René Schoof
Dipartimento di Matematica
Università di Roma "Tor Vergata"
schoof@mat.uniroma2.it

De oplossing

De vervloekte kromme

De wat oudere Ajax-fan kent de vervloekte kromme eigenlijk al jaren. Dat is de Feyenoord-speler Willem van Hanegem. Van Hanegem had de bijnaam 'de kromme', omdat hij de bal zo mooi in een curve kon schieten. Hij was een van de beste voetballers die Nederland ooit gekend heeft. Helaas voor Ajax speelde hij bij Feyenoord. Dit artikel gaat over een andere vervloekte kromme. Namelijk deze: $(-3y+1)x^3+2(y^2-y)x^2+(y^2+y-1)x-y^3+2y^2-y=0$. In dit artikel legt René Schoof eerst uit waarom deze kromme, net als Willem van Hanegem trouwens, een hele interessante kromme is. Dan legt hij uit waarom hij vervloekt werd en ten slotte waarom hij inmiddels vervloekte kromme af is.

Het uniformiteitsvermoeden van Serre

In de tweede helft van de twintigste eeuw zijn *elliptische krommen* een steeds grotere rol gaan spelen in getaltheoretisch onderzoek. Een hoogtepunt was het bewijs in 1995 van Andrew Wiles van één van de hoofdvermoedens in de theorie en de toepassing hiervan op de Laatste Stelling van Fermat. Er zijn nog steeds veel belangrijke open vragen. De bekendste is misschien wel het vermoeden van Birch en Swinnerton-Dyer. Het staat naast het Riemannvermoeden in de lijst van zeven 'million dollar problems' van het Clay Institute.

Het jaar 1972 was belangrijk voor de ontwikkeling van de theorie. In dat jaar publiceerde de Franse wiskundige Jean-Pierre Serre — Fields-medaille, ICM Amsterdam 1954 — een artikel dat grote invloed zou hebben [8]. Serre bewees in dit artikel een stelling over torsiepunten van elliptische krommen. Torsiepunten hebben eindige orde in de groep van punten op een elliptische kromme E. Ze spelen een belangrijke rol in de theorie. Dit geldt in het bijzonder voor de punten van priemorde l. Deze *l-torsiepunten* vormen een ondergroep $E[l]$, die isomorf is met $\mathbb{Z}/l\mathbb{Z}\times\mathbb{Z}/l\mathbb{Z}$.

Willem van Hanegem

Zelfs als de elliptische kromme een vergelijking heeft met coëfficiënten in $\mathbb{Q}$, zijn de l-torsiepunten in het algemeen *niet* rationaal. Ze worden gepermuteerd door de Galoisgroep. Deze werkt via de automorfismengroep $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$ op $E[l]$. Als het beeld van de Galoisgroep in $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$ triviaal is, dan betekent dat precies dat de punten in $E[l]$ rationale coördinaten hebben. Als het beeld klein is, dan zijn de coördinaten algebraïsche getallen van kleine graad. Voor een speciale klasse van elliptische krommen, de zogenaamde *CM-krommen*, is het beeld inderdaad klein. Dit wordt veroorzaakt door de extra symmetrieën die CM-krommen hebben. De Galoisgroep moet deze respecteren.

Maar in het algemeen is het beeld van de Galoisgroep in $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$ juist heel groot. De stelling van Serre maakt dit precies: voor een gegeven elliptische kromme die niet een CM-kromme is, het beeld van de Galoisgroep voor grote priemgetallen l, *gelijk* is aan $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$. De stelling van Serre bevestigt de filosofie die zegt dat als er geen evidente restricties op het beeld van de Galoisgroep zijn (zoals bij CM-elliptische krommen), het beeld meestal zo groot mogelijk is. Het beeld van de Galoisgroep in $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$ is voor heel veel elliptische krommen en priemen uitgerekend. Voor kleine priemen l gebeurt het regelmatig dat het strikt kleiner is dan $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$, maar voor grote l komt dat heel zelden voor. Serre stelde de vraag of er

een uniforme grens bestaat, zodat voor *alle* elliptische krommen en alle priemen groter dan die grens, het beeld van de Galoisgroep gelijk is aan $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$. Dit is het 'uniformiteitsvermoeden' van Serre.

