De komst van krachtige computers heeft het mogelijk gemaakt om allerlei wiskundige vermoedens te verifiëren Maar zo'n check is niet hetzelfde als een bewijs. Als je voor grote aantallen gevallen een wiskundig vermoeden bevestigd hebt gezien, waarvoor heb je het bewijs nog nodig? In de wiskunde is het Vermoeden van Goldbach nog steeds niet bewezen. Het was in 2006 positief bevestigd voor ongeveer de eerste 4.10^{18} getallen. In de natuurkunde zou men in zo'n geval allang over de *Wet* van Goldbach spreken. Hoe zit het met het vertrouwen in zo'n vermoeden dat alsmaar bevestigd lijkt te worden? Kun je zulke vermoedens niet toch op een of andere manier gebruiken? Binnen de wiskunde? Erbuiten? En hoe? Trouwens, wat is nu eigenlijk een bewijs? In dit artikel discussiëren **Manuel Nepveu** en **Nico Krijn** over deze vragen.

Wiskundige bewijzen

Manuel: Op de middelbare school, lang, lang geleden werd nog planimetrie gegeven. Het leerboek had typisch de structuur van 'Stelling, gegeven, te bewijzen, bewijs, stelling, gegeven, te bewijzen, bewijs, enzovoort'. Je leerde allerlei stellingen uit de axioma's af te leiden. En het was een sport om een bewijs te vinden. Er kwam uiteraard niet aan de orde dat op de geleverde bewijzen behoorlijk wat aan te merken was. Wat verstaan we onder een *correct* bewijs? Badinerend zou ik zeggen: vermoedelijk iets van grote lengte... Tijdens mijn studie sterrenkunde werd duidelijk gemaakt dat veel resultaten in het leerboek analyse weliswaar aannemelijk waren, maar strikt genomen niet *bewezen*. Het boek zou volgens de docent dan vier keer zo dik worden. Trouwens, *waarom* bewijzen we? Dat wil zeggen, wat betekent een bewijs voor ons? Misschien wat veel vragen ineens, maar ik ben benieuwd naar je antwoord.

Nico: Christian Goldbach vertrok in 1728 naar Moskou om leraar te worden van Peter de Grote en zijn familie. Hij onderhield schriftelijk contact met zijn oude wiskundige vrienden. In 1742 schreef hij een brief aan Leonhard Euler met daarin zijn beroemde Vermoeden dat elk positief even getal groter of gelijk aan vier de som is van twee priemgetallen[1]. Euler had vertrouwen in het Vermoeden. Hij schreef terug aan Goldbach: "Het theorema [...] beschouw ik als helemaal zeker, ondanks dat ik het niet kan bewijzen".

De Engelse wiskundige Edward Waring was de eerste die het Vermoeden publiceerde. Het verscheen in 1770 in zijn *Meditationes algebraicae*. Hiernaast is het Vermoeden afgebeeld voor de even getallen 4 tot en met 28. Sommige getallen kennen meerdere oplossingen. Zo is 26 te schrijven als 13 + 13, als 19 + 7 en ook als 23 + 3. Hoe groter de getallen worden, hoe lastiger het wordt om geschikte priemgetallen te vinden. In 1855 heeft Adolphe Desboves berekend dat het Vermoeden waar is voor $n < 10^4$.

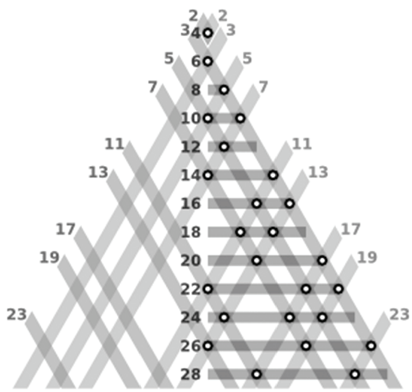

fig. 1 Vermoeden afgebeeld voor de even getallen 4 tot en met 28.

Vijfduizend getallen had hij met de hand omgezet in de som van twee priemgetallen. Geen peulenschil! In 2006 is met de computer berekend dat het Vermoeden klopt tot $n < 4.10^{18}$. En het blijft maar goed gaan: er is niet één tegenvoorbeeld gevonden. Een tegenvoorbeeld zou een positief even getal zijn dat nièt de som is van twee priemgetallen. Zo'n enkel tegenvoorbeeld zou het hele theorema van tafel vegen. Je zou denken dat zo'n enorme hoeveelheid experimentele gegevens die het Vermoeden bevestigen vertrouwen oplevert.

