Kennismaking met de priemgetallen

Frits Beukers

PWN Vakantiecursus voor wiskundeleraren 2023

Priemgetallen

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137
139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199,
211, 223, 227, . . .

Oneindig veel priemgetallen I

Stelling (Euclides)

Voor elk getal N bestaat een priemgetal groter dan N.

Bewijs:

- Neem het product van $1, 2, 3, \ldots, N$. Dit noteren we als $N!$
- Tel daar 1 bij op.
- Kies een priemdeler p van $N! + 1$.
- Stel dat $p \leq N$. Dan is p een deler van $N!$, maar p kan geen deler van zowel $N!$ als $N! + 1$ zijn.
- Dus concluderen we dat $p > N$.

Lemma

Elk positief geheel getal is deelbaar door een priemgetal.

Bewijs: Kies de kleinste deler > 1 van dit getal.

Een opgave

Opgave

Laat op analoge manier zien dat er bij elke $N \geq 4$ een priemgetal groter dan N en van de vorm $4n - 1$ bestaat. (Hint: merk op dat $N! - 1$ van de vorm $4n - 1$ is).

Euler

Leonhard Euler (1707-1783)

Oneindig veel priemgetallen II

Stelling (Euler)

De oneindige reeks

$$\sum_{p \text{ priem}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots$$

divergeert.

Ter herinnering

Harmonische reeks

De oneindige reeks

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

divergeert.

Oneindig veel priemgetallen II

Bewijs: kies N. Dan,

$$\prod_{p \leq N} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) > \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{N}$$

Ten tweede,

$$\prod_{p \leq N} \left(1 + \frac{1}{p}\right)^2 > \prod_{p \leq N} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right)$$

Ten derde,

$$\sum_{p \leq N} \frac{1}{p} > \sum_{p \leq N} \log\left(1 + \frac{1}{p}\right) = \log \prod_{p \leq N} \left(1 + \frac{1}{p}\right)$$

Divergentiesnelheden

Terzijde:

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{N}\approx\int_1^N\frac{dx}{x}=\log N.$$

