Hoofdstuk VIII

Oplossingen van vergelijkingen in rationale getallen

Don Zagier

Het gebied van de diophantische vergelijkingen, genoemd naar de grote Griekse wiskundige Diophantus, is een van de oudste en mooiste theorieën in de wiskunde. In dit hoofdstuk wordt een kort overzicht gegeven van een aantal belangrijke ideeën uit deze theorie en we zullen aangeven hoe deze ideeën in de laatste jaren tot een bewijs van de laatste stelling van Fermat hebben geleid.

De centrale vraag van de theorie van diophantische vergelijkingen is de oplosbaarheid van polynomiale vergelijkingen in rationale getallen. Men heeft dus een vergelijking—Fermat's vergelijking $a^n + b^n = c^n$ met n vast is een goed voorbeeld—en men wil weten

— zijn er oplossingen waar alle voorkomende variabelen rationale getallen (dat wil zeggen breuken) zijn?
— zo ja, zijn er oneindig veel zulke oplossingen?
— is er een procedure om sommige of alle oplossingen aan te geven?

Men kan natuurlijk vergelijkingen in vele veranderlijken, of stelsels van vergelijkingen, beschouwen, maar we zullen ons in dit hoofdstuk voor het gemak tot vergelijkingen met slechts twee variabelen x en y beperken. De vergelijking van Fermat past hier in, omdat we in plaats van

$$a^n + b^n = c^n \qquad (a,\ b,\ c \text{ geheel})$$

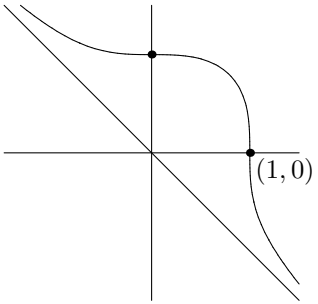
ook

$$x^n + y^n = 1 \qquad \left(x = \frac{a}{c},\quad y = \frac{b}{c} \text{ rationaal}\right) \tag{1}$$

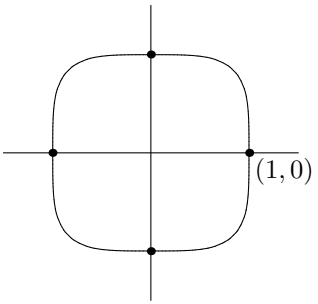
kunnen schrijven. De vergelijkingen met twee veranderlijken zijn niet alleen de eenvoudigste en belangrijkste, maar ze hebben ook het voordeel dat ze met hulp van een grafiek als krommen in het vlak kunnen worden gerealiseerd. Zo is de grafische voorstelling van de Pythagoreïsche vergelijking

$$x^2 + y^2 = 1 \tag{2}$$

een cirkel, terwijl de grafieken van de Fermat-vergelijkingen voor n oneven en n even er zo uitzien:



$x^3 + y^3 = 1$



$x^4 + y^4 = 1$

De vraag naar de rationale oplossingen van de vergelijking wordt dan vertaald in de vraag naar het bestaan van punten met rationale coördinaten x en y op de kromme. Deze meetkundige interpretatie van vergelijkingen als krommen zal ons in onze latere beschouwingen zeer van pas komen.

Laten we eerst eens kijken met welke methoden Diophantus zelf aan het werk ging toen hij rationale oplossingen wilde vinden. Eerst een paar woorden over Diophantus zelf. Over de man weten wij heel weinig—niet eens precies de eeuw, waarin hij leefde. (De beste schattingen zijn AD 250±100.) Maar wij weten dat hij als wetenschapper zo ver zijn tijd vooruit was dat toen 1300 jaren na zijn dood zes delen van zijn werk *Arithmetika*, dat bij de verwoesting van de bibliotheek in Alexandria verdwenen was, weer opdoken, deze een veel hoger niveau hadden dan de Europese wiskunde van die tijd. Het duurde dan ook nóg zeventig jaar, voordat een Europese wiskundige verder kon komen in de getaltheorie dan Diophantus, en deze wiskundige was geen ander dan onze held Fermat! Diophantus heeft niet alleen vrijelijk met het getal nul en met negatieve en rationale getallen gerekend, iets dat pas vele eeuwen later in Europa gebruikelijk zou worden, maar hij was ook de eerste die een systematische algebraïsche notatie heeft uitgevonden. Deze notatie was weliswaar niet erg handig vergeleken met de onze. Men kon niet meer dan één variabele tegelijk schrijven—bijvoorbeeld werd $2x^3 - 3x^2 = 4$ geschreven als $K^\Upsilon \bar{\beta} \Phi \Delta^\Upsilon \bar{\gamma} \iota \overset{0}{M} \bar{\delta}$ waarbij K^Υ (kubos), Δ^Υ (dynamos) en $\overset{0}{M}$ (monad) voor x^3, x^2 en $x^0 = 1$ staan en $\bar{\beta} = 2$, $\bar{\gamma} = 3$, $\bar{\delta} = 4$ coëfficiënten zijn. Maar het was een enorme vooruitgang vergeleken met de voorgangers van Diophantus, die zo'n vergelijking überhaupt niet hadden kunnen opschrijven.

