Partities en priemgetallen

Jan-Willem van Ittersum
Korteweg-de Vries Instituut voor Wiskunde
Universiteit van Amsterdam

Leve de wiskunde!
10 april 2026

Priemgetallen: bouwstenen van de multiplicatieve getaltheorie

Definitie (Priemgetal)

Een ***priemgetal*** *is een positief geheel getal dat precies twee positieve delers heeft: één en zichzelf.*

De eerste priemgetallen zijn:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ \ldots$$

Stelling (Hoofdstelling van de rekenkunde)

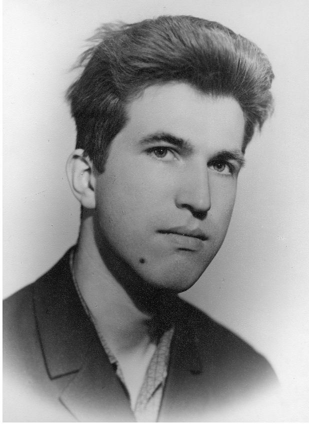
Elk geheel getal kan op een ***unieke manier*** *geschreven worden als product van priemgetallen (afgezien van de volgorde van de priemgetallen).*

Voorbeelden van ontbinding in priemgetallen

$$\ldots \qquad 60 = 2^2 \cdot 3 \cdot 5 \qquad 61 = 61 \qquad 62 = 2 \cdot 31 \qquad \ldots$$

De eeuwenoude droom: priemgetallen vatten in een formule

- Wiskundigen vragen zich al lang af of je de priemgetallen kunt beschrijven met **één eenvoudige formule**.
- In de jaren '70 bewees Yuri Matiyasevich dat je verrassend veel verzamelingen van gehele getallen kunt beschrijven door middel van een **veelterm**.
- Bijvoorbeeld **priemgetallen** zijn zo te beschrijven!
- Enkele jaren later gaven Jones, Sato, Wada en Wiens zo'n formule expliciet: een **veelterm van graad 25 in 26 variabelen** waarvan de positieve waarden precies de priemgetallen zijn.
- Het werkt — maar praktisch is het zeker niet.



Yuri Matiyasevich, 1969

Is er een makkelijkere manier om priemgetallen te detecteren?

DIOPHANTINE REPRESENTATION OF THE SET OF PRIME NUMBERS

JAMES P. JONES, DAIHACHIRO SATO, HIDEO WADA AND DOUGLAS WIENS

1. Introduction. Martin Davis, Yuri Matijasevič, Hilary Putnam and Julia Robinson [4] [8] have proven that every recursively enumerable set is Diophantine, and hence that the set of prime numbers is Diophantine. From this, and work of Putnam [12], it follows that the set of prime numbers is representable by a polynomial formula. In this article such a prime representing polynomial will be exhibited in explicit form. We prove (in Section 2)

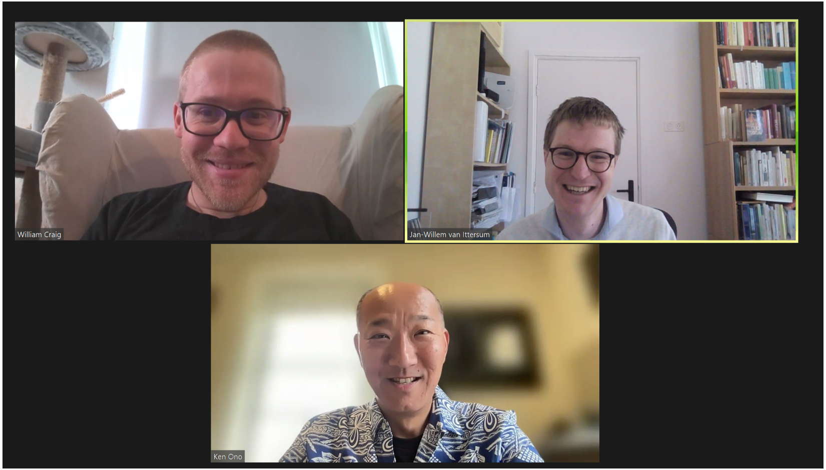
THEOREM 1. *The set of prime numbers is identical with the set of positive values taken on by the polynomial*

$$
\begin{aligned}
\text{(1)}\quad & (k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)\cdot(h+j)+h-z]^2-[2n+p+q+z-e]^2\\
& -[16(k+1)^3\cdot(k+2)\cdot(n+1)^2+1-f^2]^2-[e^3\cdot(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2\\
& -[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)\cdot(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2\\
& -[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2\\
& -[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}
\end{aligned}
$$

as the variables range over the nonnegative integers.

