Wiskunde in de laatste zestig jaar: exponentiële groei en structurele vernieuwing

Tom H. Koornwinder

Korteweg-de Vries Instituut, Universiteit van Amsterdam, thk@science.uva.nl

1 Inleiding

Bij veel niet ingewijden heerst de mening dat de wiskunde af is. Men is verbaasd te horen dat professionele wiskundigen een deel van hun werktijd besteden aan onderzoek naar nieuwe zaken, zoals het formuleren en bewijzen van nieuwe stellingen. Deze misvatting is niet zo verwonderlijk. Vergelijk de publiciteit die sterrenkunde, natuurkunde en DNA-gerelateerd onderzoek in de wetenschapsbijlagen van de kranten krijgen met de aandacht voor de wiskunde. Wel heeft de krantenlezer rond 1993 uitgebreid kunnen lezen over de laatste stelling van Fermat. Ook nieuwe records bij het uitrekenen van de decimalen van π en bij factorisatie van grote getallen bereiken de krant. Maar het overgrote deel van de nieuwe wiskunde klinkt niet door, en is vaak ook inderdaad moeilijk in begrijpelijke vorm aan de leek te presenteren. Wat dat betreft hebben de wiskundigen het met hun abstracte materiaal, dat bovendien sterk voortbouwt op eerdere resultaten, veel moeilijker dan hun collega's in de natuurwetenschappen.

Uiteraard kampte de schrijver van dit hoofdstuk ook met bovengenoemde problemen. Om de lezer gevoel bij te brengen van het belang van nieuwe wiskundige ontwikkelingen, moeten de betreffende begrippen eigenlijk tot in enig technisch detail worden uitgelegd. Dan kom je al gauw tot een omvang van honderden i.p.v. 20 pagina's. Ik heb er daarom voor gekozen om veel aandacht te besteden aan anderssoortige aspecten van de nieuwe wiskundige ontwikkelingen: trends en nieuwe werkvormen. Voor één onderwerp, Lie-theorie, heb ik een wat langere lijn gemaakt om de dynamiek van de (vooral zuivere) wiskunde te illustreren, waarbij steeds verdergaande verbanden tussen deelgebieden van wiskunde worden gelegd, en waarbij nieuwe ideeën zoals quantisatie en deformatie over een breed front en gedurende lange tijd richtinggevend kunnen zijn.

2 Groei van de wiskunde

Voor een betere indruk van de groei van de wiskunde zal ik nu enige indicatoren van groei bespreken, nl. de groei van het aantal deelgebieden, van het aantal publicaties per jaar, en van het aantal tijdschriften. Een belangrijke bron voor dit soort gegevens zijn de reviewtijdschriften

c.q. databases *Mathematical Reviews / MathSciNet*[1] en *Zentralblatt für Mathematik*[2]. Beide pretenderen een tamelijk overdekkende documentatie van alle verschijnende wiskundepublicaties te geven.

2.1 Groei van het aantal deelgebieden

Het is interessant om de opdeling in vakgebieden in 1945 en in 2000, zoals gehanteerd door Math. Reviews, met elkaar te vergelijken. In 1945 zijn er 12 hoofdonderwerpen, waarvan een paar nog licht vertakt zijn. Dit betreft vooral de analyse, waarbinnen 17 deelgebieden worden onderscheiden.

In 2000 is het aantal onderwerpen op het eerste classificatieniveau gegroeid tot 62 (er zijn nog twee niveaus onder). Van deze 62 staan er 13 op zichzelf. De overige 49 kunnen gegroepeerd worden in 5 hoofdgebieden: algebra (12 onderwerpen), analyse (19), meetkunde (7), stochastiek (2), mathematische fysica (10). In de vergelijking tussen 1945 en 2000 valt direct op dat in de traditionele drie hoofdgebieden van zuivere wiskunde de algebra en meetkunde in 2000 meer zijn opgedeeld en de analyse in dit opzicht tamelijk constant is gebleven. Volledig nieuwe vakken sinds 1945 bij de algebra zijn categorie-theorie en K-theorie.

In de meer toegepaste gebieden is het cluster mathematische fysica flink gegroeid. Uiteraard zijn er nieuwe gebieden gerelateerd aan de computer: computer science en information & communication. Toch doet het aantal clusters of rubrieken waarbij al in de naam een toepassing wordt genoemd, geen recht aan het hedendaagse aandeel van toegepaste wiskunde in de totale wiskunde. In feite bevatten veel onderdelen van analyse (zoals gewone en partiële differentiaalvergelijkingen), van de combinatoriek (i.e. discrete wiskunde), maar ook van de getaltheorie een groot aandeel toegepaste wiskunde.

2.2 Discussie van de relatieve groei van deelgebieden

De genoemde verschuivingen in aantallen deelgebieden van analyse, algebra, meetkunde en toegepaste wiskunde geven een zekere indicatie van de daadwerkelijke relatieve verschuivingen in onderzoeksactiviteit binnen de hoofdgebieden. De vraag naar een verklaring komt dan op. Wat de analyse betreft, dit hoofdgebied stond al sinds Newton veruit nummer 1. Het is moeilijk om zo'n eeuwenlange voorsprong altijd vol te houden. Sinds de wiskunde in de tweede helft van de negentiende eeuw een grote sprong voorwaarts maakte in gestrengheid, heeft de analyse zich sneller uitgekristalliseerd dan algebra en meetkunde. Daardoor was de dynamiek van algebra en meetkunde in de laatste decennia groter. Aanvankelijk na 1945 was de verwerking van de methodes uit de functionaalanalyse, en zeker ook de distributietheorie, een krachtige motor voor de analyse in zijn geheel, en ook voor de theorie van de Lie-groepen (continue symmetriegroepen) en voor de mathematische fysica. Vanaf eind jaren zeventig werden de impulsen uit algebra

[1] `http://www.ams.org/mathscinet`
[2] `http://www.emis.de/ZMATH`

en meetkunde echter krachtiger, vooral in de mathematische fysica, en ging ook omgekeerd de natuurkunde nieuwe ideeën leveren aan de algebra en vooral de meetkunde.

Algemener kan gesteld worden dat doorbraken in de wiskunde van de laatste decennia, meer dan eerder in de twintigste eeuw, tot stand kwamen door combinatie van ideeën en technieken uit verschillende hoofdgebieden. Bijv. gebruikte Andrew Wiles in zijn bewijs van het Vermoeden van Fermat (de laatste stelling van Fermat), wat een getaltheoretisch resultaat is, technieken uit algebra, meetkunde en analyse. Dit maakt de vraag in welk hoofdgebied de meeste activiteit is minder relevant: het gaat om het samengaan van twee of meer hoofdgebieden.

Wat de toegepaste wiskunde betreft, bij Newton en nog lang daarna was toegepaste wiskunde eigenlijk toegepaste analyse en was er geen echt onderscheid tussen zuivere en toegepaste analyse. De toepassingen liepen vooral via lineaire differentiaalvergelijkingen. De enorme hoeveelheid toepassingen van anderssoortige wiskunde heeft zich pas goed sinds de tweede wereldoorlog doorgezet. De spectaculaire groei van de toegepaste wiskunde had zijn start ongetwijfeld vanwege deze oorlog, toen alle expertise, dus ook die uit de wiskunde, werd aangegrepen om de oorlogsinspanningen te ondersteunen. De grote successen hierbij werden natuurlijk niet onmiddellijk na de oorlog vergeten. Men ging de expertise opnieuw inzetten ten behoeve van het economisch herstel na de oorlog en ten behoeve van de wapenwedloop vanwege de koude oorlog. Meer geld en meer faciliteiten voor toegepaste wiskunde leidden ook tot meer output van toegepaste wiskunde. Maar tegelijk was er ook bij een deel van de wiskundigen een sterkere motivatie om toepassingsgericht werk te doen.

Een verdere trend is de relatieve groei van de discrete wiskunde t.o.v. de continue wiskunde. De overgang van continu naar discreet is ook sterk waarneembaar in de ontwikkeling van de techniek en daardoor in de hele maatschappij. Al lang geleden gingen we van rekenlineaal naar zakjapanner over. Onze oude vaste telefoon was een continu apparaat, de mobiele telefoon is discreet. Displays gaan steeds meer over van wijzers naar digitale aanduiding. Thans breekt de digitale televisie door. De digitale computer is al lang een aanjager van deze ontwikkeling. Omdat zijn input en output digitaal zijn, ligt het voor de hand om de input ook discreet voor te bereiden en de output discreet te verwerken in plaats van een vertaalslag tussen discreet en continu te maken. De informatica, als wetenschap die de processen in de computer bestudeert en de programmatuur ontwikkelt, is van nature discreet. Binnen de wiskunde betekent de discretisering terreinverlies voor de analyse en de meetkunde, beide typisch continue vakken, en terreinwinst voor de algebra, een discreet vak. Toch loopt dit niet zo'n vaart omdat de ideeën uit de analyse en de meetkunde ook in discrete en eindige context gebruikt kunnen worden. Eindige meetkunde is een erkend vakgebied. Op grafen kan men heel goed analyse bedrijven. In feite is het heen en weer gaan tussen continu en discreet al een oude gewoonte in de analyse. Weerbarstige oneindige sommaties benadert men met integralen om de krachtige technieken van de integraalrekening te kunnen gebruiken. Omgekeerd benadert men integralen numeriek door ze te vervangen door eindige sommaties.