Maar hoeveel paren priemgetallen er ook gevonden worden, het Vermoeden zal niet als gevestigd worden beschouwd zolang er geen analytisch bewijs is geproduceerd. Bewijzen worden immers beschouwd als de 'gouden standaard' van de wiskundige waarheid. Tot op de dag van vandaag is het Vermoeden van Goldbach niet bewezen. Hoe groter de onderzochte getallen worden, des te meer mogelijkheden er ontstaan een getal te schrijven als de som van twee getallen. De kans op ten minste één paar priemgetallen wordt dus steeds groter. In figuur 2 is de toename van mogelijkheden bij groter wordende getallen duidelijk te zien. Uiteraard komt deze heuristische benadering niet eens in de buurt van een informeel bewijs van het Vermoeden, maar toch…

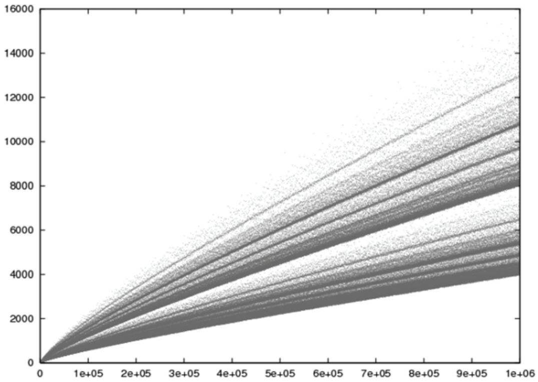

fig. 2 Het aantal manieren waarop een even getal n als de som van twee priemgetallen kan worden geschreven, met $4 \leq n \leq 10^6$.

Manuel: Maar wat is een correct bewijs eigenlijk? Dat is niet zo gemakkelijk aan te geven. Welke standaard is er?

Nico: Een bewijs wordt als correct beschouwd als de wiskundige gemeenschap het er unaniem over eens is. Meer kun je er volgens mij niet van maken. De praktijk van het bewijzen is weerbarstig; bewijzen zijn in de loop der tijd steeds complexer geworden. Zelfs zodanig, dat een individuele wiskundige het soms niet meer kan overzien. Tegenwoordig controleert men bewijzen met behulp van de computer. Freek Wiedijk van de Radboud Universiteit stelt: “Nu zijn computerbewijzen nog een soort kunst omwille van de kunst. Maar ik ben ervan overtuigd dat het de toekomst van de wiskunde wordt. Over enkele decennia zullen wiskundigen blij zijn met de computer als bewijsverificator” (Mols, 2009).

Manuel: Maar dan is er dus toch iets meer te vertellen over de standaard voor een correct bewijs... meer dan alleen maar de unanimiteit van een werkgemeenschap. Overigens is de bewijstechniek de afgelopen eeuwen veel veranderd. Een Fransman als Augustin-Louis Cauchy (1789-1857) bracht een nauwkeurigheid in die geheel nieuw was. Zijn strakke bewijzen voor allerlei stellingen uit de analyse getuigen daarvan. Hij ging bijvoorbeeld heel precies en formeel om met continuïteit van functies en limieten. De vraag die je jezelf kunt stellen is of je daar nog verder in kunt gaan. Is het denkbaar dat iemand op een goede – kwade? – dag tot het inzicht komt dat het allemaal nog rigoureuzer kan? Bekend is dat L.E.J. Brouwer (1881-1966) alleen constructieve bewijzen accepteerde en het bewijs uit het ongerijmde om die reden niet acceptabel vond. Dit heeft vergaande inhoudelijke consequenties en zijn strengheid werd om die reden ook niet massaal overgenomen. Hier zit een subjectief element in en daarmee de intersubjectiviteit van een wiskundige gemeenschap die een bewijs als zodanig erkent.

