Diophantische vergelijkingen

een onmogelijke uitdaging

Frits Beukers

Vakantiecursus 2010

Eerste voorbeeld

Bedenk twee gehele getallen x en y zó dat

$$x^7 - y^3 = 3$$

Een oplossing is $x = 2, y = 5$. Waarschijnlijk is dit de enige oplossing, alleen weet niemand dit te bewijzen.

Tweede voorbeeld

Bedenk twee gehele getallen x en y zó dat

$$x^2 - 61y^2 = 3$$

De "kleinste" is $x = 8, y = 1$.
De "één na kleinste" heeft $y = 42912791$. Er zijn oneindig veel oplossingen en de structuur daarvan is bekend.

Derde voorbeeld

Bedenk drie positieve rationale getallen (breuken) x, y, z zó dat

$$x^4 + y^4 + z^4 = 1$$

In 1988 ontdekte Noam Elkies dat er oneindig veel oplossingen zijn. De "kleinste" luidt

$$x = \frac{95800}{422481},\ y = \frac{217519}{422481},\ z = \frac{414560}{422481}.$$

Definitie

Een diophantische vergelijking is een vergelijking van de vorm

$$F(x_1, x_2, \ldots, x_n) = 0$$

in de gehele of rationale onbekenden $x_1, x_2, \ldots, x_n$. Het symbool F staat voor een polynoom (veelterm) in de variabelen $x_1, \ldots, x_n$. Voorbeelden zijn:

1. $F = x^7 - y^3 - 3$ (twee variabelen, graad 7)
2. $F = x^2 - 61y^2 - 3$ (twee variabelen, graad 2)
3. $F = x^4 + y^4 + z^4 - 1$ (drie variabelen, graad 4)

Diophantus

Diophantus van Alexandrië,

- leefde waarschijnlijk rond 200 A.D
- Bekendste werk: *Arithmetica*, een collectie van 13 boeken, elk bestaande uit een 30-tal opgaven, waarin naar rationale oplossingen wordt gevraagd.
- Er zijn slechts 6 boeken bekend, via Byzantijnse wereld in Europa gekomen.
- Rond 1970 werd nog een viertal boeken ontdekt, in het Arabisch vertaald, waarvan men veronderstelt dat het ook delen van de Arithmetica zijn.

Een simpele vergelijking

We lossen de vergelijking

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

op in rationale getallen x, y. Herschrijf,

$$(x + y)(x - y) = 1.$$

Stel $u = x + y$. Dan volgt uit de vergelijking dat $x - y = 1/u$. Conclusie:

$$x = \frac{1}{2}\left(u + \frac{1}{u}\right), \quad y = \frac{1}{2}\left(u - \frac{1}{u}\right).$$

Op dezelfde manier heeft $x^2 - y^2 = A$ (voor gegeven A) de algemene oplossing

$$x = \frac{1}{2}\left(u + \frac{A}{u}\right), \quad y = \frac{1}{2}\left(u - \frac{A}{u}\right).$$

Nog een simpele vergelijking

We lossen de vergelijking

$$x^2 + y^2 = 1$$

op in rationale getallen x, y.
Breng y^2 naar rechts en deel door x^2,

$$1 = \left(\frac{1}{x}\right)^2 - \left(\frac{y}{x}\right)^2$$

Dus er is een rationaal getal u zó dat

$$\frac{1}{x} = \frac{1}{2}\left(u + \frac{1}{u}\right), \quad \frac{y}{x} = \frac{1}{2}\left(u - \frac{1}{u}\right).$$

Hieruit volgt,

$$x = \frac{2u}{u^2 + 1}, \quad y = \frac{u^2 - 1}{u^2 + 1}.$$

Pythagoreische drietallen

We gaan wat waarden voor u invullen in

$$x = \frac{2u}{u^2+1}, \quad y = \frac{u^2-1}{u^2+1}.$$

Neem $u = 2$,

$$\left(\frac{4}{5}\right)^2 + \left(\frac{3}{5}\right)^2 = 1 \Rightarrow 4^2 + 3^2 = 5^2.$$

Neem $u = 5/4$,

$$\left(\frac{40}{41}\right)^2 + \left(\frac{9}{41}\right)^2 = 1 \Rightarrow 40^2 + 9^2 = 41^2.$$

