Spookgetallen

Jan van de Craats en Janina Müttel

leadtekst
In de serie *Open Problemen* deze keer drie beroemde onopgeloste raadsels. Je kunt er geen miljoen dollar mee winnen, maar wel onsterfelijke roem. Alledrie gaan ze over getallen die misschien helemaal niet bestaan. Spookgetallen dus. De eerste vraag luidt: *bestaat er een zesde Fermat-priemgetal?* De tweede: *bestaat er een oneven volmaakt getal?* En de derde: *bestaat er een even getal groter dan twee dat niet de som is van twee priemgetallen?* Al die vragen kun je in verband brengen met de grote wiskundige Euler: hij heeft bij alledrie een rol gespeeld. Maar sindsdien zijn we op dit gebied nog niet zo veel wijzer geworden. Jan van de Craats en Janina Müttel vertellen er meer over.

Fermatgetallen

Toen de Zwitserse wiskundige Leonhard Euler (1707-1783) in 1727 als twintigjarige in dienst trad van de Academie van Sint Petersburg trof hij daar een oudere Duitse collega aan, Christian Goldbach (1690-1764), met wie hij al snel bevriend raakte. Goldbach vertrok korte tijd later naar Moskou maar ze bleven geregeld brieven wisselen, vaak over wiskundige onderwerpen. Goldbach was geïnteresseerd in getallentheorie en hij wist Euler in zijn enthousiasme mee te slepen. In 1729 schreef hij: *Kent u de opmerking in het werk van Fermat dat alle getallen* $2^{2^n}+1$ *priemgetallen zijn? Hij schrijft dat hij het niet kan bewijzen, en voor zover ik weet heeft ook niemand anders een bewijs kunnen vinden.* Euler liet het probleem een tijdje liggen, maar begon er toen toch aan te werken. Fermat had al opgemerkt dat de getallen $F_n = 2^{2^n}+1$ voor $n = 0, 1, 2, 3, 4$ priemgetallen zijn: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ en $F_4 = 65537$, vandaar zijn vermoeden. Maar $F_5 = 4\,294\,967\,297$ ging zijn krachten te boven. Euler liet zich niet afschrikken en begon slim te rekenen, overigens met middelen die Fermat zelf had aangedragen. Hij kwam tot het verrassende resultaat dat F_5 *geen* priemgetal is omdat het deelbaar is door 641. Controleren is makkelijk, maar het vinden van zo'n ontbinding is andere koek, zeker als je geen rekenmachine hebt. Hoe dan ook, dit vermoeden van Fermat bleek dus niet waar te zijn – een van de zeldzame keren dat Fermat een vermoeden uitsprak dat onjuist is gebleken!

Waar komt trouwens die vreemde vorm $2^{2^n} + 1$ vandaan? Waarom niet gewoon $2^m + 1$ genomen? Wel, het is eenvoudig om te bewijzen dat $2^m + 1$ alleen maar een priemgetal kan zijn als m van de vorm $m = 2^n$ is. Algemeen gesproken is $a^q + 1$ namelijk nooit een priemgetal als q oneven is en groter is dan 1, want

$$a^q + 1 = (a+1)(a^{q-1} - a^{q-2} + a^{q-3} - \cdots - a^1 + 1)$$

Zo is bijvoorbeeld $18^5 + 1 = (18+1)(18^4 - 18^3 + 18^2 - 18 + 1)$, oftewel $1889569 = 19 \times 99451$. Zou nu $2^m + 1$ een priemgetal zijn, en zou m een oneven deler $q > 1$ hebben, dus $m = kq$ met k geheel, dan zou $2^m + 1 = 2^{kq} + 1 = (2^k)^q + 1 = a^q + 1$ met $a = 2^k$. Maar we hebben net gezien dat $a^q + 1$ geen priemgetal is – tegenspraak. Het getal m kan dus alleen maar priemfactoren 2 hebben, met andere woorden, het is een gehele macht van 2.

Hoe zit het met $F_6 = 18\,446\,744\,073\,709\,551\,617$? Daar lijkt zonder computer geen beginnen aan. Toch lukte het Landry en Le Lasseur in 1880 een volledige ontbinding te vinden: $F_6 = 274\,177 \times 67\,280\,421\,310\,721$. Ook van F_7, een getal van 39 cijfers, F_8 (78 cijfers), F_9 (155 cijfers) en F_{11} (617 cijfers) zijn inmiddels volledige ontbindingen gevonden. Geen van alle zijn het priemgetallen. Ook F_{10} is geen priemgetal, maar daarvan is alleen maar bekend dat het deelbaar is door 455 925 777 en 6 487 031 809. Van de resterende factor, een getal van 291 cijfers, weten we dat het geen priemgetal is, maar we kennen de ontbinding ervan niet. Van nog veel meer Fermatgetallen is bewezen dat ze geen priemgetallen zijn. In feite is er nog steeds geen enkele grotere priem dan F_4 bekend. Het kleinste Fermatgetal waarvan we niet weten of het priem is, is F_{22}, een getal van 1 262 612 cijfers.

