Wat te bewijzen is (42)

Rubriek

Kort na het verschijnen van nummer 40 van deze rubriek werd ik via de elektronische post op aimabele wijze door Martinus van Hoorn en Hans Klein geattendeerd op een fout. Het betrof dit fragment:

> Terug naar de diophantische vergelijking:
>
> $$a^2 - ab + b^2 = c^2 \qquad (*)$$
>
> Daarvan ken ik nu oneindig veel oplossingen:
>
> $$a = 2mn - n^2 \quad , \quad b = m^2 - n^2 \quad , \quad c = m^2 - mn + n^2$$
>
> met m, n natuurlijke getallen. Voor wie het niet vertrouwt, ligt hier een mooie algebra-oefening: substitueer deze vormen voor a, b en c en werk uit.
>
> Andere geheeltallige oplossingen dan die beschreven worden door bovenstaande formule, zijn er niet.

Het venijn zit hem in de laatste uitspraak. Martinus en Hans merkten terecht op dat behalve $(a, b, c) = (5, 8, 7)$ ook $(3, 8, 7)$ voldoet aan de vergelijking (*) terwijl dit drietal niet geproduceerd wordt door bovengenoemde formules. In feite is het zo dat bij iedere geheeltallige oplossing (a, b, c) met $a < b$ van (*) ook het trio $(b - a, b, c)$ een oplossing is.
Dat wordt direct duidelijk als (*) herschreven wordt als:

$$a(b - a) = b^2 - c^2$$

Er is dus een tweede tabel van – zeg 'complementaire' – oplossingen te maken die wordt gegenereerd door

$$a = m^2 - 2mn \quad , \quad b = m^2 - n^2 \quad , \quad c = m^2 - mn + n^2$$

Substitutie van $m = 3$, $n = 1$ geeft dan $(a, b, c) = (3, 8, 7)$. De fout is minder ernstig dan zij op het eerste gezicht lijkt. Als ik in de bovenste parametervoorstelling voor (m, n) het paar $(5, 1)$ invul, komt er $(a, b, c) = (9, 24, 21)$ en dit trio is evenredig met $(3, 8, 7)$. Doe ik dit in de tweede formule, dan komt er $(a, b, c) = (15, 24, 21)$ en dat is weer evenredig met $(5, 8, 7)$.
Er kan wel degelijk worden volstaan met één parametervoorstelling, maar die moet dan niet als gelijkheid, maar als evenredigheid van tripels worden gezien en de laatste zin uit bovengenoemd fragment zou bijvoorbeeld zo kunnen worden verbeterd: *geheeltallige oplossingen die niet evenredig zijn met de door de formule beschreven exemplaren, zijn er niet.*

Terugdenkend moet ik bekennen dat ik opkomende lichte argwaan bij het opschrijven van de gewraakte zin uit het fragment destijds heb weggewuifd met de gedachte aan de beroemde formule

$$a = m^2 - n^2 \quad , \quad b = 2mn \quad , \quad c = m^2 + n^2$$

die de zogenaamde Pythagorese drietallen voortbrengt. Daarom ga ik daar nu eerst even op in.

Pythagorese drietallen

Het kleitablet Plimpton 322 (gedateerd zo'n 1800 v.Chr.) wordt wel eens beschouwd als de grootste prestatie van de Babylonische wiskunde. Het bevat vijftien geheeltallige oplossingen van de vergelijking $a^2 + b^2 = c^2$ die, op een enkele na, indrukwekkend groot zijn.
Wat bijvoorbeeld te denken van:

$$4961^2 + 6480^2 = 8161^2 \ ?$$

Is het niet buitengewoon onwaarschijnlijk dat dit drietal tevoorschijn gekomen is na slim proberen? De deskundigen zijn het er wel over eens dat de Babyloniërs over een algoritme beschikten om zulke drietallen te vinden, zoiets als de formules onderaan in de vorige kolom.
Substitutie van $m = 81$ en $n = 40$ in die formules levert inderdaad het drietal (4961, 6480, 8161) op.
Die formules kunnen worden afgeleid via de methode: 'maak een rationale parametervoorstelling van de cirkel $x^2 + y^2 = 1$ met hulp van de draaiende lijn $y = tx - 1$ en stel vervolgens $t = m/n$ met m, n geheel.' Zo kunnen de Babyloniërs echter onmogelijk hebben gehandeld.
Hoe dan wèl?
We weten dat zij beschikten over 'inversentabellen' (van getallen met hun omgekeerde in het zestigtallig stelsel).
Als we $a^2 + b^2 = c^2$ herschrijven als

$$\frac{c+a}{b} \times \frac{c-a}{b} = 1$$

geeft dat een indicatie voor een mogelijke rekenwijze.
Stel bijvoorbeeld:

$$\frac{c+a}{b} = \frac{81}{40} \quad \text{en} \quad \frac{c-a}{b} = \frac{40}{81}$$

Na respectievelijk optellen en aftrekken van deze twee breuken komt er

$$\frac{c}{b} = \frac{8161}{6480} \quad \text{en} \quad \frac{a}{b} = \frac{4961}{6480}$$

en dat verklaart de vondst (4961, 6480, 8161).

