De band tussen algebra en meetkunde

Sinds juli 2001 ben ik als KNAW-onderzoeker verbonden aan het KdV Instituut voor Wiskunde. Mijn vakgebied is de algebraïsche meetkunde. Algebra en meetkunde, die kom je wel vaker samen tegen. Maar waarom eigenlijk?

In 1997 had ik een sollicitatiegesprek bij de KNAW, voor mijn huidige positie. De commissie bestond uit een aantal exacte wetenschappers. Geen algebraïsch-meetkundigen, maar wel mensen die behoorlijk wat van wiskunde weten. Dus had ik een mooi verhaal voorbereid over mijn onderzoek. Echter, zodra ik over algebra en meetkunde begon kwamen er vragen over wat die twee met elkaar te maken hebben, en uiteindelijk ging het hele gesprek over niets anders.

Toch is het niet moeilijk om iets van het samenspel tussen algebra en meetkunde zichtbaar te maken. Laten we ons een eenvoudig meetkundig object voorstellen, bijvoorbeeld een kromme in het platte vlak. Een simpel voorbeeld is de cirkel C om de oorsprong met straal 1. Zoals bekend kunnen we C geven door een vergelijking, namelijk $x^2+y^2=1$. Nu is die relatie $x^2+y^2=1$ 'betekenisvol' zodra we kunnen praten over vermenigvuldiging, optelling en over het element 1. Anders gezegd: als x en y elementen zijn in een willekeurige ring (met eenheidselement) dan is het betekenisvol om te onderzoeken of $x^2+y^2=1$.
Bijvoorbeeld, als p een priemgetal is dan is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (rekenen modulo p) een ring (zelfs een lichaam) en we kunnen kijken naar de verzameling $C(\mathbb{F}_p)$ van alle paren $(x,y) \in \mathbb{F}_p \times \mathbb{F}_p$ die voldoen aan de relatie $x^2+y^2=1$. Je zou dit 'de eenheidscirkel over $\mathbb{F}_p$' kunnen noemen.

Wanneer ik het over de cirkel heb dan ziet men natuurlijk direct een plaatje voor zich van een cirkel in het platte vlak. Meetkunde dus! Als ik werk met andere getallensystemen, en bijvoorbeeld geïnteresseerd ben in verzamelingen zoals $C(\mathbb{F}_p)$, dan is het minder duidelijk of daar een plaatje bij hoort. Is $C(\mathbb{F}_p)$ een meetkundig object? Mijn antwoord is een volmondig *ja!* Onderzoek bijvoorbeeld eens voor verschillende priemgetallen p hoeveel elementen de verzameling $C(\mathbb{F}_p)$ heeft. Je zult een eenvoudig patroon vinden. Dit is heel simpel te verklaren door projectieve meetkunde te gebruiken; deze methode vereist vrijwel geen berekeningen.

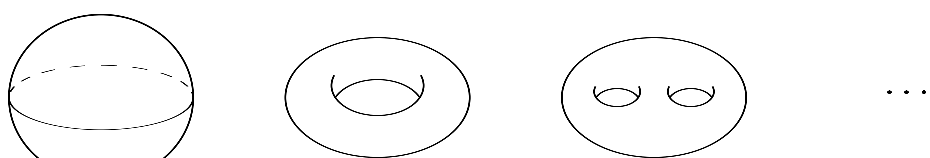
Een beroemd ander voorbeeld: voor een gegeven $n \geqslant 3$, wat zijn de paren *rationale* getallen (x, y) die voldoen aan $x^n + y^n = 1$? Fermat beweerde dat er alleen de "triviale" oplossingen zijn, waarbij $x = 0$ of $y = 0$, maar het duurde meer dan 350 jaar voordat Andrew Wiles (bouwend op resultaten van vele anderen) dit uiteindelijk bewees. Bij deze stelling denk je misschien niet direct aan meetkunde; toch wordt het bewijs gerekend tot het vakgebied van de aritmetische algebraïsche meetkunde.

Algebraïsche meetkunde is, ruw geschetst, het vakgebied waarin men probeert met (hoofdzakelijk) algebraïsche middelen meetkundige objecten te begrijpen. De meetkundige objecten kunnen 'leven' over de reële getallen, maar net zo gemakkelijk over heel andere getallensystemen (lees: ringen). Zoals hierboven al wordt gesuggereerd, is er een nauwe band met de getaltheorie, maar ook overlapt het vak met diverse andere disciplines, waaronder de analyse, topologie, logica en de mathematische fysica.

Al leven onze meetkundige objecten soms in werelden die je niet echt kunt visualiseren, veel van de technieken die we gebruiken zijn 'algebraïsche versies' van methoden uit de analyse en de differentiaalmeetkunde. Dus ook al werken we met getallensystemen zoals $\mathbb{F}_p$, toch kunnen we het hebben over raakruimten, differentiaalvormen of Taylorontwikkelingen. De kracht van het vak zit hem er in dat we kunnen werken met abstracte, algebraïsche begrippen (die bijvoorbeeld op getaltheoretische vragen toegepast kunnen worden) en dat we ons daarbij kunnen laten leiden door een meetkundige intuïtie.