Volmaakte getallen volgens Euclides

Reeds de oude Grieken waren gefascineerd door *volmaakte getallen*, dat wil zeggen natuurlijke getallen N die gelijk zijn aan de som van hun delers, waarbij ze N zelf niet als deler meetelden. Doe je dat wel, dan is de som van de delers dus $2N$. Het kleinste volmaakte getal is 6, want de delers van 6 zijn 1, 2, 3 en 6 met som $12 = 2 \times 6$. Het volgende volmaakte getal is 28, want de delers daarvan zijn 1, 2, 4, 7, 14 en 28. Ook 496 en 8128 zijn volmaakte getallen, en er zijn er nog veel meer.

De Griekse wiskundige Euclides (ca. 300 voor Christus) gaf een recept om volmaakte getallen te vinden. Hij bewees namelijk: als $2^m - 1$ een priemgetal is, dan is $2^{m-1}(2^m - 1)$ een volmaakt getal. Neem bijvoorbeeld $m = 2$, dan is $2^m - 1 = 3$ een priemgetal, en $2^{m-1}(2^m - 1) = 3 \times 2 = 6$ is inderdaad volmaakt. Voor $m = 3$ krijg je $2^3 - 1 = 7$ en $2^2(2^3 - 1) = 28$. $m = 5$ geeft 496 en $m = 7$ geeft 8128.

Het bewijs van Euclides is niet moeilijk. We illustreren het aan de hand van een voorbeeld. Een algemeen bewijs kun je dan zelf wel verzinnen. Neem $m = 7$ en noem $p = 2^m - 1 = 2^7 - 1 = 127$. Inderdaad is $p = 127$ een priemgetal, en dus zou $V = 2^6 \times 127 = 8128$ een volmaakt getal moeten zijn. Schrijf alle delers van V (inclusief V zelf) op. In zo'n deler kunnen alleen maar priemfactoren 2 (hoogstens zes) en p (hoogstens één) zitten, dus de delers zijn: 1, 2, 2^2, 2^3, 2^4, 2^5, 2^6 en p, $2p$, 2^2p, 2^3p, 2^4p, 2^5p, $2^6p(= V)$. Bedenk nu dat $1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 = 2^7 - 1$ en dat $2^7 - 1 = p$. De som van alle delers is dus $p + (p \times p) = p(1 + p) = (2^m - 1)2^m = 2 \times 2^{m-1}(2^m - 1) = 2V$. Conclusie: $V = 8128$ is inderdaad een volmaakt getal.

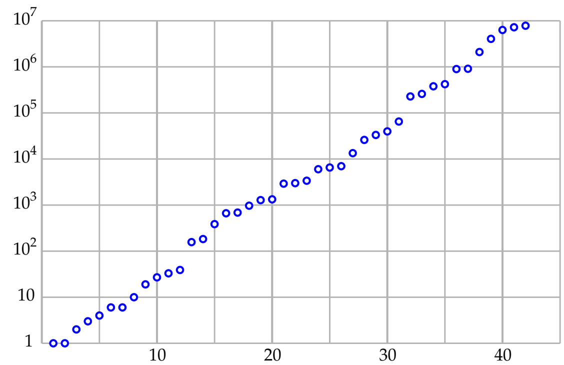
Mersenne-priemgetallen

Priemgetallen van de vorm $2^m - 1$ heten *Mersenne-priemgetallen* naar de Franse monnik en amateurwiskundige *Marin Mersenne* (1588-1648). Elk Mersenne-priemgetal levert volgens Euclides dus een volmaakt getal op. Maar hoeveel Mersenne-priemgetallen zijn er? We weten het niet. Op het moment dat we dit schrijven, zijn er 42 bekend. De grootste is $2^{25\,964\,951} - 1$, een getal van 7 816 230 cijfers, gevonden op 18 februari 2005 door Martin Novak uit Duitsland. Op het internet kun je meedoen met de jacht naar Mersenne-priemgetallen. Daar kun je ook vinden of dit record inmiddels al weer gebroken is (zie `http://www.mersenne.org/prime.htm`).

Er zijn dus heel wat meer Mersenne-priemgetallen dan Fermat-priemgetallen bekend. Bij de Fermat-priemgetallen zou het vinden van één nieuwe Fermat-priem al een sensatie betekenen. Maar bijna elk jaar wordt er wel een nieuwe Mersenne-priem ontdekt, en dat komt dan ook steeds weer in de krant (en in Pythagoras). Toch is 42 nog niet zo'n groot getal. Wiskundigen willen natuurlijk meer weten. Komt er ooit een eind aan die rij? Er zijn redenen om aan te nemen dat dit niet zo is, maar een bewijs ontbreekt. Dat is dus een open probleem:

Open probleem: Zijn er oneindig veel Mersenne-priemgetallen?

