Hoofdstuk VII

Meetkunde en getaltheorie in de laatste stelling van Fermat

Peter Stevenhagen

Inleiding

De laatste stelling van Fermat zegt dat voor ieder geheel getal n groter dan 2 de vergelijking

$$a^n + b^n = c^n$$

geen oplossingen bezit waarvoor a, b en c gehele getallen verschillend van nul zijn. Dat klinkt als een tamelijk speciale uitspraak, en men kan zich er daarom over verbazen dat het bewijs van deze stelling, dat in 1993 door Wiles gegeven werd [5], tot een van de grootste prestaties van de moderne wiskunde gerekend wordt. In dit hoofdstuk en het volgende zullen we zien dat het niet alleen om een enkele beroemde vergelijking gaat, maar tevens om een fascinerende bundeling van fundamentele ideeën uit zowel de getaltheorie als de meetkunde.

De onopgeloste status van de Fermatvergelijking heeft in het verleden een belangrijke rol gespeeld bij het ontstaan van de *algebraïsche getaltheorie*, een tak van getaltheorie die de eigenschappen van zogenaamde 'algebraïsche getallen' bestudeert. Deze 'algemenere' getallen zijn uitgevonden om vat te krijgen op de eigenschappen van de *gewone* gehele getallen waarop bijvoorbeeld de stelling van Fermat betrekking heeft. Er blijkt een flinke hoeveelheid abstracte algebra nodig te zijn om basiseigenschappen van gewone getallen, zoals de vertrouwde ontbinding van getallen in hun priemfactoren, ook voor deze algemenere getallen te formuleren. Het is daarom niet zo verbazend dat de algebraïsche getaltheorie tot ver in de twintigste eeuw een aureool van hoge abstractie en complexiteit gehad heeft – een aureool dat overigens aansluitend door de zich stormachtig ontwikkelende algebraïsche meetkunde werd overgenomen.

In de moderne wiskunde zijn getaltheorie en meetkunde zo zeer verweven geraakt dat men wel van *arithmetische algebraïsche meetkunde* spreekt – een grensgebied tussen de eerder genoemde disciplines dat al tot vele fraaie resultaten aanleiding gegeven heeft. Ook Wiles' bewijs is een goed voorbeeld van de kracht van deze *unificatie* binnen de wiskunde. Hoewel het bewijs grotendeels tot het domein van de algebraïsche getaltheorie gerekend kan worden, is het onmiskenbaar dat veel stappen in het complete bewijs, zoals de in het volgende

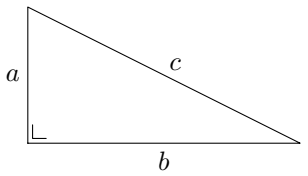
hoofdstuk genoemde stelling van Ribet uit 1986, sterk meetkundig geïnspireerd zijn.

In dit hoofdstuk maken we kennis met de meetkundige aspecten van vergelijkingen als die van Fermat, en ontdekken we hoe men oplossingen van dergelijke vergelijkingen vindt door met algebraïsche getallen te werken. Het volgende hoofdstuk schetst in meer detail de meetkundige principes die de achtergrond vormen van Wiles' bewijsstrategie. Het is duidelijk dat beide hoofdstukken niet bij benadering het complete bewijs van Wiles kunnen geven. Een zeer uitgebreide bron van verdere informatie vormen de proceedings van de in 1995 in Boston gehouden Fermatconferentie [2]. Wie een wiskundig minder veeleisende beschrijving prefereert kan één van de meer populaire boeken over het onderwerp raadplegen, bijvoorbeeld het ook in het Nederlands vertaalde boek van Singh [4].

Pythagoreïsche tripels

De Fermatvergelijking kan gezien worden als een generalisatie van de veel oudere *Pythagoreïsche vergelijking* $a^2 + b^2 = c^2$, die we zullen gebruiken om een aantal belangrijke punten te illustreren.

De Pythagoreïsche vergelijking heeft, anders dan die van Fermat, een directe meetkundige betekenis. Hij kan namelijk gezien worden als een fundamentele formule voor het berekenen van afstanden in het vlak of in de ruimte.



