

De stelling van Pythagoras en de laatste stelling van Fermat

In de eerste lezing van deze cyclus heeft Professor Icke het belang van wiskundige formules benadrukt. Formules zijn echter niet het wezen van de wiskunde. Ze bieden gelegenheid om een structurele gedachte concreet uit te drukken. Het doorgronden van structuren is voor mij het doel van de wiskunde. Ik wil dit vanavond duidelijk maken aan iets simpels waar we van jongs af aan mee vertrouwd zijn, n.l. de *natuurlijke getallen*: 1,2,3,4,... . Ik zal de lezing dan ook eenvoudig houden en alle ingewikkelde details achterwege laten.

We onderscheiden twee basisbewerkingen op de natuurlijke getallen, de *optelling* en de *vermenigvuldiging*. De som zowel als het product van twee natuurlijke getallen levert weer een natuurlijk getal op. Aftrekken van twee natuurlijke getallen, noch deling van een door een ander hoeft een natuurlijk getal op te leveren, want 3-7 is geen natuurlijk getal en 3:7 ook niet.

De *optelstructuur* van de natuurlijke getallen is heel simpel. Door met 1 te beginnen en telkens 1 bij het vorige totaal op te tellen krijgen we precies alle natuurlijke getallen:

$$1, 1+1, 1+1+1, 1+1+1+1, 1+1+1+1+1, \dots$$

Dat we 1,2,3,4,5,... schrijven is efficiënt, maar niet essentieel. In feite worden de natuurlijke getallen opgebouwd met één bouwsteen, namelijk het getal 1, waarbij de + het cement is. Je zou de natuurlijke getallen groter dan 1 ook kunnen opbouwen met bouwstenen 2 en 3:

$$2, 3, 2+2, 2+3, 2+2+2, 2+2+3, 2+2+2+2, 2+2+2+3, \dots$$

maar dit is onbevredigend. We gebruiken meer bouwstenen dan nodig is en bovendien is deze schrijfwijze niet uniek, want $2+2+2=3+3$. We streven naar een minimum aantal verschillende bouwstenen en willen liefst dat elk getal maar op één manier uit de bouwstenen kan worden opgebouwd.

Je kunt de natuurlijke getallen ook *met de vermenigvuldiging* opbouwen. Met het getal 1 kom je niet ver: $1 \cdot 1=1$, $1 \cdot 1 \cdot 1=1$, $1 \cdot 1 \cdot 1 \cdot 1=1$, enz. Met 2 als bouwsteen boeken we al meer resultaat:

$$2 \cdot 2=4, 2 \cdot 2 \cdot 2=8, 2 \cdot 2 \cdot 2 \cdot 2=16, 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2=32, \dots$$

We schrijven kortweg:

$$(2^0 = 1, 2^1 = 2,) 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32, \dots$$

en noemen dit de machten van 2. Er zijn er oneindig veel van, maar de gaten ertussen worden steeds groter. Het kleinste getal dat we missen in de rij van machten van 2 is 3. We nemen 3 als nieuwe bouwsteen:

$$3^0 = 1, 3^1 = 3, 3^2 = 9, 3^3 = 27, 3^4 = 81, 3^5 = 243, \dots$$

maar we kunnen nu ook getallen bouwen met bouwstenen 2 en 3. Zo krijgen we

$$1, 2, 3, 4=2 \cdot 2, 6=2 \cdot 3, 8=2 \cdot 2 \cdot 2, 9=3 \cdot 3, 12=2 \cdot 2 \cdot 3, 16=2 \cdot 2 \cdot 2 \cdot 2, \dots$$

Er zijn nog steeds gaten. 5 is het kleinste getal dat we missen. We maken het tot de volgende bouwsteen. Met de getallen 2,3 en 5 kunnen we de volgende getallen maken:

1,2,3,4,5,6,8,9,10,12,15,16,18,20,24,25,27,30,32,36,40,45,48,50,54,60,64,72,75,80,81,90,96,100
,... .

