Gunther Cornelissen
Universiteit Utrecht
Mathematisch Instituut
Postbus 80.010
3508 TA Utrecht
cornelis@math.uu.nl

Diophantische vergelijkingen

Kunnen we het echt?

Hoe moeilijk is het oplossen van een polynoomvergelijking in breuken? Kan de computer een handje helpen? Is het probleem algoritmisch beslisbaar? Recente ontwikkelingen onthullen de theorie van diophantische vergelijkingen als een in zijn eigen staart bijtende slang: als we voldoende begrijpen over één dergelijk probleem, kunnen we aantonen dat het algemene probleem bijzonder complex is.

We zullen de term *diophantische vergelijking* gebruiken voor een polynoomvergelijking in meerdere veranderlijken, met rationale breuken als coëfficiënten. We zoeken naar oplossingen in gehele getallen, of in rationale breuken. Dit vraagstuk staat al heel lang in de wiskundige belangstelling, getuige bijvoorbeeld de naamgeving naar Diophantus van Alexandrië (derde eeuw n.Chr.) en zijn boek de *Arithmetica*, waarin een grote verzameling van dergelijke problemen wordt genoemd en met ad-hoc methoden opgelost.

De volgende 'meetkundige' terminologie is voor deze vraagstukken ondertussen standaard [1] : noem een stelsel polynoomvergelijkingen in meerdere veranderlijken met gehele coëfficiënten een *variëteit V*

$$V : \begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \cdots \\ f_m(x_1, \ldots, x_n) = 0. \end{cases}$$

We schrijven $\mathbf{Z}, \mathbf{Q}$ en $\mathbf{R}$ voor de verzameling van alle gehele, rationale en reële getallen, respectievelijk. Stel dat $R = \mathbf{Z}, \mathbf{Q}, \ldots$ en schrijf vervolgens $V(R)$ voor de verzameling oplossingen van het stelsel in R:

$$V(R) := \{(x_1, \ldots, x_n) \in R^n : \forall i : f_i(x_1, \ldots, x_n) = 0\}.$$

In plaats van oplossingen van het stelsel V praten we ook over *R-rationale punten van de variëteit V*. Dan wordt de centrale vraag: Wat zijn $V(\mathbf{Z})$ en $V(\mathbf{Q})$? Is er een algemene methode om dit soort problemen aan te pakken? David Hilbert formuleerde de vraag op het Internationale Wiskundecongres van 1900 in Parijs als volgt:

"Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist."

Hilbert zelf geloofde waarschijnlijk wel in het bestaan van zo'n 'Verfahren' (in onze interpretatie is dit een algoritme in de zin van Turing), getuige een radiotoespraak uit 1930 waarin hij fulmineerde tegen het relativisme van fysioloog DuBois-Reymond:

"Statt des törichten Ignorabimus heiße im Gegenteil unsere Losung: Wir müssen wissen, Wir werden wissen." [2]

In zijn algemeenheid overstijgt de vraag naar een mechanische oplossingsmethode voor zulke problemen de getaltheorie. Heel veel bekende wiskundige problemen zijn *expliciet* herschreven als de vraag of een diophantische vergelijking een oplossing heeft of niet, zo onder andere: de Riemannhypothese, het bepalen of een integraal over $(-\infty, +\infty)$ van een algebraïsche functie convergeert of niet, de laatste stelling van Fermat [3]... Meestal helpt dit niet om het oorspronkelijke probleem op te lossen, maar laat wel zien hoe universeel het oplossen van diophantische vergelijkingen is [4].

Hilbert stelt de vraag naar gehele oplossingen, maar het is net zo zinvol te vragen naar rationale oplossingen. Hoewel we voor gehele oplossingen sinds 1970 het antwoord op zijn vraag kennen (zie wat verder), weten we niet veel over de vraag in breuken. In dit stukje willen we wat recente ontwikkelingen over dit probleem behandelen op het grensgebied van logica, topologie en getaltheorie. Daarvoor zullen we elliptische krommen nodig hebben, en die zullen we invoeren aan de hand van een concreet getaltheoretisch probleem.

