Jan Vonk
Mathematisch Instituut
Universiteit Leiden
j.b.vonk@math.leidenuniv.nl

Geschiedenis

Het twaalfde probleem van Hilbert

Voor Carl Friedrich Gauß (1777–1855) gold de getaltheorie als de koningin der wiskunde, en de theorie der *complexe vermenigvuldiging* van elliptische krommen wordt door sommigen als haar kroonjuweel gezien. David Hilbert (1862–1943) droeg deze theorie een bijzonder warm hart toe, en nam diens veralgemening op als het twaalfde op zijn lijst van 23 open problemen, die hij in 1900 voordroeg aan de wiskundige wereld. Wat hebben we over dit probleem geleerd sinds die tijd? En wat is het belang van beroemde open problemen in de wiskunde? In dit artikel laat Jan Vonk zijn licht schijnen op deze vragen.

Drijfveren van de wiskunde

Het belang van open problemen in de wiskunde is zo oud als de discipline zelf. Ze gelden als mijlpalen, en de vooruitgang en de kracht van het vakgebied worden erdoor gemeten. Maar waarom worden wiskundigen er zo door gegrepen? Dit heeft niet altijd te maken met het praktische nut van de vraag, en hoeft in sommige gevallen weinig meer te zijn dan schoonheid of persoonlijke nieuwsgierigheid. In sommige gevallen is het een zoektocht naar nieuwe structurele verbanden tussen verschillende vakgebieden, of krachtige toepassingen waar in de maatschappij vraag naar is, en in andere gevallen ligt het dan weer ergens anders. De open problemen van het grootste historische belang komen voor in elke kleur van het spectrum.

Voorbeeld 1. Dat belangrijke open problemen in de wiskunde lang niet altijd van groot praktisch nut hoeven te zijn, blijkt uit het voorbeeld van de *laatste stelling van Fermat*. Dit bekende probleem, geformuleerd door Pierre de Fermat (1607–1665) en opgelost door Andrew Wiles in 1993, stelt dat elke gehele oplossing $(x,y,z) \in \mathbb{Z}^3$ van de vergelijking

$$x^n + y^n = z^n, \quad n \geq 3,$$

noodzakelijk aan $xyz = 0$ moet voldoen. Dat wil zeggen, minstens één van haar coordinaten moet gelijk zijn aan nul. Dit staat in sterk contrast met het geval $n = 2$, waar oneindig veel niet-nul-oplossingen bestaan zoals $3^2 + 4^2 = 5^2$ en $5^2 + 12^2 = 13^2$, waarvan reeds tabellen gemaakt werden ten tijde van de Babyloniërs. De ontwikkeling van de wiskunde heeft enorm veel te danken aan dit probleem, en generaties wiskundigen zijn in hun creatieve pogingen tot inzichten gekomen van onschatbare waarde. De aantrekkingskracht van het probleem ligt dus in zijn eenvoud en schoonheid, maar het nut voor de wiskunde ligt vooral in de ontwikkelingen die tot haar oplossing geleid hebben, en de (vaak onvoorziene) toepassingen van die ontwikkelingen.

Voorbeeld 2. Aan de andere kant van het spectrum zijn er open problemen die een dieper structureel verband zoeken tussen verschillende takken van de wiskunde. Een klassiek voorbeeld is het vermoeden van Birch en Swinnerton-Dyer, dat een diep verband voorspelt tussen de *analyse* en *algebra* van zogenaamde elliptische krommen. Kies bijvoorbeeld je favoriete gehele getal $d > 0$ en beschouw de vergelijking