De volgende bouwsteen is 7, de daaropvolgende zijn

11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,

Deze bouwstenen noemen we *priemgetallen*. We beschouwen 1 niet als priemgetal. Door onze constructie is elk natuurlijk getal het product van priemgetallen:

1 is het product van 0 priemgetallen,

2 is het product van het priemgetal 2,

3 is het product van het priemgetal 3,

4 is het product van 2 priemgetallen 2,

enz.

Immers, als een getal niet het product is van kleinere priemgetallen, dan is het getal zelf een priemgetal en is het dus het product van één priemgetal. Zo kan dus elk natuurlijk getal uit priemgetallen worden opgebouwd. (Omdat we toch alleen maar over natuurlijke getallen praten, zal ik voortaan 'getal' zeggen als ik natuurlijk getal bedoel.)

Er zijn twee vragen die bij deze constructie rijzen en al door de Griek Euclides (omstreeks het jaar

- 300) zijn beantwoord. De eerste vraag is: Is het mogelijk om een getal op meer dan één manier uit priemgetallen op te bouwen? Is het bijvoorbeeld mogelijk dat $11213 \cdot 139559 = 19937 \cdot 78491$? Het helemaal niet vanzelfsprekende antwoord is: nee. De zogenaamde *hoofdstelling van de rekenkunde* zegt dat elk natuurlijk getal maar op één manier door vermenigvuldiging van priemgetallen is op te bouwen, afgezien van de volgorde.

In bovenstaand voorbeeld zijn de twee grootste getallen dan ook geen priemgetallen, maar veelvoud van 7.

De tweede vraag is of we bij de opbouw van priemgetallen op een gegeven moment alle priemgetallen gevonden hebben. M.a.w. is het aantal priemgetallen eindig? Euclides redeneerde ongeveer als volgt om het tegendeel te bewijzen (en dit is een voorbeeld van zijn bewijzen).

Stel er zijn maar eindig veel priemgetallen, $2, 3, 5, \dots, p$.

Dan is $2 \cdot 3 \cdot 5 \cdot \dots \cdot p + 1$ een getal. Noem dit $n+1$.

Elk getal is het product van priemgetallen. Dus ook $n+1$. Dus $n+1 = q \cdot \dots$, waarbij q een priemgetal is.

Het priemgetal q komt ook als factor voor in het vorige getal, $n = 2 \cdot 3 \cdot 5 \cdot \dots \cdot p$.

In welke getallen komt q in de priemontbinding voor? Dat zijn $q, q^2, q^3, q^4, q^5, \dots$

Tussen twee verschillende getallen die een priemfactor q bevatten zit dus minstens een gat q .

Dus moet tussen n en $n+1$ tenminste een gat q zitten. Omdat elk priemgetal groter is dan 1, kan dat niet. Dus er zijn oneindig veel priemgetallen.

Een bewijs zoals we zojuist gegeven hebben heet *een bewijs uit het ongerijmde*. Je bewijst dat een bewering A waar is door aan te tonen dat A niet waar kan zijn. Meer dan 99% van de wiskundigen werkt met dit soort redeneringen, maar er zijn wiskundigen, waartoe de Nederlandse intuïtionisten L.E.J. Brouwer, A. Heyting en A.S. Troelstra behoord hebben, die het gebruik van dit soort redeneringen vermijden. Zij eisen constructieve bewijzen.

Samenvattend kan ik zeggen dat de getallen op te bouwen zijn op een simpele manier via de optelling en op een ingewikkelde en interessantere manier via de vermenigvuldiging. Bij de vermenigvuldiging krijgen we te maken met onregelmatige rijen zoals de rij van de priemgetallen,

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...

en de rij van *machten* (getallen x^n met $x > 1$ en $n > 1$),

4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, 169, 196, 216, 225, 243, 256, 289, ...