en

$$\sum_{p\text{ priem},p\leq N}\frac{1}{p}>\log\log N-1.$$

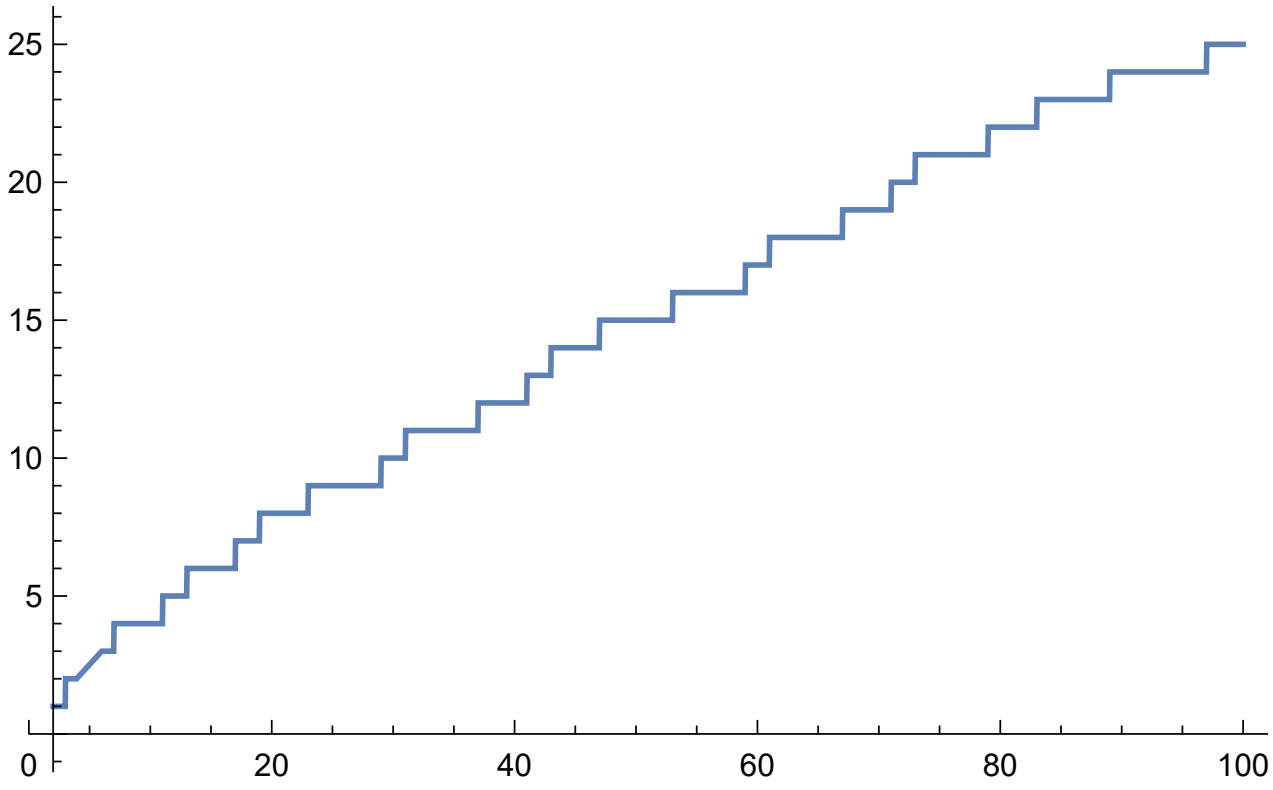
Oneindig veel priemgetallen III

Stel er zijn eindig veel priemgetallen, zeg $p_1, p_2, \ldots, p_n$.
Dan kan elk getal geschreven worden in de vorm $p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ met $k_1, k_2, \ldots, k_n \geq 0$.
Hoeveel getallen zijn er van deze vorm en $\leq x$?
Dan moet zeker gelden, $p_1^{k_1} \leq x, p_2^{k_2} \leq x, \ldots, p_n^{k_n} \leq x$.
Omdat $p_i \geq 2$ voor alle i volgt hieruit dat $k_i \leq \log x / \log 2$ voor alle i.
Het aantal getallen dat hiermee gevormd kan worden is hooguit $(\log x / \log 2)^n$.
Omdat $x > (\log x / \log 2)^n$ als x groot genoeg is hebben we een tegenspraak.

Priemgetallen tellen

Definieer

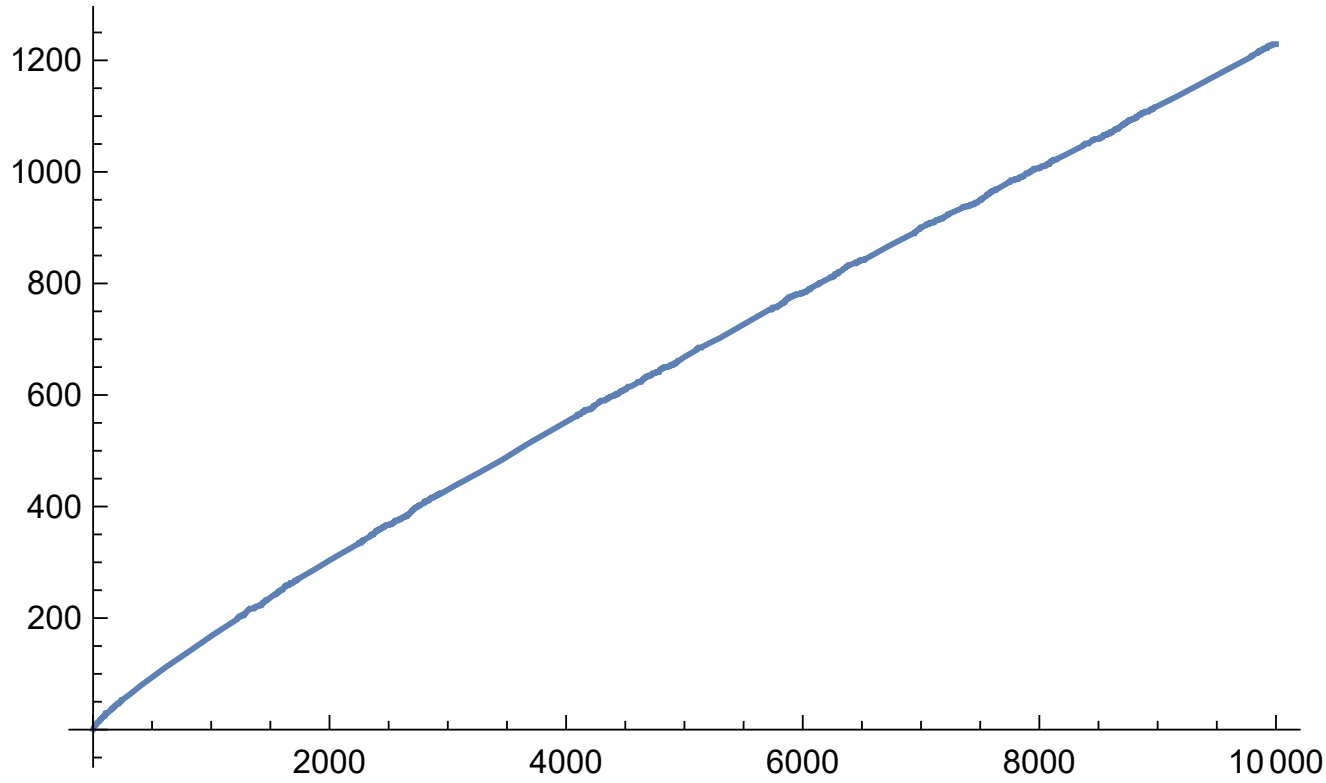
$$\pi(x) = \#\{p \leq x | \ p \text{ priem}\}.$$