$$E_d \colon y^2 = x^3 + dx. \tag{1}$$

We kunnen ons afvragen hoeveel *rationale* oplossingen (x,y) deze vergelijking heeft. Het antwoord hangt sterk af van de gekozen waarde van d. Zo zijn er voor $d = 4$ eindig veel oplossingen (precies drie, namelijk $(0,0)$, $(2,4)$ en $(2,-4)$), en voor $d = 5$ oneindig veel oplossingen. Welk van deze gevallen het is, wordt bepaald door de zogenaamde *rang*, een algebraïsche invariant van de elliptische kromme E_d. Aan de hand van uitgebreide berekeningen met een computer, merkten Bryan Birch (geb. 1931) en Peter Swinnerton-Dyer (1927–2018) een onverwacht verband op met de limiet $\lim_{X \to +\infty} P(X)$, die de kritieke waarde van de L-functie van E meet; een *analytische* invariant van E_d. Hier is $P(X)$ de functie van X gedefinieerd door

$$P(X) \coloneqq \prod_{p < X} \frac{N_p}{p},$$

waarbij N_p het aantal oplossingen van (1) *modulo* p beduidt, en het product loopt over all priemgetallen $p < X$. De spectaculaire ontdekking van Birch–Swinnerton-Dyer was dat $P(X)$ groeit als een veelvoud van $\log(X)^r$, waarbij $r \geq 0$ de rang van E_d is. In het bijzonder is $P(X)$ begrensd wanneer E_d eindig veel rationale oplossingen heeft, en divergeert ze als er oneindig veel rationale oplossingen zijn.

Zelfs zonder de precieze vaktechnische formulering van het vermoeden van Birch–Swinnerton-Dyer, voelen we nu al aan dat dit een vraag van een andere aard is dan de laatste stelling van Fermat: haar kracht ligt in het onverwachte verband dat ze voorspelt tussen algebra en analyse. De verbazing die dit opwekte doet verwachten dat een bewijs zodanig baanbrekend zal moeten zijn, dat het onze inzichten fundamenteel zal veranderen. Dat het vermoeden waar is, betwijfelt inmiddels niemand meer. Wat we dus eigenlijk willen weten is niet *dat* het waar is, maar *waarom* het waar is.

De wiskundige gemeenschap hecht een enorm belang aan aantrekkelijke open problemen, en ze bepaalt ook steevast toonaangevende nieuwe open problemen. Soms gebeurt dat met de nodige publiciteit: op het Internationaal Congres voor Wiskundigen (ICM) in 1900 hield Hilbert een bijzondere rede, waarin hij een selectie van belangrijke open problemen voorstelde als uitdagingen voor de eeuw die komen zou. Bij de volgende eeuwwisseling in 2000 werd een gelijkaardige lijst met open problemen samengesteld door het Clay Mathematics Institute. Op deze laatste lijst staan zeven open problemen, waarvan reeds het vermoeden van Poincaré bewezen werd door Grigori Perelman (2003). De overige zes, inclusief het vermoeden van Birch–Swinnerton-Dyer dat we eerder noemden, zijn op dit moment nog steeds open.

Fermat en Euler

We zullen het hier nu hebben over één specifiek open probleem: Het twaalfde probleem van Hilbert. Zijn formulering is het resultaat van een lange evolutie, en maakt deel uit van een heus epos dat tot op de dag van vandaag nog steeds in volle ontwikkeling is. We beginnen ons verhaal met Pierre de Fermat (1607–1665) die voor priemgetallen p bewees dat

$$p = x^2 + y^2 \iff p = 2 \text{ of } p \equiv 1 \pmod 4$$

Hij dacht ook na over een algemenere versie: Wanneer is een priemgetal p van de vorm

$$p = x^2 + ny^2?$$

Het antwoord hangt sterk af van het gekozen gehele getal n. Vele generaties wiskundigen bogen zich over dit probleem, en we moedigen de energieke lezer aan om zelf hun favoriete waarde van n te kiezen, en hun eigen vermoeden te formuleren aan de hand van (al dan niet manuele) experimenten. Laat ons ter illustratie $n = 3$ kiezen, en voor enkele kleine priemgetallen nagaan of ze al dan niet van de gewenste vorm zijn. Het resultaat staat in Tabel 1, tweede kolom, waarbij een leegte duidt op een negatief antwoord.