Modulaire krommen

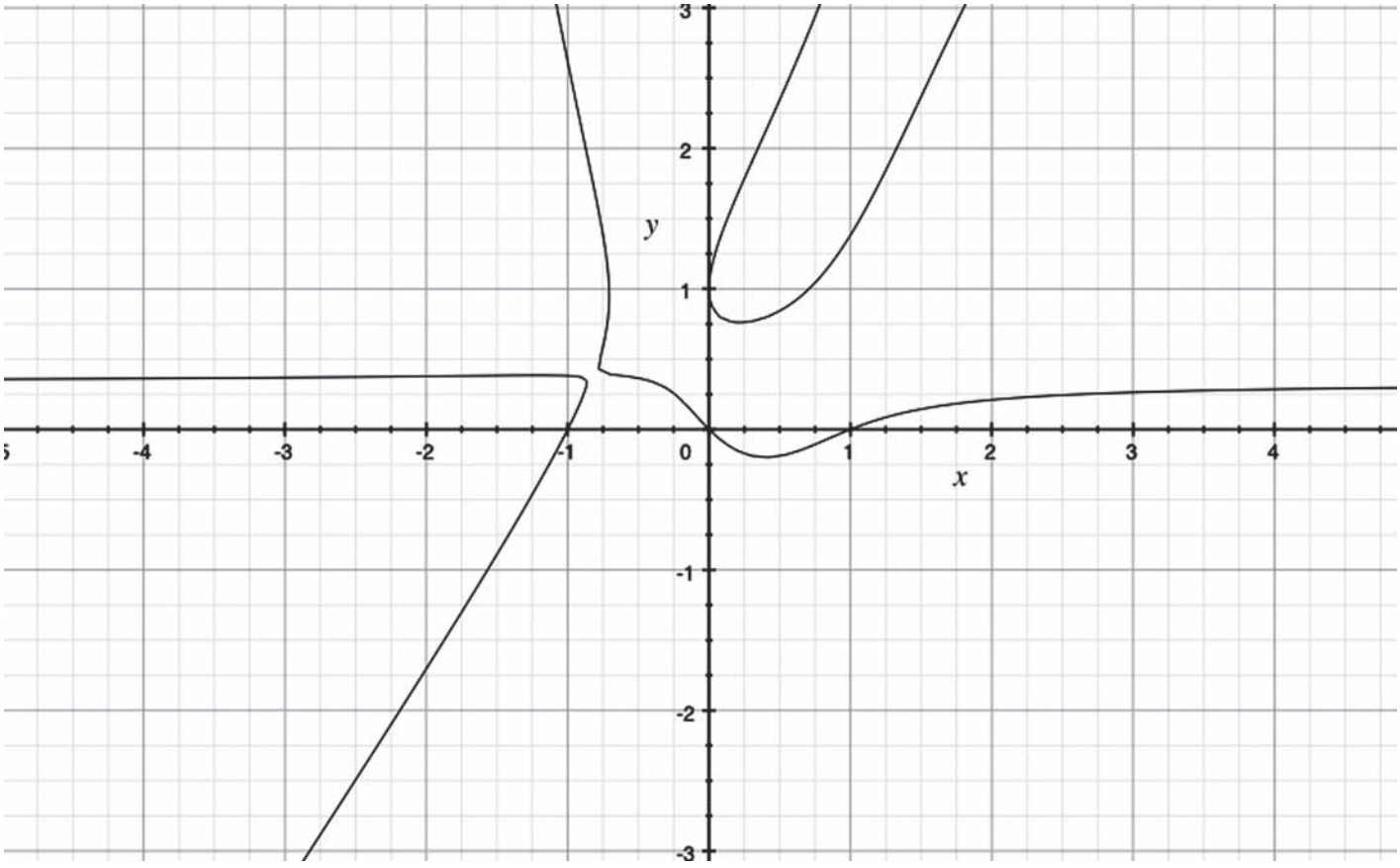
Modulaire krommen zijn 1-dimensionale parameterruimten. Ze parametriseren isomorfieklassen van elliptische krommen, eventueel met wat extra structuur die met torsiepunten te maken heeft. Het eenvoudigste voorbeeld is de j-lijn. Elke elliptische kromme E heeft een zogenaamde j-invariant. Dat is een complex getal, dat E karakteriseert als kromme over $\mathbb{C}$. Daarom parametriseert de j-lijn alle elliptische krommen over $\mathbb{C}$. Andere voorbeelden zijn de krommen $X(l)$. Deze parametriseren elliptische krommen samen met een basis voor de 2-dimensionale $\mathbb{Z}/l\mathbb{Z}$-vectorruimte $E[l]$ van l-torsie punten.

