De prijs van een priemgetal

Als wiskundige in hart en nieren en begenadigd verteller weet prof.dr. Hendrik Lenstra als geen ander mensen te boeien voor zijn vak. Hij mocht dan ook niet ontbreken op de Science and Technology Summit Vliegende Hollanders 2008, die op 11 november plaatsvond in Amsterdam. Wij woonden voor u zijn presentatie bij. Een verslag van Betty Majoor.


Bron: www.nieuwsarchief.leidenuniv.nl

Zijn populariteit is Lenstra vooruitgesneld en het (te) kleine zaaltje zit afgeladen vol. Tussen al het techniekgeweld - minister Plasterk opende de dag samen met zijn virtuele alter ego - , heeft Lenstra genoeg aan een bord en een krijtje (oftewel whiteboard en marker). Met de souplesse van iemand die getallen van binnen en buiten kent, leidt Lenstra ons rond in priemgetalland. Hij doet daarbij een paar bijzondere getallen aan.

1728

Het grootst bekende priemgetal op dit moment is $2^{43112609} - 1$. Dit getal wordt een Mersenne-priemgetal genoemd, de algemene benaming voor priemgetallen die zijn opgebouwd als een tweemacht min één.
Als je dit getal zou uitschrijven heb je daar vele miljoenen cijfers voor nodig. Bij uitschrijven denken we meteen aan een getal in ons 10-tallig stelsel, maar je kunt het ook in een ander stelsel doen, zoals het 12-tallig, Amerikaanse stelsel met 12 inches in een foot. Een vierkante foot bestaat dan uit 144 vierkante inches en 1728 inches^3 maken samen een kubieke foot.

1729

Als we 1 optellen bij 1728 krijgen we 1729, een getal met een bijzondere glans. Lenstra legt uit waarom:

In 1913 ontvangt de beroemde Engelse wiskundige Godfrey Harold Hardy een brief van een jonge klerk uit India. Hierin legt de klerk aan Hardy een aantal berekeningen voor met het verzoek deze na te kijken en eventueel voor hem te publiceren. Na bestudering van de brief is er maar één conclusie mogelijk, de schrijver ervan, Srinivasa Ramanujan, is een wiskundig genie. Hardy haalt Ramanujan over om naar Cambridge te komen, waar hij zich volledig aan de wiskunde kan wijden.

Door het slechte klimaat en slechte voeding wordt Ramanujan ernstig ziek en hij belandt in het ziekenhuis. Als Hardy hem daar opzoekt ontspint zich het volgende gesprek: “De taxi waarmee ik ben gekomen”, vertelt Hardy, “had het nummer 1729, een nummer waar niets over te melden is.” “Integendeel”, spreekt Ramanujan hem tegen, “het is juist een heel interessant getal. Het is het kleinste getal dat je op twee manieren kunt uitdrukken als de som van twee verschillende derde machten. 1729 is gelijk aan de som van 1^3 en 12^3 en ook aan de som van 9^3 en 10^3.” Wiskundigen hebben dus alle reden om 1729 te koesteren als een bijzonder getal.

Priemfactorisatie

Is 1729 een priemgetal? We kunnen dit uitzoeken met priemfactorisatie, het ontbinden van een getal in priemgetallen. Lenstra maakt hierbij handig gebruik van de merkwaardige producten. Kent u ze nog?

1. $(a + b)^2 = a^2 + 2ab + b^2$
2. $(a - b)^2 = a^2 - 2ab + b^2$
3. $a^2-b^2 = (a+b)(a-b)$
4. $(a+b+c)^2 = a^2+b^2+c^2+2ab+2bc+2ca$
5. $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
6. $(a - b)^3 = a^3 - 3a^2b + 3ab^2 - b^3$
7. $a^3+b^3 = (a+b)(a^2-ab+b^2)$
8. $a^3-b^3 = (a-b)(a^2+ab+b^2)$
9. ...

Merkwaardige producten maken het hoofdrekenen een stuk makkelijker, bijvoorbeeld $98 \cdot 102$ kun je berekenen met $(100-2) \cdot (100+2) = 100^2 - 2^2 = 10000 - 4 = 9996$.

Met wat we al weten over het getal 1729, kunnen we het nu eenvoudig ontbinden. Gebruik van merkwaardig product nummer 7 geeft:

$$1729 = 12^3 + 1^3 = (12 + 1) \cdot (12^2 - 12 \cdot 1 + 1^2) = 13 \cdot 133$$
$$= 10^3 + 9^3 = (10 + 9) \cdot (10^2 - 10 \cdot 9 + 9^2) = 19 \cdot 91$$

Nu is het handig te weten dat *‘als in een product een van de getallen deelbaar is door 13, dit ook het geval is in een tweede product dat dezelfde uitkomst heeft’*. We kunnen nu eenvoudig concluderen dat $1729 = 7 \cdot 13 \cdot 19$ en in het bijzonder dat 1729 geen priemgetal is.