Bij het maken van deze tabel vallen ons onmiddellijk enkele dingen op. Zo lijkt het bijvoorbeeld alsof we ongeveer de helft van de priemgetallen kunnen schrijven in de gewenste vorm. Daarnaast kunnen we ons laten inspireren door het geval $n = 1$ van Fermat, en pogen om een gelijkaardige congruentievoorwaarde te verzinnen. We komen al snel uit op het vermoeden dat

$$p = x^2 + 3y^2 \iff p = 3 \text{ or } p \equiv 1 \pmod 3.$$

Wie tot dezelfde conclusie kwam, is in goed gezelschap: Fermat zelf kwam tot deze conclusie, en beweerde ook een bewijs te hebben. Later schopte Euler (1707–1783) het nog veel verder, en vond niet alleen een bewijs voor de uitspraken van Fermat, maar dacht ook na over grotere waarden van n. Zijn ontdekkingen waren vaak erg verrassend. Laat ons bijvoorbeeld $n = 27$ kiezen. Dan is het resultaat de derde kolom van Tabel 1, een uitgedunde versie van de tweede kolom. Dit keer vinden we een heel stuk minder priemgetallen. De volgende priemgetallen in dit rijtje zijn

$$229, 277, 283, 307, 397, 433,$$
$$439, 457, 499, 601, 643, 691, \ldots$$

en als we deze berekening doorzetten krijgen we gemiddeld de indruk dat het aantal priemgetallen van deze vorm ongeveer $\frac{1}{6}$ van het totaal is. Het is een stuk minder duidelijk hoe deze priemgetallen beschreven kunnen worden. We zien dat ze noodzakelijk 1 modulo 3 zijn, maar die voorwaarde is duidelijk niet voldoende. Op basis van experimentele observaties kwam Euler tot het vermoeden dat de priemgetal-

p	x^2+3y^2	x^2+27y^2
2		
3	$0^2+3\cdot1^2$	
5		
7	$2^2+3\cdot1^2$	
11		
13	$1^2+3\cdot2^2$	
17		
19	$4^2+3\cdot1^2$	
23		
29		
31	$2^2+3\cdot3^2$	$2^2+27\cdot1^2$
37	$5^2+3\cdot2^2$	
41		
43	$4^2+3\cdot3^2$	$4^2+27\cdot1^2$
47		
53		
59		
61	$7^2+3\cdot2^2$	
67	$8^2+3\cdot1^2$	
71		
73	$5^2+3\cdot4^2$	
79	$2^2+3\cdot5^2$	
83		
89		
97	$7^2+3\cdot4^2$	
101		
103	$10^2+3\cdot1^2$	
107		
109	$1^2+3\cdot6^2$	$1^2+27\cdot2^2$
113		
127	$10^2+3\cdot3^2$	$10^2+27\cdot1^2$
131		
137		
139	$8^2+3\cdot5^2$	
149		
151	$2^2+3\cdot7^2$	
157	$7^2+3\cdot6^2$	$7^2+27\cdot2^2$
163	$4^2+3\cdot7^2$	
167		
173		
179		
181	$13^2+3\cdot2^2$	
191		
193	$1^2+3\cdot8^2$	
197		
199	$14^2+3\cdot1^2$	
211	$8^2+3\cdot7^2$	
223	$14^2+3\cdot3^2$	$14^2+27\cdot1^2$

Tabel 1 Priemgetallen van de vorm $p = x^2 + 3y^2$ naast priemgetallen van de vorm $p = x^2 + 27y^2$.

len van de vorm $p = x^2 + 27y^2$ *precies* deze zijn waarvoor

$$p \equiv 1 \pmod 3$$

en

$x^3 - 2 \equiv 0 \pmod p$ een oplossing heeft.

Euler kon dit vermoeden nooit bewijzen, en een bewijs kwam eerst van de hand van Gauß (1777–1855) die gebruikmaakte van zijn kubische wederkerigheidswet. De vlijtige lezer die ijverig tot zijn of haar eigen vermoedens kwam voor kleine waarden van n zal een schril contrast zien met $n = 27$, waar een congruentievoorwaarde niet toereikend is, en de 'magische' polynoom $x^3 - 2$ opduikt.