Elliptische krommen waarvoor de l-torsiepunten de eigenschap hebben dat het beeld van de Galoisgroep in $\mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$ klein is, geven aanleiding tot rationale punten op zekere modulaire krommen die gerelateerd zijn aan de krommen $X(l)$. De modulaire krommen die relevant zijn voor het uniformiteitsvermoeden van Serre hebben vergelijkingen met rationale coëfficiënten. Meestal hebben ze evidente rationale punten, zoals spitsen of CM-punten. De laatste worden ook wel *Heegnerpunten* genoemd en corresponderen met CM-elliptische krommen. Het uniformiteitsvermoeden van Serre laat zich nu vertalen in een diofantisch probleem. De vraag is namelijk of deze modulaire krommen ook *exotische* rationale punten hebben. De verwachting is, dat als er geen evidente redenen zijn voor het bestaan van extra rationale punten, dat ze ze dan, op eindig veel uitzonderingen na, ook niet hebben.

Het vermoeden van Serre valt op een natuurlijke manier uiteen in drie gevallen: drie families van modulaire krommen. Deze trichotomie vinden we al in het bewijs van de stelling van Serre uit 1972. Elke familie bestaat uit oneindig veel krommen: één kromme voor elk priemgetal l. De krommen worden steeds ingewikkelder naarmate l groter wordt. In het bijzonder groeit het geslacht met l.

De eerste familie bestaat uit de bekende modulaire krommen $X_0(l)$. De methoden ontwikkeld door Mazur in zijn studie van de krommen $X_0(l)$ in het 'Eisenstein ideal'-artikel [7] uit 1977 bleken in staat om ook het eerste geval van het uniformiteitsvermoeden van Serre te bewijzen. De methode van Mazur is een uiterst verfijnde versie van de klassiek descent-methode. Deze methode om diofantische vergelijkingen op te lossen gaat terug op Fermat. Mazur kreeg eerst de Coleprijs voor zijn artikel, en een paar decennia later ook de Steeleprijs.

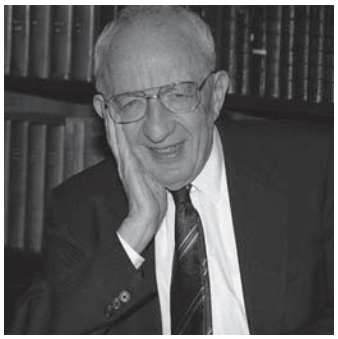
Aan de status van het probleem voor de andere twee families — split Cartan en nonsplit Cartan — veranderde in de jaren na 1977 niet veel. Pas in 2012 gebeurt er weer iets. Dan bewijzen Yuri Bilu en Pierre Parent [2], dat er ook in het split Cartan geval een uniforme grens is. Zij gebruikten een methode van Runge. Carl Runge was een toegepast wiskundige uit het begin van de vorige eeuw. In het enige artikel dat hij ooit over getaltheorie publiceerde, beschrijft hij een efficiënte methode om *gehele* oplossingen van vergelijkingen te vinden. Omdat Mazur, Momose, Bilu en Parent al hadden



Figuur 1 De vervloekte kromme $(-3y+1)x^3+2(y^2-y)x^2+(y^2+y-1)x-y^3+2y^2-y=0$.


Carl Runge


Claude Chabauty


Alan Baker


Barry Mazur

bewezen dat in het split Cartan-geval alle rationale oplossingen vanzelf geheel moesten zijn, konden Bilu en Parent de methode van Runge toepassen.

De vervloekte kromme

Na 2012 was er dus alleen nog het derde geval, de non-split Cartan-familie over. Dit leek tot voor kort hopeloos. Alle methoden die gebruikt waren in de andere twee gevallen, konden om hele fundamentele redenen niet werken in dit geval. Er is een natuurlijke manier om de rationale punten van een kromme C te zien als deelverzameling van de *groep* van punten van de Jacobi-variëteit van C. Als die groep klein is, dan zijn er methoden om de rationale punten op de kromme C te bepalen. In het derde geval van het uniformiteitsvermoeden van Serre, is die groep echter vreselijk groot.

De descent-methode van Mazur is daarom bijvoorbeeld onbruikbaar. Hetzelfde geldt voor de klassieke p-adische methode die Claude Chabauty [3], een van de vroege leden van de Bourbaki-groep, in de jaren veertig van de vorige eeuw ontwikkelde. In het derde geval is er ook geen a priori-reden om aan te nemen dat de rationale punten geheel zouden zijn. Daarom is de methode van Alan Baker (linear forms in logarithms) niet geschikt. Het is ook een van de redenen waarom de methode van Runge niet kan werken. En met deze vier methoden is het lijstje van beschikbare methoden wel zo'n beetje uitgeput...

