Middelbare schoolmethoden

Frits Beukers

PWN Vakantiecursus voor wiskundeleraren 2023

Priemgetallen van Mersenne

Stelling

Gegeven gehele getallen $a, n \geq 2$. Stel dat $a^n - 1$ priem is. Dan geldt dat $a = 2$ en n is priem.

Voorbeeld met $a = 10$: $10^n - 1 = 999 \cdots 9$ is deelbaar door 9.
In het algemeen is $a^n - 1$ deelbaar door $a - 1$:

$$\frac{a^n - 1}{a - 1} = a^{n-1} + a^{n-2} + \cdots + a + 1.$$

Gevolg: als $a^n - 1$ priem is dan geldt $a = 2$.
Stel nu dat $a = 2$ en $n = rs$ met $r, s > 1$.
Stel $2^n - 1 = (2^r)^s - 1$ priem.
Uit voorgaande volgt dat $2^r = 2$, kan niet omdat $r > 1$.
NB: n priem hoeft niet te impliceren dat $2^n - 1$ priem is.
Bijvoorbeeld $2^{11} - 1$ is niet priem.
Getallen van de vorm $2^n - 1$ heten *Mersenne getallen* en als $2^n - 1$ priem is hebben we een *Mersenne priemgetal*

Perfecte getallen

Pari opgave

De volgende code print de exponenten n van Mersenne priemgetallen voor $n \leq 500$.

```
for(n=2,500,if(isprime(2^n-1),print(n)))
```

Probeer 500 te verhogen en zie wanneer het mis gaat.

Fermat was geinteresseerd in Mersenne priemgetallen vanwege de volgende toepassing op perfecte getallen. Een getal N heet *perfect* als hij gelijk is aan de som van zijn delers $< N$. Voorbeelden, $N = 6, 28, 496, \ldots$

Stelling (Euclides)

Als $2^n - 1$ priem is dan is $2^{n-1}(2^n - 1)$ een perfect getal.

Priemgetallen van Fermat

Stelling

Gegeven gehele getallen $a, n \geq 2$. Stel dat $a^n + 1$ priem is. Dan geldt dat a even is en $n = 2^k$.

Als a oneven zou zijn dan is $a^n + 1$ even. Dus a even.
Stel n oneven, dan

$$\frac{a^n + 1}{a + 1} = a^{n-1} - a^{n-2} + a^{n-3} - \cdots + 1,$$

dus $a^n + 1$ is deelbaar door $a + 1$.
Stel nu dat $n = rs$ met $r > 1$ oneven. Dan is $a^n + 1 = (a^s)^r + 1$ deelbaar door $a^s + 1$. Conclusie $n = 2^k$.
Getallen van de vorm $2^{2^k} + 1$ heten *Fermatgetallen* en *Fermat priemgetal* als het priem is.
De eerste vijf: $5, 17, 257, 65537, 4294967297$, waarvan de eerste vier priem.

Fermat-achtige priemgetallen

Een Fermat-achtig priemgetal is een priemgetal van de vorm $a^{2^n} + 1$ met a even. We gaan er naar op zoek.

Pari opgave

De opdracht

```
for(n=1,10,if(isprime(2^(2^n)+1),print(n))
```

print een lijst van n waarvoor het n-e Fermatgetal priem is. Je kunt de grens 10 iets verhogen, maar PARI geeft het al gauw op vanwege de enorme grootte van de Fermatgetallen.
Herhaal het experiment ook voor andere even grondtallen dan 2

Chebyshev's ongelijkheden

Stelling (Chebyshev, 1850)

Er bestaan positieve getallen α, β zó dat voor voldoend grote x geldt,

$$\alpha \frac{x}{\log x} < \pi(x) < \beta \frac{x}{\log x}.$$

Chebyshev toonde aan dat je $\alpha = 0.82$ en $\beta = 1.11$ kunt nemen.

Wij zullen laten zien dat we $\alpha = 0.66$ kunnen nemen.

Lemma

Voor elk positief geheel getal n geldt $\mathrm{kgv}(1, 2, 3, \ldots, n) \leq n^{\pi(n)}$.