2.3 Groei van het aantal artikelen

Een kwantitatieve indruk van de groei van de wiskunde kan men krijgen uit het aantal publicaties dat per jaar vermeld wordt in MathSciNet. Hierbij wordt voor het gemak alles geteld waar autersnamen aan verbonden zijn, dus ook boeken en overzichtsartikelen. Via andere bronnen, zoals het nu electronisch toegankelijk gemaakte *Jahrbuch der Mathematik*[3] kan men een indruk krijgen van de wiskundeproductie in de 19e eeuw en de eerste decennia van de 20e eeuw. Twee auteurs, Odlyzko [13] en Grossman [7], zich beiden baserend op gegevens van Math. Reviews, geven schattingen van het aantal wiskundepublicaties per jaar, zoals zich dat in de laatste decennia ontwikkelde. Odlyzko gaat zelfs terug tot 1870, in welk jaar er ca. 840 wiskundepublicaties waren. In 2000 waren er ca. 55000 publicaties. De groei van het aantal publicaties per jaar in deze periode van 130 jaar was niet gelijkmatig. Sinds 1945 is de groei sterk toegenomen. Gedurende enige decennia was er zelfs een verdubbeling van het aantal publicaties in elke tien jaar. Sinds ca. 1985 is de groei minder sterk. De gegevens worden echter vertroebeld omdat Math. Reviews minder artikelen is gaan verwerken uit bezuinigingsoverwegingen.

Odlyzko [13] schatte in 1994 dat het aantal ooit tot dan gepubliceerde wiskundepublicaties ca. 1 miljoen bedroeg. Dat zouden er dan nu al anderhalf miljoen zijn. Mogelijk 90% van de totale menselijke wiskundeproductie verscheen na 1945. In het hypothetische geval van constante groei van het aantal publicaties (thans niet meer geldig) geldt er dat er in het aantal jaren van de verdubbelingsperiode, zeg 10 jaar, evenveel gepubliceerd wordt als in alle jaren daarvoor.

Een interessant fenomeen is de toenemende samenwerking in het wiskunde-onderzoek, wat zich laat aflezen aan het percentuele aantal publicaties met meer dan 1 auteur, zie [7]. In de jaren '40 had slechts 9% van de publicaties meer dan 1 auteur, in de jaren '90 is dit 46% geworden: 33% met 2 auteurs, 10% met 3 auteurs en 3% met meer dan 3 auteurs.

Is er een verklaring voor deze laatste ontwikkeling? Een hoe gaat zo'n samenwerking die leidt tot een artikel met meer dan één auteur? Een deel van de verklaring is dat de verschaffers van onderzoeksgelden de experimentele natuurwetenschappen namen als meest succesvolle voorbeeld van hoe een wetenschap zich kan ontwikkelen, en dat als norm stelden voor andere wetenschappen: de theoretische bèta-wetenschappen, maar ook de sociale en geesteswetenschappen. Terwijl bij een experimentele natuurwetenschap de omvang van het experiment op een natuurlijke wijze het aantal hierbij betrokken onderzoekers bepaalt, werden voor de theoretische wetenschappen financiële prikkels ingebouwd die het samenwerken stimuleerden.

Er is echter ook een meer positieve verklaring. Samenwerking bij wiskundig onderzoek kan echt helpen om verder te komen. Verschillende expertise die bij elkaar gebracht wordt kan tot een nieuw inzicht leiden. Zulke contacten worden in toenemende mate gefaciliteerd door internationale instituten die of vele korte conferenties organiseren of wat langere gefocuste programma's met geselecteerde deelnemers hebben.

Het uiteindelijke schrijven van het artikel bij meer auteurs kan zich op allerlei manieren voltrekken. Vaak schrijft een van de auteurs een eerste versie, dan wordt deze door een medeauteur becommentarieerd en bewerkt, etc. Soms neemt ieder van de auteurs een deel van het artikel

[3] `http://www.emis.ams.org/projects/JFM`

voor zijn rekening, overeenkomend met elks expertise.

2.4 Andere vormen van groei

Het aantal publicerende wiskundigen bedroeg ca. 10 000 in de jaren '40, 50 000 in de jaren '60 en 200 000 in de jaren '90, zie [7]. Ook hier eerst een verdubbeling in minder dan 10 jaar en later een afzwakking van de groei. Ik verwacht dat het aantal wiskundigen in de westerse wereld zich zal stabiliseren of zelfs zal teruglopen gezien het geringe aantal studenten. Wereldwijd is er misschien voorlopig nog een stijging gezien het enorme potentieel van China en andere landen in de derde wereld.

Het aantal wiskundetijdschriften is sinds 1945 sterk gegroeid. Terwijl de oudere tijdschriften meestal algemeen wiskundig waren, zijn de meeste nieuwere tijdschriften gespecialiseerd op een deelgebied. Sinds 1995 verandert de tijdschriftensituatie ingrijpend, enerzijds doordat bibliotheken de abonnementsprijzen niet meer kunnen opbrengen (serials crisis), anderzijds door de technologische ontwikkelingen, waardoor tijdschriften nu via het web toegankelijk kunnen worden gemaakt. Dit heeft geleid tot nieuwe gratis of goedkope electronische tijdschriften. Er is nog veel dynamiek en onzekerheid in de verdere ontwikkeling van de wetenschappelijke tijdschriftenmarkt

3 Nieuwe wiskunde rond 1945

Tijdens de tweede wereldoorlog recruteerden de oorlog voerende partijen veel wetenschappers, waaronder wiskundigen, voor onderzoek dat de oorlogsinspanningen moest ondersteunen. Vooral het militaire onderzoek in de US en Engeland leidde tot nieuwe takken van wiskunde:

- De *operations research* werd ontwikkeld om de logistiek van de massale militaire operaties efficiënter te maken.
- *Control theory* was nodig i.v.m. geleide projectielen.
- Veel militaire zaken (bijv. de ontwikkeling van de atoombom) gaven aanleiding tot grootschalig rekenen, dat nauwelijks meer te doen was met de klassieke tafelrekenmachines. Dit gaf een krachtige impuls tot de ontwikkeling van de *digitale computer*.

De reeds bestaande gebieden *mathematische statistiek* en *cryptografie* kregen in de oorlog een grote stimulans.

Sommige nieuwe richtingen onstonden tijdens of kort na de oorlog, maar tamelijk onafhankelijk van de oorlogsinspanningen. Ik noem de *speltheorie*, die ontstond met het invloedrijke boek *Theory of games and economic behavior* van von Neumann en Morgenstern, en de *informatietheorie* (Shannon, 1948). In de zuivere wiskunde ontwikkelde Laurent Schwartz [15] de *distributietheorie* (1944–1945).

4 Een momentopname: het ICM 1954 te Amsterdam

Het ICM[4] (*International Congress of Mathematicians*) wordt eens in de vier jaar gehouden. Op het tweede congres in die serie, in 1900 in Parijs, presenteerde Hilbert zijn beroemde lijst van open problemen. Sinds 1936 worden er *Fields medals*[5] op deze congressen uitgereikt, twee tot vier per keer, aan wiskundigen jonger dan 40 jaar. Zij worden wel beschouwd als het equivalent voor de wiskunde van de Nobelprijs, maar de vereiste jonge leeftijd en de betrekkelijk snelle toekenning na het verkrijgen van de wetenschappelijke resultaten zijn natuurlijk zeer verschillend van de gang van zaken bij de Nobelprijzen.

In 1954 viel Nederland de eer te beurt om het ICM te organiseren. Het werd in Amsterdam gehouden. Volgens oudere Nederlandse wiskundigen die (toen jong) aan het congres deelnamen en bij de organisatie waren betrokken, was dit een zeer geslaagd congres, niet in het minst voor de Nederlandse wiskunde. De organisatie ging met veel elan gepaard. Zeer vele jonge Nederlandse wiskundigen kregen een grotere of kleinere taak toebedeeld.

Het is interessant om in de Proceedings van het congres sommige voordrachten na te lezen. Allereerst is er de openingsvoordracht van congresvoorzitter J. A. Schouten in het Amsterdamse Concertgebouw. Hij sprak in het perspectief van de nog vers in het geheugen liggende tweede wereldoorlog en de wederopbouw, maar veel van zijn woorden zijn thans nog verwonderlijk actueel. Hij zei dat "het nu absoluut duidelijk was dat de plaats van de wiskunde in de wereld volledig veranderd is na WO2. Veel wiskunde van allerlei aard, van de eenvoudigste schoolrekenkunde tot de hoogst ontwikkelde theoretische onderdelen, is nodig in de moderne maatschappij, in oorlog en in vrede. De voorspelling van Felix Klein is uitgekomen dat alle zuivere wiskunde vroeg of laat een practische toepassing vindt." (En hoeveel meer is dat nu, weer 50 jaar verder, uitgekomen.) Schouten betreurde het dat de intuïtieve kant van de wiskunde bij het onderwijs minder nadruk krijgt dan de formele, logische kant, waardoor de scholieren worden afgestoten.