Het wordt pas echt ingewikkeld als optelling en vermenigvuldiging een rol spelen. Er zijn talloze simpele vragen van dit type waarop we het antwoord niet weten. Zo is nog steeds niet bekend

of het oneindig vaak voorkomt dat priemgetallen twee verschillen (*priemgetaltweelingen*)

(bijv. 11 en 13, 29 en 31, 59 en 61, 101 en 103)

of het oneindig vaak voorkomt dat een priemgetal een macht $+1$ is

(bijv. 5, 17, 37, 101)

of het oneindig vaak voorkomt dat een priemgetal een macht -1 is (*Mersennepriemgetal*)

(bijv. 7, 31, 127, 1023)

of elk even getal >2 te schrijven is als som van twee priemgetallen (Goldbach, 1770)

(bijv. $4=2+2$, $6=3+3$, $8=5+3$, $100=89+11$)

of 8 en 9 de enige opeenvolgende getallen zijn die beide van de vorm x^n zijn met x en n groter dan 1. (*Vermoeden van Catalan*, 1844).

Vermenging van optelling en vermenigvuldiging vindt al plaats bij de stelling van Pythagoras, die prof. Van Baal in de tweede lezing van deze cyclus heeft afgeleid. We vermenigvuldigen om kwadraten te krijgen en tellen dan twee kwadraten op om een derde te krijgen:

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

Pythagoras leefde omstreeks het jaar - 550. Al in zijn tijd, en ook in oudere Chinese en Hindoe vondsten, werden getallen gevonden die hieraan voldoen, zoals

$$32 + 42 = 52$$

$$122 + 52 = 132$$

$$152 + 82 = 172.$$

Er zijn zelfs oneindig veel van zulke *Pythagoreïsche drietallen*. Neem n.l. twee getallen r, s met r groter dan s . Definieer $a = r^2 - s^2$, $b = 2rs$, $c = r^2 + s^2$. Dan geldt $a^2 + b^2 = c^2$. Zo vinden we

bijvoorbeeld bij $r=20$, $s=17$ het Pythagoreïsche drietal $a = 111$, $b = 680$, $c = 689$. Euclides bewees dat alle Pythagoreïsche drietallen via zo'n representatie gevonden kunnen worden, maar ik zie ervan af u het bewijs voor te schotelen. Ik verwijs daarvoor naar [6, sectie 8-1].

Het bepalen van alle oplossingen van een vergelijking is iets dat in de Griekse oudheid nog niet algemeen gangbaar was. Een van de meest creatieve vergelijkingenoplossers, Diophantos van Alexandrië (rond het jaar 250), stelde zich ten doel om voor elk van zijn problemen een (rationale) oplossing te vinden en was daarmee tevreden. Vaak deed hij dat op een ingenieuze manier en soms kunnen met zijn methode ook alle oplossingen bepaald worden, maar hij lijkt er eenvoudigweg niet in geïnteresseerd geweest te zijn. Zijn boeken over Arithmetica werden in het westen bekend door vertalingen in het Latijn, eerst in 1575 een nogal gebrekkige door Xylander, daarna in 1621 een met commentaar door Bachet de Méziriac. Vergelijkingen in gehele of rationale getallen worden tegenwoordig dan ook *Diophantische vergelijkingen* genoemd. Een jurist uit Toulouse, Pierre de Fermat (1601-1665) heeft waarschijnlijk Bachet's vertaling met rode oortjes gelezen. Het vormde vermoedelijk Fermat's introductie tot de getaltheorie. Fermat heeft talrijke fundamentele eigenschappen van getallen ontdekt, maar er zijn maar weinig door hem gegeven (volledige) bewijzen aan ons bekend. Evenals veel van zijn tijdgenoten daagde hij anderen uit om bewijzen te vinden die hijzelf ook gevonden had. Een aantal resultaten werd door Fermat genoemd in zijn correspondentie met tijdgenoten, zoals Descartes, Huygens en Mersenne. Ook in de marge van zijn Diophantos noteerde Fermat verschillende observaties, zoals deze bij hem opkwamen bij het lezen van het boek. Na Fermat's dood werd het gehele boek, tezamen met de aantekeningen van Fermat, in 1670 gepubliceerd door zijn zoon Samuel.

