Primtal - hvor mange, hvordan og hvorfor?

Johan P. Hansen [1]

[1] Institut for Matematiske Fag, Aarhus Universitet

Gult foredrag, EULERs Venner, oktober 2009

Disposition

EUKLIDs bevis

Sætning (EUKLIDs sætning)

Der er uendelig mange primtal.

Bevis.

Lad $p_1, p_2, \ldots, p_j$ være primtal. Så er

$$p_1 \cdot p_2 \cdot \cdots \cdot p_j + 1$$

et tal, der har en primdivisor $p \notin \{p_1, p_2, \ldots, p_j\}$. Heraf følger straks, at der må være uendelig mange primtal! □

FERMAT-tal

FERMAT-tal

$$F_n := 2^{2^n} + 1$$

Eksempler

$$F_1 = 5, F_2 = 17, F_3 = 257, F4 = 65537$$

- FERMAT troede, at alle F_n er primtal. Deri havde han ikke ret; EULER fandt i 1732, at $F_5 = 641 \cdot 6700417$.
- GAUSS viste, at hvis F_n er et primtal p, så kan en regulær p-kant konstrueres med passer og lineal.

Bevis baseret på FERMAT-tal

Sætning (EUKLIDs sætning)

Der er uendelig mange primtal.

Bevis.

Følger umiddelbart af følgende lemma - hvert FERMAT-tal har jo mindst en primdivisor, der ikke er divisor i noget andet FERMAT-tal. □

Lemma

To Forskellige FERMAT-tal er indbyrdes primiske.

Bevis.

For $k > 0$ og $x = 2^{2^n}$ er

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{x^{2k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1,$$

et helt tal og vi slutter, at

$$F_n | F_{n+k} - 2.$$

En fælles divisor i F_n og F_{n+k} er altså også en divisor i 2 - altså 1 eller 2; men FERMAT-tallene er ulige, så den fælles divisor må være 1. □

EULERs bevis

Sætning (EUKLIDs sætning)

Der er uendelig mange primtal.

Bevis.

Antag $p_1, p_2, \ldots, p_j$ er SAMTLIGE primtal. For $x, n \in \mathbb{N}, n \leq x$:

$$n = {n_1}^2 \cdot m, \quad m = 2^{b_1} \cdot 3^{b_2} \cdot \ldots {p_j}^{b_j}, \quad b_j \in \{0, 1\}$$

Der er højest 2^j muligheder for m. Da $n_1 \leq \sqrt{n} \leq \sqrt{x}$ er der højest $\sqrt{x}$ muligheder for n_1. Ialt højest $2^j\sqrt{x}$ muligheder for n:

$$x \leq 2^j\sqrt{x},$$

hvilket IKKE er sandt for store x, altså modstrid! □

EULERs bevis - efterskrift

Sætning (EULER)

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

Bevis.

Essensen ovenfor i EULERs bevis for EUKLIDs sætning kan udvides til at vise påstanden. □

GAUSS - HADAMARD - D. L. VALLEE POUSSIN

Lad $\pi(x)$ betegne antallet af primtal $p \leq x$ for $x \in \mathbb{R}$.
Eksempelvis er $\pi(10) = 4$. Primtalssætningen siger, at

$$\pi(x) \sim \frac{x}{\ln x}$$

C. F. GAUSS fremsatte i 1973 denne formodning som 15-årig på baggrund af observationer!
Lidt mere præcist siger primtalssætningen:

$$\frac{\pi(x)}{\frac{x}{\ln x}} \to 1 \quad \text{for} \quad x \to \infty$$

og den indeholder vurderinger af fejlmargin.
Bevist i 1896 af J. HADAMARD og C. DE LA VALLEE POUSSIN via analytiske metoder (Riemanns ζ-funktion) - senere er der givet elementære beviser.

CHEBYCHEVs sætning

CHEBYCHEV beviste før primtalssætningen var vist følgende:

Sætning

For store x er

$$0,9\,\frac{x}{\ln x} < \pi(x) < 1,1\,\frac{x}{\ln x}$$

Et kort (2 sider) elementært bevis af sætningen findes på
`http://www.jstor.org/pss/2322510`

Anvendelse af CHEBYCHEVs sætning

For at estimere antallet af primtal med 100 cifre anvender vi CHEBYCHEVs sætning:

$$0,9\ \frac{10^{99}}{99 \cdot \ln 10} < \pi(10^{99}) < 1,1\ \frac{10^{99}}{99 \cdot \ln 10}$$

$$0,9\ \frac{10^{100}}{100 \cdot \ln 10} < \pi(10^{100}) < 1,1\ \frac{10^{100}}{100 \cdot \ln 10}$$

Herved kan vi estimere, at antallet af primtal med netop 100 cifre er mellem $3,42 \cdot 10^{97}$ og $4,38 \cdot 10^{97}$ svarende til at mellem $0,38$ % og $0,48$ % af alle tal med netop 100 cifre er primtal.

