Pythagoras-redacteur Paul Levrie schreef samen met zijn collega Rudi Penne het boek *De pracht van priemgetallen*, dat in het begin van dit jaar verscheen en waarover we al schreven in het aprilnummer. Ondertussen is het boek bekroond met een prijs van de Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten. In dit artikel bespreken de twee auteurs een paar priemfeiten en priemvragen. Over Mersennepriemgetallen, Fermatpriemgetallen, priemtweelingen, priempaarden en meer.

■ door Paul Levrie en Rudi Penne (Faculteit Toegepaste Ingenieurswetenschappen, Universiteit Antwerpen)

PRIEMGETALLEN: VEEL VRAGEN, WEINIG ANTWOORDEN

Is 1234567 een priemgetal? Stel je voor dat je in een tijd leeft dat er geen computers zijn (en ook geen rekentoestellen), dan is dit een knap lastig probleem. Met computers gaat het natuurlijk iets vlotter, maar ook dan blijft de vraag: hoe begin je er aan, en waarom is dit zoveel moeilijker dan bijvoorbeeld de vraag: is 1234567 deelbaar door 2?

Priemgetallen zijn getallen die enkel deelbaar zijn door 1 en door zichzelf. Uitgezonderd 1. De rij van de priemgetallen begint dus zo: 2, 3, 5, 7, 11, 13, 17, 19, ... We kennen ze al meer dan 2000 jaar, maar ze blijven raadselachtig en geven hun geheimen slechts met mondjesmaat prijs. Wat we wel weten, is dat er oneindig veel van zijn, en dat kunnen we dankzij Euclides (rond 300 v.C.) eenvoudig bewijzen (zie het kader op pagina 22). Daarnaast zijn er heel wat onopgeloste problemen.

OPEN PROBLEMEN De wereld van de priemgetallen zit vol vragen (en vermoedens), en vaak beginnen die zo: zijn er oneindig veel ...

• *Zijn er oneindig veel Mersennepriemgetallen?*

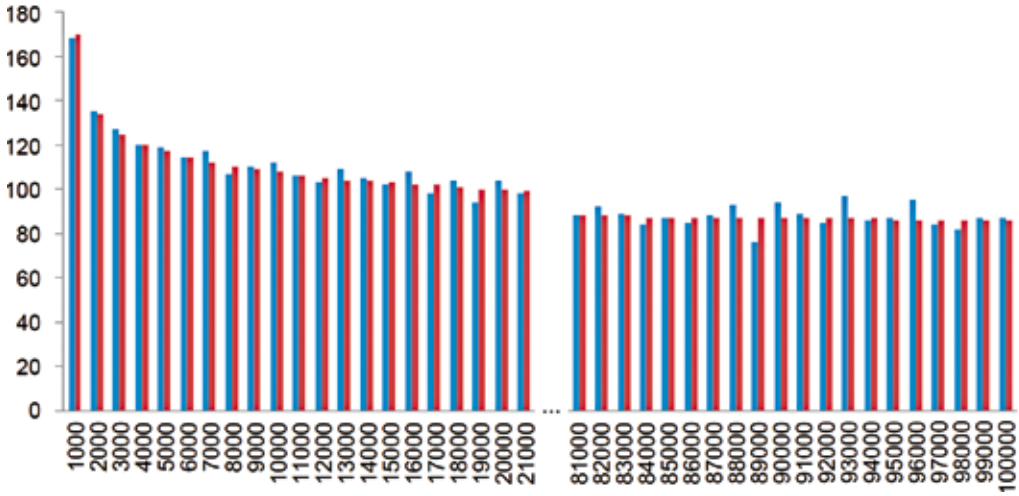
Een Mersennepriemgetal is een priemgetal van de vorm $2^n - 1$. Het is een eenvoudige oefening om te bewijzen dat n noodzakelijk een priemgetal moet zijn opdat $2^n - 1$ kans heeft om zelf priem te zijn (maar het is geen voldoende voorwaarde, getuige $2^{11} - 1 = 23 \times 89$). De vijf kleinste Mersennepriemgetallen zijn 3, 7, 31, 127 en 8191. Er is niemand die weet of er oneindig veel van zijn. Tot nog toe kennen we achtenveertig Mersennepriemgetallen, waarvan het grootste in januari 2013 ontdekt is, namelijk $2^{57.885.161} - 1$. Dit is meteen ook het grootst bekende priemgetal bij het verschijnen van dit nummer van *Pythagoras*. Dat is geen toeval, want voor Mersennegetallen – getallen van de vorm $2^p - 1$ (met p priem) – is het eenvoudiger om te testen of ze inderdaad priem zijn dan voor willekeurige kandidaten. Dat komt doordat we bij Mersennegetallen gebruik kunnen maken van de *Lucas-Lehmertest*, maar de details hiervan laten we weg.

