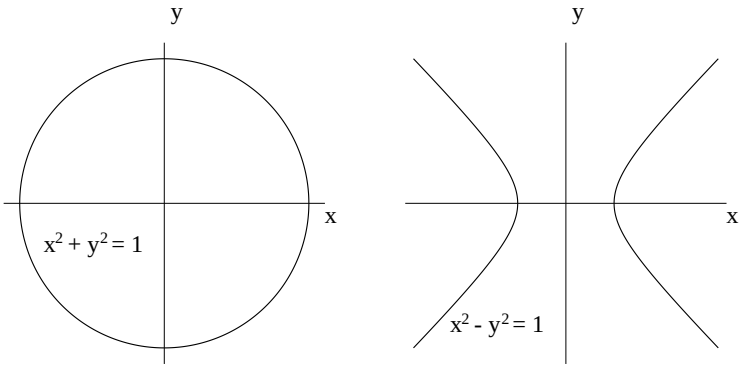
Diophantische vergelijkingen
Een onmogelijke uitdaging

Frits Beukers

8 juni 2010

1 Wat is het probleem?

"Wetende, mijn beste vriend Dionysius, dat jij ernaar verlangt om problemen in de getallen te onderzoeken, heb ik getracht om je, vanuit de grondslagen, het karakter en de kracht die in getallen schuilt uiteen te zetten. Door onbekendheid met het onderwerp zal het eerste begin misschien moeilijk lijken, de beginner kan snel wanhopig worden als succes uitblijft. Maar jij, met je enthousiasme als drijfveer, en mijn begeleiding als leermeester, zult snel in de materie thuisraken. Want passie om te leren, geleid door goede instructie zijn de middelen tot snelle vooruitgang".
Aldus begint, zeer vrij vertaald, de *Arithmetica* van Diophantus van Alexandrië, een boek uit de tijd rond het begin van de jaartelling dat, in tegenstelling tot veel Grieks werk over wiskunde, over getaltheorie gaat. De Arithmetica is een verzameling van 13 boeken, waarvan veel verloren is gegaan. Zes delen, bekend als de Griekse versie, zijn via de Arabische wereld in de 16e eeuw in Europa terecht gekomen en hebben sinds die tijd een inspiratiebron gevormd voor de Europese wiskunde. Vier andere delen zijn rond 1970 ontdekt, hoewel er nog steeds discussie is of het werkelijk om verloren delen van de Arithmetica gaat. In ieder geval staan deze delen bekend als de Arabische versie. In de Arithmetica behandelt Diophantus een lange serie wiskundeproblemen waarin een oplossing in rationale getallen (breuken) gevraagd wordt.
Ter illustratie nemen we een voorbeeld dat bij Diophantus welbekend was. Het is algemeen bekend dat de vergelijkingen $x^2 - y^2 = 1$ en $x^2 + y^2 = 1$ de vergelijkingen zijn van een hyperbool en een cirkel,

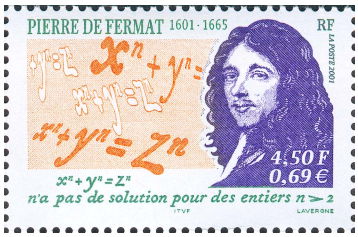


De plaatjes die we hierboven zien zijn een beeld van de oplossingsverzameling van de twee vergelijkingen in de reële getallen x, y. Laten we nu de volgende academische vraag stellen: wat zijn de oplossingen van $x^2 - y^2 = 1$ in rationale getallen (breuken) x, y? En dezelfde vraag voor $x^2 + y^2 = 1$. Anders gezegd, bepaal de punten op bovenstaande hyperbool en cirkel waarvan de coördinaten rationale getallen zijn. Het antwoord op deze vragen was al bij Diophantus, en zelfs daarvoor, bekend en in de volgende paragraaf zullen we de oplossing geven.
In elk geval hebben we nu twee voorbeelden van een diophantische vergelijking gezien. In zijn meest algemene vorm, en in moderne taal, kan een diophantische vergelijking als volgt beschreven worden. Kies een veelterm (of polynoom) $F(x_1, \ldots, x_n)$ in n variabelen $x_1, \ldots, x_n$ met coëfficienten in $\mathbb{Z}$ (gehele getallen). De vergelijking $F(x_1, \ldots, x_n) = 0$ in de gehele of rationale onbekenden $x_1, \ldots, x_n$ noemen we een diophantische vergelijking. De veeltermen uit de eerste twee voorbeelden zijn natuurlijk $F = x^2 - y^2 - 1$ en $F = x^2 + y^2 - 1$. De beroemdste diophantische vergelijking is natuurlijk de vergelijking van Fermat

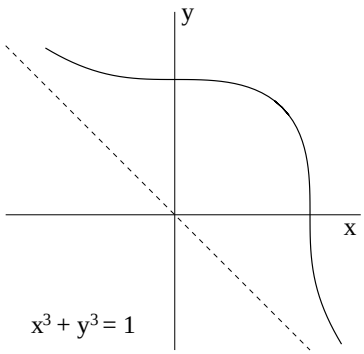
$$x^n + y^n = z^n \quad \text{in } x, y, z \text{ positief geheel.}$$

De exponent n is daarbij een gegeven geheel getal ≥ 2. In de volgende paragraaf zien we dat, als $n = 2$, er oneindig veel oplossingen zijn. Maar Fermat vermoedde al in 1635 dat deze vergelijking geen oplossing heeft als $n \geq 3$. Gedurende de 350 jaar hebben talloze wiskundigen geprobeerd Fermat's vermoeden aan te tonen, maar zonder succes. Wel hebben deze pogingen aanleiding gegeven tot nieuwe ontwikkelingen in de getaltheorie. Pas in 1994 slaagde Andrew Wiles erin het vermoeden van Fermat te bewijzen. Wiles deed nog veel meer, hij gaf namelijk een bewijs van het zogenaamde

Shimura-Taniyama-Weil vermoeden en Fermat was hiervan een gevolg. Het bedwingen van Fermat's probleem was een dermate grote triomf van het menselijk vernuft, dat het voorpagina nieuws was voor bijvoorbeeld de New York Times, en zijn er postzegels uitgebracht om dit feit te herdenken.



Ook zijn er diverse boeken over Wiles' vondst geschreven, met bijbehorende historie, waarvan ik S.Sing, *Fermat's Last Theorem* in het bijzonder kan aanraden. Een andere aanrader is A.J. van der Poorten, *Notes on Fermat's Last Theorem* maar deze vereist een flinke portie wiskundige achtergrond.
Neem nu het geval $n = 3$ van Fermat's vergelijking, dus $x^3 + y^3 = z^3$, en deel door z^3. We krijgen $(x/z)^3 + (y/z)^3 = 1$ en zien, na herschrijving van de breuken $x/z, y/z$ als x, y, dat volgens Fermat de kromme $x^3 + y^3 = 1$ geen rationale punten bevat behalve de voor de hand liggende $(0, 1)$ en $(1, 0)$. Hier is een plaatje van $x^3 + y^3 = 1$ in $\mathbb{R}^2$.



