Het vinden van oplossingen van een polynoomvergelijking in gehele getallen of breuken is één van de oudste wiskundige kaskrakers. Kan meetkunde hierbij helpen? Kunnen computers ons een handje toesteken? Wat weten we eigenlijk überhaupt over het probleem in zijn algemeenheid? **Gunther Cornelissen** hield hierover een voordracht op de Nationale Wiskunde Dagen 2004.

Diophantische vergelijkingen vanuit de verte bekeken

Om de lezer actief bij de tekst te betrekken, komen veelvuldig opgaven voor waarop meestal meteen een oplossing volgt. Voor huiswerkopgaven moet je even gaan zitten. Na het artikel volgen drie werkbladen op VWO-niveau. Referenties staan op de webpagina's van de *Nieuwe Wiskrant*, evenals printklare versies van de werkbladen. Veel plezier!


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS.
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& observationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inventorum nonnullorum collectio
ex variis auctoribus D. de FERMAT Epistolis.
TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Jesu.
M. DC. LXX.

fig. 1 Titelpagina van een Latijnse uitgave van de Arithmetica met opmerkingen van Fermat

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. Hij leefde in de derde eeuw na Christus en schreef onder andere een lijvig boekwerk, de *Arithmetica*, waarin een grote verzameling dergelijke problemen wordt genoemd en opgelost. Over Diophantus zelf weten we bijna niks, alleen stond in een Griekse *Anthologie* van Metrodorus uit de zesde eeuw volgend epitaaf:

> Zijn jeugd maakte een zesde van zijn leven uit; na een verder twaalfde kreeg hij een baard; na een verder zevende trouwde hij, en zijn zoon werd vijf jaar daarna geboren; de zoon werd maar half zo oud als zijn vader, en de vader overleed vier jaar na de zoon.

Opgave 1. Hoe oud was Diophantus?

Dit vraagstuk geeft meteen aanleiding tot een diophantische vergelijking: als x de leeftijd van Diophantus is, dan moet dus:

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x$$

en dus $x = 84$.

Maar dit voorbeeld is een beetje flauw: het is een polynoom in één veranderlijke van graad één. Laat ons liever naar een typische voorbeeld kijken: graad twee in twee veranderlijken (het is trouwens in de buurt van dit voorbeeld in zijn kopie van de *Arithmetica* dat Pierre de Fermat in de zeventiende eeuw zijn beroemde 'grote stelling' poneerde).

Als lemma bij Vraagstuk VI.12 staat een bewering die in moderne taal equivalent is met

> **Bewering**. Als A en C rationale breuken zijn zodat $A + C$ een kwadraat is (van een rationale breuk), dan heeft $Ax^2 + C = y^2$ oneindig veel rationale oplossingen in (x, y).

Dus heeft bijvoorbeeld $x^2 + 3 = y^2$ oneindig veel oplossingen. Met rationale oplossing bedoelen we een oplossing in breuken. We schrijven $\boldsymbol{Q}$ voor de verzameling van alle rationale getallen (en $\boldsymbol{Z}$, $\boldsymbol{R}$ en $\boldsymbol{C}$ voor respectievelijk de gehele, reële en complexe getallen).

Opgave 2. Geef tenminste één oplossing van de vergelijking in de bewering.

Je kunt bijvoorbeeld aan $(1, \sqrt{A+C})$ denken; herinner je dat $A + C$ een kwadraat is, dus $\sqrt{A+C} \in \boldsymbol{Q}$.

De meetkunde van Vraagstuk I.12

Geheel tegen de traditie van Diophantus in zullen we dit vraagstuk op een meetkundige manier behandelen. De reële grafiek van $Ax^2 + C = y^2$ in het (x, y)-vlak is een kegelsnede K (als $A < 0$ een ellips). Een rationale oplossing (x_o, y_o) van de vergelijking noemen we een rationaal punt van K. De stelling is nu:

Stelling. Stel dat een lijn L_t met rationale richtingscoëfficiënt $t \in \mathbf{Q}$ de kegelsnede K in twee punten P en Q snijdt. Als P rationaal is, dan ook Q.

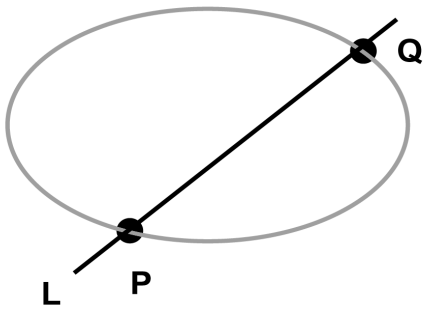

fig. 2 Een kegelsnede en een rechte lijn

Opgave 3. Hieruit volgt meteen dat de bewering van Diophantus waar is. Waarom?

Kies $P = (1, \sqrt{A+C})$. Er zijn oneindig veel rationale richtingscoëfficiënten, en voor elke keuze ontstaat er een nieuw rationaal punt Q.
Ik wil twee manieren laten zien om deze stelling te bewijzen: de eerste is door rekenen (en dus wat meer knoeien), maar wel constructief, dat wil zeggen alle oplossingen worden ook daadwerkelijk gevonden. De tweede manier is een elegant bewijs zonder rekenen.

