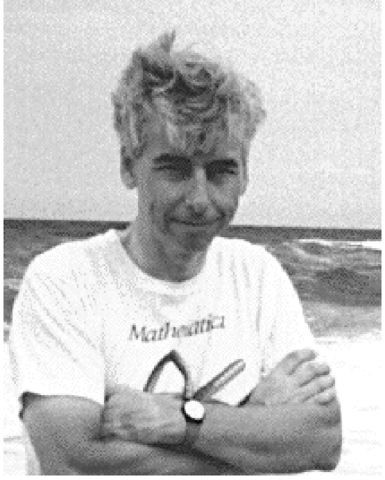
Brian Hayes
211 Dacian Avenue
Durham NC 27701
Verenigde Staten
bhayes@amsci.org



Brian Hayes

Research

Foolproof

Wat voor betekenis heeft een bewijs als het door een computer is gegenereerd? Hoe belangrijk is de mening van het publiek eigenlijk en over welk publiek hebben we het eigenlijk, als het gaat om het accepteren van een wiskundig bewijs? En omgekeerd, wat moeten we met een bewijs, dat alleen door een computer kan worden begrepen? Brian Hayes, wiskundige en tientallen jaren publicist en redacteur van onder andere de Scientific American probeert u te verleiden met allerlei foute bewijzen. Dit artikel verscheen eerder in de 'American Scientist' volume 95. De vertaling is van Reinie Erné en Jaap Molenaar.

In mijn tienerjaren was ik een trisecteur. Mijn eerste baan direct na de middelbare school bestond uit het dag in dag uit in drieën delen van hoeken, voor 1,75 dollar per uur. Mijn werkgever maakte voltmeters, ampèremeters en allerlei andere elektrische instrumenten. Dit was nog in het analoge tijdperk, toen een meter bestond uit een dun wijzertje dat in een boog langs een schaal bewoog. Mijn werk bestond uit het tekenen van die schaal. Een technicus ijkte de meter, en stelde de hoek vast voor een aantal belangrijke intervallen, zeg 3, 6, 9, 12 en 15 volt. Ik maakte vervolgens de schaal door met passer, liniaal en een fijn pennetje de tussenliggende waarden in te tekenen door middel van interpolatie. Daar had ik de trisectie van hoeken voor nodig. Ik moest ook weleens hoeken in vijven delen en andere onmogelijke taken uitvoeren.

Ik maakte hier grapjes over met mijn collega en directe baas Dmytro, die al een aantal jaar schalen tekende. We zouden meer betaald moeten worden, zei ik, voor het oplossen van één van de beroemdste onoplosbare problemen uit de Oudheid. Maar Dmytro was een skepticus en daagde mij uit om te bewijzen dat trisectie niet kan. Dat kon ik niet. Na een column van Martin Gardner over het onderwerp herlezen te hebben, deed ik mijn best om een bewijs te schetsen, maar ik beheerste de onderliggende wiskunde te weinig, mijn argumenten waren onsamenhangend, en mijn gehoor bleef onovertuigd.

Aan de andere kant liet Dmytro zelf snel zien dat onze methode van trisectie, een koord over de hoek spannen en die in drie gelijke stukken delen, niet werkt voor grote hoeken. Vanaf dat moment letten we er op alleen nog maar kleine hoeken in drieën te delen. En we waren het erover eens dat onze werkgever hier niets van af hoefde te weten. Onze omzichtige stilte leek enigzins op de Pythagoreïsche samenzwering om de irrationaliteit van $\sqrt{2}$ geheim te houden.

Als ik terugkijk op die periode krijg ik vage twijfels over de rol van bewijzen in wiskundige verhandelingen, en in het alledaagse leven. Ik geef toe, het feit dat ik Dmytro niet kon overtuigen lag geheel aan mij, en niet aan het bewijs. Maar toch, als een bewijs een toverstok is die alleen werkt in de handen van tovenaren, wat heeft de rest van ons er dan aan?

Euclides achterstevoren lezen

De volgende anecdote in *Brief Lives* van John Aubrey over de 17e eeuwse filosoof Thomas Hobbes illustreert wat het effect van een bewijs behoort te zijn:

"He was forty years old before he looked on geometry; which happened accidentally. Being in a gentleman's library in ..., Euclid's Elements lay open, and 'twas the 47 *El. libri* I. He read the proposition.

'By G—,' sayd he (he would now and then swear, by way of emphasis), 'this is impossible!' So he reads the demonstration of it, which referred him back to such a proposition; which proposition he read. That referred him back to another, which he also read. *Et sic Deinceps*, that at last he was demonstratively convinced of that trueth. This made him in love with geometry."

Wat hierin het meeste opvalt, of het nu waar is of niet, is hoe Hobbes zich tegen zijn wil toch laat overtuigen. Hij begint ongelovig, maar kan de overtuigingskracht van de deductieve logica niet weerstaan. Vanuit propositie 47, toevallig de stelling van Pythagoras, werd hij gedwongen terug te bladeren in het boek, van de conclusies naar de daarbij gebruikte vooronderstellingen en uiteindelijk terug naar de axioma's. Al zoekt hij naar een fout, iedere stap van de redenering dwingt instemming af. Dit is de kracht van zuiver redeneren.