Laten we de 1 aan de rechterzijde vervangen door 22, dus $x^3 + y^3 = 22$. Het reële plaatje van $x^3 + y^3 = 22$ is op een vergrotingsfactor na hetzelfde als bovenstaande plaatje. Echter, nu zijn er wel oneindig veel rationale punten. De oplossing met kleinste noemers is $(25469/9954, 17299/9954)$. De variant $x^3 + y^3 = 4$, op zijn beurt, heeft weer geen oplossingen. Sommige getallen zijn dus wel som van twee rationale derde machten (dwz derde machten van rationale getallen), zelfs op oneindig veel manieren, anderen weer niet. Een dergelijk grillig gedrag, gecombineerd met de enorme moeilijkheidsgraad van

de problemen, is voor de ene wiskundige een nachtmerrie en voor de ander een ultieme uitdaging.
Een ander succesverhaal, naast Wiles, is Mihailescu's bewijs van het vermoeden van Catalan in 2002. Kijken we naar de rij zuivere machten (kwadraten, derde machten, vierde machten, ...) dan begint deze met

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, \ldots$$

Het valt op dat het verschil tussen de achtereenvolgende getallen in deze rij gemiddeld genomen toeneemt. Catalan formuleerde in 1844 het vermoeden dat de enige zuivere machten met onderling verschil 1 de getallen $2^3 = 8$ en $3^2 = 9$ zijn. Meer dan anderhalve eeuw bleef dit vermoeden onbewezen, totdat in 2002 Preda Mihailescu een bewijs van deze stelling gaf. Hoewel het niet de diepte en reikwijdte van Wiles' werk heeft, is dit toch een prestatie van formaat. Talloze wiskundigen voor Mihailescu waren er niet uitgekomen en vele van mijn vakgenoten hadden niet gedacht dit moment nog mee te mogen maken. Momenteel zijn er twee boeken over dit bewijs geschreven, maar helaas bestemd voor wiskundige experts. De methode maakt sterk gebruik van het verschil 1. Kijkend naar de rij zuivere machten zou men kunnen vermoeden dat $5^2 = 25$ en $3^3 = 27$ de enige machten zijn die 2 verschillen, maar niemand heeft enig idee hoe dit aan te pakken. Dezelfde opmerking geldt voor alle andere verschillen groter dan 1.
Terug naar Diophantus. In de rest van dit verhaal zullen we een voorbeeld uit de Arithmetica behandelen en daarbij iets laten zien van de enorme ingenieusiteit van Diophantus om een oplossing te geven. Daarna maken we een grote sprong in de tijd en beschrijven heel kort moderne pogingen om enige orde in de wereld van diophantische vergelijkingen te scheppen. Ondanks alle successen van de getaltheorie zal daarbij blijken dat veel problemen waar Diophantus mee worstelde nog steeds een probleem vormen. Men zou zich zelfs kunnen afvragen of we met dit gebied een fundamentele scheidslijn benaderen van dingen die men weet en dingen die men nooit zal kunnen weten. Bepalen waar die lijn precies ligt is de grote uitdaging.

2 Een probleem van Diophantus

Laten we eerst eens kijken naar twee vergelijkingen uit de inleiding, te beginnen met $x^2 - y^2 = 1$ in de rationale onbekenden x, y. We kunnen deze

vergelijking herschrijven als $(x-y)(x+y)=1$. Laten we $x+y$ aangeven met u. Dan volgt uit onze vergelijking dat $x-y=1/u$. Dus

$$x+y=u, \qquad x-y=1/u.$$

Hieruit leiden we gemakkelijk af dat

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

Elke oplossing heeft dus deze gedaante. Omgekeerd gaat men eenvoudig na dat voor elke keuze van u de bijbehorende x, y voldoen aan $x^2-y^2=1$. Het moet nu niet moeilijk zijn om de volgende algemenere vraag te beantwoorden.

Opgave 2.1 *Stel A is een geheel of rationaal getal ongelijk aan 0. Bepaal alle rationale oplossingen x, y van $x^2-y^2=A$.*

Hoewel het een beetje van onze hoofdlijn afwijkt is hier nog een opgave.

Opgave 2.2 *Stel A is een geheel getal. Als A oneven is, of deelbaar door 4, dan is A te schrijven als verschil van twee gehele kwadraten. Bewijs dit. Bewijs daarna dat in het overblijvende geval $A \equiv 2 (\mathrm{mod}\ 4)$ er geen oplossing is.*

Laten we nu overgaan naar de vraag $x^2+y^2=1$ in de rationale getallen x, y. Stel $x \neq 0$ en deel aan beide zijden door x^2. We krijgen $1+(y/x)^2=(1/x)^2$, waaruit $(1/x)^2-(y/x)^2=1$ volgt. Ons probleem is nu teruggebracht tot het schrijven van 1 als verschil van twee kwadraten. Er bestaat dus een rationaal getal u zo dat

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

Hieruit leiden we af dat

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

Dit is dus de algemene oplossing. Laten we een paar voorbeelden nemen. Kies $u=3/10$ en we krijgen $(60/109)^2+(91/109)^2=1$. Kies $u=4/7$ en we krijgen $(56/65)^2+(33/65)^2=1$. Het is trouwens aardig om uit deze

gelijkheden de noemer weg te vermenigvuldigen. We krijgen $60^2+91^2 = 109^2$ en $56^2 + 33^2 = 65^2$, met andere woorden, oplossingen van de vergelijking $x^2 + y^2 = z^2$ in x, y, z geheel. Dit lukt uiteraard ook in het algemeen. Stel $u = r/s$ met r, s geheel en we vinden $x^2 + y^2 = z^2$ met $x = r^2 - s^2, y = 2rs, z = r^2 + s^2$.

Opgave 2.3 *Stel r, s geheel en $\gcd(r, s) = 1$ (dwz grootste gemeenschapelijke deler van r, s is 1). Stel $x = r^2 - s^2, y = 2rs, z = r^2 + s^2$. Laat zien dat $\gcd(x, y, z) = 1$ als $r \not\equiv s \pmod 2$ en $\gcd(x, y, z) = 2$ als r, s beide oneven zijn.*

Dan nog een iets lastiger opgave ter vermaak.

Opgave 2.4 *Zij a, b, c een drietal gehele getallen zo dat $a^2 + b^2 = c^2$. Toon aan dat minstens een van deze getallen deelbaar is door 5.*

Konden we iedere rationale A schrijven als verschil van twee kwadraten van rationale getallen, voor sommen van twee rationale kwadraten lukt dat niet meer. Bijvoorbeeld $A = 3$. Stel er zijn rationale getallen x, y zo dat $x^2 + y^2 = A$. De kleinste gemeenschappelijke noemer van x, y geven we aan met c. Dus er zijn gehele a, b zo dat $x = a/c$ en $y = b/c$ en $\gcd(a, b, c) = 1$. Uit onze vergelijking volgt nu dat $a^2 + b^2 = 3c^2$. Bekijk deze vergelijking modulo 4. Omdat gehele kwadraten alleen 0 of 1 modulo 4 zijn, volgt hieruit dat $a^2 \equiv b^2 \equiv c^2 \equiv 0 \pmod 4$. Dus a, b, c moeten even zijn en dit is in tegenspraak met onze voorwaarde dat $\gcd(a, b, c) = 1$. We concluderen dat er geen oplossingen bestaan.

Opgave 2.5 *Zij A een geheel getal dat $3 \pmod 4$ is. Laat zien dat $x^2 + y^2 = A$ geen oplossing in rationale x, y heeft.*

De volgende opgave is wat lastiger.

