Yfke constructed a new QHE scheme where the server can certify, using a classical computation log as 'proof', that a particular homomorphic computation was performed on a quantum ciphertext. The main idea is that some additional qubits are used during the quantum computation, so-called *traps*. These trap-qubits don't contribute to the actual computation, their role is purely to yield information whether the desired computation is performed correctly. During the computation these trap-qubits will be measured at suitably chosen moments, where their state can be theoretically predicted. If all the measurements of the trap-qubits agree with the outcomes that were predicted theoretically, we have a verification that the desired quantum computation was performed correctly!

The more personal aspect

Before we conclude we would like to give the word to the doctorate.

Yfke, would you like to share some memories with us?

"The final result in my thesis (about the impossibility of obfuscation) was very surprising to me. Obfuscation refers to encrypting the code of a (quantum) program, instead of an input value. A computer must be able to run the encrypted program but a user should not be able to retrieve the source code. It was already known to be impossible using classical computers, but for a long time it was believed that 'quantum obfuscation' could exist. There were good reasons to believe this, given the nature of qubits, which rarely reveal all of the information stored in them. Surely, one could use those quantum states to encode information about a secret function? From the start of my PhD, I had been set on constructing such quantum obfuscation. I had ideas on how to do it, but every time, it seemed that some ingredient was still missing. This led to at least two other papers, which were interesting in their own right, but for me they were mostly intermediate steps toward the ultimate goal of quantum obfuscation. As the deadline for my dissertation was approaching, I started to lose hope to ever construct it. My advisor, who had been trying alongside me to construct this elusive cryptographic notion, suggested that maybe it was not possible after all and we should try to prove that. He was right: within a few weeks we had the rough outline of an impossibility proof, just in time for this major result to be included into my thesis. Not exactly the result I had been aiming for, but the dissertation did feel a lot more complete with it."

Were you also involved in some activities you would like to share with the readers?

"Because the field is still relatively young, and therefore still growing, there is a small international network of researchers who actively reach out to the younger members of the community. I have been given many opportunities to showcase my work, by being invited to speak at workshops and summer schools in Barbados, Canada and Switzerland, among others. In the spring of 2020, I spent a semester at the Simons Institute for the Theory of Computing in Berkeley (California) as a fellow during one of their research programs, which always attract many international visitors."

Concluding

Yfke's research focused on quantum cryptography, and more specifically, on cryptographic primitives for delegated and distributed quantum computation. She studied three quantum-cryptographic primitives, namely quantum homomorphic encryption, multi-party quantum computation, and quantum obfuscation.

Since January Yfke is working as a postdoctoral researcher at QuSoft and the CWI, where she furthers her research on quantum cryptography. We wish Yfke all the best with her further research trying to make the quantum world a safe place to compute.

Boekbesprekingen

| Book Reviews

Redactie: Hans Cuypers en Hans Sterk

Review Editors NAW - MF 5.092
Faculteit Wiskunde & Informatica
Technische Universiteit Eindhoven
Postbus 513
5600 MB Eindhoven

reviews@nieuwarchief.nl
www.win.tue.nl/wgreview

Jean-Pierre Serre
with contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler

Rational Points on Curves over Finite Fields

Documents Mathématiques, Vol. 18
Société Mathématique de France, 2020
x + 187 p., prijs € 45,00
ISBN 9782856299234

In 1985 gaf Jean-Pierre Serre een college aan Harvard University: 'The number of points on curves over a finite field'. De handgeschreven aantekeningen van F.Q. Gouvêa hebben veel wiskundigen inspiratie gegeven om aan dit prachtige onderwerp te werken. Het boek dat nu verschenen is geeft dat materiaal en nog veel meer: Serre heeft het materiaal opnieuw bekeken en op een aantal aspecten aangevuld, Everett Howe, Joseph Oesterlé en Christophe Ritzenthaler hebben nieuwe resultaten toegevoegd, en een groot aantal wiskundigen heeft geholpen met het verzorgen van de TeX-versie, zodat we nu dit prachtige boek met Alp Bassa, Elisa Lorenzo García, Christophe Ritzenthaler en René Schoof als editors tot onze beschikking hebben.

Over de vraag wat het aantal rationale punten op een algebraïsche kromme over een eindig lichaam is, schrijft Serre in zijn voorwoord: "After more than a century of general theorems in algebraic geometry, one should be able to answer such a concrete question." We beschrijven wat de bevindingen zijn van Serre (en veel andere wiskundigen) hierover, en we zullen zien dat die 'general theorems' lang niet altijd een antwoord geven zonder nog meer werk te verrichten.

In deze bespreking geef ik eerst wat achtergrondinformatie: meetkunde, getaltheorie en coderingstheorie.

We schrijven $q = p^e$ voor een macht van een priemgetal p. We weten dat er voor elke q een eindig lichaam is met q elementen, genoteerd als $\mathbb{F}_q$, eenduidig op isomorfie na. Voor een reëel getal t is $[t]$ het grootste gehele getal niet groter dan t. Voor elke algebraïsche variëteit V over een eindig lichaam $K = \mathbb{F}_q$ is het aantal punten op V met coördinaten in K eindig: $\#(V(\mathbb{F}_q)) < \infty$. Wat kunnen we zeggen over dit aantal, en waarom is het interessant? We nemen over van het boek: $N_q(g)$ *is het maximale aantal rationale punten op een kromme van geslacht* g *over* $\mathbb{F}_q$.

In een dagboekaantekening in 1814 beschreef Gauss een wonderlijk vermoeden over het aantal rationale punten op een specifieke kromme over een priemlichaam. Later bleek dat hij de precieze formule voor die gevallen juist had. We weten niet hoe Gauss tot dat diepe inzicht kwam. Kende en gebruikte Gauss de volgende observatie? De afbeelding die de coördinaten tot de macht q verheft geeft een afbeelding $F : V \to V$, die we de *Frobenius afbeelding* noemen. Was Hasse de eerste (in 1930) die deze afbeelding formuleerde? Het is eenvoudig in te zien dat voor V gedefinieerd over $\mathbb{F}_q$ de verzameling V^F van dekpunten van F gelijk is aan $V(\mathbb{F}_q)$. Deze meetkundige formulering blijkt de sleutel te zijn tot opmerkelijke ontwikkelingen.

We gaan een verband zien met het klassieke Riemann Vermoeden, we schrijven RH, dat Riemann formuleerde in 1895 voor de Riemann zetafunctie.