• *Zijn er oneindig veel perfecte getallen?*

Een perfect of volmaakt getal is gelijk aan de som van zijn delers (zichzelf niet maar 1 wel meegerekend). Zo is 6 perfect, want $6 = 1 + 2 + 3$. Euclides wist al dat je perfecte getallen kon fabriceren via de formule $2^{p-1} \cdot (2^p - 1)$ met $2^p - 1$ een Mersennepriemgetal. Bijvoorbeeld, met $7 = 2^3 - 1$ maken we het volmaakte getal 28. Euler toonde aan dat bovendien ieder *even* perfect getal van deze vorm is. We vermoeden dat er geen oneven perfecte getallen bestaan, maar dit is nog niet bewezen. In dit geval is de vraag of er oneindig veel perfecte getallen bestaan een equivalente herformulering van de vraag of er oneindig veel Mersennepriemgetallen bestaan.

• *Zijn er oneindig veel Fermatpriemgetallen?*

Een Fermatpriemgetal is een priemgetal van de vorm $2^{2^n} + 1$. Er zijn er vijf bekend: 3, 5, 17, 257 en 65.537. Er is niemand die weet of er meer van dit soort getallen bestaan, maar men vermoedt dat er geen andere zijn dan deze vijf. Dit zou spijtig zijn, want voor ieder Fermatpriemgetal N bestaat er een meetkundige constructie met passer en liniaal om exact een regelmatige N-hoek te construeren. Zul-



Figuur 1 Blauw: het aantal priemgetallen tussen $i \cdot 1000$ en $(i + 1) \cdot 1000$.
Rood: een benadering van dit aantal, gebruikmakend van de zogeheten *priemgetallen-telfunctie*.

ke constructies bestaan ook als N een product van Fermatpriemgetallen is, eventueel vermenigvuldigd met een macht van 2, maar andere regelmatige veelhoeken kan je niet construeren met passer en liniaal.

• *Zijn er oneindig veel priemtweelingen?*

Een priemtweeling is een paar priemgetallen die 2 van elkaar verschillen, dus twee getallen p en $p + 2$, beide priem. Voorbeelden hiervan vind je bij kleine getallen bij de vleet, want voor kleine getallen is het niet moeilijk priem te zijn: 3 en 5, 11 en 13, 17 en 19, ... Er zijn er ook grote; de grootst bekende priemtweeling bij het verschijnen van deze *Pythagoras* is het paar $3.756.801.695.685 \cdot 2^{666.669} \pm 1$. Maar zijn er oneindig veel van?

Het is bekend dat hoe verder je gaat, hoe minder priemgetallen je tegenkomt. In figuur 1 geeft de hoogte van de blauwe staafjes het aantal priemgetallen tussen $i \cdot 1000$ en $(i + 1) \cdot 1000$. De hoogte van de rode staafjes geeft een benadering ervan met een formule die een logaritmische functie bevat en die al bekend was in het begin van de negentiende eeuw. Zoiets kom je wel vaker tegen bij de priemgetallen: er zijn formules waarmee je kan schatten met hoeveel ze zijn, maar je hebt geen formules waarmee je ze dan ook effectief kan vinden.

Met andere woorden, het exacte patroon van de priemgetallen blijft een mysterie, maar we hebben wel een redelijk goed idee van hun statistische spreiding. Hierdoor weten we dat voor grotere getallen het gemiddeld langer duurt alvorens een volgend priemgetal opduikt. Maar ze blijven wel verschijnen, al worden ze steeds zeldzamer en dus ook moeilijker te vinden, want – zoals we in het begin al opmerkten – er zijn oneindig veel priemgetallen.