Immers, de beroemde *stelling van Pythagoras* zegt dat voor een rechthoekige driehoek in het platte vlak de relatie tussen de lengtes a en b van de rechthoekszijden en de lengte c van de schuine zijde gegeven wordt door de vergelijking

$$a^2 + b^2 = c^2.$$

Zijn twee van de zijden gegeven, bijvoorbeeld $a = 2$ en $b = 3$, dan kan men hiermee de derde zijde $c = \sqrt{13}$ berekenen. Zoals uit dit voorbeeld al blijkt is het niet zo dat, indien we twee van de zijden een gehele lengte geven, de derde zijde geheel of zelfs maar rationaal is. Het feit dat getallen als $\sqrt{13}$ niet als (rationale) breuk $\frac{m}{n}$ te schrijven zijn was de oude Grieken reeds bekend, en het had ironischerwijs tot gevolg dat de Pythagoreïsche natuurfilosofie, die de harmonie in de natuur aan geheeltallige verhoudingen toe wilde schrijven, toch niet geheel aan de verwachtingen voldeed.

Enig proberen laat al snel zien dat er niettemin veel rechthoekige driehoeken met geheeltallige zijden zijn, en fraaie gelijkheden als

$$3^2 + 4^2 = 5^2 \qquad \text{en} \qquad 5^2 + 12^2 = 13^2$$

zijn dan ook heel lang bekend. Geheeltallige oplossingen (a, b, c) van de vergelijking $a^2 + b^2 = c^2$ staan bekend onder de naam *Pythagoreïsche tripels*. Uit een gegeven tripel (a, b, c) kunnen we door vermenigvuldiging met een geheel getal k willekeurig veel andere tripels (ka, kb, kc) maken. Dat is een beetje een flauwe manier, en het ligt dan ook voor de hand verder alleen naar *primitieve* Pythagoreïsche tripels te kijken. Dit zijn tripels (a, b, c) waarvoor a, b en c geen gemeenschappelijke factor $k > 1$ hebben. In het bijzonder geldt dan $(a, b, c) \neq (0, 0, 0)$.

Het blijkt dat er heel veel primitieve Pythagoreïsche tripels bestaan: als m en n willekeurige gehele getallen zijn, dan is het eenvoudig te verifiëren dat

$$(m^2 - n^2, 2mn, m^2 + n^2)$$

een Pythagoreïsch tripel is. Nemen we m en n met grootste gemene deler 1 en $m + n$ oneven, dan krijgen we een primitief tripel. Voor de kleine waarden $(m, n) = (2, 1)$ en $(m, n) = (3, 2)$ krijgen we de eerder genoemde tripels $(3, 4, 5)$ en $(5, 12, 13)$.

Men kan zich afvragen of onze methode om Pythagoreïsche tripels te maken *alle* mogelijke tripels geeft. Een stelling, die we al bij Euclides ($\pm$300 v. Chr.) kunnen vinden, zegt dat dit in essentie het geval is. Alvorens de stelling te formuleren merken we op dat in een primitief tripel a en b niet allebei oneven kunnen zijn: immers, vanwege het eenvoudig te verifiëren feit dat een oneven kwadraat een viervoud plus 1 is zou dit betekenen dat c^2 een even kwadraat is dat niet deelbaar is door 4, en dit is onmogelijk. Door eventueel a en b om te wisselen mogen we wel aannemen dat in een primitief tripel het getal b even is. Verder merken we op dat we voor a, b en c ook *negatieve* getallen kunnen nemen, daar immers $(-x)^2 = x^2$ geldt. Daar we van plan zijn de tripels (a, b, c) en (ka, kb, kc) als 'hetzelfde' te beschouwen kunnen we door eventueel ons tripel met $k = -1$ te vermenigvuldigen steeds uitgaan van tripels waarin c positief is. Onze classificatiestelling luidt dan als volgt.

STELLING 1. *Laat (a, b, c) een primitief Pythagoreïsch tripel zijn waarin b even is en c positief. Dan bestaan er gehele getallen m en n zodat*

$$a = m^2 - n^2 \qquad b = 2mn \qquad c = m^2 + n^2.$$

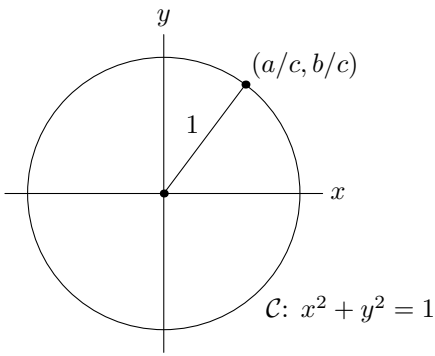
De getallen m en n hebben grootste gemene deler 1 en $m + n$ is oneven.