Bewijs: $\mathrm{kgv}(1, 2, 3, \ldots, n)$ is gelijk aan het product van alle priemmachten $p^k \leq n$ waarbij k maximaal gekozen is en $p \leq n$.

$$\text{Voorbeeld:} \quad \mathrm{kgv}(2, \ldots, 10) = 2^3 \times 3^2 \times 5 \times 7.$$

Elk van de $\pi(n)$ factoren is $\leq n$.

Bewijs van Chebyshev's ondergrens

Bekijk de integraal

$$I_n = \int_0^1 x^n(1-x)^n dx.$$

- Omdat $x(1-x) \leq 1/4$ voor $0 \leq x \leq 1$ geldt $I_n < 1/4^n$.
- I_n is de integraal is van een polynoom $a_n x^n + a_{n+1}x^{n+1} + \cdots + a_{2n}x^{2n}$ met gehele coefficienten. Dus

$$I_n = \frac{a_n}{n+1} + \frac{a_{n+1}}{n+2} + \cdots + \frac{a_{2n}}{2n+1} \in \frac{\mathbb{Z}}{\mathrm{kgv}(1, 2, \ldots, 2n+1)}.$$

- Omdat $I_n > 0$ moet gelden dat

$$I_n \geq \frac{1}{\mathrm{kgv}(1, 2, \ldots, 2n+1)}.$$

Combineer de ongelijkheden: $\mathrm{kgv}(1, 2, \ldots, 2n+1) > 4^n$.

Bewijs van Chebyshev's ondergrens

Uit ons Lemma en de zojuist afgeleide $\mathrm{kgv}(1, 2, \ldots, 2n+1) > 4^n$ volgt:

$$(2n+1)^{\pi(2n+1)} > 4^n.$$

Neem de logaritme en deel door $\log(2n+1)$,

$$\pi(2n+1) > \frac{n \log 4}{\log(2n+1)} > 0.66 \frac{2n+1}{\log(2n+1)} \quad \text{als } n > 10.$$

Chebyshev gebruikte dit soort methoden in zijn bewijs van het volgende.

Postulaat van Bertrand

Voor elk geheel getal $n \geq 2$ bestaat er een priemgetal p met $n \leq p < 2n$.

Verscherping postulaat van Bertrand

Uit de priemgetalstelling volgt een sterkere uitspraak.

Stelling

Kies $\epsilon > 0$. Dan geldt voor voldoend grote x dat het interval $[x, (1+\epsilon)x]$ altijd een priemgetal bevat.

Bewijs: We laten zien dat $\frac{\pi((1+\epsilon)x)}{\pi(x)} \to 1+\epsilon$ als $x \to \infty$.

$$\frac{\pi((1+\epsilon)x)}{\pi(x)} \sim \frac{(1+\epsilon)x}{\log((1+\epsilon)x)} \Bigg/ \frac{x}{\log x} \sim 1+\epsilon.$$

Verschillen tussen opeenvolgende priemgetallen

Vraag

Geef de rij opeenvolgende priemgetallen aan met $p_1 = 2, p_2 = 3, p_3, \ldots, p_n, \ldots$. Hoe groot en hoe klein kunnen de verschillen $g_n = p_{n+1} - p_n$ worden?

- Uit het postulaat van Bertrand volgt dat $g_n < p_n$ voor alle n.
- Uit de priemgetalstelling volgt voor elke $\epsilon > 0$ dat $g_n < \epsilon p_n$ mits n groot genoeg is.
- Ingham (1937) Elk interval van de vorm $[N^3, (N+1)^3]$ en N groot genoeg bevat een priemgetal. Dit komt neer op $g_n < 3p_n^{2/3}$.
- Het is niet bekend of elk interval $[N^2, (N+1)^2]$ een priemgetal bevat.
- Het priemtweeling vermoeden komt neer op de vraag of $g_n = 2$ voor oneindig veel n.

Gaten tussen de priemgetallen

In de volgende opgave kun je een indruk krijgen van de gaten tussen opeenvolgende priemgetallen.

