De laatste stelling van Fermat

F. Oort
Mathematisch Instituut, Universiteit Utrecht

FLT

In een kantlijn van een uitgave van het werk van Diophantus formuleerde Pierre de Fermat rond 1637 de volgende stelling (die we nu FLT = Fermat's Last Theorem noemen):

> *voor gehele getallen a, b, c, n met* $n \geq 3$ *geldt:*
> $a^n + b^n = c^n \Rightarrow a \,.\, b \,.\, c = 0;$

anders geformuleerd: voor $n \geq 3$ bestaan er geen positieve gehele getallen a, b, c met $a^n + b^n = c^n$. Daarbij schreef hij dat de kantlijn te weinig ruimte bood om ook het bewijs ervan op te schrijven. Sinds die tijd hebben veel wiskundigen geprobeerd deze 'Laatste Stelling van Fermat' te bewijzen. Zie bijvoorbeeld Ribenboim (1979).
Opmerking: Als de uitspraak waar is voor exponent n, dan volgt de uitspraak voor elk veelvoud van n (waarom? ga na!).

Er is veel te zeggen over de boeiende geschiedenis van FLT. Het geval $n = 4$ werd door Fermat zelf bewezen, zijn methode is schitterend (hij neemt een hypothetische oplossing, produceert daaruit een kleinere, maar in positieve gehele getallen kan zo iets niet oneindig vaak herhaald worden!). Voor $n = 3$ gaf Euler een bewijs. Inspanningen van voornamelijk Duitse en Franse wiskundigen uit de negentiende eeuw geven stellingen voor nieuwe gevallen. Ze geven een boeiende rivaliteit te zien en zetten een ontwikkeling in gang van een nieuw vakgebied, de algebraïsche getaltheorie (de 'idealtheorie' werd ontwikkeld om dit probleem op te lossen). Veel gevallen werden toen reeds bewezen. Die inspanningen tezamen met het gebruik van krachtige computers in onze tijd hebben een bewijs geleverd voor vele gevallen: in 1976 bewees Wagstaff dat voor alle priemgetallen $p < 125.000$ de uitspraak met exponent een veelvoud van p juist is, in 1993 weten we dit voor alle $p < 4.000.000$. *Een bewijs voor alle* $n \geq 3$ *is nu in 1993 aangekondigd door A. Wiles; zijn manuscript wordt momenteel door experts zorgvuldig op juistheid getest.* Zijn bewijs gebruikt moderne ontwikkelingen in de wiskunde en maakt geen gebruik van computerberekeningen. Het blijkt dat zodra een probleem vanuit een andere gezichtshoek benaderd wordt, nieuwe technieken een andere toegang geven (en nu ook tot een bewijs gevoerd hebben). Die methoden (uit de aritmetische algebraïsche meetkunde) liggen te ver voor een behandeling hier, aan het eind van het artikel zal ik er iets over zeggen.

Pythagoreïsche drietallen

De Fermat-vergelijking $X^2 + Y^2 = Z^2$ doet ons direct denken aan de stelling van Pythagoras. Daarom geven we de volgende definitie.

Definitie: Een Pythagoreïsch drietal (afkorting: PD) is een drietal (a, b, c) van positieve gehele getallen die kunnen optreden als lengtes van de zijden van een rechthoekige driehoek, met andere woorden $a^2 + b^2 = c^2$. *We zeggen dat het drietal primitief is als ggd(a, b) = 1.*

(En ga na: dan zijn ook de grootste gemene deler van b en c, en de ggd van c en a gelijk aan 1.)

Zulke drietallen zijn al heel lang bekend, bijvoorbeeld in het Babylonië van rond 1500 voor Christus. Werden ze gebruikt bij het bouwen van de piramides in Egypte om rechte hoeken te construeren? Doe het als volgt: maak een touw van lengte 12, met knoopjes op afstanden 3 en 3 + 4; vorm de driehoek, met het touw precies strak gespannen langs de zijden en de knoopjes in de hoekpunten; dat is een rechthoekige driehoek. Hoe langer het touw, des te nauwkeuriger de constructie!