Een veelterm van graad 25 in 26 variabelen die priemgetallen detecteert. . .

Onderzoek met Will Craig en Ken Ono



Partities: de bouwstenen van de additieve getaltheorie

Definitie (Partitie)

Een partitie van een geheel getal n is een eindige rij positieve gehele getallen $(\lambda_1, \lambda_2, \ldots, \lambda_r)$ met $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq 1$ waarvan de som gelijk is aan n.

Voorbeeld (Partities van 4 in twee groepen)

(4), $(2,2)$, $(1,1,1,1) \mid (3,1)$, $(2,1,1)$

Vraag: hoeveel partities zijn er van het getal 5? Verdeel ze ook in twee groepen.

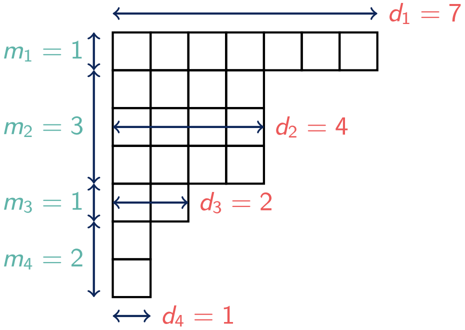
Er zijn er 7, namelijk (5), $(1,1,1,1,1) \mid (4,1)$, $(3,2)$, $(3,1,1)$, $(2,2,1)$, $(2,1,1,1)$.

We schrijven $p(n)$ voor het aantal partities van n. Euler vond de volgende formule:

$$\sum_{n\geq 0} p(n)\, q^n = \frac{1}{\prod_{n\geq 1}(1-q^n)}.$$

Partities worden bepaald door hun delen en hun multipliciteiten

Merk op dat een partitie eenduidig wordt bepaald door de verschillende delen $d_1 > d_2 > \ldots > d_a$ en de bijbehorende multipliciteiten $m_1, m_2, \ldots, m_a$.



Voorbeeld (Stanley-coördinaten)

Voor $\lambda = (7, 4, 4, 4, 2, 1, 1) = (7^1, 4^3, 2^1, 1^2)$ geldt $\mathbf{d} = (7, 4, 2, 1)$ en $\mathbf{m} = (1, 3, 1, 2)$.

Vraag: bepaal $\mathbf{d}$ en $\mathbf{m}$ voor $\lambda = (5, 5, 5, 5, 3, 1, 1, 1)$.

Er geldt $\mathbf{d} = (5, 3, 1)$ *en* $\mathbf{m} = (4, 1, 3)$.

Percy Alexander MacMahon: pionier van de partitie-theorie

- Percy Alexander MacMahon (1854–1929) was een Brits wiskundige.
- Hij werkte vooral aan **partities** en **combinatorische structuren**.
- Hij werkte hard om partities **systematisch te tellen**.

Definitie (Product van multipliciteiten)

Voor een partitie λ met delen $\mathbf{d} = (d_1, \ldots, d_a)$ en multipliciteiten $\mathbf{m} = (m_1, \ldots, m_a)$, definieer $\mathrm{MM}(\lambda) = m_1 m_2 \cdots m_a$.

Voorbeeld

Voor $\lambda = (7, 4, 4, 4, 2, 1, 1)$ hebben we $\mathbf{d} = (7, 4, 2, 1)$ en $\mathbf{m} = (1, 3, 1, 2)$. Dan is $\mathrm{MM}(\lambda) = 1 \cdot 3 \cdot 1 \cdot 2 = 6$.