Opgave 2.6 *Toon aan dat 21 geen som van twee rationale kwadraten is (hint: kijk modulo 3, of 7). Geef nog een ander geheel getal A dat $1 \pmod 4$ is, maar geen som van twee rationale kwadraten.*

Nadat we aldus warm gedraaid zijn, kunnen we naar een probleem van Diophantus kijken. Bovenstaande methoden waren trouwens in Diophantus tijd al gemeengoed en hij maakt er veelvuldig gebruik van. Hier is probleem 3 uit het Griekse Boek V van de Arithmetica in moderne taal opgeschreven.

Opgave 2.7 (Diophantus V.3) *Gegeven een getal A (niet nul), vindt drie rationale getallen zo dat elk van deze getallen alsmede hun producten vermeerderd met A een kwadraat opleveren. Anders gezegd, vindt rationale x, y, z zo dat*

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

De notatie $\square$ (kwadraat) spreekt hopelijk voor zich. Diophantus zelf gebruikte trouwens de notatie Δ^Υ voor kwadaten (en K^Υ voor derde machten, $\Delta^\Upsilon\Delta$ voor vierde machten, ΔK^Υ voor vijfde machten en $K^\Upsilon K$ voor zesde machten).
Laten we ter illustratie van Diophantus oplossing het voorbeeld $A = 1$ nemen. Tegenwoordig zouden we meteen de flauwe oplossing $x = y = z = 0$ opmerken. Diophantus werkte echter impliciet met positieve getallen en dus doen wij dit ook in dit voorbeeld. Alvorens te beginnen is het misschien goed om te kijken of een oplossing meteen te zien is. Als dat na enige tijd niet gelukt is, hebben we daarna des te meer respect voor Diophantus' oplossing. Het is belangrijk om te weten dat Diophantus tevreden was als hij 1 oplossing had gegeven. Blijkbaar was dit een illustratie want zijn methoden waren meestal voor uitbreiding vatbaar. Diophantus streefde er niet naar om een volledige oplossingsverzameling te vinden, zoals we dat tegenwoordig graag willen.
Zoals gezegd, we kiezen $A = 1$ en volgen Diophantus. Noem het eerste kwadraat t^2 en stel dat het tweede kwadraat $(t+1)^2$ is. Dat wil zeggen dat $x = t^2-1$ en $y = (t+1)^2-1 = t^2+2t$. Het slimme van Diophantus keuze is dat nu ook $xy+1$ een kwadraat is, namelijk $xy+1 = (t^2-1)(t^2+2t)+1 = (t^2+t-1)^2$. Daarmee zouden we het probleem $x+A = \square, y+A = \square, xy+A = \square$ hebben opgelost. Blijkbaar was dit te eenvoudig naar Diophantus' smaak en heeft hij er een interessanter opgave van gemaakt door er nog een derde getal z bij te halen. Diophantus merkt nu op dat als we $z = 2(x + y) - 1 = (2t+1)^2-4$ nemen, ook de getallen $xz+1$ en $yz+1$ kwadraten zijn, namelijk $(2t^2 + t - 2)^2$ en $(2t^2 + 3t - 1)^2$ zoals men zelf gemakkelijk kan narekenen.

De enige vergelijking die overblijft is $z+1=\square$, ofwel $(2t+1)^2-3=s^2$ voor zekere s. Het probleem is nu teruggevoerd tot het schrijven van 3 als verschil van twee kwadraten, een techniek die we nu beheersen. Uit opgave 2.1 weten we dat er een u bestaat zo dat $2t+1=\frac{1}{2}(u+3/u)$. Kies bijvoorbeeld $u=1/2$. We vinden $t=9/8$ en

$$x=\frac{17}{64},\quad y=\frac{225}{64},\quad z=\frac{105}{16}.$$

Uiteraard kunnen we oneindig veel oplossingen maken door oneindig veel verschillende waarden voor u te nemen. We moeten daarbij wel oppassen dat $t>1$ blijft, anders wordt x negatief.
Het opmerkelijke van Diophantus' methode is dat hij voor alle waarden van A werkt, dus niet alleen $A=1$. In de Arithmetica geeft Diophantus een oplossing bij $A=5$,

$$x=\frac{2861}{676},\quad y=\frac{7645}{676},\quad z=\frac{20336}{676}.$$

Opgave 2.8 *Vindt een oneindige serie oplossingen voor Diophantus' opgave met $A=2$.*

Laten we Diophantus' opgave nog eens opschrijven, nu met de kwadraten expliciet opgeschreven,

$$\begin{aligned} x+A &= p^2\\ y+A &= q^2\\ z+A &= r^2\\ xy+A &= u^2\\ xz+A &= v^2\\ yz+A &= w^2 \end{aligned}$$

Tgenwoordig zouden we het probleem als volgt aanpakken. We zien dat $x=p^2-A, y=q^2-A, z=r^2-A$. Vul deze in de laatste drie vergelijkingen in en we krijgen het stelsel

$$\begin{aligned} (p^2-A)(q^2-A)+A &= u^2\\ (p^2-A)(r^2-A)+A &= v^2\\ (q^2-A)(r^2-A)+A &= w^2 \end{aligned}$$

in de onbekende breuken p, q, r, u, v, w. In plaats van één diophantische vergelijking hebben we nu een stelsel diophantische vergelijkingen gekregen. Diophantus vond één of meer oplossingen en was daar tevreden mee. Tegenwoordig rusten wij niet voordat we de gehele oplossingsverzameling gevonden hebben. Maar helaas, ondanks alle technieken die tussen Diophantus' tijd en nu gevonden zijn, is het totaal niet duidelijk hoe dit probleem moet worden aangepakt.
Hier is nog een ander probleem uit de Arithmetica,

Opgave 2.9 (Diophantus, V.27) *Gegeven een getal A, vindt drie kwadraten zo dat de som van elk tweetal plus A weer een kwadraat is.*

Laten we het geval $A = 0$ eens opschrijven,

$$\begin{array}{ccccccc} a^2 & + & b^2 & & & = & \square \\ a^2 & & & + & c^2 & = & \square \\ & & b^2 & + & c^2 & = & \square \end{array}$$

Meetkundig kunnen we dit probleem opvatten als vragen naar een rechthoeking blok met rationale zijden a, b, c waarvan de zijvlaksdiagonalen ook rationale lengte hebben. Diophantus' methode komt grofweg neer op het volgende. Leg één van de zijden vast, zeg $c = 1$. Dan komen de tweede en derde vergelijking weer neer op het schrijven van 1 als verschil van twee kwadraten. Laten we $a = \frac{1}{2}(u - 1/u)$ en $b = \frac{1}{2}(v - 1/v)$ kiezen. Stel $v = -tu$. De eerste vergelijking wordt

$$\frac{1}{4}\left(u - \frac{1}{u}\right)^2 + \frac{1}{4}\left(\frac{u}{t} - \frac{t}{u}\right)^2 = \square.$$