De gemiddelde afstand tussen opeenvolgende priemgetallen mag dan wel groter worden, dit sluit niet uit dat we ook bij de grote getallen plots een dekselse priemtweeling tegenkomen. Maar uiteraard: naarmate je verder oprukt worden ook de priemtweelingen zeldzamer. En misschien sterven ze vanaf een bepaald moment uit, wie weet?

PRIEMPAARDEN Het priemtweelingenvermoeden zegt:

er zijn oneindig veel priemtweelingen.

Het is voor de eerste keer geformuleerd in 1849 door Alphonse de Polignac. Wat deze Franse wiskundige zei was een stuk ruimer:

elk even getal is op oneindig veel manieren te schrijven als verschil van twee (opeenvolgende) priemgetallen.

Als we voor het even getal het getal 2 kiezen, dan hebben we het priemtweelingenvermoeden.

Sinds de formulering van dit vermoeden proberen wiskundigen ijverig te bewijzen dat het inderdaad zo is. Op dit ogenblik is het priemtweelingenvermoeden echt een hot topic. Vorig jaar kwam er een doorbraak, we komen dichter en dichter bij de bevestiging, maar we zijn er nog (net) niet.

HET BEWIJS VAN EUCLIDES Euclides toonde al aan dat er oneindig veel priemgetallen zijn. Wij presenteren het bewijs op een net even andere manier, maar het komt in feite neer op Euclides' redenering. Stel dat er maar eindig veel priemgetallen zijn, we geven ze elk een kleur. En de veelvouden ervan krijgen dezelfde kleur. We doen het even voor de kleinste priemgetallen apart, maar je moet je voorstellen dat alles tegelijk gebeurt op één lijn, de lijn van de getallen 1, 2, 3, 4, ...:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

We merken op dat
(1) alle getallen (behalve het getal 1) één of meerdere kleuren hebben, want ofwel zijn ze priem, en dan hebben ze precies één kleur, ofwel zijn ze niet priem, en dan hebben ze de kleuren van al hun priemfactoren (neem bijvoorbeeld 30: het heeft de kleuren van 2, 3 en 5). Let op: Euclides steunde hierbij op de eigenschap dat ieder *samengesteld getal* (een niet-priemgetal groter dan 1) een priemgetal als deler heeft (dit had hij eerder aangetoond met een inductieve redenering).
(2) twee opeenvolgende getallen nooit dezelfde kleur kunnen hebben. Dat wordt snel duidelijk als je naar de figuur kijkt.
We veronderstelden dat er maar eindig veel priemgetallen zijn. Dit betekent dat we aan eindig veel kleuren genoeg hebben. Neem nu het product van alle priemgetallen en noem dat N. Dit getal krijgt dus ook alle kleuren mee:

En dan zijn we er. Want neem nu het getal $N + 1$: voor dit getal is er geen kleur meer over! Dit volgt uit (2), omdat N alle mogelijke kleuren heeft. Maar volgens (1) moet ook $N + 1$ een kleur hebben. We komen zo tot een tegenspraak. En onze veronderstelling dat er maar eindig veel priemgetallen zijn, is dus fout: ze zijn met oneindig veel.

Hoe dicht zijn we precies genaderd? Om dat duidelijk te maken spreken we af dat we twee priemgetallen die een verschil van d hebben, een priempaar-d of kortweg priempaard zullen noemen. Voor bepaalde waarden van d zijn er ook andere benamingen: voor $d = 2$ hebben we de priemtweelingen, voor $d = 4$ spreken we over priemneven, voor $d = 6$ over sexy priemgetallen. Het priemtweelingenvermoeden kunnen we nu zo schrijven:

er zijn oneindig veel priempaarden met $d = 2$.

De onbekende wiskundige Yitang Zhang bewees in 2013 het volgende: er zijn oneindig veel koppels priemgetallen die minder dan 70 miljoen uit elkaar liggen. Anders gezegd: er zijn oneindig veel intervallen met lengte 70 miljoen waarin (minstens) twee priemgetallen liggen. Je weet niet hoever die priemgetallen in die intervallen uit elkaar liggen, en toch kan je hieruit het volgende besluiten:

er is een $d \leq 70.000.000$ waarvoor geldt dat er oneindig veel priempaarden zijn.