De organisatie van dit ICM in Amsterdam spoorde ook goed met de ontwikkeling die in Nederland in gang was gezet met de oprichting van het Mathematisch Centrum (thans CWI) in Amsterdam in 1946. Een opkomend besef van het maatschappelijk belang van (toegepaste) wiskunde en van *wiskundig modelleren* (zie Alberts [1]) had mede tot deze oprichting geleid.

Van Dantzig, chef van de afdeling Statistiek van het Mathematisch Centrum, hield een plenaire voordracht over *Mathematical problems raised by the flood disaster 1953*. Deze watersnoodsramp van een jaar tevoren had aanleiding gegeven tot onderzoeksopdrachten aan het Mathematisch Centrum, welke de wetenschappelijke basis zouden leggen voor de Deltawerken. De onderzoeksvragen waren van drieërlei aard: statistisch, besliskundig en toegepast analytisch.

J. von Neumann hield een plenaire voordracht over *Unsolved problems in mathematics*. De organisatoren hadden gehoopt op een lezing vergelijkbaar met die van Hilbert in 1900. Uiteindelijk concentreerde von Neumann zich op de betekenis van operator-algebra's voor quantummechanica, logica en waarschijnlijkheidsrekening.

Ter gelegenheid van het congres werd er een tentoonstelling in het Stedelijk Museum te

[4] `http://www.mathunion.org/ICM/`

[5] `http://www-groups.dcs.st-and.ac.uk/~history/Societies/FieldsMedal.html`, [11]

Amsterdam georganiseerd over het grafische werk van M. C. Escher, "which shows many mathematical tendencies and is connected in a remarkable way with the mathematical way of thought". Escher was met de wiskundig aansprekende grafiek pas later in zijn carrière begonnen, en dit werk was in 1954 nog niet erg bekend. De tentoonstelling leidde tot een ontmoeting tussen de Canadese meetkundige Coxeter en Escher, en een verdere briefwisseling. Coxeter inspireerde Escher tot zijn serie van *Cirkellimieten* (vullingen van het hyperbolische vlak).

Ook de toen nog jonge Roger Penrose samen met zijn vader Lionel Penrose bezochten deze Escher-tentoonstelling en waren er diep van onder de indruk. Het inspireerde hen tot de publicatie in 1958 van een artikel over onmogelijke figuren [14] zoals de *Penrose triangle*[6] en de *Penrose stairway*[7], die vervolgens weer in het werk van Escher terugkwamen. Roger Penrose werd later ondermeer bekend bij het grote publiek door zijn *Penrose-betegelingen*[8], die veel aandacht kregen in de columns van Martin Gardner in de Scientific American.

5 Wiskunde en de computer

De computer, althans zijn niet-fysische aspecten, en de computerwetenschap (informatica, computer science) zijn kinderen van de wiskunde, inmiddels volwassen of volwassen wordend. Omgekeerd heeft de computer een enorme invloed gehad op de ontwikkeling van de wiskunde en op de wiskundebeoefening. Ik noem een paar aspecten.

Turing bedacht de *Turing-machine* als een theoretisch model voor een ideale computer. Dit model is thans werkelijkheid geworden. De meesten van ons hebben er een op hun bureau staan of dragen hem als laptop met zich mee. Er is nu een vergelijkbare ontwikkeling rond de *quantumcomputer*. Deze bestaat nog voornamelijk in theorie, afgezien van een paar primitieve implementaties. Maar men is al ver gevorderd met algoritmes voor zeer snelle berekeningen op quantumcomputers.

Von Neumann[9] was veelzijdig betrokken bij de ontwikkeling van de computer rond het eind van WO2. Zo ontwierp hij de *architectuur van de sequentiële programmeerbare digitale computer*. Hij had veel stimulerende ideeën over hoe de *numerieke wiskunde*, die al heel lang bestond voor benaderende berekeningen met de hand of met tabellen of met mechanische rekenmachines, zich kon ontwikkelen in verband met de digitale computer. Ook introduceerde hij stochastische ideeën in de numerieke wiskunde om met behulp van de "dobbelsteen" toch nog tot realistische benaderingen te komen als dat conventioneel niet mogelijk is, bijv. bij een integratie over zeer veel variabelen. Dit staat bekend als de *Monte Carlo-methode*[10] (zie ook §5.1). Ook had von Neumann een visie op de *parallelle computer*, op *neurale netwerken*, en op *computational science* (de computer gebruikt als laboratorium). Alle hier genoemde richtingen hebben sindsdien een enorme ontwikkeling doorgemaakt en zijn van een moeilijk te overschatten praktische betekenis.

[6] `http://mathworld.wolfram.com/PenroseTriangle.html`
[7] `http://mathworld.wolfram.com/PenroseStairway.html`
[8] `http://www.ams.org/featurecolumn/archive/penrose.html`
[9] `http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Von_Neumann.html`
[10] `http://www.riskglossary.com/link/monte_carlo_method.htm`

De *logica*, een aloude tak van wetenschap liggend tussen wiskunde en filosofie, vond nieuwe toepassingsgebieden in de informatica. Zelfs de *intuïtionistische wiskunde* van Brouwer kreeg hier nieuwe relevantie.

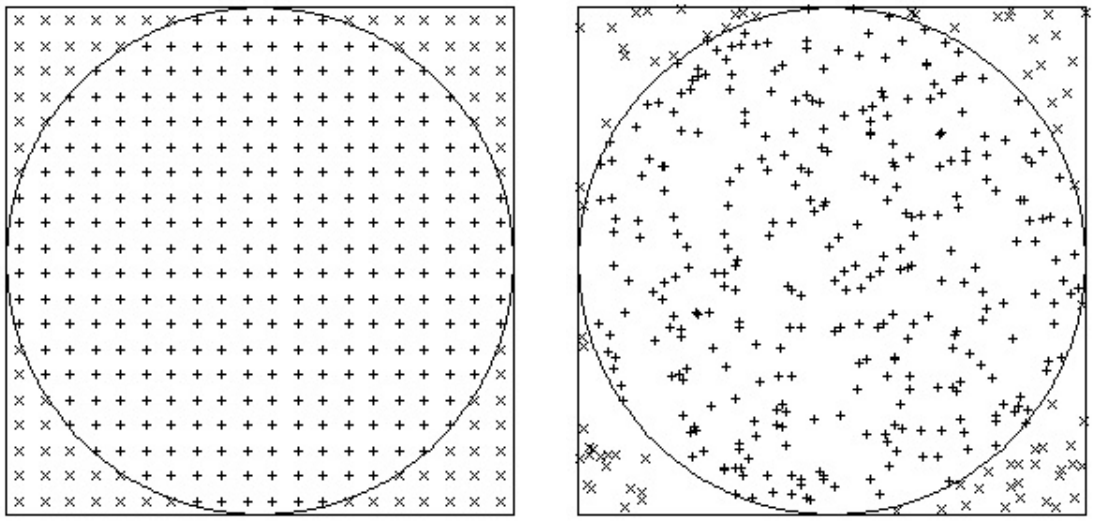
Veel zuivere wiskunde in de definitie-stelling-bewijs vorm is niet-constructief. Er wordt bijvoorbeeld wel existentie van een object bewezen, maar niet hoe het geconstrueerd kan worden. Een *algoritme* geeft een recept hoe dat wel kan. Uiteraard moet bewezen worden dat het recept goed doet wat het claimt. De *algoritmische wiskunde* heeft een enorme stimulans gekregen toen het mogelijk werd om algoritmen op de computer te implementeren. Zelfs dan, met een snelle computer, stuit men bij grotere input al snel op de grenzen van wat de computer in beperkte tijd vermag. De *complexiteitstheorie* komt hierbij in het spel: Hoe hangt de rekentijd af van de grootte van de input? Zijn er wellicht algoritmen denkbaar die dezelfde taak sneller verrichten? Zie een eenvoudig voorbeeld in §5.2.

Sommige stellingen (bijv. de vierkleuren-stelling) maken voor hun bewijs essentieel van de computer gebruik. Zulke *computer ondersteunde bewijzen* ondervonden aanvankelijk veel weerstand in de wiskundige gemeenschap. Tegenwoordig is het meer geaccepteerd. Goede documentatie en reproduceerbaarheid zijn hierbij natuurlijk van belang. Een verdergaande ontwikkeling is om een volledig bewijs van een stelling door de computer te laten leveren. Het kan om een bewijs van een reeds bekende stelling gaan, maar de computer zou ook nieuwe stellingen kunnen formuleren en bewijzen (waarbij het dan de vraag is of die stellingen interessant zijn). Zeilberger [19] schrijft dat veel stellingen in de toekomst potentieel bewezen zullen kunnen worden, maar dat hun volledige verificatie door de computer een hoge prijs in rekentijd kan hebben. Met minder rekentijd kan een bewijs tot op zekere waarschijnlijkheid gegeven worden.