In zijn proefschrift in 1921 beschrijft Emil Artin een vermoeden hoe we het aantal rationale punten op een *elliptische kromme*

over $\mathbb{F}_p$ kunnen berekenen. Niet alleen ondersteunt Artin dit vermoeden door een veertigtal voorbeelden door te rekenen, maar vooral laat Artin in zijn proefschrift zien hoe dit vermoeden een analogon is van het klassieke RH. Om mogelijke verwarring te voorkomen zal ik het vermoeden over een eindig lichaam noteren als pRH. Aanvankelijk werd pRH als even moeilijk gezien als het klassieke RH, maar vanaf 1933 gaf H. Hasse verschillende bewijzen voor het pRH voor elliptische krommen.

In 1940–1949 generaliseerde André Weil dit vermoeden tot een indrukwekkend inzicht, geformuleerd in de *Weil-vermoedens*, voor variëteiten over een eindig lichaam. Weil bewees deze vermoedens voor algebraïsche krommen van willekeurig geslacht. Daaruit zien we de (Hasse-)Weil-grens: voor een kromme C van geslacht g over $\mathbb{F}_q$ zijn de eigenwaarden van Frobenius $\pi_1,\ldots,\pi_{2g}$ algebraïsche, gehele getallen en voor elke inbedding $\mathbb{Q}(\pi)\subset\mathbb{C}$ geldt $|\pi|=\sqrt{q}$; een dergelijk getal noemen we een q-Weil-getal; met behulp daarvan is bewezen dat

$$\#(C(\mathbb{F}_q)) = 1 - S + q \le 1 + [2g\sqrt{q}] + q, \quad \text{met } S := \sum_{1\le j\le 2g} \pi_j.$$

Voor $g=1$ zijn deze eigenwaarden π_j óf een geheel getal, e is even, en $\pi = \pm p^{e/2}$, óf $\pi\notin\mathbb{Z}$ en de complex geconjugeerden π en $\bar{\pi}=q/\pi$ komen voor. Met deze informatie is het niet moeilijk om voor het geval $g=1$ alle mogelijkheden op te schrijven.

In Hoofdstuk 2 zien we hoe de Weil-grens

$$N_q(g) \le 1 + [2g\sqrt{q}] + q$$

eenvoudig verscherpt kan worden tot

$$N_q(g) \le W(g) := 1 + g\cdot[2\sqrt{q}] + q.$$

Bovendien, als we weten welke q-Weil-getallen $\{\pi_1,\ldots,\pi_{2g}\}$ optreden voor $C/\mathbb{F}_q$ dan zijn de q^m-Weil-getallen voor $C/\mathbb{F}_{q^m}$ precies $\{\pi_1^m,\ldots,\pi_{2g}^m\}$. Verbluffend: als we voor een elliptische kromme $E/\mathbb{F}_q$ weten wat $\#(E(/\mathbb{F}_q))$ is, dan kennen we π en q/π, en berekenen we eenvoudig het aantal $\#(E(\mathbb{F}_{q^m}))$ voor alle m.

We vermelden nog dat de Weil-vermoedens geformuleerd en gegeneraliseerd kunnen worden voor de zetafunctie van een algebra Λ van eindig type over $\mathbb{Z}$. Het geval $\Lambda=\mathbb{Z}$ geeft het klassieke RH, en is niet opgelost; de gevallen met $0=p\cdot 1\in\Lambda$ vallen onder de pRH. Een indrukwekkend aspect van twintigste-eeuwse wiskunde. Speciale gevallen zijn bewezen. Het algemene vermoeden, met daaronder het klassieke RH lijkt nog ver buiten ons bereik te liggen.

De Weil-vermoedens begonnen met de verrassende observatie van André Weil dat de formule

$$\#(C^F) = \#(C(\mathbb{F}_q)) = 1 - S + q$$

lijkt op de 'dekpuntenstelling' van Lefschetz uit 1926, die het aantal dekpunten van een afbeelding $f: T\to T$ op een compacte topologische ruimte berekent als wisselsom van de sporen op de relevante homologiegroepen; een fascinerend aspect van de wiskunde van de twintigste eeuw. Vele jaren en vele pagina's prachtige, maar moeilijke wiskunde waren nodig om dit idee exact te kunnen formuleren in de algebraïsche meetkunde (welke cohomologiegroepen heb je nodig?) en te bewijzen (Weil, Grothendieck, Serre, Deligne en vele anderen). Compacte topologische ruimten enerzijds en variëteiten over een eindig lichaam anderzijds lijken begrippen die ver uiteen liggen.

We zullen zien dat de Weil-grens in veel gevallen niet bereikt wordt. Zelfs weten we niet voor gegeven $g\ge 3$ of het verschil tussen $N_q(g)$ en de Weil-grens begrensd is. Om de lezer een indruk te geven laten we een paar eenvoudige voorbeelden zien; ik hoop zo de complexiteit van het probleem duidelijk te maken.

$(g=1, q=p)$ Neem de nulpunten van $T^2+[2\sqrt{p}]T+p$; met behulp van de Honda–Tate-theorie zien we dat deze nulpunten p-Weil-getallen zijn van een elliptische kromme, en

$$N_p(1) = 1 + [2\sqrt{p}] + p$$

is de Weil-grens. Een paar voorbeelden $(g=1, e=1)$: $p=2$, $\pi=-1\pm\sqrt{-1}$, $N_2(1)=5$; $p=3$, $\pi=(-3\pm\sqrt{-3})/2$,$N_3(1)=7$. Voor $p=19$ is $[2\sqrt{19}]=8$, en $\pi=-4\pm\sqrt{-3}$ geeft $N_{19}(1)=1+8+19=28$. Voor $p=23$ nemen we $\pi=(-9\pm\sqrt{-11})/2$, en $N_{23}(1)=1+9+23=33$.

Voor $N_q(1)$ met $q=p^e$, met $m=m(q):=[2\sqrt{q}]$, geeft Theorem 2.6.3:

$$q+m \le N_q(1) \le 1+m+q.$$

Meestal is m niet deelbaar door p, en de Weil-grens wordt wel bereikt door $N_q(1)$. Maar voor $p>3$ en m deelbaar door p wordt de Weil-grens niet bereikt: voor $q=2^7$ met $m=22$, $q=3^7$ met $m=93$, $q=5^9$ met $m=2795$, en $q=7^5$ met $m=259$ en $q=13^{17}$, is $m(q)$ deelbaar door p (de 'exceptionele gevallen'); in die gevallen is $N_q(1)=m+q$ en in deze gevallen wordt de Weil-grens niet bereikt. (Opgave voor de lezer: kies $p=11$; vind een oneven e zo dat $m(q)=[2\sqrt{11^e}]$ deelbaar is door 11.)

