

Na een jarenlange studie waarin met het fijnste fileermesje de wiskunde steeds verder werd opgedeeld in onderdelen van onderdelen stootte ik op een zin¹ van J. Dieudonné (1906-1992): — vrij vertaald: “dat opdelen is helemaal kaduuk”. Het is zo een beetje mijn motto geworden. Ik zal nu een voorbeeld uit mijn eigen “onderdeel van een onderdeel” (aritmetische meetkunde) laten zien waar dat cross-over-gevoel tot zijn recht komt.

Alles begint met een schijnbaar eenvoudige vraag: los een vergelijking op in rationale getallen (d.w.z., breuken). Om de kwestie spannend te maken nemen we een vergelijking in twee veranderlijken (x en y). Bijvoorbeeld $3x + 2y = 1$. De oplossing is natuurlijk dat we een willekeurige x kiezen en $y = \frac{1-3x}{2}$ stellen — zo zijn $(1, -1)$, $(2, -\frac{5}{2})$, maar net zo goed $(\frac{1234}{5678}, \frac{494}{2839})$ oplossingen. In het bijzonder zijn er *oneindig veel* oplossingen. Het lukt omdat voor x rationaal, ook y rationaal is.

Wat gebeurt er met vergelijkingen van graad twee? Die zijn van de vorm $a_1x^2 + a_2x + b_1y^2 + b_2y + cxy + d = 0$ waarbij a_1, a_2, b_1, b_2, c en d gegeven rationale getallen zijn. We beginnen zoals voorheen en kiezen x , lossen dan de vergelijking op naar y , maar nu is er een probleem. De gevonden y is slechts een rationaal getal als de discriminant van de vergelijking een kwadraat is van een rationaal getal, d.w.z. als er y_0 rationaal bestaat met $y_0^2 = (b_2 + cx)^2 - 4b_1(a_1x^2 + a_2x + d)$ (Waarom?). We zitten dus

¹ “Il serait absurde et contraire à l’esprit même de notre science que de vouloir la compartimenter en divisions rigides, à la manière du découpage traditionnel en Algèbre, Analyse, Géométrie etc. complètement caduc aujourd’hui”

weer opgescheept met een vergelijking van graad twee met twee veranderlijken (nu x en y_0), dus er lijkt iets circulair te zijn aan deze redenering...

We keren terug en delen het oorspronkelijke probleem op in deelvragen: gegeven een polynoom in twee veranderlijken, (a) zijn er überhaupt oplossingen; (b) zijn er eindig veel of oneindig veel oplossingen; (c) hoeveel oplossingen zijn er precies? Over de tweede vraag kunnen we iets zeggen door te kijken naar de *meetkunde* achter de vergelijking. Een lineaire vergelijking (zoals $3x + 2y = 1$) geeft als plaatje in het (x, y) -vlak een rechte lijn. We zeggen dat *er oneindig veel rationale punten op een lijn liggen*. Er geldt meer: de rationale punten liggen *dicht* in de reële punten. Dit is een zogenaamde *topologische* eigenschap van de oplossingen en betekent dat er willekeurig dicht bij elk reëel punt op de lijn (dus een oplossing zoals $(\pi, \frac{1-3\pi}{2})$) een rationale oplossing ligt. Je kan dit zien door de oplossingen te projecteren op een as (bv. de x -as). Omdat elke waarde van x tot een oplossing voor de vergelijking leidt, komt het erop neer te zien dat elk reëel getal op de x -as willekeurig dicht ligt bij een rationaal getal, wat natuurlijk klopt (Zie je dat in?).