Het allermooiste is het wanneer begrippen uit verschillende gebieden iets met elkaar te maken blijken te hebben. Ik geef een voorbeeld dat weer een getaltheoretisch tintje heeft. Neem een polynoom $f(x,y)$ in twee variabelen, waarvan de coëfficiënten gehele getallen zijn. We kunnen ons afvragen of er gehele getallen a en b zijn zo dat $f(a,b) = 0$, en zo ja hoeveel? Dit probleem is een voorbeeld van wat men een Diophantische vergelijking noemt. Ook kunnen we vragen hoeveel rationale getallen a en b met $f(a,b) = 0$ er zijn.

Door een meetkundige bril bekeken wordt door de vergelijking $f(x,y) = 0$ een kromme S in het platte vlak beschreven. Om onjuiste beweringen te vermijden zal ik aannemen dat deze kromme geen singulariteiten heeft. Nu kunnen we kijken naar de verzameling $S(\mathbb{C})$ bestaande uit alle paren $(x,y) \in \mathbb{C}^2$ waarvoor $f(x,y) = 0$. We kunnen proberen te begrijpen hoe deze verzameling er uit ziet als topologische ruimte. Het resultaat is dat $S(\mathbb{C})$, als topologische ruimte, er uit ziet als een van de volgende figuren, met daaruit een eindig aantal punten weggelaten.



$g = 0$ $\qquad$ $g = 1$ $\qquad$ $g = 2$ $\qquad$ $\cdots$

Het aantal 'gaten' in de figuur noemt met het *geslacht* $g(S)$ van S. Als het polynoom f graad d heeft dan is het geslacht van S gelijk aan $(d-1)(d-2)/2$. Bijvoorbeeld, nemen we $f(x,y) = x^2 + y^2 - 1$, dan is $d = 2$ en $g(S) = 0$; in dit geval ziet $S(\mathbb{C})$ er uit als een sfeer met daaruit 2 punten weggelaten.

Merk op dat de topologische informatie over $S(\mathbb{C})$ vrij grof is. Twee krommen kunnen heel verschillend zijn als meetkundige objecten (of, zoals we zeggen, als variëteiten) terwijl ze als topologische ruimten 'hetzelfde' zijn. Desondanks blijkt de topologische informatie over $S(\mathbb{C})$ een relatie te hebben met de getaltheoretische vraag naar rationale getallen a en b met $f(a,b) = 0$. Er zijn drie gevallen te onderscheiden:

(1) Als $g(S) = 0$ dan zijn er ofwel helemaal geen $(a,b) \in \mathbb{Q}^2$ met $f(a,b) = 0$, ofwel er zijn oneindig veel zulke paren. Bovendien

is er een methode om te beslissen welk van de twee mogelijkheden optreedt. Het aardige is dat dat gaat door te onderzoeken of, gegeven een natuurlijk getal n, de vergelijking $f(x, y) = 0$ oplossingen heeft met $(x, y) \in (\mathbb{Z}/n\mathbb{Z})^2$. Omdat $\mathbb{Z}/n\mathbb{Z}$ eindig is, is deze vraag (in principe) te beantwoorden door alle mogelijkheden voor x en y na te gaan.

(2) Als $g(S) = 1$ dan is alles mogelijk: de verzameling van alle $(a, b) \in \mathbb{Q}^2$ met $f(a, b) = 0$ kan leeg zijn, of eindig maar niet leeg, of oneindig. Dit geval betreft de zogenaamde *elliptische krommen*. Deze krommen hebben heel bijzondere eigenschappen en staan al decennia lang volop in de belangstelling. Het werk van Wiles speelt zich af in dit domein.

(3) Als $g(S) \geqslant 2$ dan zegt een stelling van Faltings dat er altijd maar eindig veel paren $(a, b) \in \mathbb{Q}^2$ zijn met $f(a, b) = 0$. Faltings bewees deze stelling, die bekend stond als het Mordell-vermoeden, samen met twee andere belangrijke stellingen in 1983, toen hij 29 jaar oud was. Hij werd er op slag beroemd door en ontving voor dit werk een Fieldsmedaille.

We zien nu ook waarom, in het Fermatprobleem, de vergelijking $x^2 + y^2 = 1$ (die oneindig veel 'rationale' oplossingen heeft) zich heel anders gedraagt dan de vergelijking $x^n + y^n = 1$ voor $n \geqslant 3$!

Ach, het is zo'n prachtig vak, en er is veel meer over te vertellen dan in een paar pagina's kan. En dan heb ik het nog niet eens gehad over de concrete toepassingen.

Ben Moonen
bmoonen@science.uva.nl