Computer-algebra wil zeggen dat de computer rekent met formules i.p.v. met getallen. Net als bij numerieke wiskunde heeft men hier de drie aspecten van theorie, implementatie en complexiteitsanalyse. Sommig hedendaags wiskundig onderzoek speelt zich geheel af binnen de computer-algebra. Veel vaker, bijna standaard, gebruikt de wiskundige de computer-algebra als hulpmiddel bij het onderzoek, bijv. bij het testen van vermoedens in speciale gevallen. Als de tests positief uitvallen, dan geeft dit meer motivatie om naar een bewijs te zoeken. Zelfs zonder dat een bewijs al verkregen is, kunnen resultaten van computer ondersteund onderzoek al interessant zijn voor publicatie: de z.g. *experimentele wiskunde*. De Nederlandse Nobelprijswinnaar natuurkunde M. Veltman was een pionier op het gebied van computer-algebra met zijn programma *Schoonschip*.

5.1 De Monte Carlo methode nader bekeken

Zoals welbekend, is de oppervlakte van een cirkelschrijf met straal 1 gelijk aan π. We gaan die oppervlakte op een wat primitieve manier berekenen door de cirkel te leggen in een vierkant met zijden van lengte 2, dan in dat vierkant een regelmatig puntrooster te tekenen en te tellen hoeveel van die n punten binnen de cirkel liggen. Als dat aantal k is, dan is $\frac{k}{n}$ een benadering van $\frac{\pi}{4}$ (het oppervlak van de cirkelschijf gedeeld door het oppervlak van het vierkant). In het voorbeeld van de linker figuur is $n = 400$, $k = 316$ en de relative fout in de benadering is $0,006$.



Een andere manier om die oppervlakte te berekenen is om op een willekeurige manier n punten in het vierkant te tekenen en weer te tellen hoeveel van die punten, zeg k, binnen de cirkel liggen. In het voorbeeld van de rechter figuur is $n = 400$, $k = 322$, en $\frac{k}{n}$ benadert $\frac{\pi}{4}$ met relatieve fout $0,025$. Herhaling van dit experiment bij vaste n zou een andere k leveren, maar gemiddeld zal $\frac{k}{n}$ gelijk zijn aan $\frac{\pi}{4}$. De spreiding in de resultaten is afhankelijk van n: evenredig met $1/\sqrt{n}$. Dus om met deze methode een naar verwachting 10 keer zo goede benadering te krijgen moeten we 100 keer zoveel punten nemen.

Het mooie is dat de methode van oppervlaktebenadering met het plaatsen van willekeurige punten precies zo doorgaat voor andere figuren en in hogere dimensie. Zo kunnen we in 3 dimemsies bijv. een bal met straal 1 (inhoud $\frac{4}{3}\pi$) leggen in een kubus met ribben van lengte 2 (inhoud 8) en de verhouding tussen beide inhouden ($\frac{\pi}{6}$) benaderen met $\frac{k}{n}$, waarbij k het aantal van n willekeurig gekozen punten is dat binnen de bal ligt. Ook hier is de spreiding in de resultaten weer evenredig met $1/\sqrt{n}$. Dit geldt in alle dimensies.

Bij de methode met tellen in een regelmatig puntenrooster van $n = m^d$ punten bij dimensie gelijk aan d zal de relatieve fout evenredig zijn met $1/m$. Bij hogere dimensies is dat veel slechter dan met willekeurige punten. Bijvoorbeeld als $d = 20$, moeten we voor het bereiken van een 2 keer zo grote nauwkeurigheid bij een regelmatig puntenrooster 2^{10}, dus ongeveer 1000 keer zoveel punten nemen als eerst, en bij willekeurige punten slechts 4 keer zoveel punten nemen.

Een soortgelijk principe geldt bij integratie van functies over een hoogdimensionaal gebied.

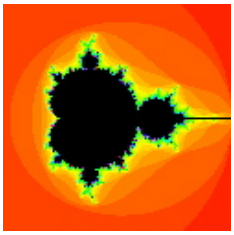
5.2 Algoritme en complexiteit: een eenvoudig voorbeeld

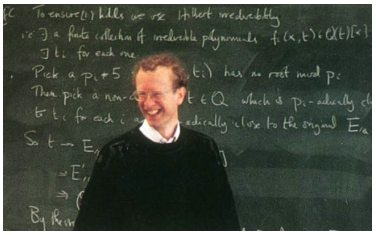
Stel je hebt n getallen $a_1, a_2, \ldots, a_n$ en je wilt het grootste van deze getallen bepalen. Je zult dit doen (of door de computer laten doen) door een aantal malen twee getallen met elkaar te vergelijken en het grootste van die twee te bewaren. Bij bovenstaand probleem zul je dan $n - 1$ keer twee getallen met elkaar moeten vergelijken om tot het maximum te komen. Bijvoorbeeld

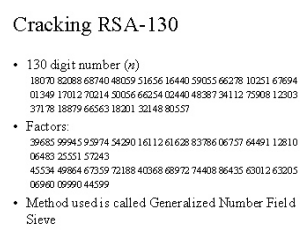
vergelijken we eerst a_1 en a_2 met elkaar en vervangen a_2 door het maximum van a_1 en a_2. Dan vergelijken we a_2 met a_3 en vervangen a_3 door het maximum van a_2 en a_3. Zo doorgaande komen we in $n-1$ stappen bij een nieuwe a_n die het gezochte maximum van de n getallen zal zijn.

Nu willen we van de n getallen zowel de grootste als de kleinste vinden. Naïef zouden we bovenstaande methode twee keer kunnen toepassen, voor de grootste en de kleinste, dus we moeten 2 maal $n-1$ keer twee getallen met elkaar vergelijken, dit is $2n-2$ keer. Het kan echter slimmer, in ongeveer $\frac{3}{2}n-2$ keer, wat precies de zuinigste methode is als n een macht van 2 is. De redenering hiervoor is: als $n=2$ dan vinden we maximum en minimum door 1 keer twee getallen met elkaar te vergelijken. Dit klopt met $\frac{3}{2}n-2$ voor $n=2$. Stel nu dat we het maximum en minimum van $\frac{1}{2}n$ getallen vinden door p getalvergelijkingen. Dan verdelen we onze verzameling van n getallen in twee delen van $\frac{1}{2}n$ getallen en bepalen door 2 keer p getalvergelijkingen maximum en minimum M_1, m_1 van het ene deel en dito M_2, m_2 van het andere deel. Nu is het maximum van de n getallen het maximum van M_1 en M_2 en het minimum van de n getallen het minimum van m_1 en m_2. Dus we hebben $2p+2$ getalvergelijkingen nodig. Merk nu op dat uit $p=\frac{3}{2}\left(\frac{1}{2}n\right)-2$ volgt dat $2p+2=\frac{3}{2}n-2$. Dit is een zogenaamd *bewijs met volledige inductie*. Het type algoritme dat we hier beschreven, met herhaalde deling van de input in twee stukken, heet *divide and conquer*. Een beroemd wiskundig voorbeeld van zo'n algoritme is de *Fast Fourier Transform* (FFT).

6 Wiskundige iconen







Een beperkt aantal onderwerpen uit de wiskunde hebben zoveel aandacht in de media gekregen dat bijna iedereen er van weet. Mede door karakteristieke plaatjes die er mee geassocieerd kunnen worden, hebben ze de status van iconen gekregen.

6.1 Fractalen

Fractalen[11] zijn meetkundige objecten die er min of meer eender uitzien wanneer je ze op verschillende schalen bekijkt. Een bekend voorbeeld uit de natuur is een kustlijn. Een bekend geconstrueerd voorbeeld is de *driehoek van Sierpinski*[12]. Veel gecompliceerder ogende fractalen

[11] `http://mathworld.wolfram.com/Fractal.html`

[12] `http://mathworld.wolfram.com/SierpinskiSieve.html`

zijn de verzamelingen van Julia en Mandelbrot. Toch is het voorschrift van hun constructie eenvoudig. Het vereist alleen elementaire kennis van de complexe getallen. Een Julia-verzameling [13] wordt verkregen door in het complexe vlak te itereren $z_{n+1} = z_n^2 + c$, waarbij c een vast complex getal (een parameter) is en een beginwaarde z_0 als complex getal gegeven is. De (gevulde) *Julia-verzameling* bestaat uit alle beginwaarden waarvoor de geïtereerden z_n begrensd blijven, dus niet naar oneindig gaan. De *Mandelbrot-verzameling* bestaat uit alle complexe waarden van c zo dat de geïtereerden $z_{n+1} = z_n^2 + c$ met $z_0 = 0$ begrensd blijven.

6.2 Fermat


Het Vermoeden van Fermat luidt: Zij n een geheel getal > 2. Dan zijn er geen positieve gehele getallen x, y, z zo dat $x^n + y^n = z^n$. Fermat [14] (1601–1665) schreef in een wiskundeboek in zijn bezit dat hij een bewijs voor dit resultaat had, maar dat het niet paste in de marge van dat boek. Andrew Wiles kondigde in 1993 een bewijs [15] aan van dit vermoeden. Zijn bewijs bleek nog een fout te bevatten, maar hij kon het in 1994 repareren.