Voor velen onders ons verliep de eerste kennismaking met wiskundig bewijzen — hoogstwaarschijnlijk tijdens een meetkundeles — nogal anders dan die van Hobbes op middelbare leeftijd. De werkelijkheid lijkt meer op een ander veelgelezen verhaal, uit de dialoog *Meno* van Plato. Terwijl Socrates figuren tekende in het zand, probeerde hij een ongeschoolde jonge slaaf te onderwijzen door hem te helpen een bepaald geval van de stelling van Pythagoras te bewijzen. Ik parafraseer heel losjes:

Socrates: Hier is een vierkant met zijde 2 en oppervlakte 4. Als we de oppervlakte verdubbelen, naar 8 eenheden, hoe lang is de zijde dan?
Jongen: Uh, 4?
Socrates: Is $4 \times 4 = 8$?
Jongen: Goed, misschien is het dan 3.
Socrates: Is $3 \times 3 = 8$?
Jongen: Ik geef het op.
Socrates: Kijk eens naar deze lijn van hoek naar hoek, die de geleerden een diagonaal noemen. Als wij hierop een vierkant plaatsen, dan is de helft van het oorspronkelijke vierkant een kwart van het nieuwe vierkant, dus moet de oppervlakte van het nieuwe vierkant tweemaal dat van het oorspronkelijke vierkant zijn. De lengte van de diagonaal is dus precies wat wij zoeken, niet waar?
Jongen: Zal wel.

Op dit punt aangekomen neem ik aan dat we allemaal de kant van de jongen kiezen. Ik zou natuurlijk graag kunnen vertellen dat de jongen vervolgens het initiatief neemt en iets zegt als 'Jij je zin, ouwe, maar wat is dan de lengte van die geleerde diagonaal van jou? Het is niet 4 en het is niet 3, dus wat is het nou precies?' Jammer genoeg vermeldt Plato geen dergelijke provocerende reactie van de kant van de jonge slaaf.

Het probleem met het *Meno* bewijs is precies het omgekeerde van wat ik meemaakte als ongeschoolde loonslaaf. Terwijl ik te onbekwaam en intellectueel te slecht uitgerust was om een bewijs te leveren dat mijn collega overtuigde (of op zijn minst mijzelf), had Socrates zo'n krachtige autoriteit dat de arme jongen vast alles zou accepteren dat de meester zei. Hij zou waarschijnlijk niet eens tegenstribbelen als Socrates zou bewijzen dat $2 = 1$. Zo'n jongen zal ongetwijfeld niet zelf stellingen gaan bewijzen.

Jammer genoeg profiteerde Hobbes niet veel meer van zijn eigen meetkundeles. Hij werd een beruchte wiskundige zonderling, die beweerde alle beroemde problemen uit de klassieke meetkunde opgelost te hebben, inclusief de trisectie van een hoek, de kwadratuur van de cirkel, en de verdubbeling van de kubus. Deze beweringen waren in de 17e eeuw iets minder dwaas dan nu, aangezien de onmogelijkheid ervan toen nog niet streng bewezen was. Desalniettemin hadden de tijdgenoten van Hobbes weinig moeite met het vinden van de blunders in zijn bewijzen.

Grootse stellingen, onhanteerbare bewijzen

De laatste tijd is bewijzen een verbazend controversieel onderwerp geworden. Een eerste bron van onbehagen was het bewijs in 1976 van het vierkleurenprobleem dat Kenneth Appel, Wolfgang Haken en John Koch van de University of Illinois at Urbana-Champaign gaven. Zij lieten zien dat je om een landkaart zo te kleuren dat twee aanliggende landen steeds verschillende kleuren hebben maar vier kleurpotloden nodig hebt. Het bewijs maakte gebruik van computerprogramma's die duizenden kaartconfiguraties controleerden. Dit binnendringen van computers in het domein van de zuivere wiskunde werd met veel argwaan en zelfs afkeer begroet. Haken en Appel maakten gewag van een opmerking van een vriend: "God zou nooit toelaten dat het beste bewijs van zo'n fraaie stelling zo lelijk is". Naast zulke emotionele en esthetische reacties was er ook de slepende vraag naar verificatie: hoe kunnen wij er ooit zeker van zijn dat de computer geen fout gemaakt heeft?

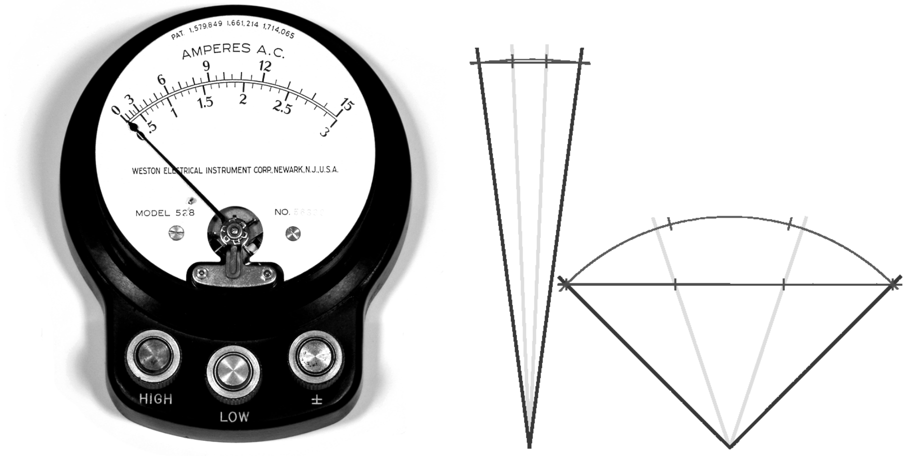
Een aantal van deze vragen zijn teruggekomen bij het bewijs van het vermoeden van Kepler door Thomas C. Hales van de University of Pittsburgh (met medewerking van zijn leerling Samuel P. Ferguson). Het vermoeden van Kepler — of is het nu de stelling van Hales-Ferguson? — zegt dat de piramide sinaasappels zoals te vinden bij de groentenboer zo dicht mogelijk gestapeld is. Weer spelen computerberekeningen een belangrijke rol in het bewijs. Al riep de afhankelijkheid van de computer minder weerstand op dan dertig jaar eerder, toch zijn de zorgen over de correctheid van het bewijs gebleven.

