Jeanine Daems
Mathematisch Instituut
Universteit Leiden
Postbus 9512
2300 RA Leiden
jdaems@math.leidenuniv.nl

Beroemde problemen

Het vermoeden van Catalan

In april 2002 is een beroemd negentiende-eeuws vermoeden uit de getaltheorie, het vermoeden van Catalan, bewezen door Preda Mihăilescu. Als onderdeel van een reeks over beroemde wiskundeproblemen geeft Jeanine Daems een overzicht van de geschiedenis van het vermoeden en vertelt ze globaal hoe het bewijs in elkaar zit. Zij is in Leiden afgestudeerd in de getaltheorie en hoopt binnenkort ook haar studie filosofie van de wiskunde te voltooien.

Op het eerste gezicht doet het vermoeden van Catalan denken aan een veel beroemder vermoeden dat rond 1637 door Fermat geformuleerd werd en als 'stelling' de geschiedenis is ingegaan.

Laatste stelling van Fermat. Zij n een geheel getal dat groter is dan 2. Dan heeft de vergelijking

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

geen oplossingen in gehele getallen x, y en z die allemaal ongelijk aan 0 zijn.

Het vermoeden van Catalan, dat in 1844 voor het eerst geformuleerd werd, zegt dat twee 'echte' machten nooit verschil 1 kunnen hebben, tenzij ze gelijk zijn aan 9 en 8.

Vermoeden van Catalan. Laat m en n gehele getallen groter dan 1 zijn. De enige oplossing van

$$x^m - y^n = 1$$

in gehele getallen x en y die allebei ongelijk aan 0 zijn, is $(\pm 3)^2 - 2^3 = 1$.

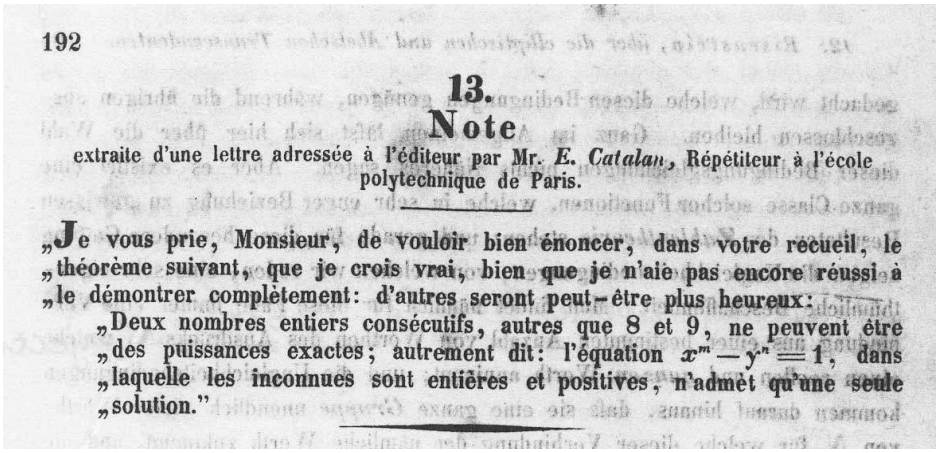
Ondanks de inspanningen van veel wiskundigen zijn zowel het vermoeden van Catalan als de laatste stelling van Fermat lange tijd onbewezen gebleven. Andrew Wiles bewees de laatste stelling van Fermat ongeveer tien jaar geleden en twee jaar geleden werd ook het vermoeden van Catalan bewezen, door Preda Mihăilescu.

Een belangrijk verschil tussen de bewijzen van deze vermoedens is dat het bewijs van Mihăilescu vooral theorie gebruikt die al enige tijd bekend was, terwijl Wiles voor zijn bewijs van de laatste stelling van Fermat een heleboel nieuwe wiskunde moest ontwikkelen.

Triviale oplossingen en priemmachten

In de formulering van de laatste stelling van Fermat zien we dat er een aantal eisen wordt opgelegd aan de oplossingen: n moet groter zijn dan 2, en x, y en z mogen niet 0 zijn. Deze eisen dienen om een aantal voor de hand liggende oplossingen uit te sluiten: een eerste macht is altijd de som van twee andere eerste machten, als n gelijk aan 2 is vinden we een heleboel oplossingen (denk aan de stelling van Pythagoras) en als bijvoorbeeld x gelijk aan 0 is, vinden we altijd oplossingen als we $y = z$ nemen.