Het twaalfde probleem van Hilbert

Voor de polynoom $x^3 - 2$, die als deus ex machina in het werk van Euler opdook, kwam later een structurele verklaring. De wiskunde ontwikkelde ongeveer een eeuw na het werk van Gauß de *klassenlichamentheorie*, een mijlpaal die ons inzicht in deze vragen volledig transformeerde. Zo leerden we het volgende:

- De *klassenlichamentheorie* vertelt ons dat er voor elke waarde van n een 'magische polynoom' $f_n(x)$ bestaat met de eigenschap dat, op een eindig aantal uitzonderingen na, er geldt dat $p = x^2 + ny^2$ als en slechts als $-n$ een kwadraat is modulo p (dit is een congruentievoorwaarde op p, door de kwadratische wederkerigheidswet) en $f_n(x) \equiv 0 \pmod p$ een gehele oplossing heeft in x. In vaktermen is f_n een polynoom wiens nulpunten voortbrengers zijn van het zogenaamde *ringklassenlichaam* van $\mathbb{Z}[\sqrt{-n}]$. (De uitzonderingen zijn zogenaamde vertakte of singuliere priemgetallen, die men voor elke f_n expliciet kan bepalen.)
- De theorie der *complexe vermenigvuldiging* van elliptische krommen (afgekort CM-theorie, van het Engelse 'complex multiplication') stelt ons in staat om voor elke *positieve* waarde $n > 0$ een 'magische polynoom' $f_n(x)$ met deze eigenschappen te construeren. Bijvoorbeeld, in het geval $n = 23$ kunnen we

  $$f_{23}(x) = x^3 - x - 1$$

  gebruiken. Er geldt dat

$$p = x^2 + 23y^2 \iff \begin{cases} -23 \text{ is een kwadraat modulo } p \\ \text{en } x^3 - x - 1 \equiv 0 \pmod p \text{ heeft een oplossing.} \end{cases}$$

Klassenlichamentheorie

De klassenlichamentheorie geeft ons een volledige beschrijving van de eindige abelse uitbreidingen van een getallenlichaam K. De absolute Galoisgroep $\mathrm{Gal}(\bar{K}/K)$ heeft een maximaal abels quotiënt $\mathrm{Gal}(\bar{K}/K)^{\mathrm{ab}}$ dat beschreven wordt aan de hand van een surjectieve afbeelding

$$\varphi : C_K \to \mathrm{Gal}(\bar{K}/K)^{\mathrm{ab}}$$

van de idèle klassengroep C_K. Deze afbeelding heet de *Artin-afbeelding*, en induceert een isomorfisme tussen de pro-eindige completering van het domein en $\mathrm{Gal}(\bar{K}/K)^{\mathrm{ab}}$. Hierin ligt de kracht van klassenlichamentheorie: ze beschrijft alle abelse uitbreidingen ('externe' objecten) aan de hand van de 'interne' idèle klassengroep, een object dat helemaal beschreven kan worden aan de hand van de elementen en lichaamsoperaties van K zelf.

Ondanks de duidelijke structurele eigenschappen van de Artin-afbeelding, is haar definitie erg abstract, en is het helemaal niet duidelijk hoe ze in de praktijk te beschrijven valt. Wie wil weten *welke* eindige abelse uitbreiding bij een gegeven open verzameling van C_K hoort, heeft weinig aan haar definitie. CM-theorie van elliptische krommen geeft een heel elegante manier om alle eindige abelse uitbreidingen van K te beschrijven (met voortbrengers), voor een speciale klasse van getallenlichamen K: de imaginair kwadratische uitbreidingen van de rationale getallen $\mathbb{Q}$.