Eerste Bewijs
Kies $P = (1, \alpha)$ met $\alpha = \sqrt{A+C}$. Vindt de snijpunten van K en L_t, dat wil zeggen, los op:

$$\begin{cases} y = \alpha + t(x-1) \\ Ax^2 + C = y^2 \end{cases}$$

Vul de uitdrukking voor y uit de eerste vergelijking in de tweede vergelijking in, dan voldoet x aan:

$$(A - t^2)x^2 + (2t^2 - 2\alpha t)x - A - t^2 + 2\alpha t = 0$$

en die vergelijking heeft (via de abc-formule) als oplossingen:

$$1, -\frac{t^2 - 2\alpha t + A}{A - t^2}$$

Bijgevolg zijn alle rationale oplossingen gegeven door

$$\left(-\frac{t^2 - 2\alpha t + A}{A - t^2}, \frac{\alpha A + \alpha t^2 - 2tA}{A - t^2}\right) : t \in \boldsymbol{Q},\ t^2 \neq A$$

Opgave 4. Waarom geeft dit *alle* oplossingen?

Als $Q \neq P$ een andere oplossing is, dan heeft de lijn door P en Q een rationale richtingscoëfficiënt. Het punt P zelf krijg je voor $t = A/\alpha$. Het weglaten van t met $t^2 = A$ heeft ook geen invloed, want als $t^2 = A$ dan heeft het snijpunt van L_t met K als x-coordinaat $x = 1$, punt dat we al hadden.

Huiswerkopgave 5. Pas deze techniek nu toe om zelf alle oplossingen in breuken te vinden van $x^2 + 3 = y^2$.

Huiswerkopgave 6. Met behulp van de relatie $x^2 + 3 = y^2$ kun je de onbepaalde integraal

$\int \frac{dx}{\sqrt{x^2+3}}$ schrijven als $\int \frac{dx}{y}$;

we doen even of het teken formeel niet uitmaakt. Doe hierin de substitutie $x = x(t)$, $y = y(t)$, waarbij $(x(t), y(t))$ de algemene vorm is van de oplossing van opgave 5. Kun je nu de integraal uitrekenen?

Het integrandum wordt een rationale functie (dat wil zeggen: quotiënt van twee polynomen) in t, namelijk $\frac{2}{1-t^2}$. Dat is meteen te integreren door splitsen in partieelbreuken, tot $\log(\frac{t+1}{t-1})$; nu nog t als functie van x uitrekenen en invullen.

Tweede Bewijs
Stel dat L_t de rechte lijn door P is met richtingscoëfficiënt t. We vinden de x-coördinaten van de snijpunten van L_t met K door invullen van de vergelijking van L_t (in de vorm $y =$ iets als functie van x) in de vergelijking van K. Dit geeft ons een kwadratische vergelijking $Q(x) = 0$ in x, waarvan we weten dat tenminste één oplossing rationaal is, en waarvan bovendien de coëfficiënten rationaal zijn. Omdat het product van de twee wortels van Q het quotiënt is van de constante door de leidende coëfficiënt van Q, is dus ook de tweede oplossing rationaal. Vervolgens is ook de bijbehorende y rationaal door invullen in de vergelijking van L_t.

Opgave 7. Je bent vast de draad kwijt in dit bewijs. Schrijf het daarom netjes uit.

Stel $P = (x_0, y_0)$. De lijn L_t heeft als vergelijking $y = y_0 + t(x - x_0)$. Invullen in $Ax^2 + C = y^2$ geeft een vergelijking

$$\alpha x^2 + bx + c = \alpha(x - x_0)(x - x_1)$$

met $\alpha, b, c, \in \boldsymbol{Q}$ en x_1 de gezochte x-coördinaat van het tweede snijpunt van K met L_t. Uitwerken van het product geeft $x_0 \cdot x_1 = c/a \in \boldsymbol{Q}$. Met $x_0 \in \boldsymbol{Q}$ is dus $x_1 \in \boldsymbol{Q}$ en dan ook $y_1 = y_0 + t(x_1 - x_0) \in \boldsymbol{Q}$.

Merk op dat dit bewijs nergens de specifieke vorm gebruikt van de vergelijking van K. De stelling is dus waar voor een willekeurige kegelsnede. En in huiswerkopgave 6 vind je dan ook een algemene methode om $\int \frac{dx}{y}$ te berekenen, als tussen x en y een kwadratische relatie bestaat.

Huiswerkopgave 8. Kun je bewijzen dat willekeurig dicht bij een reële oplossing van $x^2 + 3 = y^2$ ook een rationale oplossing ligt?

We zien de reële oplossingen als $(x(t), y(t))$ voor $t \in \boldsymbol{R}$, en de rationale oplossingen als $(x(t_0), y(t_0))$ voor $t_0 \in \boldsymbol{Q}$. Dan is de bewering: voor elke $t \in \boldsymbol{R}$ en $\varepsilon > 0$ bestaat er een $t_0 \in \boldsymbol{R}$ zodat $|x(t) - x(t_0)| < \varepsilon$ (omdat de punten namelijk ook op L_t liggen, volgt daaruit onmiddellijk dat $|y(t) - y(t_0)| < \varepsilon|t - t_0|$).