Diophantus heeft twee algemene methoden uitgevonden om de oplossingen van bepaalde vergelijkingen te vinden, en deze zijn tot vandaag de enige methoden van algemene toepassing die ons bekend zijn. De eerste methode werkt voor vergelijkingen van graad 2. Laten wij als voorbeeld de Pythagoreïsche vergelijking (2) nemen (hoewel de oplossingen in dit speciaal geval al eeuwen vóór Diophantus bekend waren). Diophantus begint met een bekende oplossing, laten we zeggen "$x = -1$, $y = 0$", en schrijft dan als probeersel een

lineaire relatie tussen die variabelen x en y op, bijvoorbeeld

$$x = 2y - 1\,, \tag{3}$$

waarbij de coëfficiënt "2" willekeurig gekozen wordt en de coëfficiënt "-1" zo gekozen is dat de relatie voor de gegevene oplossing $(x, y) = (-1, 0)$ juist is. Hij substitueert dan (3) in (2) en vindt

$$\begin{aligned} (2y-1)^2 + y^2 &= 1 \\ 5y^2 - 4y + 1 &= 1 \\ 5y^2 &= 4y \end{aligned}$$

en daarmee $y = \dfrac{4}{5}$, $x = 2y - 1 = \dfrac{3}{5}$ (of natuurlijk $y = 0$, $x = 2y - 1 = -1$, de eerste oplossing). Dit geeft de bekende rechthoekige driehoek met zijden 3, 4, 5. Die methode werkt altijd: door de keuze van de coëfficiënt "-1" in (3) krijgt men een kwadratische vergelijking met constante term 0; deze kan door y gedeeld worden om een lineaire vergelijking te krijgen; en dit geeft een rationale oplossing. In formules uitgedrukt: als we de coëfficiënt "2" in (3) door een willekeurig gekozen ander rationaal getal "t" vervangen, vinden we op dezelfde manier als boven

$$\begin{aligned} (ty-1)^2 + y^2 &= 1 \\ (t^2+1)\,y^2 - 2ty &= 0 \\ y = \frac{2t}{t^2+1}, \quad x = ty - 1 &= \frac{t^2-1}{t^2+1} \end{aligned}$$

Als we de breuk t als m/n met m en n geheel en onderling priem schrijven, krijgen wij weer onze oude vriend $(a, b, c) = (m^2 - n^2, 2mn, m^2 + n^2)$ als algemene oplossing van de oorspronkelijke vergelijking van Pythagoras $a^2 + b^2 = c^2$ (zie het hoofdstuk van Peter Stevenhagen).

Maar wat doet Diophantus als de graad hoger is dan 2? Laten wij als voorbeeld het Vraagstuk 24 uit Deel 4 van zijn *Arithmetika* bekijken. De opgave luidt: een gegeven getal, bijvoorbeeld 6, moet in twee delen (laten we zeggen y en $6 - y$) gesplitst worden waarvan het product gelijk is aan een derde macht min haar wortel (dus $y\,(6-y) = x^3 - x$). Weer heeft men de speciale oplossing $x = -1$, $y = 0$ en weer probeert Diophantus als eerste poging de substitutie $x = 2y - 1$. Maar nu werkt het niet: de constante term van de vergelijking verdwijnt weer als consequentie van de keuze "-1" en we kunnen weer door y delen, maar daardoor wordt onze derdegraads vergelijking slechts kwadratisch en kan nog niet rationaal opgelost worden:

$$\begin{aligned} y\,(6-y) = x^3 - x &= (2y-1)^3 - (2y-1) \\ -y^2 + \underline{6}y &= 8y^3 - 12y^2 + \underline{4}y \\ 8y^2 - 11y - 2 &= 0 \\ y &= ?? \end{aligned}$$