Het is belangrijk te vermelden dat de toepassing op ons motiverend probleem van priemgetallen van de vorm $p = x^2 + ny^2$ slechts een vage schaduw is van wat klassenlichamentheorie en CM-theorie in werkelijkheid verwezenlijkt hebben. De lezer met meer achtergrond kan te rade gaan bij [2] en [1]. Desondanks zien we zelfs in deze bescheiden context al een opmerkelijk defect in CM-theorie: Wat gebeurt er als $n < 0$? Bijvoorbeeld, wanneer is een priemgetal p van de vorm $p = x^2 - 205y^2$? De eerste

Complexe vermenigvuldiging

De stelling van Kronecker–Weber vertelt ons dat elke eindige abelse uitbreiding van $K = \mathbb{Q}$ bevat is in een *cyclotomisch* lichaam $\mathbb{Q}(\zeta_n)$, voor een zekere n, waarbij ζ_n een primitieve n-de eenheidswortel is. Deze eenheidswortels kan men zien als speciale waarden van de complex analytische functie

$$z \mapsto \exp(\pi i z)$$

bij rationale waarden van het argument z. Deze functie, of althans diens imaginaire deel, komt ons bekend voor uit de hoofdtekst, en geeft ons een heel expliciete beschrijving van de eindige abelse uitbreidingen van $\mathbb{Q}$.

Voor imaginair kwadratische getallenlichamen K geeft de theorie van complexe vermenigvuldiging ons een heel gelijkaardige beschrijving van de eindige abelse uitbreidingen van K, door middel van voortbrengers die speciale waarden van bijzondere complex analytische functies zijn. Het primaire voorbeeld is de j-functie van Klein, een holomorfe functie op het Poincaré-halfvlak

$$\mathfrak{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$$

die symmetrisch is voor de werking van de groep $\mathrm{SL}_2(\mathbb{Z})$ door Möbius-transformaties op het argument z. In het bijzonder is deze functie ook invariant onder $z \mapsto z + 1$, en ze heeft een Fourier-ontwikkeling van de vorm

$$j(q) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots, \quad q = e^{2\pi i z}.$$

De j-functie is een ongekende bron van rijkdommen, die haar belang in de klassenlichamentheorie ver overstijgt. Haar waarden voor imaginair kwadratische argumenten $z \in K$, de zogenaamde *singuliere moduli*, waren de genesis van het werk van Gross en Zagier over het vermoeden van Birch en Swinnerton-Dyer. Haar Fourier-coëfficiënten werden in verband gebracht met de Monster-groep in het werk van Borcherds. Daarnaast duikt ze op in een horde van verschillende contexten binnen de wiskunde en natuurkunde.

priemgetallen van deze vorm zijn

$$5, 59, 131, 139, 241, 269, 271, 359, 409, 541,$$
$$569, 599, 661, 701, 761, 859, 881, 911, 941, \ldots$$

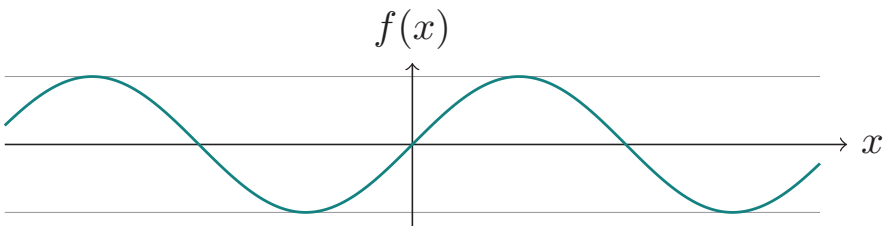
Klassenlichamentheorie voorspelt weliswaar het bestaan van een magische polynoom $f_n(x)$ zoals tevoren, maar CM-theorie, waarvan Kronecker vele grondslagen legde, laat ons in de steek om deze te construeren. Dit is wat het twaalfde probleem van Hilbert ons vraagt: een algemene versie van CM-theorie die alle klassenlichamen expliciet beschrijft, en niet enkel die van de rationale getallen $\mathbb{Q}$ en imaginair kwadratische lichamen $\mathbb{Q}(\sqrt{-n})$ voor $n > 0$. Een vrije vertaling van het origineel Franse citaat van Hilbert stelt:

> "De uitbreiding van de stelling van Kronecker naar het geval waarbij, in de plaats van rationale of imaginair kwadratische lichamen, een willekeurig algebraïsch lichaam genomen wordt als domein, schijnt mij van het grootste belang. Ik beschouw dit probleem als een van de diepste en meest verregaande in de theorie der getallen en functies. [...] Het is duidelijk dat in dit probleem de drie fundamentele gebieden der wiskunde, getaltheorie, algebra, en functietheorie, in de dichtste aanraking met elkaar komen, en ik ben ervan overtuigd dat in het bijzonder de theorie van functies in meerdere variabelen verrijkt zal worden indien men erin slaagt functies te vinden die de rol vervullen voor willekeurige getallenlichamen van de exponentiële en elliptische modulaire functies." David Hilbert

De aanpak van Kronecker, en de functies waarover Hilbert zo laaiend enthousiast klinkt, kunnen we zien als verfijningen van een oude bekende: de sinusfunctie $f : x \mapsto \sin(\pi z)$, zie Figuur 1. Van belang voor de theorie zijn de waarden van deze functie bij rationale argumenten, zoals

$$\begin{aligned}
\sin\left(\frac{\pi}{2}\right) &= 1, \\
\sin\left(\frac{\pi}{4}\right) &= \frac{\sqrt{2}}{2}, \\
\sin\left(\frac{\pi}{8}\right) &= \frac{\sqrt{2-\sqrt{2}}}{2}, \\
\sin\left(\frac{\pi}{16}\right) &= \frac{\sqrt{2-\sqrt{2+\sqrt{2}}}}{2}, \\
&\vdots
\end{aligned}$$

Alle waarden $f(x)$ bij rationale getallen zijn *algebraïsch*; ze voldoen aan een polynoom met gehele coëfficiënten. Kronecker (en Eisenstein, in onafhankelijk werk) ontdekte een analogon hiervan in twee dimensies, gebruikmakend van functies met translatiesymmetrie in twee verschillende richtingen, wiens waarden algebraïsche getallen opleveren die nulpunten zijn van de magische polynomen van voordien. Deze historische ontwikkelingen, wiens veralgemening het doel van Hilberts twaalfde probleem is, werden op meesterlijke wijze beschreven door Weil [7].



Figuur 1

Dirichlet en Stark

Een recente doorbraak in Hilberts twaalfde probleem kwam van Samit Dasgupta en Mahesh Kakde [4], die een analytische constructie bewezen voor voortbrengers van klassenlichamen van totaal reële getallenlichamen. Een speciaal geval is de systematische constructie voor de 'magische polynomen' $f_n(x)$ met $n < 0$. Dit werk bouwt verder op vele spectaculaire ontwikkelingen die het vooraf gaan, en die steunen op een rijke traditie die haar wortels heeft in het werk van Dirichlet en Stark.

Het beginpunt komt deze keer uit een verrassend andere richting. We merkten reeds op dat de tweede kolom van Tabel 1 ruwweg voor de helft gevuld leek. Het werk van Dirichlet (1805–1859) impliceert dat dit inderdaad het geval is. Zijn argument berust op technieken uit de *analyse*, en was het beginpunt van de bloeiende discipline van de *analytische getaltheorie*. Dirichlet gebruikt in zijn werk veralgemeningen van de vertrouwde Riemann-zèta-functie; van het meeste belang voor ons is het gedrag van de *Dedekind-zèta-functie* $\zeta_K(s)$ van een getallenlichaam K (i.e. een eindige lichaamsuitbreiding van $\mathbb{Q}$) in de limiet $s \to 1$. Dit is het zogenaamde *kritieke punt*, een concept dat we al eerder ontmoetten in de context van elliptische krommen en het vermoeden van Birch–Swinnerton-Dyer. Deze functie is gedefinieerd door

$$\zeta_K(s) := \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{Nm}(\mathfrak{p})^s}\right)^{-1}, \quad \mathrm{Re}(s) > 1,$$