Uitwerken geeft

$$\left(\frac{1}{t^2} + 1\right) u^2 - 4 + (t^2 + 1)\frac{1}{u^2} = \square.$$

Om ervoor te zorgen dat de linkerzijde een kwadraat wordt, willen we t, u zodanig kiezen dat $4 = (t^2 + 1)/u^2$. Met andere woorden, $4u^2 = t^2 + 1$. En alweer moeten we 1 als verschil van twee kwadraten schrijven, $(2u)^2 - t^2 = 1$. Diophantus maakt hier de specifieke keuze $t = 3/4$, maar wij kiezen $t = (\tau - 1/\tau)/2$. Voor u kunnen we dan $u = (\tau + 1/\tau)/4$ nemen. Vervolgens vinden we $v = -ut = (\tau^2 - 1/\tau^2)/8$ en voor a, b,

$$a \;=\; \frac{1}{2}(u - 1/u) = \frac{t^4 - 14t^2 + 1}{8t(t^2 + 1)}$$

$$\begin{aligned} b &= \frac{1}{2}(v - 1/v) = \frac{3t^4 - 10t^2 + 3}{4(t^4 - 1)} \\ c &= 1 \end{aligned}$$

Als we alle zijden van ons gevonden blok vermenigvuldigen met $8t(t^4 - 1)$ krijgen we de oplossingen

$$\begin{aligned} a &= t^6 - 15t^4 + 15t^2 - 1 \\ b &= 6t^5 - 20t^3 + 6t \\ c &= 8t^5 - 8t \end{aligned}$$

We mogen t hierin willekeurig rationaal kiezen. Door de keuzen die we gemaakt hebben is dit natuurlijk niet de volledige oplossingsverzameling, net zo min als dat bij Diophantus het geval is. Naast bovenstaande oplossing zijn er nog vele andere series oplossingen gevonden, er zijn zelfs oneindig veel van dit soort series. Helaas is de volledige oplossingsverzameling nog steeds niet bekend.
Tenslotte, om de zaak nog iets dramatischer te maken kunnen we aan ons stelsel de extra eis $a^2 + b^2 + c^2 = \square$ toevoegen. Meetkundig vragen we dan naar een rechthoekig blok met rationale zijden waarvan alle diagonalen, zowel zijvlaksdiagonalen als lichaamsdiagonaal, ook rationale lengte hebben. Een dergelijk blok noemen we *rationale cuboide*. Tot op de dag van vandaag is het niet bekend of dergelijke rationale cuboiden al of niet bestaan.

Opgave 2.10 *Geef een oplossing met drie verschillende getallen a, b, c van opgave 2.9 voor $A = 1$,*

$$\begin{array}{ccccccccc} a^2 & + & b^2 & & & + & 1 & = & \square \\ a^2 & & & + & c^2 & + & 1 & = & \square \\ & & b^2 & + & c^2 & + & 1 & = & \square \end{array}$$

3 Stand van zaken

Uiteraard is er sinds Diophantus veel gebeurd op het gebied van diophantische vergelijkingen. De technieken van Diophantus bestonden uit eenvoudige algebra die op buitengewoon slimme manier werden ingezet. Tegenwoordig beschikken we over een veel ruimer arsenaal aan technieken. Zonder uit te leggen wat ze precies betekenen noemen we hier de belangrijkste.

- Algebraische meetkunde. Dit is het gebied dat de reëel- of complex-meetkundige eigenschappen van de objecten gegeven door vergelijkingen $F(x_1, \ldots, x_n) = 0$ bestudeerd. Alvorens een diophantische vergelijking op te lossen is het goed om eerst de meetkundige structuur te kennen. Men zou kunnen zeggen dat Diophantus' aanpak een eenvoudige vorm van algebraische meetkunde is, hoewel Diophantus zelf nooit meetkundige termen gebruikt.

- 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 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. Toepassingen op diophantische vergelijkingen vonden pas plaats vanaf de 80-er jaren. De meest spectaculaire is de oplossing van Fermat's vermoeden door A.Wiles.

Naast resultaten zijn er ook veel vermoedens geformuleerd over de oplossingsverzameling van een diophantische vergelijking. De meest vergaande zijn de zogenaamde *Vojta vermoedens*. Deze geven een mooie systematiek in de aard van oplossingsverzamelingen van diophantische vergelijkingen. Helaas zijn dit slechts vermoedens en ligt het bewijs ervan waarschijnlijk in een nog verre toekomst.
Om toch een idee te geven van de systematiek van diophantische vergelijkingen geven we een korte bloemlezing over diophantische vergelijkingen in twee en drie variabelen. Voor iets uitgebreidere informatie verwijzen we naar F.Beukers, *Getaltheorie voor beginners*, Hoofdstukken 12.4, 13, 15, 16 en 17.

Twee variabelen
De algemene vorm is $F(x, y) = 0$ in rationale x, y, waarbij F een polynoom is in twee variabelen en met gehele coefficienten. Meetkundig gezien stelt deze vergelijking een algebraische kromme voor, denk maar aan $x^2 + y^2 = 1$

(cirkel) of $xy = 1$ (hyperbool). We sorteren onze vergelijkingen eerst naar hun totale graad.
Vergelijkingen van graad 1 hebben we de vorm $ax + by = c$. De bepaling van rationale punten hierop is simpel. We kiezen gewoon een rationale x en berekenen $y = (c - ax)/b$.

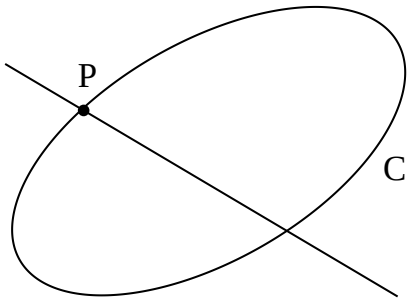
graad 2
Vergelijkingen van graad 2 zien er uit als

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

waarin $a, b, c, d, e, f \in \mathbb{Z}$ gegeven zijn. Meetkundig levert deze vergelijking ons een ellips, parabool,hyperbool of een tweetal rechte lijnen op. We noemen dergelijke krommen *kegelsneden*. Bijvoorbeeld $x^2+2y^2 = 1$ (ellips) of $y = 2x^2$ (parabool) of $xy = 1$ (hyperbool) of $(x+y-1)(x+2y) = 0$ (paar rechte lijnen). Het geval dat de kegelsnede uit twee lijnen bestaat noemen we *reducibel*. De andere gevallen noemen we *irreducibel*. Soms krijgen we de lege verzameling zoals bij $x^2 + y^2 + 1 = 0$.
Laten we eerst eens kijken hoe het zit met de rationale oplossingen, dat wil zeggen punten (x, y) op de kegelsnede met rationale x, y. We geven hier de stelling en een voorbeeld hoe we eraan komen. We zullen hier het taalgebruik bezigen dat we een rationale oplossing van de vergelijking een rationaal punt op de kegelsnede noemen en een geheeltallige oplossing een geheel punt op de kegelsnede.

Stelling 3.1 *Stel a, b, c, d, e, f geheel. Als de kegelsnede $ax^2 + bxy + cy^2 + dx + ey + f = 0$ irreducibel is en een rationaal punt bevat. Dan bevat hij er oneindig veel.*

Deze stelling berust op het feit dat het heel eenvoudig is om, uitgaand van een rationaal punt, andere rationale punten te construeren.