Of $u = 37/21$,

$$\left(\frac{777}{905}\right)^2 + \left(\frac{464}{905}\right)^2 = 1 \Rightarrow 777^2 + 464^2 = 905^2.$$

Niet altijd $\square + \square$

NB: Niet elk getal A is te schrijven als som van twee rationale kwadraten. Bijvoorbeeld:

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

Of

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

(zie Opgave 2.5 en 2.6)

Probleem V.3 uit de Arithmetica

Gegeven een getal A, vindt drie rationale getallen x, y, z zó dat

$$\begin{aligned} x + A &= \square \\ y + A &= \square \\ z + A &= \square \\ xy + A &= \square \\ yz + A &= \square \\ zx + A &= \square \end{aligned}$$

Hierin staat $\square$ voor het kwadraat van een rationaal getal.
Wij kiezen $A = 2$ (Opgave 2.8 uit de syllabus).

Oplossing van Opgave 2.8

We lossen op,

$$\begin{aligned} x+2 &= \square \\ y+2 &= \square \\ z+2 &= \square \\ xy+2 &= \square \\ yz+2 &= \square \\ zx+2 &= \square \end{aligned}$$

Diophantus stelde $x+2=t^2$ en $y+2=(t+1)^2$ (met t voorlopig nog willekeurig te kiezen) en merkt vervolgens op dat

$$xy+2=(t+2)^2(t-1)^2,$$

een kwadraat!!

Oplossing Opgave 2.8 (vervolg)

Vervolgens kiest Diophantus $z = 2(x+y) - 1 = 4t^2 + 4t - 7$ en merkt op dat

$$zx + 2 = (2t^2 + t - 4)^2, \quad yz + 2 = (2t^2 + 3t - 3)^2.$$

Aan de laatste en één na laatste vergelijking is nu ook voldaan! Blijft over de vergelijking $z + 2 = \square$. Uitgeschreven (met $\square = s^2$),

$$(2t+1)^2 - 6 = s^2 \Rightarrow (2t+1)^2 - s^2 = 6.$$

Dus is er een u zó dat

$$2t + 1 = \frac{1}{2}\left(u + \frac{6}{u}\right).$$

Kies $u = 12$, dan volgt $t = 21/8$ en

$$x = \frac{313}{64}, \; y = \frac{713}{64}, \; z = \frac{497}{16}.$$

Algebraische meetkunde

Dit is het gebied dat de reëel- of complex-meetkundige eigenschappen van de objecten gegeven door vergelijkingen $F(x_1, \ldots, x_n) = 0$ bestudeert.

Algebraische getaltheorie

Deze tak van de getaltheorie ontstond uit pogingen halverwege de 19e eeuw om Fermat's vermoeden op te lossen. Echter, de toepassingsmogelijkheden van de algebraische getaltheorie zijn veel breder.

Diophantische approximatie en transcendentietheorie

Vanaf het begin van de twintigste eeuw ontwikkeld. Het zijn deze technieken die, in combinatie met algebraische methoden, tot nu toe het meest succesvol zijn gebleken in de volledige oplossing van speciale diophantische vergelijkingen.

Galoisrepresentaties

Deze tak van de getaltheorie is pas tot volle ontwikkeling gekomen vanaf de tweede helft van de vorige eeuw. De meest spectaculaire toepassing is de oplossing van Fermat's vermoeden door A.Wiles.

Cirkelmethode

Oorspronkelijk bedacht om het probleem van Waring aan te pakken. Komt recent weer in de belangstelling om vergelijkingen in grote aantallen variabelen aan te pakken.

Poging tot overzicht

We gaan diophantische vergelijkingen sorteren naar *aantal variabelen* en *graad*. We spreken ook af dat we naar rationale oplossingen zoeken.
Filosofie:

- Hoe hoger de graad, des te kleiner de "kans" op oplossingen
- Hoe meer variabelen, des te groter de "kans" op oplossingen.

We beginnen met vergelijkingen in twee variabelen, dat zijn vergelijkingen van de vorm $F(x, y) = 0$ in de twee rationale onbekenden x, y.