Hoe zit het met onze vergelijking van graad twee? Dit keer is het inderdaad mogelijk dat er helemaal geen oplossingen zijn. Kan je daarvan een voorbeeld geven?² Maar wat als er *wél* een rationale oplossing (x_0, y_0) bestaat (dus als we weten dat het antwoord op vraag (a) positief is)? Het plaatje dat bij de vergelijking van graad twee hoort is een kegelsnede. Het ver-

²Denk maar aan $x^2 + y^2 = -1$: omdat kwadraten positief zijn, zijn er zelfs helemaal geen reële getallen (x, y) die aan deze vergelijking voldoen.

rassende is nu dat je dit meetkundige plaatje kan gebruiken om op basis van de oplossing (x_0, y_0) andere oplossingen te vinden. Trek namelijk een (niet raak)lijn door (x_0, y_0) , bv. $y = y_0 + t(x - x_0)$ voor een gekozen rationaal getal t . Die lijn snijdt de kegelsnede in (x_0, y_0) en in een verder punt (x_1, y_1) , dat als belangrijkste eigenschap heeft dat het weer rationaal is — kan je dat bewijzen?³

Dit is dus een manier om de viciëuze cirkel van voorheen een beetje te omzeilen (tenminste als we aannemen dat we één oplossing hebben). Bovendien kan je de richtingscoëfficiënt t van de lijn variëren, en voor elke rationale waarde van t krijg je een rationale punt; i.h.b. dus oneindig veel. Er geldt nog meer: door opnieuw te projecteren op een as zie je dat er rationale oplossingen zijn willekeurig dicht bij reële oplossingen.

Stelling (in principe ≤ 3 e eeuw). *Op een kegelsnede liggen ofwel géén rationale punten, ofwel oneindig veel, en die punten liggen dan dicht in de reële punten van de kegelsnede.*

Dit is een mooi staaltje van het vermengen van algebra, meetkunde en topologie. Waar is de analyse? Op de kegelsnede $x^2 + y^2 = 1$ passen we het voorgaande proces toe met een varia-

³Door substitutie van de vergelijking van de lijn in de kegelsnede verschijnt een vergelijking voor de x -coördinaten van de snijpunten van de lijn en de kegelsnede. De exacte gedaante doet er niet toe, maar de coëfficiënten zijn rationale getallen. Omdat x_0 en x_1 hieraan voldoet, moet x_0x_1 de constante term van deze vergelijking zijn (op de rationale leidende coëfficiënt na), dus is ook x_1 rationaal, en bijgevolg ook $y_1 = y_0 + t(x_1 - x_0)$.

bele lijn door het rationale punt $(0, 1)$. Er komt een parametrisatie uit voor de cirkel: alle punten zijn van de vorm $(\frac{-2t}{t^2+1}, \frac{1-t^2}{t^2+1})$ met t de richtingscoëfficiënt van de gekozen lijn (Kan je dat bewijzen?). Door deze parametrisatie in te vullen in de integraal $\int \frac{dx}{\sqrt{1-x^2}}$ komt er $-2 \int \frac{dt}{t^2+1}$, dus een rationale integrand. Het lukt algemeen voor $\int \frac{dx}{\sqrt{Q(x)}}$ met Q van graad twee (en dat wist Euler (1707-1783) al).

Na kwadraten is het tijd voor een derde macht, bv. in de vergelijking $y^2 = x^3 + ax + b$ met a en b rationale getallen. Dit keer hebben we een zogenaamde *elliptische kromme*, die we als E noteren. Er is opnieuw een mooie meetkundige constructie van een nieuwe rationale oplossing (x_1, y_1) vertrekkende van een gekende oplossing (x_0, y_0) : de raaklijn aan de kromme in (x_0, y_0) snijdt de kromme in een verder punt, en dit is opnieuw rationaal (Kan je dat bewijzen?).

Het blijkt nog beter te zijn het volgende te doen: je kan twee rationale punten P en Q op E *optellen* door ze te verbinden door een rechte lijn (als $P = Q$ neem je de raaklijn in P), en het derde snijpunt met E te spiegelen om de x -as. Het resulterende punt noemen we $P \oplus Q$, de “som” van P en Q . Men kan laten zien dat deze bewerking op punten zich gedraagt zoals het hoort voor een “som” (technisch: (E, \oplus) is een groep).