Priemgetallen tellen

Definieer

$$\pi(x) = \#\{p \leq x | \ p \text{ priem}\}.$$



Gauss

Johann Carl Friedrich Gauss (1777-1855)

Heuristiek van Gauss

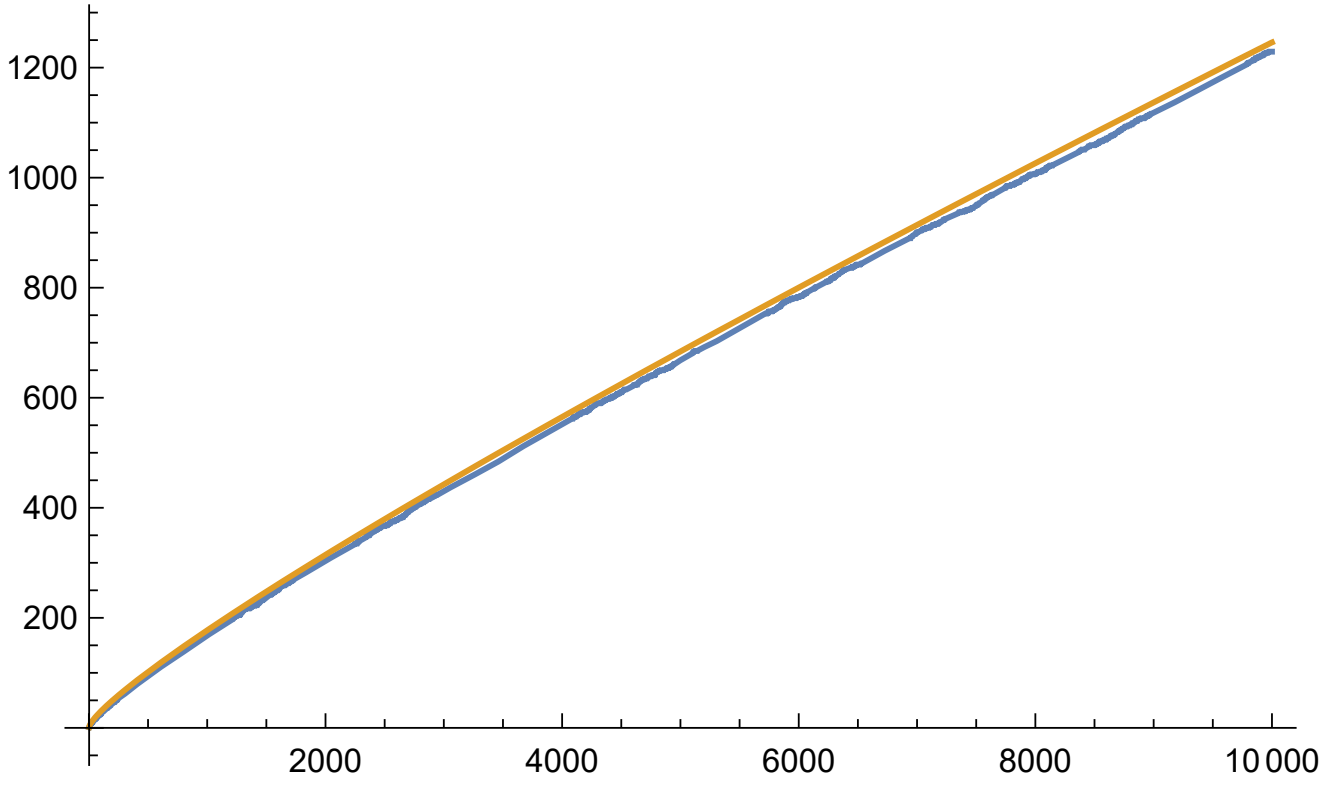
Gauss: Neem X groot en Δ minder groot. Dan is het aantal priemgetallen in $[X, X + \Delta]$ ongeveer gelijk aan $\Delta / \log(X)$.
Anders gezegd: dichtheid van de priemgetallen van de grootte X is ongeveer $1/\log(X)$.
Priemtelling in $[x, x + 10^5]$