Twee variabelen, graad $= 1$

De vergelijking is van de vorm $ax + by = c$ met gegeven a, b, c.
Oplossing: y willekeurig en $x = (c - by)/a$.

Twee variabelen, graad $= 2$

In dit geval is $F(x, y) = 0$ de vergelijking van een cirkel, ellips, parabool of hyperbool. Voorbeelden $x^2 - y^2 = 1$ en $x^2 + y^2 = 1$.
Er zijn ofwel geen oplossingen, ofwel oneindig veel.
Voorbeeld van vergelijkingen zonder oplossing:

- $x^2 + y^2 = -1$ (hopelijk duidelijk)
- $x^2 + y^2 = 3$ (modulo 3 kijken)

Twee variabelen, graad $= 3$

In dit geval is $F(x, y) = 0$ de vergelijking van een derde graads kromme, ook wel elliptische kromme genoemd. Voorbeelden: $x^3 + y^3 = 1$ en $y^2 = x^3 - 2$. Hierover zijn talloze boeken en artikelen geschreven. Het aantal oplossingen kan zowel eindig als oneindig zijn.

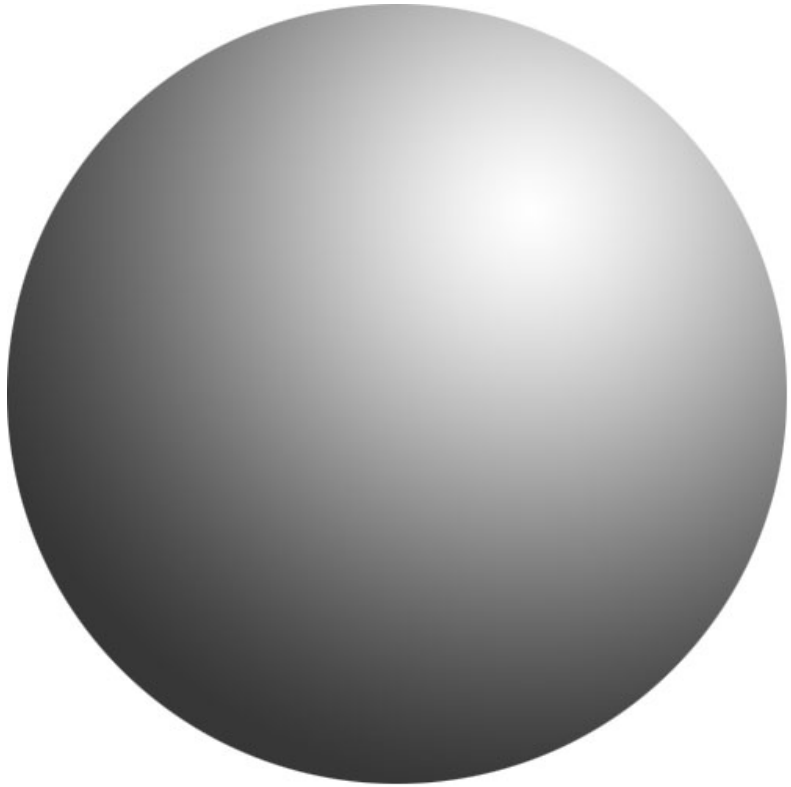
Twee variabelen, graad ≥ 4

In dit geval geldt de *stelling van Faltings* (1984): $F(x, y) = 0$ heeft hooguit eindig veel rationale oplossingen. Dit probleem had sinds 1925 bekend gestaan als het *vermoeden van Mordell*.
NB: De stelling van Faltings is een *eindigheidsuitspraak*. Zij geeft geen enkele methode om de vergelijkingen ook daadwerkelijk op te lossen! Elke vergelijking heeft zijn eigen aanpak nodig, sommige zijn makkelijk, anderen moeilijk. Een paar voorbeelden:

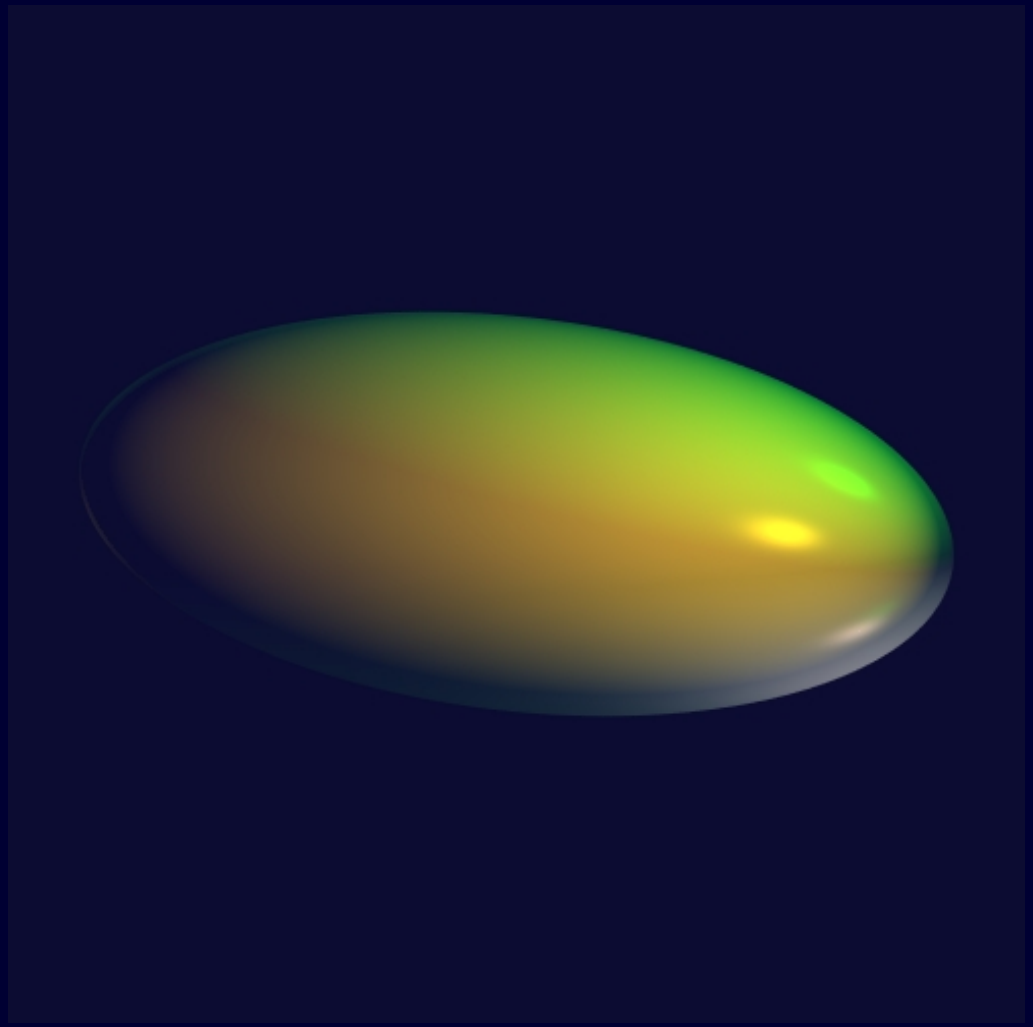
1. $x^4 + y^4 = 3$ heeft geen oplossingen want 3 kan geen som van twee rationale kwadraten zijn (makkelijk dus)
2. $x^4 + y^4 = 17$ heeft als enige oplossing $1^4 + 2^4 = 17$. Om dit aan te tonen is een artikel van 9 bladzijden met geavanceerde technieken nodig
3. $y^2 = x^6 + x^2 + 1$ (probleem VI.17 uit de Arabische versie van de Arithmetica) heeft als enige oplossingen $(x, y) = (0, \pm 1), (1/2, \pm 9/8)$. Dit aantonen was het proefschrift onderwerp van J.Whetherall in 1998

Drie variabelen

De algemene vergelijking luidt $F(x, y, z) = 0$ en het reële plaatje is een oppervlak in de drie-dimensionale ruimte.
Bijvoorbeeld $x^2 + y^2 + z^2 = 1$, de bol

