

Diophantische vergelijkingen vanuit de verte bekeken



door

Gunther Cornelissen
Universiteit Utrecht

Plan

0. Hoe oud was Diophantus?
1. Probleem VI.12 van Diophantus meetkundig bekeken (en los het dan zelf op).
2. Tekenen en projecteren.
3. De slag bij Hastings: een foutje bij de bisschop van Amiens.
4. Wat kunnen computers zeggen over diophantische vergelijkingen (en wat niet)?
5. Vanuit de verte kijken naar de oplossingen (met Mazur).

Diophantus van Alexandrië (3e eeuw)

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 5 jaar daarna geboren; de zoon werd maar half zo oud als zijn vader, en de vader overleed vier jaar na de zoon.

uit een Griekse Anthologie
van **Metrodorus** (6e eeuw)

Diophantus van Alexandrië (3e eeuw)

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 5 jaar daarna geboren; de zoon werd maar half zo oud als zijn vader, en de vader overleed vier jaar na de zoon.

uit een Griekse Anthologie
van **Metrodorus** (6e eeuw)

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

Diophantus' Arithmetica

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NUMERIS MULTANGVLIS.
LIBER VNVS.

*CVM COMMENTARIIS C. G. BACHETI V. C.
& obseruationibus D. P. de FERMAT Senatoris Tolosani.*

*Accessit Doctrina Analytica inuentum nouum, collectum
ex varijs eiusdem D. de FERMAT Epistolis.*



TOLOSAE,
Excudebat BERNARDVS BOSCH, à Regione Collegij Societatis Iesu.
M. DC. LXXX. m

Lemma bij vraagstuk VI.12

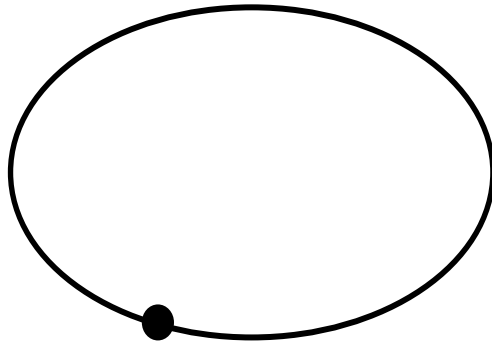
Als $A + C$ een kwadraat is, dan heeft

$$Ax^2 + C = y^2$$

oneindig veel rationale oplossingen.

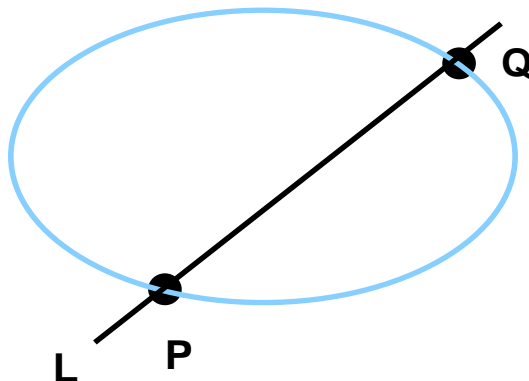
De meetkunde van Lemma VI.12

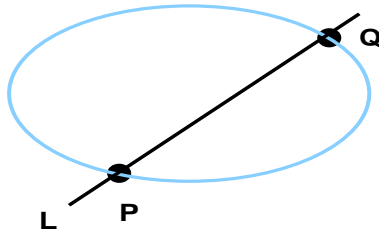
De grafiek van $Ax^2 + C = y^2$ in het (x, y) -vlak is een **kegelsnede**



$P = (x_0, y_0)$ met $x_0, y_0 \in \mathbb{Q}$ heet een **rationaal punt**

Stelling. Stel dat een lijn L met rationale richtingscoëfficiënt de kegelsnede in twee punten P en Q snijdt. Als P rationaal is, dan ook Q .





Bewijs.

- De lijn L_t door $P = (x_0, y_0)$ met richtingscoëfficiënt t is $y = y_0 + t(x - x_0)$.
- De kegelsnede is $Ax^2 + C = y^2$.

Om het tweede snijpunt $Q = (x_1, y_1)$ te vinden moeten we dus oplossen

$$\begin{cases} y = y_0 + t(x - x_0) \\ Ax^2 + C = y^2 \end{cases}$$

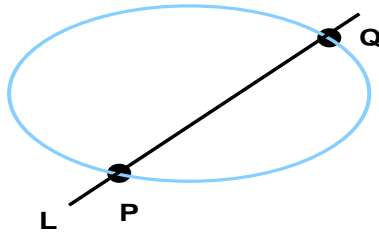
Invullen geeft een kwadratische vergelijking voor x_0, x_1 waarvan de coëfficiënten rationale getallen zijn, dus er zijn $a, b, c \in \mathbb{Q}$ met

$$ax^2 + bx + c = a(x - x_0)(x - x_1)$$

Bijgevolg is $x_0 \cdot x_1 = c/a \in \mathbb{Q}$.