Eén aantekening zou wereldberoemd worden. Diophantos liet zien hoe je een gegeven kwadraat kunt splitsen in de som van twee kwadraten (van rationale getallen). Hier schreef Fermat de volgende woorden in de kantlijn:

Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Vertaald in het Nederlands staat er: Het is echter onmogelijk om een derdemacht als de som van twee derdemachten te schrijven, een vierdemacht als de som van twee vierdemachten en in het algemeen enige macht voorbij de tweede als de som van twee gelijke machten. Hiervoor heb ik een waarlijk wonderbaarlijk bewijs, maar de marge is te klein om het te bevatten.

Het is verbazingwekkend dat deze tekst nog in de marge paste. Dat zijn bewijs er niet in paste wekt minder verbazing. Nergens anders heeft Fermat het probleem in deze algemeenheid genoemd. Voor de bewering dat een vierdemacht niet te schrijven is als som van twee

vierdemachten had Fermat duidelijk zelf een bewijs. Met dezelfde, door Fermat ontdekte, methode kan ook voor derdemachten bewezen worden dat ze niet de som van twee derdemachten kunnen zijn, zoals later door Euler werd aangetoond. Deze twee gevallen worden ook genoemd in brieven van Fermat. Zo vraagt Fermat in een brief aan Engeland en Holland om te denken over het probleem om een derdemacht te schrijven als som van twee derdemachten. [4, p. 342] De methode werkt echter niet voor machten die hoger zijn dan de vierde.

Nadat Euler alle nog openstaande beweringen van Fermat op de bovenstaande na bewezen of weerlegd had, werd bovenstaande bewering bekend als *de laatste stelling van Fermat*. Hoewel de stelling zelf betrekkelijk weinig consequenties heeft voor de rest van de wiskunde, leidde het zoeken van een bewijs tot de ontwikkeling van nieuwe methoden in de wiskunde. Fermat's bewering komt erop neer dat de vergelijking

$$x^n + y^n = z^n$$

geen oplossingen in getallen x, y, z, n met $n > 2$ heeft. Merk op dat we zonder verlies van algemeenheid mogen aannemen dat x, y en z *onderling ondeelbaar* zijn, d.w.z. niet door hetzelfde priemgetal deelbaar zijn. Zoals gezegd bewees Fermat zelf het geval $n=4$ en Euler het geval $n=3$. Zonder verlies van algemeenheid kan men zich nu verder tot priemexponenten beperken. Het geval $n=5$ werd omstreeks 1825 bewezen door de Duitser Lejeune-Dirichlet en de Fransman Legendre, het geval $n=7$ in 1839 door de Fransman Lamé. Op 1 maart 1847 kondigde Lamé in de Parijse *Académie des Sciences* aan dat hij de laatste stelling van Fermat geheel bewezen had [3]. In zijn bewijs had hij echter aangenomen dat de algebraïsche getallen die hij gebruikte unieke priemontbinding bezaten. Dit bleek niet het geval te zijn. Ook grote wiskundigen liepen in de val van de onterechte aanname van unieke priemontbinding. Hoe de zaken werkelijk in elkaar staken was juist daarvoor ontdekt door Kummer in Duitsland. In 1845 had hij de theorie van *ideale getallen* ontwikkeld die de grondslag vormt van de hedendaagse algebraïsche getaltheorie. In de ideaaltheorie is door een uitbreiding van de algebraïsche getallen met idealen de unieke priemontbinding weer herwonnen. Kummer gebruikte zijn theorie om aan te tonen dat de laatste stelling van Fermat juist is voor alle priemexponenten onder de 100 met uitzondering van 37, 59 en 67. Zie [7].