FERMATs lille sætning

Sætning

Lad p være et primtal og lad a være primisk med p, altså $\mathrm{sfd}(a, p) = 1$*, så er*

$$a^{p-1} \equiv 1 \mod p.$$

Det giver grundlaget for en metode til at afprøve, om et n er et primtal. Metoden er imidlertid langt fra sikker.
Vi kan ikke af, at

$$a^{n-1} \equiv 1 \mod n,$$

for et a med $\mathrm{sfd}(a, n) = 1$ slutte, at n er primtal. Det mindste tal, hvor der kommer en FALSK positiv, er $n = 341 = 11 \cdot 31$ med $a = 2$.

pseudo-primtal

Definition

Lad n være et naturligt og lad a være primisk med n, altså $\mathrm{sfd}(a, n) = 1$. Hvis

$$a^{n-1} \equiv 1 \mod n$$

kaldes n et pseudo-primtal med hensyn til basen a.

For ethvert a er der uendelig mange pseudo-primtal med hensyn til base a.
Der er (Carmichael) tal - det er pseudo-primtal for alle a, der er primiske med n. Det mindste er $561 = 3 \cdot 11 \cdot 17$. Faktisk er der uendelig mange (vist i 1994): For store n er der mindst $n^{2/7}$ Carmichael tal mellem 1 og n.

En videreudvikling af FERMATs lille sætning

Sætning

Lad $p \neq 2$. Lad p være et primtal og lad a være primisk med p, altså $\mathrm{sfd}(a, p) = 1$.
Lad $p - 1 = 2^s d$, hvor $1 \leq s$ og d ulige.
Enten er

$$a^{\,d} \equiv 1 \mod p$$

eller også findes der et r med $0 \leq r < s$, så

$$a^{\,2^r d} \equiv -1 \mod p.$$

Bevis.

Vælg det mindste k med $0 \leq k \leq s$, så

$$a^{2^k d} \equiv 1 \mod p.$$

Der findes et k, f. eks. $k = s$, jvf. FERMATs lille sætning. Hvis $k = 0$ er vi i det første tilfælde og er færdige. Hvis $k > 0$ betragter vi $b = a^{2^{k-1} d}$:

$$b^2 \equiv a^{2^k d} \equiv 1 \mod p \Rightarrow b \equiv \pm 1 \mod p.$$

$b \equiv a^{2^{k-1} d} \neq 1 \mod p$ på grund af minimaliteten af k, derfor er $b \equiv a^{2^{k-1} d} = -1 \mod p$ og vi vælger $r = k - 1$. □

Stærke pseudo-primtal

Definition

Lad $n \neq 2$ være et naturligt tal, der ikke er et primtal, og lad a være primisk med n, altså $\mathrm{sfd}(a, n) = 1$.
Lad $n - 1 = 2^s d$, hvor $1 \leq s$ og d ulige. Hvis enten

$$a^d \equiv 1 \mod n$$

eller der findes et r med $0 \leq r < s$, så

$$a^{2^r d} \equiv -1 \mod n,$$

så kaldes n er stærkt pseudo-primtal med hensyn til basen a.

$n = 2047 = 23 \cdot 89$ er et stærkt pseudo-primtal med $a = 2$. For ethvert $a \geq 2$ er der uendelig mange stærke pseudo-primtal med hensyn til basen a!

RABINs sætning - 1996

Sætning

Antag at n ikke er et primtal. Antallet af baser a, hvori n er et stærkt pseudo-primtal er højest:

$$\frac{1}{4}(n-1).$$

RABINs test

Sandsynligheden for at et n, der ikke er et primtal, er et pseudo-primtal for k tilfældigt valgte baser a er altså højest:

$$\frac{1}{4^k}.$$

Det er grundlaget for RABINs test, hvormed vi med stor sikkerhed kan producere store primtal (med for eksempel 100 cifre).
Vælges $k = 30$ er risikoen for en FALSK positiv af en test af et tilfældigt tal højest

$$\frac{1}{4^{30}},$$

hvilket er mindre end 1 ud af 1 000 000 000 000 000 000 gange!