Omdat $x_0 \in \mathbb{Q}$, is dus $x_1 \in \mathbb{Q}$.

Uit $(x_1, y_1) \in L_t$ volgt dan $y_1 \in \mathbb{Q}$.



Alle oplossingen van Diophantus' probleem.

- Kies $P = (1, \alpha)$ met $\alpha = \sqrt{A + C}$
- Los op

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

Dus voldoet x aan:

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

en die vergelijking heeft als oplossingen:

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

Bijgevolg zijn **alle rationale oplossingen** gegeven door

$$\left\{ \left(-\frac{t^2 - 2\alpha t + A}{A - t^2}, \frac{\alpha A + \alpha t^2 - 2tA}{A - t^2} \right) : t \in \mathbb{Q} \cup \{\pm\infty\} \right\}$$

Terminologie

- Een stelsel polynoomvergelijkingen (in meerdere veranderlijken) met **gehele coëfficiënten** heet een **variëteit**:

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

- $V(R)$ is de verzameling oplossingen

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

van het stelsel V , bijv.

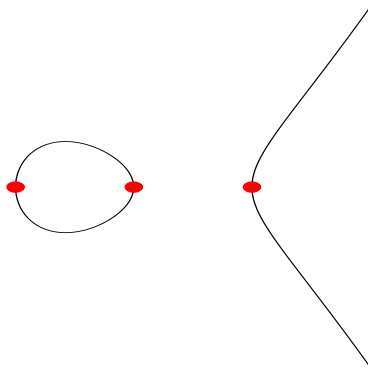
- $V(\mathbf{Z})$ zijn de gehele oplossingen
- $V(\mathbf{Q})$ zijn de rationale oplossingen
- $V(\mathbf{R})$ zijn de reële oplossingen
- $V(\mathbf{C})$ zijn de complexe oplossingen

Centrale vraag: Wat zijn $V(\mathbf{Z})$ en $V(\mathbf{Q})$?

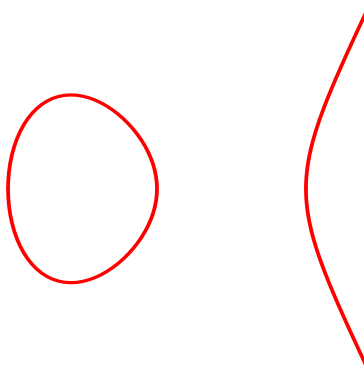
Tekenen...

We kunnen $V(\mathbf{R})$ in de n -dimensionale ruimte \mathbf{R}^n tekenen en daarop $V(\mathbf{Q})$ rood inkleuren:

- $V_1 : y^2 - x^3 + x = 0$



- $V_2 : y^2 - x^3 + 2x = 0$



bijvoorbeeld: $(-\frac{1803649}{2325625}, \frac{3693595151}{3546578125}) \in V_2(\mathbf{Q})$

Niet zo makkelijk voor te stellen als $n \geq 3 \dots$



Projecteren ...



We zullen $V(\mathbf{R})$ (en de rode $V(\mathbf{Q})$) vanuit de n -dimensionale ruimte \mathbf{R}^n op een coördinaatas projecteren:

- $V : y^2 - x^3 + x = 0$ op x -as



- $V : y^2 - x^3 + 2x = 0$ op x -as



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

“Een diophantische verzameling is een verzameling van gehele (of rationale) x waarvoor gehele (of rationale) (x_2, \dots, x_n) bestaan met

$$f_1(\mathbf{x}, x_2, \dots, x_n) = \dots = f_m(\mathbf{x}, \dots, x_n) = 0”$$

Centrale vraag.

Wat is de aard van Z -diophantische verzamelingen?

Zijn Z -diophantische verzamelingen **misschien zelf de verzameling gehele oplossingen van een polynoom** (in één veranderlijke)?

[Nee, want (flauw tegenvb.) $y - x$ projecteert op Z].

Nee, leuk tegenvoorbeeld:



De slag van Hastings op 14 oktober 1066

“Harold’s 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!””

Carmen de Hastigae Proelio
van **Guy, bisschop van Amiens**

De slag van Hastings op 14 oktober 1066 (II)



- y manschappen op een rij per klein vierkant.
- 13 kleine vierkanten.
- Één groot vierkant met x manschappen op een rij.

$$x^2 - 13y^2 = 1$$

- Alle $(x, y) \in \mathbf{Z}$ bepaald door

$$x + y\sqrt{13} = (649 + 180\sqrt{13})^n$$

voor een $n \in \mathbf{Z}_{>0}$ geven een gehele oplossing.

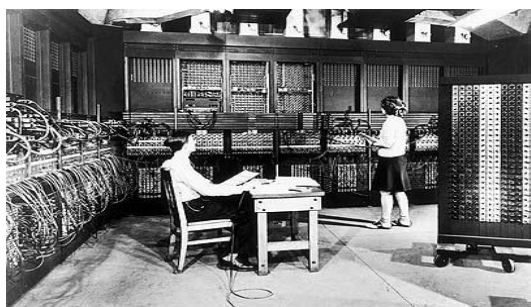
- Er zijn dus **oneindig vele mogelijke x** .
- Een polynoom heeft maar eindig veel wortels.