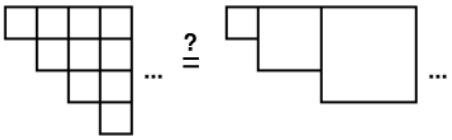
De Utrechtse elliptische kromme

De computer heeft de praktijk van het

oplossen van diophantische vergelijkingen dramatisch beïnvloed. Veel klassieke problemen kunnen bijna mechanisch worden aangepakt. Tijdens mijn college *Elliptische Krommen* in 2002 vroeg derdejaarsstudent Wouter Waalewijn het volgende: voor welke natuurlijke getallen x en y is de som van de eerste y getallen gelijk aan de som van de eerste x kwadraten:

$$1+2+\ldots+y = 1^2+2^2+\ldots+x^2\ ?$$

De lezer kan misschien proberen een paar waarden voor x en y te vinden zodat dit klopt. Zijn er eindig of oneindig veel oplossingen?

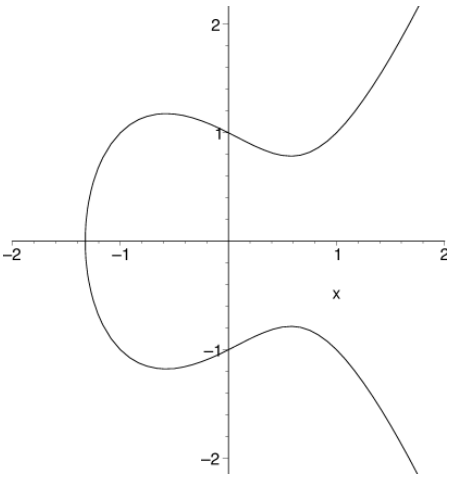


Het probleem van Wouter Waalewijn

Gesloten formules voor linker- en rechterlid van deze vergelijking herleiden het vraagstuk tot: bepaal de positieve gehele punten op de kromme E van graad drie gegeven door

$$E\ :\ \frac{y(y+1)}{2} = \frac{x(x+1)(2x+1)}{6}.$$

Dit is een zogenaamde elliptische kromme (in het algemeen van de vorm 'kwadratisch in y = kubisch in x' en glad). In zijn kleine scriptie loste derdejaarsstudent Marius de Leeuw dit probleem op aan de hand van elliptische logaritmen [5]. Het vreemde aan de methode is dat eerst alle oplossingen in breuken worden 'bepaald', en dan gekeken wordt welke daarvan geheel zijn. Kort door de bocht gegaan werkt dit als volgt. De rationale punten $E(\mathbf{Q})$ vormen een eindig voortgebrachte torsievrije abelse groep van rang twee (die twee is trouwens heel uitzonderlijk, er wordt verwacht dat een elliptische kromme over $\mathbf{Q}$ rang ≤ 1 heeft met waarschijnlijkheid één). Dit betekent dat er twee oplossingen P en Q zijn zodat elke oplossing te schrijven is als $aP+bQ$ met a,b gehele getallen, waarbij de 'som' $+$ gedefinieerd is door het feit dat drie collineaire punten op E bij definitie som 0 hebben.



De elliptische kromme $y^2 = x^3 - x + 1$

Als vrije voortbrengers van die groep kunnen we volgende twee punten kiezen: $P = (1,1)$ en $Q = (-9/8, -1/16)$. Dit kan door de zogenaamde methode van 2-descent met het computerprogramma *MWrank* van John Cremona onvoorwaardelijk worden bewezen binnen luttele seconden. Een resultaat uit de diophantische approximatie van Sinou David, aan de praktijk aangepast door Stroeker en Tzanakis, levert een methode voor het bepalen van alle combinaties $aP+bQ$ die geheel zijn.