Noem de kegelsnede C en het rationale punt P. Kies een willekeurige rechte lijn l door P waarvan de helling rationaal is. Deze lijn snijdt de kegelsnede C in twee punten. Een ervan kennen we al, dat is P. Het andere punt blijkt ook rationaal te zijn. Door de helling van l te varieren kunnen we op deze manier alle rationale punten op C vinden.
Hier is een voorbeeld. Beschouw de kromme $x^2+3y^2-5x+1=0$. Het is duidelijk dat $x=1, y=1$ een rationaal punt is. Trek een willekeurige rechte door $(1,1)$ met rationale helling. Deze heeft de vorm $y=1+t(x-1)$ met t rationaal. Snijdt deze lijn met $x^2+3y^2-5x+1=0$. We vinden,

$$\begin{aligned} 0 &= x^2+3(1+t(x-1))^2-5x+1 \\ &= x^2-5x+4+6t(x-1)+3t^2(x-1)^2 \\ &= (x-1)(x-4)+6t(x-1)+3t^2(x-1)^2 \end{aligned}$$

Eén oplossing kennen we al, $x=1$, vanwege het punt $P=(1,1)$. De x-coördinaat van het andere snijpunt wordt $x=(4-6t+3t^2)/(1+3t^2)$. De bijbehorende waarde van y is $y=(1+3t-3t^2)/(1+3t^2)$. Het resultaat is dat $x=(4-6t+3t^2)/(1+3t^2), y=(1+3t-3t^2)/(1+3t^2)$ voor willekeurige rationale t een oplossing van $x^2+3y^2-5x+1=0$ is. Neem bijvoorbeeld $t=5/4$, waarmee we $x=19/91, y=1/91$ vinden. De oplossingen kunnen er dus best spectaculair uitzien. We noemen deze methode de *koordenmethode*.

Opgave 3.2 *Gebruik de koordenmethode met het punt* $(1,0)$ *om de oplossingen van* $x^2+y^2=1$ *in rationale* x, y *te vinden.*

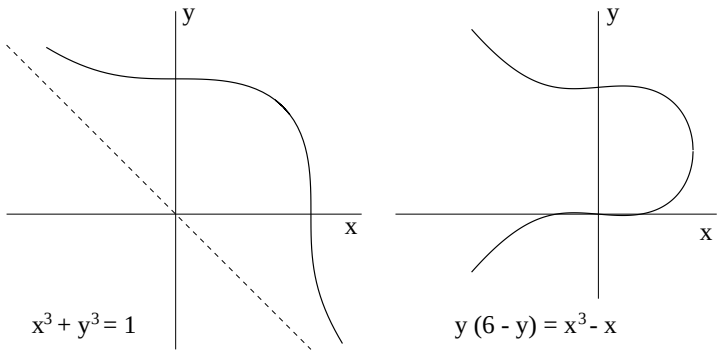
Opgave 3.3 *Gebruik de koordenmethode om de oplossingen van* $x^2-3xy+3y^2-x-y=0$ *in rationale* x, y *te vinden.*

Tenslotte zij opgemerkt, dat er ook kegelsneden zijn met gehele coëfficienten waarop helemaal geen rationale punten liggen, zoals $x^2+y^2=-1$ (hopelijk duidelijk) of $x^2+y^2=3$, die we eerder hebben uitgewerkt.
Over gehele oplossingen van kwadratische vergelijkingen in twee variabelen bestaan ook resultaten, maar daarvoor verwijzen we naar F.Beukers, *Getaltheorie voor Beginners* Hoofdstuk 16.3.

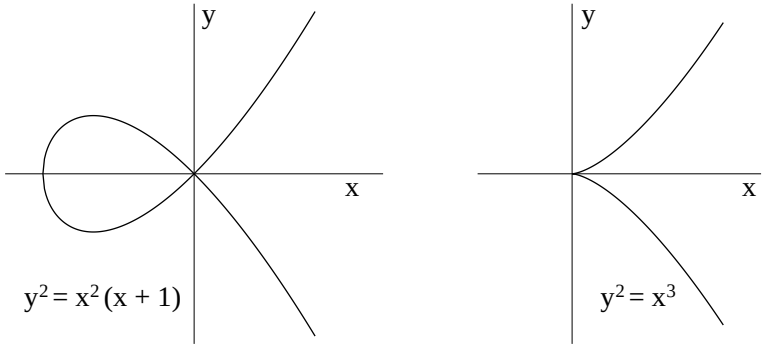
graad 3
Dit is het geval van de vergelijking

$$a_{30}x^3+a_{21}x^2y+a_{12}xy^2+a_{03}y^3+a_{20}x^2+a_{11}xy+a_{02}y^2+a_{10}x+a_{01}y+a_{00}=0$$

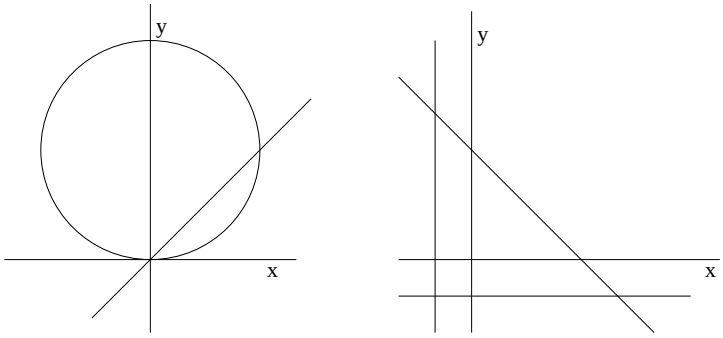
waarin $a_{ij} \in \mathbb{Z}$ voor alle i, j gegeven zijn en x, y, zoals gewoonlijk, de onbekenden. Neem even aan dat niet alle coëfficienten nul zijn. De punten gedefinieerd door deze vergelijking noemen we een cubische kromme en we zullen hem C noemen. In deze paragraaf beperken we ons tot *niet-singuliere* krommen C. Het zou iets te ver voeren om hier precies te omschrijven wat ermee bedoeld wordt. Grof gezegd betekent het dat de kromme geen singuliere punten bevat, ook niet in het 'oneindige'. Hier zijn een paar voorbeelden,



Een punt op de kromme C heet singulier als de kromme in dat punt geen raaklijn heeft. De volgende voorbeelden hebben een singulier punt in $(0, 0)$.



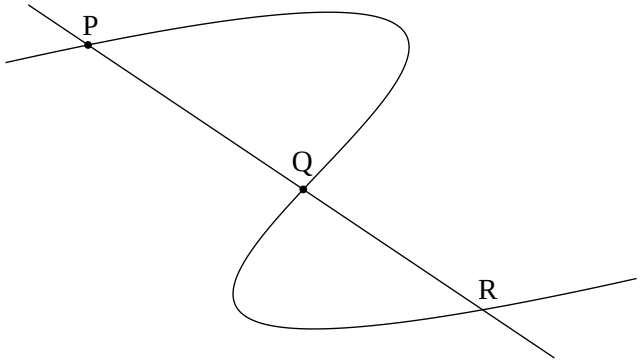
Vervolgens zijn ook de reducibele krommen, dat wil zeggen krommen die uit meerdere deelkrommen bestaan, singulier. Zoals $(y - x)(x^2 + y^2 - y) = 0$ en $(x + 1)(y + 1)(x + y - 3) = 0$,



$(x - y)(x^2 + y^2 - y) = 0$ $(x + 1)(y + 1)(x + y - 3) = 0$

We zullen het verder alleen over niet-singuliere cubische krommen, ook wel *elliptische kromme* genoemd, hoewel ze verder helemaal niets met ellipsen te maken hebben. Het is een naam die historisch zo gegroeid is. Het bekendste voorbeeld van een elliptische kromme is $y^2 = x^3+ax^2+bx+c$ waarin het polynoom $x^3 + ax^2 + bx + c$ geen meervoudige nulpunten mag hebben. De studie van rationale punten op elliptische krommen is één van de verst ontwikkelde takken van de theorie van de diophantische vergelijkingen. De afgelopen 30 jaar heeft dit onderwerp een enorme ontwikkeling doorgemaakt en een deel van deze ontwikkeling heeft geculmineerd in het bewijs van de Laatste Stelling van Fermat, zie F.Beukers, *Getaltheorie voor Beginners* Hoofdstuk 13.