Stel $t_0 = t + \varepsilon$ en vul de parametrisatie in, dan reken je zo

na dat $|x(t)-x(t_0)| = \varepsilon \cdot f(\varepsilon,t)$ met $\lim_{\varepsilon \to 0} f(\varepsilon, t) = 4\frac{t-t^2-1}{t^2-1^2} < \infty$ voor $t \neq \pm 1$. Nu is er voor elke reële t een rationale t_0 zodat $|t-t_0|$ willekeurig klein wordt.

Tekenen en projecteren

Omdat de 'meetkundige' aanpak zo succesvol blijkt, formuleren we het algemene vraagstuk naar het oplossen van polynoomvergelijkingen als volgt: noem een stelsel polynoomvergelijkingen (in meerdere veranderlijken) met gehele coëfficiënten een variëteit V:

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

Stel dat $\boldsymbol{R} = \boldsymbol{Z}, \boldsymbol{Q}, \ldots$ en schrijf vervolgens $V(\boldsymbol{R})$ voor de verzameling oplossingen van het stelsel in $\boldsymbol{R}$:

$V(\boldsymbol{R}) := \{(x_1, \ldots, x_n) \in \boldsymbol{R}^n : V(x_1, \ldots, x_n) = 0\}$

van het stelsel V in R, bijvoorbeeld:

- $V(\boldsymbol{Z})$ zijn de gehele oplossingen;
- $V(\boldsymbol{Q})$ zijn de rationale oplossingen;
- $V(\boldsymbol{R})$ zijn de reële oplossingen;
- $V(\boldsymbol{C})$ zijn de complexe oplossingen.

Dan wordt de centrale vraag: wat zijn $V(\boldsymbol{Z})$ en $V(\boldsymbol{Q})$? Hier is het geval van Vraagstuk I.12 (graad twee in twee veranderlijken) niet typisch. Daar hadden we namelijk een algo-ritme om alle oplossingen te bepalen (uitgaande van één oplossing). Zoiets is in het algemeen onbekend. Maar we kunnen wel vragen naar de aard van het beestje. Wat we daar precies mee bedoelen, zal later duidelijk worden. In elk geval kunnen we alvast vragen of er een relatie is tussen $V(\boldsymbol{Q})$ en $V(\boldsymbol{R})$ of $V(\boldsymbol{C})$. Een hele tak van de getaltheorie houdt zich bezig met die laatste vraag. Het blijkt namelijk dat de meetkunde van V en de structuur van $V(\boldsymbol{Q})$ heel veel met elkaar te maken hebben. Voorbeeld: als V een kromme is (dus ééndimensionaal), heeft V een zogenaamd geslacht g. Dat is een geheel getal, berekenbaar in termen van de meetkunde van $V(\boldsymbol{C})$. Gerd Faltings bewees in 1983 de beroemde stelling dat als $g \geq 2$, de verzameling $V(\boldsymbol{Q})$ eindig is. Maar wij willen de kwestie nóg algemener, zonder dimensiebeperkingen, begrijpen.

Eerst maken we een bescheiden tekening: we kunnen $V(\boldsymbol{R})$ in de n-dimensionale ruimte $\boldsymbol{R}^n$ tekenen en daarop $V(\boldsymbol{Q})$ grijs inkleuren. Hier zijn twee voorbeelden: voor $V_1 : y^2 - x^3 + x = 0$ zijn er maar drie losse grijze punten:

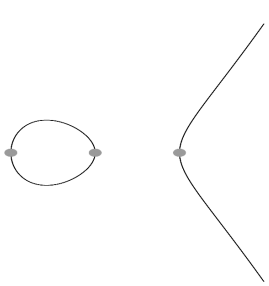

fig. 3 Eindig veel (grijze) rationale punten op V_1

Maar voor de vergelijking $V_2 : y^2 - x^3 + 2x = 0$ die er wel erg op lijkt, zijn er oneindig veel (hier is gewoon de hele grafiek grijs, want de rationale punten liggen weer willekeurig dicht bij de reële, zoals in huiswerkopgave 8):

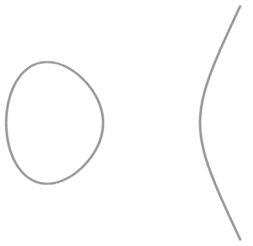

fig. 4 Oneindig veel rationale punten op V_2

Zo is bijvoorbeeld $(-\frac{1803649}{2325625}, \frac{3693595151}{3546578125}) \in V_2(\boldsymbol{Q})$.