Er zijn veel bewijzen bekend van deze stelling. We zullen een bewijs van de stelling aangeven dat ook in het volgende hoofdstuk nog een rol zal spelen. Het laat zien hoe men getaltheoretische stellingen soms met *meetkundige* argumenten kan bewijzen.

Omdat c niet nul is kunnen we de vergelijking $a^2 + b^2 = c^2$ herschrijven als

$$(a/c)^2 + (b/c)^2 = 1.$$

Dit laat zien dat ons tripel (a, b, c) aanleiding geeft tot een punt $(\frac{a}{c}, \frac{b}{c})$ dat gelegen is op de eenheidscirkel $\mathcal{C}$ in het platte vlak, die immers door de vergelijking $x^2 + y^2 = 1$ gegeven wordt.

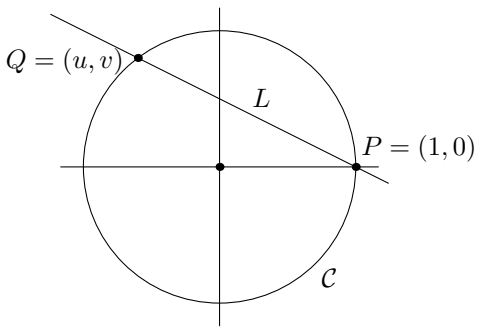


Het punt $(\frac{a}{c}, \frac{b}{c})$ is een punt met *rationale coördinaten*, en omgekeerd ziet men gemakkelijk in dat we voor een punt (x, y) op $\mathcal{C}$ met rationale coördinaten door 'gelijknamig maken van x en y' een primitief Pythagoreïsch tripel met $c > 0$ kunnen krijgen. Hiermee hebben we een getaltheoretisch probleem, namelijk het vinden van Pythagoreïsche tripels, teruggebracht tot een *meetkundig* probleem, namelijk het vinden van punten met rationale coördinaten op de eenheidscirkel.

Om alle rationale punten op $\mathcal{C}$ te vinden gebruiken we dat we tenminste één rationaal punt op $\mathcal{C}$ kennen, bijvoorbeeld $P = (1, 0)$. Is nu $Q = (u, v)$ een willekeurig ander rationaal punt op $\mathcal{C}$, dan wordt de verbindingslijn L van P en Q gegeven door de vergelijking

$$L: \quad y = r(x - 1) \qquad \text{met} \qquad r = \frac{v}{u - 1}.$$

De richtingscoefficient $r = \frac{v}{u-1}$ van deze lijn is rationaal, en omgekeerd is het zo dat we voor *iedere* rationale keuze van r een rationaal snijpunt Q van L met $\mathcal{C}$ vinden.



We krijgen hiermee een correspondentie tussen rationale punten op $\mathcal{C}$ en rationale waarden van r. In de meetkunde spreekt men wel van een rationale *parametrisatie* van de eenheidscirkel.

Een korte berekening leert dat we voor gegeven rationale richtingscoefficient $r = s/t$ het punt Q kunnen schrijven als

$$Q = \Big(\frac{r^2 - 1}{r^2 + 1}, \frac{2r}{r^2 + 1}\Big) = \Big(\frac{s^2 - t^2}{s^2 + t^2}, \frac{2st}{s^2 + t^2}\Big).$$

Nemen we s en t zonder gemeenschappelijke factoren, dan correspondeert dit met een primitief tripel $(s^2-t^2, 2st, s^2+t^2)$ van de gewenste vorm als $s+t$ oneven is. Is $s+t$ even, dan is $((s^2-t^2)/2, st, (s^2+t^2)/2)$ primitief en we hebben

$$\left(st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2}\right) = \left(m^2-n^2, 2mn, m^2+n^2\right)$$

voor $m=(s+t)/2$ en $n=(s-t)/2$.

We hebben hiermee een stelling die ons precies vertelt hoe Pythagoreïsche tripels er uit zien, en zelfs een meetkundige interpretatie die ons aan deze tripels laat denken als rationale punten op de eenheidscirkel $\mathcal{C}$. De doorsnijdingen van $\mathcal{C}$ met de coördinaatassen corresponderen met de 'triviale' tripels (a,b,c) waarin a of b nul is. Dit is zeker niet de formulering zoals we die bij Euclides vinden—al was het maar omdat onze moderne notatie die met letters rekent pas in de zestiende en zeventiende eeuw ontwikkeld werd en eerst door Euler in de achttiende eeuw in de ons nu bekende vorm gestandaardiseerd werd. De stelling zelf is echter een klassiek Grieks resultaat.