Uiteraard kunnen wij niet op al deze ontwikkelingen ingaan. Het staat wel vast dat de eerste technieken om oplossingen te vinden in primitieve gedaante al aan Diophantus en Fermat bekend waren. We geven een schets van deze oplossingsmethode en daarna een voorbeeld. Het idee gaat als volgt. Beschouw de cubische kromme C en stel dat we twee rationale punten P en Q op C hebben.



Verbind deze twee punten door een rechte lijn l. Aangezien in het algemeen een rechte lijn een cubische kromme in drie punten snijdt, bevat $l \cap C$ naast P en Q nog een derde snijpunt dat we R noemen. Het blijkt dat dit ook een rationaal punt is en op deze manier kunnen we uit bestaande rationale punten nieuwe rationale punten maken.
Er is ook een variant mogelijk waarin we met één rationaal punt P op C beginnen. Trek vervolgens de raaklijn l door P aan de kromme C. Dan snijdt l de kromme C tweevoudig in het punt P en enkelvoudig in een derde punt dat we weer R noemen. Het blijkt dat R weer een rationaal punt is.
Bovenstaande constructie noemen we de *koorde-raaklijn constructie*. Door deze constructie herhaald uit te voeren, kunnen oneindig veel rationale punten op C vinden, mits ze bestaan.
Laten we de koorde-raaklijn methode eens aan de hand van een voorbeeld uitvoeren. Beschouw de vergelijking $x^3+y^3 = 1729$. Tussen haakjes, men kan opmerken dat 1729 het kleinste positieve getal is dat op meer dan één manier als som van twee gehele derde machten geschreven kan worden, namelijk $1729 = 1^3 + 12^3 = 10^3 + 9^3$. Dit geeft ons meteen een tweetal oplossingen van onze vergelijking. We gaan nu andere rationale oplossingen construeren. Bepaal de rechte lijn die door de twee punten $(1, 12)$ en $(10, 9)$ gaat, $y = -x/3 + 37/3$. Snijd deze met de kromme $x^3 + y^3 = 1729$. We verwachten hierbij drie snijpunten, omdat een rechte lijn een derdegraads kromme (cubische kromme) in het algemeen in drie punten snijdt. Twee snijpunten kennen we al, $(10, 9)$ en $(1, 12)$. We willen graag het derde snijpunt bepalen. Dit kunnen we doen door bijvoorbeeld y uit beide vergelijkingen te elimineren. We krijgen,

$$x^3 + (-x/3 + 37/3)^3 = 1729.$$

Na uitwerking,

$$\frac{26}{27}x^3 + \frac{37}{9}x^2 - \frac{1369}{9}x + \frac{3970}{27} = 0.$$

We vermenigvuldigen dit met $27/26$ om de coefficient van x^3 gelijk aan 1 te maken en vinden,

$$x^3 + \frac{111}{26}x^2 - \frac{4107}{26}x + \frac{3970}{26} = 0.$$

Twee oplossingen van deze vergelijking kennen we al, dat zijn $x = 10$ en $x = 1$. Na wegdeling van de factoren $(x - 1)(x - 10)$ houden we over, $x + \frac{397}{26} = 0$. Dus de x-coördinaat van het derde snijpunt is $x = -397/26$ en

de bijbehorende y-coördinaat is $y = -x/3 + 37/3 = 453/26$. Controle leert inderdaad dat

$$\left(\frac{-397}{26}\right)^3 + \left(\frac{453}{26}\right)^3 = 1729.$$

Om rekenwerk te besparen hadden we derde graadsvergelijking niet door $(x-1)(x-10)$ hoeven delen. We hadden simplweg kunnen opmerken dat minus het product van de drie oplossingen gelijk is aan $3970/26$, de constante term in onze cubische vergelijking. Twee ervan kennen we al, 1 en 10, en blijft dus over minus $3970/26$ gedeeld door 10, en dat is $-397/26$.
Aangemoedigd door het succes van deze constructie kunnen we natuurlijk proberen nog een punt te vinden door $(1, 12)$ en $(-397/26, 453/26)$ op analoge wijze te combineren. Helaas vinden we dan weer het oude punt $(10, 9)$. *Waarom?* Maar geen nood, $(453/26, -397/26)$ (coordinaten verwisselen) is ook een punt op onze kromme en combinatie met $(1, 12)$ levert inderdaad weer een nieuw punt, te weten

$$(2472830/187953, -1538423/187953).$$

Zo doorgaand kan men oneindig veel rationale oplossingen van $x^3+y^3 = 1729$ vinden.
In plaats van een verbindingsrechte tussen twee punten kunnen we ook de raaklijn aan de kromme in een punt, zeg $(1, 12)$ nemen.In het algemeen wordt de raaklijn aan $x^3 + y^3 = A$ in het punt $P = (x_0, y_0)$ gegeven door $x_0^2 x + y_0^2 y = A$. In ons geval krijgen we $x + 144y = 1729$. Deze raaklijn snijdt de kromme in $(1, 12)$ (dubbel) en in een ander punt. De berekening van dit laatste punt gaat op dezelfde manier als daarnet. Eliminatie van y geeft $x^3 + (1729 - x)^3/144^3 = 1729$ en na uitwerking,

$$\frac{2985983}{2985984}x^3 + \frac{1729}{995328}x^2 - \frac{2989441}{995328}x + \frac{5977153}{2985984} = 0$$

Na vermenigvuldiging met $\frac{2985984}{2985983}$ vinden we

$$x^3 + \frac{3}{1727}x^2 - \frac{5187}{1727}x + \frac{3457}{1727} = 0.$$

Een dubbele oplossing kennen we al, $x = 1$. Na wegdeling van de factor $(x-1)^2$ houden we over, $x + \frac{3457}{1727} = 0$. Dus $x = -\frac{3457}{1727}$ en de bijbehorende y-waarde is $y = (1729 - x)/144 = \frac{20760}{1727}$. Controle levert dat inderdaad

$$\left(-\frac{3457}{1727}\right)^3 + \left(\frac{20760}{1727}\right)^3 = 1729.$$

Opgave 3.4 *Beschouw de diophantische vergelijking $y^2 = x^3 + 17$ in rationale onbekenden x, y. De oplossingen $P = (-1, 4)$ en $Q = (-2, 3)$ zijn makkelijk te zien.*

1. *Probeer voor alle gehele x met $|x| < 10$ of er een bijbehorende gehele y bestaat zo dat $y^2 = x^3 + 17$.*

2. *Bepaal de lijn door P, Q en snijdt deze met de kromme $y^2 = x^3 + 17$. Bepaal het derde snijpunt R.*

3. *Verander het teken van de y-coördinaat in R en herhaal de constructie met dit nieuwe punt en Q.*

4. *Construeer nog een paar punten met de reeds gevonden punten. Een klein computerprogramma kan hier erg behulpzaam zijn.*