Een open probleem is het volgende: is er een priemgetal $p>7$ zo dat p een deler is van $[2\sqrt{p^5}]$? Een dergelijke p is groter dan 10^7, zie Remark 2.6.5. Een andere vraag luidt: is er voor elk priemgetal p een oneven e zo dat $m(p^e)=[2\sqrt{p^e}]$ deelbaar is door p? We geven wat nadere uitleg. Voor $q=3^7$ met $m=93$ is een nulpunt π van $T^2+93T+3^7$ wel een q-Weil-getal, π is niet een Frobeniuseigenwaarde op een elliptische kromme, maar wel een Frobeniuseigenwaarde van een abelse variëteit van dimensie 7.

We zien het onvoorspelbare gedrag van $N_q(1)$. Er lijkt geen 'algemene formule' te zijn voor $N_q(g)$.

$(g=2, q=2)$ De Weil-grens hier is $1+2[2\sqrt{q}]+2=7$; nagaan welke expliciete gevallen van 2-Weil-getallen mogelijk zijn, laat zien dat $\#(C(\mathbb{F}_2))\le N_2(2)=6$. Evenzo:

$$N_4(2) = 10 < 13 = 1 + 2[2\sqrt{4}] + 4 = 13.$$

Voor een discussie van de waarden van $N_q(2)$ zie Theorem 3.2.3.

$(g>1, q=p^e$ met $e=2s)$ Als $\#(C(\mathbb{F}_q)) = 1+2g\cdot\sqrt{q}+q$, dan is e even en er geldt $\pi_j=-\sqrt{q}$. Dan is $\pi_j^2=q$ en uit

$$1 - 2gq + q^2 = \#(C(\mathbb{F}_{q^2})) \ge \#(C(\mathbb{F}_q))$$

volgt eenvoudig $2g\le q-\sqrt{q}$. We zien: voor *even* e en grote g wordt de Weil-grens $W(g)$ niet bereikt.

Over het verbeteren van grenzen op $\#(C(\mathbb{F}_q))$ is veel onderzoek gedaan. Een groot deel van het boek is besteed aan de vraag: *kunnen we een scherpe bovengrens bepalen voor het maximale aantal rationale punten $N_q(g)$ als g en q gegeven zijn*?

Coderingstheorie. Hoe kun je een bericht coderen, zodat bij kleine verstoring een verminkte code nog hersteld kan worden. Een lineaire code van type $[n,k,d]$ wordt gegeven door een lineaire deelruimte van dimensie k van de eindigdimensionale vectorruimte $V=(\mathbb{F}_q)^n$; schrijf d voor het minimale aantal niet-nulcoördinaten

in een niet-nul element van V. We zoeken codes met d en k groot (je wilt veel fouten kunnen corrigeren), en n zo klein mogelijk (je wilt kleine gecodeerde woorden). In 1970 en in 1982 liet V.D. Goppa zien hoe een kromme van klein geslacht met veel rationale punten een efficiënte lineaire code geeft. Voor een beschrijving zie § 1.2, pp. 2–4, in het boek. We gebruiken graag $\mathbb{F}_2$ als grondlichaam.

In 1981 bespreekt Yu.I. Manin "What is the maximum number of points on a curve over $\mathbb{F}_2$?" Is dit een moeilijk probleem? Voor wie dit onderwerp niet kent: probeer het maar eens voor $g = 7$ over $\mathbb{F}_2$; de Weil-grens geeft

$$N_2(7) \leq 1 + 7 \cdot [2\sqrt{2}] + 2 = 17.$$

We laten zien hoe $N_2(7)$ bepaald wordt (en we zien dat het een lastig probleem is).

We zien dat $N_2(g)$ momenteel berekend is voor slechts 17 waarden van g, zie Table 2 op pagina 169.

In 1972/1975 werd de Gilbert–Varshamov-grens geformuleerd, ook wel bekend als de Gilbert–Shannon–Varshamov-afschatting. Ik weet nog hoe het een schok was toen in 1982 M.A. Tsfasman, S.G. Vlădut en Th. Zink lieten zien dat de methode van reductie modulo p van modulaire krommen en van Shimura-variëteiten een verscherping van de GV-grens geeft. Ideeën, standaard in het ene vak, waren plotseling relevant in een heel andere tak van wiskunde.

Nu richten we ons op algemene methoden. Een *abelse variëteit* is een projectieve algebraïsche variëteit A waarvan de punten een groep vormen. In het werk van Abel komen punten op sommige A voor als waarden van een bepaalde integraal van een differentiaalvorm op een Riemann-oppervlak, vandaar de naam. Zo zien we dat elke kromme C van geslacht g aanleiding geeft tot een abelse variëteit $A = \mathrm{Jac}(C)$ van dimensie g. Vaak geeft meetkunde van $\mathrm{Jac}(C)$ waardevolle informatie over C. Over de constructie van $C \mapsto \mathrm{Jac}(C)$ en uitwisseling van eigenschappen van C en van $\mathrm{Jac}(C)$ bestaat veel literatuur.

T. Honda en J.T. Tate lieten in 1986 zien dat voor elk q-Weil-getal π er een abelse variëteit A over $\mathbb{F}_q$ bestaat waarvan π een eigenwaarde van de Frobenius $\mathrm{Frob}_{A/\mathbb{F}_q} = F_A : A \to A$ is. Tate liet in 1966 zien hoe aritmetische eigenschappen van π invarianten van A bepalen, waaronder de dimensie van A. Een krachtig hulpmiddel om langs deze weg abelse variëteiten over een eindig lichaam te construeren. Die algemene stelling, de Honda–Tate-theorie, is goed begrepen.

Hoe kunnen we dit gebruiken om krommen te vinden met veel rationale punten? Voor $g \leq 3$ 'komt elke abelse variëteit af van een kromme'; echter, voor $g > 3$ zijn er 'veel meer' abelse variëteiten dan algebraïsche krommen.