Fermat en zijn laatste stelling

De resultaten die de Grieken in de wiskunde bereikten bleven lange tijd het eindpunt in een ontwikkeling. Na de teloorgang van het wetenschappelijke centrum Alexandrië en de val van het Romeinse Rijk verzonk West-Europa in een duizendjarig moeras van christelijk ridderdom, terwijl het Byzantijnse Rijk en de opgekomen Arabische moslimcultuur de erfenis van de Klassieken bewaarden. Eerst in de Renaissance kwam hier verandering in, en sommigen stellen dat de geboorte van de moderne getaltheorie samenvalt met het verschijnen in 1621 van een gedrukt exemplaar van de overgeleverde boeken van Diophantus' Arithmetica met Latijnse vertaling en commentaar van Bachet de Méziriac. Pierre de Fermat (1601–1665), werkzaam als jurist te Toulouse en één van de beste wiskundigen van zijn tijd, bezat een exemplaar en noteerde een aantal van zijn getaltheoretische ontdekkingen in de marge. Wat er met Fermats exemplaar gebeurd is is onbekend, maar Fermats zoon Samuel gaf in 1670 een gedrukte versie van zijn vaders Diophantus uit, inclusief de opmerkingen in de marge. De beroemde marginale opmerking bij probleem II.8 in Diophantus, dat gewijd is aan de ons nu bekende Pythagoreïsche tripels, luidt als volgt:

> *Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*

Deze opmerking, waarin Fermat beweert een wonderbaarlijk bewijs gevonden te hebben voor het feit dat een derde-macht niet als (echte) som van twee derde-machten geschreven kan worden, of een vierde-macht als som van twee vierde-machten en zo verder voor alle machten groter dan 2, is bekend geworden als de laatste stelling van Fermat. De reden hiervan is dat andere nagelaten

problemen en stellingen zonder bewijs van Fermat in de loop der tijd opgelost werden, terwijl de status van deze opmerking onduidelijk bleef.

Men kan zich afvragen hoe Fermat tot zijn generalisatie kwam: er zijn tenslotte andere generalisaties van de vergelijking $a^2+b^2=c^2$ denkbaar, zoals $a^2+b^2=c^2+d^2$. Zonder ons te wagen aan algemene beschouwingen over wiskundige esthetiek is Fermats generalisatie wiskundig gesproken de meest voor de hand liggende in de zin dat de meeste wiskundigen dit zo ervaren. Andere generalisaties zoals de genoemde zijn zeker ook bestudeerd, en er zijn vele fraaie stellingen over sommen van kwadraten. Geen van deze stellingen heeft echter een rol gespeeld in de ontwikkeling van de getaltheorie die vergelijkbaar is met die van Fermats laatste stelling.

Als we er van uitgaan dat Samuel de woorden van zijn vader correct heeft weergegeven—het originele Diophantus-exemplaar van Fermat zelf is immers verdwenen—blijft het een onderwerp van speculatie of Fermat daadwerkelijk het bewijs had dat hij claimde, en zo ja hoe het er uit gezien moet hebben. De meeste moderne wiskundigen zijn van mening dat het zeer onwaarschijnlijk is dat hij een *correct* bewijs bezat. Eén van de argumenten hiervoor is dat Fermat zelf sinds de beroemde aantekening in de marge, die hij rond 1638 gemaakt moet hebben, tot aan zijn dood in 1665 nergens in zijn overgeleverde wetenschappelijke correspondentie op dit wonderbaarlijke bewijs terugkomt. Fermats slotopmerking dat zijn bewijs helaas niet in de marge van het boek paste is zeker van toepassing op het bewijs van Wiles dat wij thans bezitten: onder aanname van vele diepe resultaten die in de laatste tien jaar verkregen zijn en ver achter de horizon van Fermats wiskundig universum liggen beslaat het altijd nog zo'n tweehonderd pagina's.

Als d een deler is van de exponent n en de vergelijking $a^n+b^n=c^n$ oplossingen met $abc\neq 0$ bezit, dan hebben we ook zulke oplossingen voor de Fermat-vergelijking met exponent d. Immers, de identiteit $a^n+b^n=c^n$ kunnen we in dit geval schrijven als

$$(a^{n/d})^d+(b^{n/d})^d=(c^{n/d})^d.$$

Het is daarom voldoende de laatste stelling van Fermat te bewijzen voor exponent $n=4$ en voor exponent n gelijk aan een oneven priemgetal. Immers, ieder getal $n>1$ is een product van priemgetallen, en voor $n>2$ is n hetzij deelbaar door 4, hetzij deelbaar door een oneven priemgetal.