Hales kondigde zijn bewijs aan in 1998 en diende zes artikelen in bij de *Annals of Mathematics*. Dit tijdschrift vroeg niet minder dan 12 referees om de artikelen en onderliggende computerprogramma's te controleren, maar het lukte ze niet. Zij vonden geen fout, maar de berekeningen waren zo lang en structuurloos dat alles nagaan onpraktisch was, waardoor de referees niet wilden verklaren dat het bewijs zonder fouten was. Dit was een storende impasse. Uiteindelijk publiceerde de *Annals* het 'menselijke gedeelte van het bewijs' en liet een deel van het computerwerk achterwege. Het volledige bewijs verscheen in de zomer van 2006 in *Discrete and Computational Geometry*. Het is interessant dat Hales vanaf toen zijn aandacht is gaan richten op het *controleren* van bewijzen met behulp van de computer.

In het geval van een ander bewijs dat berucht is om zijn omstredenheid hebben computers er niets mee te maken. In de jaren vijftig begon men te proberen alle mathematische objecten bekend als eindige enkelvoudige groepen te classificeren; de classificatie berust op een bewijs dat groepen in vijf bekende categorieën zijn in te delen. Aan het begin van de tachtiger jaren dachten de organisatoren van het project dat het bewijs nagenoeg af was, maar het stond verspreid in zo'n 500 publicaties van in totaal minstens 10.000 pagina's. Drie hoofdauteurs namen het herzien en vereenvoudigen van het bewijs op zich, met als doel de hoofdlijnen in een serie artikelen samen te brengen. Deze onderneming, die nog niet af is, loopt aan tegen de grenzen van wat mensen aankunnen — en tegen de menselijke levensduur (een van de drie leiders van het project is in 1992 overleden).

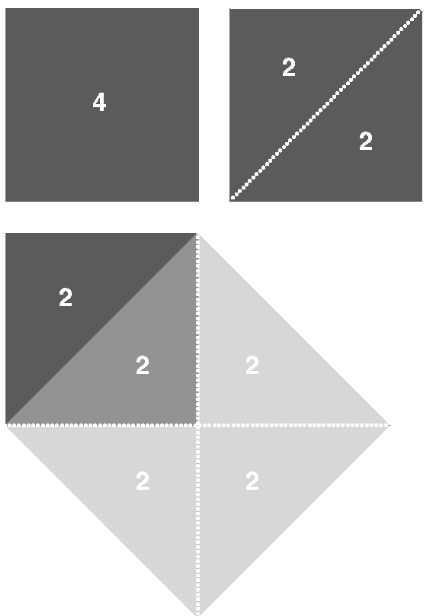
Terwijl sommige bewijzen te lang zijn om te bevatten, zijn andere weer te beknopt en cryptisch. Vier jaar geleden kondigde de Russische wiskundige Grigory Perelman een bewijs van het Poincarévermoeden aan. Dit vermoeden zegt — ik parafraseer nu Christina Sormani van Lehman College — dat als een klodder slijm zich uit iedere lasso die je eromheen gooit weet te wurmen, dan is die klodder niets anders dan een vervormde bol, zonder gaten of handvaten. In het dagelijks leven komen wij dit vaak tegen bij twee-dimensionale objecten ingebed in de drie-dimensionale ruimte, en het vermoeden was al enige tijd geleden bewezen voor oppervlakken (of variëteiten) van dimensie vier of meer. Het moeilijke geval was dimensie drie, en Perelman heeft het opgelost door het algemenere vermoeden van Thurston te bewijzen.

Het bewijs van Perelman leest niet gemakkelijk. Zoals Sormani het uitlegt, bestaat zijn strategie uit "de klodder opwarmen, hem laten zingen, hem uitrekken als gesmolten kaas, en daarna in een miljoen stukjes hakken". De levendigheid van deze omschrijving stel ik zeer op prijs, maar toch helpt hij mij niet bij het volgen van Perelmans logica. Gezien



Figuur 1 Voor het tekenen van schalen op meetinstrumenten zoals ampèremeters is soms trisectie van hoeken nodig om te interpoleren tussen grote waarden. De trisectiemethode van de auteur bestond uit het spannen van een koord over de hoek en die in drie gelijke stukken delen. Het resultaat is een benadering die goed is voor kleine hoeken maar duidelijk slecht voor grotere hoeken. In het plaatje rechts is het resultaat grijs, terwijl de correcte hoeken met kleine streepjes op de boog aangegeven zijn. De meter links is uit de tijd dat de auteur zijn trisecties uitvoerde, maar is niet door de auteur gedaan. Het vertoont tekenen van een meer geavanceerd algoritme.

de moeilijkheid van Perelmans bewijs hebben anderen er veel langere versies van gepubliceerd, waarin het wordt uitgelegd en aangevuld. Dit zijn geen popularisaties voor een groot publiek; ze zijn bedoeld om de wiskunde uit te leggen aan wiskundigen. Dit leidde tot een controverse. Willen deze andere mensen delen in de roem? *Verdienen* ze een aandeel? In augustus 2006 werd de Fields Medaille, de grootste prijs in de wiskunde,



Figuur 2 Verdubbeling van het vierkant. Het verdubbelen van het vierkant is een bewijs dat aan een jonge slaaf wordt geleerd in de *Meno* van Plato. Een vereenvoudigde versie begint met een vierkant met zijden 2 en oppervlakte 4, deelt deze langs de diagonaal, en maakt weer een nieuw vierkant op die diagonaal. De gelijkbenige driehoek die de helft van de oppervlakte van het kleinere vierkant voorstelt is ook een kwart van het oppervlakte van het grotere vierkant, dus de oppervlakte is verdubbeld.

toegekend aan Perelman. Mogelijk heeft dit een eind gemaakt aan de controverse. (Perelman heeft, zoals bekend, de prijs geweigerd.)

Crisis

Deze en soortgelijke gebeurtenissen hebben ertoe geleid dat men is gaan spreken van een crisis in de wiskunde, en tot de vrees dat wij niet meer op bewijzen kunnen vertrouwen om eeuwige en ontwijfelbare waarheid te verkrijgen. Al in 1972 schreef Philip J. Davis van Brown University:

> The authenticity of a mathematical proof is not absolute but only probabilistic . . .Proofs cannot be too long, else their probabilities go down, and they baffle the checking process. To put it another way: all really deep theorems are false (or at best unproved or unprovable). All true theorems are trivial.