Hoe zien we welke π met $|\pi| = \sqrt{q}$ gerealiseerd wordt door een kromme? 'General theorems' zoals Serre dat noemt in zijn voorwoord, zijn voor dit geval niet direct toepasbaar in het probleem van rationale punten op krommen van geslacht $g > 3$. En, zoals Serre het formuleert in zijn introduction: "When one reads Mumford's booklet *Curves and their Jacobians*, one realizes the sad fact that we have 'no reasonable effective way' to describe the curves with ... a large genus."

Bijvoorbeeld, hoe krijgen we expliciete informatie over 'alle' krommen van geslacht 7 over $\mathbb{F}_q$, die we zouden kunnen gebruiken om $N_q(7)$ te bepalen? We zullen zien dat reeds voor $q = 2$ dit een lastig probleem is. We zien diepe, algemene stellingen en constructies die wel bovengrenzen, echter niet een formule voor $N_q(g)$ lijken te geven, het beginpunt van dit boek.

We geven een korte samenvatting van (een deel van) de inhoud van dit boek. Algemene methoden geven niet in alle gevallen de scherpste grenzen voor het maximale aantal rationale punten $N_q(g)$. Betere grenzen worden bestudeerd met behulp van *meetkunde* (van algebraïsche krommen), met behulp van *getaltheorie* (eigenschappen van Weil-getallen), en met behulp van methoden uit de *analytische getaltheorie* (zie Hoofdstuk 6). We zien dat een merkwaardige en ingenieuze mix van deze methoden verscherpingen van bestaande grenzen geeft. In een aantal gevallen geven constructies van expliciete voorbeelden aan dat die scherpe bovengrens ook gerealiseerd wordt; in die gevallen wordt $N_q(g)$ bepaald.

Vaak wordt de vraag naar het aantal rationale punten op twee manieren gesteld: óf kies g vast en laat alle mogelijke $q = p^e$ toe, óf kies q vast en bestudeer alle mogelijke g. Beide benaderingen vinden we hier terug. Serre behandelde deze twee onderwerpen op twee verschillende dagen in zijn college.

In het eerste deel worden 'kleine' g bestudeerd. We zien, Hoofdstuk 2, dat voor $g = 1$ resultaten bekend zijn (Deuring, Waterhouse, Tate). Extra aandacht voor de gevallen waar de verscherpte Weil-grens bereikt wordt (storende drukfout op pagina 24: "voor $q = p^e = 2^3$ is p een deler van $m := [2\sqrt{q}]$": we zien $[2\sqrt{8}] = 5$).

Voor $E/\mathbb{F}_q$ schrijven we $E'/\mathbb{F}_q$ voor de kwadratische $\mathbb{F}_{q^2}/\mathbb{F}_q$-twist van E. Voor maximale $E/\mathbb{F}_q$ is $E'/\mathbb{F}_q$ minimaal (storende drukfout in de vijfde regel van 2.6.5). Zo zien we dat hier 'algemene stellingen' mooie antwoorden geven.

In Hoofdstuk 3 worden allerlei algemene methoden ontwikkeld, en wordt het geval $g = 2$ besproken. Resultaten over $N_q(2)$ bewees Serre in 1982 en 1983 (zie vooral ook de brieven hierover van Serre aan Tate). Het resultaat, Theorem 3.2.3, bespreekt alle gevallen; in het bijzonder geldt voor $g = 2$:

$$\big(1 + 2 \cdot [2\sqrt{q}] + q\big) - N_q(2) \leq 3;$$

we zien dat voor $g = 2$ de waarde $N_q(2)$ weinig afwijkt van de Weil-grens. Het bewijs in dit boek van deze stelling bestaat uit een bespreking van algemene methoden en de bestudering van bijzonder gevallen en het kost veertig bladzijden. Dit geeft een mooi beeld van de moeilijkheden in dit onderwerp: dit geval van een kleine g, waar bovendien elke abelse variëteit van dimensie 2 'afkomstig' is van een kromme vergt al zoveel inspanning om tot een complete beschrijving van $N_q(g)$ te komen.

Hoofdstuk 4 bespreekt $g = 3$. Voor $q \leq 29$ geeft het boek een tabel voor de exacte waarde van $N = N_q(3)$. Jaap Top beschreef in 2003 alle gevallen $g = 3$ en $q < 100$. Hier helpt de meetkunde: we weten dat elke kromme C van geslacht drie óf hyperelliptisch is óf dat de kanonieke afbeelding $C \to \mathbb{P}^2$ een isomorfisme geeft met een vlakke kromme van graad 4. In dit laatste geval spelen (een twist) van de Klein-kromme, nulpunten van $X^3Y + Y^3Z + Z^3X$, en (een twist) van de Fermat-kromme, nulpunten van $X^4 + Y^4 + Z^4$ in $\mathbb{P}^2(\mathbb{F}_q)$, een belangrijke rol bij het vinden van voorbeelden. In Conjecture 4.3.1 wordt gevraagd of

$$\big(1 + 3 \cdot [2\sqrt{q}] + q\big) - N_q(3)$$

begrensd is, misschien wel ≤ 6 voor $g = 3$ en alle q? Uit het eerste deel van het boek zien we: een 'algemene formule' die $N_q(g)$ geeft lijkt niet te bestaan, zelfs niet voor kleine g.

In een serie van artikelen en tabellen vanaf 1993 geven Gerard van der Geer en Marcel van der Vlugt een grote hoeveelheid schattingen van $N_q(g)$ en krommen met het maximale aantal rationale punten.

Deel twee van dit boek beschrijft algemene methoden voor grote g. Algemene methoden worden ontwikkeld, en allerlei expliciete voorbeelden geconstrueerd. Uit het rijke palet van technieken en resultaten noem ik een paar aspecten.

Hoofdstuk 7 is gewijd aan een poging om de vraag van Manin "What is the maximum number of points on a curve over $\mathbb{F}_2$?" te beantwoorden. Hier is $q=2$ vast, maar we beschouwen 'alle' g. Om een indruk te geven van technieken en resultaten neem ik over uit het boek de gevallen $g=7$, $g=50$ en $g=120$ met grondlichaam $\mathbb{F}_2$.

In Hoofdstuk 5, en in Hoofdstuk 6 met methodes hoofdzakelijk ontwikkeld door J. Oesterlé, vinden we een indrukwekkende hoeveelheid techniek, die culmineert in het vinden van veel scherpere grenzen op $N_2(g)$. Dat is de ene kant van de benadering van het probleem. We zien bij voorbeeld, een combinatie van allerlei schattingen: $N_2(7)\leq 11<17$, $N_2(50)\leq 40<103$, $N_2(120)\leq 82<243$, aanzienlijke verscherpingen van de Weil-grens gegeven door $1+g\cdot[2\sqrt{2}]+2=2g+3$.