6.3 Cryptografie

$$\begin{aligned}\mathrm{RSA}-130 =& 1807082088687404805951656164405905566278102516769401349170127021450056662540244048387341127590812303371781887966563182013214880557\\ =& 96859994595974542901611261628837860675764491128100648325551572435536\\ &\times 45534498646735972188403686897274408864356301263205069600999044599\end{aligned}$$

Iedereen kent de romantische maar grimmige episode in de cryptografie tijdens WO2 met de *Enigma machine* [16] in Bletchley Park, Engeland. In 1977 introduceerden Rivest, Shamir en Adleman een geheel andere aanpak, de *RSA versleutelingsmethode* [17] die een vorm is van *public-key cryptografie*. Iedereen die wel eens een beveiligde pagina op het internet bezoekt (bijv. bij betaling met credit card) komt ermee in aanraking, misschien zonder het te beseffen. Bij deze methode kiest iedere gebruiker twee priemgetallen en een zogenaamde exponent en maakt alleen de exponent en het produkt van de priemgetallen bekend (de *public key*). Iedereen die hem een boodschap wil sturen vercijfert deze boodschap met behulp van het bekend gemaakte produkt en de exponent. Die vercijfering zit zodanig in elkaar dat alleen wie de oorspronkelijke priemgetallen kent, de boodschap kan ontcijferen. RSA Laboratories publiceren *RSA challenge numbers*: grote getallen die producten zijn van twee priemgetallen. De uitdaging is om de factoren te vinden. Het grootste tot nu toe gefactoriseerde RSA-getal is RSA-200 [18] (mei 2005), een getal van 200 cijfers.

[13] http://vmoc.museophile.com/mandelbrot/
[14] http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Fermat.html
[15] http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Fermat's_last_theorem.html
[16] http://en.wikipedia.org/wiki/Enigma_cryptography_machine
[17] http://www.cwi.nl/research/2001/TeRiele_Ned/
[18] RSA-200 http://www.loria.fr/%7Ezimmerma/records/factor.html

6.4 Pi

$\pi = 3.14159265358979323846264\ldots = \left(\int_{-\infty}^{\infty} e^{-x^2}dx\right)^2 = 4\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots\right)$. Lees meer [19]. Japanse informatici berekenden in 2002 meer dan een biljoen (10^{12}) decimalen van π. Het is reeds lang bekend dat π irrationaal en transcendent is, maar men weet niet of π een *normaal getal* [20] is.

7 Spectaculaire wiskundige toepassingen

Er is veel meer wiskunde van belang voor ons dagelijks leven dan de iconen uit hoofdstuk 7. Alleen blijft deze wiskunde onzichtbaar. Hij zit ingebed in de hightechapparaten die we zo graag kopen, en in de dienstverlening waar we gebruik van maken. Zonder die wiskunde zou alles veel minder goed werken, of wel goed maar veel minder efficiënt en daardoor veel duurder. Ik bespreek een paar voorbeelden.

7.1 Compressie van beeld en geluid: FFT

Wie de foto's van zijn digitale camera op zijn computer overbrengt, ziet files verschijnen waarvan de naam eindigt op `.jpg`, en wie met geluidsbestanden werkt heeft te maken met files waarvan de naam eindigt op `.mp3` (maar andere suffixen voor nieuwere formaten zijn ook gangbaar). Kenmerkend voor deze fileformaten is dat de bestanden aanzienlijk kleiner zijn dan bij de oorspronkelijke manier van beeldopslag per pixel of van geluidopslag per fractie van een seconde. Maar ook kunnen zulke bestanden gebruikt worden om in real time een video of muziekstuk af te spelen. Nog een kenmerk, alleen waar te nemen door mensen met een scherpe blik of fijn gehoor, is dat er bij deze gecomprimeerde opslag informatie verloren is gegaan, die bij het afspelen niet meer geheel terug komt.

Slimme algoritmes liggen aan deze compressiemethodes ten grondslag, waarvoor de theorie door de wiskunde geleverd wordt. Het betreft hier vooral de *Fast Fourier transform* [21] (FFT), gevonden door Cooley en Tukey (1965). De *Fourier-transformatie* zet een geluidssignaal om in een functie die van de frequentie afhangt. Dit is een continue operatie. Voor praktische doeleinden kunnen we hem discretiseren en eindig maken. De discrete Fourier-transformatie (DFT) is nog steeds traag: de tijd om hem uit te rekenen is evenredig met het kwadraat van de grootte van de input ($O(n^2)$). De FFT verbetert dit tot $O(n \log n)$ (maar net iets trager dan evenredig met de grootte van de input). Tot zover hebben we nog niet gecomprimeerd: alles kan in omgekeerde volgorde worden gedaan en we krijgen het oorspronkelijke bestand terug. Maar voor die frequenties waar de intensiteit laag is, kunnen we de informatie best weggooien. Zo wordt flink bezuinigd op de bestandsgrootte.

[19] `http://mathworld.wolfram.com/Pi.html`, [3]
[20] `http://mathworld.wolfram.com/NormalNumber.html`
[21] `http://en.wikipedia.org/wiki/Fast_Fourier_transform`

Een verdere ontwikkeling bij verwerking en opslag van beeld en geluid gebruikt *wavelets* (zie [8]), een theorie die eind jaren '80 is opgekomen.

7.2 CT scans: de Radon-transformatie

Met een CT scan (*computerized tomography*) van een deel van het menselijk lichaam worden er van parallelle plakken beelden gemaakt. Elke plak wordt door vele in een rechte lijn lopende röntgenstralen doorlopen. De oorspronkelijke data zijn dus getallen, die voor al die verschillende lijnen verkregen zijn. Wiskundig kan men zich voorstellen dat elk getal verkregen is door integratie over de bijbehorende lijn. Het is dan een wiskundig probleem om de informatie over punten op die plak uit deze data te reconstrueren. Dit was analytisch al opgelost in 1917 door de Oostenrijkse wiskundige Radon. Cormack, gemotiveerd door de medische toepassingen en onbekend met het werk van Radon, loste het probleem rond 1960 opnieuw op en kreeg daar samen met Hounsfield in 1979 de Nobelprijs voor Medicijnen [22] voor.

7.3 Zoekmachines: lineaire algebra

Het succes van de zoekmachine van Google is ondermeer te danken aan de manier waarop Google de zoekresultaten ordent. Deze is gebaseerd op *Pagerank* [23], een bepaald algoritme dat neerkomt op het toekennen van een ranggetal aan iedere webpagina door het oplossen van een stelsel van n lineaire vergelijkingen met n onbekenden, waarbij n in de orde van een miljard (10^9) is. Dit is het terrein van de (numerieke) lineaire algebra: op zich zeer eenvoudige wiskunde, maar gecompliceerd door de grootschaligheid.

7.4 Optieprijzen: stochastische differentiaalvergelijkingen

Het beleggen in opties evolueerde van een gok in een tamelijk rationele activiteit dank zij de *Black-Scholes vergelijking* [24] uit 1973, waarvoor Merton en Scholes in 1997 de Nobelprijs voor economie [25] ontvingen (Black was toen al overleden). Deze formule geeft de prijs van een optie betrekking hebbend op recht tot koop of verkoop van een aandeel op een later tijdstip voor een afgesproken prijs. De enige input van de formule die niet zondermeer kan worden waargenomen is de *volatiliteit* tussen nu en het moment van uitoefenen van de optie. Hiervoor moet een voorspelling worden gedaan. De formule wordt afgeleid op basis van een stochastisch model dat de koersontwikkeling van een aandeel beschouwt als een *Brownse beweging* (dit is de beweging van een deeltje waarbij op elk tijdstip het deeltje in een willekeurig klein volgend tijdsinterval zich random verplaatst volgens een normale kansverdeling die onafhankelijk is van de voorgeschiedenis van het deeltje). De bijbehorende wiskunde is die van de stochastische differentiaalvergelijkingen.

[22] `http://nobelprize.org/medicine/laureates/1979/`
[23] `http://www.google.com/corporate/tech.html`, cite20
[24] `http://en.wikipedia.org/wiki/Black-Scholes`
[25] `http://nobelprize.org/economics/laureates/1997/`

De grondslag van deze theorie van optieprijzen werd reeds in 1900 gelegd in de dissertatie van de Fransman Bachelier, die zijn tijd hiermee ver vooruit was. Hij had ook al een notie van Brownse beweging, 5 jaar voordat Einstein hierover publiceerde en er beroemd door werd.

De theorie van de optieprijzen is van groot maatschappelijk belang, denk bijv. aan het beheer van uw pensioengelden.

7.5 Rechtspraak: forensische statistiek

Resultaten van forensisch onderzoek in verband met een misdrijf krijgen steeds meer gewicht in de rechtstpraak. Veel conclusies uit het forensisch onderzoek zijn niet absoluut zeker, maar slechts met een bepaalde kans. Denk bijv. aan DNA-onderzoek, wanneer de op de plaats van het misdrijf aangetroffen DNA-sporen matchen met het DNA van de verdachte. Hier betreden we het terrein van de *forensische statistiek*. Deskundige statistische rapportage in de rechtzaal, gecombineerd met enige statistisch begrip bij de optredende juristen, is van groot belang en kan grove fouten in het vonnis voorkomen zie [16].