Deze wanhopige situatie is perfect terrein voor de experimentele computationale getaltheoreticus. Als we het niet kunnen bewijzen, dan gaan we de kleinste niet-triviale gevallen doorrekenen. In het non-split Cartan-geval hebben we te maken met een oneindige familie diofantische vergelijkingen. Voor elk priemgetal l is er een kromme $X_{ns}(l)$ en de vraag is of er, afgezien van de voorspelbare CM-punten, nog andere, exotische, rationale punten zijn.

Voor de kleine priemen $l = 2,3,5,7,11$ is de situatie eenvoudig en helemaal onder controle. Er zijn dan oneindig veel rationale exotische punten. Voor $l \geq 13$, heeft elke kromme $X_{ns}(l)$ maar eindig veel rationale punten en het is niet onredelijk te vermoeden dat dit alleen maar CM-punten zijn.

Het eerste interessante geval is $X_{ns}(13)$. Dit is de kromme die David Zureick-Brown een paar jaar geleden de 'vervloekte kromme' is gaan noemen. Het is een vierdegraads kromme in het vlak. De vergelijking is in 2010 uitgerekend door Burcu Baran. De grafiek staat in Figuur 1. Er zijn vier evidente rationale punten: $(0,0)$, $(0,1)$, $(1,0)$ en $(-1,0)$. Er zijn ook nog drie rationale punten in oneindig. Deze worden zichtbaar als we de kromme in het projectieve vlak inbedden. Deze zeven punten zijn allemaal CM-punten. De vraag is of er ook nog exotische rationale punten zijn. In 2016 kon dit probleem met geen enkele bekende methode opgelost worden.

Niet-abelse Chabauty

In 1983 bewees Gerd Faltings het vermoeden van Mordell: een kromme van geslacht $g \geq 2$ heeft maar eindig veel rationale punten. Dit spectaculaire resultaat bezorgde Faltings in 1986 de Fieldsmedaille. Toch is het niet het laatste woord over deze materie. De stelling van Faltings is namelijk niet effectief. Dat wil zeggen dat, gegeven een expliciete kromme, zijn bewijs geen grens geeft op het aantal rationale punten of op de grootte van hun coördinaten.

De klassieke methode van Chabauty, die we al eerder noemden, is *wel* effectief. Maar helaas werkt deze niet altijd. Het idee is als volgt. We kiezen een priemgetal p en werken in de $\mathbb{Q}_p$-vectorruimte $J(\mathbb{Q}_p) \otimes \mathbb{Q}_p$. Hier is J de Jacobiaan van de kromme X en staat $\mathbb{Q}_p$ voor het lichaam van de p-adische getallen. We nemen aan dat X minstens één rationaal punt heeft en gebruiken dat om X via de Abel–Jacobi-afbeelding in J in te bedden. Dan krijgen we een commutatief diagram:

$$\begin{array}{ccc} X(\mathbb{Q}) & \hookrightarrow & J(\mathbb{Q}) \otimes \mathbb{Q}_p \\ \downarrow & & \downarrow \\ X(\mathbb{Q}_p) & \hookrightarrow & J(\mathbb{Q}_p) \otimes \mathbb{Q}_p \end{array}$$

De $\mathbb{Q}_p$-vectorruimte $J(\mathbb{Q}_p) \otimes \mathbb{Q}_p$ rechtsonder heeft dimensie g. Wegens de stelling van Mordell–Weil is $J(\mathbb{Q})$ een eindig voortgebrachte abelse groep van, zeg, rang r. De dimensie van $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ is dus op zijn hoogst r. Als het nu zo is dat $r < g$, dan is het beeld van $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ een *echte* deelruimte van $J(\mathbb{Q}_p) \otimes \mathbb{Q}_p$. Dat betekent dat er een niet triviale lineaire vorm f bestaat, die nul is op het beeld van $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ en dus ook op het beeld van de verzameling $X(\mathbb{Q})$ van rationale punten. Omdat de groep voortgebracht door de p-adische punten van $X(\mathbb{Q}_p)$ dicht ligt in de p-adische topologie van $J(\mathbb{Q}_p) \otimes \mathbb{Q}_p$, is f ook niet-triviaal op $X(\mathbb{Q}_p)$ en heeft maar eindig veel nulpunten in de 1-dimensionale verzameling $X(\mathbb{Q}_p)$. Als er nu een expliciete lineaire vorm f voorhanden is, dan kan men de nulpunten van f in $X(\mathbb{Q}_p)$ bepalen en checken of het punten in $X(\mathbb{Q})$ zijn.