Nu komt de andere benadering van het probleem: het bestaan van voorbeelden met 'veel' rationale punten. Voor $g=7$ wordt er bewezen dat er *wel* een kromme C over $\mathbb{F}_2$ bestaat met $N(C)=10$, zie 7.3.5, zie een discussie verderop, maar er bestaat *niet* een kromme C van geslacht 7 over $\mathbb{F}_2$ met $N(C)=11$, zie 7.2; omdat de Oesterlé-grens bewijst dat $N_2(7)\leq 11$ krijgen we de conclusie: $N_2(7)=10$. Kortom: een lastige schatting en een gecompliceerd voorbeeld geven samen een bewijs dat $N_2(7)=10$. De lezer krijgt bij het bepalen van $N_2(7)$ een beeld van de complicaties van dit probleem.

Voor $g=50$ wordt bewezen dat er een C bestaat met $N(C)=40$; we komen hier op terug; conclusie: $N_2(50)=40$. De schattingen geven $N_2(120)\leq 82$, en het is onbekend wat $N_2(120)$ precies is.

Als antwoord op de vraag van Manin zien we dat een algemene uitspraak over de waarde van $N_g(2)$ voor slechts zeventien waarden van g bekend is.

Twee relevante meetkundige technieken.

(1) *'Plakken' van algebraïsche krommen,* zie § 3.3 en § 4.2. Laat ik een voorbeeld geven. Neem elliptische krommen E_1 en E_2 over een lichaam van karakteristiek ongelijk 2, beschouw $\varphi_1: E_1\to\mathbb{P}^1=S$ van graad twee, vertakt in vier punten, en idem $\varphi_2: E_2\to\mathbb{P}^1=S$. Kies coördinaten op $\mathbb{P}^1$ zo dat drie vertakkingspunten van φ_1 en drie van φ_2 boven eenzelfde punt op $\mathbb{P}^1$ liggen en de andere vertakkingspunten boven twee verschillende punten van $\mathbb{P}^1$. De kromme $C:=E_1\times_S E_2$ is een kromme van geslacht twee; eigenschappen van C kunnen afgelezen worden uit eigenschappen van E_1 en E_2. Deze methode, besproken in § 3.3 en § 4.2, geeft een rijk arsenaal aan nieuwe voorbeelden.

(2) *Klasselichamentheorie voor algebraïsche krommen.* In 1959 beschreef Serre deze methode over een algebraïsch gesloten grondlichaam, en in Hoofdstuk 5 vinden we hier een verdere uitleg. Een kromme Y wordt gegeven, en een abelse overdekking $X\to Y$ wordt geconstrueerd, waar de Galois-groep en een (mogelijk vertakte) overdekking gekozen wordt. Eigenschappen van Y en van de overdekking X/Y geven toegang tot eigenschappen van X.

Laat ik als voorbeeld geven de constructie van $g(C)=7$ over $\mathbb{F}_2$ met $N(C)=10$, zie Table 2, pagina 160. Kies een elliptische kromme E over $\mathbb{F}_2$ met een punt $Q\in E(\mathbb{F}_{2^6})$ zo dat dit een gesloten punt $Q_6\subset E/\mathbb{F}_2$ geeft van graad 6 en kies $C\to E/\mathbb{F}_2$ met $\mathrm{Gal}(C/E)=\mathbb{Z}/2$ met vertakking in $2Q_6$ zodat er precies $n=5$ rationale punten op E totaal splitsen in C/E; zo komt er $N(C)=10$; zie Case 2 van 7.3.5 op pagina 169. De Riemann–Hurwitz-formule geeft $2g-2=2(2-2)+2.6.(2-1)$, dus $g(C)=7$. We weten al $N_2(7)\geq 10$; conclusie: $N_2(7)=10$.

Voor $g=50$ wordt een keuze gemaakt met een elliptische kromme E, met $2Q_7\subset E$, en $\mathrm{Gal}(C/E)\cong(\mathbb{Z}/2)^3$ met $n=5$. Een berekening levert $g(C)=50$ en $N(C)=8\cdot 5=40$; conclusie: $N_2(50)=40$.

Dit boek laat me weer nadenken over de manieren van wiskundig denken en werken. Een simplificatie: als we een probleem proberen op te lossen, dan kunnen we óf algemene methoden ontwikkelen, óf zoveel concreet materiaal (voorbeelden) beschrijven dat we 'zien' wat de oplossing is. Grothendieck was een voorbeeld van de eerste methode: generaliseer een probleem, en los dat dan op; er is veel mee bereikt, en velen van ons vinden dat de juiste manier van werken.

Maar wat te doen als algemene methoden niet een antwoord geven? Ik ken gevallen waar de algemene aanpak leek te falen, maar waar concrete informatie in de vorm van voorbeelden ons liet zien hoe het probleem wel op te lossen is.

Andrew Wiles zegt in een beschrijving van zijn zoektocht naar een bewijs van de Laatste Stelling van Fermat: "Perhaps I could best describe my experience of doing mathematics in terms of entering a dark mansion. One goes into the first room, and it's dark, completely dark. One stumbles around bumping into the furniture, and gradually, you learn where each piece of furniture is, and finally, after six months or so, you find the light switch. You turn it on, and suddenly, it's all illuminated. You can see exactly where you were."

Dit boek geeft een voorbeeld hoe je verder kunt gaan als algemene methoden niet lijken te werken: doorrekenen van speciale gevallen, voorbeelden maken, verschillende technieken combineren. Toepassingen in de coderingstheorie zijn in dit geval het resultaat. Maar ik vraag me af of we wel de goede vragen stellen in het probleem van aantallen rationale punten over een eindig lichaam.

Ook hebben we in het verleden gezien dat methoden uit het ene vakgebied soms een verrassend inzicht geven in een andere tak van wiskunde. De manier waarop Weil de Lefschetz dekpuntenstelling gebruikte als bron van inspiratie is daar een voorbeeld van. Een ander voorbeeld is het inzicht dat Deligne kreeg bij het lezen van een artikel van Rankin: het bleek de sleutel te geven voor het vinden van een bewijs van de Weil-vermoedens.