We merken nog op dat bewijzen dat een bepaalde vergelijking *geen* oplossingen heeft in principe moeilijker is dan bewijzen dat de vergelijking *wel* oplossingen heeft. In het laatste geval is het namelijk voldoende een oplossing op te schrijven, die bijvoorbeeld door proberen op een computer gevonden kan worden. In het eerste geval echter is een computer niet direct van nut, omdat we immers willen weten dat voor elk van de oneindig veel mogelijke waarden van a en b de som a^n+b^n geen n-de macht is.

Er is zoals gezegd geen bewijs van Fermat zelf overgeleverd voor zijn laatste stelling. Dit is wel het geval voor de speciale waarde $n=4$ van de exponent. Het argument dat Fermat hiervoor geeft is een klassiek voorbeeld van

wat men tegenwoordig een 'descent-argument' noemt. Hierbij construeert men uitgaande van een gegeven oplossing steeds een 'kleinere' oplossing.

Omdat iedere vierde macht zeker een kwadraat is, is het voldoende te bewijzen dat de vergelijking $a^4 + b^4 = d^2$ geen oplossingen met $abd \neq 0$ heeft.

STELLING 2. *Er zijn geen gehele getallen a, b en d verschillend van 0 die voldoen aan de vergelijking*

$$a^4 + b^4 = d^2.$$

Als er wel zulke getallen bestaan, dan kunnen we een tripel (a, b, d) vinden waarvoor d positief is (vervang anders d door $-d$) en *zo klein mogelijk*. We gaan nu bewijzen dat zo'n kleinste waarde van d niet kan bestaan door uitgaande van een tripel (a, b, d) met $abd \neq 0$ en $a^4 + b^4 = d^2$ een *nieuwe* oplossing (u, v, w) te construeren waarvoor $0 < w < d$ geldt. De conclusie is dat onze hypothetische oplossing (a, b, d) niet kan bestaan, en de stelling is bewezen.

Voor onze oplossing (a, b, d) is (a^2, b^2, d) een (primitief) Pythagoreïsch tripel, en onder gebruikmaking van stelling 1 kunnen we concluderen (na geschikte keuze van tekens en eventueel verwisselen van a en b) dat er getallen m en n zonder gemeenschappelijke factoren bestaan zodat

$$a^2 = m^2 - n^2 \qquad b^2 = 2mn \qquad d = m^2 + n^2.$$

Uit de eerste vergelijking leiden we af dat m oneven moet zijn en n even (gebruik dat a^2 een viervoud plus 1 is), en de tweede vergelijking laat dan zien dat m een kwadraat en n twee keer een kwadraat is (gebruik dat m en n geen gemeenschappelijke priemfactoren hebben—op dit principe komen we dadelijk uitvoerig terug). Schrijven we nu de eerste vergelijking als $a^2 + n^2 = m^2$, dan zien we dat (a, n, m) weer een (primitief) Pythagoreïsch tripel is. We passen dus nogmaals onze stelling toe om getallen s en t zonder gemeenschappelijke factoren te vinden zodat

$$a = s^2 - t^2 \qquad n = 2st \qquad m = s^2 + t^2$$

geldt. Omdat n twee keer een kwadraat is kunnen we uit de tweede van deze vergelijkingen concluderen dat s en t kwadraten zijn.

Het resultaat van al deze overwegingen is dat er getallen u, v en w bestaan zodat we $s = u^2$, $t = v^2$ en $m = w^2$ hebben. De vergelijking $m = s^2 + t^2$ kunnen we dan herschrijven als

$$w^2 = u^4 + v^4,$$

zoals gewenst. We hebben $uvw \neq 0$ (ga na) en de ongelijkheden

$$0 < w < w^2 = m < m^2 + n^2 = d$$

laten zien dat de nieuw geconstrueerde oplossing (u, v, w) inderdaad kleiner is dan de 'beginoplossing' (a, b, d). Dit besluit het bewijs.

Hoewel dit uit bovenstaande manipulaties met formules niet direct duidelijk zal zijn, kan men het zojuist gegeven bewijs *ook* meetkundig interpreteren. De meetkundige vertaling, die we hier niet geven, verloopt in dit geval via de

constructies van punten op een bijbehorende *elliptische kromme* en is beduidend ingewikkelder. Een informele beschrijving van elliptische krommen wordt gegeven in het volgende hoofdstuk.