In het voorbeeld vindt men dat alle gehele punten $|a|, |b| < 2,1 \cdot 10^{38}$ hebben — maar niet alle dergelijke combinaties zijn geheel, Q zelf bijvoorbeeld niet. De methode levert in elk geval eindig veel mogelijke punten, maar wel met meer cijfers dan er atomen zijn in het melkwegstelsel. Gelukkig kan de bovengrens op $|a|$ en $|b|$ met het roosterreductiealgoritme van Lenstra-Lenstra-Lovász (bijvoorbeeld in *Mathematica*) worden gereduceerd tot 7, en aldus vindt men alle oplossingen voor het probleem:

$$(x,y) \in \{(1,1),(5,10),(6,13),(85,645)\}.$$

Op een voorlichtingsdag in Utrecht vond het publiek, bestaande uit 6-vwo leerlingen en hun ouders, de eerste drie oplossingen, dacht eerst dat er oneindig veel zouden zijn ("omdat er zoveel kleine oplossingen zijn"), en dan dat die drie de enige waren ("omdat we er niet meteen nog meer vinden").

Een ander meer klassiek voorbeeld: de computer bewijst ook bijna ogenblikkelijk dat $W(\mathbf{Q}) = \{(12, \pm 36)\}$ voor de elliptische kromme $W\ :\ y^2 = x^3 - 432$. Dit onschuldige probleem is via een eenvoudige variabelensubstitutie equivalent met de bewering dat $U(\mathbf{Q}) = \{(1,0),(0,1)\}$ voor $U\ :\ x^3+y^3 = 1$; het Fermatprobleem voor exponent drie, dat voor het eerst door Euler werd opgelost! Ook het Fermatprobleem voor exponent vier '$x^4 + y^4 = 1$' en zeven '$x^7 + y^7 = 1$' kunnen worden herleid tot het bepalen van rationale punten op elliptische krommen ($y^2 = x^3 - x$ en $y^2 = 4x^3 + 21x^2 + 28x$, respectievelijk) [6].

Kleuren en projecteren

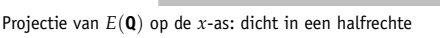
Bekijken we nu kort de vraag of er een relatie is tussen $V(\mathbf{Q})$ en $V(\mathbf{R})$. We kunnen $V(\mathbf{R})$ in de n-dimensionale ruimte $\mathbf{R}^n$ tekenen en daarop $V(\mathbf{Q})$ inkleuren. Op een kegelsnede (graad 2 vergelijking in 2 veranderlijken) liggen ófwel géén rationale punten, ófwel liggen de rationale punten willekeurig dicht bij de reële punten; de $\mathbf{R}$-topologische afsluiting van $V(\mathbf{Q})$ is dus de hele $V(\mathbf{R})$. Op een elliptische kromme (graad 3 in twee veranderlijken) gebeurt dat soms, en soms ook niet: op W liggen maar eindig veel rationale punten, terwijl de rationale punten op E dicht liggen in de reële punten.

Barry Mazur stelde in 1990 het volgende vermoeden op dat beide gevallen dekt [7].

Vermoeden van Mazur. De topologische afsluiting van $V(\mathbf{Q})$ in $V(\mathbf{R})$ heeft maar eindig veel samenhangingscomponenten.

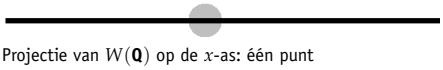
Dit lijkt een heel elementaire uitspraak over de ligging van rationale punten in variëteiten. Maar niemand weet of dit vermoeden klopt. Het kan worden bewezen voor een handjevol speciale V's (van lage dimensie of bepaalde soorten vezelingen). Om er iets zinvols over te kunnen zeggen gaan we de tekeningen nu nog wat vereenvoudigen en komen zo vanzelf op een begrip uit de logica.

We zullen eerst $V(\mathbf{R})$ en de ingekleurde $V(\mathbf{Q})$ vanuit de n-dimensionale ruimte $\mathbf{R}^n$ op een coördinaatas projecteren: een soort cartografische aanpak van het diophantische probleem. Voor de elliptische kromme E krijgen we schematisch:



Projectie van $E(\mathbf{Q})$ op de x-as: dicht in een halfrechte

en voor de kromme W:



Projectie van $W(\mathbf{Q})$ op de x-as: één punt

Dit soort plaatjes worden nu de centrale objecten in onze studie.

Definitie. Het beeld van $V(\mathbf{Q})$, respectievelijk $V(\mathbf{Z})$ onder een projectie op een coördinaatas heet een **Q**-, respectievelijk **Z**-*diophantische verzameling*.