We gaan laten zien dat ook voor $n = 2$ de Fermat-vergelijking oneindig veel oplossingen heeft, anders gezegd dat er oneindig veel verschillende primitieve Pythagoreïsche drietallen bestaan. We zien dat:
$(v^2 - u^2)^2 + (2uv)^2 = (v^2 + u^2)^2$
(gewoon uitschrijven levert het bewijs), en elke keuze van $u,v \in \mathbb{Z}$ met $0 < u < v$ levert een oplossing van de Fermat-vergelijking voor $n = 2$. Voorbeelden (de bete-

kenis van d en m leggen we uit in de volgende paragraaf):

v	u	$a = v^2 - u^2$	$b = 2uv$	$c = v^2 + u^2$	d	$m = ab/2d^2$
2	1	3	4	5	1	6
3	2	5	12	13	1	30
4	1	15	8	17	2	15
4	3	7	24	25	2	21
5	2	21	20	29	1	210
5	4	9	40	41	6	5
6	1	35	12	37	1	210
6	5	11	60	61	1	330
7	2	45	28	53	3	70
7	4	33	56	65	2	231
7	6	13	84	85	1	546
etc.	etc.	...	...	...	...	...

Bovendien: als u en v onderling ondeelbaar zijn, en $u + v$ oneven, dan is het zo verkregen drietal primitief. Merk op dat voor een *PD* òf a òf b even is, door verwisselen kunnen we bereiken dat b even is. Sinds Euclides (boek X, Propositie 26a) weten we omgekeerd dat we zo ook al zulke drietallen krijgen:

Stelling: Als (a, b, c) een primitief PD is met b even, dan zijn er u, v ∈ ℤ met 0 < u < v, en ggd(u, v) = 1, en u + v = oneven zodat $a = v^2 - u^2$, $b = 2uv$, $c = v^2 + u^2$.

Er zijn verschillende bewijzen voor deze stelling, één die gebruik maakt van elementaire getaltheorie, één die gebruikt maakt van factorizatie-methoden in de ring $\mathbb{Z}[\sqrt{-1}]$, één die gebruik maakt van meetkunde, we gaan hier verder – helaas – niet op in. Zie Hardy and Wright (1938), 13.2.

Een voor de hand liggende vraag: kunnen we op een dergelijke manier ook oplossingen van $X^n + Y^n = Z^n$ voor grotere n krijgen? Meer hierover volgt hierna in de paragraaf 'Iets over het bewijs'.

Congruente getallen

In een Arabisch manuscript uit de tiende eeuw (zie ook *Liber quadratorum* van Leonardo di Pisa, Fibonacci, uit 1225) vinden we het volgende probleem. We definiëren dat een getal $m \in \mathbb{Z}$ *congruent* is als het gelijk is aan de oppervlakte van een rechthoekige driehoek waarvan de zijden een rationaal getal als lengte hebben, in formules:

m heet *congruent* als er bestaan $\alpha, \beta, \gamma \in \mathbb{Q}$ met $m = \alpha \,.\, \beta\,/2$, en $\alpha^2 + \beta^2 = \gamma^2$.

Wat zijn de congruente getallen? Zie Guy (1991). Leuk detail: afhankelijk van de manier waarop deze vraag gesteld wordt is de oplossing òf triviaal, òf moeilijk en nog steeds onopgelost.
Inderdaad, zoals de vraag gesteld wordt is het antwoord eenvoudig: maak (in gedachten) de lijst zoals die in de eerste paragraaf begonnen is; als bij een gegeven u en v de resulterende $(v^2 - u^2) \,.\, (2uv)/2$ deelbaar is door d^2, met $d \in \mathbb{Z}_{>0}$, beschouw dan

$\alpha := (v^2 - u^2)/d$, $\beta := (2uv)/d$

en we zien dat deze $m := \alpha \,.\, \beta\,/2$ congruent is.
Voorbeeld:

$u = 4, v = 5, d = 6, m = 9 \,.\, 40\,/(2 \,.\, 6^2) = 5$

is een congruent getal. Elk congruent getal verschijnt op deze manier. Hebben we nu het probleem opgelost? Laten we dit eens proberen: we nemen $m = 1$ en zonder eerst na te denken, beginnen we die lijst te maken (zo maar aan de slag, zonder eerst na te denken is bijna altijd slecht in de wiskunde!). Na een week rekenen verschijnt $m = 1$ nog niet, we schakelen een heel grote computer in, na een eeuw rekenen verschijnt $m = 1$ nog stéédś niet, hebben we een conclusie? (nee, mogelijk wel een donkerbruin vermoeden...; we hadden beter eerst kunnen nadenken: het is niet zo moeilijk in te zien dat uit (FLT,4), reeds door Fermat bewezen, eenvoudig volgt dat $m = 1$ niet een congruent getal is).
D. Zagier construeerde een mooi voorbeeld: $m = 157$ blijkt een congruent getal te zijn, maar tellers en noemers in de benodigde lengtes van de zijden van die rechthoekige driehoek hebben meer dan 22 cijfers (zie Koblitz (1984), p. 5). Je moet dus wel een hele tijd met de lijst doorgaan voor we in kunnen zien dat $m = 157$ wél congruent is. Deze methode blijkt niet erg handig!

Een goede vraag: geef een effectieve procedure om te beslissen of een gegeven getal $m \in \mathbb{Z}$ congruent is. Met 'effectief' bedoelen we: de hoeveelheid rekenwerk om tot een beslissing te komen bij gegeven m is uit de drukken in m. Het is niet bekend of de banale methode die hierboven geschetst is, effectief is in deze zin. Het boek van Koblitz is geheel gewijd aan de theorie die achter de vraagstelling van de congruente getallen zit, indrukwekkend veel theorie, en op bladzijde 221 van dat boek vinden we een resultaat van Tunnell uit 1983 waar een vermoeden voor een effectieve oplossing van het probleem wordt geformuleerd. Voor kwadraatvrije, *oneven* m luidt dat vermoeden:

Vermoeden: m is congruent dan en slechts dan als

$\#\{x, y, z \text{ in } \mathbb{Z} \mid m = 2x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{x, y, z \in \mathbb{Z} \mid m = 2x^2 + y^2 + 8z^2\}$.

Voorbeeld: Laat zien dat $m = 157$ voldoet aan deze voorwaarde (probeer op te lossen $m = 157 = 2x^2 + y^2 + 8z^2$, reduceer modulo 8, algemener: neem $m \equiv 5$ of 7 (mod 8)). Concludeer: als het vermoeden juist is, dan volgt dat $m = 157$ een congruent getal is (dit gaat heel wat sneller dan het vinden van die grote oplossing!).

Het ABC-vermoeden

Sinds 1985 is er een, elementair uitziend, vermoeden geformuleerd door D. Masser, en J. Oesterlé. Later is dit door Szpiro en anderen nog anders geformuleerd. Er zijn

vele vormen van het vermoeden, zie Lang (1993), Oesterlé (1988). We zullen zien: Indien het ABC-vermoeden juist is, dan volgt FLT.
Om het vermoeden op te schrijven maken we gebruik van de volgende notatie: als $D \in \mathbb{Z}_{>0}$, dan schrijven we $N(D)$ voor het produkt van alle priemgetallen (tot de macht 1) die D delen:

$$N(D) = \prod_{\text{p deelt } D} p.$$

Vermoeden (A, B, C; α): Kies een α *in* $\mathbb{R}_{>0}$*; het vermoeden voor deze keuze zegt dat voor elke A, B, C in* $\mathbb{Z}_{>0}$ *met* $ggd(A, B) = 1$ *en* $A + B = C \overset{?}{\Rightarrow} C < (N(ABC))^{\alpha}$.

Merk op: voor $\alpha = 1$ is het vermoeden niet juist. Merk ook op: als $\alpha < \beta$, en het vermoeden is juist voor α, dan ook voor β.

Verrassing 1: Er zijn geen tegenvoorbeelden bekend voor het geval $\alpha = 2$.