Methodes van Euler en Kummer

Nu we de laatste stelling van Fermat bewezen hebben voor de exponent $n = 4$ moeten we nog laten zien dat voor ieder priemgetal $p > 2$ de implicatie

$$a^p + b^p = c^p \qquad \Longrightarrow \qquad abc = 0$$

geldt. Om dit te bewijzen zijn sinds Fermat heel veel verschillende methoden ontwikkeld, en ter afsluiting bekijken we een methode die we in geschreven vorm voor het eerst tegen komen bij de grootste wiskundige van de achttiende eeuw, de Zwitser Leonhard Euler (1707–1783). Onder de handen van Gauss (1777–1855) en Kummer (1810–1893) ontwikkelden dergelijke argumenten zich tot de fundamenten van de algebraïsche getaltheorie.

Heel onnauwkeurig gezegd komt de methode er op neer dat we proberen het linkerlid van onze vergelijking $a^p + b^p = c^p$ te splitsen in lineaire factoren en te bewijzen dat voor een oplossing elk van deze factoren een p-de macht is. Dit zal in veel gevallen tot een tegenspraak leiden.

Alvorens naar het geval van oneven priemexponent p te kijken zullen we het geval van Pythagoreïsche tripels nog eens in detail bestuderen. Veel fundamentele problemen blijken al in dit eenvoudige voorbeeld aan het licht te treden. Stel dus dat we weer proberen primitieve oplossingen te vinden van de kwadratische vergelijking $a^2 + b^2 = c^2$, zeg met b even en $c > 0$. Als we de vergelijking herschrijven als $c^2 - a^2 = b^2$ kunnen we het linkerlid schrijven als $c^2 - a^2 = (c + a)(c - a)$, en omdat a en c oneven zijn zijn alle factoren in de vergelijking

$$\Big(\frac{c+a}{2}\Big)\Big(\frac{c-a}{2}\Big) = \Big(\frac{b}{2}\Big)^2$$

geheel. Als (a, b, c) een primitief tripel is hebben de factoren in het linkerlid geen gemeenschappelijke factoren, want een factor k die zowel $(c + a)/2$ als $(c - a)/2$ deelt ook de som $c = \frac{c+a}{2} + \frac{c-a}{2}$ en het verschil $a = \frac{c+a}{2} - \frac{c-a}{2}$, en dus zowel a, b als c. We beroepen ons nu op een welbekend feit.

PRINCIPE. *Als het product van twee positieve getallen A en B zonder gemeenschappelijke factoren een kwadraat is, dan is zowel A als B een kwadraat.*

Uitgaande van de stelling van de eenduidige priemfactorontbinding, die zegt dat elk getal op een unieke manier te schrijven is in een product van priemgetallen, is het bewijs van dit principe niet moeilijk te geven. Passen we dit principe toe op de positieve getallen $A = \frac{c+a}{2}$ en $B = \frac{c-a}{2}$, dan vinden we getallen m en n met $m^2 = \frac{c+a}{2}$ en $n^2 = \frac{c-a}{2}$. Het nemen van som, verschil en product geeft de gelijkheden

$$a = m^2 - n^2 \qquad\qquad c = m^2 + n^2 \qquad\qquad b^2/4 = m^2 n^2,$$

en we zien dat we een nieuw bewijs hebben gekregen van stelling 1.

Bovenstaand bewijs berust op het feit dat we de uitdrukking $c^2 - a^2$ in lineaire factoren kunnen ontbinden. Voor exponenten groter dan 2 is dat niet meer het geval, en men kan denken dat het bewijs daarom niet te generaliseren is. De revolutionaire gedachte van Euler was dat niet-ontbindbare uitdrukkingen wel ontbindbaar worden onder uitbreiding van het getalbegrip. Ik wil dit illustreren aan de hand van de vergelijking $a^2 + b^2 = c^2$ zelf, waarvan het linkerlid onontbindbaar lijkt omdat het niet het verschil maar de som van twee kwadraten is. Schrijven we $a^2 + b^2 = a^2 - (-b^2)$, dan zien we dat het probleem verdwijnt als we $-b^2$ tot een kwadraat praten. De voor de hand liggende identiteit is $-b^2 = (b\sqrt{-1})^2$ en daarmee