MacMahon

Vraag: bepaal $\mathrm{MM}(\lambda)$ voor $\lambda = (5, 5, 5, 5, 3, 1, 1, 1)$

We hebben $\mathbf{d} = (5, 3, 1)$ en $\mathbf{m} = (4, 1, 3)$, dus $\mathrm{MM}(\lambda) = 4 \cdot 1 \cdot 3 = 12$.

MacMahon-partitiefunctie telt sommen van producten van multipliciteiten

Definitie (MacMahon-partitiefunctie, 1920)

Voor $a \geq 1$ definiëren we de MacMahon-partitiefunctie door

$$M_a(n) = \sum_{\substack{\lambda \text{ partitie van } n \text{ met} \\ a \text{ verschillende delen}}} \mathrm{MM}(\lambda), \qquad \textit{waar} \qquad \mathrm{MM}(\lambda) = m_1 m_2 \cdots m_a\,.$$

Waarden van $M_1(3)$ en $M_2(3)$

$n = 3, a = 1$: $\lambda = (3)$ of $\lambda = (1,1,1)$, dus $M_1(3) = 1 + 3 = 4$.
$n = 3, a = 2$: $\lambda = (2,1)$, dus $M_2(3) = 1 \cdot 1 = 1$.

Vraag: bepaal $M_1(4)$ en $M_2(4)$.

$n = 4, a = 1$: $\lambda = (4)$, $(2,2)$ of $(1,1,1,1)$, dus $M_1(4) = 1 + 2 + 4 = 7$.
$n = 4, a = 2$: $\lambda = (3,1)$ of $(2,1,1)$, dus $M_2(4) = 1 \cdot 1 + 1 \cdot 2 = 3$.

Een nieuwe partitiefunctie: $\Psi(n)$

Definieer $$\Psi(n) := (n^2 - 3n + 2)M_1(n) - 8M_2(n).$$

Herinnering:

$$M_a(n) = \sum_{\substack{\lambda \text{ partitie van } n \text{ met} \\ a \text{ verschillende delen}}} \mathrm{MM}(\lambda), \qquad \text{waar} \qquad \mathrm{MM}(\lambda) = m_1 m_2 \cdots m_a\,.$$

Vraag: bepaal $\Psi(3)$ en $\Psi(4)$. *Hint:* $M_1(3) = 4$, $M_2(3) = 1$, $M_1(4) = 7$, $M_2(4) = 3$.

$$\Psi(3) = 2M_1(3) - 8M_2(3) = 0, \qquad \Psi(4) = 6M_1(4) - 8M_2(4) = 18.$$

Tabel

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...
$\Psi(n)$	0	0	18	0	120	0	270	192	504	0	1680	0	1296	1536	...

Ψ detecteert priemgetallen

Herinnering:

$$\Psi(n) \;=\; (n^2 - 3n + 2)M_1(n) - 8M_2(n)$$

met

$$M_a(n) \;=\; \sum_{\substack{\lambda \text{ partitie van } n \text{ met} \\ a \text{ verschillende delen}}} \mathrm{MM}(\lambda) \qquad \text{en} \qquad \mathrm{MM}(\lambda) \;=\; m_1 m_2 \cdots m_a\,.$$

Stelling (Craig–vl–Ono, '24)

Voor $n \geq 2$ geldt:

- $\Psi(n) \geq 0$
- $\Psi(n) = 0$ *dan en slechts dan als n een priemgetal is.*

Ψ detecteert

$(n^2-3n+2)M_1(n)-8M_2(n)$
$(3n^3-13n^2+18n-8)M_1(n)+(12n^2-120n+212)M_2(n)-960M_3(n)$
$(25n^4-171n^3+423n^2-447n+170)M_1(n)+(300n^3-3554n^2+12900n-14990)M_2(n)+$ $(2400n^2-60480n+214080)M_3(n)-725760M_4(n)$
$(126n^5-1303n^4+5073n^3-9323n^2+8097n-2670)M_1(n)+$ $(3024n^4-48900n^3+288014n^2-737100n+695490)M_2(n)+$ $(60480n^3-1510080n^2+10644480n-23496480)M_3(n)+$ $(725760n^2-36288000n+218453760)M_4(n)-580608000M_5(n)$
$(300n^8-1542n^7-33049n^6+377959n^5-1651959n^4+3726801n^3-4575760n^2+2903750n-746500)M_1(n)+$ $(12000n^7-91008n^6-2799900n^5+50637162n^4-351366300n^3+1239098170n^2-2210467000n+1585493500)M_2(n)+$ $(432000n^6-3548160n^5-236343840n^4+5133219840n^3-42370071840n^2+161101416000n-236150560800)M_3(n)+$ $(12096000n^5-72817920n^4-17599680000n^3+396192142080n^2-3123876672000n+8555162112000)M_4(n)+$ $(193536000n^4-1056513024000n^2+21310248960000n-112944125952000)M_5(n)+$ $(-46495088640000n+604436152320000)M_6(n)-1115882127360000M_7(n)$

