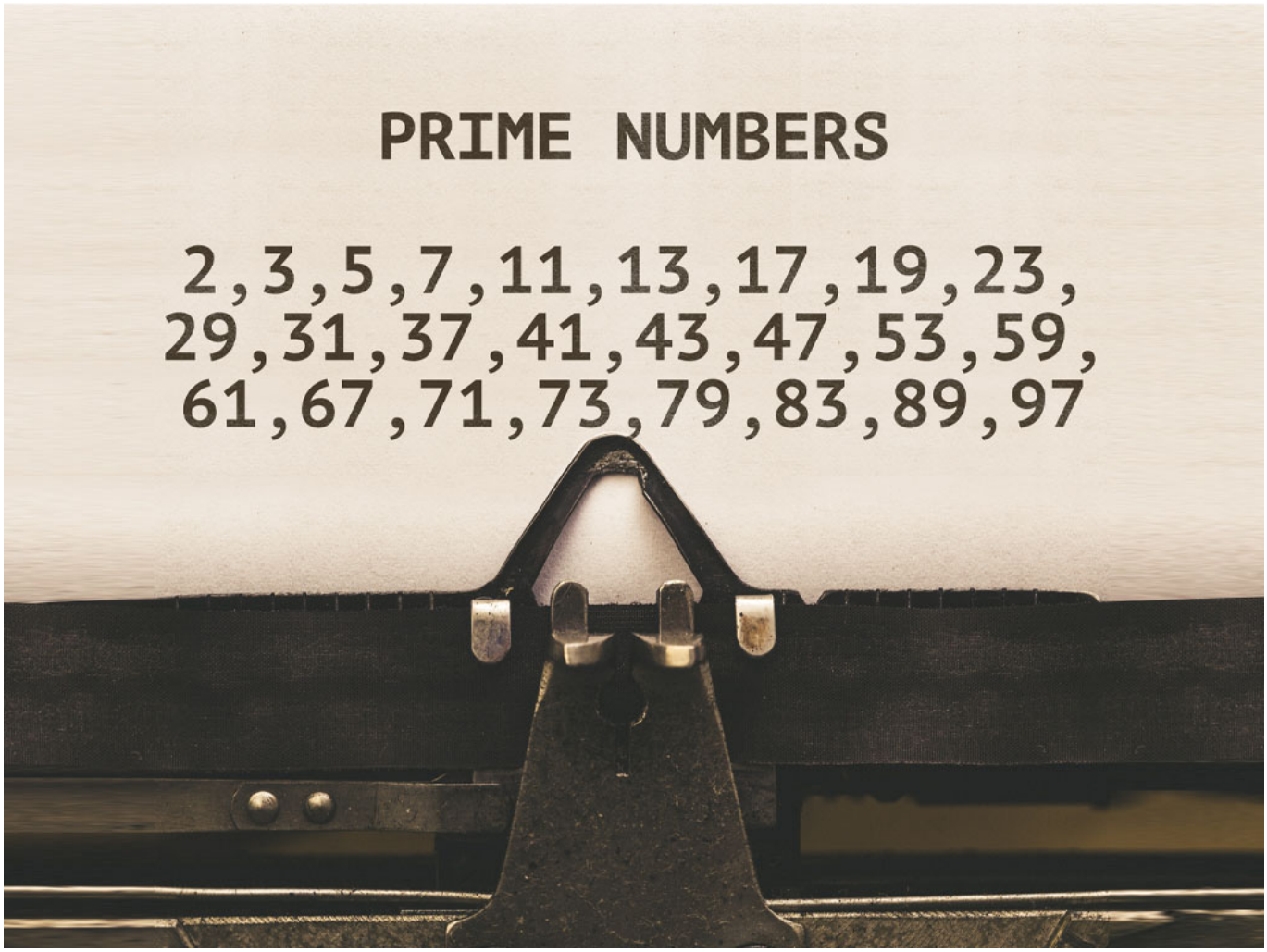
# Nieuw priemgetal ontdekt!