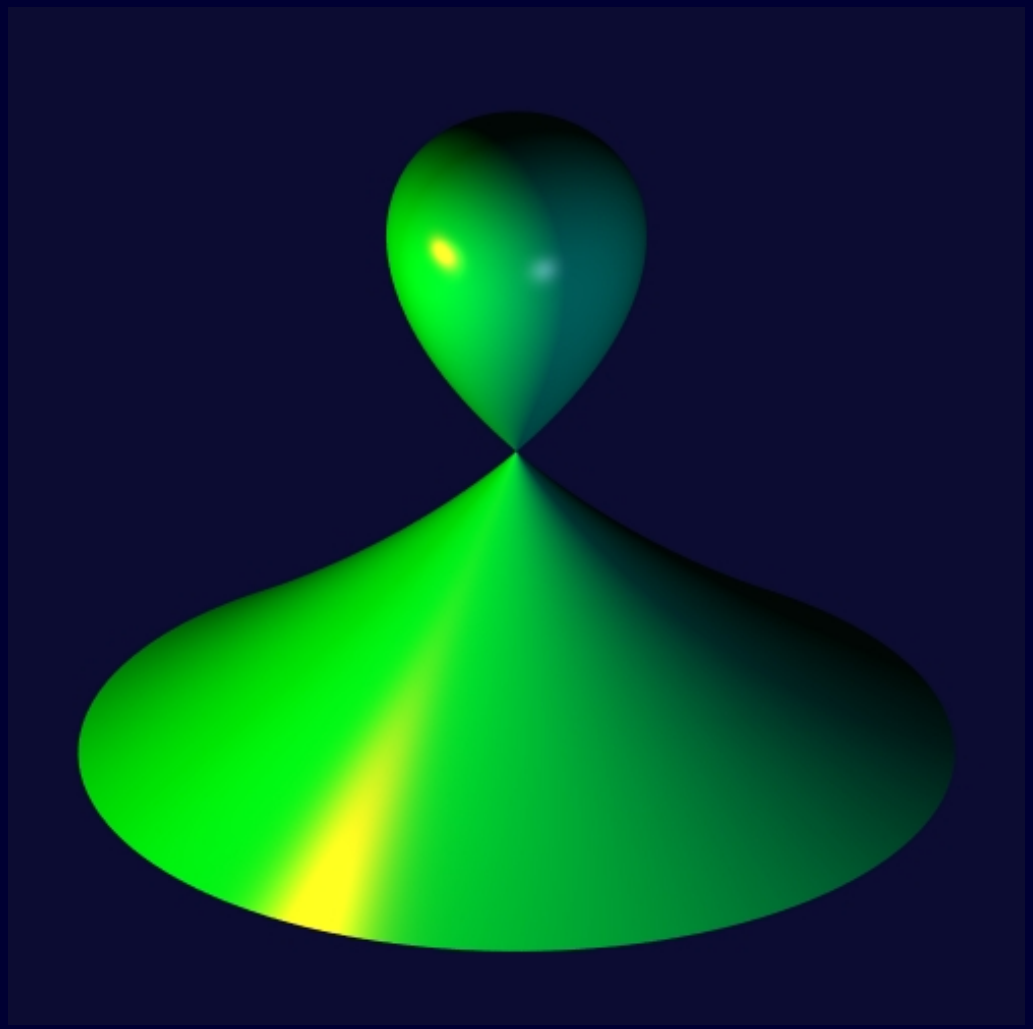


De ellipsoide



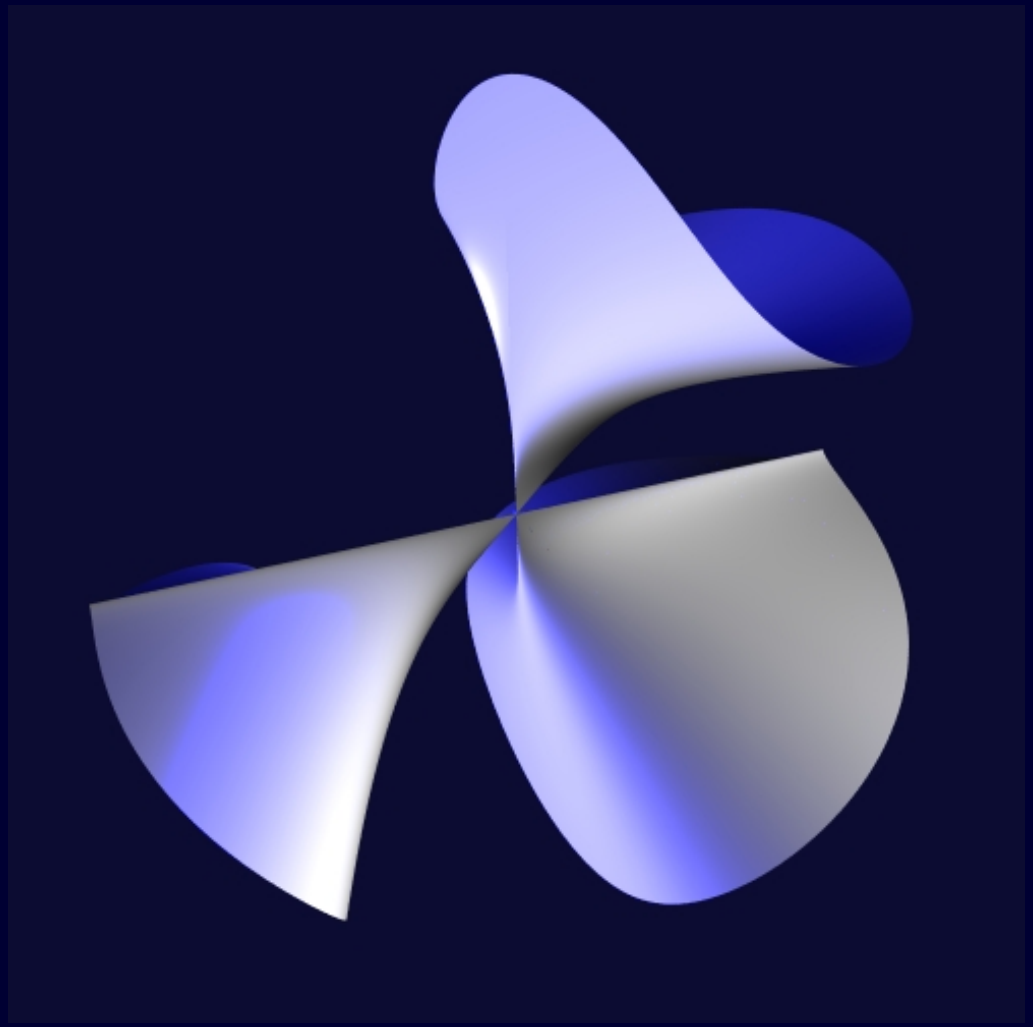
$$3x^2 + 3y^2 + z^2 = 1$$

De druppel



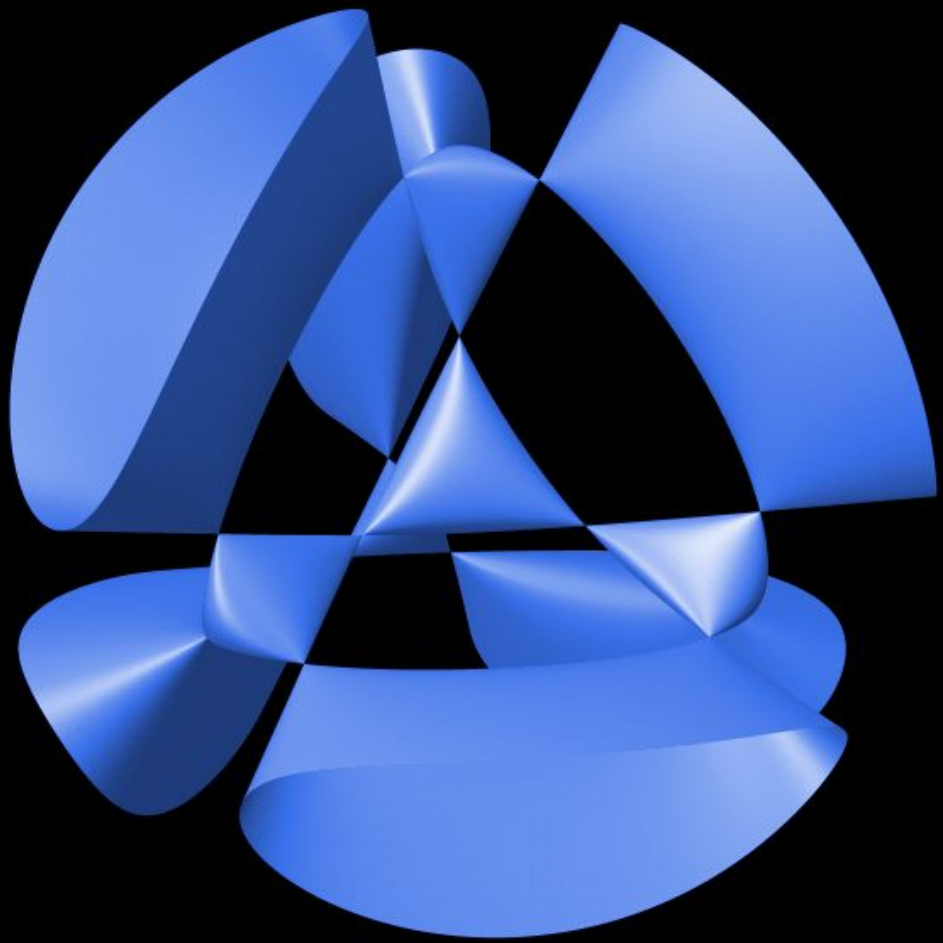
$$x^2 + y^2 + z^3 = z^2$$

De sneeuwvlok



$$x^3 + y^2z^3 + yz^4 = 0$$

Kummer oppervlak



$$(x^2 + y^2 + z^2 - 2)^2 = 5(2x^2 - (z-1)^2)(2y^2 - (z+1)^2)$$

Vergelijkingen in drie variabelen

- Graad 1 of 2: Deze zijn goed aan te pakken, net als in het geval van twee variabelen.
- Graad 3: De vergelijking $F(x, y, z) = 0$ geeft een zogenaamd *cubisch oppervlak*. Stelling van Segre (1948): De vergelijking heeft ofwel geen oplossing, ofwel oneindig veel.
- Graad ≥ 4: Terra incognita....

Hilbert's 10e probleem

David Hilbert (Mathematisch Wereld Congres 1900):
Eine D i o p h a n t i s c h e Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Anders gezegd: *Bestaat er een methode om van een willekeurige diophantische vergelijking te beslissen of er een oplossing in gehele getallen bestaat of niet?*