Een paar jaar later stelde Morris Kline in *Mathematics: The Loss of Certainty* wiskunde voor als een wankelende megakolos met ondeugdelijke balken en een afbrokkelend fundament; doorgaand op deze bouwkundige vergelijking, betoogde hij dat "bewijzen eerder de voorgevel dan de ondersteunende zuilen van de wiskundige structuur zijn".

Davis en Kline schreven als wiskundig ingewijden — als leden van de club, zij het wel beeldenstormers. Daarentegen liet Johan Horgan zich kennen als een uitdagende buitenstaander toen hij in 1993 een verhandeling schreef in de *Scientific American* met de titel 'The Death of Proof'. "De twijfels die het moderne denken doen schudden hebben eindelijk ook de wiskunde besmet," zei hij. "Mogelijk zullen wiskundigen eindelijk ook gedwongen worden om te aanvaarden wat vele wetenschappers en filosofen al erkend hebben: hun beweringen zijn slechts voorwaardelijk waar, waar totdat bewezen wordt dat ze fout zijn."

Mijn eigen positie als waarnemer van deze gebeurtenissen zit ergens tussen deze twee in. Ik ben zeker geen wiskundige, maar ik loop als journalist al zolang mee in de wiskundige gemeenschap dat ik niet kan beweren onverschillig of onpartijdig te zijn. Ik rapporteer vanuit het niemandsland tussen de fronten.

Ik geloof dat er inderdaad een crisis aan de gang is, maar alleen omdat de hele geschiedenis van de wiskunde bestaat uit de ene crisis na de andere. De fundamenten zijn altijd al aan het afbrokkelen, en de barbaren staan altijd al voor de poort. Toen Haken en Appel hun met hulp van een computer verkregen bewijs publiceerden was het echt niet de eerste keer dat een technische vernieuwing een controverse veroorzaakte. In de 17e eeuw, toen algebraïsche methoden voor het eerst gebruikt werden in de meetkunde, spraken de erfgenamen van de Euclidische traditie er schande van. (Hobbes was er één van.) En toen David Hilbert aan het einde van de 19e eeuw voor het eerst niet-constructieve bewijzen gebruikte, en in feite zei "Ik weet dat x bestaat, maar ik kan je niet vertellen waar je hem kunt vinden", was er weer een opstand. Volgens een criticus: "Dit is geen wiskunde. Dit is godgeleerdheid."

Vergelijkenderwijze lijkt de huidige crisis nogal mild vergeleken met die van een eeuw geleden, toen paradoxen in de verzamelingenleer Gottlob Frege deden verzuchten "Helaas, de arithmetiek wankelt". Als antwoord op die crisis besloot een groep ambitieuze wiskundigen onder leiding van Hilbert een reddingsactie op te zetten en de wiskunde opnieuw op te bouwen op een stevig fundament. Het plan van Hilbert was om het proces van bewijzen toe te passen op het bewijzen zelf en te laten zien dat de axioma's en stellingen in de wiskunde nooit tot een tegenspraak kunnen leiden — dat men niet zowel 'x' als 'niet x' kan bewijzen. Het gevolg is bekend: Kurt Gödel bewees in plaats hiervan dat als je consequent wilt blijven, er beweringen zijn die waar zijn maar niet bewezen kunnen worden. Je zou verwachten dat zo'n Toren van Babel-achtige ramp de verschillende stammen van wiskundigen voor generaties terneer zou slaan, maar de wiskundigen gingen gewoon door met hun werk.

Het lijkt mij volstrekt niet vreemd dat een aantal recente bewijzen aan de grenzen van de wiskunde ingewikkeld zijn en gebruik maken van nieuw gereedschap. *Natuurlijk* zijn deze bewijzen moeilijk te doorgronden; ze waren ook moeilijk te bedenken. Het zijn oplossingen voor problemen waar briljante geesten zich al tientallen of honderden jaren op kapot bijten. Als ik niet in staat blijk het bewijs van Perelman te doorgronden is dit een teleurstelling maar geen verrassing. (Ik kan Olympische marathonlopers ook niet bijhouden.) Als ik mij zorgen maak over de wiskunde op dit moment is het niet de onnavolgbaarheid van de diepste denkers. Het is eerder over mijn eigen onhandigheid als ik alledaagse problemen aanpak, die ver af liggen van de grenzen van wetenschap.

Hoe zit het nu?