Het bewijs dat dit de goede plaatjes zijn, is trouwens helemaal niet triviaal. Zo is het bewijs dat $V(\boldsymbol{Q}) = \{(12, \pm 36)\}$ voor $V : y^2 = x^3 - 432$ equivalent met de bewering dat $W(\boldsymbol{Q}) = \{(1, 0), (0, 1)\}$ voor $W : x^3 + y^3 = 1$. Maar dat is het Fermatprobleem voor exponent drie, dat voor het eerst door Euler werd opgelost! Ondertussen kan een computer voor dit soort beweringen automatisch een bewijs geven.
Dankzij huiswerkopgave 8 hierboven weet je nu hoe je zo een plaatje moet tekenen voor een kegelsnede met een rationaal punt: de rationale punten liggen willekeurig dicht bij de reële punten. We komen hier nog op terug.
Omdat we dergelijke plaatjes niet goed kunnen maken in hogere dimensies (als $n \geq 4$), zullen we $V(\boldsymbol{R})$ (en de grijze $V(\boldsymbol{Q})$) vanuit de n-dimensionale ruimte $\boldsymbol{R}^n$ op een coördinaatas projecteren: een soort cartografische aanpak van het diophantische probleem. Voor V_1 krijgen we:

fig. 5 Projectie van $V_1(Q)$ op de x-as: drie punten

en voor V_2:

fig. 6 Projectie van $V_2(Q)$ op de x-as: dicht in twee intervallen

Dit soort plaatjes worden nu de centrale objecten in onze studie. Om deze verzamelingen te kunnen bestuderen maken we meteen de volgende definitie:

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

Losjes gezegd is een diophantische verzameling dus een verzameling van gehele (of rationale) x waarvoor gehele (of rationale) $(x_2, \ldots, x_n)$ bestaan met

$f_1(x, x_2 \ldots, x_n) = \ldots = f_m(x, \ldots, x_n) = 0$.

We hopen nu $V(\boldsymbol{Z})$ en $V(\boldsymbol{Q})$ beter te begrijpen aan de hand van hun projecties.

Wat zijn *Z*-diophantische verzamelingen?

Zijn *Z*-diophantische verzamelingen misschien zelf de verzameling gehele oplossingen van een (niet-nul) polynoom (in één veranderlijke)? Dat zou wel heel makkelijk zijn, want polynomen in *n* veranderlijke kunnen we makkelijk in gehele getallen oplossen.

> Opgave 9. Geef zelf een negatief antwoord op deze vraag.

Voor $V: y - x = 0$ is de projectie van $V(\boldsymbol{Z})$ op de x-as de oneindige aftelbare verzameling $\boldsymbol{Z}$, maar een niet-nul polynoom heeft maar eindig veel nulpunten.

Hier is een leuker tegenvoorbeeld, dat alles te maken heeft met het beroemde tapijt van Bayeux. In 'Carmen de Hastigae Proelio' van Guy, bisschop van Amiens, lezen we over de slag van Hastings op 14 oktober 1066:

fig. 7 Harold op zijn troon (op het tapijt van Bayeux)

> Harolds mannen stonden als gewoonlijk dicht samengedromd in 13 vierkanten van gelijke grootte, en wee de Noorman die het waagde in zulk een falanx te willen indringen. Maar toen Harold zelf op het slagveld verscheen, vormden de Saksen één gigantisch vierkant met hun koning aan de top en stormden voorwaarts onder de strijdkreten 'Ut!', 'Olicrosse!' en 'Godemite!'.

De 'Saksen' zijn hier trouwens de 'Angelsaksen' die in de vijfde eeuw vanuit Duitsland naar Engeland migreerden.

> Opgave 10. Als x het aantal manschappen op een rij in het grote vierkant, en y dat in het kleine vierkant is, wat is dan de relatie tussen x en y?

Dan moet $x^2 - 13y^2 = 1$. Dit is een zogenaamde 'Pellvergelijking'.

> Opgave 11. Bewijs dat alle $(x, y) \in \boldsymbol{Z}$ bepaald door
> $x + y\sqrt{13} = (649 + 180\sqrt{13})^n$
> voor zekere n in $\boldsymbol{Z}_{>0}$ een oplossing van het probleem geven.

Voor $\varepsilon = 649 + 180\sqrt{13}$ en $\overline{\varepsilon} = 649 - 180\sqrt{13}$ is $\varepsilon \cdot \overline{\varepsilon} = 1$ zoals men meteen narekent. Dan is natuurlijk ook $\varepsilon^n \cdot \overline{\varepsilon}^n = 1$.
Er zijn dus oneindig veel mogelijke x, dus de projectie op de x-as van de oplossingen van dit probleem zijn niet de verzameling nulpunten van een niet-nul polynoom. De kleinste oplossing ($n = 1$) geeft trouwens een leger van 421200 man. Dat lijkt niet bijzonder realistisch. Harold, koning van Engeland, verloor overigens de slag tegen Willem van Normandië …

Als *Z*-diophantische verzamelingen zelf niet van de vorm $W(\boldsymbol{Z})$ zijn voor zekere W, wat zijn ze dan wel? Hoe 'complex' kunnen ze zijn? Kunnen we ze berekenen? We stellen in elk geval vast dat ze recursief opsombaar zijn:

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

In deze wat vage definitie betekent 'computerprogramma' eigenlijk een programma op 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. Voor het bewijs dat diophantische verzamelingen recursief opsombaar zijn, 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:

> Opgave 12. Laat zien dat de verzameling priemgetallen recursief opsombaar is; laat zien dat de verzameling gehele niet-priemgetallen diophantisch is (hint: een resultaat van Lagrange zegt dat elke positief geheel getal de som van vier kwadraten is).