x	aantal	$10^5/\log(x)$
10^8	5411	5428
10^9	4832	4825
10^{10}	4306	4342
10^{11}	4019	3948
10^{12}	3614	3619
10^{13}	3382	3340
10^{14}	3045	3102
10^{15}	2804	2895

Benadering van $\pi(x)$

Uit Gauss's idee volgt dat $\pi(x)$ ongeveer gelijk is aan $\mathrm{li}(x)$, waarin

$$\mathrm{li}(x) := \int_2^x \frac{dt}{\log t} \approx \frac{1}{\log 2} + \frac{1}{\log 3} + \cdots + \frac{1}{\log x}.$$



Priemgetalstelling

Als de verhouding van twee functies $f(x)$ en $g(x)$ naar 1 gaat als $x \to \infty$ noteren we dit als $f(x) \sim g(x)$.

Priemgetalstelling
(Hadamard, De la Vallée-Poussin, 1896)

$\pi(x) \sim \mathrm{li}(x)$.

Voor het bewijs gebruikt men eigenschappen van de Riemann ζ-functie.

Opgave

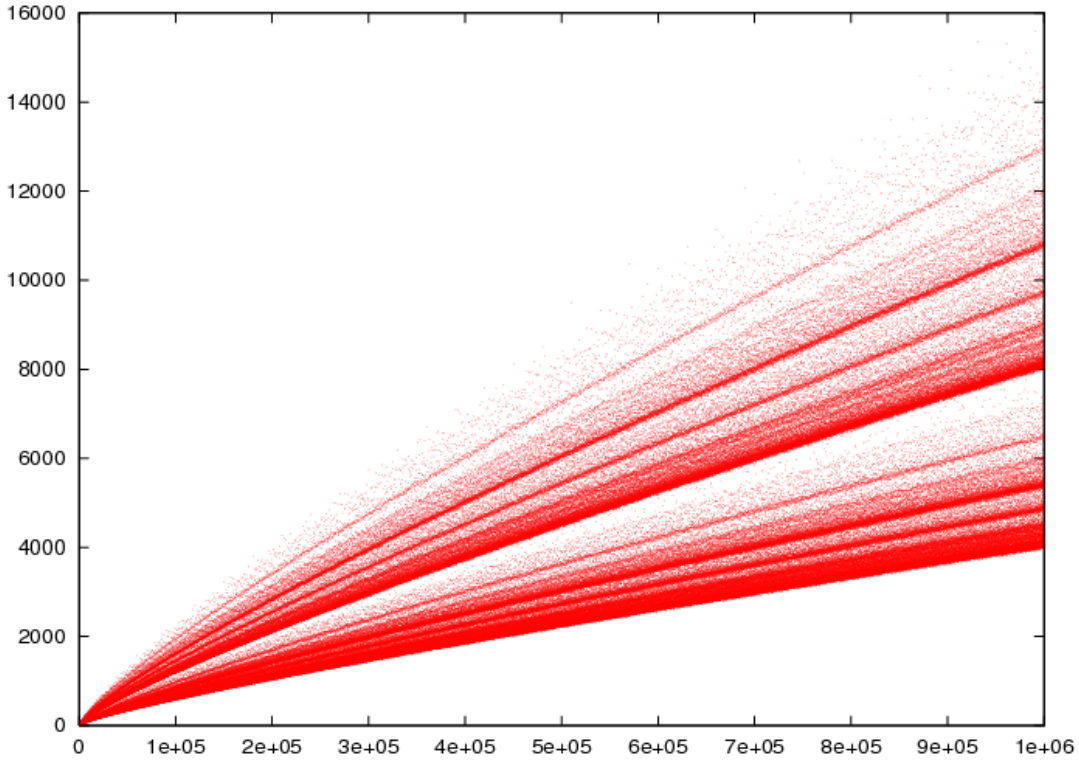
Laat zien dat $\mathrm{li}(x) \sim x/\log(x)$.