In de twintigste eeuw ging de grens waarvoor de stelling bewezen was snel omhoog, met name door de steeds snellere rekenmachines. In 1937 was ze bewezen voor exponenten tot 617, in 1954 tot 4001, in 1976 tot 125000 and in januari 1993 tot 4000000. Overigens zou met de gebruikte methode nooit een volledig bewijs voor de laatste stelling van Fermat verkregen kunnen worden, omdat er oneindig veel priemgetallen zijn en elk priemgetal apart getest moest worden. Er waren dus andere methoden nodig. Een heel belangrijke stap leek door Faltings in 1983 gezet te worden. Faltings bewees met een nieuwe methode o.a. dat er voor een vaste exponent n maar eindig veel oplossingen x, y, z kunnen zijn die onderling ondeelbaar zijn. Toch zou het uiteindelijke bewijs met een heel andere methode bewezen worden. In een voordracht in Cambridge in juni 1993 kondigde de Engelsman A. Wiles, hoogleraar aan de universiteit van Princeton in de Verenigde Staten, aan dat hij een bewijs van de laatste stelling van Fermat gevonden had. Elk jaar waren er aankondigingen van bewijzen van de laatste stelling van Fermat en vaak werd er nauwelijks op gereageerd, maar het vertrouwen in Wiles en de in zijn voordracht gegeven argumenten was zo groot dat direct de internationale pers op de hoogte werd gebracht. De volgende dag stond het nieuws met foto van Wiles op de voorpagina van de New York Times en vergelijkbare kranten. Vijf referenten, deskundigen op het gebied van de gebruikte algebraïsche meetkunde methoden, ploegden het lange bewijs door waaraan Wiles zeven jaar in stilte had gewerkt. Het bleef stil tot Wiles in december 1993 in een e-mail toegaf dat zijn "bewijs" een gat bevatte, dat hij binnen een half jaar hoopte te repareren. Overigens bevatte het manuscript van Wiles vele originele en diepe gedachten die wel goed uitgewerkt waren. Er werden door wiskundigen discussies gevoerd of het nu wel of niet goed was voor de wiskunde dat de aankondiging van Wiles zoveel aandacht had gekregen en nu onjuist bleek. Enerzijds werd betoogd dat dit het vertrouwen in wiskundigen schaadde, anderzijds dat mensen nu bij het

proces van het ontdekken betrokken werden en niet pas nadat alles al in details uitgewerkt was. Na een jaar was er nog geen nieuws. Inmiddels had Wiles echter met behulp van R. Taylor een totaal andere weg gevonden om het ravijn in zijn bewijs te vermijden. In mei 1995 verscheen een uitgave van de Annals of Mathematics, het meest vooraanstaande wiskundetijdschrift, die geheel bestond uit het bewijs van het semi-stabiele geval van het vermoeden van Taniyama-Shimura-Weil, waaruit zoals al eerder bewezen was de laatste stelling van Fermat volgt. Nadat in de loop van eeuwen duizenden "bewijzen" van de laatste stelling van Fermat de toets der kritiek niet hadden kunnen doorstaan, was er eindelijk een bewijs dat wel door leidinggevende wiskundigen als correct beoordeeld werd. Voor een levendig verslag van de worsteling van Wiles verwijs ik naar een BBC-documentaire waarin alle betrokkenen te zien en te horen zijn en naar een boekje van Singh [8]. Ik zal niet proberen u het bewijs uit te leggen. Ik volsta ermee te zeggen dat het gaat met algebraïsche getaltheorie en algebraïsche meetkunde. Net als in het geval van Kummer en Faltings is de reikwijdte van de bewezen resultaten veel verder dan alleen de laatste stelling van Fermat.