Nico: Er komt nog een heel ander verschijnsel om de hoek kijken. Bij het zoeken naar bewijzen gaat men volgens mij voorbij aan onvolledigheidsstellingen van Kurt Gödel. In 1931 toverde hij een bijzonder giftig konijn uit de wiskundige hoge hoed en bewees dat er in elk voldoende rijk formeel systeem stellingen zijn die waar zijn en niet binnen dat systeem bewezen kunnen worden. Het is onmogelijk zo’n Gödelstelling te ontdekken. Tot op heden is het Vermoeden niet bewezen en het zou dus zo’n Gödelstelling kunnen zijn die niet te bewijzen valt. Maar het kan ook betekenen dat we nog niet voldoende goed gezocht hebben. De Hongaarse filosoof Imre Lakatos (1922-1974) heeft daar een uitgesproken mening over. De informele wiskunde lag hem na aan het hart, en hij beschouwde wiskunde niet als een systeem van geaccumuleerde waarheden. De formalistische wiskunde van David Hilbert was volgens Lakatos na Gödels ontdekking een illusie. En dat was volgens hem niet doorgedrongen tot de wiskundige praktijk. Wiskunde kan geen deductieve wetenschap zijn…

fig. 3 Imre Lakatos, professor of logic, omstreeks 1960.

Manuel: Pardon? Nu moet ik je toch echt even onderbreken. De wiskunde houdt zich bezig met haar eigen ‘hersenspinsels’, die in principe niets te maken hebben met ‘matters of fact’, zoals de filosoof David Hume zou zeggen. Maar dan kan de wiskunde volgens mij alleen maar deductief zijn. Feiten uit de waarneembare wereld spelen geen rol en je kunt dus niet anders dan een tak van de wiskunde beoefenen door naar het systeem zelf te kijken. Nou, dan schiet er niets over dan het deductieve element. Wiskunde is een deductieve wetenschap.

Nico: Wacht maar even, ik laat je zien hoe Lakatos daarover dacht. Hij brengt de ontwikkelingsgang van de informele wiskunde in beeld en laat zien hoe het proces vooruitgang boekt. Maar uiteindelijk wordt de informele theorie toch ingebed in de formele axiomatische. In principe is de informele wiskunde dan aangekomen bij een eindstation.

Manuel: Oh, maar dan heb je het over de manier waarop een wiskundige aan vermoedens komt, die hij vervolgens deductief uit het systeem van axioma's wil afleiden. Of zitten we nu langs elkaar heen te praten?

Nico: Daar kom ik op terug. Lakatos is beïnvloed door Karl Popper. Dat is voor de hand liggend, want ze werkten nauw samen: beiden waren verbonden aan de London School of Economics. Popper is van mening dat alle wetenschappelijke kennis feilbaar is. De wetenschappelijke kennis groeit in een proces van *trial and error*. Dat is, we proberen een theorie, kijken of onze problemen er door worden opgelost en gaan na of de theorie bestand is tegen weerleggingen. Als de theorie weerlegd wordt, dan proberen we ze te repareren. Als deze nieuwe theorie niet weerlegd wordt, dan hebben we geen garantie dat de theorie onfeilbaar is, want er kan morgen een tegenvoorbeeld gevonden worden. Volgens Popper boekt wetenschap vooruitgang als oude theorieën worden verworpen en vervangen door nieuwe en betere. Deze theorieën worden opnieuw vervangen door andere, en zo gaat het proces van *trial and error* verder. Volgens Popper kan elke theorie verworpen worden en vervangen door een betere. Er wordt geen waarheid ontdekt in absolute zin, want het vermoeden waarvan we hopen dat het waar is, kan in de toekomst onwaar blijken te zijn. In plaats van waarheid als een maat te kiezen voor de groei van kennis, stelt Popper een andere standaard voor: die van de *benadering* van de waarheid. Hij zegt dat elke nieuwe theorie een betere benadering van de waarheid is dan de theorie die weerlegd is. Door het verbeteren van de theorieën in het licht van de weerleggingen, komen we dichter bij de waarheid – een convergerend realisme.

Manuel: Maar dit gaat over de (natuur)wetenschap. Toch niet over de wiskunde? Je zegt: "...het vermoeden waarvan we hopen dat het waar is, kan in de toekomst onwaar blijken te zijn..." Maar niet als het eenmaal volgens de wiskundige gemeenschap bewezen is, kom nou! Je kunt wel een generalisatie proberen te vinden, maar daarmee is datgene wat je bewezen hebt niet onwaar geworden!

Nico: Nou, volgens Lakatos dus wel! Lakatos stelt dat ook wiskunde ontwikkeld wordt in een proces van vallen en opstaan. Hij ziet geen wezenlijk verschil tussen natuurwetenschap en wiskunde. Zowel in onderwerp als methode komen ze overeen. De mechanicawetten van Newton hebben dezelfde status als de wiskundige stelling van Pythagoras. Lakatos spreekt niet over een benadering van waarheid. Alle wiskundige kennis berust op vermoedens die per definitie feilbaar zijn.