waar het product loopt over alle niet-triviale priemidealen van de ring van gehelen van K. Wanneer $K = \mathbb{Q}$ is dit precies de Riemann-zèta-functie, bekend van een ander befaamd open probleem: de Riemann-hypothese. De *Dirichlet-klassengetalformule* stelt dat

$$\lim_{s \to 1} (s-1)\, \zeta_K(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot |\,\mathrm{Cl}_K\,| \cdot \mathrm{Reg}_K}{|\,O_{K,\mathrm{tors}}^{\times}\,| \cdot \sqrt{|\,\Delta_{K/\mathbb{Q}}\,|}}$$

waarin alle termen belangrijke aritmetische varianten zijn wiens definitie hier achterwege gelaten wordt. Voor ons is de term Reg_K van belang, de *regulator* van K, die een ingewikkelde uitdrukking is in een collectie *grondeenheden*, speciale elementen van het lichaam K die voldoen aan 'magische polynomen'.

Veel later kwam Stark (geb. 1939) tot het belangrijke inzicht dat het voor een klassenlichaam K mogelijk zou moeten zijn de Dirichlet-klassengetalformule te verfijnen, door de Galois-symmetrieën van K uit te buiten. Dit leidde tot de vermoedens van Stark [6], die in het bijzonder een analytische constructie impliceren van grondeenheden van K. De vermoedens van Stark zijn nog steeds open, maar in het begin van de 21ste eeuw kwam hier verandering in voor een p-*adische variant* van het vermoeden, door het werk van Darmon, Dasgupta en Pollack [3], dat op zijn beurt steunde op ideeën van Gross, Ribet, Mazur, Greenberg, Stevens, en vele anderen, in de context van het vermoeden van Birch–Swinnerton-Dyer en de laatste stelling van Fermat. Dit illustreert mooi hoe wiskundige ideeën vaak krachtige toepassingen vinden in een probleem dat volledig verschilt van hun oorspronkelijke doel. Sinds afgelopen jaar [4] bestaat er een systematische constructie van de ontbrekende 'magische polynomen', die bovendien ook praktisch berekenbaar is. We vinden bijvoorbeeld voor *oneven* priemgetallen dat

$$p = x^2 - 205y^2 \iff \begin{cases} 205 \text{ is een kwadraat modulo } p, \text{ en} \\ 16x^4 + 31x^3 + 31x^2 + 31x + 16 \equiv 0 \pmod{p} \\ \text{heeft een oplossing.} \end{cases}$$

Terugblik op Hilberts twaalfde probleem

De ontwikkelingen rond de p-adische variant van het vermoeden van Stark doen in zekere zin helemaal wat het twaalfde probleem van Hilbert vraagt. Is het probleem dan eindelijk opgelost, meer dan een eeuw nadat het in 1900 werd voorgedragen aan de wiskundige gemeenschap?

Het is duidelijk dat dit een van de grote wiskundige ontwikkelingen van ons tijdsgewricht vormt, maar langs de andere kant is het ook een begin van een lange en spannende weg die lonkt. Voorlopig is de toepasbaarheid van deze ideeën beperkt tot klassenlichamen van totaal reële $K/\mathbb{Q}$, zodat Hilbert zijn probleem nog niet helemaal zou kunnen opdoeken. Daarnaast moeten we ook opmerken dat sinds de tijd van Hilbert een enorme hoeveelheid belangrijke ontwikkelingen heeft plaatsgevonden, waaronder:

- In de 19de eeuw lag de nadruk op expliciete klassenlichamentheorie, de achterliggende wiskunde van het soort vraagstukken als priemgetallen van de vorm $p = x^2 + ny^2$. Deze theorie was destijds nog in volle ontwikkeling, en vormde toen een heel belangrijk onderzoeksgebied binnen de wiskunde.
- In de late 20ste eeuw vond een ware revolutie plaats door het werk van Gross en Zagier [5] die op spectaculaire wijze CM-theorie uitbreidden om een deel van het vermoeden van Birch en Swinnerton-Dyer te bewijzen. Er is sindsdien sprake van een heuse renaissance van CM-theorie.
- In de 21ste eeuw is het belang van CM-theorie nog sterk toegenomen, door toepassingen binnen de cryptografie, zoals in het relatief jonge vakgebied van de post-quantumcryptografie, wiens doel het is om elektronische betalingen, virtuele authenticatie, et cetera, veilig te maken tegen aanvallen met quantumcomputers.