5. *Bepaal het derde snijpunt van de raaklijn in Q met $y^2 = x^3 + 17$. Doe hetzelfde mat de raaklijn in P.*

Wat betreft *gehele* oplossingen van derde graadsvergelijkingen in twee variabelen is er een diepe stelling van C.L.Siegel uit 1929, zie Stelling 3.5.

graad $\geq$4 Het zal duidelijk zijn dat naarmate de graad van een diophantische vergelijking groter wordt, de kans dat er oplossingen zijn, rationale of gehele, steeds kleiner wordt. Het blijkt dat de graad van een vergelijking niet altijd een goede indicatie geeft van de complexiteit van de bijbehorende kromme. Een veel betere graadmeter is het zogenaamde *geslacht* van een kromme. Daarmee bedoelen we niet het geslacht in biologische zin, maar een geheel getal $g \geq 0$ dat we aan iedere kromme $F(x, y) = 0$ kunnen toekennen. Het is lastig om in dit boek uit te leggen hoe dit geslacht precies gedefinieerd is. Daarvoor verwijzen we naar de boeken over algebraïsche meetkunde. We volstaan hier met de opmerking dat als een kromme van graad n geen singuliere punten heeft, dan is het geslacht gelijk aan $g = (n-1)(n-2)/2$. Dit betekent dat kegelsneden ($n = 2$) geslacht $1 \cdot 0/2 = 0$ hebben en elliptische krommen ($n = 3$) geslacht $2 \cdot 1/2 = 1$. Een niet-singuliere vierde graadskromme daarentegen heeft geslacht $3 \cdot 2/2 = 3$.
Er zijn twee hoofdresultaten die behoren tot de belangrijkste resultaten op het gebied van diophantische vergelijkingen. De allereerste is van C.L.Siegel.

Stelling 3.5 (Siegel, 1929) *Een kromme van geslacht $g > 0$ bevat hoogstens eindig veel geheeltallige punten.*

In de vorige paragraaf hebben we gezien dat een elliptische kromme ($g = 1$) oneindig veel rationale punten kan bevatten. Echter, in de twintiger jaren vermoedde L.J.Mordell al dat een kromme van geslacht $g > 1$ hooguit eindig veel rationale punten bevat. Dit vermoeden gold jarenlang als buitengewoon lastig tot in 1983 G.Faltings een bewijs gaf.

Stelling 3.6 (Faltings, 1983) *Zij C een algebraïsche kromme van geslacht > 1. Dan bevat C hooguit eindig veel rationale punten.*

Het bewijs van deze stelling is echter nog steeds lastig en berust op zeer diepe methoden uit de arithmetisch algebraïsche meetkunde.
De stellingen van Siegel en Faltings zijn stellingen die de eindigheid van de oplossingsverzameling geven. Ze geven echter geen enkele methode om eventuele oplossingen ook inderdaad te vinden. Er is wel een aantal standaardtypen van vergelijkingen dat routine-matig kan worden opgelost. Hierbij worden vaak technieken gebruikt die pas in de 70-er jaren beschikbaar kwamen. Vergelijkingen die afwijken van deze standaardtypen kunnen buitengewoon lastig zijn. Om een paar dramatische voorbeelden te noemen, er is een artikel van 9 bladzijden voor nodig om aan te tonen dat $2^4 + 1^4 = 17$ de enige rationale oplossing (op verwisseling en tekenwisseling na) van $x^4 + y^4 = 17$ is. Een ander voorbeeld, in de Arabische versie van de Arithmetica staat als probleem VI.17 de vraag om $y^2 = x^6 + x^2 + 1$ op te lossen in rationale x, y. Dat de enige oplossingen $(0, \pm 1)$ en $(1/2, \pm 9/8)$ zijn, was het onderwerp van het proefschrift van J.Wheterall in 1998. Men zou kunnen zeggen dat dit tot nu het langst open staande probleem in de geschiedenis van de wiskunde is geweest.

Drie variabelen
Deze vergelijkingen zien er als volgt uit

$$F(x, y, z) = 0$$

waarin F een polynoom met gehele coëfficienten is. Meetkundig gezien hebben we hier met de vraag te maken of een gegeven oppervlak gehele of rationale punten bevat. Denk bijvoorbeeld aan de vergelijking $x^2+y^2+z^2 = 1$ in rationale x, y, z. Anders gezegd, bepaal alle punten met rationale coördinaten op een bol met straal 1. We geven een korte ordening naar graad.

graad 2

In het algemeen ziet deze er uit als

$$a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + a_{12}xy + a_{13}xz + a_{23}yz + b_1x + b2y + b_3z + c = 0$$

in de rationale onbekenden x, y. Vergelijkingen van dit type kunnen op dezelfde manier worden aangepakt als kwadratische vergelijkingen in twee variabelen. Kies namelijk een rationaal punt P op dit kwadratische oppervlak. Construeer vervolgens een rechte lijn l door P en bepaal het tweede snijpunt. Omdat de richting van l vastgelegd door twee parameters kunnen we een parametrisatie met twee parameters verwachten.

Opgave 3.7 *Pas deze methode toe op de vergelijking $x^2+y^2+z^2 = 1$ en het punt $P = (0, 1)$.*

Opgave 3.8 *Toon aan dat de vergelijking $x^2+y^2+z^2 = 7$ in rationale x, y, z geen oplossingen heeft.*

graad 3
Het oppervlak $F(x, y, z) = 0$ noemen we een cubisch oppervlak. Bepaling van rationale punten op een cubisch oppervlak kan lastig zijn. Wel hebben we de volgende stelling.

Stelling 3.9 (Segre, 1946) *Zij $F(x, y, z) = 0$ een cubisch oppervlak. Als er 1 rationaal punt op ligt dan liggen er oneindig veel op.*

De methode om deze stelling te bewijzen gaat geheel via een aantal meetkundige constructies. Met enige fantasie zou men kunnen zeggen dat deze methode bij Diophantus' aanpak aansluit. We laten nu een voorbeeld zien van oppervlakken met oneindig veel rationale punten. Misschien is het leuk om te weten dat deze werd gevonden door een schoolmeester uit Engeland.

Stelling 3.10 (Riley, 1825) *Voor elke gehele n zijn er oneindig veel positieve rationale drietallen x, y, z zó dat $x^3 + y^3 + z^3 = n$.*

Om deze stelling te zien, kies

$$A = \frac{12t - (t+1)^2}{6(t+1)}, \quad B = \frac{(t+1)^3 - 12t(t-1)}{6(t+1)^2}, \quad C = \frac{2t(t-1)}{(t+1)^2}$$

en merk op dat $A^3 + B^3 + C^3 = t/3$. Kies $t = 3nu^3$ met u rationaal, zelf te kiezen zó dat $1 < 3nu^3 < 2$. Vul vervolgens deze t in A, B, C in deel alle drie

door u. De derde machten van de zo gevormde getallen hebben als som n. De ongelijkheid $1 < 3nu^3 < 2$ zorgt ervoor dat de gevonden getallen positief worden. Als men tevreden is met eventueel negatieve getallen dan kan het ook zonder deze voorwaarde.