Soms wordt me verbaasd gevraagd wat een wiskundige aan onderzoek doet. Is niet alles al bekend? Sommige leken kregen door de berichtgeving het gevoel dat met het resultaat van Wiles de ontbrekende schakel gevonden was en wiskundigen nu ander werk moesten gaan zoeken. Ik wil de rest van mijn voordracht gebruiken om een beeld te geven van de latere ontwikkelingen.

Waarom zou je je beperken tot machten met gelijke exponenten? Hoe zit het met de oplossingen van de vergelijking

$$(2) x^k + y^m = z^n$$

waarbij k, m, n, x, y, z , getallen zijn die alle groter dan 1 zijn? In een voordracht in Utrecht in november 1993 tijdens de toen gehouden Fermat-dag ter ere van de eerste aankondiging van Wiles heb ik deze diophantische vergelijking besproken [2]. Als er geen beperking aan x , y en z wordt opgelegd, is het niet moeilijk om willekeurig veel oplossingen te construeren. We veronderstellen daarom dat x , y en z onderling ondeelbaar deelbaar zijn. Verder zijn er vele oplossingen als $(1/k) + (1/m) + (1/n)$ groter is dan 1, wat alleen het geval is als de exponenten in enige volgorde gelijk zijn aan $(2, 2, *)$, $(2, 3, 3)$, $(2, 3, 4)$ of $(2, 3, 5)$. Als $(1/k) + (1/m) + (1/n)$ gelijk is aan 1, zijn er geen oplossingen. Dit is het geval voor de drietallen $(2, 2, 4)$, $(2, 3, 6)$, $(3, 3, 3)$. Voor de resterende exponenten is het een moeilijk probleem. Dat is niet zo vreemd, want de vergelijking van Fermat krijgen we door $k=m=n$ te nemen.

Vergelijking (2) is dus nog moeilijker dan die van Fermat.

Er waren al enkele kleine oplossingen van (2) met de aangegeven restricties bekend. Tijdens de voorbereidingen van de Fermat-dag vonden Frits Beukers en Don Zagier totaal onverwacht nog vijf grote oplossingen. Daarna zijn geen nieuwe oplossingen meer gevonden. De nu bekende oplossingen van (2) met x, y, z , onderling ondeelbaar en $(1/k) + (1/m) + (1/n) < 1$ zijn: [1, blz. 180-188; 2, blz. 19-23]

$$132 + 73 = 29, 27 + 173 = 712, 25 + 72 = 34, 35 + 114 = 1222,$$

$$177 + 762713 = 210639282, 14143 + 22134592 = 657, 92623 + 153122832 = 1137,$$

$$438 + 962223 = 300429072, 338 + 15490342 = 156133.$$

Tijdens mijn voordracht merkte ik op dat in elke vergelijking een exponent 2 voorkomt. Naar aanleiding daarvan formuleerde ik het volgende vermoeden, dat door $k=m=n$ te nemen de laatste

stelling van Fermat inhoudt:

Er zijn geen getallen k, m, n, x, y, z , alle groter dan 1 en met de eigenschappen dat x, y, z onderling ondeelbaar zijn, dat k, m, n alle groter dan 2 zijn en dat $x^k + y^m = z^n$.

Inmiddels heeft de Amerikaanse bankier Beal enige tientallen duizenden dollars voor de oplossing van dit probleem uitgelooft en staat dit probleem bekend als het vermoeden van Beal [5].

In Leiden is er inmiddels wat vooruitgang geboekt. Mijn promovendus Nils Bruin is vorig jaar gepromoveerd op een proefschrift waarin hij bewees dat er geen andere oplossingen bestaan dan de hierboven aangegeven oplossingen als de exponenten in enige volgorde gelijk zijn aan (2,4,5), (2,4,6) of (2,3,8). Ook elders is vooruitgang geboekt met betrekking tot gegeneraliseerde Fermatvergelijkingen.