De conditie $r < g$ is cruciaal. Echter, de krommen $X_{ns}(l)$ uit de derde familie van het uniformiteitsvermoeden van Serre, voldoen hier geen van alle aan. Dat geldt in het bijzonder voor de vervloekte kromme $X_{ns}(13)$. In dat geval is r gelijk aan g. Minhyong Kim, wiskundige in Oxford, liep al jaren rond met ideeën om de Chabauty-methode te modificeren, zodat deze ook zou kunnen werken als $r \geq g$. Zijn idee was om in een ruimte te werken die *groter* is dan

Minhyong Kim

$J(\mathbb{Q}_p) \otimes \mathbb{Q}_p$, zodat het beeld van $X(\mathbb{Q})$ toch weer in een *echte* deelruimte terechtkomt. Dit betekent dat de rationale punten van X dus weer in de eindige verzameling nulpunten van een p-adisch analytische functie op $X(\mathbb{Q}_p)$ bevat zijn. Omdat de Jacobiaan gerelateerd is aan het abelse stuk van de étale fundamentaalgroep, zocht en construeerde Kim zo'n ruimte in de fundamentaalgroep. Zie [4, 5, 6].

Na jaren werk is de methode van Kim nu eindelijk toegepast op een expliciete kromme, en wel op de vervloekte kromme $X_{ns}(13)$, waarvoor alle bekende methoden faalden. In een recente preprint [1] beschrijven Jennifer Balakrishnan, Netan Dogra, Steffen Müller, Jan Tuitman en Jan Vonk de berekeningen die ze met Kims methode gedaan hebben om de rationale punten op de modulaire kromme $X_{ns}(13)$ te bepalen. Het zijn inderdaad precies de zeven voorspelbare CM-punten.

Terwijl de klassieke methode van Chabauty gebruikmaakt van een *abelse quotiënt* van de fundamentaalgroep, werken Balakrishnan, Dogra, Müller, Tuitman en Vonk met het eenvoudigste niet-abelse unipotente quotiënt. Deze aanpak heet *quadratic Chabauty*. Het is belangrijk dat r precies gelijk is aan g, en dat de Jacobiaan van $X_{ns}(13)$ een grote endomorfismenring heeft. De auteurs kiezen $p = 17$. De berekeningen worden uitgevoerd in termen van de p-adische hoogtes van Jan Nekovář en met behulp van computerprogramma's om p-adische differentiaalvergelijkingen op te lossen. En het werkt! Dit is een spectaculaire stap in de theorie van de diofantische vergelijkingen.

Toevallig hebben alle auteurs van [1] wel iets met Nederland te maken. Jan Tuitman is zelfs een Nederlander. Hij werkt in Leuven. Jennifer Balakrishnan was een studente van Kiran Kedlaya, die een student van onze Johan de Jong was, toen die nog bij MIT werkte. Steffen Müller is UD in Groningen en Netan Dogra was een paar jaar geleden post-doc in Nijmegen. Jan Vonk ten slotte, is een Vlaamse zuiderbuur, die volgend jaar in Leiden komt werken.

Jennifer Balakrishnan

Netan Dogra

Steffen Müller

Jan Tuitman

Jan Vonk

Referenties

1 J. Balakrishnan, N. Dogra, S. Müller, J. Tuitman en J. Vonk, Explicit Chabauty–Kim for the Split Cartan Modular Curve of Level 13, arXiv:1711.05846 (2017).

2 Yu. Bilu en P. Parent, Serre's uniformity problem in the split Cartan case, *Ann. Math.* 173 (2011), 569–584.

3 C. Chabauty, Sur les points rationels des courbes algébriques de genre supérieur à l'unité, *C. R. Acad. Sci* 212 (1941), 882–884.

4 M. Kim, The motivic fundamental group of the projective line minus three points and the theorem of Siegel, *Invent. Math.* 161 (2005), 629–656.

5 M. Kim, The unipotent Albanese map and Selmer varieties for curves, *Publ. Res. Inst. Math. Sci.* 45 (2009), 89–133.

6 M. Kim, Galois Theory and Diophantine Geometry, in *Non-abelian Fundamental Groups and Iwasawa Theory*, J. Coates, M. Kim, F. Pop, M. Saïdi en P. Schneider (eds.), LMS Lecture Notes Series 393, Cambridge University Press, 2012, pp. 162–187.

7 B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. de l'IHÉS* 47 (1977), 33–186.

8 J.-P. Serre, Propriétées galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972), 259–331.