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. Zo niet, output n.
De verzameling niet-priemgetallen is de projectie op de x-as van de oplossingen van
$y = (A^2 + B^2 + C^2 + D^2)$, $z = (E^2 + F^2 + G^2 + H^2)$,
$[x - (y + 2)(z + 2)][x + (y + 2)(z + 2)] = 0$
in de $(x, y, z, A, \ldots H)$-ruimte. Volgens Lagrange is namelijk een geheel getal positief 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.
Het opmerkelijke feit is dat de omkering van bovenstaande bewering ook waar is: de stelling van Davis, Matijasevich, Putnam en Robinson (bewezen tussen 1950 en 1970):

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

Hieruit volgt dan (op niet-triviale wijze) dat er géén computerprogramma bestaat dat van een willekeurige diophantische vergelijking kan bepalen of er een gehele oplossing is of niet. Dit levert dan weer een negatief antwoord op het tiende probleem dat Hilbert op het Internationale Wiskundecongres in 1900 formuleerde.
Maar aan de positieve kant betekent het bijvoorbeeld ook dat er een polynoom is dat de verzameling $\wp$ der priem-

getallen oplevert (zie opgave 12). En inderdaad is $\wp$ de projectie op de X-as van de gehele oplossingen in $X, A, B, C, D, a, \ldots$ z van volgende vergelijkingen:

$$
\begin{aligned}
&X = A^2 + B^2 + C^2 + D^2 = \\
&(k+2)(1-(wz+h+j-q)^2 \\
&-((gk+2g+k+1)(h+j) \\
&+h-z)^2 - (2n+p+q+z-e)^2 \\
&-(16(k+1)^3(k+2) \\
&(n+1)^2 + 1 - f^2)^2 - (e^3(e+2)(a+1)^2 + 1 \\
&-o^2)^2 - ((a^2-1)y^2 + 1 - x^2)^2 - (16r^2y^4 \\
&(a^2-1) + 1 - u^2)^2 - (((a+u^2(u^2-a))^2 - 1) \\
&(n+4dy)^2 + 1 - (x+cu)^2)^2 - (n+l+v-y)^2 - \\
&((a^2-1)l^2 + 1 - m^2)^2 - (ai+k+1-l-i)^2 - \\
&(p+l(a-n-1) \\
&+b(2an+2a-n^2-2n-2)-m)^2 - \\
&(q+y(a-p-1) \\
&+s(2ap+2a-p^2-2p-2)-x)^2 \\
&-(z+pl(a-p)+t(2ap-p^2-1)-pm)^2)
\end{aligned}
$$

Wat zijn *Q*-diophantische verzamelingen?

fig. 8 Barry Mazur

Je denkt nu misschien dat de corresponderende vraag voor Q-diophantische verzamelingen makkelijk te beantwoorden is. Maar de waarheid tot op heden is: niemand weet het! Barry Mazur stelde in 1990 daarom voor verzamelingen van het type $V(\boldsymbol{Q})$ vanuit de verte te bekijken. Volgens huiswerkopgave 8 ligt op een kegelsnede met een rationaal punt (bijvoorbeeld $x^2 + 3 = y^2$) willekeurig dicht bij een reële oplossing ook een rationale oplossing. Dat wil zeggen dat als je van ver naar $V(\boldsymbol{Q})$ kijkt, je geen verschil ziet met $V(\boldsymbol{R})$. Voor $y^2 - x^3 + x$ is dat niet het geval: er zijn precies drie punten in $V(\boldsymbol{Q})$, en dat ziet er vanuit de verte uit als de lichten van een auto die 's avonds een fietser (met werkend achterlicht) inhaalt. Mazur stelt het volgende vermoeden op dat beide gevallen dekt:

> **Vermoeden van Mazur.** Vanuit de verte gezien heeft $V(\boldsymbol{Q})$ maar eindig veel componenten.

Of, voor wie topologie kent, wat precieser: het vermoeden zegt dat de topologische afsluiting van $V(\boldsymbol{Q})$ in $V(\boldsymbol{R})$ maar eindig veel samenhangingscomponenten heeft.
Je ziet dat het klopt in onze voorbeelden: er is één component voor $x^2 + 3 = y^2$, er zijn er twee voor $y^2 = x^3 - 2x$ en drie voor $y^2 = x^3 - x$.
Dit vermoeden van Mazur heeft ondermeer tot gevolg dat de verzameling $\boldsymbol{Z}$ géén Q-diophantische verzameling is. Anderzijds:

Opgave 13. Gebruik de DMPR-stelling om aan te tonen: als de verzameling $\boldsymbol{Z}$ der gehele getallen Q-diophantisch is, dan is er geen computerprogramma dat beslist of een diophantische vergelijking rationale oplossingen heeft of niet.

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

Als je dus zo een computerprogramma hebt, kan dat van de rechterkant van deze equivalentie beslissen of zo een x bestaat, dus ook van de linkerkant. Maar dat kan niet volgens de DMPR-stelling. 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? In dit vrij nieuwe gebied van de wiskunde, dat getaltheorie, topologie en wiskundige logica vermengt, is nog flink wat werk aan de winkel!