8 Wiskunde in de cultuur

8.1 Muziek

Reeds in de oudheid werd er een verband gelegd tussen wiskunde en muziek, denk aan de school van Pythagoras. Het idee van de harmonie der sferen inspireerde de sterrenkunde gedurende vele eeuwen. De composities van Johann Sebastian Bach, vooral *die Kunst der Fuge* doen onweerstaanbaar aan wiskunde denken, hoewel de muzikale meerwaarde tot in lengte van dagen ongrijpbaar lijkt voor wiskunde of kunstmatige intelligentie. De Grieks-Franse componist Iannis Xenakis [26] (1922–2001) gebruikte stochastische wiskundige principes in zijn composities. John Cage (1912–1992) was een andere belangrijke vertegenwoordiger van deze *aleatorische muziek* [27]. Veel hedendaagse componisten geven in programmatoelichtingen aan dat zij zich bij het componeren laten leiden door een structurerend wiskundig principe, meestal met computerondersteuning. In de regel is het niet de bedoeling dat de luisteraar dit bewust hoort. Bij deze wiskundige ondersteuning zijn de fractalen erg populair. De Nederlandse componist Theo Verbeij noemde een van zijn werken *Fractale Symfonie*.

8.2 Literatuur

Het refereren aan wiskundige zaken in literaire werken is van alle tijden. Denk bijvoorbeeld aan Plato, Jonathan Swift, Edgar Allen Poe, Multatuli. Het aantal nieuwe romans, toneelstukken, films met een wiskundig thema lijkt de laatste jaren flink toe te nemen [28]. In veel van deze werken gaat het om wiskundigen als eigenaardige, licht of ernstig gestoorde personen, soms wel erg

[26] `http://en.wikipedia.org/wiki/Iannis_Xenakis`

[27] `http://en.wikipedia.org/wiki/Aleatoric_music`

[28] `http://math.cofc.edu/faculty/kasman/MATHFICT/Default.html`, [2]

stereotiep. Gelukkig speelt de wiskunde zelf vaak ook een rol. Sommige boeken leggen wiskundige principes in een literaire vorm uit, andere gebruiken de wiskunde. Opsporing van misdaad en science fiction zijn hierbij uiteraard goed vertegenwoordigd. Twee van mijn favorieten, waarbij de wiskunde niet expliciet maar wel impliciet aanwezig is, zijn *Le città invisibili* (Onzichtbare steden) van Italo Calvino (1972) en *Das Glasperlenspiel* van Herman Hesse (1943).

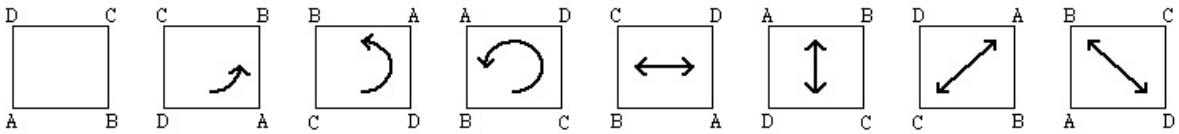
8.3 Architectuur

Geodetische koepels zijn benaderingen van boloppervlakken door triangulaties. Buckminster Fuller [29] (USA, 1895–1983) patenteerde dit idee in 1954. Piet Hein (Denemarken, 1905–1996) propageerde de toepassing van de *superellips* [30]. Grillige gekromde oppervlakken doen opgang in moderne architectuur[31]. Zie bijvoorbeeld het Opera House in Sydney en het Guggenheim Museum in Bilbao. Deze constructies werden mede mogelijk gemaakt door moderne systemen voor Computer Aided Design.

9 Lie-theorie

Om te illustreren hoe deelgebieden van de zuivere wiskunde zich ontwikkelen doordat er telkens weer nieuwe onverwachte verbanden worden gelegd met andere gebieden van wiskunde of met de theoretische natuurkunde, bespreek ik in wat meer detail de theorie van de Lie-groepen (continue symmetrieën) en de algemenere Lie-theorie die daaruit is voortgekomen. Lie-groepen zijn genoemd naar de Noorse wiskundige Sophus Lie [32] (1842–1899). Algemeen wordt de Lie-theorie gezien als een van de meest centrale onderwerpen binnen de wiskunde.

9.1 Symmetrieën en groepen



We beginnen met het begrip *groep* in de wiskunde. Dit is het gemakkelijkst duidelijk te maken aan de hand van een voorwerp met enige symmetrie, bijv. een vierkant. Een *symmetrie-operatie* (kortweg *symmetrie*) van het vierkant beeldt het vierkant op zichzelf af zonder het te vervormen. Het vierkant heeft acht symmetrieën (zie figuur): vier draaiingen over hoeken van resp. 0, 90, 180 en 270 graden (altijd tegen de wijzers van de klok in gemeten) en vier spiegelingen. Een symmetrie gevolgd door nog een symmetrie is weer een symmetrie. Bijv. een rotatie over 90

[29] http://en.wikipedia.org/wiki/Buckminster_Fuller
[30] http://en.wikipedia.org/wiki/Super_ellipse
[31] http://www.sciencemag.org/cgi/content/full/285/5429/839
[32] http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Lie.html

graden gevolgd door een spiegeling t.o.v. een diagonaal geeft een spiegeling t.o.v. een middellijn. Er is altijd een *identiteit*: de operatie die alle punten van het voorwerp op zijn plaats laat. Verder heeft iedere symmetrie een *inverse*: de operatie die elk punt weer terugvoert naar zijn oorspronkelijke plaats.

De verzameling G van alle symmetrieën van een object vormt een zogenaamde *groep*. Als g en h symmetrieën zijn, dus elementen van G, dan bedoelen we met het *product* gh de symmetrie die het resultaat is van eerst h en dan g toepassen op het object. Dus gh zit dan weer in G. Met e duiden we de identiteit, als element van G, aan. Met g^{-1} duiden we het element van G aan dat de inverse is van de symmetrie g. Nu kunnen we direct inzien dat voor elementen g, h, k van G de volgende wetten gelden:

$$eg = g \text{ en } ge = g, \qquad gg^{-1} = e \text{ en } g^{-1}g = e, \qquad (gh)k = g(hk).$$

Laatstgenoemde wet beschrijft de z.g. *associativiteit* van de vermenigvuldiging: het resultaat van eerst operaties k en h na elkaar uitvoeren, en dan nog eens g, geeft dezelfde operatie als eerst operatie k uitvoeren en dan nog eens de operatie die het resultaat is van eerst h en dan g uitvoeren. Deze wet, evenals de twee andere wetten, lijkt tamelijk flauw als het gaat om een groep G die uit symmetrieën is gevormd. Maar we kunnen een groep ook abstract invoeren als een verzameling G waarin er bij elk tweetal elementen g, h weer een element gh van G is, en waarin er een element e is, en waarin er bij elk element g een element g^{-1} is, dit alles zo dat bovenstaande drie wetten gelden.

We noemen een groep G *commutatief* als voor elke g en h in G geldt dat $gh = hg$. Commutativiteit hoeft lang niet altijd te gelden. Bijv. de groep van symmetrieën van het vierkant is niet commutatief (ga zelf na). Een voorbeeld van een commutatieve groep is de groep van de positieve rationale getallen, dat zijn alle getallen die als breuk te schrijven zijn met positieve gehele getallen in teller en noemer. In die groep nemen we als product van twee elementen het gewone product van die twee breuken.

9.2 Lie-groepen en representaties van groepen

Laten we nu eens naar de cirkel of de bol kijken. Een symmetrie van zo'n voorwerp kunnen we continu veranderen zo dat het een symmetrie blijft. Bijv. bij de cirkel zijn de draaiingen om het middelpunt symmetrieën. We draaien over een bepaalde hoek (tegen de wijzers van de klok in). Het maakt natuurlijk niet uit als we nog 360 graden (de wiskundige zegt 2π radialen) verder draaien, maar in ieder geval vormen alle mogelijke draaiingen een continuum. Al deze draaiingen samen vormen weer een groep. Omdat deze groep een continue structuur heeft, wordt hij een *Lie-groep* genoemd, naar de Noorse wiskundige Sophus Lie. Dit is wel een erg eenvoudig voorbeeld van een Lie-groep. Hij is bijvoorbeeld commutatief. Veel interessanter is al de symmetriegroep van alle draaiingen van de bol. Dit is een niet-commutatieve Lie-groep.

Zodra een wiskundige een groep aangeboden krijgt, wil hij daarvan de *representaties* (of *voorstellingen*) bekijken. Hierbij wordt de groep G afgebeeld naar de groep van rotaties van een bol (mogelijk in hogere dimensie, die zelfs oneindig kan zijn). De afbeelding gaat zo dat

de structuur van de groep (de vermenigvuldiging) behouden blijft. Bij een Lie-groep G moet in een representatie ook de continue structuur behouden blijven. Meestal kan een representatie worden opgedeeld in kleinere stukken (van lagere dimensie), totdat men stuit op een soort atomen: representaties die niet verder te splitsen zijn. Zulke representaties heten *irreducibel*. Een vaste opgave voor de groepentheoreticus is om een classificatie te geven van alle irreducibele representaties van een gegeven groep. Soms is dit makkelijk, soms moeilijk, en soms nog een open probleem. Verder is dit zeker niet alleen van theoretisch belang. Sinds de opkomst van de quantummechanica hebben de irreducibele representaties van sommige speciale groepen een directe natuurkundige interpretatie, bijv. als de *spin* van een elementair deeltje.