Dat er inderdaad oneindig veel Mersenne-priemgetallen bestaan, wordt aannemelijk gemaakt door figuur 1 waarin het aantal cijfers van het n-de Mersenne-priemgetal uitgezet is tegen n. De gegevens hiervoor hebben we van het internet geplukt. De verticale schaal is zelf ook logaritmisch, zoals je aan de schaalverdeling kunt zien. Maar je ziet ook dat de 42 punten vrijwel op een rechte lijn lijken te liggen. Er zijn wel wat argumenten te bedenken waarom dat ook zo zou moeten zijn, maar een bewijs is er nog niet!



Figuur 1: De logaritme van het aantal cijfers van het n-de Mersennepriemgetal, uitgezet tegen n.

Oneven volmaakte getallen

Hebben we met het recept van Euclides ook alle volmaakte getallen beschreven? We weten het niet. In zekere zin weten we het maar voor de helft. Om dat uit te leggen, merken we eerst op dat $2^{m-1}(2^m - 1)$ even is als $m \geq 2$. Alle volmaakte getallen die volgens het recept van Euclides uit Mersennepriemgetallen zijn gemaakt, zijn dus even. Ongeveer tweeduizend jaar na Euclides bewees Euler dat het omgekeerde ook waar is: elk *even* volmaakt getal is van deze vorm. Een bewijs hiervan vind je in een apart kader. Daarmee is dus bewezen dat bij elk Mersennepriemgetal een even volmaakt getal hoort en omgekeerd. Maar dat laat nog één vraag onbeantwoord: is elk volmaakt getal even?

Open probleem: Bestaan er oneven volmaakte getallen?

Misschien bestaan ze niet. Dan zijn het dus spookgetallen. Maar toch is er wel het een en ander over zulke spoken bewezen. Als er een oneven volmaakt getal N bestaat, dan moet N de volgende eigenschappen hebben.
1. N kan niet deelbaar zijn door 105.
2. N bevat minstens 47 priemfactoren (die overigens niet verschillend hoeven te zijn).
3. N bevat minstens 8 verschillende priemfactoren.
4. N is een getal van minstens 300 cijfers.
5. N heeft een priemfactor die groter is dan 10^{20}.
6. De op één na grootste priemfactor van N is groter dan 1000.
Maak dus je borst maar nat als je op zoek gaat naar zo'n spookgetal!

Het vermoeden van Goldbach

Op 7 juni 1742 schreef Goldbach een brief aan Euler met daarin een zin die in modernere taal geformuleerd neerkomt op: *het lijkt erop dat elk geheel getal groter dan* 5 *geschreven kan worden als de som van drie priemgetallen* en hij vraagt Euler of deze weet of die uitspraak inderdaad in het algemeen geldig is. Hier is het begin van een lijstje dat Goldbach ongetwijfeld zelf ook gemaakt heeft om te controleren of het klopt:

$$\begin{aligned}
6 &= 2+2+2\\
7 &= 2+2+3\\
8 &= 2+3+3\\
9 &= 3+3+3\\
10 &= 2+3+5\\
11 &= 3+3+5\\
12 &= 2+3+7\\
\cdots &= \cdots
\end{aligned}$$

Je kunt het zelf net zo lang maken als je wilt. Of het door de computer laten controleren. We willen best wedden dat het je niet lukt een tegenvoorbeeld te vinden; zo dadelijk vertellen we waarom. Maar een weddenschap is geen bewijs. Hoe zit het? Is het echt waar?

Euler antwoordde dat hij ook geen bewijs had, maar dat je het probleem ook op de volgende manier kunt formuleren: *elk even getal groter dan* 2 *is de som van twee priemgetallen.* Daar hoort ook een lijstje bij. Dat begint zo:

$$\begin{aligned}
4 &= 2+2\\
6 &= 3+3\\
8 &= 3+5\\
10 &= 3+7\\
12 &= 5+7\\
14 &= 7+7\\
16 &= 5+11\\
\cdots &= \cdots
\end{aligned}$$

Eulers formulering lijkt wat overzichtelijker. Het is echter nog steeds een open probleem. Als het *niet* waar is, zou er dus een even getal zijn dat *niet* te schrijven is als som van twee priemgetallen. Zou er zo'n spookgetal bestaan?

Open probleem: Bestaat er een even getal groter dan 2 dat niet te schrijven is als som van twee priemgetallen?