In een prachtig interview met Elisa Lorenzo García en Christophe Ritzenthaler vertelt Serre hoe het vergelijken van de discriminant $\mathrm{discr}(K/\mathbb{Q})$ en de graad $[K:\mathbb{Q}]$ van een algebraïsch getallenlichaam K leidt tot interessante beschouwingen (en hoe Serre en Hendrik Lenstra daar een interessante briefwisseling over hebben: maak K met kleine discriminant en grote graad); er is een analogie met geslacht — aantal rationale punten op een algebraïsche kromme over een eindig lichaam. Dit was een van de motivaties om aan dit onderwerp te gaan werken; voor een uitleg zie Remark 5.3.1 van het boek.

Conclusie. Een prachtig boek. Het plezier in wiskundebeoefening straalt je tegemoet. Een bron van inspiratie. *Frans Oort*

Jan Guichelaar, Paul Levrie, Roosmarij Vanhommerig

De dikke pythagoras

Lannoo, 2020
304 p., prijs € 19,99
ISBN 9789401471831

Zoals u op de foto rechtsonder ziet, liggen diverse jaargangen vanaf het begin van de jaren zestig op tafel. De eerste twee jaargangen ontbreken. De derde jaargang komt overeen met het jaar dat ik in de derde klas zat van de hbs. Dat was het schooljaar 1963–64. Vanaf die tijd heb ik het redelijk compleet. Hier en daar ontbreekt een nummer. Van sommige bezit ik meerdere exemplaren.

Wat opvalt is dat de zevende jaargang geheel oranje gekleurd is. Waarom? Ik weet het niet. Als leerling heb ik geworsteld, soms nu nog, met de opgaven in *Pythagoras*, als wiskunde-natuurkundestudent begon ik het belang van het tijdschrift in te zien en werd ik gebiologeerd door een artikel waarin een schaakbord binnenstebuiten (inversie) wordt gekeerd. *Pythagoras* heb ik tijdens mijn werk als docent ervaren als een grote rijkdom. Ik heb er vaak opgaven voor mijn lessen of testen uitgehaald. Het tijdschrift, met lezers en auteurs zowel in Nederland als België, bestaat zestig jaar zoals u waarschijnlijk weet. De redactie van nu laat ons weten dat zestig voor hen belangrijker is dan vijftig. Waarom? Het oude Babylonië (rond 3000 v. Chr.) wordt beschouwd als de geboorteplaats van de wiskunde en de Babyloniërs gebruiken een talstelsel op basis van 60. Ondertussen zijn er al meer dan 360 nummers van het tijdschrift uitgebracht. Toch was 2011 ook een mijlpaal, ter gelegenheid waarvan het boek *De Pythagoras Code* werd uitgebracht. Dit boek werd al een schatkamer genoemd. Denkertjes, puzzels, spellen, maar ook de nodige artikelen over geschiedenis van de wiskunde, meetkunde, getallen en op het eind van het boek de oplossingen.

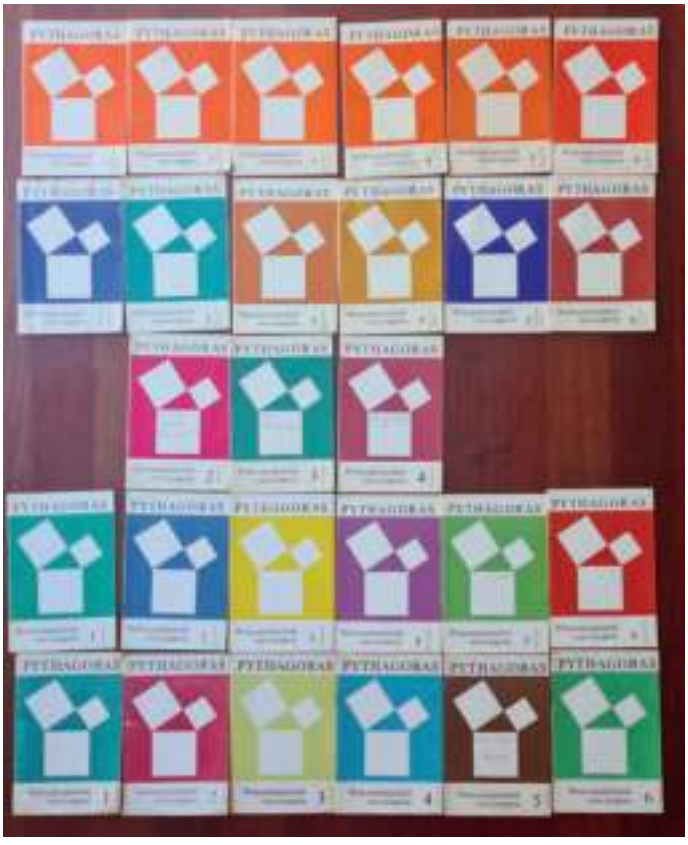
Vergeleken met de speciale uitgave uit 2011 is *De dikke pythagoras*, 303 pagina's rijk, sowieso fysiek van een ander formaat maar ook van een andere opzet. Foto's zul je er niet in aantreffen, maar wel grappige, gekleurde tekeningen. Ook dit boek bevat geen echte artikelen, maar naast de talloze puzzels en problemen (601) — net als in *Pythagoras* wordt de moeilijkheidsgraad met 1, 2 of 3 bolletjes aangegeven — heel veel 'Wist je dit' of 'Wist je dat' wiskundige weetjes. Er wordt dan een probleem uit de doeken gedaan waarvan niet altijd de oplossing wordt gegeven. Dat zet aan tot echt denken en puzzelen. Overigens van veel problemen — meetkundig van aard, bord-roosterpuzzels, getal- en rekenpuzzels, verdeelproblemen, kans- en telproblemen, logische problemen — staan de oplossingen achterin, deel 2 van het boek. Liefst 87 pagina's zijn er voor uitgetrokken. Vaak zijn de uitwerkingen van een tekening voorzien. Ook wordt jaargang en nummer van de *Pythagoras* vermeld waar de opgave vandaan komt. De naam van de ontwerper van een opgave wordt niet genoemd. In die zestig jaar is er een keur van redacteuren en (vaste) medewerkers aan de slag gegaan. Op pagina 9, en dat schrijven we als $-1+12-2$, staat een trots overzicht. U zult er heel wat bekende namen aantreffen, zoals van een van de oprichters Bruno Ernst (pseudoniem van Hans de Rijk), auteur van heel veel wiskundeboeken en artikelen. Hij schreef ruim 250 werken. Een bekende uitspraak van hem is: "Ik weet niets maar ben nieuwsgierig naar alles." Ik beschouw het als een van de fundamenten van dit tijdschrift.