Maar krijgen we door deze constructie oneindig veel oplossingen, of een dichte verzameling van oplossingen? Niet altijd: als je bv. begint met $P = (3, 8)$ voor $a = -43, b = 166$, dan is

$8P (= P \oplus \dots \oplus P)$ hetzelfde als P . Hier vind je dus maar eindig veel oplossingen, maar wie zegt dat er geen andere zijn? Als je begint met $P = (-1, 4)$ voor $a = 0, b = 17$, dan vind je oneindig veel verschillende oplossingen nP voor verschillende n (maar dat is niet makkelijk te bewijzen), als eerste bv. $2P = (\frac{137}{64}, -\frac{2651}{512})$.

Stelling. (Mordell, 1888-1972) *Er bestaan elliptische krommen met eindig veel en met oneindig veel rationale punten, maar alle rationale punten zijn de “som” (voor \oplus) van veelvoud van slechts eindig veel vast gekozen rationale punten.*

Alle veeltermvergelijkingen die niet tot een lineaire, kwadratische of elliptische kromme kunnen worden herleid (door geschikte substituties) heten *hyperbolische krommen*. Eén van de kroonjuwelen van de aritmetische meetkunde is volgende stelling, met een enorm moeilijk bewijs:

Stelling. (G. Faltings (*1954), 1983) *Op een hyperbolische kromme liggen slechts eindig veel rationale punten.*

In het bijzonder heeft dus de Fermatvergelijking $a^n + b^n = c^n$ maar eindig veel gehele oplossingen voor $n > 3$ (= rationale punten op de kromme $x^n + y^n = 1$). Helaas geeft het bewijs van Faltings geen methode om effectief de oplossingen te vinden. Modeltheorie (onderdeel van wiskundige *logica*) werd rond 1970 gebruikt om te bewijzen dat er geen (bv.) C+-programma is dat vraag (a) voor *gehele* punten kan beantwoorden voor willekeurige krommen.

Ook met de integralen gaat het grondig mis: $\int \frac{dx}{\sqrt{Q(x)}}$ voor Q van graad groter dan twee kan je bijna nooit door een geschikte

substitutie als elementaire functie uitrekenen, precies omdat je een elliptische of hyperbolische kromme *niet* “eenvoudig” kan parametriseren. Een vierde booglengte van een cirkel ($\pi/2$) is onze oude bekende $\int_0^1 \frac{dx}{\sqrt{1-x^2}}$, en zijn grote broer $I = \int_0^1 \frac{dx}{\sqrt{1-x^4}}$ is een vierde booglengte van het lemniscaat $(x^2 + y^2)^2 - x^2 + y^2 = 0$. Gauss (1777-1855) ontdekte dat voor $a_0 = \sqrt{2}, b_0 = 1$ en $a_{n+1} = \frac{a_n + b_n}{2}, b_{n+1} = \sqrt{a_n b_n}$ (dus afwisselend aritmetisch en geometrisch gemiddelde nemen), de rij $\frac{\pi}{2} a_n$ convergeert naar I . Dit getal is zo een beetje de “ π van het lemniscaat”.

Met de stelling van Faltings is, tenminste wat betreft de Fermatvergelijking, niet het laatste woord gezegd, dat werd in het vorige decenium gesproken:

Stelling. (A. Wiles (*1953) 1994) *Voor elke gehele oplossing (a, b, c) van de Fermatvergelijking $a^n + b^n = c^n$ voor $n > 2$ geldt $abc = 0$.*

Vreemd genoeg begint het bewijs van Wiles met het bekijken van de elliptische kromme $y^2 = x(x - a^n)(x + b^n)$. In het bewijs laat men zien dat deze kromme zowel “modulair” *moet* zijn, als “niet-modulair” *kan* zijn. Wat dit precies betekent is, opnieuw, een boek vol algebra, meetkunde en analyse. Kortom, wiskunde.