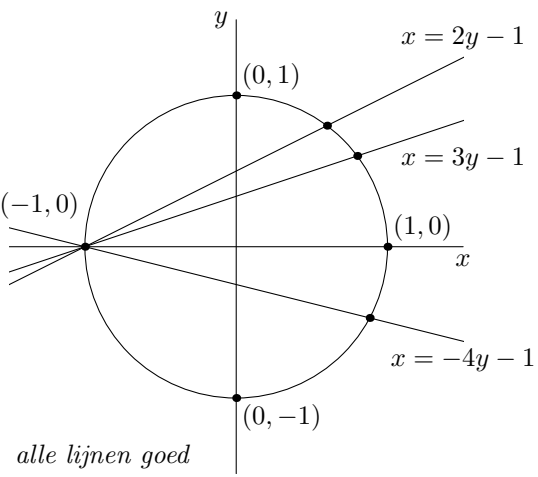
Nu komt het geniale idee van Diophantus. Hij ziet dat als de onderstreepte lineaire termen "6" en "4" gelijk waren geweest, we *een tweede keer* door y zouden hebben kunnen delen en daarmee een rationaal oplosbare lineaire vergelijking krijgen. De eerste coëfficiënt "6" is het gegeven getal en mag dus niet veranderd worden, maar de coëfficiënt "4" is twee keer de gekozen coëfficiënt "2" in (3) (ga na!) en kan daarom door een willekeurig ander getal vervangen worden. We beginnen dus opnieuw, maar nu met de substitutie $x = 3y - 1$ in plaats van (3):

$$\begin{aligned} 6y - y^2 = (3y-1)^3 - (3y-1) = 27y^3 - 27y^2 + 6y \\ 27y^3 = 26y^2 \end{aligned}$$

en voilà de gezochte niet-triviale oplossing :

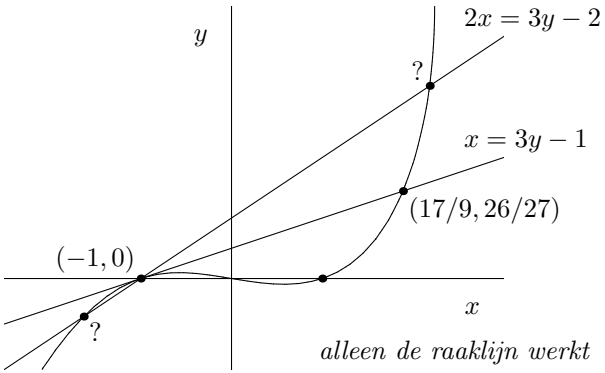
$$y = \frac{26}{27},\ x = 3y - 1 = \frac{17}{9}\ .$$

Meetkundig gezien—maar dit wist Diophantus immers niet—komt zijn methode erop neer dat we in het eerste geval door een gegeven punt $P = (-1, 0)$ op de cirkel een willekeurige lijn kunnen trekken; deze lijn heeft precies één tweede snijpunt met de cirkel (omdat de graad van de vergelijking 2 is) dat dan automatisch rationaal is. Het volgende plaatje illustreert dit.



In het tweede geval is de graad en daarom ook het aantal snijpunten van een lijn met de kromme gelijk aan 3. Een slecht gekozen lijn door P heeft dan nog *twee* snijpunten met de kromme en deze hoeven niet rationaal te zijn. Maar door de *raaklijn* door P te kiezen bereiken we dat er maar één ander snijpunt

van lijn en kromme bestaat, en dat geeft de gewenste oplossing.



Diophantus heeft ook vergelijkingen van hogere graad bestudeerd, maar het is noch hem, noch iemand anders ooit gelukt een algemene methode aan te geven om rationale oplossingen van zulke vergelijkingen te vinden. Als wij dus de resultaten van Diophantus samenvatten en vanuit een modern standpunt interpreteren, zien we dat alle vergelijkingen (of krommen) $f(x, y) = 0$ in drie grote klassen ingedeeld kunnen worden:

(I) De eerste klasse, vertegenwoordigd door kwadratische vergelijkingen zoals ons eerste voorbeeld $x^2 + y^2 = 1$. Deze bezitten oneindig veel oplossingen die alle gevonden kunnen worden door een lijn door een bekend punt op de kromme te tekenen en naar het tweede snijpunt te kijken. De oplossingen kunnen geparametriseerd worden op twee manieren. Ten eerste kunnen we *rationale* functies gebruiken, dat wil zeggen quotiënten van polynomen; in ons voorbeeld,