**Op 21 oktober 2024 gebeurde iets wat al bijna zes jaar niet meer was gebeurd: er werd een nieuw grootste priemgetal ontdekt. Luke Durant bewees dat dit getal – met ruim 41 miljoen cijfers – daadwerkelijk niet te delen valt door een ander getal dan één en zichzelf. Het nieuwe priemgetal is een zogenaamd *mersennepriemgetal*, en werd gevonden via de *Great Internet Mersenne Prime Search (GIMPS)*.**




**Afbeelding 1. De priemgetallen onder de honderd.** Afbeelding via Wikimedia Commons.

Om te beginnen: het nu ontdekte getal is natuurlijk niet echt een ‘nieuw’ priemgetal – het was ook al een priemgetal vóórdat wij dat wisten – en belangrijker: het is ook niet het

'grootste' – je kunt vrij eenvoudig bewijzen dat er oneindig veel priemgetallen bestaan, dus hoe groot een bepaald priemgetal ook is, er bestaat altijd wel een nóg grotere! Een betere omschrijving zou dus zijn 'het grootste getal waarvan wij nu weten dat het een priemgetal is', maar om die mondvol niet steeds te hoeven schrijven houden we het toch maar bij 'een nieuw grootste priemgetal'.

Het nieuw ontdekte priemgetal bestaat uit maar liefst 41 miljoen cijfers – veel te veel om op de Quantum Universe-website uit te schrijven. Het is echter een bijzonder soort priemgetal: het valt namelijk te schrijven als

$$2^p - 1,$$

waarbij $p$ een geheel getal is. Op deze manier is het bizar grote getal toch op één regel te schrijven[1]:

$$2^{136279841}-1.$$

Een getal $M_p$ van deze vorm heet een *mersennegetal*:

$$M_p = 2^p - 1.$$

Als een mersennegetal ook een priemgetal is, noemen we het een mersennepriemgetal.

De eerste zes mersennegetallen zijn 0, 1, 3, 7, 15, 31 met respectievelijk $p=0, 1, 2, 3, 4, 5$. Te zien is dat niet al deze getallen priemgetal zijn: alleen 3, 7 en 31, met bijbehorende machten $p=2,3,5$, zijn priemgetallen. Deze machten zijn niet toevallig zelf ook allemaal priem. Als $p$ géén priemgetal is, is het mersennegetal namelijk ook geen priemgetal. Dat is te zien via de identiteit

$$2^{ab} - 1 = (2^a-1)(1 + 2^a + 2^{2a} + ... + 2^{(b-1)a}),$$

die de enthousiaste lezer zelf kan proberen te bewijzen. In woorden: als je $p$ kunt schrijven als een product van $a$ en $b$, zie je rechts dat het bijbehorende mersennegetal óók een product is – en dus geen priemgetal.

Dit betekent niet dat elk mersennegetal met $p$ wél priem ook zelf weer een priemgetal is. Het kleinste tegenvoorbeeld is $M_{11}$:

$$M_{11} =2047 = 23 \times 89.$$

Als $p$ een heel groot priemgetal is, is het bijbehorende mersennegetal zelfs meestal géén priemgetal, maar het nieuwste grootste priemgetal is dus wél ook zo'n mersennepriemgetal, met $p  =136,279,841$ en wel 41 024 320 cijfers.


**Afbeelding 2. Marin Mersenne.** Marin Mersenne, een Franse monnik, bestudeerde in de zeventiende eeuw getallen die later bekend zouden komen te staan als de mersennepriemgetallen. Afbeelding via Wikimedia Commons.

De laatste achttien keer dat het priemrecord werd gebroken, was het ook met een mersennepriemgetal. Dit komt doordat er  voor mersennepriemgetallen een relatief makkelijke test bestaat, waarmee gecheckt kan worden of dit getal daadwerkelijk priem is: de zogeheten *Lucas-Lehmertest*. Die werkt als volgt: definieer $s_0=4$. Vanuit hier kunnen we $s_i$ definiëren als

$$s_i = s_{i-1}^2 -2.$$

Dus $s_1 = 4^2 – 2 = 14, s_2 = 14^2 – 2 = 194$, enzovoort. Het mersennegetal $M_p = 2^p – 1$ is alleen een priemgetal als $s_{p-2}$ deelbaar is door $M_p$, of in nette wiskundenotatie:

$$s_{p-2} \equiv 0 \quad (\text{mod } M_p).$$

Laten we dit voor een paar voorbeelden uitwerken. Als $p=3$, dan is

$$s_{p-2} = s_1 = 14 \equiv 0 \quad (\text{mod } 7).$$

Dit klopt! Nemen we $p=11$, dan is

$$s_{p-2} = s_9 \equiv 1736 \quad (\text{mod } 2047),$$

dus $s_9$ (zelf een getal van bijna 300 cijfers) is niet deelbaar door 2047, en $M_{11}$ is zoals we gezien hebben ook géén priemgetal.