De grote priemgetalvermoedens

Goldbach vermoeden (1752)

Elk even getal ≥ 4 is te schrijven als som van twee priemgetallen.

Aantal manieren om even N met $N \leq 10^6$ te schrijven als som van twee priemgetallen:



De grote priemgetalvermoedens

Zwak Goldbach vermoeden

Elk oneven getal $N \geq 7$ is te schrijven als som van drie priemgetallen.

Bewezen,

- als N groot genoeg is, door I.M.Vinogradov (1937)
- volledig door H.Helfgott (2013) (maar nog niet gepubliceerd).

Stel Goldbach vermoeden is waar.
Schrijf $N - 3 = p + q$, met p, q priem.
Dan geldt: $N = 3 + p + q$.
Dus:
Goldbach vermoeden is waar $\Rightarrow$ Zwak Goldbach vermoeden is waar

De grote priemgetalvermoedens

Dit vermoeden gaat over paren $(11, 13)$, $(41, 43)$, $(101, 103)$, etc.

Priemtweelingvermoeden

Er bestaan oneindig veel priemgetallen p zó dat $p + 2$ ook priem is.

Een eerste resultaat,

Stelling (Brun, 1919)

De reeks

$$\sum_{p,p+2 \text{ priem}} \frac{1}{p}$$

convergeert.

Priemtweelingen

In 2014 was er een spectaculaire vooruitgang.

- Y.Zhang (2014): er bestaat een getal $A < 70.000.000$ zó dat er oneindig veel priemgetalparen $p, p + A$ bestaan.
- J.Maynard (2015): er bestaat een getal $A < 246$ zó dat er oneindig veel priemgetalparen $p, p + A$ bestaan.

Opgaven

- Laat zien dat er oneindig veel priemgetallen p bestaan zó dat $p + 2$ *niet* priem is.
- Laat zien dat er maar één priemgetaldrieling $p, p + 2, p + 4$ bestaat.

Markante resultaten

Een rij getallen $k_0 < k_1 < k_2 < \cdots < k_n$ heet een rekenkundige rij van lengte n als alle verschillen $k_{i+1} - k_i$ dezelfde waarden hebben.

Stelling (Green, Tao, 2008)