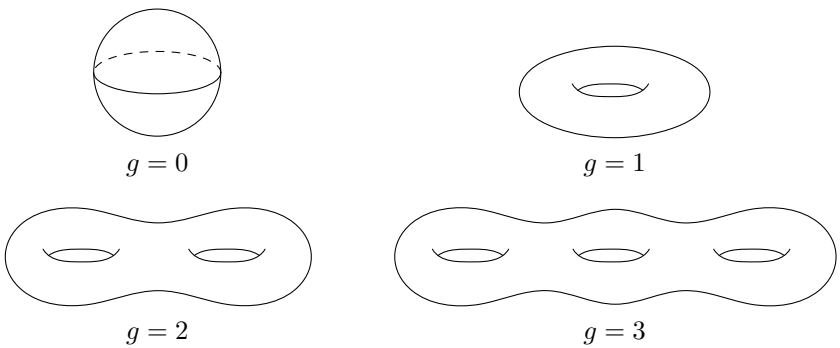
$$x = \frac{t^2 - 1}{t^2 + 1}, \qquad y = \frac{2t}{t^2 + 1}.$$

Ten tweede hebben we een parametrisatie met trigonometrische functies: $x = \cos t$, $y = \sin t$. De krommen van deze klasse worden *rationaal* genoemd.

(II) De tweede klasse, vertegenwoordigd door derdegraads vergelijkingen zoals ons tweede voorbeeld $y\,(6 - y) = x^3 - x$. Deze kunnen oneindig of eindig veel oplossingen bezitten. Uit een bekende oplossing krijgen we een tweede door de raaklijn aan het gegeven punt te tekenen en naar het andere snijpunt van deze lijn met de kromme te kijken. Dit procédé kan herhaald worden en wij krijgen nog meer oplossingen, maar het kan gebeuren dat we na een eindig aantal stappen naar ons uitgangspunt terugkeren. Krommen van deze klasse kunnen niet door rationale of trigonometrische functies geparametriseerd worden, wél door "elliptische" (dat zijn generalisaties van de trigonometrische functies "sinus" en "cosinus" die in de zuivere en toegepaste wiskunde veel bestudeerd werden). Zij worden daarom *elliptische krommen* genoemd.

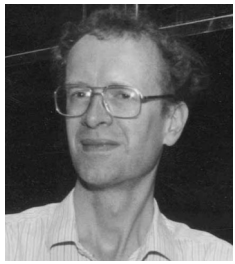
(III) De derde klasse bevat vergelijkingen van hogere graad. Zij kunnen niet door rationale, trigonometrische of elliptische functies geparametriseerd worden, en de algemene mening is dat er überhaupt geen bijzondere structuur op de verzameling van rationale oplossingen is. Mordell heeft in 1922 het vermoeden uitgesproken dat vergelijkingen van deze klasse altijd maar een eindig aantal oplossingen hebben. 60 jaar later werd dit door de jonge Duitse wiskundige Gerd Faltings bewezen. De krommen uit deze derde klasse heten *van algemeen type*.

Wij gebruikten hier de woorden "vertegenwoordigd door" omdat de classificatie in "rationaal," "elliptisch" en "algemeen type" in werkelijkheid niet alleen naar de graad van de vergelijking gaat. Zo geeft de derdegraads vergelijking $y = x^3$ een rationale kromme, geparametriseerd door $x = t$, $y = t^3$. De juiste manier, zoals door de Franse wiskundige Henri Poincaré rond de eeuwwisseling begrepen werd, berust op topologie: men moet kijken naar de ruimte van oplossingen in het "complexe projectieve vlak." We kunnen hier helaas niet precieze definitie geven, maar we kunnen deze oplossingsruimten wel beschrijven als oppervlakken in de gewone drie-dimensionale ruimte: ze zien eruit als een bol, of een fietsband, of een krakeling met een aantal gaten. Dat aantal gaten geven we aan met g en we noemen dit getal het *geslacht* van de vergelijking.

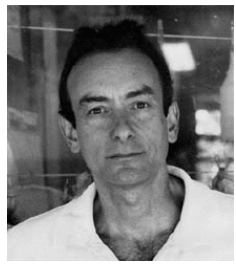


De drie klassen worden dan gegeven door $g = 0$ (rationaal), $g = 1$ (elliptisch), en $g \geq 2$ (algemeen type).