Manuel: Wacht even. De zaak is klaar op het moment dat een vermoeden bewezen is. Dat wil zeggen: het resultaat staat! Jij lijkt aan te geven dat het nog altijd mogelijk zou zijn dat de Stelling van Pythagoras, ondanks dat er talloze bewijzen van bestaan, gewoon foutief zou kunnen zijn. Dat wil zeggen, dat zij toch niet uit de axioma's van de vlakke meetkunde volgt. Of bedoelt Lakatos wat anders? Heeft hij het misschien over het ontwikkelen van vermoedens? Het ontdekken van vermoedens gebeurt inductief, experimenteel, en dat kan zelfs bijna niet anders, zou ik denken. Zo schijnt Gauss voor zijn beroemde priemgetallentheorema eerst heel platvloers te hebben geteld hoeveel priemgetallen er waren kleiner dan N voor N 'groot'. Pas toen hij er vertrouwen in had dat dit aantal asymptotisch als N/ln(N) verloopt is hij het bewijs gaan zoeken. Als Lakatos dat bedoelt...

Nico: Een bewijs van een vermoeden komt veelal moeizaam tot stand. Wanneer we een blik werpen in de aantekeningen van wiskundige grootheden, dan vinden we bladzij na bladzij gevuld met ideetjes en probeersels. Hun zoektocht blijft buiten beeld en alleen het eindresultaat – nauwkeurig geformuleerde ware uitspraken met de bijbehorende bewijzen, gebaseerd op axioma's – verschijnen in gedrukte vorm. De 'experimentele' wiskundige Carl Friedrich Gauss schreef aan János Bolyai in 1808: "Het grootste plezier is niet de kennis, maar het leerproces, niet het bezit maar hoe er te komen".

Het vinden van een bewijs wordt als een eindpunt beschouwd, het wordt gepubliceerd en alle probeersels verdwijnen van het toneel. Bij Lakatos begint het feest dan weer van voren af aan, er komt geen eindresultaat. In zijn boek *Proofs and refutations* (1976) probeert hij dit aan te tonen door de ontstaansgeschiedenis van Leonhard Eulers formule voor een regelmatig veelvlak te analyseren. Deze formule bepaalt de relatie tussen V(ertices), E(dges) en F(aces). Euler publiceerde hem in 1758: er geldt $V - E + F = 2$. Als voorbeeld nemen we een kubus. Dit veelvlak heeft acht hoekpunten, twaalf ribben en zes vlakken, dus $V - E + F = 8 - 12 + 6 = 2$. Later ontdekte men echter dat deze formule niet opgaat voor een geneste kubus: een kubus met daarin een holle kubus. Voor elk van de kubussen geldt de bovenstaande formule, dus voor het geheel geldt $V - E + F = 4$. Naar aanleiding van dit tegenvoorbeeld bracht men een extra voorwaarde aan. Een veelvlak zou convex moeten zijn, zodat geneste veelvlakken erbuiten vallen.

Manuel: Maar dan gaat het spelletje nog verder: de eis van convexiteit kan men proberen af te zwakken. Je kunt als researchwiskundige immers denken dat die eis te streng is. En inderdaad, die is ook te streng.

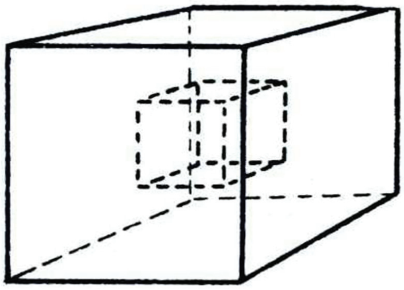

fig. 4 Een kubus met daarin een holle kubus. Er geldt $V - E + F = 4$.

Men kan bij enkelvoudige samenhang van de meetkundige structuur uitkomen, maar dat moet al puzzelend nog wel even ontdekt worden. Idealiter kom je uiteindelijk bij een 'dan en slechts dan' situatie terecht. En dan is de zaak gesloten! Toch? Ook binnen dat afzwakkingstraject zouden ongelukken kunnen gebeuren natuurlijk. Maar wat je hebt gezegd, betekent vooral dat sommige van de bewijzen, voor zover al gegeven, dus gewoon niet deugen. In feite zegt Lakatos dat je maar nooit weet of een bewijs niet toch stiekem een fout bevat.

