De kunst van het bewijzen

Freek Wiedijk

In de geschiedenis van de wiskunde zijn er drie revoluties geweest:

- De eerste revolutie was de ontwikkeling van **bewijzen** in de Griekse oudheid. Vóór deze revolutie bestond wiskunde voornamelijk uit *berekeningen* (waarbij we het oplossen van een vergelijking ook als een vorm van het berekenen van een antwoord zien.) Bij berekenen gaat het om het *wat* van een antwoord, terwijl het bij bewijzen om het *waarom* van dat antwoord gaat. Deze Griekse ontwikkeling vond zijn hoogtepunt in *De Elementen* van Euclides, een boek waarin – bewijs na bewijs – de meetkunde systematisch wordt ontwikkeld.

- De tweede revolutie was de ontwikkeling van **rigor** aan het eind van de negentiende eeuw. Daarvoor was wiskunde niet volledig precies. Zo rammelt Euclides' ontwikkeling van de meetkunde als je er met moderne ogen naar kijkt, en ook de ontwikkeling van de infinitesimaalrekening door Isaac Newton en Gottfried Leibniz was niet rigoureus, met referenties naar oneindig kleine grootheden. Eind negentiende eeuw kwam hieraan een eind met de ontwikkeling van ϵ/δ definities van limieten door Augustin Louis Cauchy. Deze ontwikkeling culmineerde in de verzamelingenleer van Georg Cantor en de ontwikkeling van de mathematische logica door Gottlob Frege.

  De meetkunde van Euclides werd voor het eerst rigoureus gemaakt rond de eeuwwisseling door David Hilbert. Een bijzonder fraaie variant hierop werd later ontwikkeld door Alfred Tarski.

- De derde revolutie is de ontwikkeling van praktische **formele** wiskunde. Hierbij wordt wiskunde in de computer gerepresenteerd op een manier dat *alle* details in de computer aanwezig zijn. De computer kan hierdoor de correctheid van de wiskunde volledig mechanisch nagaan. Bij rigoureuze wiskunde is het *in principe* mogelijk om bewijzen volledig precies op te schrijven, maar bij formele wiskunde wordt dit ook *in de praktijk* gedaan. Deze derde revolutie vindt momenteel plaats. Ze begon eind jaren zestig in Eindhoven met de ontwikkeling van het Automath systeem door professor N.G. de Bruijn, en heeft daarna een hoge vlucht genomen.

Er zal een presentatie geven worden van de huidige toestand van formele wiskunde.

Ten eerste zal formele wiskunde worden afgezet tegen andere vormen van wiskunde in de computer: rigoureuze numerieke methoden, computer algebra, en automatisch stellingenbewijzen.

Vervolgens zullen de belangrijkste systemen die tegenwoordig voor formele wiskunde bestaan de revue passeren: het Engelse **HOL** systeem, de Engels/Duitse opvolger hiervan genaamd **Isabelle**, het Franse **Coq** systeem, en het Poolse **Mizar** systeem.

Er zullen verschillende formele bewijzen in deze systemen worden vertoond, zoals formele bewijzen van:

- De hoofdstelling van de algebra (voor het eerst bewezen door de 'prins der wiskundigen' Carl Friedrich Gauss, in diens proefschrift uit 1799) die zegt dat iedere niet-triviale polynomiale vergelijking altijd een oplossing heeft in de complexe getallen.

- De priemgetalstelling als eerst bewezen door Jacques Hadamard en Charles Jean de la Vallée-Poussin, die zegt dat het aantal priemgetallen kleiner dan n ongeveer $\frac{n}{\log n}$ is als n naar oneindig gaat, in de zin dat de verhouding van deze twee grootheden naar 1 gaat. Het bewijs van deze stelling maakt gebruik van de locatie in het complexe vlak van de nulpunten van de ζ functie van Bernhard Riemann, waarover ook de fameuze *Riemann-hypothese* gaat.

- De stelling van Camille Jordan (ondanks de naam bewezen door Oswald Veblen) die zegt dat een gesloten continue kromme die zichzelf niet doorsnijdt het platte vlak in precies twee delen verdeelt: een binnenkant en een buitenkant. Dit is een stelling uit de topologie, een vakgebied dat werd ontwikkeld door onze landgenoot L.E.J. Brouwer.

- De eerste onvolledigheidsstelling van Kurt Gödel, die zegt dat er voor ieder axiomasysteem ware uitspraken bestaan die niet uit die axioma's te bewijzen zijn (de zogenaamde *Gödel-zin*).

- De vierkleurenstelling, die zegt dat een landkaart altijd met vier kleuren is te kleuren op een manier dat aangrenzende landen steeds verschillende kleuren hebben. Aan de correctheid van het bewijs van deze stelling door Kenneth Appel en Wolfgang Haken uit 1976 werd lange tijd getwijfeld, omdat er bij het bewijs grote computerberekeningen waren gebruikt. Maar nu dit bewijs is geformaliseerd is het zeker dat het bewijs klopt.

Tenslotte zal een eenvoudiger voorbeeld van een formeel bewijs in meer detail worden gepresenteerd. Het gaat hierbij om een formule die *Pythagoreïsche drietallen* genereert. Dit zijn drietallen van gehele getallen (a, b, c) met $a^2 + b^2 = c^2$, die dus met rechthoekige driehoeken met geheeltallige zijden corresponderen. Er zal worden getoond hoe met het Mizar-systeem kan worden bewezen dat alle Pythagoreïsche drietallen door de gegeven formule worden gegenereerd.