Generalisatie van het voorbeeld levert op:

$$\frac{c+a}{b} = \frac{m}{n} \quad \text{en} \quad \frac{c-a}{b} = \frac{n}{m}$$

optellen en ***aftrekken***

$$\frac{c}{b} = \frac{m^2+n^2}{2mn} \quad \text{en} \quad \frac{a}{b} = \frac{m^2-n^2}{2mn}$$

Dus: a, b en c moeten zich wel verhouden als $m^2 - n^2$, $2mn$ en $m^2 + n^2$.
Zo leveren $m = 2$ en $n = 1$ de bekende 3-4-5-verhouding op; $m = 3$ en $n = 1$ doen dit trouwens ook, zij het in de gedaante (8, 6, 10). Een andere bekende van school, de rechthoekige driehoek (5, 12, 13), correspondeert met het paar $m = 3$, $n = 2$.

Primitieve Pythagorese drietallen

Om *primitieve* Pythagorese drietallen (a, b, c onderling ondeelbaar) te vinden, is het in de eerste plaats zaak om m en n onderling ondeelbaar te kiezen. Dat zo'n keuze niet garant staat voor een primitief drietal, laat het voorbeeld (m, n) = (3, 1) zien. Wèl zeker is het dat 2 de enige kandidaat is om gemeenschappelijke priemdeler te zijn van a, b en c.

Het bewijs is kort maar krachtig. Stel p is een priemdeler van zowel $a = m^2 - n^2$ als $b = 2mn$ (en dan automatisch ook van c). Uit $p \neq 2$ volgt dat p deler is van m óf van n, maar niet van beide. Dit is echter in strijd met p is deelbaar op $m^2 - n^2$.

Ik onderscheid nu twee gevallen.
(I) m is even en n is oneven (of omgekeerd).
(II) m en n zijn beide oneven.

In geval **I** is a het product van de oneven getallen $m + n$ en $m - n$ en daarom niet deelbaar door 2, dus (a, b, c) zal nu een primitief drietal zijn.

In geval **II** is a het product van twee even getallen, dus een viervoud terwijl b (het dubbele van het oneven getal mn) een viervoud + 2 is. Dus 2 is de ggd van a, b (en c). Na deling door 2 ontstaat er een primitief Pythagorees drietal (A, B, C). De vraag is nu: wordt dit drietal ook voortgebracht door onze parametervoorstelling?

Wel, kies $M = \frac{1}{2}(m+n)$ en $N = \frac{1}{2}(m-n)$ en er komt $A = \frac{1}{2}(m^2 - n^2) = 2MN$ en $B = mn = M^2 - N^2$.

Het antwoord is dus 'ja' en daarmee is aangetoond dat *alle* primitieve Pythagorese drietallen worden verkregen door in de parametervoorstelling voor m en n onderling ondeelbare getallen van verschillende pariteit te nemen.

Ter illustratie: zie onderstaande tabel van Pythagorese drietallen bij onderling ondeelbare m en n.

Categorie **I** Categorie **II**

(m,n)	***(a, b, c)***	***(m,n)***	***(a, b, c)***
(2,1)	(3, 4, 5)	(3,1)	(8, 6, 10)
(3,2)	(5, 12, 13)	(5,1)	(24, 20, 26
(4,1)	(15, 8, 7)	(5,3)	(16, 30, 40)
(4,3)	(7, 24, 25)	(7,1)	(48,14, 50)
(5,2)	(21, 20, 29)	(7,3)	(40, 42, 58)
(5,4)	(9, 40, 41)	(7,5)	(24, 70, 74)
(6,1)	(35, 12, 37)	(9,1)	(80,18, 82)
(6,5)	(11, 60, 61)	(9,5)	(56, 90, 106)
(7,2)	(45, 28, 53)	(9,7)	(32, 126, 130)
(7,4)	(33, 56, 65)	(11,1)	(120, 22, 122)

Terug naar $a^2 - ab + b^2 = c^2$

In de tabel hieronder staan naast elkaar de geheeltallige oplossingen (a, b, c) voortgebracht door de parametervoorstellingen $a = 2mn - n^2$ links, $a = m^2 - 2mn$ rechts, $b = m^2 - n^2$ en $c = m^2 - mn + n^2$ waarbij voor m en n onderling ondeelbare getallen zijn genomen met bovendien $m > 2n$.