Hier een greep van drie puzzels in bolletjesvolgorde. Voor elk wat wils. We beginnen met opgave (136) die van één bolletje is voorzien. "Boer Japiks fokte kippen met vreemdsoortige eieren, soms met 1 dooier, soms met 2 dooiers en dan weer zonder dooier. Boer Japiks hield hiervan een boekhouding bij, maar na het 5000ste ei raakte hij zijn gegevens kwijt. Hij herinnerde zich alleen nog dat de meeste van de eieren slechts 1 dooier bevatten en precies de helft van de resterende eieren 2 dooiers had. Hoeveel dooiers zaten er in totaal in deze 5000 eieren?"

De auteurs schrijven in de inleiding dat de *éénbolletjesopgaven* met gezond verstand en eenvoudig rekenwerk op te lossen zijn. Ik zou zelf willen toevoegen: "Eerst heel goed lezen en dan een schetsje maken."

Kijken we naar pagina 60, het wordt genoteerd als $(1+1+2)*((2+3)*3$, dan zien we in opgave 140, een *tweebolletjesopgave*, het 'Zes Gelijke Gebieden probleem'. Jawel, het getal 6 speelt weer een rol. Bij dit soort opgave kan wiskundekennis uit de onderbouw nodig zijn. Je moet een driehoek tekenen met zijn drie zwaartelijnen. Er wordt meegedeeld dat de zwaartelijnen door één punt gaan (kennis onderbouw). Er staat een tekening van de driehoek bij. Ik noem de driehoek: $\triangle ABC$. De drie zwaartelijnen verdelen $\triangle ABC$ in zes kleinere driehoeken. Je moet nu aantonen dat de zes driehoeken dezelfde oppervlakte hebben. Achter in het boek staat een uitwerking met tekening. Soms zou je willen dat er meer strategieën worden gegeven. Maar misschien moet dat toch maar de taak van de docent blijven.

Op pagina 206 $(=(11-2)\times 23\times(-3+4))$ hebben we een van de *driebolletjesopgaven*. Volgens de auteurs vergt zo'n opgave



goed inzicht en denk- en/of puzzelwerk. Maar ook wiskunde uit de bovenbouw. De titel van opgave 577 luidt: 'Allemaal vierkanten'. Het gaat om een serie steeds kleiner wordende vierkanten die op eenzelfde basislijn staan. Het grootste vierkant heeft zijde 1. Als je naar rechts gaat, is elk vierkant half zo hoog als het vorige. De linkeronderhoek ligt steeds op twee derde deel van de onderzijde van het vorige vierkant. Bepaal de totale oppervlakte van het gebied dat door de vierkanten wordt bedekt.

De opgave komt uit een *Pythagoras* van februari 2017. Het gaat om nummer 4 van de 56ste jaargang. Er is in dat nummer een mooie afbeelding toegevoegd. Je ziet zeven verschillend gekleurde vierkanten. In het boek moeten we het doen met één kleur en zes vierkanten, maar de afbeelding is veel groter. Ook de hoekpunten rechtsboven van de vierkanten zijn met een stippellijn verbonden. En dat maakt een verschil. Dat ziet u zo.

Op pagina 73 vind je een van de aardigste puzzels van 'Wist je dat'. Het 'Probleem van Leuven' verscheen in 1914, het beginjaar van de Eerste Wereldoorlog en wel in het Britse tijdschrift *The Strand*. Dat magazine kreeg bekendheid door de publicatie van de verhalen van Sherlock Holmes. Van zijn detectivewerk is ook veel verfilmd. Maar nu het huisnummerprobleem. De tekst luidt als volgt: "'I was talking the other day,' said William Rogers to the other villagers gathered round the inn fire, 'to a gentleman about that place called Louvain, what the Germans have burnt down. He said he knowed it well — used to visit a Belgian friend there. He said the house of his friend was in a long street, numbered on his side one, two, three, and so on, and that all the numbers on one side of him added up exactly the same as all the numbers on the other side of him. Funny thing that! He said he knew there was more than fifty houses on that side of the street, but not so many as five hundred. I made mention of the matter to our parson, and he took a pensil and worked out the number of the house where the Belgian lived. I don't know how he done it.' Perhaps the reader may like to discover the number of that house."

Dit is een probleem waarbij de meeste leerlingen halverwege zullen stagneren. Maar is dat erg? Mag er geworsteld worden? Met wat gereken met rekenkundige rijen kom je wel bij de oplossing, maar een sluitend bewijs vinden is niet zo simpel. Bij deze opgave is achterin het boek geen uitwerking te vinden. Is dat erg? Natuurlijk niet, maar het zou toch heel leuk zijn als de lezer zijn of haar pogingen zou doorsturen naar de redactie. Het zou weer een mooi artikel kunnen opleveren.

Het is niet geheel duidelijk voor wie dit boek geschreven is. In het voorwoord richt men zich niet meteen tot de leerling. De leraar functioneert nu als intermediair. Sommige opgaven zouden in een college 'Probleem Oplossen' of bij 'Wiskundige Denkactiviteiten' goede diensten kunnen bewijzen. Er zijn veel puzzels met verschillenden oplossingsstrategieën. En dat maakt het zo boeiend. Je lost het op en ziet achteraf een elegantere aanpak. Dat noem ik winst en rijkdom. Maar sommige aanpakken staan ver weg van de leerling. Jammer dat je niet echte leerlingenuitwerkingen ziet. Al waren er maar een paar van afgedrukt. Kwam ik bij dit boek doorwerken omissies tegen? Op bladzijde 115 moeten acht koninginnen op het schaakbord staan. Die staan er ook, maar vier ervan zijn op het zwarte vlakje nauwelijks te zien! Op pagina 155 onderaan moet staan 'Wist je dat 4 april(4–4), enz.'