Ook in de formulering van het vermoeden van Catalan dienen de voorwaarden die we aan de oplossingen opleggen ertoe om een aantal triviale oplossingen uit te sluiten. Zo verschilt een macht altijd 1 van een eerste macht (bijvoorbeeld $10^1 - 3^2 = 1$) en geldt voor alle m en n dat



192

13.

Note

extraite d'une lettre adressée à l'éditeur par Mr. *E. Catalan*, Répétiteur à l'école polytechnique de Paris.

„Je vous prie, Monsieur, de vouloir bien énoncer, dans votre recueil, le „théorème suivant, que je crois vrai, bien que je n'aie pas encore réussi à „le démontrer complètement: d'autres seront peut-être plus heureux:

„Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être „des puissances exactes; autrement dit: l'équation $x^m - y^n = 1$, dans „laquelle les inconnues sont entières et positives, n'admèt qu'une seule „solution."

Figuur 1 In het jaar 1844 stuurde de Belgische wiskundige Eugène-Charles Catalan (1814–1894) deze brief, waarin hij zijn vermoeden formuleerde, naar de redactie van het wiskundetijdschrift Crelle.

$1^m - 0^n = 1$.

Merk op dat we om het vermoeden van Catalan te bewijzen niet naar alle mogelijke exponenten m en n groter dan 1 hoeven te kijken. Iedere echte macht is een priemmacht, x^{21} is behalve een 21ste macht immers ook een derde en een zevende macht: $x^{21} = (x^7)^3 = (x^3)^7$. Zo zien we: als er een niet-triviale oplossing bestaat van $x^m - y^n = 1$ als m of n geen priemgetal is, dan bestaat er ook een niet-triviale oplossing van een vergelijking $x^p - y^q = 1$ waarbij p en q allebei priemgetallen zijn. Daarom hoeven we alleen te laten zien dat de vergelijking $x^p - y^q = 1$ voor priemgetallen p en q geen niet-triviale oplossingen heeft (op het uitzonderingsgeval na).

Catalan

In het jaar 1844 stuurde de Belgische wiskundige Eugène-Charles Catalan (1814–1894) een brief naar de redactie van het wiskundetijdschrift *Crelle* waarin hij zijn vermoeden formuleerde. Catalan heeft zelf geprobeerd zijn vermoeden te bewijzen, maar het is hem niet gelukt. In de brief sprak hij de hoop uit dat andere wiskundigen daar misschien wel in zouden slagen:

Je vous prie, Monsieur, de vouloir bien énoncer, dans votre recueil, le théorème suivant, que je crois vrai, bien que je n'aie pas encore réussi à le démontrer complètement: d'autres seront peut-être plus heureux:

Deux nombres entiers consécutifs, autres que 8 *et* 9, *ne peuvent être des puissances exactes; autrement dit: l'équation* $x^m - y^n = 1$, *dans laquelle les inconnues sont entières et positives, n'admèt qu'une seule solution.*

Na deze brief heeft Catalan lange tijd niets meer over zijn vermoeden gepubliceerd, tot in 1885. Toen publiceerde de Société Royale des Sciences de Liège [4] een overzicht van zijn leven en werk, waarin Catalan vertelt over zijn verrichtingen in de periode dat hij zelf over zijn vermoeden nadacht. Hij vond het onderzoek zo vermoeiend dat hij er na bijna een jaar mee is gestopt:

Après avoir perdu près d'une année à la recherche d'une démonstration qui fuyait toujours, j'abandonnai cette recherche fatigante.

Euler: het geval met oplossingen

Al voor Catalan de algemene formulering van zijn vermoeden publiceerde, waren sommige speciale gevallen van de vergelijking $x^m - y^n = 1$ onderzocht. Eén van deze gevallen is

$$x^2 - y^3 = 1,$$

de vergelijking die in het vermoeden een uitzondering vormt, omdat ze wel niet-triviale oplossingen heeft, bijvoorbeeld $x = \pm 3$ en $y = 2$. Leonhard Euler (1707–1783) bewees in 1738 dat dit ook alle niet-triviale oplossingen van deze vergelijking zijn [6]. In zijn bewijs gebruikte hij Fermats methode van oneindige descent.

