Priemgetalformules

Frits Beukers

PWN Vakantiecursus voor wiskundeleraren 2023

Polynomen

Euler: $x^2 - x + 41$ heeft een priemwaarde voor $x = 0, 1, 2, \ldots, 40$.

Stelling

Gegeven een niet-constant polynoom $F(x)$. Dan zijn oneindig veel van de waarden $F(0), F(1), F(2), \ldots$ niet priem.

Bewijs: Neem bijvoorbeeld $F(x) = x^2 + 1$. Merk op $F(2) = 5$. Dan geldt $F(2 + 5k) \equiv F(2) \equiv 0 (\mathrm{mod}\ 5)$. Dus alle waarden $F(2 + 5k)$ zijn deelbaar door 5.

Hoe zit het met de priemwaarden van $F(x)$?

Priemwaarden van polynomen

Vermoeden van Bunyakowsky, 1857

Stel dat $F(x)$ een irreducibel polynoom is en $\mathrm{ggd}(F(1), F(2), \ldots) = 1$. Dan heeft $F(x)$ oneindig veel priemwaarden.

NB:

- Het is duidelijk dat bijvoorbeeld $(x+1)(x+2)$ hooguit eindig veel priemwaarden kan aannemen. Vandaar de conditie $F(x)$ irreducibel.
- Het polynoom $3x^2 - x + 2$ is irreducibel, maar neemt alleen even waarden aan. Vandaar de ggd-conditie.

Priemgetallen van de vorm $n^2 + 1$

Stel

$$\pi_F(x) = \#\{n^2 + 1 \leq x \text{ en } n^2 + 1 \text{ priem}\}.$$

x	$\pi_F(x)$	$1.55\sqrt{x}/\log x$
10^3	10	7.09
10^4	19	16.82
10^5	51	45.57
10^6	112	112.19
10^7	316	304.10
10^8	841	841.44
10^9	2378	2365.23
10^{10}	6656	6731.56

Priemgetallen in een rekenkundige rij

Vermoeden van Bunyakowksy is bewezen voor lineaire polynomen.

Stelling (Dirichlet, 1837)

Zij a, q een tweetal positieve getallen met $\mathrm{ggd}(a, q) = 1$. Dan heeft het polynoom $qx + a$ oneindig veel priemwaarden.
Anders gezegd, er zijn oneindig veel priemgetallen p van de vorm $p \equiv a \pmod{q}$.

Het blijkt zelfs dat de priemgetallen min of meer gelijkmatig over de restklassen $a \pmod{q}$ verdeeld zijn.

Formule van Mills

Stelling (Mills, 1947)

Er bestaat een reëel getal A zó dat $\lfloor A^{3^n} \rfloor$ priem is voor alle gehele $n \geq 0$.

Bewijs: Elk interval $[N^3, (N+1)^3]$ met $N \geq N_0$ bevat een priemgetal (Ingham, 1937).
Kies een priem getal $P_0 \geq N_0$ en vervolgens $P_1, P_2, P_3, \ldots$ zó dat

$$P_n^3 < P_{n+1} < (P_n + 1)^3 - 1 \quad n = 0, 1, 2, \ldots$$

Definieer $u_n = P_n^{1/3^n}, v_n = (P_n + 1)^{1/3^n}$ voor elke $n \geq 0$. Merk op dat $v_n > u_n$ voor alle n.
Uit $P_n^3 < P_{n+1}$ volgt $u_n < u_{n+1}$
Uit $P_{n+1} + 1 < (P_n + 1)^3$ volgt $v_{n+1} < v_n$.Dus

$$[u_0, v_0] \supset [u_1, v_1] \supset \cdots \supset [u_n, v_n] \supset \cdots \ni A$$

Bewijs stelling van Mills

We hebben $u_n < A < v_n$ voor alle n.
Verheffen tot de macht 3^n geeft

$$P_n < A^{3^n} < P_n + 1.$$

Dus

$$\lfloor A^{3^n} \rfloor = P_n.$$

Diophantische vergelijkingen

Een diophantische vergelijking is een vergelijking van de vorm $P(x_1, \ldots, x_n) = 0$, met P een polynoom in n variabelen met gehele getallen als onbekenden.
Voorbeelden:

- De vergelijking van Pell voor gegeven $D > 0$: $x^2 - Dy^2 = 1$.
  Deze vergelijking heeft oneindig veel oplossingen als D geen kwadraat is, en alleen $x = \pm 1, y = 0$ als D een kwadraat is.
  Kleinste oplossing van $x^2 - 313y^2 = 1$ met $y > 0$,

$$x = 32188120829134849, \quad y = 1819380158564160.$$

- De vergelijking van Mordell voor gegeven $k \neq 0$: $y^2 = x^3 + k$.
  Deze heeft hooguit eindig veel oplossingen.
  - Oplossingen van $y^2 = x^3 + 7$: geen
  - Oplossingen van $y^2 = x^3 - 2$: $x = 3$
  - Oplossingen van $y^2 = x^3 + 17$: $x = -2, -1, 2, 4, 8, 43, 52$

Hilbert probleem

Hilbert, 1900 (moderne versie)

Bestaat er een computerprogramma dat in in staat is om van iedere diophantische vergelijking te beslissen of er wel of geen oplossing in positief gehele getallen bestaat?