Pari opgave

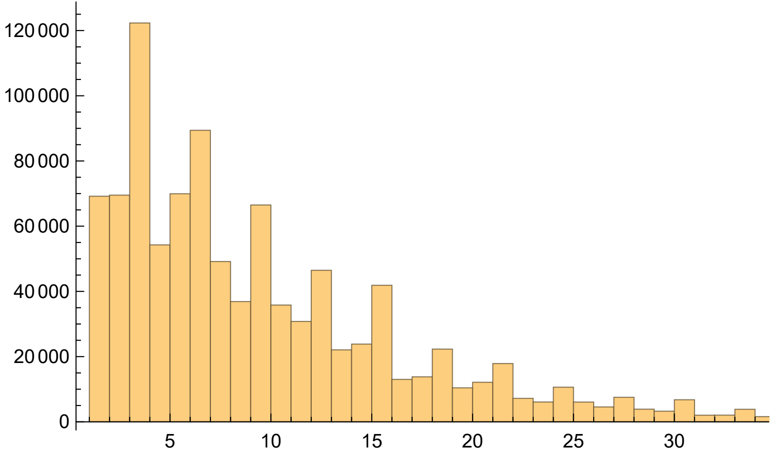
De PARI opdracht `nextprime(n)` geeft het kleinste priemgetal $\geq n$. Voor het kleinste priemgetal met meer dan 100 cijfers: `nextprime(10^100)`. Probeer ook eens wat andere waarden van n. Daarmee krijg je een idee hoe lang het duurt voor je een priemgetal tegenkomt. Vergelijk dit met `log(n)`.
Typ nu de volgende functiedefinitie in:

```
nextprimes(n,k)=q=n;for(m=1,k,q=nextprime(q+1);print(q))
```

De opdracht `nextprimes(10^100,15)` geeft dan de eerste 15 priemgetallen groter dan 10^{100}. Speel een beetje met deze functie om een idee te krijgen van de verschillen tussen heel grote opeenvolgende priemgetallen.

Verschillen tussen opeenvolgende priemgetallen

Histogram van de halve verschillen $(p_{n+1} - p_n)/2$ met $n = 10 \times 10^6, \ldots, 11 \times 10^6$.



NB: $\log(p_{10^7}) \approx 19$

Gaten in de rij priemgetallen

Hier is een rij van $m-1$ opeenvolgende getallen die niet priem zijn:

$$m!+2, m!+3, \ldots, m!+m.$$

Er geldt dat $m > \frac{\log(m!+1)}{\log\log(m!+1)}$. Stel p_n is het grootste priemgetal $\leq m!+1$. Dan geldt $g_n \geq m > \frac{\log(p_n)}{\log\log(p_n)}$.
Tegenwoordig weten we dat $g_n > \log(p_n)$ voor oneindig veel n.

Vermoeden (Cramér, 1936)

Er bestaat een constante C zó dat $g_n < C(\log p_n)^2$ voor alle n

Priemtweelingen zoeken

Tenslotte is hier een programma om priemtweelingen te vinden.

Pari opgave

Type zelf in,

```
nexttwin(n)=q=nextprime(n);
while(!isprime(q+2),q=nextprime(q+1));q
```

`nexttwin(n)` zoekt de kleinste priemtweeling $p, p+2$ met $p > n$ en levert de waarde p. Wat is de kleinste priemtweeling boven 10^{100} ?. Bepaal nog een aantal tweelingen $\geq n$ voor zelfgekozen n. Vergelijk de antwoorden met $(\log n)^2$.

Priemtweelingen zoeken

Pari opgave

We kunnen ook lijstjes opeenvolgende priemtweelingen laten uitprinten.

```
nexttwins(n,k)=q=nexttwin(n);
for(m=1,k,print(q);q=nexttwin(q+1))
```

`nexttwins(n,k)` zoekt de p-waarden van de eerste k priemtweelingen met $p > n$ en print ze uit. Probeer eens `nexttwins(10^100,15)` en bekijk de achtereenvolgende verschillen. Neem ook wat andere waarden van n.

Palindroompriemgetallen

Pari opgave

Een getal zoals 1251521 of 113311 noemt men een palindroom getal. Bepaal met PARI een aantal grote palindroom priemgetallen. De rep-unit met 19 of 23 enen is een voorbeeld daarvan. Of 32000000023. Palindroompriempriemgetallen hebben altijd een oneven aantal cijfers, behalve 11. Om je op gang te helpen een loop:

```
for(a=1,9,for(b=1,9,
if(isprime((a+10*b)*10^19+(b+10*a)),print(a+10*b))))
```

De exponent 19 kun je door ieder ander oneven getal vervangen. Maar niets houdt je tegen om ook andere mogelijkheden te proberen.