We kunnen ook meer algemeen een projectie op een coördinaat(hyper)vlak toelaten en noemen dit dan nog steeds een diophantische verzameling. Een diophantische verzameling D is dus een verzameling van gehele (of rationale) $\mathbf{x}$ waarvoor gehele (of rationale) $(x_2, \ldots, x_n)$ *bestaan* die aan een stel vergelijkingen voldoen:

$$\mathbf{x} \in D \iff (\exists x_2, \ldots, x_n)$$
$$(f_1(\mathbf{x}, x_2, \ldots, x_n) = 0 \wedge \ldots$$
$$\ldots \wedge f_m(\mathbf{x}, x_2, \ldots, x_n) = 0).$$

Zonder het te merken zijn we een stukje dichter bij een logica-probleem gekomen: terwijl de oorspronkelijke variëteit door een stelsel polynoomvergelijkingen is gedefinieerd, is een diophantische verzameling, als projectie, gedefinieerd als de verzameling punten $\mathbf{x}$ waarvoor een formule *met existentiële kwantoren* waar is.

De DMPR-stelling

Voor we iets zeggen over **Q**-diophantische verzamelingen, bekijken we eerst verzamelingen $V(\mathbf{Z})$ en hun projecties. Zijn **Z**-diophantische verzamelingen misschien *zelf de verzameling gehele oplossingen van een niet-nulpolynoom in één veranderlijke*? Dat zou wel heel makkelijk zijn, want polynomen in één veranderlijke kunnen we makkelijk in gehele getallen oplossen. Maar neen, voor $V : y - x = 0$ is de projectie van $V(\mathbf{Z})$ op de x-as de *oneindige* aftelbare verzameling **Z**, maar een niet-nul polynoom heeft maar eindig veel nulpunten (en dit is géén pathologisch voorbeeld).

Als **Z**-diophantische verzamelingen zelf niet van de vorm $W(\mathbf{Z})$ zijn voor een zekere variëteit W, wat zijn ze dan wel? Hoe 'complex' kunnen ze zijn? Kunnen we ze berekenen? Hiervoor maken we volgende definitie:

Definitie. Een verzameling $V \subseteq \mathbf{Z}$ is *recursief opsombaar* als er een computerprogramma bestaat dat de elementen van V opsomt.

In deze wat vage definitie betekent 'computerprogramma' eigenlijk een Turingmachine. Men stelt zich een gewone computer voor zonder beperkingen op het geheugen en de precisie van de hardware, met daarop een C++-programma, waarvan de snelheid irrelevant is.

Bewering. *Diophantische verzamelingen zijn recursief opsombaar.*

Voor het bewijs, doorloop alle mogelijke $x_1, \ldots, x_n$ in één of andere volgorde en kijk of ze een oplossing zijn. Zo ja, output x_1. Recursief opsombare verzamelingen kunnen heel ingewikkeld zijn; omdat de lezer die het tot dit punt heeft gehaald moe is geworden nu het net spannend wordt, is het de hoogste tijd voor een opgave.

Opgave. Laat zien dat de verzameling priemgetallen recursief opsombaar is, en laat zien dat de verzameling gehele niet-priemgetallen diophantisch is [8].

Het opmerkelijke feit is dat de omkering van bovenstaande bewering ook waar is; dit is de zogenaamde stelling van Davis, Matijasevich, Putnam en Robinson (bewezen tussen 1950 en 1970) [9].

DMPR-stelling. *Recursief opsombare verzamelingen zijn diophantisch (en omgekeerd).*

Uit de DMPR-stelling volgt op niet-triviale wijze een onbeslisbaarheidsresultaat: er bestaat géén computerprogramma dat van een willekeurige diophantische vergelijking kan bepalen of er een gehele oplossing is of niet — en dat is dan weer het beroemde negatieve antwoord op de vraag van Hilbert.

Over het bewijs van de DMPR-stelling kunnen we alleen zeggen dat een centrale plaats wordt ingenomen door de studie van de oplossingen van één specifiek soort diophantische vergelijking (namelijk een Pell-vergelijking). Van Martin Davis zelf komt in een wat andere context de uitdrukking dat er "One Equation to Rule Them All" lijkt te bestaan.