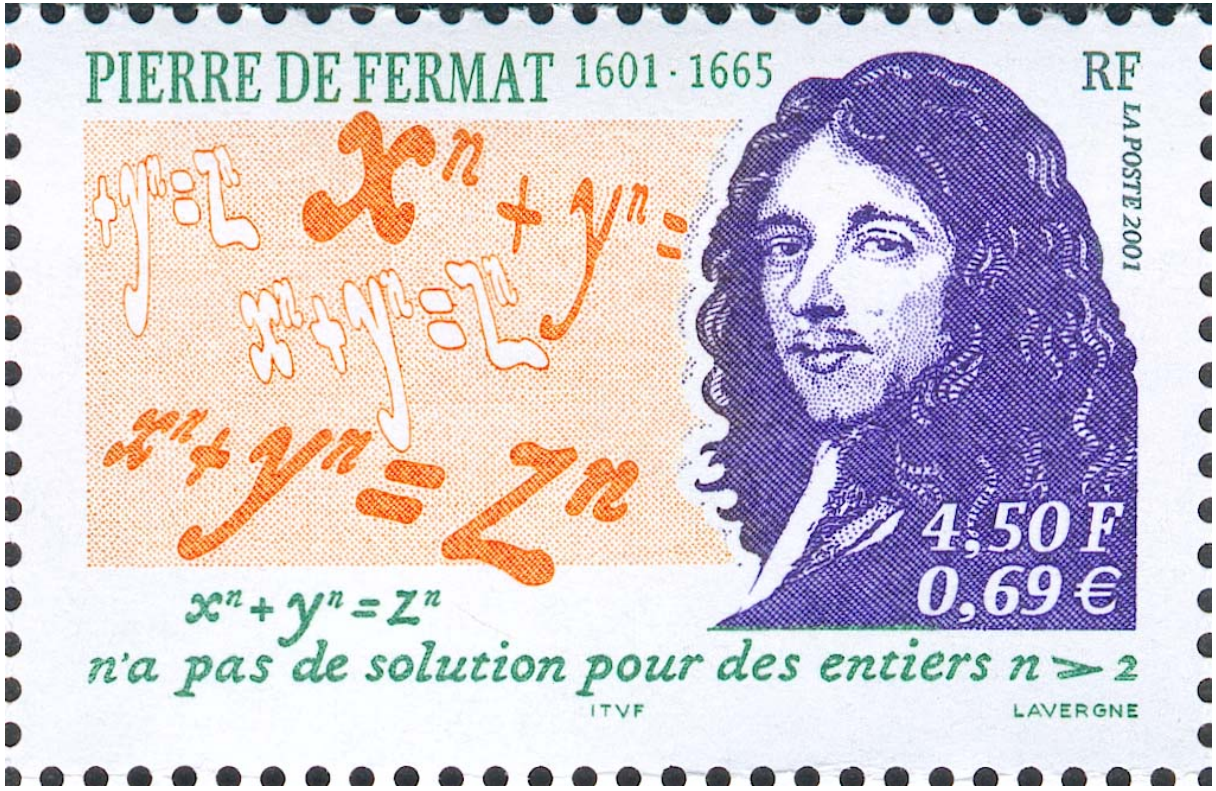
Er bestaan willekeurig lange rekenkundige rijen bestaande uit priemgetallen.

Voorbeelden: $150n + 7$ voor $n = 0, 1, \ldots, 6$ (Lemaire, 1910) en $26n + 4943$ voor $n = 0, 1, \ldots, 12$ (Seredinskij, 1963).
Een ander opmerkelijk resultaat.

Stelling (Maynard 2016)

Kies $a_0 \in \{0, 1, \ldots, 9\}$. Dan zijn er oneindig veel priemgetallen waarvoor a_0 niet in de cijfers voorkomt.

Fermat en de priemgetallen



Pierre de Fermat (1607-1665)

Pythagoreïsche driehoeken

$$5^2 = 3^2 + 4^2, \qquad 13^2 = 12^2 + 5^2 \qquad 17^2 = 15^2 + 8^2$$

$$29^2 = 21^2 + 20^2 \qquad 37^2 = 35^2 + 12^2 \qquad 41^2 = 40^2 + 9^2$$

$$904281937^2 = 281660465^2 + 859298088^2$$

Algemene formule als ggd gelijk is aan 1:

$$(a^2 + b^2)^2 = (a^2 - b^2)^2 + (2ab)^2$$

De schuine zijdes zijn dus van de vorm $a^2 + b^2$.

Sommen van twee kwadraten

Stelling van Girard (1630)

Elk priemgetal van de vorm $4k+1$ is te schrijven als som van twee kwadraten.

Voorbeelden: $13 = 2^2 + 3^2, 61 = 6^2 + 5^2, 113 = 8^2 + 7^2$, etc.