De terminologie van *elliptische krommen* geeft een modernere manier om over deze vergelijking te praten. De vergelijking $x^2 - y^3 = 1$ is namelijk de vergelijking van een elliptische kromme. De theorie van elliptische krommen geeft een standaard descent-methode om de rationale punten op zo'n kromme te bepalen. Als we deze methode toepassen, vinden we dat de enige rationale punten op deze kromme de punten $(x, y) = (0, -1)$, $(1, 0)$, $(-1, 0)$, $(3, 2)$ en $(-3, 2)$ zijn. Dit betekent dat de vergelijking inderdaad de twee niet-triviale oplossingen uit het vermoeden heeft en geen andere.

Uit het vergelijken van de beide bewijzen blijkt dat ze eigenlijk hetzelfde zijn. Als we Eulers bewijs vertalen in termen van elliptische krommen, dan zien we dat Eulers slimme substituties overeenkomen met voor de hand liggende operaties op de kromme. Meer details zijn te vinden in [5].

Resultaten voor even exponenten

Catalan spoorde in zijn brief uit 1844 andere wiskundigen aan zich over zijn probleem te buigen. Het eerste resultaat verscheen na zes jaar, in 1850. De Franse wiskundige Victor Amédée Lebesgue (1791–1875) (niet te verwarren met de veel beroemdere Henri Lebesgue) publiceerde een artikel [9] over de vergelijking

$$x^p - y^2 = 1,$$

waarbij p een priemgetal is. Hij bewees dat deze vergelijking geen niet-triviale oplossingen heeft.

Hij schreef de vergelijking als $x^p = y^2 + 1$. We zien dat $y^2 + 1$ de p-de macht van een geheel getal moet zijn. Lebesgue werkte in de ring $\mathbf{Z}[i]$, de ring van *gehele getallen van Gauss*. Deze ring bestaat uit getallen van de vorm $a + bi$, waarbij a en b gehele getallen zijn en i^2 gelijk is aan -1. In de ring $\mathbf{Z}[i]$ kunnen we $y^2 + 1$ verder ontbinden als $(y + i)(y - i)$. Wat Lebesgue vervolgens bewees is dat ook $y + i$ en $y - i$ gelijk moeten zijn aan p-de machten van getallen uit $\mathbf{Z}[i]$. Daaruit leidde hij een tegenspraak af.

Ook de volgende resultaten die geboekt werden, hadden betrekking op de Catalanvergelijking met kleine exponenten.

In 1965 bewees Ko Chao [8] dat de vergelijking $x^2 - y^q = 1$ geen oplossingen heeft als q een priemgetal groter dan 3 is. We hebben al gezien wat de oplossingen zijn als q gelijk aan 3 is, dus hiermee is de vergelijking $x^2 - y^n = 1$ voor alle n groter dan 1 behandeld. Aangezien Lebesgue het geval $x^m - y^2 = 1$ al had opgelost, is het vermoeden van Catalan nu teruggebracht tot de volgende uitspraak.

Stelling van Mihăilescu. Laat p en q oneven priemgetallen zijn. Dan heeft de vergelijking

$$x^p - y^q = 1$$

geen oplossingen in gehele getallen x en y ongelijk aan 0.

Slechts eindig veel oplossingen

Deze uitspraak zegt iets heel sterks, namelijk dat de vergelijking $x^p - y^q = 1$ helemaal geen oplossingen heeft. Op het eerste gezicht is echter helemaal niet duidelijk waarom de Catalanvergelijking zelfs niet oneindig veel oplossingen zou kunnen hebben. Uit een resultaat van Siegel uit 1929 volgt dat de Catalanvergelijking voor *vaste* p en q slechts eindig veel oplossingen heeft, maar er zouden nog wel oneindig veel paren priemgetallen kunnen bestaan waarvoor er oplossingen zijn.

In 1976 gaf Robert Tijdeman [13] uitsluitsel over deze vraag. Hij bewees dat er maar eindig veel viertallen p, q, x en y kunnen bestaan die een niet-triviale oplossing vormen van $x^p - y^q = 1$. Hij gebruikte hiervoor Alan Bakers methode van logaritmische vormen.