Nico: Lakatos is ook beïnvloed door George Pólya die de nadruk legt op heuristiek:

> Finished mathematics presented in a finished form appears as purely demonstrative, consisting of proofs only. Yet mathematics in the making resembles any other human knowledge in the making. You have to guess a mathematical theorem before you prove it; you have to guess the idea of a proof before you carry through the details.

Manuel: Dat laatste herken ik wel. Het aardige is overigens dat een bewijs nieuw gereedschap aanlevert dat onderdeel van het wiskundig arsenaal gaat uitmaken. Dat zie je bijvoorbeeld bij de diagonaalprocedure die Georg Cantor gebruikte om de overaftelbaarheid van de reële getallen te bewijzen. Later is deze procedure bijvoorbeeld weer door Gödel gebruikt bij het bewijs van zijn onvolledigheidsstelling (Penrose, 1989). Maar nu even iets anders. Goldbachs Vermoeden is niet bewezen, maar wel getest voor een krankzinnig groot aantal gevallen. Je noemde het al. Een natuurkundige zou geneigd zijn van de experimentele Wet van Goldbach te spreken. Natuurlijk wil je een bewijs, maar desondanks denk ik niet dat er een mathematicus te vinden is die aan de correctheid van het Vermoeden twijfelt. Maar nu even een gedachtenexperiment. Stel, je wilt een bemand ruimteschip naar Mars sturen. Alles is zo'n beetje klaar en als eindverantwoordelijke hoor je – nogal laat – van de ontwerper het volgende: ergens in het besturingssysteem wordt het Vermoeden van Goldbach expliciet gebruikt. En vermoedelijk niet alleen maar voor getallen in het geteste gebied tot 10^{18}. Is het vermoeden onjuist, dan zou het zomaar kunnen dat het ruimteschip onbestuurbaar wordt. Als je deze informatie hebt, stuur je het ruimteschip dan toch, bemand en al, weg?

Nico: Van afgeleide stellingen weet je zeker dat ze waar zijn, zo'n stelling heeft de status van een deductief bepaalde 'wiskundewet'. Met het toepassen van een vermoeden in het besturingssysteem introduceer je een onzekerheid, te vergelijken met die van een inductief ontwikkelde natuurwet. Je loopt dus een risico dat er bij de besturing iets mis kan gaan. Dat risico moet in kaart worden gebracht en er moet worden nagegaan of het aanvaardbaar is. Op vergelijkbare wijze gaat men om met alle andere risico's. De lijm waarmee het hitteschild is gemonteerd kan loslaten bij hoge temperaturen of trillingen. Daar kun je aan rekenen en er een onzekerheid aan toekennen. Wanneer alle risicofactoren onder een bepaalde drempel liggen wordt pas besloten tot een lancering.

Manuel: Inderdaad, het resultaat staat (momenteel) kennistheoretisch op hetzelfde niveau als een experimentele natuurwet. Het is overigens een aardige vraag welke kans je zou toekennen aan de mogelijkheid dat een nog niet getest even getal ook weer een som van twee priemgetallen is. Met de achtergrondinformatie dat het voor zoiets als de eerste 10^{18} even getallen positief is getest en voor geen enkel getal negatief. Ik zou geneigd zijn – maar dat zeg ik enigszins voorzichtig – de 'Rule of Succession' van Pierre-Simon Laplace te gebruiken (Jaynes, 2003). Dan zou die kans maar iets van 10^{-18} van 1 afwijken. Dit is in praktische zin nauwelijks van zekerheid te onderscheiden... Ik zou het ruimteschip op weg sturen, gewoon met een gerust hart. Maar dat alles neemt niet weg dat het bewijs er natuurlijk ooit moet komen, tenzij het een Gödelstelling is natuurlijk.

Manuel Nepveu & Nico Krijn

Literatuur

Jaynes, E.T. (2003). *Probability theory, the logic of science*. Cambridge University Press.

Lakatos, I. (1976). *Proofs and refutations*. Cambridge University Press.

Mols, B. (2009). '*QED zegt de computer*', opgenomen in NRC, 9 januari 2009.

Penrose, R. (1989). *The emperor's new mind, concerning computers, minds and the laws of physics*. Oxford University Press.

Noten

[1] De uitspraak van Goldbach is hier modern geformuleerd. In zijn tijd beschouwde men '1' ook als een priemgetal. Goldbachs Vermoeden geformuleerd in de predicaatlogica is: $\forall x \exists y \exists z\ (x = \text{even} \wedge x \geq 4 \wedge \text{Priem}(y) \wedge \text{Priem}(z)) \leftrightarrow x = y + z$