$$a^2 + b^2 = (a + b\sqrt{-1})(a - b\sqrt{-1}).$$

Dit ziet er op het eerste gezicht wat bizar uit, omdat het bekend is uit de elementaire wiskunde dat men geen wortel kan trekken uit negatieve getallen. Wie bekend is met complexe getallen weet al dat $\sqrt{-1}$ een bijzonder nuttige uitvinding is, maar dat wil ik hier niet aannemen. Laten we dus niet bang zijn voor het symbool $\sqrt{-1}$ en doodleuk verder rekenen met de verkregen uitdrukkingen van de vorm $a + b\sqrt{-1}$, met a en b 'gewone' gehele getallen. Deze *complexe gehele getallen*, waaraan de naam van Gauss verbonden is, laten zich eenvoudig optellen en vermenigvuldigen:

$$\begin{aligned}(a + b\sqrt{-1}) + (c + d\sqrt{-1}) &= (a + c) + (b + d)\sqrt{-1}\\ (a + b\sqrt{-1})(c + d\sqrt{-1}) &= (ac - bd) + (ad + bc)\sqrt{-1}.\end{aligned}$$

Hierbij zijn in de tweede regel de bekende regels voor het wegwerken van haakjes gebruikt. We willen graag ons principe toepassen op de Pythagoreïsche vergelijking

$$(a + b\sqrt{-1})(a - b\sqrt{-1}) = c^2.$$

Hiertoe moeten $A = a + b\sqrt{-1}$ en $B = a - b\sqrt{-1}$ geen gemeenschappelijke factoren hebben, en dit lijkt het geval te zijn omdat de som $A + B = 2a$ en het verschil $A - B = 2b\sqrt{-1}$ van A en B vanwege de primitiviteit van ons tripel (a, b, c) slechts een factor 2 gemeenschappelijk hebben en hun product (c^2) oneven is. Passen we nu zonder verder nadenken ons principe toe, dan moet $a + b\sqrt{-1}$ een kwadraat zijn van een complex geheel getal, zeg

$$a + b\sqrt{-1} = (m + n\sqrt{-1})^2 = (m^2 - n^2) + 2mn\sqrt{-1}.$$

Vergelijken we de uitdrukkingen links en rechts, dan komen we voor een derde keer terecht op de vertrouwde gelijkheden $a = m^2 - n^2$ en $b = 2mn$.

Het bereikte resultaat boezemt natuurlijk vertrouwen in, ook al zijn we met de methode op enigszins speculatief terrein geraakt. Iets preciezer geformuleerd hebben we de positiviteits-voorwaarde in ons principe onder tafel gemoffeld en over 'gemeenschappelijke factoren' van complexe gehele getallen gepraat alsof het duidelijk was wat dat betekende. Indien we soortgelijke argumenten op de Fermatvergelijking $a^p + b^p = c^p$ met priemgetal-exponent $p > 2$ toepassen zijn de problemen voor een klein priemgetal als $p = 3$ nog redelijk te overzien, en

dit 'verklaart' dat Euler voor dit geval een min of meer sluitend bewijs kon geven.

De lezer kan nagaan dat de introductie van een complex getal $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, dat voldoet aan de vergelijking $\zeta^2 + \zeta + 1 = 0$, leidt tot een ontbinding

$$a^3 + b^3 = (a+b)(a+\zeta b)(a+\zeta^2 b) = c^3$$

van de Fermatvergelijking voor exponent 3. Getallen van de vorm $a+b\zeta$ gedragen zich 'net zo' als de getallen $a + b\sqrt{-1}$. Voor priemgetal-exponenten $p > 3$ heeft men niet langer genoeg aan wortels uit negatieve gehele getallen: de rol van het element ζ hierboven wordt dan overgenomen door een oplossing van de vergelijking

$$\zeta^{p-1} + \zeta^{p-2} + \ldots + \zeta^2 + \zeta + 1 = 0.$$

Zo'n oplossing is bijvoorbeeld het complexe getal $\cos(2\pi/p) + \sin(2\pi/p)\sqrt{-1}$.

Voor grotere waarden van p treden er echter serieuze problemen op. Het soort complexe gehele getallen dat hierbij optreedt blijkt zich in een aantal opzichten totaal verschillend te gedragen van de ons bekende 'gewone' gehele getallen. De problemen zijn hierbij van tweeërlei aard.

Het eerste probleem betreft de geschikte generalisatie van de positiviteitsvoorwaarde in ons principe. Dit is een 'tekenkwestie' die verband houdt met de twee delers 1 en -1 van het getal 1. Voor algemene complexe gehele getallen moeten we ook naar delers van het getal 1 kijken, en het blijkt dat dat er *oneindig veel* kunnen zijn.