De DMPR-stelling heeft trouwens allerlei onfrisse bijwerkingen: zo volgt eruit dat men een spel met twee spelers kan bedenken, zodat één van de spelers bij elke beginzet van de andere speler een winnende strategie heeft, maar die nooit door een algoritme zal kunnen bepalen. Maar aan de positieve kant betekent het bijvoorbeeld ook dat er een polynoom is dat de verzameling der priemgetallen oplevert (zie de opgave hierboven).

Q-diophantische verzamelingen en Mazur

De lezer denkt nu misschien dat **Q**-diophantische verzamelingen op een soortgelijke manier te beschrijven zijn. Maar de waarheid tot op heden is weerom: niemand weet het! Het feit dat het vinden van **Q**-oplossingen hetzelfde is als het vinden van **Z**-oplossingen van homogene vergelijkingen lijkt niet te helpen.

Er is wel een verband met het vermoeden van Mazur: dat heeft tot gevolg dat de verzameling **Z** géén **Q**-diophantische verzameling is. Als namelijk **Z** de projectie is van $V(\mathbf{Q})$, dan heeft de afsluiting van $V(\mathbf{Q})$ oneindig veel componenten omdat **Z** discreet is in **Q**. Dit is in contrast met de volgende opgave.

Opgave. Gebruik de DMPR-stelling om aan te tonen: als de verzameling **Z** der gehele getallen **Q**-diophantisch is, dan is er geen algoritme dat beslist of een diophantische vergelijking *rationale* oplossingen heeft of niet [10].

We weten echter niet of er een computerprogramma bestaat dat beslist of een diophantische vergelijking een rationale oplossing heeft of niet ... Moeten we dus het vermoeden van Mazur geloven of niet?

Intermezzo: Orakels

We kunnen niet beslissen of een diophantische vergelijking een oplossing heeft in gehele getallen of niet, laat staan die oplossingen mechanisch vinden. Maar hoeveel moeilijker is het écht vinden van oplossingen vergeleken met het beslissen of er een oplossing bestaat of niet?

Bekijk voor een ring R volgende problemen voor een willekeurige variëteit V:
- Ex(R): is $V(R)$ leeg of niet?
- Fin(R): is $V(R)$ eindig of niet?
- Sol(R): als $V(R)$ eindig is, bepaal de verzameling $V(R)$.

De DMPR-stelling zegt dat Ex(**Z**) onbeslisbaar is. Maar men kan ook vragen wat de relatie tussen de onbeslisbaarheid van deze problemen is. Davis, Matijasevich en Robinson vermoeden dat, zelfs als er een orakel is dat Ex(**Z**) kan beslissen, het probleem Fin(**Z**) nog steeds onbeslisbaar is.

Stel dat V een kromme is, gegeven door één polynoomvergelijking in twee veranderlijken $f(x, y) = 0$. Als V geen kegelsnede is en geen elliptische kromme, dan volgt uit een stelling van Faltings (ook wel bekend als het Vermoeden van Mordell) dat $V(\mathbf{Q})$ eindig is. Minhyong Kim [11]

bewees in 2003 dat voor dit soort krommen het Sol($\mathbf{Q}$)-probleem oplosbaar is als Ex($\mathbf{Q}$) oplosbaar is (bijvoorbeeld door een orakel). Anders gezegd: als er een methode bestaat die van een willekeurige dergelijke kromme kan beslissen of er een rationaal punt op ligt of niet, dan kunnen van een willkeurige dergelijke kromme alle oplossingen ook écht gevonden worden.

Als de eerste methode een orakel vereist, dan ook de tweede. Merk wel op dat om alle oplossingen van een gegeven kromme te vinden er van eindig veel *andere* krommen moet worden beslist of ze een rationaal punt hebben of niet. Het is dus niet voldoende om van een specifieke V te kunnen beslissen of $V(\mathbf{Q})$ leeg is of niet om $V(\mathbf{Q})$ te kunnen berekenen.