Ten slotte wil ik nog even de verdienste vermelden van Matthijs Wielders, oud-docent van de Open Universiteit, met wie ik de ervaringen van het maken van diverse opgaven heb uitgewisseld. *De dikke pythagoras* hoort sowieso in de mediatheek van een school maar hoort ook in de boekenkast van elke wiskundedocent naast *De Pythagoras Code* te staan. Naast dit boek zou ook een bundeling van de zestig interessantste artikelen en de zestig mooiste of opvallendste uitwerkingen van leerlingen uit de ruim 360 nummers niet misstaan. *Jacques Jansen*

Peter Scholze, Jared Weinstein

Berkeley Lectures on p-adic Geometry

Princeton University Press, 2020
x + 250 p., prijs $75.00
ISBN 9780691202082

Dit boek is gebaseerd op een college dat Scholze — toen 26 jaar oud — in het najaar van 2014 gaf in Berkeley. Het onderwerp was p-adische meetkunde. Dit speelt een grote rol in de aritmetische meetkunde omdat het de brug slaat tussen meetkunde over lichamen van karakteristiek 0 en van karakteristiek p. Er is dan ook een lange lijst met belangrijke resultaten waarin p-adische meetkunde een rol speelt.

Twee jaar eerder was Scholzes zeer invloedrijke artikel over perfectoïde ruimten verschenen. Je zou kunnen denken dat zijn college in Berkeley gewijd was aan een uitleg van die moeilijke theorie. Niet dus. Een van de fascinerende aspecten van Scholzes werk is dat hij bezig is met een groot programma en dat hij het vermogen heeft om zich, ondanks de soms meer dan formidabele technische obstakels, met mokerslagen een weg vooruit te banen. Het hoofdthema van dit boek is niet de theorie van perfectoïde ruimten maar een wezenlijke uitbreiding daarvan, die gaat over zogenoemde 'diamonds'. Kort gezegd zijn dergelijke diamanten quotiënten van perfectoïde ruimten onder equivalentierelaties, ongeveer zoals algebraïsche ruimten quotiënten zijn van schema's.

Deze theorie is niet ontwikkeld om er maar een beetje op los te generaliseren maar met een helder doel. Een van de spraakmakende ontwikkelingen van de laatste jaren is een door Fargues en Fontaine ontwikkelde totaal nieuwe visie op p-adische Hodgetheorie en de daarop gebaseerde 'geometrisatie' van het lokale Langlandsvermoeden door Fargues en Scholze. Het komt erop neer dat resultaten uit de p-adische Hodgetheorie, die voorheen gebaseerd waren op Fontaines 'periodenringen' (die niet erg intuïtief zijn), nu geïnterpreteerd kunnen worden als uitspraken over vectorbundels op een kromme — de 'Fargues–Fontaine-kromme', soms gewoon 'la courbe' genoemd. De grote winst is hier vooral dat dingen veel conceptueler worden gemaakt. Bovendien blijken ideeën te kunnen worden overgenomen uit het bewijs van het locale Langlandsvermoeden in karakteristiek p (V. Drinfeld, L. Lafforgue) en uit het meetkundige Langlandsprogramma. Voorlopig hoogtepunt hierin is het recente werk van Fargues en Scholze, dat voor willekeurige reductieve groepen over p-adische locale lichamen een zeer conceptuele meetkundige manier geeft om aan gladde irreducibele representaties L-parameters te associëren.

De interpretatie van ‘la courbe’ als een diamant speelt hierin een belangrijke rol.

Prachtige wiskunde, en het einde van al deze ontwikkelingen is nog lang niet in zicht. Het is wel verschrikkelijk technisch allemaal en wie bij wil blijven heeft al snel een enorme stapel literatuur op zijn bureau liggen. (Alleen al Fargues–Fontaine en Fargues–Scholze is zo’n 750 pagina’s.) Fijn dus wel dat er ‘lecture notes’ zijn waar je een begin mee kan maken. Deze Berkeley Lectures zijn uitgewerkt door Scholze samen met Jared Weinstein. De stijl is meer die van ‘lecture notes’ dan die van een definitieve tekst, en voor preciezere technische details is een andere tekst van Scholze (weer 165 pagina’s erbij…) de aangewezen bron. De lezer wordt in hoog tempo door de theorie geloodst maar door de grote nadruk op de intuïtie en motivatie is dit boek een heel nuttige toevoeging aan de literatuur. Als preprint was deze tekst al langer beschikbaar maar juist in een veld dat zich explosief ontwikkelt is het fijn om ook in boekvorm wat steunpunten te hebben op de steile weg omhoog.

Ben Moonen

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.

Edward van de Vendel, Ionica Smeets

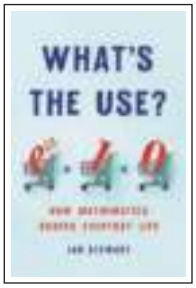
Rekenen voor je leven

Uitgeverij Nieuwezijds, 2021
ISBN 9789057125188
nieuwezijds.nl/boek/rekenenvoorjeleven

Ananyo Bhattacharya

The Man from the Future
The Visionary Life of John von Neumann

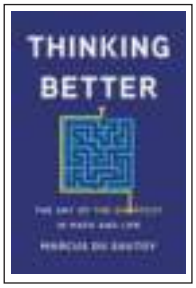
Penguin books, Imprint Allen Lane, 2021
ISBN 9780241398852
penguin.co.uk/books/313/313705/the-man-from-the-future/9780241398852.html



Ian Stewart

What’s the Use?
How Mathematics Shapes Everyday Life

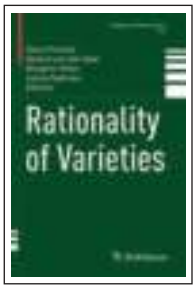
Basic Books, 2021
ISBN 9781541699489
basicbooks.com/titles/9781541699489



Marcus Du Sautoy

Thinking Better
The Art of the Shortcut in Math and Life

Basic Books, 2021
ISBN 9781541600362
basicbooks.com/titles/9781541600362



Gavril Farkas, Gerard van der Geer, Mingmin Shen, Lenny Taelman

Rationality of Varieties

Birkhäuser, 2021
ISBN 9783030754204
springer.com/978-3-030-75420-4

Mario Gerwig

Der Satz des Pythagoras in 365 Beweisen

Springer, 2021
ISBN 9783662628850
springer.com/978-3-662-62885-0

Stephen Budiansky

Journey to the Edge of Reason
The life of Kurt Gödel

W. W. Norton & Company, 2021
ISBN 9781324005445
wwnorton.com/books/9781324005445

David J. Hand

Dark Data
Why What You Don’t Know Matters

Princeton University Press, 2022
ISBN 9780691234465
press.princeton.edu/books/paperback/9780691234465/dark-data