Lenstra formuleert twee stellingen:
1. *Elk getal dat zelf geen priemgetal is en groter dan 1, kun je opdelen in priemgetallen.*
2. *Het eindresultaat is altijd hetzelfde, ongeacht hoe je eraan komt.*

▶ *Lees verder op volgende pagina.*

Samen met het publiek (en een klein spiekbriefje) verkent hij vervolgens het 'priemgehalte' rondom het getal 1729:

1721 = priemgetal
1722 = $2 \cdot 3 \cdot 7 \cdot 41$
1723 = priemgetal
1724 = $2^2 \cdot 431$
1725 = $3 \cdot 5^2 \cdot 23$
1726 = $2 \cdot 863$
1727 = $11 \cdot 157$
1728 = $2^6 \cdot 3^3$
1729 = $7 \cdot 13 \cdot 19$
1730 = $2 \cdot 5 \cdot 173$

1730

Je kunt getallen ook op andere manieren uiteenrafelen, bijvoorbeeld met 'hulp' van Pierre de Fermat. Fermat is beroemd vanwege zijn stelling:
'$x^n + y^n = z^n$ voor $n>2$ heeft geen oplossing met natuurlijke getallen x, y en z ongelijk aan 0'.
Deze bedrieglijk eenvoudige bewering die hij in 1637 noteerde, heeft eeuwenlang grote wiskundegeesten beziggehouden. Pas in 1994 kreeg de Britse wiskundige Andrew Wiles het bewijs van deze stelling rond.

Hier echter, gebruikt Lenstra Fermat's stelling:
'*als er een priemgetal p is dat een 4-voud plus 3 is en dat tot een ONEVEN macht in de ontbinding in priemgetallenvan een getal n voorkomt, dan is n niet een som van twee kwadraten; als er niet zo'n p te vinden is, dan is n wel een som van twee kwadraten.*'

Bijvoorbeeld: $1728 = 3^3 \cdot 2^6$. Het priemgetal 3 komt dus 3 maal voor. Ook is 3 een 4-voud plus 3 (namelijk 0 + 3). Dus op grond van de stelling is 1728 niet de som van twee kwadraten. In de ontbinding $1727 = 11 \cdot 157$ komt 11 één maal voor terwijl het ook een 4-voud plus 3 is, dus ook 1727 is niet de som van twee kwadraten. Zo vallen bijna alle getallen in ons rijtje af als de som van twee kwadraten, immers:
p = 3 (of p = 7) voor n = 1722; p = 1723 voor n = 1723;
p = 431 voor n = 1724; p = 3 (of p = 23) voor n = 1725;
p = 863 voor n = 1726; p = 11 voor n = 1727;
p = 3 voor n = 1728; p = 7 (of 19) voor n = 1729.

De getallen die overblijven zijn 1721 en 1730. $1721 = 40^2 + 11^2$
De twee kwadraten die samen 1730 opleveren, vinden we als volgt:

$1730 = 10 \cdot 173$ en $10 = 3^2 + 1^2$ en $173 = 13^2 + 2^2$

Met behulp van merkwaardige producten - in dit geval nummer 1 en 2 – en wat gegoochel met sommen en verschillen en kruiselings vermenigvuldigen en optellen, rekent Lenstra voor dat $1730 = 41^2 + 7^2 = 37^2 + 19^2$. (Reken het nog eens rustig na.)

$10 = 3^2 + 1^2$ $173 = 132 + 22$	
$3 \cdot 13 = 39$ en $1 \cdot 2 = 2$	$13 \cdot 1 = 13$ en $3 \cdot 2 = 2$
$39 + 2 = 41$	$13 + 6 = 19$
$39 - 2 = 37$	$13 - 6 = 7$

1730 kan dus zelfs op twee verschillende manieren geschreven worden als som van twee kwadraten. Bovendien zijn dit kwadraten van priemgetallen. Uiteindelijk blijken priemgetallen de bouwstenen van alle getallen te zijn.

Spielerei?

Priemgetallen zijn fantastisch wiskundig speelgoed, maar kun je er ook iets nuttigs mee doen? Sinds een jaar of dertig is het antwoord "Ja". Priemgetallen spelen een belangrijke rol in het beveiligen van vertrouwelijke transacties (bijvoorbeeld bij banken). Hiervoor worden cryptografische systemen ontwikkeld waarin priemgetallen van 50 tot 500 cijfers worden gebruikt. Omdat er in de loop der eeuwen veel kennis over priemgetallen is opgedaan, zijn er nu geavanceerde methodes beschikbaar om priemgetallen te zoeken.

Het zoeken van een priemgetal heeft natuurlijk een prijs. Deze hangt samen met de grootte van het getal. Lenstra legt ons het volgende voor: "Hoe verhouden zich de volgende prijzen: de prijs van een priemgetal van 105 cijfers en de prijs van een priemgetal van 100 cijfers. Is de eerste ongeveer 1,05 keer zo duur als de tweede of scheelt het een factor 100.000?" In het eerste geval zou de prijs proportioneel zijn met het aantal cijfers, in het tweede geval met het getal zelf. Het publiek is 50/50 verdeeld. Een ruwe gok voor deze verhouding is volgens Lenstra 1,13. "Gelukkig maar", houdt hij ons voor, "want anders zouden de grotere priemgetallen onbetaalbaar zijn." Onbetaalbaar is zeker de wijze waarop Lenstra wiskunde tot leven brengt.

Op http://www.kennislink.nl/web/show?id=100896 staat een korte beschrijving van het leven van Srinivasa Aiyangar Ramanujan.

*Op Kennislink staat ook een artikel over Hendrik Lenstra zelf: http://www.kennislink.nl/web/show?id=204896 .
Het artikel bevat een aantal links naar onderwerpen waarmee Lenstra bijdraagt aan de popularisering van wiskunde.*

*Op Wiskunde online vindt u een animatie en oefenmateriaal over merkwaardige producten:
http://www.wiskundeonline.nl/lessen/merkw_producten.htm.*

Leestip (voor de Kerst?): Het laatste raadsel van Fermat, geschreven door Simon Singh, is een ware thriller over een wiskundige speurtocht van meer dan driehonderd jaar.