De Lucas-Lehmertest werkt overigens niet voor alle getallen: alleen voor mersennegetallen kun je op deze manier nagaan of ze priem zijn of niet. Zeker voor heel grote getallen is deze procedure wel een stuk sneller dan voor alle kleinere getallen expliciet nagaan of het factoren van het kandidaat-priemgetal zijn. Dit is dan ook hoe GIMPS, de *Great Internet Mersenne Prime Search*, nagaat of bepaalde mersennegetallen daadwerkelijk priem zijn.

## Probabilistische test

Ook de Lucas-Lehmertest duurt nog erg lang voor grote getallen. Daarom wordt er bij GIMPS eerst iets anders berekend. Voor een kandidaatspriemgetal wordt eerst expliciet van de getallen 1 tot en met 77 berekend of het factoren zijn van het getal. Is dat niet het geval, dan wordt een probabilistische test toegepast. Die is een consequentie van de *kleine stelling van*

*Fermat*. Volgens die stelling geldt voor ieder priemgetal $p$ en voor ieder geheel getal $a$ dat

$$a^p \equiv a \quad (\text{mod } p).$$

Weer een snel voorbeeld: voor $p=3$ en $a=2$ zien we dat

$$2^3 = 8 = 6 + 2 \equiv 2 \quad (\text{mod } 3).$$

Het omgekeerde is niet waar: er zijn getallen $q$ die geen priemgetal zijn, waarvoor toch

$$a^q \equiv a \quad (\text{mod } q)$$

wél geldt. Een voorbeeld is het getal 341 als je $a=2$ kiest: je kunt uitrekenen dat

$$2^{341} \equiv 2 \quad (\text{mod } 341)$$

maar 341 is geen priem: $341 = 11 \times 31$.

Een getal dat aan deze voorwaarde voldoet, wordt een *pseudopriemgetal met basis* $a$ genoemd. Er zijn, net als priemgetallen, oneindig veel pseudopriemgetallen, maar die zijn alsnog wel zeldzamer dan de echte priemgetallen. Zo zijn er slechts 3 pseudopriemgetallen met basis 2 onder de 1000. Dit betekent dat als een getal aan de bovenstaande eigenschap voldoet voor een willekeurige $a$, het waarschijnlijker een priemgetal is dan niet[2].

Deze zogenoemde *fermattest* is nog sneller uit te voeren dan de Lucas-Lehmertest. Luke Durant testte van vele mersennegetallen of het priemgetallen zijn. Hiervoor paste hij dus eerst de fermattest toe, en ontdekte zo dat $2^{136279841}-1$ eraan voldeed. Dit gebeurde op 11 oktober 2024. De dag erna werd met de Lucas-Lehmertest nagegaan of het getal ook daadwerkelijk een priemgetal was – het kon immers nog steeds een pseudopriemgetal zijn. Na nog een aantal dagen dubbelchecken was het dan op 21 oktober 2024 echt zeker: het record van het grootste priemgetal was voor het eerst in zes jaar verbroken!

## Priemgetallen en natuurkunde

Hoewel het op het eerste gezicht niet zo lijkt, heeft de studie van priemgetallen ook banden

met de natuurkunde. Een voorbeeld daarvan heeft te maken met een van de beroemdste onbewezen wiskundige hypotheses: de riemannhypothese.

De riemannhypothese, geformuleerd door Bernhard Riemann in 1859, heeft te maken met de verdeling van de priemgetallen. Hoe groter de getallen, hoe minder getallen een priemgetal zullen zijn: er zijn nou eenmaal veel meer kleinere getallen waardoor ze deelbaar zouden kunnen zijn. Het blijkt dat er een relatief simpele formule is om te voorspellen hoe groot het $n$'de priemgetal zal zijn: ongeveer $n\ln n$. Zo is het tiende priemgetal 29, en deze formule zegt dat het ongeveer 23 zou moeten zijn. Het honderdste priemgetal is 541, en volgens de formule ligt het rond de 461. Het duizendste priemgetal zou volgens deze formule rond de 6908 liggen, in werkelijkheid is het 7919.