Gunther Cornelissen
Mathematisch Instituut, Universiteit Utrecht

Werkblad: Een probleem van Diophantus

Diophantus van Alexandrië leefde in de derde eeuw en is vooral bekend om zijn boek *Arithmetica*, waarin hij probeert oplossingen te vinden voor allerlei vergelijkingen. Hij zoekt in het bijzonder naar oplossingen in gehele getallen en/of breuken. Kijk op:
www-history.mcs.st-and.ac.uk/history/Mathematicians/Diophantus.html voor meer historische informatie. Bij Vraagstuk I.12 staat in de *Arithmetica* een bewering die we wat precieser willen bekijken. Het is de volgende:

> Als A en C gehele getallen zijn, zodat $A + C$ een kwadraat is (van een geheel getal), dan heeft $Ax^2 + C = y^2$ oneindig veel oplossingen in breuken x en y

Opdracht 1.
Schrijf hieronder drie voorbeelden van gehele getallen *A* en *C* zodat *A* + *C* het kwadraat is van een derde geheel getal.

	A	*C*	$\sqrt{A+C}$
1.			
2.			
3.			

Opdracht 2.
Schrijf hieronder voor die drie waarden van A en C uit opdracht 1 één oplossing in breuken *x, y* van de vergelijking.$Ax^2 + C = y^2$

	x	*y*
1.		
2.		
3.		

In de vergelijking $Ax^2 + C = y^2$ van Diophantus zijn x, y veranderlijken, en A en C constanten. Je hebt zonet drie voorbeelden van zulke constanten A en C gegeven. Diophantus heeft in zijn bewering een *aanname* staan over deze constanten: hij neemt aan dat $A + C = \alpha^2$ met A, C, α gehele getallen.

Opdracht 3.
Kun je één oplossing (*x, y)* geven van $Ax^2 + C = y^2$ in gehele getallen (voor algemene *A*, *C* met *A* + *C* = α^2 met *A*, *C*, α gehele getallen)?

We gaan nu verder met een voorbeeld: $A = -1$, $C = 5$. Dan is $A + C = 4 = 2^2$.

Opdracht 4.
Teken de oplossingen van $-x^2 + 5 = y^2$ in het (*x, y*)-vlak (misschien met de grafische rekenmachine).
Je ziet (hopelijk) een ellips. Op deze ellips ligt het punt $P = (1, 2)$.

Opdracht 5.
Schrijf de vergelijking op in het (*x, y*)-vlak van een rechte lijn L_t door $P = (1, 2)$ met richtingscoëfficiënt *t.*

Opdracht 6.
Bereken de snijpunten van L_t met de ellips $-x^2 + 5 = y^2$. Je vindt uiteraard het punt *P* terug, maar er is nog een punt (dat afhangt van *t)*.

Opdracht 7.
Kun je nu de bewering van Diophantus voor $-x^2 + 5 = y^2$ bewijzen? Het belangrijke punt aan zijn bewering is dat er oneindig veel oplossingen zijn in *breuken*.

We keren terug naar het algemene geval, $Ax^2 + C = y^2$, met $A + C = \alpha^2$ met A, C, α gehele getallen.

Opdracht 8.
Schrijf de vergelijking op in het (*x*,*y*)-vlak van een rechte lijn door *P* = (1,α) met richtingscoëfficiënt *t*. Bereken de snijpunten van L_t met $Ax^2 + C = y^2$. Kun je de bewering van Diophantus nu in het algemeen bewijzen?

Je hebt op dit werkblad een algebraprobleem (bewijzen dat een vergelijking oneindig veel oplossingen heeft) door een meetkundige methode opgelost (het berekenen van het snijpunt van een 'kegelsnede' en een rechte lijn).

Extra opdracht I.
Kun je bewijzen dat je door deze methode ook *alle* oplossingen van de vergelijking in breuken vindt?

Extra opdracht II.
Bekijk een vergelijking van graad twee
$ax^2 + bxy + cy^2 + dx + ey + f = 0$
in veranderlijken *x* en *y* met gehele coëfficiënten *a,....,f.*
Toon aan dat, als de vergelijking één oplossing heeft in breuken, er oneindig veel oplossingen zijn.

Werkblad: de slag bij Hastings

Misschien heb je wel gehoord van het tapijt van Bayeux. in het Franse stadje Bayeux hangt een linnen doek ('tapijt') van ongeveer zeventig meter lengte en vijftig centimeter hoogte, waarop als bij een stripverhaal 58 taferelen zijn geborduurd. Deze taferelen geven onder meer de slag bij Hastings in 1066 weer. In totaal heeft men op het tapijt onder andere 626 personen, 202 paarden, 41 schepen en 37 gebouwen geteld. Lees meer over het tapijt op:
http://home.hccnet.nl/aw.slager/html/bayeux.nl
Op een latere datum is ook een boekje geschreven over die slag bij Hastings van 14 oktober 1066, de '*Carmen de Hastigae Proelio*' door Guy, bisschop van Amiens. Op dit werkblad zullen we met wiskunde één van de beweringen in dit boekje in twijfel trekken. Lees mee:

Harold op zijn troon (op het tapijt van Bayeux)

> Harolds mannen stonden als gewoonlijk dicht samengedromd in 13 vierkanten van gelijke grootte, en wee de Noorman die het waagde in zulk een falanx te willen indringen. Maar toen Harold zelf op het slagveld verscheen, vormden de Saksen één gigantisch vierkant met hun koning aan de top en stormden voorwaarts onder de strijdkreten 'Ut!', 'Olicrosse!' en 'Godemite!'.