—————

- De kleinste oplossing ($n = 1$) geeft een leger van 421200 man. Realistisch?

Centrale vraag. Wat is de aard van \mathbb{Z} -diophantische verzamelingen?

Vaststelling. \mathbb{Z} -diophantische verzamelingen zijn recursief opsombaar.



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

- geen beperkingen op het geheugen en de precisie van de hardware.
- programma is bijv. C++-programma.
- snelheid van het programma is irrelevant.

Bewijs van de vaststelling.

Doorloop alle mogelijke x_1, \dots, x_n in één of andere volgorde en kijk of ze een oplossing zijn. Zo ja, output x_1 .

Centrale vraag. Wat is de aard van \mathbb{Z} -diophantische verzamelingen?



M. Davis J. Robinson Y. Matiyasevich (H. Putnam)

1950-1970

Stelling. Recursief opsombare verzamelingen zijn \mathbb{Z} -diophantisch (en omgekeerd).

Niet-zo-makkelijk Gevolg. Er is geen computerprogramma dat van een willekeurige diophantische vergelijking kan bepalen of er een gehele oplossing is of niet.

Voorbeeld. De verzameling **priemgetallen**

$$2, 3, 5, 7, \dots, 2^{20996011} - 1, \dots$$

is precies de projectie op de X -as van de gehele oplossingen in $X, A, B, C, D, a, \dots, z$ van volgende vergelijkingen:

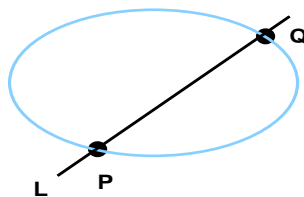
$$\begin{aligned} X = A^2 + B^2 + C^2 + D^2 = & \\ & (k + 2)(1 - (wz + h + j - q)^2 - ((gk + 2g + k + 1)(h + j) \\ & + h - z)^2 - (2n + p + q + z - e)^2 - (16(k + 1)^3(k + 2) \\ & (n + 1)^2 + 1 - f^2)^2 - (e^3(e + 2)(a + 1)^2 + 1 \\ & - o^2)^2 - ((a^2 - 1)y^2 + 1 - x^2)^2 - (16r^2y^4 \\ & (a^2 - 1) +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

Centrale vraag II. Wat is de aard van \mathbb{Q} -diophantische verzamelingen?



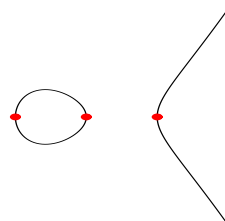
Idee van **Barry Mazur** (1990):
Bekijk $V(\mathbb{Q})$ vanuit de verte.

- Terug naar $Ax^2 + C - y^2$:



Vaststelling. Willekeurig dicht bij elke reële oplossing ligt ook een rationale oplossing: vanuit de verte ziet $V(\mathbb{Q})$ eruit als $V(\mathbb{R})$.

- Merk op: hoeft niet waar te zijn voor alle V : voor $y^2 - x^3 + x = 0$ ziet $V(\mathbb{Q})$ er vanuit de verte uit als een auto die 's nachts een fietser inhaalt:



Vermoeden van Mazur. Vanuit de verte heeft $V(\mathbb{Q})$ maar eindig veel componenten: de topologische afsluiting van $V(\mathbb{Q})$ in $V(\mathbb{R})$ heeft maar **eindig veel samenhangende componenten**.

- **Gevolg** (van het vermoeden). De verzameling gehele getallen \mathbf{Z} is **géén \mathbb{Q} -diophantische verzameling**, d.w.z. er is geen V met een projectie π zodat $\mathbf{Z} = \pi(V(\mathbb{Q}))$.

[Bewijs: eenvoudige topologie.]

- **Als \mathbf{Z} \mathbb{Q} -diophantisch is**, dan is er ook **geen computerprogramma** dat beslist of een diophantische vergelijking **rationale oplossingen** heeft of niet.

[Bewijs: voor willekeurige W in N veranderlijken is

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

- We weten **niet** of er een computerprogramma bestaat dat beslist of een diophantische vergelijking **rationale oplossingen** heeft of niet.

- **Stelling** (C-Zahidi, 1999). Als Mazur's vermoeden waar is, dan is er geen **diophantisch model** van \mathbf{Z} in \mathbb{Q} , d.w.z. geen berekenbare injectie $\mathbf{Z} \hookrightarrow \mathbb{Q}^k$ die \mathbf{Z} -diophantische verzamelingen op \mathbb{Q} -diophantische verzamelingen afbeeldt.

[Bewijs gebruikt DPMR-stelling.]

Conclusie.