Tijdeman bewees niet alleen dat er maar eindig veel oplossingen bestaan, maar ook dat er een effectief berekenbare bovengrens voor de absolute waarden van p, q, x en y van een mogelijke oplossing van $x^p - y^q = 1$ bestaat. Langevin berekende dat p en $q \leq 10^{110}$ zijn. Deze bovengrens was echter zo groot, dat het niet mogelijk was om alle mogelijkheden na te gaan met een computer. De bovengrens werd aanzienlijk verlaagd, bijvoorbeeld door Mignotte en Roy, maar nog niet voldoende om een computerbewijs te kunnen leveren.

Het bewijs van Mihăilescu gebruikt de consequenties van het resultaat van Tijdeman niet. Het bewijs zoals het nu is, is vooral algebraïsch van aard.

Bewijs uit het ongerijmde

Om te laten zien dat een bepaalde vergelijking oplossingen heeft, is het voldoende om een oplossing te construeren. Het is moeilijker om te laten zien dat een bepaalde vergelijking *geen* oplossingen heeft. Een bewijs daarvan is meestal een *bewijs uit het ongerijmde*: we nemen aan dat de vergelijking in kwestie wel een oplossing heeft en vervolgens leiden we zoveel eigenschappen van deze hypothetische oplossing af dat er een tegenspraak ontstaat. Dan kan deze oplossing dus niet bestaan.

Wiles nam in zijn bewijs aan dat de Fermatvergelijking een oplossing heeft. Gerhard Frey had in 1984 met behulp van een dergelijke oplossing een elliptische kromme, de *Freykromme*, geconstrueerd. Kenneth Ribet had bewezen dat de Freykromme niet modulair kon zijn. Wiles heeft uiteindelijk laten zien dat alle elliptische krommen modulair zijn. De Freykromme kan dus niet bestaan en de hypothetische oplossing van de Fermatvergelijking ook niet.

Het bewijs van Mihăilescu is ook een bewijs uit het ongerijmde, maar zijn bewijs verloopt directer. Hij neemt een hypothetische niet-triviale oplossing van de Catalanvergelijking aan en hij leidt vervolgens eigenschappen van die oplossing af die in tegenspraak zijn met al bekende theorie.

Het resultaat van Cassels

Laat vanaf nu de oneven priemgetallen p en q en de gehele getallen x en y een hypothetische niet-triviale oplossing van $x^p - y^q = 1$ vormen.

Een aantal belangrijke eigenschappen van zo'n hypothetische oplossing van de Catalanvergelijking werd afgeleid door John William Scott Cassels [2] in 1960. Hij bewees onder andere dat p een deler van y is en q een deler van x.

In 1964 scherpte Seppo Hyyrö de resultaten van Cassels verder aan. Zo bewees hij een aantal relaties tussen p, q, x en y en hij vond een hoge ondergrens voor de absolute waarde van x. In het huidige bewijs van het vermoeden van Catalan wordt inderdaad een ondergrens voor $|x|$ gebruikt, maar het is niet nodig om deze hoge ondergrens van Hyyrö te gebruiken: uit Cassels' resultaat volgt ook al een ondergrens en deze is goed genoeg voor Mihăilescu's bewijs.

Cyclotomische lichamen

Zoals we al gezien hebben, rekende Lebesgue in de ring $\mathbf{Z}[i]$ in plaats van met gewone gehele getallen, omdat $y^2 + 1$ in $\mathbf{Z}[i]$ wel in lineaire factoren te ontbinden is. Iets soortgelijks is handig nu we kijken naar de vergelijking $x^p - y^q = 1$. Deze vergelijking is te schrijven als $y^q = x^p - 1$. Het polynoom $x^p - 1$ heeft 1 als nulpunt, maar de andere nulpunten zijn niet reëel.

Foto rechts: Eugène-Charles Bardin (1814–1894), geboren in Brugge, werd pas in 1821 door zijn vader, de Parijse juwelier Joseph Catalan, erkend. Catalan ging in 1825 in Parijs wonen. Als briljante leerling verkreeg hij *licences* (bachelors) in de wiskunde en natuurkunde, een doctoraat in de wiskunde, en een eerste plaats bij de *agrégation*, het landelijke concours voor de eerstegraads lerarenopleiding. Na les gegeven te hebben aan verschillende Parijse instellingen, nam hij in 1865 een universitaire positie in Luik. In 1884 ging hij met emeritaat. Als republikein stortte Catalan zich met hartstocht in politieke activiteiten, voornamelijk tussen ongeveer 1830 en 1850. Zijn werkzaamheden betroffen vooral de meetkunde.