De 'Saksen' (dat wil zeggen 'Harold's mannen) zijn hier trouwens de 'Angelsaksen' die in de vijfde eeuw vanuit Duitsland naar Engeland migreerden.

Opdracht 1. Als x het aantal manschappen op een rij in het grote vierkant, en y dat in het kleine vierkant is, wat is dan de relatie tussen x en y?

Heb je ook gevonden dat $x^2 - 13y^2 = 1$?. Dit is een zogenaamde 'Pell-vergelijking', genoemd naar John Pell (1611 - 1685). (Er is een hele controverse ontstaan of de vergelijking wel zijn naam verdient; ze was al in het oude Indië bekend bij Brahmagupta en Bhaskara; verder hoort men de namen Lagrange, Brouncker en Rahn). Er is heel veel over de Pell-vergelijking te vertellen. Zie www-history.mcs.st-and.ac.uk en vergelijk met het tijdschriftartikel van H. W. Lenstra Jr., *Solving the Pell equation*, Notices American Mathematical Society, 49 (2002), no 2, 182-192.

Extra opdracht. Die laatste referentie staat op het web (www.ams.org/notices). Zoek er het zogenaamde 'veeprobleem' van Archimedes in op en laat zien hoe dat ook tot een Pell-vergelijking leidt.

We zullen niet ingaan op de vraag hoe men een oplossing voor de Pell-vergelijking kan vinden. Maar de Pell-vergelijking heeft oneindig veel oplossingen, zoals we nu zullen laten zien.

Opdracht 2. Controleer dat $x = 649$, $y = 180$ een oplossing is van $x^2 - 13y^2 = 1$.

Opdracht 3. Bewijs dat de vergelijking $x^2 - 13y^2 = 1$ equivalent is met de vergelijking $(x + y\sqrt{13})(x - y\sqrt{13}) = 1$.

Opdracht 4. Bewijs dat de vergelijking $x^2 - 13y^2 = 1$ oneindig veel oplossingen heeft.
(als het niet lukt: op www.fi.uu.nl/wiskrant, kijk bij nummer 24.4).

Men kan aantonen dat de oplossing uit opdracht 2 de kleinste positieve oplossing is.

Opdracht 5. Hoe groot was dus het leger van Harold minstens (volgens Guy)? Lijkt je dat realistisch? Om die laatste vraag te beantwoorden moet je eigenlijk de bevolkingsaantallen van Engeland uit de middeleeuwen kennen. Zoek dat in een betrouwbare bron op (bijvoorbeeld: Medieval Sourcebook: *Tables on Population in Medieval Europe* op het web) en ga hierover een discussie aan.

Harold, koning van Engeland, verloor overigens de slag tegen Willem van Normandië...

Werkblad: Wat is beslisbaar?

Van welke wiskundige problemen kan een computer eigenlijk beslissen of ze een oplossing hebben of niet? Rond 1900 speculeerde de beroemde wiskundige David Hilbert dat het antwoord eigenlijk altijd 'ja' is (hij had het natuurlijk niet over computers, want die waren er toen nog niet, maar je kan zijn uitspraak wel zo vertalen). We gaan er nu wel van uit dat we op een ideale computer werken, dat wil zeggen dat we niet door praktische bezwaren worden gehinderd: we hebben onbeperkt geheugen en onbeperkte rekenkracht tot onze beschikking, en de tijd voor het uitvoeren van een programma doet er niet toe.
Op dit werkblad staat een aantal opdrachten. Bij sommige opdrachten kun je hints vinden op www.fi.uu.nl/wiskrant (kijk bij nummer 24.4).

Opdracht 1. Wat denk jij over deze vraag? Ga de discussie aan. Bedenk een aantal wiskundige problemen waarvan een computer kan beslissen of er een oplossing is of niet.

Om het probleem wat duidelijker te stellen, kijken we eerst wat er überhaupt als output uit zo'n computer kan komen. Het zijn eigenlijk altijd lijstjes van gehele getallen (die iets kunnen coderen, bijvoorbeeld letters of pixels). Daarom maken we de volgende definitie:

> **Definitie**. Een verzameling getallen heet *recursief opsombaar* als ze de output is van een eindig computerprogramma (dat wil zeggen een programma met eindig veel regels) op een ideale computer (die daarvoor oneindig lang mag draaien).

Zo zijn 'de machten van 2' recursief opsombaar: laat je computer 2^0, 2^1, 2^2,... afdrukken. Eindige verzamelingen zijn natuurlijk recursief opsombaar (waarom?). Ook ingewikkeldere verzamelingen kunnen recursief opsombaar zijn.