Hier is heel veel werk verzet door met name Hilary Putnam, Martin Davis, Julia Robinson.
Met de afronding door Yuri Matiyasevich in 1970.

Stelling

Zo'n computerprogramma bestaat niet.

Diophantische verzamelingen

Definitie

Een verzameling S van positief gehele getallen heet Diophantisch als er een polynoom $M(y, x_1, \ldots, x_n)$ bestaat zó dat $s \in S$ precies dan als $M(s, x_1, \ldots, x_n) = 0$ oplosbaar is in gehele $x_1, \ldots, x_2 \geq 0$.

- S: kwadraten, $M(y, x) = y - x^2$.
- S: niet-priemgetallen, $M(y, x_1, x_2) = y - (x_1 + 2)(x_2 + 2)$.
- S: niet-kwadraten, $M(y, x_1, x_2) = x_1^2 - y(x_2 + 1)^2 - 1$.
- S: Fibonaccigetallen
  $F_n = 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$.Beschouw ook de rij $G_n = 2, 1, 3, 4, 7, 11, 18, 29, \ldots$. Dan geldt

$$G_n^2 - 5F_n^2 = (-1)^n 4.$$

  We nemen $M(y, x) = (x^2 - 5y^2)^2 - 16$.
- S: De machten van twee, 2^k. M is zeer gecompliceerd.

Priemproducerend polynoom

Stelling (Matiyasevich)

De verzameling priemgetallen is diophantisch.

Er bestaat dus een polynoom $M(y, x_1, \ldots, x_n)$ zó dat $k + 2$ priem precies dan als $M(k, x_1, \ldots, x_n) = 0$ oplosbaar is in gehele $x_1, \ldots, x_n \geq 0$.

Uit de contructie blijkt dat M een som van kwadraten is en dus waarden ≥ 0 heeft.
Hieruit volgt:

Gevolg

De verzameling positieve waarden van het polynoom $(k + 2) \times (1 - M(k, x_1, \ldots, x_n)$ met $k, x_1, \ldots, x_n \geq 0$ is precies de verzameling priemgetallen.

Het polynoom

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

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

as the variables range over the nonnegative integers.

Opmerking: Als n een samengesteld getal is dan kan dit bewezen worden met 1 vermenigvuldiging.

Gevolg van de vorm van M

Als p een priemgetal is dan kan dit bewezen worden in hooguit 87 optellingen en vermenigvuldigingen.

Criterium van Wilson

Hoe construeren we M?

Stelling (Wilson, 1770)

Voor elk priemgetal p geldt $(p-1)! \equiv -1 (\mathrm{mod}\ p)$.

Bewijs: $x^{p-1} - 1$ heeft modulo p de nulpunten $1, 2, \ldots, (p-1)$ (kleine stelling van Fermat).
Dus $x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) (\mathrm{mod}\ p)$.
Vul links en rechts $x = 0$ in: $-1 \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) (\mathrm{mod}\ p)$.

Als n niet priem en > 4, dan geldt $(n-1)! \equiv 0 (\mathrm{mod}\ n)$.
Conclusie: k is priem precies dan als k een deler is van $(k-1)! + 1$.
Ofwel: k is priem precies dan als er een gehele x bestaat zó dat $(k-1)! + 1 = kx$.

Faculteiten zijn Diophantisch

Hier staat een diophantische karakterisering van $f = k!$

LEMMA 2.11. *For any positive integers k and f, in order that $f = k!$ it is necessary and sufficient that there exist nonnegative integers j, h, n, p, q, w and z such that*

$$\text{(I)} \quad q = wz + h + j, \qquad \text{(IV)} \quad p = (n+1)^k,$$

$$\text{(II)} \quad z = f(h+j) + h, \qquad \text{(V)} \quad q = (p+1)^n,$$

$$\text{(III)} \quad (2k)^3(2k+2)(n+1)^2 + 1 = \square, \qquad \text{(VI)} \quad z = p^{k+1}.$$