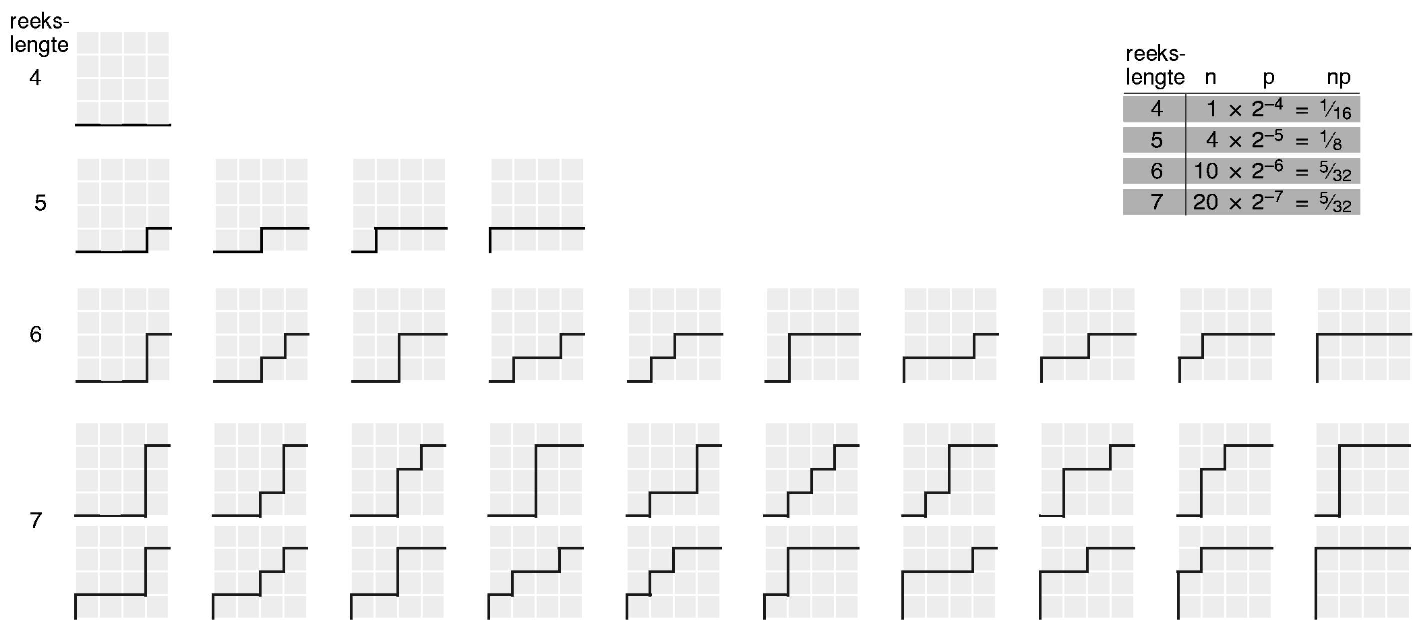
Donald E. Knuth schreef ooit een opmerking bij een computer programma: "Pas op voor bugs in dit computerprogramma; ik heb slechts bewezen dat het werkt, maar het niet uitgeprobeerd." Als Knuth dit schrijft weet je dat de waarschuwing een grapje is, maar als ik het zou zeggen, kun je het beter wel serieus nemen.

Laten wij even teruggaan naar Socrates en zijn jonge slaaf voor een beetje kansrekening. Zij hebben het over sport: wat is in een best-of-seven reeks (zoals de World Series bij honkbal), de kans dat de zaak beslist wordt doordat een team vier wedstrijden achter elkaar wint? We nemen aan dat de teams even sterk zijn, zodat ieder team kans $1/2$ heeft om iedere wedstrijd te winnen.

Socrates: Op hoeveel manieren kan een team vier wedstrijden achter elkaar winnen in een best-of-seven reeks?
Jongen: Maar op één manier. Je moet vier keer achter elkaar winnen, zonder verlies.
Socrates: En op hoeveel manieren kunnen wij een reeks van vijf wedstrijden krijgen met vier keer winnen en één keer verliezen?
Jongen: Nou, je kunt de eerste, tweede, derde of vierde wedstrijd verliezen en de rest winnen.
Socrates: Waarom kun je de laatste wedstrijd dan niet verliezen?
Jongen: Als je de eerste vier wint behoef je geen vijfde wedstrijd meer te spelen.
Socrates: Dus om een reeks van vijf te maken nemen wij een reeks van vier en voegen wij een verloren wedstrijd toe op iedere plaats behalve de laatste, is dat het?
Jongen: Zoiets.
Socrates: Dus kunnen we een reeks van zes maken door met eentje van vijf te beginnen en een verloren wedstrijd toe te voegen op ieder van de vijf posities. Dan zijn er dus 4×5, ofwel 20, reeksen van zes wedstrijden.
Jongen: Als jij het zegt.
Socrates: Die 20 reeksen van zes kunnen we op zes verschillende manieren uitbreiden tot een reeks van zeven, dus er zijn 120 variaties van zeven uitkomsten mogelijk. Als we alles optellen krijg we $1 + 4 + 20 + 120$ gevallen, totaal dus 145. Precies eentje hiervan is het geval dat wij zoeken, dus de kans is $1/145$.

Hier aangekomen zegt de jongen, die enig vestand heeft van honkbal, dat van de 98 best-of-seven World Series er 19 gewonnen zijn met vier keer winnen achter elkaar, wat suggereert dat de empirische kans eerder $1/5$ is dan $1/145$. Socrates raakt niet van zijn stuk door dat feit.

Socrates: Laat je niet afleiden door de schijn; wij bestuderen hier het *ideale* honkbal. Laat ik het nog eens uitleggen, op een andere manier.
Jongen: Kom maar op.
Socrates: Neem eens even aan dat de teams altijd alle zeven wedstrijden uitspelen. Aangezien iedere wedstrijd twee mogelijke uitkomsten heeft zijn er 2^7, oftewel 128 mogelijke uitkomsten. Haal nu uit die 128 uitkomsten diegene waar het spelen doorgaat nadat een team al vier keer gewonnen heeft. Dan zijn er nog zeventig verschillende patronen over. In twee van deze gevallen heeft een team vier wedstrijden achter elkaar gewonnen, een keer voor ieder team. De kans is dus $1/35$.
Jongen: U komt in de buurt. Probeer dit eens: De kans om vier wedstrijden achter elkaar



reeks-lengte	n	p		np
4	1	× 2^{-4}	=	$1/16$
5	4	× 2^{-5}	=	$1/8$
6	10	× 2^{-6}	=	$5/32$
7	20	× 2^{-7}	=	$5/32$