Opdracht 2. Geef drie voorbeelden van recursief opsombare verzamelingen met oneindig veel elementen.

Opdracht 3. Laat zien dat de verzameling priemgetallen recursief opsombaar is.

Rond 1950 werkten Martin Davis en Julia Robinson aan het volgende typische probleem:

> **DR-probleem**. Is er een eindig computerprogramma op een ideale computer dat als input neemt: een willekeurige polynoomvergelijking $f(x_1, ..., x_m) = 0$, waarvan de coëfficiënten gehele getallen zijn en als ouput geeft: 'JA' als de vergelijking een oplossing heeft met $x_1, ..., x_m$ natuurlijke getallen, en 'NEEN' anders.

Intuïtief wordt hier de vraag gesteld: hoe moeilijk is het te beslissen of een polynoomvergelijking een oplossing in natuurlijke getallen heeft? Je zou de computer kunnen laten testen of er een oplossing is of niet door gewoon alle mogelijke waarden voor $x_1, ..., x_m$ in te vullen, maar als er geen oplossing is krijg je nooit een antwoord. Dat is dus niet goed.
Voor sommige vergelijkingen kan je het DR-probleem oplossen, bijvoorbeeld $x^2 + x - 1 = 0$. Als x een natuurlijk getal is met $x^2 + x - 1 = 0$, dan moet namelijk $x(x+1) = 1$. Omdat x een natuurlijk getal is, is dat ook waar voor $x+1$. Maar dus is x een deler van 1, en dus is $x = 1$. Maar dan is $x(x+1) \neq 1$. In het algemeen is het probleem echter veel moeilijker.
Julia Robinson was een heel bijzondere wiskundige. Ten eerste was ze als vrouw in de universitaire wiskunde werkzaam. Ze was de eerste vrouwelijke voorzitter van het Amerikaans Wiskundig Genootschap, en ze leed aan leukemie.

> Opdracht 4. Zoek iets op over het leven en werk van Julia Robinson. Ga een discussie aan: zijn er veel vrouwelijke wiskundigen? Voldoen die aan de stereotypen van een wiskundige (en wat zijn dat)? Kunnen vrouwen wel even goed wiskunde als mannen?

Om iets over het DR-probleem te kunnen zeggen, maken we volgende definitie:

> **Definitie**. Stel dat $f(x_1, ..., x_m)$ een polynoom is in m veranderlijken met gehele coëfficiënten. Stel dat t een natuurlijk getal is, en vul voor x_m dat getal t in het polynoom in. Je krijgt een polynoomvergelijking $f(x_1, ..., x_{m-1}, t) = 0$ in $m-1$ veranderlijken $x_1, ..., x_{m-1}$. De verzameling getallen t waarvoor deze vergelijking een oplossing heeft in gehele getallen heet een diophantische verzameling.

Een verzameling V is dus diophantisch als ze de verzameling 'parameters' t is waarvoor een polynoomvergelijking $f(x_1, ..., x_{m-1}, t) = 0$ een oplossing heeft in de 'veranderlijken' $x_1, ..., x_{m-1}$.

Voor $f(x_1, x_2) = x_1 \cdot x_2 - 1$ krijg je de verzameling $V = 1$.

> Opdracht 5. Laat zien dat de verzameling niet-priemgetallen diophantisch is.

Hier komt nu het verband met de computer:

> Opdracht 6. Toon aan dat een diophantische verzameling recursief opsombaar is.

Als klap op de vuurpijl bewezen Davis en Robinson tussen 1950 en 1970 samen met Hilary Putnam en Yuri Matijasevich de volgende stelling:

> **DMPR-stelling**. Recursief opsombare verzamelingen zijn diophantisch. }

Dus is bijvoorbeeld de verzameling priemgetallen diophantisch. Dat werd jarenlang als heel ongeloofwaardig gezien.

Wat zegt de stelling over het DR-probleem? In de wiskundige logica kan men het volgende bewijzen (maar het bewijs is wat te moeilijk om hier te geven): }

> **Feit**. Er is een recursief opsombare verzameling R waarvan het complement $N - R$ niet recursief opsombaar is.

In dit feit is N de verzameling natuurlijke getallen. Dus als $R = \{2, 3, 5, 7, 11, ...\}$ de verzameling priemgetallen is, dan is $N - R = \{0, 1, 4, 6, 8, 9, 12, ...\}$ het complement. De laatste opdracht stelt je redeneervermogen op de proef:

> Opdracht 7. Gebruik dit feit en de DMPR-stelling om aan te tonen dat het antwoord op de DR-vraag negatief is.

Conclusie: er zijn wiskundige problemen die er op het eerste gezicht niet zo moeilijk uitzien, maar waarvan we met wiskundige middelen kunnen aantonen dat een computer ze nooit zal kunnen beslissen. De vraag is natuurlijk of de mens ze ooit zal kunnen beslissen...

U kunt de complete werkbladen met hints en aanwijzingen downloaden van de site van de *Nieuwe Wiskrant*: http://www.fi.uu.nl/wiskrant/