Het belang van CM-theorie binnen en buiten de wiskunde groeit met de dag, in vakgebieden waarvoor ze oorspronkelijk niet ontworpen werd, en haar rol is nog lang niet uitgespeeld. De 20ste- en 21ste-eeuwse ontwikkelingen van CM-theorie komen voort uit miraculeuze eigenschappen van de *singuliere moduli* van Kronecker en Weber, geconstrueerd aan de hand van analytische functies die enorm verschillen van de L-functies in de aanpak van Stark. Het waren precies deze functies waarover Hilbert met zo veel enthousiasme schreef, maar daarvan ontbreekt helaas nog steeds elk spoor voor algemene getallenlichamen. Meer dan een eeuw na Hilbert moeten we dus misschien wel onze blik verruimen, en het twaalfde probleem ook in een context zien die al de spannende ontwikkelingen sinds de tijd van Hilbert weerspiegelt. De mijlpaal die met het werk van Dasgupta en Kakde bereikt werd, is dus tegelijk ook een beginpunt van een nieuw avontuur dat ons op ongekende nieuwe plaatsen zal brengen.

Oplossen, of niet oplossen?

De verleiding om bekende open problemen als opgelost te bestempelen is altijd groot, en geeft ons als gemeenschap een gevoel van vooruitgang en voldoening. Langs de andere kant mogen we niet overhaast zulke uitspraken doen, want een goed onopgelost probleem is een schatkist, die net door zijn gebrek aan oplossing grote bijdragen levert aan de wiskunde. In de nasleep van de oplossing van de laatste stelling van Fermat deed John Conway (1937–2020) de volgende uitspraak.

> "I'm relieved that this result is now settled. But I'm sad in some ways, because Fermat's Last Theorem has been responsible for so much. What will we find to take its place?" John H. Conway

Deze uitspraak kan ons tot nadenken stemmen. Hilbert formuleerde zijn twaalfde probleem op een meesterlijke manier. Hij wist als geen ander de diepte en kracht van de vraag te formuleren, op een manier die bovendien vaag genoeg blijft over hoe een 'oplossing' er precies moet uitzien. Misschien voorzag Hilbert welke ongekende rijkdom de theorie der complexe vermenigvuldiging nog zou blootgeven lang na zijn dood. Een aanpak als die van Stark geeft ons prachtige wiskunde, maar kan nooit deze volledige rijkdom evenaren. We staan duidelijk nog maar aan het begin van onze ontdekkingstocht. Om zulke ontwikkelingen mogelijk te blijven maken, is het misschien wel belangrijker om open problemen niet te kunnen oplossen, dan het is om ze wel op te lossen.

Dankwoord

Mijn bijzondere dank gaat uit naar Mike Daas voor een uitzonderlijk grondige proeflezing.

Referenties

1 J.W.S. Cassels en A. Fröhlich, *Algebraic Number Theory,* Academic Press, 1967.

2 D.A. Cox. *Primes of the Form $x^2 + ny^2$*, Wiley, 1989.

3 S. Dasgupta, H. Darmon en R. Pollack, Hilbert modular forms and the Gross–Stark conjecture, *Ann. of Math. (2)* 174(1) (2011), 439–484.

4 S. Dasgupta en M. Kakde, Brumer–Stark units and Hilbert's 12th problem, arXiv:2103.02516.

5 B.H. Gross en D.B. Zagier, On singular moduli, *J. Reine Angew. Math.* 355 (1985), 191–220.

6 H.M. Stark, L-functions at $s = 1$. IV. First derivatives at $s = 0$, *Adv. Math.* 35(3) (1976), 197–235.

7 A. Weil, *Elliptic Functions According to Eisenstein and Kronecker,* Springer, 1976.