- Een echt bewijs werd pas geleverd door Euler rond 1740.
- De priemgetallen van de vorm $4k-1$ zijn daarentegen *niet* te schrijven als som van twee kwadraten.
  Voorbeelden: $3, 7, 11, \ldots$
- Reden: een even kwadraat $(2m)^2 = 4m^2$ is deelbaar door 4 en een oneven kwadraat $(2n+1)^2 = 4n^2 + 4n + 1$ is een 4-voud plus 1. Hun som is dus ook 4-voud plus 1.
- A fortiori: geen enkel getal van de vorm $4k-1$ is som van twee kwadraten.
- *Maar*, niet elk getal van de vorm $4k+1$ is som van twee kwadraten. Bijvoorbeeld $21, 33, 57, 77, \ldots$

Kleine stelling van Fermat

Stelling (Fermat)

Gegeven een priemgetal p. Dan geldt voor elk getal a, niet deelbaar door p, dat $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

Een bewijs staat in de voorbereidingstekst van deze cursus.

Stelling

Gegeven een polynoom $f(x)$ van graad d met gehele coefficienten en een priemgetal p. Dan heeft de congruentievergelijking $f(x) \equiv 0 (\mathrm{mod}\ p)$ niet meer dan d oplossingen $a (\mathrm{mod}\ p)$.

NB: Dit geldt *niet* als p geen priem is. Bijvoorbeeld $x^2 - 1 \equiv 0 (\mathrm{mod}\ 24)$ heeft de oplossingen $1, 5, 7, 11, 13, 17, 19, 23 (\mathrm{mod}\ 24)$.

Twee gevolgen van Fermat's stelling

Lemma

Zij p een oneven priemgetal en a, b geheel met $\text{ggd}(a, b) = 1$. Stel dat p een deler is van $a^2 + b^2$. Dan geldt $p \equiv 1 (\text{mod } 4)$.

Voorbeeld: $671^2 + 444^2 = 17 \times 113 \times 337$.
Bewijs Er geldt $a^2 \equiv -b^2 (\text{mod } p)$. Verhef aan beide zijden tot de macht $(p-1)/2$. We krijgen

$$a^{p-1} \equiv (-1)^{(p-1)/2} b^{p-1} (\text{mod } p).$$

Met behulp van Fermat's stelling volgt hieruit
$1 \equiv (-1)^{(p-1)/2} (\text{mod } p)$. Dit kan alleen als $(p-1)/2$ even is, dus $p \equiv 1 (\text{mod } 4)$.

Toepassing (opgave)

Toon aan dat er bij elke $N \geq 2$ een priem $p > N$ bestaat van de vorm $p \equiv 1 (\text{mod } 4)$. (Hint: bekijk $(N!)^2 + 1$)

Bewijs(schets) van de stelling van Girard

Stel p priem met $p \equiv 1 (\mathrm{mod}\ 4)$. De eerste stap is om aan te tonen dat er een *veelvoud* van p is dat geschreven kan worden als som van twee kwadraten met $\mathrm{ggd} = 1$.
Voor elk geheel getal $a = 1, 2, \ldots, p-1$ geldt dat

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$$

deelbaar is door p (kleine stelling van Fermat).
De factor links is deelbaar door p voor hooguit $(p-1)/2$ waarden van a.
Dus is er een getal a zó dat $a^{(p-1)/2} + 1$ deelbaar is door p.
Kies $A = a^{(p-1)/4}$. Dan geldt dat $A^2 + 1$ deelbaar is door p.

Bewijs(schets) van de stelling van Girard

Stel p priem met $p \equiv 1 (\mathrm{mod}\ 4)$. We hebben zojuist gezien dat er een geheel getal A is, zó dat $A^2 \equiv -1 (\mathrm{mod}\ p)$. Bekijk nu de verzameling

$$\Lambda = \{b(A,1) + c(p,0) | b, c \in \mathbb{Z}\}.$$

We noemen een dergelijke verzameling een *rooster* in $\mathbb{Z}^2$. Kies nu $(a,b) \in \Lambda$. Dan geldt dat

$$a^2 + b^2 \equiv (cp + bA)^2 + b^2 \equiv b^2A^2 + b^2 \equiv 0 (\mathrm{mod}\ p).$$

Dus $a^2 + b^2$ is een veelvoud van p.
Kies $(r,s) \in \Lambda$ met $(r,s) \neq (0,0)$ zó dat $r^2 + s^2$ minimaal is. Het blijkt dat $r^2 + s^2$ niet alleen een veelvoud van p is, maar zelfs gelijk er aan.
Hiermee is de stelling van Girard bewezen.