Zij liggen in het lichaam $\mathbf{Q}(\zeta_p)$. Dit lichaam ontstaat als we aan het lichaam $\mathbf{Q}$ van de rationale getallen de primitieve p-de eenheidswortel

$$\zeta_p = \mathrm{e}^{\frac{2\pi i}{p}}$$

toevoegen.

De p-de eenheidswortels liggen in het complexe vlak allemaal op de eenheidscirkel en ze delen deze cirkel precies in p gelijke stukjes op. Daarom noemen we het lichaam $\mathbf{Q}(\zeta_p)$ ook wel een *cyclotomisch* lichaam, naar de Griekse woorden $\kappa\upsilon\kappa\lambda o\varsigma$ ('kring') en $\tau o\mu\eta$ ('snede' of 'deling').

In $\mathbf{Q}(\zeta_p)$ ontbindt het polynoom $x^p - 1$ als

$$(x-1)(x-\zeta_p)(x-\zeta_p^2)\cdot\ldots\cdot(x-\zeta_p^{p-1}).$$

Als er een niet-triviale oplossing bestaat van de Catalanvergelijking, moet dit product een q-de macht zijn van een geheel getal.

Het lichaam $\mathbf{Q}(\zeta_p)$ verschilt in een belangrijk opzicht van de lichamen $\mathbf{Q}$ of $\mathbf{Q}(i)$: voor $p > 19$ is er in $\mathbf{Q}(\zeta_p)$ geen eenduidige priemfactorisatie. Er bestaat echter in $\mathbf{Q}(\zeta_p)$ wel eenduidige priemfactorisatie van *idealen*. Het verschil tussen unieke priemfactorisatie in getallen en unieke priemfactorisatie in idealen wordt gemeten door het *klassengetal* h_p, een positief geheel getal. Als het klassengetal gelijk aan 1 is, dan is er unieke priemfactorisatie in getallen, anders niet.

Het klassengetal is op natuurlijke wijze een product $h_p = h_p^+ \cdot h_p^-$, waarbij h_p^+ en h_p^- de ordes van andere invarianten van $\mathbf{Q}(\zeta_p)$ zijn. Het getal h_p^- is de index van het zogenaamde *Stickelbergerideaal* en h_p^+ is de index van de cyclotomische eenheden in de hele eenhedengroep. Zowel het Stickelbergerideaal en de cyclotomische eenheden spelen een belangrijke rol in Mihăilescu's bewijs.

Wieferichparen en klassengetallen

In de jaren negentig vond een aantal ontwikkelingen plaats die de aanzet vormen van Mihăilescu's bewijs. In 1990 werd door Kustaa Inkeri [7] het begrip *dubbel Wieferichpaar* geïntroduceerd. Een dubbel Wieferichpaar is een paar oneven priemgetallen (P, Q) zodat geldt: $P^{Q-1} \equiv 1 \mod Q^2$ en $Q^{P-1} \equiv 1 \mod P^2$.

Er zijn maar vijf dubbele Wieferichparen bekend: $(3, 1006003)$, $(5, 1645333507)$, $(83, 4871)$, $(911, 318917)$ en $(2903, 18787)$.