Opgave 3.11 *Gebruik de zojuist gegeven methode om* 11 *als som van drie positieve rationale derde machten te schrijven.*

graad $\geq$4
We komen nu op een gebied waar weinig bekend is. Er zijn nauwelijks oppervlakken van graad ≥ 4 waarvan men de verzameling rationale punten kent. Technieken om dit soort vergelijkingen aan te pakken zijn er ook nauwelijks. Ter illustratie, Euler vermoedde in de 18e eeuw dat de vergelijking $1 = x^4 + y^4 + z^4$ in rationale x, y, z alleen triviale oplossingen zoals $1 = 1^4 + 0^4 + 0^4$ heeft. Het heeft tot 1988 geduurd voordat N.Elkies het tegendeel aantoonde. Er bestaan zelfs oneindig veel oplossingen. De "kleinste"niet-triviale is

$$\left(\frac{95800}{422481}\right)^4 + \left(\frac{217519}{422481}\right)^4 + \left(\frac{414560}{422481}\right)^4 = 1.$$

Het bewijs van Elkies' resultaat is een ingenieuze combinatie van meetkundige methoden en een aantal gelukkige omstandigheden.
We zijn hiermee aan de grens van onze mogelijkheden gekomen om diophantische vergelijkingen aan te pakken. Dat we daarmee langzaam maar zeker een grens naderen waarin de aanpak van diophantische vergelijkingen ook fundamenteel onmogelijk is, zal uit de volgende paragraaf blijken.

4 Hilbert's tiende probleem

Tijdens het Wereld Mathematisch Congres in 1900 te Parijs hield één van de bekendste wiskundigen uit die tijd, David Hilbert, een voordracht over wat hij dacht dat de grote wiskundeproblemen voor de komende eeuw zou zijn. De volledige tekst is te vinden op de website
`www.mathematik.uni-bielefeld.de/~kersten/hilbert/rede.html`
Hilbert's lijst bestond uit 23 problemen, die allemaal een zekere status hebben gekregen, juist doordat ze in deze lijst voorkomen. Sommigen zijn inmiddels opgelost, anderen niet. Een voorbeeld van een onopgelost probleem is

Hilbert's probleem 8: de zogenaamde *Riemann hypothese*. Deze komt ook voor in de lijst van *Clay Prize problems*, de grote wiskunde problemen voor het nieuwe millenium, ditmaal met een prijzengeld van 1.000.000 US dollar per probleem. Zie de website `www.claymath.org/millennium`.
Het 10e Hilbertprobleem is voor ons van belang. In Hilbert's woorden:

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 Gelichung in ganzen rationalen Zahlen lösbar ist.

Hoewel Hilbert het misschien niet zo formuleerde kwam zijn vraag neer op de vraag of er een methode bestaat om van een willekeurige diophantische vergelijking te beslissen of deze wel of geen oplossingen heeft. Om deze vraag goed te kunnen beantwoorden moeten we ons eerst afvragen wat er verstaan wordt onder een 'methode' of 'algoritme'. In de eerste helft van de 20e eeuw is diep nagedacht over berekenbaarheid, algoritmen en de onderliggende logica. Een van de pioniers op dit gebied was Alan Turing, die de Turingmachine voorstelde als universeel instrument om algoritmen uit te voeren. Tegenwoordig hebben we allemaal een Turingmachine op ons bureau staan, namelijk de gewone computer. Iets preciezer: een Turingmachine is een computer met onbeperkt geheugen. Onze computers hebben altijd een begrensde hoeveelheid geheugen, maar het zal niet moeilijk zijn om er een met onbeperkt geheugen voor te stellen immers, elke keer als we meer geheugen nodig hebben kopen we er wat bij. In deze opvatting is een algoritme (of 'methode') niets anders dan een computerprogramma. Hilbert's tiende probleem komt dus neer op de vraag of er computerprogramma bestaat waarmee van elke diophantische vergelijking beslist kan worden of het wel of geen oplossing in gehele getallen heeft. Hier is het antwoord,

Stelling 4.1 (Matijasevich, 1970) *Er bestaat geen algoritme (=computerprogramma) om van een willekeurige diophantische vergelijking te beslissen of er wel of geen gehele oplossingen zijn.*

Deze stelling werd in 1970 door Yuri Matijasevich bewezen na belangrijk voorbereidend werk van Martin Davis en Julia Robinson. Hiermee was Hilbert's tiende probleem opgelost, maar misschien niet op de manier die Hilbert bedoeld had.

Het is misschien verrassend dat het mogelijk is de onmogelijkheid van het bestaan van een algoritme aan te tonen. Zoiets was echter niet geheel nieuw, het was al eerder vertoond. In de dertiger jaren van de 20e eeuw is er veel fundamenteel werk binnen de grondslagen van de wiskunde verricht, onder anderen door Turing, Church en Gödel, waarin ook al onbeslisbare problemen werden ontdekt, waaronder het bekende 'Halting probleem'. Een spectaculair resultaat uit die tijd was Gödel's onvolledigheidsstelling die grofweg zegt dat er binnen elk axiomasysteem uitspraken zijn die noch te bewijzen, noch te weerleggen zijn. De stelling van Matijasevich past geheel in deze trend, zij het aan de late kant omdat er eerst nog een aantal lastige problemen uit de weg moesten worden geruimd.
Uit het werk van Matijasevich volgt nog meer,

Stelling 4.2 *Er is een polynoom $U(n, x_1, \ldots, x_r)$, dat expliciet geconstrueerd kan worden, met de volgende eigenschap: er bestaat geen enkel algoritme dat voor elke gehele waarde van n kan beslissen of $U(n, x_1, \ldots, x_r) = 0$ oplosbaar is in gehele $x_1, \ldots, x_r$ of niet.*

Er zijn artikelen waarin $U(n, x_1, \ldots, x_r)$ expliciet gegeven wordt. Het zijn reusachtige polynomen, met veel variabelen, die we hier niet zullen reproduceren.
De filosofische impact van Matijasevich's stelling is groot. Allereerst leert het ons dat elke nieuwe diophantische vergelijking een nieuwe uitdaging vormt, er bestaat geen universele methode om ze op te lossen. Een tweede belangrijke consequentie ligt in het volgende. Het blijkt dat veel bekende wiskundige problemen, al of niet opgelost, kunnen worden omgevormd tot een diophantische vergelijking waarvan aangetoond moet worden dat er geen oplossing bestaat. Voorbeelden van dergelijke problemen zijn,

1. Het Goldbach vermoeden, nog steeds onopgelost, dat zegt dat elk even getal ≥ 4 de som is van twee priemgetallen.

2. De Riemannhypothese, nog steeds onopgelost.

3. De Fermatvergelijking $x^n + y^n = z^n$ in de onbekenden $x, y, z \geq 1$ en $n \geq 3$. Inmiddels opgelost.

4. Het vierkleurenprobleem, inmiddels opgelost.

De diophantische vergelijking die bij elk van deze problemen hoort is gigantisch, ze bevatten tientallen variabelen of hebben een enorm hoge graad. Oplossing van dergelijke vergelijkingen is uitgesloten. Dat neemt echter niet weg dat we hiermee zien dat diophantische vergelijkingen een fundamentelere rol in de wiskunde spelen dan alleen maar als bron van interessante vraagstukken. De stelling van Matijasevich laat zien dat we de oplossing van diophantische vergelijkingen, het bewijs van bijvoorbeeld het Goldbach probleem en de Riemann hypothese niet kunnen overlaten aan een machine. Het aangaan van deze uitdagingen blijft mensenwerk.