Lie-groepen zijn niet alleen continu, ze zijn ook glad. Daarom hoort er bij elk element van een Lie-groep G een raakruimte. De raakruimte bij het identiteitselement e van G erft in het bijzonder een "oneindig kleine" versie van de vermenigvuldiging op G. Dit resulteert in een bepaalde algebraïsche structuur op die raakruimte die het *Lie-haakje* genoemd wordt. Zo wordt deze raakruimte een *Lie-algebra* $\mathfrak{g}$. Belangrijk is dat de Lie-groep G de Lie-algebra $\mathfrak{g}$ bepaalt en dat omgekeerd $\mathfrak{g}$ bijna (in ieder geval lokaal) G bepaalt. Ook is er zo'n heen en weer gaan tussen representaties van G en representaties van $\mathfrak{g}$. Deze laatste representaties zijn in zekere zin gemakkelijker: ze hoeven alleen maar een algebraïsche structuur en geen meetkundige te behouden.

Bij de Lie-groepen is er een belangrijk onderscheid tussen compacte en niet-compacte Lie-groepen. *Compact* wil ongeveer zeggen dat de Lie-groep een begrensde omvang heeft (nergens naar oneindig gaat) en zonder randen is. Bijv. de groep van draaiingen van een bol (van willekeurige dimensie) is compact. Een voorbeeld van een niet-compacte Lie-groep is de groep van afstand en oriëntatie behoudende symmetrieën van het platte vlak (een groep bestaande uit draaiingen en verschuivingen). Alle irreducibele representaties van een compacte groep zijn eindig-dimensionaal. Bij een niet-compacte groep zijn er doorgaans ook oneindig-dimensionale irreducibele representaties.

9.3 Halfenkelvoudige Lie-groepen en wortelsystemen

De representatietheorie van de compacte Lie-groepen werd al in de jaren dertig van de vorige eeuw ontwikkeld, met name door Hermann Weyl, die daarbij sterk gemotiveerd werd door de quantummechanica. Voor de niet-compacte Lie-groepen kwam dit echter pas op gang na WO2. Vooral Harish-Chandra ontwikkelde de representatietheorie van niet-compacte halfenkelvoudige reële Lie-groepen in volledige algemeenheid. *Halfenkelvoudig* betekent ruwweg dat de Lie-groep zelf in kleinere stukken (wederom Lie-groepen) kan worden opgesplitst, net zo lang tot men belandt bij niet verder te splitsen Lie-groepen, die men *enkelvoudig* noemt. In het algemeen zijn er binnen de Lie-groepen twee extreme vormen: de half-enkelvoudige en de oplosbare groepen. Deze twee types vereisen volledig verschillende technieken. De half-enkelvoudige Lie-groepen kunnen tot de enkelvoudige worden teruggebracht en deze laatste kunnen geclassificeerd worden. Die classificatie vindt plaats door op te merken dat een halfenkelvoudige Lie-groep bepaald wordt door de bijbehorende halfenkelvoudige Lie-algebra en dat die weer wordt bepaald door

een zogenaamd *wortelsysteem*. Dit is een veel eenvoudiger structuur: een stelsel vectoren in de n-dimensionale ruimte ($\mathbb{R}^n$) met bepaalde eigenschappen die aanleiding geven tot spiegelingen in de $\mathbb{R}^n$ die dat stelsel vectoren weer in zichzelf overvoeren. De irreducibele (niet verder te ontbinden) wortelsystemen, en dus de enkelvoudige Lie-groepen, worden aangegeven met codenamen A_n, B_n, C_n, D_n, G_2, F_4, E_6, E_7, E_8, waaronder ze op veel plaatsen in de wiskunde opduiken. Hiermee gepaard gaat een rijke structuur van grote esthetische kwaliteit, die associaties met Bach en Escher oproept.

9.4 Deformaties en quantumgroepen

In de jaren '80 werden nieuwe structuren geassocieerd met wortelsystemen ontwikkeld waarbij het begrip *deformatie* een belangrijke rol speelt. Een deformatie is een kleine continu verlopende vervorming van een wiskundige structuur, waarbij de structuur wel tot dezelfde klasse van structuren moet blijven behoren. De vraag is dan of het vervormde object al of niet *isomorf* is met het onvervormde object (isomorf wil zeggen: op grond van de structuur niet van elkaar te onderscheiden). Een structuur heet *rigide* als elk vervormd object isomorf is met het oorspronkelijke object. Halfenkelvoudige Lie-groepen zijn rigide, althans zolang men de blik niet opent voor radicalere deformaties. Dit laatste inzicht was 20 jaar geleden een enorme eye-opener, zoiets als wanneer een platlander gewezen wordt op de mogelijkheden van de derde dimensie.

Om enig begrip voor die deformaties te krijgen, moet je op een nieuwe manier naar Lie-groepen, of algemener naar meetkundige objecten gaan kijken. Zo'n object is zeker ook een verzameling punten en op die verzameling kun je functies bekijken. Elke functie is een voorschrift om aan elk punt van de verzameling een getal toe te voegen. Verder moet dat voorschrift zich netjes t.o.v. de meetkundige structuur gedragen. De functies kun je bij elkaar optellen en met elkaar vermenigvuldigen. Ook verdere eigenschappen van de structuur, bijv. dat het een groep is, kan men herformuleren in termen van bepaalde operaties op de functies. In feite is alle informatie over die meetkundige structuur bevat in het geheel van de beschouwde functies op de verzameling, samen met de verschillende operaties die op de functies werken. Je zou de oorspronkelijke meetkundige structuur kunnen vergeten en verder kunnen gaan met deze structuur van functies. In het bijzonder zou je de functiestructuur kunnen deformeren. We constateerden dat je functies met elkaar kunt vermenigvuldigen, dat is een commutatieve operatie: de volgorde van de twee factoren doet er niet toe. Sta nu eens deformaties toe waarbij die volgorde er wel toe doet: we gaan *van commutatief naar niet-commutatief*. Dit principe ligt ten grondslag aan de *quantumgroepen* en meer algemeen aan de *niet-commutatieve meetkunde*. Je beoefent een soort algebra met een niet-commutatieve vermenigvuldiging maar aan veel zaken ken je toch meetkundige benamingen toe en je houdt associaties met een zichtbaar te maken meetkunde.

Bij de deformaties is er doorgaans een *deformatieparameter* die vaak met q wordt aangeduid. De waarde $q = 1$ staat voor de onvervormde toestand. Door q van 1 weg te laten lopen geeft men de deformatie aan. De parameter q werd al in de negentiende eeuw gebruikt om *q-hypergeometrische functies* te beschrijven, deformaties van hypergeometrische functies. Deze q-hypergeometrische functies blijken ook in verband te kunnen worden gebracht met quantum-

groepen, en deze laatste hebben weer wat te maken met quantisatie in de natuurkunde. Hier is dan het wonderlijke: de negentiende eeuwse wiskundigen kozen de letter q, die anderhalve eeuw later een prachtig passende nieuwe betekenis krijgt als de q van quantum.

9.5 Enkelvoudige eindige groepen

Bij eindige groepen (dit zijn groepen met eindig veel elementen) kan met net als bij de Lie-groepen naar de "atomen" gaan kijken: de *enkelvoudige eindige groepen*, die niet verder op een rechtstreekse manier opgedeeld kunnen worden. Voor eindige groepen is de classificatie van de enkelvoudige groepen veel moeilijker dan voor Lie-groepen. Naast groepen "uit het dagelijks leven" (cyclische groepen waarvan het aantal elementen een priemgetal is en de groepen van alle even permutaties van een eindig aantal elementen) en groepen geassocieerd met wortelsystemen, zijn er ook 26 *sporadische groepen* (groepen die op zichzelf staan, niet in een oneindige serie voorkomen). De grootste hiervan is de *monstergroep*[33], die bestaat uit $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$ (ongeveer $8 \cdot 10^{53}$) elementen. De classificatie van de enkelvoudige eindige groepen, in het bijzonder het bewijs dat er niet meer zulke groepen bestaan dan er nu in de lijst voorkomen, werd in de jaren '70 verricht door een team van zo'n 100 wiskundigen. Het volledige bewijs, verspreid over boeken en vaak lange tijdschriftartikelen omvat wel zo'n tienduizend pagina's. Sommige details zijn nog steeds niet gepubliceerd. Verder lijkt het voor een enkele persoon onmogelijk om het hele bewijs te lezen en te verifiëren. De meeste betrokkenen geloven dat de classificatie volledig en correct is. Maar dit is dan toch een ander type wiskundige waarheid dan die van onze kleinschaliger stellingen.

10 Mathematische fysica

Van ouds is er een nauwe relatie en interactie tussen wiskunde en (theoretische) natuurkunde. In een veel geciteerd artikel [18] spreekt E. P. Wigner over de *unreasonable effectiveness of mathematics in physics*. De wetten van de natuurkunde zijn (door de mens) in de taal van de wiskunde geschreven, waardoor de natuurbeschrijving een grote elegantie en esthetische kwaliteit krijgt en, veel belangrijker nog, een wiskundige afleiding geboden wordt om uit de meetgegevens voorspellingen te doen die met grote precisie blijken uit te komen. Dit heeft zich o.a. voorgedaan met de klassieke mechanica van Newton, de algemene relativiteitstheorie van Einstein, de quantummechanica, de quantumelectrodynamica en het z.g. standaardmodel van de elementaire deeltjes en hun interacties. Waarom zijn het heelal en de materie juist zo dat de wiskunde ze zo goed beschrijft? Een waarom is er zoveel onder de door de mens ontwikkeled wiskunde dat vroeg of laat bruikbaar is in de natuurkunde?