Belang van Hilbert's vraag

Het blijkt dat notoire problemen uit de wiskunde vertaald kunnen worden in een vraag naar de oplosbaarheid van een diophantische vergelijking.

Goldbach vermoeden: elk even getal ≥ 4 is som van twee priemgetallen.

Er bestaat een polynoom G in (veel) variabelen $x_1, \ldots, x_n$ zó dat

Goldbach vermoeden is waar

$$\Updownarrow$$

$G(x_1, \ldots, x_n) = 0$ heeft geen oplossingen in gehele getallen

Belang van Hilbert's vraag

Het blijkt dat notoire problemen uit de wiskunde vertaald kunnen worden in een vraag naar de oplosbaarheid van een diophantische vergelijking.

Riemann vermoeden: De niet-triviale nulpunten van $\zeta(s)$ liggen allen op de lijn $\mathrm{Re}(s) = 1/2$ in het complexe vlak.

Er bestaat een polynoom G in (veel) variabelen $x_1, \ldots, x_n$ zó dat

Riemann vermoeden is waar

$$\Updownarrow$$

$G(x_1, \ldots, x_n) = 0$ heeft geen oplossingen in gehele getallen

Antwoord

In 1970 beantwoordde Yuri Matijasevich de vraag van Hilbert met:

Nee, er bestaat geen programma dat van iedere diophantische vergelijking beslist of er wel of geen gehele oplossing bestaat.

Het bewijs van Matijasevich was een laatste stap na een lange periode van voorbereidend werk door met name Martin Davis en Julia Robinson.

Slot

Samenvattend:

- Diophantische vergelijkingen zijn nog steeds lastig om op te lossen, ondanks alle moderne ontwikkelingen in de getaltheorie
- Veel problemen uit de wiskunde kunnen worden teruggebracht tot het oplosbaarheidsprobleem van een (fikse) diophantische vergelijking
- Het oplosbaarheidsprobleem kan niet geautomatiseerd worden (Matijasevich)
- Kortom: diophantische vergelijkingen blijven een uitdaging!