Dat zie je als volgt. Als je al die intervallen van lengte 70 miljoen bekijkt, en je neemt er steeds twee priemgetallen uit, waarvan je de afstand opschrijft, dan krijg je een oneindig lange lijst met afstanden die allemaal kleiner zijn dan 70 miljoen. Omdat het om gehele getallen gaat, en omdat er maar eindig veel gehele getallen zijn kleiner dan 70 miljoen, zal er zeker een afstand tussen zitten die oneindig vaak voorkomt. Dat is onze d! (Als dat namelijk niet zo was, en elke afstand in de lijst maar

een eindig aantal keer voorkomt, dan kom je nooit aan een oneindig lange lijst.)

Sinds Zhang zijn bewijs voorstelde, is er nog enorme vooruitgang geboekt, via het Polymath8-project, een samenwerkingsverband tussen wiskundigen uit de hele wereld die samen (gebruikmakend van het internet als communicatiemiddel) zoeken naar verbeteringen van de bestaande methodes. In april 2014 hadden ze dit bereikt:

er is een $d \leq 246$ waarvoor geldt dat er oneindig veel priempaarden zijn.

Ondertussen is dit deel van het Polymath8-project stopgezet, dus het lijkt twijfelachtig dat de gebruikte methodes nog verder verfijnd kunnen worden om van de 246 een 2 te maken, waarmee het priemtweelingenvermoeden bewezen zou zijn.

TOCH NOG EEN ANTWOORD We willen dit artikel vol vraagtekens dan toch eindigen zoals we het gestart zijn: met een positieve noot! In het begin hebben we verteld (en bewezen) dat er oneindig veel priemgetallen zijn. Maar we weten meer, we weten zelfs dat er oneindig veel priemgetallen bestaan die niet tot een priemtweeling behoren. Als de priemtweelingen ooit eindig in aantal blijken te zijn, dan onthult deze bewering niets nieuws, maar voorlopig gaan we er van uit dat dit niet het geval is.

De oneindigheid van priemeenlingen wordt gegarandeerd door een aparte studie van de *harmonische reeks*:

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\cdots,$$

de reeks (d.w.z. oneindige som) van alle omgekeerde natuurlijke getallen. Je weet misschien dat deze oneindige som als uitkomst ∞ heeft. In 1737 bewees Leonhard Euler dat dit resultaat ook geldt als we ons in deze som beperken tot de omgekeerde priemgetallen:

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\cdots=\infty.$$

(Hiermee vond Euler overigens een alternatief bewijs voor de stelling van Euclides dat er van de priemgetallen oneindig veel zijn, maar daar gaat het nu niet om.) Stel nu dat er slechts eindig veel priemeenlingen zijn. Dan zou je de termen met een priemeenling in de noemer kunnen schrappen in de bovenstaande reeks van Euler. Je houdt dan de volgende reeks over:

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\cdots,$$

die nog altijd ∞ als uitkomst zou hebben, omdat je slechts een eindig aantal termen zou hebben geschrapt. Maar dit is in tegenspraak met het kippenvelresultaat van Viggo Brun uit 1919: *de (al dan niet oneindige) som van alle omgekeerde priemtweelingen is eindig!*

De uitkomst van deze som van omgekeerde priemtweelingen wordt de *constante van Brun* genoemd. Deze constante is iets meer dan 1,9, maar de exacte waarde ervan is onbekend. Welke verrassingen hebben de mysterieuze priemtweelingen nog voor ons in petto? ■

ZOEKEN NAAR PRIEMTWEELINGEN

Het vinden van (grote) priemtweelingen is geen eenvoudige zaak, en dat lijkt vreemd want er is het volgende criterium waarmee je het priemtweelingzijn van een koppel getallen kan nagaan:

het koppel $(m, m + 2)$ is een priemtweeling dan en slechts dan als $m + 4 + 4\cdot(m - 1)!$ deelbaar is door $m(m + 2)$.

Deze stelling is eenvoudig te bewijzen, maar helemaal niet handig om te gebruiken. De term $4\cdot(m - 1)!$ wordt namelijk zo snel onnoemelijk groot, dat zelfs de beste computers aan deze stelling niets hebben bij het zoeken naar priemtweelingen. Je krijgt al een goed idee van het probleem indien je voor m de (kleine) waarde 17 kiest: dan moet je nagaan of $17 + 4 + 4\cdot 16! = 83.691.159.552.021$ deelbaar is door 323 (en dat is inderdaad zo).