Hierboven was sprake van effectief gebruik van de wiskunde in de natuurkunde. Maar ook de wiskunde profiteert hiervan. De wiskunde die de natuurkundigen in gebruik nemen, en soms ook zelf bedacht hebben, is vaak wiskundig nog onbevredigend, ondanks zijn effectiviteit in de

[33] `http://en.wikipedia.org/wiki/Monster_group`

natuurkunde. Dit zet de wiskundigen dan aan om daarvoor een mooie en wiskundig rigoureuze theorie te ontwikkelen, een werk dat soms tientallen jaren vergt en waar de natuurkundigen gelukkig niet op wachten. Denk aan Dirac's delta-functie gevolgd door de distributietheorie van L. Schwartz, en aan de Feynman-integralen die voor de wiskundigen nog steeds een harde noot vormen.

Een nog sterkere beïnvloeding van de wiskunde door de natuurkunde werd opgemerkt door Robbert Dijkgraaf als de *onredelijke effectiviteit van de fysica in de moderne wiskunde* [5]. Een natuurkundig geïnspireerde denkwijze, vooral geleverd door de quantumveldentheorie, blijkt doorbraken te kunnen leveren in weerbarstige wiskundige problemen, veelal meetkundig van aard, zoals de 4-dimensionale topologie.

Een zeer actief gebied in de meer speculatieve theoretische natuurkunde is de *snarentheorie*, die Einstein's oude droom probeert te verwezenlijken van vereniging van de krachten die op het allerkleinste niveau spelen met de tot op de grootste schalen werkende zwaartekracht. Gedreven door fysische intuïtie wordt er binnen de snarentheorie veel nieuwe wiskunde ontwikkeld. Dit gaat zover dat vanuit de snarentheorie voorspellingen worden gedaan over numerieke waarden geassocieerd met bepaalde objecten in de algebraïsche meetkunde, met name moduli-ruintes (zie bijv. Fields-medaille-winnaar Ed Witten [34]), die vervolgens door wiskundigen bewezen worden (zie bijv. Fields-medaille-winnaar Maxim Kontsevich [9]).

11 Millennium Prize Problems van het Clay Institute

Hilbert structureerde veel wiskundig onderzoek in de 20e eeuw met zijn lijst van 23 problemen gepresenteerd in 1900 in Parijs. Het Amerikaanse *Clay Mathematics Instititute* presenteerde op 24 mei 2000 in Parijs zes *Millennium Prize Problems* [35]. Voor de goede oplossing van elk van die problemen werd een prijs van 1 miljoen dollar uitgeloofd. Het enige Clay-probleem day ook al in Hilbert's lijst voorkwam, is de *Riemann-hypothese*: het vermoeden van Riemann uit 1859 dat alle niet-triviale nulpunten van de *zetafunctie* op een verticale lijn in het complexe vlak liggen. Dit vermoeden kan beschouwd worden als de heilige graal van de wiskunde. Bewijs ervan zou grote implicaties hebben voor de manier waarop priemgetallen gespreid liggen [36].

In de lijst van het Clay Institute is ook het *P versus NP probleem*, van geheel andere aard maar minstens zo belangrijk. Een probleem van klasse P kan door een computer geverifieerd worden in een tijd die hoogstens een macht is van de grootte van de input (in *polynomiale tijd*). Bij een probleem van klasse NP kan in polynomiale tijd nagegaan worden of een gegeven oplossing inderdaad voldoet. De grote vraag is of de klasse NP echt groter is dan de klasse P. Het bekende *handelsreizigersprobleem* [37] is een goede kandidaat om NP maar niet P te zijn.

[34] `http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Witten.html`
[35] `http://www.claymath.org/millennium`
[36] `http://www.maa.org/reviews/primeobsession.html`
[37] `http://www.tsp.gatech.edu/problem/`

Van de zes millenniumproblemen is het *Vermoeden van Poincaré* (een eenvoudige meetkundige karakterisering van de 3-sfeer $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$) het dichtst bij een oplossing door het werk van de Russische wiskundige Perelman.

12 Nawoord en handreiking naar de literatuur

We hebben een vluchtige wiskundereis door de laatste 60 jaar voltooid. Lang niet alle topbezienswaardigheden hebben we bezocht. Het was een gouden tijd voor de wiskunde. Inhoudelijk gezien is er nog veel meer goud te verwachten, maar dat zal ook afhangen van de mensen en de maatschappij. In een somber scenario kan er over 100 jaar bijna niemand meer rekenen en begrijpt bijna niemand meer de wiskunde die ten grondslag ligt aan de algortitmen waarmee de software geschreven is waarop alle technologie gebaseerd is. Dan moet men maar wat Babyloniërs door de tijd laten reizen voor hulp, want onder hen waren zeer goede rekenaars. Laat ik toch maar inzetten op een positief bewijs van de Riemann-hypothese nog in deze eeuw.

Wie verder over moderne wiskunde wil lezen, kan al veel vinden op het web, bijv. in de encyclopedische websites *MathWorld*[38] en *Wikipedia: Mathematics*[39] en in een *History of Mathematics archive*[40]. De Nederlandstalige website `www.kennislink.nl` brengt actueel wetenschappelijk nieuws, waaronder wiskunde, vooral gericht op scholieren. Voor uitgebreidere uitleg gericht op de ontwikkelde leek kan ik de Nederlandstalige boeken [4], [17], [6], [12] aanbevelen.

Referenties

[1] G. Alberts, *Jaren van berekening. Toepassingsgerichte initiatieven in de Nederlandse wiskunde-beoefening 1945–1960*, Amsterdam University Press, 1998.

[2] *De macht van het getal*, Raster nr. 100, De Bezige Bij, 2002.

[3] J.-P. Delahaye, *Het fascinerende getal Pi*, Veen Magazines, 2004.

[4] K. Devlin, *Wiskunde: wetenschap van patronen en structuren*, Natuur & Techniek, 1998.

[5] R. Dijkgraaf, *De onredelijke effectiviteit van de fysica in de moderne wiskunde*, Ned. Tijdschr. v. Natuurk. 62 (1996), 255–257.

[6] T. Gowers, *Wiskunde: De kortste introductie*, Het Spectrum, 2003.

[7] J. W. Grossman, *Patterns of collaboration in mathematical research*, SIAM News 35 (2002), no. 9; `http://www.siam.org/siamnews/11-02/collaboration.pdf`.

[38] `http://mathworld.wolfram.com/`
[39] `http://en.wikipedia.org/wiki/Category:Mathematics`
[40] `http://www-groups.dcs.st-and.ac.uk/~history/`

[8] B. B. Hubbard, *The world according to wavelets. The story of a mathematical theory in the making*, A K Peters, Wellesley, MA, 1998.

[9] A. Jackson, *Borcherds, Gowers, Kontsevich, and McMullen receive Fields medals*, Notices Amer. Math. Soc. 45 (November 1998), 1358–1360; `http://www.ams.org/notices/199810/199810-toc.html`.

[10] N. Litvak, *Googling maths*, Nieuw Archief voor Wiskunde (5) 7 (2006), no.1, 33–38.

[11] M. Monastyrsky, *Modern mathematics in the light of the Fields medals*, A K Peters, Wellesley, MA, 1997.

[12] P. Odifreddi, *Geschiedenis van de wiskunde in de twintigste eeuw*, Epsilon Uitgaven, 2005.

[13] A. Odlyzko, *Tragic loss or good riddance? The impending demise of traditional scholarly journals*, Notices Amer. Math. Soc. 42 (Jan. 1995), 49–53; `http://www.dtc.umn.edu/~odlyzko/doc/eworld.html`.

[14] L. S. Penrose & R. Penrose, *Impossible objects: a special type of visual illusion*, Brit. J. Psychology 49 (1958), 31–33.

[15] L. Schwartz, *A mathematician grappling with his century*, Birkhäuser, 2001.

[16] M. Sjerps, *Forensische statistiek*, Nieuw Archief voor Wiskunde (5) 5 (2004), no. 2, 106–111; `http://www.math.leidenuniv.nl/~naw/serie5/deel05/jun2004/pdf/sjerps-HR.pdf`.

[17] B. de Smit & J. Top (red.), *Speeltuin van de wiskunde. Opties, kansspelen, Escher, pi, Fermat en meer*, Veen Magazines, 2003.

[18] E. P. Wigner, *The unreasonable effectiveness of mathematics in the natural sciences*, Comm. Pure Appl. Math. 13 (1960), 1–14.

[19] D. Zeilberger, *Theorems for a price: tomorrow's semi-rigorous mathematical culture*, Notices Amer. Math. Soc. 40 (October 1993), 978–981; `http://www.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/priced.html`.