Figuur 3 Mogelijke uitkomsten bij de *World Series*. De honkbal World Series leidt tot een probleem dat het beste via wiskundige analyse begrepen kan worden, maar waarvoor deze weg niet de zekerste is naar een juist antwoord. De World Series is een best-of-seven serie, die eindigt zodra een van de teams vier wedstrijden gewonnen heeft. Uitgaande van even sterke teams, wat is de kans dat de serie vier, vijf, zes of zeven wedstrijden zal duren? Een serie kan voorgesteld worden als een pad over een vier-bij-vier rooster; we beginnen linksonder, een gewonnen wedstrijd voor een van de teams geeft een stap naar rechts, en een gewonnen wedstrijd voor het andere team geeft een stap omhoog. De 35 gevallen hierboven zijn alle gevallen waarin het 'rechts' team wint. Het is belangrijk om de gevallen goed te tellen en een gewicht te geven dat afhangt van de mogelijkheden. Bijvoorbeeld, aangezien het 'rechts' team iedere wedstrijd met kans $1/2$ wint is de kans op een bepaalde rij uitkomsten 2^{-5}, ofwel $1/32$; er zijn vier wedstrijden, dus de kans dat 'rechts' in vijf keer wint is $1/8$. De foute manieren van redenering in de tekst tellen verkeerd of nemen aan dat alle gevallen dezelfde kans hebben. Dit soort blunders vermijden is waarschijnlijk gemakkelijker met een computersimulatie, maar zo'n simulatie verklaart de uitkomsten niet. De getallen 1, 4, 10 en 20 zijn binomiaalcoëfficiënten. (Deze verschijnen natuurlijk bij toepassing van enige elementaire kansrekening, maar *daar* gaat het in dit artikel juist *niet* om. (red.))

te winnen is $1/2 \times 1/2 \times 1/2 \times 1/2$, oftewel $1/16$. Aangezien ieder van de teams vier wedstrijden achter elkaar kan winnen is de kans $1/16 + 1/16 = 1/8$.

Deductieve logica heeft hier geleid tot drie verschillende antwoorden, waarvan er minstens twee fout moeten zijn. Al heb ik in deze ‘comedy of errors’ Socrates de rol van dwaas laat spelen, ik moet toegeven dat de fouten van mij zelf zijn. Een paar jaar geleden maakte ik deze berekening en kreeg ik een verkeerd antwoord. Hoe wist ik dat mijn antwoord fout was? Het klopte niet met een eenvoudig computerexperiment: een programma dat een miljoen World Series simuleerde en 124.711 keer uitkwam op een serie waarin een team vier keer achter elkaar won. (Dat is bijna precies $1/8$.)

Wat betekent het dat ik meer geloof in de uitkomst van een computerprogramma dan in mijn eigen redenering? Welnu, ik beweer niet dat computersimulaties superieur zijn aan bewijzen of betrouwbaarder zijn dan logica. Er is niets mis met klassieke wiskunde. Alledrie de manieren van aanpak in mijn pseudo-Socratische dialoog zullen de juiste uitkomst geven, mits ze zorgvuldig toegepast worden. Maar bewijs is een hulpmiddel dat ook kan bewijzen dat je een dwaas bent.

Degenen die menen nooit zo’n fout te kunnen maken feliciteer ik, maar ik herinner ze ook aan de affaire met het beruchte drie-deuren-probleem. In 1990 schreef Marilyn vos Savant, een columniste van het tijdschrift *Parade*, een stuk over het drie-deuren-probleem. Stel, in een spelshow sta je voor drie gesloten deuren. Achter één van die deuren zit een prijs. Als de speler deur 1 kiest, opent de quizmaster deur 3, waar niets achter staat, en geeft hij de speler alsnog de kans om deur 2 te kiezen in plaats van deur 1. Vos Savant beredeneerde (correct, onder bepaalde aannames) dat je door te veranderen je kans van $1/3$ vergroot naar $2/3$. Duizenden waren het hier niet mee eens, waaronder een behoorlijk aantal wiskundigen. Zelfs Paul Erdös, een grote kansrekenaar, had het fout. Uiteindelijk werd hij overtuigd door een computersimulatie.

Bewijs

In een rechtszaak wordt er een bewijs gezocht ‘buiten gerede twijfel’, maar wiskunde vraagt meer. In een traditie die teruggaat op Euclides, wordt een bewijs gezien als een garantie van onfeilbaarheid. Het is het vlammende zwaard van een schildwacht die waakt over gepubliceerde wiskunde en die alle onwaarheden buitensluit. En de wiskundeliteratuur heeft *inderdaad* bewaking nodig. Als je wiskunde ziet als een formeel systeem van axioma’s en stellingen, dan is de structuur gevaarlijk kwetsbaar. Laat ook maar één foute stelling toe, en je kunt iedere onzinnigheid bewijzen die je maar wilt.

De speciale status van wiskundige waarheid, waarin dit vak verschilt van andere kunsten en wetenschappen, wordt nog steeds door veel wiskundigen gekoesterd, maar het bewijzen speelt ook andere rollen. Het is niet alleen een zegel van goedkeuring. Het boek *Proofs and Confirmations* van David Bressoud geeft naar mijn mening de beste insider’s kijk op wat het betekent om wiskunde te bedrijven. Bressoud benadrukt dat de belangrijkste functie van het bewijs niet is het bepalen of iets waar is (of niet), maar het duidelijk maken *waarom* iets waar is. “De zoektocht naar een bewijs is de eerste stap in de zoektocht naar begrip”.

En natuurlijk, wiskunde is meer dan alleen stellingen en bewijzen. Een belangrijke tak die zich experimentele wiskunde noemt doet het erg goed op dit moment. Er zijn tijdschriften en congressen gewijd aan dit onderwerp, en een tweetal boeken van Jonathan Borwein en David Bailey fungeren als grondleggend op dat gebied. Niet dat experimentele wiskundigen bewijzen willen opgeven of afschaffen, maar ze willen andere activiteiten een belangrijkere rol laten spelen: spelen met voorbeelden, vermoedens uitspreken, berekeningen doen.