(m,n)	***(a, b, c)***	***(m,n)***	***(a, b, c)***
(3, 1)	(5, 8, 7)	(3, 1)	(3, 8, 7)
(4, 1)	(7, 15, 13)	(4, 1)	(8, 15, 13)
(5, 1)	(9, 24, 21)	(5, 1)	(15, 24, 21)
(5, 2)	(16, 21, 19)	(5, 2)	(5, 21, 19)
(6,1)	(11, 35, 31)	(6,1)	(24, 35, 31)
(7, 1)	(13, 48, 43)	(7, 1)	(35, 48, 43)
(7, 2)	(24, 45, 39)	(7, 2)	(21, 45, 39)
(7, 3)	(33, 40, 37)	(7, 3)	(7, 40, 37)
(8,1)	(15, 63, 57)	(8,1)	(48, 63, 57)
(8,3)	(39, 55, 49)	(8,3)	(16, 55, 49)

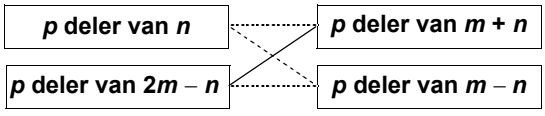
De voorwaarde $m > 2n$ zorgt er in de linkerhelft van de tabel voor dat er geen doublures optreden door verwisseling van de uitkomsten van a en b en in de rechterhelft dat er geen negatieve uitkomsten voor a optreden.

Evenmin als bij de Pythagorese drietallen staat de onderlinge ondeelbaarheid van m en n garant voor het primitief zijn van het tripel (a, b, c). In een e-mail merkte Hans Klein op dat a, b en c drievouden zijn als de som $m + n$ een drievoud is. In de tabel wordt dat bevestigd in de grijs gemaakte regels. De waarheid volgt uit de twee identiteiten: $2mn - n^2 = 3mn - n(m + n)$ en $m^2 - n^2 = (m + n)(m - n)$.

Omgekeerd: als m en n onderling ondeelbaar zijn en als a en b beide deelbaar zijn door het priemgetal p, dan moet $p = 3$ en $m + n$ een drievoud zijn.

Bewijs: $a = n(2m - n)$ en $b = (m + n)(m - n)$.

Uit de onderlinge ondeelbaarheid van n en m volgt eenvoudig de onderlinge ondeelbaarheid van n en $2m - n$ en ook van $m + n$ en $m - n$. Stel nu dat p deelbaar is op zowel a als b. Er zijn dan precies vier combinaties mogelijk, waarvan er drie tot tegenspraak leiden.



De beide combinaties met 'p *is* deler van n' leiden tot 'p is deler van zowel m als n', hetgeen was uitgesloten.

Uit p is deler van $2m - n$ en van $m - n$ volgt dat p een deler is van $(2m - n) - (m - n) = m$ en vervolgens ook van n, opnieuw tegenspraak dus.

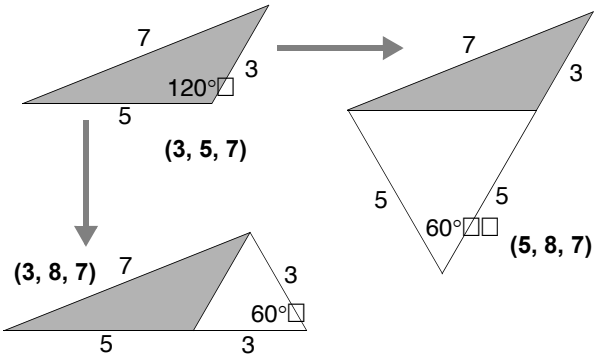
Uit p is deler van $2m - n$ en van $m + n$ volgt dat p een deler

is van $(2m - n) + (m + n) = 3m$ (&). In samenhang met p is deelbaar op $m + n$ leidt dit dan tot $p = 3$.
De conclusie is nu: *als $m + n$ niet deelbaar is door 3, dan is (a, b, c) een primitief tripel.*

Zijn m en n onderling ondeelbaar en is $m + n$ wèl deelbaar door 3, dan is 3 de ggd van a en b (en c).
Immers in dat geval is n zeker geen drievoud, evenmin als m en $m - n$. Is nu $m + n$ een negenvoud, dan is $2m - n$ weliswaar een drievoud, maar geen negenvoud, op grond van de identiteit (&).
Laat (a, b, c) zo'n trio met ggd 3 zijn dat in de linkerhelft van de tabel staat. Deling van a, b en c door 3 resulteert in een primitief drietal (A, B, C) dat zeker in de rechterhelft van de tabel is te vinden!
Kies $M = \frac{1}{3}(2m - n)$ en $N = \frac{1}{3}(m - 2n)$
M en N zijn geheel en onderling ondeelbaar, want $2m - n$ en $m - 2n$ zijn beide drievoud, maar geen negenvoud.
Er geldt dan:

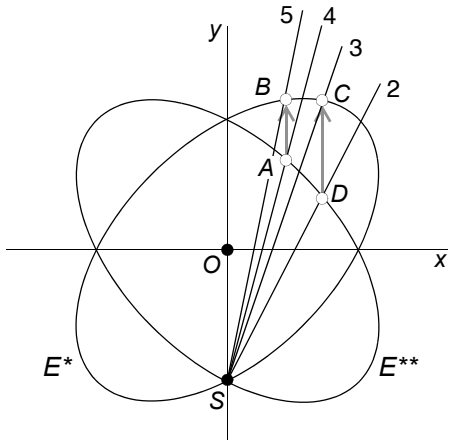
$$M(M - 2N) = \tfrac{1}{3}(2m - n) \cdot n = \tfrac{1}{3}a = A \qquad \text{en}$$
$$(M - N)(M + N) = \tfrac{1}{3}(m + n)(m - n) = \tfrac{1}{3}b = B$$

Geheelzijdige driehoeken
De oorsprong van de Pythagorese drietallen ligt in het zoeken naar geheelzijdige rechthoekige driehoeken. Net zo kan het oplossen van de diophantische vergelijking $a^2 - ab + b^2 = c^2$ (*) worden gezien als het vinden van geheelzijdige driehoeken met een hoek van 60°, denk maar aan de cosinusregel. En in samenhang daarmee kan de vergelijking $a^2 + ab + b^2 = c^2$ (**) worden beschouwd om geheelzijdige driehoeken met een hoek van 120° op te sporen. Er bestaat een innige relatie tussen deze beide laatste typen driehoeken



Neem bijvoorbeeld de driehoek met $a = 3$, $b = 5$, $c = 7$.
Omdat $3^2 + 3 \cdot 5 + 5^2 = 7^2$ geldt $\gamma = 120°$.
Door aanplakken van gelijkzijdige driehoeken aan de beide zijden om de hoek van 120° ontstaan twee driehoeken met een hoek van 60°.
Iedere oplossing van (**) brengt aldus twee complementaire oplossingen van (*) voort. De algebraïsche bevestiging hiervan is een aardig oefensommetje.

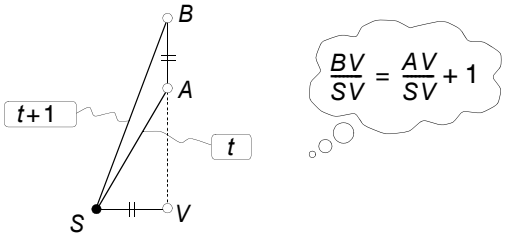
Afschuiving van de draaiende lijn
Alle geheelzijdige 120°- en 60°-driehoeken kunnen worden gevonden door lijn $y = tx - 1$ (t rationaal) te snijden met E^*: $x^2 - xy + y^2 = 1$ en E^{**}: $x^2 + xy + y^2 = 1$.



Het snijpunt van de lijn $t = 4$ met de ellips E^{**} is het punt A $(\frac{3}{7}, \frac{5}{7})$, corresponderend met de driehoek (3, 5, 7).
De snijpunten B $(\frac{3}{7}, \frac{8}{7})$ en C $(\frac{5}{7}, \frac{8}{7})$ van de ellips E^* met de lijnen $t = 5$ en $t = 3$ corresponderen met de driehoeken (3, 8, 7) en (5, 8, 7). Het punt D $(\frac{5}{7}, \frac{3}{7})$ is het spiegelbeeld van A ten opzichte van de as $x = y$, is het snijpunt van E^{**} met de lijn $t = 2$ en hoort bij het tripel (5, 3, 7).
De relatie tussen geheelzijdige 120°- en 60°-driehoeken zoals die hiervoor is geschetst, wordt nu gerepresenteerd door een afbeelding van de ellips E^{**} op E^*. Daarbij gebruik ik twee punten (A en D) om de 120°-driehoek voor te stellen. De formule bij die afbeelding is

$$(x, y) \to (x, x + y)$$

Dit is een bekende affiene afbeelding die *afschuiving* heet. Elk punt wordt daarbij in verticale richting verschoven, waarbij de lengte en de richting van de vector wordt bepaald door de x-coördinaat van het punt.
Deze afbeelding kan ook worden beschreven in termen van de richtingscoëfficiënt t van de lijn door S en heeft dan de voorstelling $t \to t + 1$.



Ik merk nog op dat complementaire oplossingen van de vergelijking (*) corresponderen met twee punten van E^* waarvan de verbindingskoorde horizontaal is (in bovenstaande figuur: B en C). Inderdaad, snijding van E^* met een geschikte lijn $y = r$ levert twee punten op waarvan de som van de x-coördinaten gelijk is aan r.

Martin Kindt, martin@fi.uu.nl