Diophantische en andere modellen

Het meest recente werk aan $\mathbf{Q}$-diophantische verzamelingen maakt gebruik van het concept 'diophantisch model van $\mathbf{Z}$'. Dit is een aftelbare diophantische verzameling D in $\mathbf{Q}^N$ met een bijectie $\iota : \mathbf{Z} \to D$ zodat de grafen van de bewerkingen $+$ en $\times$ in $\mathbf{Z}^{3N}$ door ι naar diophantische verzamelingen in $\mathbf{Q}^{3N}$ worden gestuurd.

Het idee is dat zo'n diophantisch model een manier oplevert om, in het bijzonder onbeslisbare, uitspraken over $\mathbf{Z}$ te vertalen naar, in het bijzonder onbeslisbare, uitspraken over $\mathbf{Q}$. Als zo'n diophantisch model bestaat, dan is het antwoord op Hilbert's probleem in breuken nog steeds negatief: zie de vorige opgave. Het vermoeden van Mazur is ook nog steeds fout [12].

Een eventueel dergelijk geconstrueerd 'logisch' tegenvoorbeeld voor het vermoeden van Mazur zou geen bijzondere meetkundige structuur hebben en dus precies aan de andere kant van het spectum variëteiten liggen dan de meetkundig bijzondere exemplaren waarvoor het antwoord op het vermoeden positief is.

Goed, we weten niet of $\mathbf{Z}$ een diophantisch model heeft in $\mathbf{Q}$, dus gaan we dit probleem op twee manieren afzwakken: door de ring $\mathbf{Q}$ te vervangen door een kleinere ring R, en door de definitie van 'diophantisch model' af te zwakken. In elk van de gevallen worden de beste resultaten bekomen door het inzetten van al onze kennis over: elliptische krommen!

Voor $R \subseteq \mathbf{Q}$ een deelring van $\mathbf{Q}$ kan de lezer nu vast zelf bedenken wat 'een diophantisch model van $\mathbf{Z}$ in R' betekent. Alle ringen R tussen $\mathbf{Z}$ en $\mathbf{Q}$ zijn van

bron: logic.pdmi.ras.ru

Julia Robinson rond 1985

de vorm $\mathbf{Z}[S^{-1}]$, dat wil zeggen, bestaan uit breuken waarvan de noemers alleen deelbaar zijn door priemen in een gegeven verzameling $S \subseteq \mathbf{Z}$. Voor $S = \{\text{alle priemgetallen}\}$ is $\mathbf{Z}[S^{-1}] = \mathbf{Q}$. Bjorn Poonen gebruikte in 2003 elliptische krommen om aan te tonen dat $\mathbf{Z}$ een diophantisch model heeft in $\mathbf{Z}[S^{-1}]$ voor een 'grote' verzameling priemgetallen (namelijk, van dichtheid 1) [13].

We kunnen ook vragen of $\mathbf{Z}$ überhaupt te definiëren is door een formule in de *eerste orde taal* van de ring $\mathbf{Q}$. Het antwoord is gelukkig ja, en werd gegeven door Julia Robinson in 1949 [14].

Dit resultaat ziet er als volgt uit: een rationaal getal $x \in \mathbf{Q}$ is een geheel getal precies dan als

$$\begin{aligned}&(\forall x_1, x_2, x_3, x_4, x_5)(\exists y_1, y_2, y_3, y_4)\\ &(\forall z_1, z_2, z_3)(\exists u)\\ &(P(x, x_1, x_2, x_3, x_4, x_5, y_1, y_2,\\ &\qquad y_3, y_4, z_1, z_2, z_3, u) = 0)\end{aligned}$$

met P een expliciet polynoom dat de lezer bespaard zij. In het algemeen heet een verzameling $D \subseteq \mathbf{Q}^N$ *definiëerbaar* als $x \in D$ equivalent is met een formule van deze vorm (met eventueel meer kwantoren en veranderlijken).