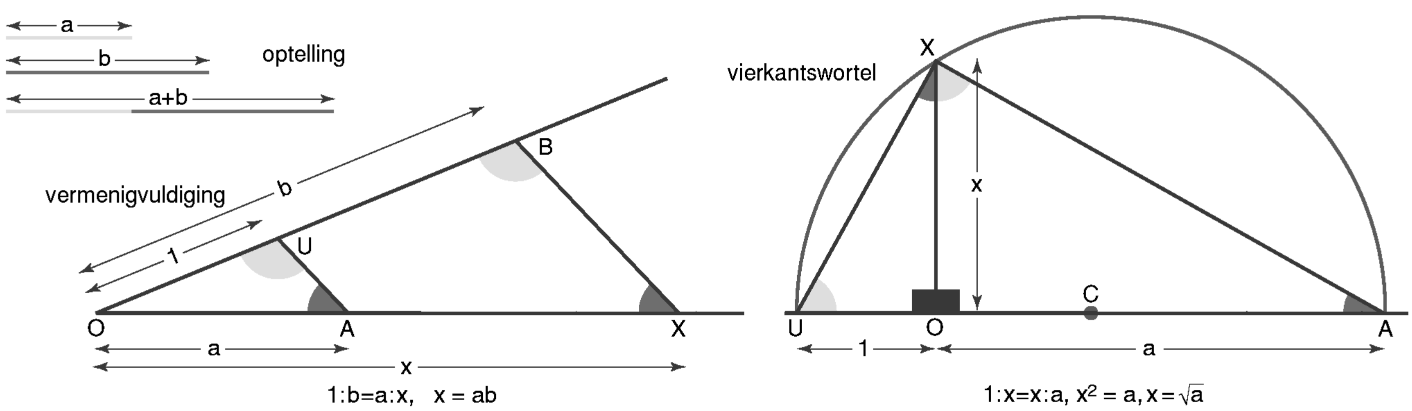
Toch zijn er ideeën waar niemand op gekomen zou zijn anders dan via het denkproces dat wij bewijzen noemen. En dat brengt me terug bij het in drieën delen van hoeken.

De stelling van Wantzel

Het feit dat trisectie onmogelijk is, is alom bekend, maar de reden waarom, de inhoud van het bewijs, is minder bekend. Veel auteurs noemen het, maar weinigen leggen het uit. Zelfs Underwood Dudley’s schitterende verzameling wiskundige ‘cranks’, *A Budget of Trisections*, geeft niet het bewijs stap voor stap.

De oorsprong en geschiedenis van het bewijs is ook nogal vaag. Dat is een les voor diegenen die onsterfelijk willen worden door een belangrijke stelling uit de wiskunde te bewijzen. Trisectie stond bijna tweeduizend jaar lang bovenaan de lijst van meestgezochte bewijzen, en toch heeft de auteur van het eerste gepubliceerde bewijs van de onmogelijkheid ervan geen plaats gekregen in de rij beroemde wiskundigen.

De auteur was de Franse wiskundige Pierre Laurent Wantzel (1814–1848), wiens naam zeer onbekend is, zelfs in wiskundige kringen. Zijn bewijs verscheen in 1837. Voor zover



Figuur 4 Constructies met passer en liniaal. Euclidische constructies met passer en liniaal leveren vijf arithmetische operaties: optellen, aftrekken, vermenigvuldigen, delen en worteltrekken. Optellen is gewoon het achter elkaar leggen van lijnstukken, aftrekken is het omgekeerde. Vermenigvuldigen houdt in dat gelijkvormige driehoeken gemaakt worden waarvan de zijden de verhoudingen $1 : b = a : x$ voorstellen, dus x is het product van a en b. Delen is weer het omgekeerde. Voor worteltrekken worden gelijkvormige driehoeken in een cirkel ingeschreven, met zijden met verhoudingen $1 : x = x : a$, zodat $x^2 = a$, en de lengte van het lijnstuk x gelijk is aan de wortel van a. *Alleen* deze vijf operaties zijn mogelijk; het is onmogelijk om derdemachtswortels te trekken, wat van belang is bij het bewijzen dat trisectie onmogelijk is.

ik weet, is het nooit herdrukt en ook nooit in het Engels vertaald. (Ik heb zelf een poging tot een vertaling op de website van de *American Scientist* gezet). Veel citaties van het artikel geven een verkeerd volumenummer, wat de indruk wekt dat sommigen die ernaar verwijzen het zelf niet gelezen hebben. En om het nog erger te maken, het artikel zelf geeft een verkeerde spelling voor de naam van de auteur: Hij staat vermeld als 'M.L. Wantzel'.

Een van de redenen voor de onbekendheid van Wantzel kan zijn dat zijn bewijs bijna niet te begrijpen is voor de moderne lezer. Later werden er duidelijkere verklaringen geschreven. Felix Klein, L.E. Dickson en Robert C. Yates publiceerden allemaal hun eigen versie van het bewijs; dat deed Willard Van Orman Quine ook, als antwoord op een 100 dollar prijsvraag. Voor een uitgebreid en leesbaar bewijs raad ik het boek *Abstract Algebra and Famous Impossibilities* van Arthur Jones, Sidney A. Morris en Kenneth R. Pearson aan.

Als boetedoening voor mijn jeugdige carrière als trisecteur zal ik nu proberen in het kort het bewijs van de onmogelijkheid ervan te geven. De hoofdvraag is: wat kun je met passer en liniaal doen? Natuurlijk kun je ermee lijnen en cirkels tekenen, maar je kunt er ook mee rekenen. Als de lengte van een lijnstuk een getal voorstelt, kun je met passer en liniaal met zulke getallen optellen, aftrekken, vermenigvuldigen en delen, en zelfs worteltrekken. Stel dat je begint met een lijnstuk van lengte 1, welke andere getallen kan je hieruit voortbrengen? De gehele getallen zijn gemakkelijk, breuken ook. Wortels leiden tot een aantal irrationale getallen; door herhaaldelijk wortel te trekken kun je ook vierdemachtwortels, achtstemachtwortels trekken, enzovoorts. Maar *meer* kun je niet. Je kunt geen derdemachtswortels, vijfdemachtswortels, of welke wortel dan ook trekken die geen macht van twee is — wat het cruciale punt is bij trisectie.