Overigens is het vermoeden van Beal niet het probleem dat tegenwoordig centraal staat in dit deel van de getaltheorie. Dat is n.l. het abc-vermoeden, in 1985 door Oesterlé en Masser geformuleerd. Een zwakke vorm hiervan luidt als volgt:

Stel er zijn drie getallen a, b, c die niet door hetzelfde priemgetal deelbaar zijn terwijl $a+b=c$.

Dan is c kleiner dan het kwadraat van het product van alle priemgetallen die abc delen.

Nemen we bijvoorbeeld $a=32=2^5$, $b=49=7^2$, $c=81=3^4$, dan is het product van alle priemgetallen die abc delen gelijk aan $2^5 \cdot 7^2 \cdot 3^4 = 42$ en inderdaad is 81 kleiner dan het kwadraat van 42, dat is 1764.

Nemen we $a=1$, $b=4374=2^3 \cdot 3^7$, $c=4375=5^4 \cdot 7$, dan is het product van de betrokken priemgetallen $2^3 \cdot 3^7 \cdot 5^4 \cdot 7 = 210$ en 4375 is inderdaad kleiner dan het kwadraat van 210.

Voor elk drietal onderling ondeelbare getallen a, b, c die tot nog toe getest zijn blijkt dit principe op te gaan.

Het wordt steeds duidelijker hoe fundamenteel dit vermoeden is. De laatste stelling van Fermat volgt in één wiskunderegule uit het abc-vermoeden evenals het vermoeden van Catalan en een zwakkere vorm van het vermoeden van Beal.

Neem bijvoorbeeld aan dat x, y, z getallen zijn die voldoen aan $x^n + y^n = z^n$.

Dan zijn x^n en y^n beide kleiner dan z^n en daarom x en y beide kleiner dan z .

We mogen zonder verlies van algemeenheid aannemen dat x, y en z onderling ondeelbaar zijn.

Het product van de priemgetallen die x^n delen is ten hoogste gelijk aan x . Evenzo vinden we voor y^n ten hoogste y en voor z^n ten hoogste z .

Het product van de betrokken priemgetallen is daarom ten hoogste xyz en dit is kleiner dan z^3 . Volgens het abc-vermoeden toegepast op $x^n + y^n = z^n$ is z^n dus kleiner dan het kwadraat van z^3 .

Met andere woorden, $z^n < z^6$. Hieruit volgt voor elke oplossing dat $n < 6$.

We weten echter al 161 jaar dat er geen oplossingen zijn met $n=3,4$ of 5.

Dus er zijn helemaal geen oplossingen van de vergelijking van Fermat.

Bij de abc-berg vergeleken zijn de laatste stelling van Fermat, het vermoeden van Beal en het vermoeden van Catalan dus heuveltjes. Hoeveel jaren of eeuwen zullen verlopen voordat we ook de abc-berg bedwongen hebben? Voorlopig is er nog voldoende werk voor wiskundigen.

Referenties.

[1] F. Beukers, Getaltheorie voor Beginners, Epsilon uitgaven, Utrecht, 1999.

[2] De Laatste Stelling van Fermat, syllabus, Wiskundig Genootschap en Universiteit Utrecht, 1993.

[3] H.W. Lenstra, Jr., Euclidean Number Fields 1, The Mathematical Intelligencer 2 Number 1 (1979), 6-15.

[4] M.S. Mahoney, The Mathematical Career of Pierre de Fermat 1601-1665, Princeton University Press, 2^{de} druk, 1994.

[5] R.D. Mauldin, A generalization of Fermat's Last Theorem: the Beal conjecture and prize problem, Notices Amer. Math. Soc. 44 (1997), 1436-1437.

[6] O. Ore, Number Theory and Its History, Mc Graw-Hill, 1948.

[7] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer-Verlag, 1979.

[8] S. Singh, Fermat's Last Theorem, Fourth Estate, 1997. Vertaald in het Nederlands: Het Laatste Raadsel van Fermat, Arbeiderspers, 1997.

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
tijdeman@math.leidenuniv.nl