Een definiëerbare verzameling kan best ingewikkeld te begrijpen zijn als er heel veel kwantorenwisselingen in staan. Een formule met alleen $\exists$-kwantoren zegt iets over het bestaan van oplossingen van een diophantische vergelijking. Een formule met $\forall$ gevolgd door $\exists$ zegt iets over het bestaan van oplossingen in een familie van diophantische vergelijkingen. Hartley Rogers Jr. schrijft: "The human mind seems limited in its ability to understand and visualize beyond four or five alternations of quantifier." [15]

Nu is $\mathbf{Z}$ een $\mathbf{Q}$-diophantische verzameling precies als er een soortgelijke formule bestaat zonder $\forall$-kwantoren. Men kan zich afvragen of we een formule kunnen bedenken met alvast minder $\forall$-kwantoren, of met minder kwantorenwisselingen (hier zijn er drie). Hiertoe nog een veralgemenisering van de notie 'diophantisch model': de verzameling $D \subseteq \mathbf{Q}^N$ is een *model* van $\mathbf{Z}$ over $\mathbf{Q}$ als D een definiëerbare verzameling is in $\mathbf{Q}^N$ en er een bijectie $\iota : \mathbf{Z} \to D$ bestaat die de grafen van $+$ en $\times$ in definiëerbare verzamelingen omzet. In recent werk van de auteur met Karim Zahidi [16] wordt aangetoond dat er een model is van $\mathbf{Z}$ over $\mathbf{Q}$ dat gedefinieerd kan worden door een formule met maar één $\forall$-kwantor en twee kwantorenwisselingen, tenminste als (bijvoorbeeld) volgend vermoeden over elliptische krommen waar is.

Vermoeden. Bekijk op de elliptische kromme

$$y^2 = x^3 + 12x^2 + 11x$$

de veelvouden nP van het punt $P = (1/4, 15/8)$ in de groep $E(\mathbf{Q})$ en schrijf

$$nP = ((A_n/B_n)^2, A_nC_n/B_n^3)$$

met A_n, B_n, C_n onderling ondeelbare gehele getallen; dan heeft voor elke $n \in \mathbf{Z}_{>0}$ het getal C_n een priemdeler $p = \pm 2 \bmod 5$, zodat p geen deler is van C_n/p en van C_i voor alle $i < n$.

Hieruit zou dan volgen dat er een onbeslisbare zin is in de eerste-orde theorie van $\mathbf{Q}$ met maar één $\forall$-kwantor, dat wil zeggen één kwantor weg van een negatief antwoord op Hilbert's probleem in breuken.

Men kan het vermoeden 'heuristisch bewijzen'. De redenering lijkt op de heuristiek voor het aantal Mersenne-priemgetallen van Wagstaff: men berekent de waarschijnlijkheid dat een random getal dat even groot is als het primitieve deel van C_n (dat men kan afschatten via diophantische approximatie) enkel delers $p = \pm 1 \bmod 5$ heeft. Men kan het vermoeden ook 'in dichtheid bewijzen': we hebben bijvoorbeeld voor een andere elliptische kromme laten zien dat voor tenminste 95.5% van alle priemgetallen n, een soortgelijk vermoeden waar is voor B_n.

Conclusie

Het valt op dat de meeste hedendaagse ontwikkelingen vlijtig gebruik maken van moderne arithmetische meetkunde (vooral elliptische krommen). In zekere zin is de getaltheorie dus een slang die in zijn eigen staart bijt: als we maar genoeg weten over de oplossingen van één diophantische vergelijking (de Pell-vergelijking voor $\mathbf{Z}$, en misschien elliptische krommen voor $\mathbf{Q}$), kunnen we aantonen dat we in het algemeen géén algoritme hebben om diophantische problemen op te lossen.

Noten en referenties

1 De kenners vergeven bij deze de auteur dit misbruik van terminologie.

2 Hier staat wel degelijk "Losung" en niet "Lösung"; de lezer die het verschil niet kent wordt aangeraden meteen naar het woordenboek te grijpen. De radiotoespraak met vertaling en geluidsfragment (met Hilbert's hoge stem en Oostpruisisch accent) is te vinden via math.sfsu.edu/smith.

3 Let op: de laatste stelling van Fermat zegt niet dat één diophantische vergelijking enkel triviale oplossingen heeft, maar oneindig veel, namelijk $x^n + y^n = z^n$ voor alle $n > 2$. De bewering is dat dit equivalent is het bestaan van een oplossing van één andere diophantische vergelijking.