Herinnering:

met

M_a … n_a .

Stelling (Cr

Voor $n \geq 2$ g

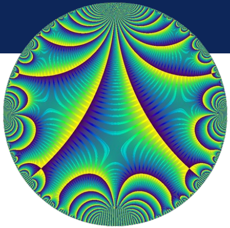
- $\Psi(n) \geq$
- $\Psi(n) =$

Achtergrond: modulaire vormen

- Sommige reële functies zijn **symmetrisch**, bv. $\sin(x)$ en $\cos(x)$ zijn periodiek.
- Sommige **complexe functies** hebben interessante symmetriën in de twee dimensies van het complexe vlak (zie rechtsboven).
- **Modulaire vormen** f zijn zulke oneindig vaak differentieerbare functies met symmetrieën

$$f(z+1) = f(z), \quad f\left(\frac{-1}{z}\right) = z^k f(z).$$

- Met behulp van modulaire vormen kan men de eigenschappen van Ψ **bewijzen**.

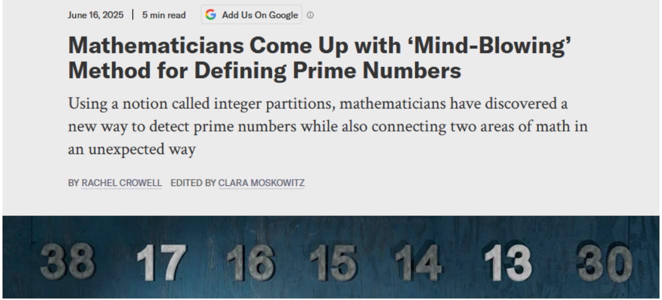


Artistieke impressie van een hyperbolische betegeling (Escher) en van een modulaire vorm (Lowry-Duda)

Modulaire vormen zijn overal!

- in de *getaltheorie*, bv. in het bewijs van de **laatste stelling van Fermat** (Wiles, 1994);
- in de *meetkunde en combinatoriek*, bv. bij het **bolpakkingsprobleem** in hogere dimensies (Viazovska, 2016);
- in de *theoretische natuurkunde*, o.a. in de **snaartheorie** (Witten, jaren 80).

- Priemgetallen zijn de bouwstenen van de multiplicatieve getaltheorie, partities van de additieve getaltheorie.
- Via de MacMahon-functie op partities hebben we een nieuwe functie $\Psi(n)$ gemaakt.
- Met behulp van modulaire vormen blijkt: $\Psi(n) = 0$ precies voor priemgetallen n.


June 16, 2025 | 5 min read Add Us On Google

Mathematicians Come Up with 'Mind-Blowing' Method for Defining Prime Numbers

Using a notion called integer partitions, mathematicians have discovered a new way to detect prime numbers while also connecting two areas of math in an unexpected way

BY RACHEL CROWELL   EDITED BY CLARA MOSKOWITZ

Een artikel in *Scientific American*.

Verder lezen

- Cepelewicz, J. (2024, 21 oktober). *Math is still catching up to the mysterious genius of Srinivasa Ramanujan.* Quanta Magazine.
- Crowell, R. (2025, 16 juni). *Mathematicians come up with 'mind-blowing' method for defining prime numbers*. Scientific American.
- Green, R. (2024, 20 mei). *Partitions and primes*. A Piece of the Pi: mathematics explained.
- Starreveld, N. (2026, maart). *Een prijs voor een jonge ontdekkingsreiziger! Interview met Jan-Willem van Ittersum*. Euclides.