Het is moeilijk om tegenvoorbeelden met kleinere α te construeren, probeer het maar eens voor $\alpha = 3/2$, met andere woorden vindt onderling ondeelbare A en B met $A + B > N^{3/2}$.

Voorbeeld (B. de Weger): $11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23$ geeft ongeveer 1,62599 als exponent, dus niet een tegenvoorbeeld voor $(A, B, C; 1{,}63)$.

Verrassing 2: Als het vermoeden (A, B, C; α*) juist is, en* $n \geq 3\alpha$*, dan heeft de Fermat-vergelijking met exponent n geen niet-triviale oplossingen.*

Conclusie: als we $(A, B, C; 1.000.000)$ bewijzen dan is FLT bewezen (want FLT is voor exponenten kleiner dan 3.000.000 bekend).

Bewijs: Onderstel dat het vermoeden $(A, B, C; \alpha)$ juist is. Neem aan dat a, b, c, n positieve gehele getallen zijn met $a^n + b^n = c^n$. Schrijf $A := a^n$, $B := b^n$, en $C := c^n$. Merk op (!!) dat $N = N(ABC) = N(abc)$ (waarom? ga na). Dus $N \leq abc$, en uit $(A, B, C; \alpha)$ volgt:

$$N^n \leq (abc)^n \leq ABC < C^3 < N^{3\alpha}.$$

We zien dat $n < 3\alpha$, tegenspraak, waaruit (FLT, n) volgt.

Een algemenere vorm van het (A, B, C)-vermoeden: *bij gegeven* $\alpha > 1$ *is het aantal paren onderling ondeelbare positieve getallen A en B met*

$$\log(A + B)/\log(N(AB(A + B))) > \alpha$$

eindig. Tot op heden is dit niet bewezen en ook niet tegengesproken.

Iets over het bewijs

In de paragraaf over de Pythagoreïsche drietallen zagen we een 'parametrizatie' van oplossingen van de vergelijking $X^2 + Y^2 = Z^2$. Kunnen we zoiets doen voor grotere n? De oplossingen van een dergelijke vergelijking met complexe getallen geeft een meetkundige ruimte, die we kunnen bestuderen. Daar is een getal aan gehecht, het zogenaamde 'geslacht'. In dit geval blijkt dat gelijk te zijn aan $g = (n-1)(n-2)/2$. Een stelling uit de meetkunde zegt dat een parametrizatie met polynomen mogelijk is dan en slechts dan als $g = 0$. In het geval van de Fermat-vergelijking: alleen als $n = 1$ of $n = 2$. Hier zien we ook dat informatie uit de meetkunde consequenties heeft in de getaltheorie:
als $n \in \mathbb{Z}_{>2}$*, en F, G, H zijn onderling ondeelbare polynomen van positieve graad dan geldt:* $F^n + G^n \neq H^n$ (een algebraïsch bewijs is niet moeilijk). Overigens: er zijn wel parametrizaties met transcendente functies, maar die helpen niet bij het vinden van oplossingen in $\mathbb{Q}$.
Dat is een algemeen verschijnsel in de wiskunde: vaak kan een probleem in het ene vakgebied pas goed begrepen worden als je er gezichtspunten uit een ander vakgebied bij haalt. Probeer uit eigen ervaring zulke voorbeelden te vinden!