De trisectiesprocedure zou gegeven een hoek θ een hoek $\theta/3$ dienen op te leveren. Aangezien de methode voor iedere hoek moet werken kun je de onmogelijkheid bewijzen met een enkel tegenvoorbeeld. Het standaardvoorbeeld is de hoek van 60 graden met hoekpunt in de oorsprong en een zijde langs de positieve x-as. Om deze hoek in drieën te delen zou je een lijn moeten trekken door de oorsprong die een hoek van 20 graden maakt met de x-as.

Om een lijn te tekenen heb je genoeg aan twee punten op die lijn. In dit geval heb je al een punt, de oorsprong. De hele trisectie komt dus neer op het vinden van een punt ergens op de gezochte lijn. Dat kan toch niet moeilijk zijn? Er liggen immers oneindig veel punten op die lijn, en wij hebben er maar eentje van nodig. Maar het bewijs laat zien dat het niet kan.

Om de oorsprong van het probleem te zien gebruiken wij goniometrie. Als we de sinus en cosinus van 20 graden kenden was het probleem opgelost; dan konden wij de punten $x = \cos 20$ en $y = \sin 20$ construeren. Wij hebben dan natuurlijk wel de exacte waarden nodig, benaderingen van een rekenmachine of tabel zijn niet goed genoeg. We kennen *wel* de sinus en cosinus van 60 graden: dat zijn $\sqrt{3}/2$ en $1/2$. Beide getallen kun je met passer en liniaal construeren. We hebben ook formules die de sinus en cosinus van een willekeurige hoek θ geven als functie van de sinus en cosinus van $\theta/3$. Deze formules geven de volgende vergelijking, waar we $\cos\theta/3$ voor het gemak vervangen hebben door u:

$$cos\theta \ = 4u^3 - 3u\,.$$

Voor de hoek van 60 graden, met $\cos\theta = 1/2$, wordt deze vergelijking $8u^3 - 6u = 1$. Dit is een derdegraadsvergelijking. En daar ligt de kern van het probleem: met optellen, aftrekken, vermenigvuldigen, delen en worteltrekken alleen kunnen wij deze vergelijking niet oplossen. (Het lastige deel van het bewijs, waar ik mij niet aan waag, toont aan dat de derdegraadsvergelijking niet herleid kan worden naar eentje van lagere graad.)

Dit bewijs, met zijn gebruik van goniometrie en algebra, zou wartaal zijn geweest voor Euclides, maar de conclusie kan eenvoudig naar meetkunde vertaald worden: Geen enkel punt op de lijn die een hoek van 20 graden met de x-as maakt (afgezien van de oorsprong) kan met passer en liniaal geconstrueerd worden uitgaande van de lijn die een hoek van 60 graden maakt. Dit resultaat is vreselijk tegenintuïtief. De twee lijnen liggen in hetzelfde vlak; ze snijden elkaar zelfs, en toch 'communiceren' ze niet met elkaar: je kunt niet van de één naar de ander komen. Net als Hobbes zou ik dit niet geloofd hebben, als niet het bewijs me ertoe zou dwingen. Ik vraag mij af of het mijn oude vriend Dmytro zou overtuigen.

Referenties

1 K. Appel, W. Haken, 'The four color proof suffices' *The Mathematical Intelligencer* **8**(1) (1986), pp. 10–20.

2 J. Aubrey, 'Brief Lives, *Chiefly of Contemporaries, Set Down by John Aubrey, between the years 1669 & 1696*, edited by Andrew Clark, The Clarendon Press, Oxford, 1898.

3 J. Borwein, D. Bailey, *Mathematics by Experiment: Plausible Reasoning in the 21st Century*, Natick, Mass.: A.K. Peters, 2004.

4 D.M. Bressoud, *Proofs and Confirmations: The Story of the Alternating Sign Matrix Conjecture*, 1999.

5 P.J. Davis, 'Fidelity in mathematical discourse: Is one and one really two?' *American Mathematical Monthly* **79**(3), pp. 252–263,1972.

6 L.E. Dickson, 'Why it is impossible to trisect an angle or to construct a regular polygon of 7 or 9 sides by ruler and compasses' *Mathematics Teacher* (14) (1921), pp. 217–218.

7 U. Dudley, *A Budget of Trisections*, Springer-Verlag, New York, 1987.

8 M. Gardner, 'Mathematical games: The persistence (and futility) of efforts to trisect the angle' *Scientific American* **214**(6) (1966), pp. 116–122.

9 T.C. Hales, 'A proof of the Kepler conjecture' *Annals of Mathematics* (162) (2005), pp. 1065–1185 en *Discrete & Computational Geometry* (36) (2005), pp. 1–265.

10 J. Horgan, 'The death of proof' *Scientific American* **269**(4) (1993), pp. 92–103.

11 D.M. Jesseph, *Squaring the Circle: The War Between Hobbes and Wallis*, University of Chicago Press, Chicago, 1999.

12 A. Jones, S.A. Morris and K.R. Pearson, *Abstract Algebra and Famous Impossibilities*, Springer-Verlag, New York, 1991.

13 F. Klein, *Famous Problems of Elementary Geometry: The Duplication of the Cube, the Trisection of an Angle; the Quadrature of the Circle*, Ginn, Boston, 1897.

14 M. Kline, *Mathematics: The Loss of Certainty*, Oxford University Press, New York, 1980.

15 W.V. Quine, 'Elementary proof that some angles cannot be trisected by ruler and compass' *Mathematics Magazine* **63**(2) (1990), pp. 95–105.

16 C. Sormani, *Hamilton, Perelman and the Poincare conjecture* comet.lehman.cuny.edu /sormani/others/perelman/introperelman.html

17 M.L. Wantzel, 'Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas' *Journal de Mathématiques Pures et Appliquées* (2) (1837), pp. 366–372.

18 R.C. Yates, *The Trisection Problem.*, Franklin Press, Baton Rouge, 1942.