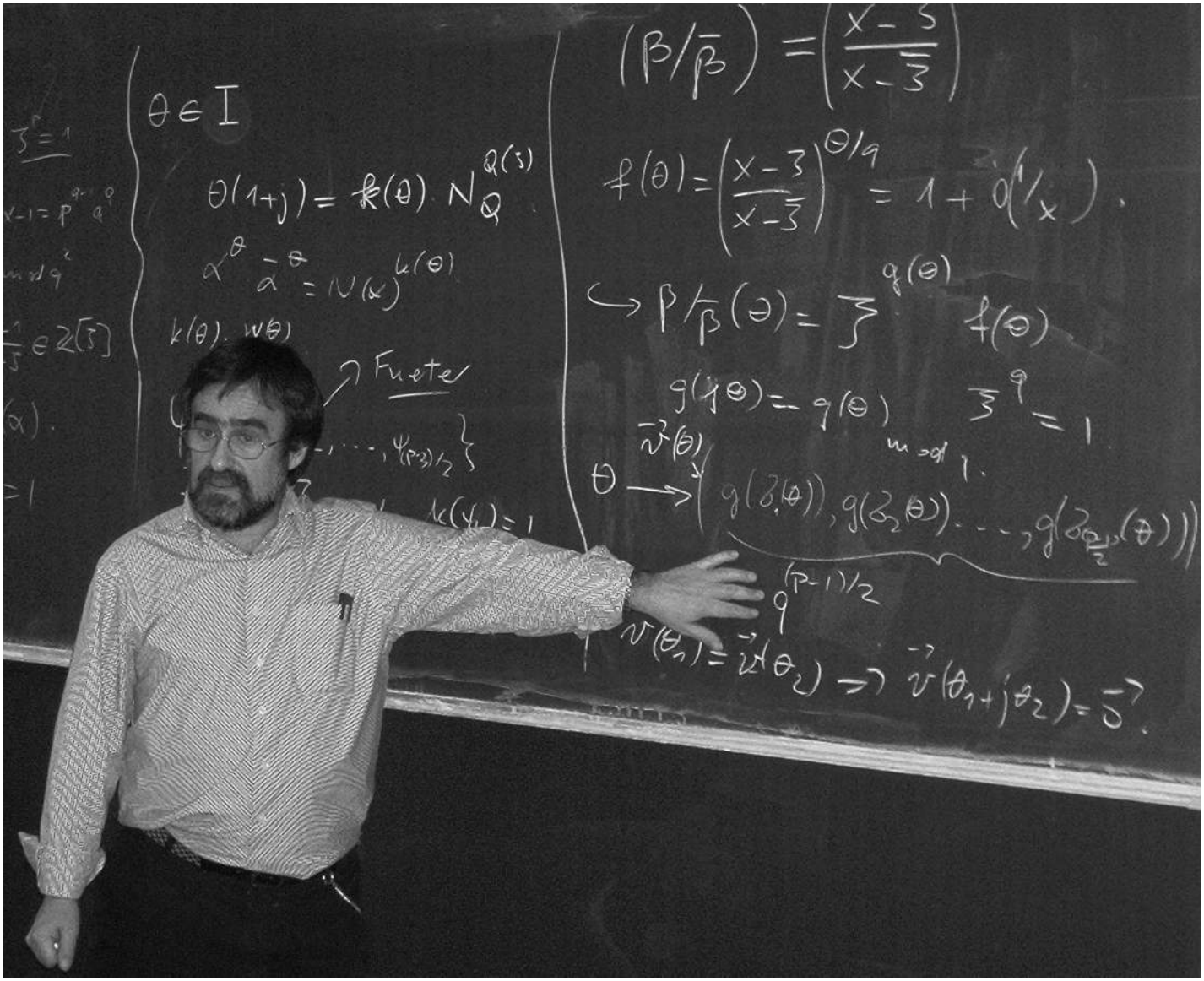


foto: Reinhold Kainhofer, Vienna University of Technology, Wenen

Preda Mihăilescu geeft een lezing op het colloquium getaltheorie van het *Institut für Mathematik A* van de Universiteit van Graz, Oostenrijk

Uit de kleine stelling van Fermat volgt al dat voor de priemgetallen p en q uit onze hypothetische oplossing geldt dat $p^{q-1} \equiv 1 \mod q$ en $q^{p-1} \equiv 1 \mod p$. Inkeri liet zien dat òf (p,q) een Wieferichpaar is, òf q deelt h_p, òf p deelt h_q.

In 2000 vonden Yann Bugeaud en Guillaume Hanrot een klassengetalconditie waaruit volgde dat de Catalanvergelijking geen niet-triviale oplossingen kan hebben als p of q kleiner is dan 43. Ook vonden Mignotte en Schwarz nog verbeteringen van de klassengetalconditie van Inkeri.

Het bewijs van Mihăilescu

Begin 2002 stuurde Mihăilescu het bericht rond dat hij het vermoeden van Catalan bewezen had. Deze mededeling werd sceptisch ontvangen door de wiskundige gemeenschap. Pas nadat Yuri Bilu het bewijs gecontroleerd had en er een overzichtelijker geheel van had gemaakt [1], ging men geloven dat het vermoeden inderdaad bewezen was.