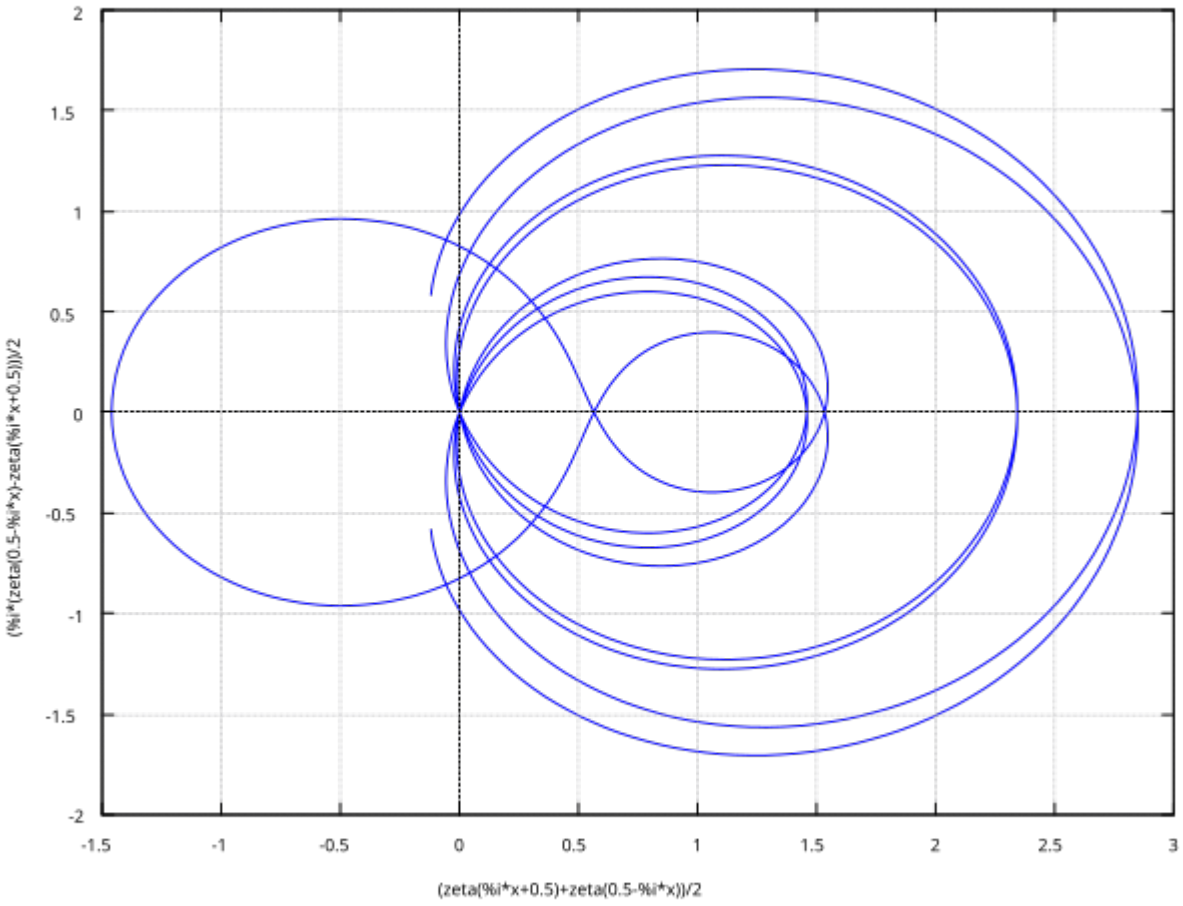
Zoals je ziet is de formule niet perfect, maar de orde van grootte is wel correct. Riemann was juist benieuwd naar de afwijking van deze voorspelling. Die valt te beschrijven aan de hand van de Riemann-zètafunctie:

$$\zeta(s) = \sum_{n=1}^\infty \frac{1}{n^s}.$$

De riemannhypothese gaat over de nulpunten van deze functie: dus de waarden van $s$ waarvoor $\zeta(s) = 0$. Als eerste blijkt dat de Riemann-zètafunctie nul oplevert voor elk even negatief getal, dus $s=-2,-4,-6$ et cetera. Dit noemde Riemann de triviale nulpunten. De riemannhypothese gaat over de *niet-triviale nulpunten*. Dat blijken geen reële getallen te zijn: ze liggen in het complexe vlak. (Zie deze serie artikelen als je meer wilt weten over complexe getallen.) De hypothese zegt dat alle niet-triviale nulpunten van Riemanns functie een reëel deel van ½ hebben: ze zijn dus van de vorm

$$s=1/2+i \times t,$$

met $t$ een reëel getal. Deze hypothese, dat alle niet-triviale nulpunten op deze *kritieke lijn* liggen, is getest voor de eerste 10,000,000,000,000 nulpunten van de functie, maar is dus niet bewezen. Het is zelfs één van de Millenniumproblemen, wat betekent dat degene die het eerste correcte bewijs levert een miljoen dollar krijgt!




**Afbeelding 3. De Riemann-zètafunctie langs de kritieke lijn.** De blauwe kromme geeft de complexe waarden van de zetafunctie weer, voor waarden van t tussen -30 en +30. De blauwe lijn komt diverse malen door de oorsprong – voor de bijbehorende waarden van t heeft Riemanns functie dus de waarde nul. Afbeelding via Wikimedia Commons.

Goed, tot zover nog niet veel natuurkunde. Maar er is heel veel onderzoek gedaan naar de riemannhypothese, en hieruit vloeien ook veel andere resultaten, die soms wel een relatie tot de natuurkunde hebben!

Zo bestudeerde Hugh Montgomery in 1972 de nulpunten van de Riemann-zètafunctie. Hij probeerde de verdeling van deze nulpunten langs de kritieke lijn te beschrijven. Zo kwam hij

tot zijn *paarcorrelatie-hypothese*, die beschrijft hoe groot de kans is om een nieuwe nul te vinden binnen een gegeven afstand van een andere nul.

Toen hij deze resultaten met Freeman Dyson besprak, ontdekten ze iets bijzonders. Dyson deed juist onderzoek naar toevalsmatrices. Bij het bestuderen van zulke toevalsmatrices had hij ook de paarcorrelatie van de *eigenwaardes* – bepaalde getallen die de matrix karakteriseren – van deze matrices berekend. Wat blijkt: de paarcorrelatie van de eigenwaardes van zogeheten hermitische toevalsmatrices, is precies hetzelfde als de paarcorrelatie van de nulpunten van de Riemann-zèta-functie! Dat klinkt ingewikkeld, maar zodra er twee op het oog heel verschillende dingen precies hetzelfde blijken te zijn, worden natuur- en wiskundigen erg enthousiast.

Toevalsmatrices zijn van groot belang in het beschrijven van veel aspecten van natuurkunde, bijvoorbeeld voor het beschrijven van atomen. Volgens Eugene Wigner, in 1951, kunnen de energieniveaus van zware atoomkernen beschreven worden aan de hand van zulke toevalsmatrices. Er wordt zelfs vermoed dat alle klassieke chaotische systemen beschreven kunnen worden met toevalsmatrices!

Blijkbaar bestaat er dus een verband tussen de verdeling van de priemgetallen en fysische concepten zoals de energieniveaus van ingewikkelde atomen. Of het nieuwe grootste priemgetal nu veel zal helpen bij het begrijpen van die relatie valt te bezien, maar elk kleine beetje kennis dat we over de priemgetallen kunnen verzamelen kan wellicht helpen. Veel van de verrassende band tussen priemgetallen en de natuurkunde wordt nog slecht begrepen; duidelijk is dat er nog veel te ontdekken valt…

---

[1] Wil je toch graag alle getallen van het nieuwe priemgetal uitgeschreven zien (of vooral: zien hoe bizar groot dat getal is), kijk dan naar deze video.

[2] Wiskundiger exact verwoord: de kans dat een niet-priemgetal $n$ voldoet aan de fermattest voor willekeurige $a$, benadert nul als $n$ oneindig groot wordt.