Het tweede probleem betreft het praten over 'factoren' van complexe gehele getallen op een manier die suggereert dat zulke getallen te schrijven zijn als unieke produkten van priemfactoren. Dit laatste blijkt helemaal niet het geval te zijn. Kijken we bijvoorbeeld naar getallen van de vorm $a+b\sqrt{-5}$, die op een even eenvoudige manier opgeteld en vermenigvuldigd worden als de getallen $a+b\sqrt{-1}$ waar we net gebruik van hebben gemaakt, dan kunnen we proberen het getal 6 in factoren te ontbinden. Er zijn twee mogelijke antwoorden, namelijk

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Alle optredende factoren kunnen niet verder 'ontbonden' worden, en de priemfactor 2 die maakt dat 6 even is lijkt in de ontbinding $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ spoorloos verdwenen te zijn.

Het is de verdienste van Kummer geweest om deze problemen, die absoluut fundamenteel zijn voor de getaltheorie, tot een bevredigende oplossing te brengen. Het zou te ver gaan Kummers theorie van *ideaalfactorisatie*, die door veel van zijn tijdgenoten als uiterst ingewikkeld en mysterieus beschouwd werd, hier uiteen te zetten. Het behoort tegenwoordig tot de standaardkennis van de getaltheoreticus. Laat ik afsluiten met het resultaat dat Kummer onder gebruikmaking van zijn nieuwe theorie voor Fermats laatste stelling kon bewijzen.

STELLING 3. *Laat $p > 2$ een regulier priemgetal zijn. Dan heeft de vergelijking $a^p + b^p = c^p$ geen oplossingen met $abc \neq 0$.*

Deze stelling is natuurlijk niet compleet zonder de mededeling dat een priemgetal $p > 3$ *regulier* genoemd wordt als geen van de getallen $1^2 + 2^2 + ... + p^2$, $1^4 + 2^4 + ... + p^4$ tot en met $1^{p-3} + 2^{p-3} + ... + p^{p-3}$ door p^2 deelbaar is. Zo is bijvoorbeeld het priemgetal 7 regulier, want $1^2 + 2^2 + ... + 7^2 = 140$ en $1^4 + 2^4 + ... + 7^4 = 4676$ zijn niet deelbaar door $7^2 = 49$. Het priemgetal 37 is niet regulier, want $1^{32} + 2^{32} + ... + 37^{32}$ is, zoals iedere bezitter van een rekenmachine gemakkelijk nagaat, deelbaar door $37^2 = 1369$. Op grond van zowel numerieke gegevens als heuristische argumenten lijkt het of ongeveer 60% van alle priemgetallen regulier is, maar het is zelfs niet bewezen dat er oneindig veel reguliere priemgetallen bestaan. Voor de priemgetallen onder de 100 vinden we de volgende verdeling, die kennelijk niet zo representatief is:

$$\begin{array}{lll} \text{regulier :} & p = & 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, \\ & & 43, 47, 53, 61, 71, 73, 79, 83, 89, 97 \\ \text{irregulier :} & p = & 37, 59, 67. \end{array}$$

Ook voor irreguliere priemgetallen p heeft de algebraïsche getaltheorie criteria geleverd die de correctheid van Fermat's laatste stelling voor exponent p impliceren. Met de computer kan men deze criteria voor vaste p verfiëren, en in 1993, het jaar dat Wiles zijn bewijs aankondigde, was dat voor alle $p \leq 4\,000\,000$ gedaan. Het was echter bij voorbaat duidelijk dat dergelijke computerverificaties nooit tot een bewijs voor alle priemexponenten konden leiden. Niet bij voorbaat duidelijk was dat we uiteindelijk een bewijs van Fermat's laatste stelling zouden hebben waar geen seconde computertijd aan te pas komt!

Literatuur

1. Frits Beukers, *Getaltheorie voor beginners*, Utrecht: Epsilon Uitgaven, deel 42, 1999.
2. G. Cornell, J.H. Silverman, G. Stevens (eds.), *Modular forms and Fermat's last theorem*, Springer-Verlag, 1997.
3. Peter Lanser, *De laatste stelling van Fermat.*, Utrecht: Epsilon Uitgaven, Zebra deel 7, 2000.
4. S. Singh, *Fermat's enigma: The quest to solve the world's greatest mathematical problem*, Walker and Co., 1997.
5. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics **141** (1995), 443–551.