Een van de belangrijkste resultaten die Mihăilescu heeft gevonden is een conditie op p en q waarin geen klassengetallen meer voorkomen [10]. Hij laat zien dat (p,q) een dubbel Wieferichpaar is. Hiervoor gebruikt hij het Stickelbergerideaal. Samen met het resultaat van Cassels dat p een deler is van y en q van x kan nu eenvoudig worden bewezen dat p^2 een deler is van y en q^2 van x.

Daarna valt Mihăilescu's bewijs in twee delen uiteen. Hij onderscheidt twee gevallen: het geval waarin p een deler is van $q-1$ en het geval waarin p geen deler van $q-1$ is.

Eerst kijken we naar het geval waarin p geen deler is van $q-1$. Een belangrijke stelling die Mihăilescu gebruikt is een stelling van Francisco Thaine uit 1988, die als voorwaarde heeft dat p geen deler is van $q-1$. Met behulp van de methode van Runge en de theorie van cyclotomische eenheden leidt hij een tegenspraak af.

Het geval waarin p wel een deler is van $q-1$ ging in eerste instantie op een heel andere manier dan in de uiteindelijke versie. Het bewijs gebruikte Mihăilescu's dubbele Wieferichcriterium, het resultaat van Tijdeman en een aantal computerberekeningen. In deze eerste versie was dus nog een aanzienlijke hoeveelheid analyse nodig.

In de zomer van 2003 gaf Bilu in Oberwolfach een lezing waaruit duidelijk werd dat Mihăilescu ook dit geval zonder computerberekeningen en zonder veel analyse had bewezen. Het bewijs is zelfs eleganter en eenvoudiger dan het bewijs van het andere geval. Ook in dit bewijs maakt hij gebruik van het Stickelbergerideaal. Met behulp van een beetje analyse en combinatoriek en de aanname dat p een deler is van $q-1$ bewijst hij dat $|x|$ klein moet zijn. De bovengrens voor $|x|$ die hij gevonden heeft, is echter kleiner dan de ondergrens voor $|x|$ die volgt uit Cassels' resultaten. Dit is met elkaar in tegenspraak. De conclusie luidt dat de hypothetische oplossing niet kan bestaan. Zo kwam Catalans hoop dat een andere wiskundige er wel in zou slagen zijn vermoeden te bewijzen na 150 jaar alsnog uit.

Referenties

1 Yuri F. Bilu, *Catalan's conjecture (after Mihăilescu)*, Séminaire Bourbaki, 909, 2002–2003.

2 J. W. S. Cassels, *On the equation $a^x - b^y = 1$. II*, Proceedings of the Cambridge Philosophical Society, volume 56, 1960; p. 97–103.

3 E. Catalan, *Note extraite d'une lettre adressée à l'éditeur*, Journal für die reine und angewandte Mathematik 27, 1844, p. 192.

4 Eugène-Charles Catalan, *Quelques théorèmes empiriques (1842–43)*, Mélanges Mathématiques, Mémoires de la Société Royale des Sciences de Liège, deuxième série, volume 12, 1885, p. 42–43.

5 J. Daems, *A Cyclotomic Proof of Catalan's Conjecture*, http://www.math.leidenuniv.nl/docs, afstudeerscriptie Universiteit Leiden, 2003.

6 L. Euler, *Commentationes Arithmeticae I*, Opera Omnia, serie I, deel II, B.G. Teubner, Basel, 1915, p. 56–58.

7 K. Inkeri, *On Catalan's Conjecture*, Journal of Number Theory, volume 34, 1990; p. 142–152.

8 Chao Ko, *On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$*, Scientia Sinica, 14, 1965; p. 457–460.

9 V. A. Lebesgue, *Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$*, Nouvelles annales de mathématiques, volume 9, 1850, p. 178–181.

10 P. Mihăilescu, *A class number free criterion for Catalan's conjecture*, Journal of Number Theory, 99, 2003; p. 225–231.

11 P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, Journal für die reine und angewandte Mathematik, te verschijnen.

12 Paulo Ribenboim, *Catalan's Conjecture – Are 8 and 9 the Only Consecutive Powers?* Academic Press, Boston, 1994.

13 R. Tijdeman, *On the equation of Catalan*, Acta Arithmetica, 29, 1976; p. 197–209.

14 Lawrence C. Washington, *Introduction to Cyclotomic Fields*, 2nd edition, Springer-Verlag, New York, 1997.