4 Als een probleem eenmaal geformaliseerd is als uitspraak P, wordt de vraag of P dan wel $\neg P$ bewijsbaar is equivalent met de vraag of het Gödelgetal van P of $\neg P$ behoort tot de recursief opsombare verzameling van bewijsbare formules; via de DMPR-stelling (zie later) wordt dit equivalent met het beslissen of een diophantische vergelijking een oplossing heeft. Natuurlijk willen we niet alleen weten of P of $\neg P$ *bewijsbaar* zijn, maar of ze *waar* zijn ...

5 M. de Leeuw, *Gehele punten op elliptische krommen*, kleine scriptie, Utrecht (2003), www. phys. uu.nl /~leeuw. Vergelijk: R.J. Stroeker en N. Tzanakis, 'Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms', *Acta Arith.* LXVII.2 (1994), 177–196.

6 Exponent vier is klassiek, voor exponent zeven, zie: Noam D. Elkies, 'The Klein quartic in number theory', in: The eightfold way, p. 51–101, *Math. Sci. Res. Inst. Publ.* vol. 35, CUP (1999) www.msri.org/publications. De rationale punten van de (projectieve) kromme $x^7 + y^7 = z^7$ worden nl. afgebeeld op rationale punten van de Kleinse kwartiek $x^3y + y^3z + z^3x$, die op hun beurt afgebeeld worden op de punten van de vermelde elliptische kromme.

7 B. Mazur, The Topology of Rational Points, *Experiment. Math.* **1** (1992), no. 1, 35–45. www.expmath.org

8 Priemgetallen zijn recursief opsombaar als volgt: doorloop de natuurlijke getallen in stijgende volgorde en kijk met het euclidisch algoritme of het getal n deelbaar is door $1 < d < n$ of niet. Zoniet, ouput n. De verzameling niet-priemgetallen is de projectie op de x-as van de oplossingen van

$$\begin{aligned} y &= (A^2 + B^2 + C^2 + D^2), \\ z &= (E^2 + F^2 + G^2 + H^2), \\ [x - (y+2)(z+2)]&\cdot \\ \cdot\, [x + (y+2)(z+2)] &= 0 \end{aligned}$$

in de $(x, y, z, A, \ldots, H)$-ruimte. Volgens Lagrange is namelijk een geheel getal groter of gelijk aan nul, precies als het de som van vier kwadraten is, en x is niet-priem precies als het plus/min het product is van twee positieve getallen ≥ 2.

9 zie Y. Matiyasevich, *Hilbert's Tenth Problem*, MIT Press (1993) voor een volledig bewijs van de DMPR-stelling en meer informatie.

10 Stel dat $\mathbf{Z} = \pi(V(\mathbf{Q}))$ voor een variëteit V en een projectie π. Voor willekeurige W in N veranderlijken is dan

$$x \in W(\mathbf{Z}) \iff x \in W(\mathbf{Q}) \cap \pi(V(\mathbf{Q}))^N.$$

Zo'n algoritme kan van de rechterkant van deze equivalentie beslissen of zo'n x bestaat, dus ook van de linkerkant. Maar dat kan niet volgens de DMPR-stelling.

11 M. Kim, 'Relating Decision and Search Algorithms for Rational Points on Curves of Higher Genus', *Arch. Math. Logic* **42** (2003), no. 6, 563–568.

12 Het bewijs is niet meer zo elementair en gebruikt de DMPR-stelling, zie: Cornelissen-Zahidi, 'Topology of Diophantine sets: remarks on Mazur's conjectures', in: Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic geometry (Ghent, 1999), p. 253–260, *Contemp. Math.* vol. 270, AMS (2000).

13 B. Poonen, 'Hilbert's Tenth Problem and Mazur's Conjecture for Large Subrings of $\mathbf{Q}$',*J. Amer. Math. Soc.* **16** (2003), no. 4, 981–990.

14 Julia Robinson, 'Definability and Decision Problems in Arithmetic', *J. Symb. Logic* **14**, 98–114 (1949).

15 *Theory of Recursive Functions and Effective Computability*, McGraw-Hill (1967), p. 322.

16 G. Cornelissen en K. Zahidi, 'Complexity of undecidable formulae in the rationals and inertial, Zsigmondy theorems for elliptic curves', *preprint math.NT*/0412473 (2004).