Bovenstaande beschouwingen vertellen ons alleen maar dat de methode die bij $n = 2$ oneindig veel oplossingen gaf, niet werkt voor hogere n. Maar daaruit volgt nog niet dat er dan ook geen oplossingen zijn (zo werkt onze logica niet...).
In 1983 bewees G. Faltings een stelling waaruit volgt dat bij gegeven vaste $n > 3$ het aantal oplossingen (a, b, c) van de Fermat-vergelijking van graad n met $ggd(a, b) = 1$ *eindig* is. We gaan hier verder niet op in.
Vele jaren is geprobeerd om direct uit de Fermatvergelijking voldoende informatie te halen om een bewijs te kunnen geven. Recent heeft men andere wegen ingeslagen. We nemen een exponent (waarvoor we een priemgetal $l > 5$ kiezen) en nemen aan dat er tenminste één oplossing (a, b, c) van de Fermat-vergelijking met $abc \neq 0$ is. Met behulp van die ene (hypothetische) oplossing construeren we een nieuw object, een zo genaamde elliptische kromme, zie Frey (1986) en Frey (1987). Een vermoeden geformuleerd door Taniyama en Weil spreekt de hoop uit dat deze kromme 'eenvoudig' beschreven kan worden; Wiles heeft nu de vorm die we nodig hebben van dit zogenaamde Taniyama-Weil vermoeden bewezen. Ribet (1990) toonde reeds aan dat daaruit volgt dat die elliptische kromme niet bestaat, en dat daarom die hypothetische oplossing niet bestaat.
We zien: zodra het probleem met andere aspecten van de wiskunde in verband gebracht wordt, komen er mogelijkheden voor andere inzichten en methoden.

Overpeinzingen

Gaat alles in deze tijd van schitterende rekenfaciliteiten en van versnelde informatie-overdracht niet veel sneller en gemakkelijker? Het is opmerkelijk dat het bewijs van FLT (waar o.a. Serre, Frey, Ribet, Mazur en Wiles, maar

ook vele anderen aan hebben bijgedragen) juist op zuiver denkwerk berust. De wiskunde maakt een periode van grote bloei door. Als zo vele malen in de geschiedenis zal blijken dat juist de wiskundigen met het ontwikkelen van nieuwe ideeën en abstracte structuren de weg openen tot fundamenteel nieuwe ontwikkelingen.
Heeft dit nu directe concrete toepassingen? Mensen denken dan meteen aan bruggen die dankzij FLT nu minder snel instorten, of dat we nu eindelijk de economie beter kunnen beheersen. Er is heel veel direct toepasbare wiskunde, maar er is ook veel abstracte wiskunde; die komt pas veel later de maatschappij tastbaar ten goede. Vandaar dat ik beweer:

wiskunde is een luxe, maar wel een absoluut noodzakelijke luxe voor onze maatschappij.

Literatuur

Edwards, H.M. (1977). *Fermat's last theorem, a genetic introduction to algebraic number theory.* Graduate Texts in Mathematics 50, Springer-Verlag.

Frey, G. (1986). Links between stable elliptic curves and certain diophantine equations. *Annales Univesitatis Saraviensis Ser. Math. 1*, 1-40.

Frey, G. (1987). Links between solutions of A – B = C and elliptic curves. In: Schlickewei, H.P. & E. Wirsing (eds), *Number theory*, Ulm. Lecture Notes in Mathematics 1380, Springer-Verlag, 31-62.

Guy, R.K. (1981). *Unsolved problems in number theory.* Springer-Verlag.

Hardy, G.H. & E. M. Wright (1938). *An introduction to the theory of numbers.* At the Clarendon Press, Oxford.

Koblitz, N. (1984). *Introduction to elliptic curves and modular forms.* Graduate Texts in Mathematics 97, Springer-Verlag.

Lang, S. (1993). Die abc-Vermutung. *Elemente der Mathematik 48*, 89 - 99.

Mazur, B. (1991). Number theory as a gadfly. *American Mathematical Monthly 98*, 593-610.

Oesterlé, J. (1988). Nouvelles approaches du Théorème de Fermat. *Séminaire Bourbaki 40*, Exp. 694, 161-162 (1988), 165-186.

Ribenboim, P. (1979) *13 lectures on Fermat's last theorem.* Springer-Verlag.

Ribet, K.A. (1990). From the Taniyama-Shimura conjecture to Fermat's last theorem. *Annales de la Faculté des Sciences de Touloun 11*, 116-139.

Ribet, K. (1993). Wiles proves Taniyama's conjecture; Fermat's last theorem follows. *Notices A.M.S. 40*, 575-576.

Weil, A. (1984). *Number theory, an approach through history, from Hammurapi to Legendre.* Birkhäuser Verlag.

Het adres van de auteur is:
Frans Oort, Mathematisch Instituut, Budapestlaan 6, 3508 TA Utrecht, email: oort @math.ruu.nl