De twee versies zijn equivalent

We geven nu Eulers bewijs dat die twee formuleringen equivalent zijn. Neem eerst aan dat Goldbachs bewering waar is dat elk getal groter dan 5 de som is van drie priemgetallen, en stel dat N een even getal groter dan 2 is. Dan is $N + 2 = p_1 + p_2 + p_3$ voor zekere priemgetallen p_1, p_2 en p_3 met $p_1 \leq p_2 \leq p_3$. Die kunnen niet allemaal oneven zijn, want dan zou $N + 2$ ook oneven zijn en dat is niet zo. Maar 2 is het enige even priemgetal, dus $p_1 = 2$ en $N = p_2 + p_3$.

Omgekeerd, als de formulering van Euler waar is, en als N een willekeurig getal groter dan 5 is, dan zijn er twee mogelijkheden.
1. N is even. Dan is ook $N - 2$ even en groter dan 2, en dus de som van twee priemgetallen: $N - 2 = p_1 + p_2$. Dit betekent dat $N = 2 + p_1 + p_2$ zoals bewezen moest worden.
2. N is oneven. Dan is $N - 3$ even en groter dan 2, en dus de som van twee priemgetallen $N - 3 = p_1 + p_2$, dat wil zeggen $N = 3 + p_1 + p_2$.

Oom Petros

Het is een vreemde draai van de geschiedenis dat Eulers formulering, en niet die van Goldbach, bekend is geworden als het *vermoeden van Goldbach*. Het luidt dus: *elk even getal groter dan* 2 *is de som van twee priemgetallen.* Je kunt het direct aan iedereen uitleggen. Er is zelfs een spannende en ontroerende roman over geschreven: *Oom Petros en het vermoeden van Goldbach* van de Griekse auteur Apostolos Doxiadis (Nederlandse vertaling: De Bezige Bij, 2000, ISBN 90-234-3953-8). Van harte aanbevolen!

Maar hoe ver zijn we inmiddels gevorderd met de oplossing? Dat valt wat tegen, of mee, het is maar hoe je het bekijkt. We noemen hier een paar resultaten. Het vermoeden is geverifieerd voor alle even getallen kleiner dan 4×10^{14} (zie `http://primes.utm.edu/notes/conjectures/`). Het beste resultaat dat in de buurt komt van een algemeen bewijs, stamt uit 1978, toen de Chinese wiskundige Chen-Jing Run bewees dat er een groot (maar onbekend) getal N_0 bestaat zo, dat elk even getal groter dan N_0 geschreven kan worden als $p + m$ waarbij p een priemgetal, en m óf een priemgetal, óf het product van twee priemgetallen is.

We zijn lang niet volledig in onze opsomming. Op het internet en in de literatuur kun je nog veel meer over het vermoeden van Goldbach vinden. Maar wat we eigenlijk willen, is gewoon een bewijs of een tegenvoorbeeld. Kortom, we willen weten of er een even getal bestaat dat *niet* de som is van twee priemgetallen. Zou er zo'n *Goldbach-spookgetal* bestaan?

IN EEN APART KADER PLAATSEN:

Stelling (Euler): Bij elk even volmaakt getal V is er een Mersenne-priemgetal $2^k - 1$ zo, dat $V = 2^{k-1}(2^k - 1)$.

Bewijs: Omdat V even is, kun je V schrijven als $V = 2^{k-1}m$ met $k \geq 2$ en m oneven. De som van alle delers van een willekeurig getal N noemen we $\sigma(N)$, daarbij tellen we N zelf ook als deler mee. Voor het volmaakte getal V geldt dus $\sigma(V) = 2V = 2^k m$.

Omdat m oneven is, hebben 2^{k-1} en m geen delers gemeen. Elke deler van V is dus het product van een deler van 2^{k-1} en een deler van m. Dat betekent dat $\sigma(V) = \sigma(2^{k-1})\sigma(m)$. De delers van 2^{k-1} zijn 1, 2, ..., 2^{k-1} dus $\sigma(2^{k-1}) = 1 + 2 + \cdots + 2^{k-1} = 2^k - 1$. Combinatie van deze resultaten geeft

$$2^k m = (2^k - 1)\sigma(m)$$

Schrijf het linkerlid als $(2^k - 1)m + m$. De getallen $2^k - 1$ en 2^k verschillen 1, en dus hebben ze geen delers gemeen. Dat betekent dat m deelbaar moet zijn door $2^k - 1$, oftewel $m = n(2^k - 1)$ voor zekere deler n van m. We kunnen de bovenstaande vergelijking dus deler door $2^k - 1$, met als resultaat $m + n = \sigma(m)$. Behalve m en n zijn er blijkbaar geen andere delers van m. Dat kan alleen als m een priemgetal is, en dan is n dus 1. Hiermee is bewezen dat $m = 2^k - 1$ inderdaad een Mersenne-priemgetal is.