Wij zien nu dat de tweede klasse, bestaand uit de elliptische krommen, de interessantste voor ons is, omdat de eerste klasse te gemakkelijk en de derde te moeilijk is om goede wiskunde mee te bedrijven. Wat valt er met deze veelbelovende klasse verder te doen? Eerst kunnen we de methode van Diophantus met de raaklijn verder ontwikkelen. Dit heeft Fermat met zijn beroemde "descente infinie" gedaan (zie het hoofdstuk van Peter Stevenhagen). Later hebben Newton en andere wiskundigen zich gerealiseerd dat men niet alleen de raaklijn aan één punt op de elliptische kromme kan nemen, maar ook de verbindingslijn tussen twee bekende punten op de kromme. Dan is het derde snijpunt van de lijn met de kromme een nieuwe oplossing. Dit geeft een methode om oplossingen "op te tellen" (wiskundigen zeggen dat de rationale oplossingen een *groep*



Andrew Wiles



Ken Ribet

vormen) die een essentiële rol in de theorie speelt. Maar er is nog een beslissend idee dat pas in onze eeuw ontdekt werd. Wij hebben reeds gezegd dat elliptische krommen door elliptische functies geparametriseerd kunnen worden en dat dit nuttig is omdat de eigenschappen van elliptische functies heel goed bekend zijn. Zij blijken echter te zwak te zijn om licht te kunnen werpen op de diepste arithmetische problemen in de theorie. *In de jaren 1954–67 is uit het werk van de wiskundigen Y. Taniyama, G. Shimura en A. Weil het idee ontstaan dat wellicht alle elliptische krommen een andere soort van parametrisering toelaten, door de zogenaamde modulaire functies.* Dit zijn functies met oneindig veel symmetrieën die een heel belangrijke rol spelen in de getaltheorie en natuurkunde en in de laatste jaren zeer intensief bestudeerd werden. Als het vermoeden van Taniyama-Shimura-Weil dus juist is, hebben we een krachtig hulpmiddel om elliptische krommen te analyseren.

Maar wat gebeurt er nu met de laatste stelling van Fermat? De vergelijking (1) is immers van algemeen type, zodra n groter dan 3 is, en alles wat we gezien hebben laat ons vrezen, dat de situatie dan hopeloos is. Maar in het jaar 1985 kreeg de Duitse wiskundige Gerhard Frey een idee, waardoor Fermat's opgave in principe uit de hopeloze klasse III in de toegankelijke klasse II gedwongen zou kunnen worden. In plaats van de Fermat kromme (1) zelf te beschouwen, gebruiken wij een oplossing van Fermat's vergelijking $a^n + b^n = c^n$ om een *andere* kromme te construeren, die slechts van graad 3 is en daarom met methoden uit de theorie van elliptische krommen geattaqueerd kan worden. Deze speciale elliptische kromme, die al eerder door de Fransman Y. Hellegouarch was beschouwd, wordt gegeven door de vergelijking

$$y^2 = x\,(x - a^n)\,(x + b^n) \tag{4}$$

Frey vond gronden om aan te nemen dat zij misschien een tegenvoorbeeld voor het Taniyama-Weil vermoeden zou kunnen zijn, en een jaar later heeft de Amerikaan Ken Ribet dit bevestigd.

Stelling (Ribet, 1986). *Zij $a^n + b^n = c^n$ een niet-triviale oplossing van de Fermat vergelijking met priem exponent $n > 3$. Dan heeft de Hellegouarch-Frey kromme (4)* **geen** *parametrisering door modulaire functies.*

Zeven jaar later heeft de Engelse wiskundige Andrew Wiles het Taniyama-Weil vermoeden bewezen:

STELLING (WILES, 1993). *Iedere elliptische kromme kan* **wél** *door modulaire functies geparametriseerd worden.*

In de stelling van Wiles is er een technische beperking[1]—de krommen moeten "semistabiel" zijn—maar dat is geen bezwaar, omdat de kromme (4) aan deze eis voldoet.

Vergelijken we deze twee beweringen, dan vinden we dat een oplossing van $a^n + b^n = c^n$ tot een tegenspraak leidt. Een dergelijke oplossing kan dus niet bestaan, en de laatste stelling van Fermat is bewezen!

Literatuur

1. Peter Lanser, *De laatste stelling van Fermat*, Utrecht: Epsilon Uitgaven, Zebra deel 7, 2000.
2. Alf van der Poorten, *Notes on Fermat's Last Theorem*, Chichester: Wiley Interscience, 1996.
3. P. Ribenboim, *Fermat's Last Theorem for Amateurs*, Springer-Verlag, 1999.
4. S. Singh, *Fermat's enigma: The quest to solve the world's greatest mathematical prob lem*, Walker and Co., 1997.
5. Jaap Top (ed.), *De Laatste Stelling van Fermat*, syllabus, Utrecht: Wiskundig Genootschap en Universiteit Utrecht, 1993.

[1] Pas in 1999 is deze laatste beperking verwijderd, en is het Taniyama-Shimura-Weil-vermoeden volledig bewezen.