

**Primtalsfaktorisering -
nogle nye resultater og anvendelser**
Regionalmøde Haderslev, 19. november 2003
<http://home.imf.au.dk/matjph/haderslev.pdf>

Johan P. Hansen,
matjph@imf.au.dk
Matematisk Institut, Aarhus Universitet

26. november 2003

Resumé

Udgangspunktet vil være aritmetikkens fundamentalsætning om entydig faktorisering af hele tal i produkter af primtal. I tilknytning hertil behandler vi primtalstest - herunder det nye resultat fra 2002: ”*Primes is in P*”, altså at der findes en algoritme, der i polynomiell tid bestemmer, hvorvidt et helt tal er et primtal.

Dernæst vil vi anvende primtal og primtalsfaktoriseringer til at beskrive og gennemgå offentlig nøgle kryptosystemet RSA.

Endelig vil vi behandle faktoriseringsteori i en mere generel sammenhæng og forsøge at knytte det til aktuel matematisk forskning.

I et vist omfang knytter foredraget sig til bogen *Algebra og Talteori*, GYLDENDAL, 2002, hvortil der henvises for detaljer.

Aritmetikkens fundamentalsætning

Hvad er et primtal p ? Kan udtrykkes på to ækvivalente måder:

- p har kun de trivielle divisorer $\pm 1, \pm p$
- p har egenskaben: $p|m \cdot n \Rightarrow p|m \vee p|n$

Sætning 1. Aritmetikkens fundamentalsætning. *Ethvert $m > 1$ kan faktoriseres i et produkt af primtal:*

$$m = p_1 \cdot \dots \cdot p_k.$$

Faktoriseringen er entydig. Hvis p_1, \dots, p_k og q_1, \dots, q_l er primtal med

$$p_1 \cdot \dots \cdot p_k = q_1 \cdot \dots \cdot q_l,$$

så er $k = l$ og $p_i = q_i$ efter ombytning.

Se [5], side 21. Eksistensdelen er IKKE konstruktivt. Dette er sikkerheden i RSA kryptosystemet.

Korollar 1. *Der er uendelig mange primtal.*

Bevis. (Euclid) Antag p_1, \dots, p_k er samtlige primtal. Betragt tallet

$$p_1 \cdot \dots \cdot p_k + 1.$$

Det kan ikke være et primtal, det er jo forskellige fra alle p_i . Tallet ikke have en primtalsdivisor, intet p_i er jo en divisor. Tallet har åbenbart ingen primtalsfaktoriserings og vi har en modstrid. □

Bemærk igen, beviset er IKKE konstruktivt og giver ikke en metode til at bestemme primtallene.

Verdens størst kendte primtal er $2^{13466917} - 1$, et tal med 4.053.946 decimaler.

Er det svært at afgøre om et tal er et primtal?

Carl Friedrich Gauss skrev i *Disquisitiones Arithmeticae* i 1801 [3]:

The problem of distinguishing prime numbers from composite numbers and to resolve the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. ... Further, the dignity of the science itself seems to require that every possible means be explored for the solution to the problem so elegant and so celebrated. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and prolix that these methods do not apply at all to larger numbers.

**Er det svært at afgøre om et tal er et primtal?
(Den trivielle metode).**

Man kunne jo prøve sig frem med at finde divisorer fra en ende af.

Lad os sige, at tallet m har 200 cifre og lad os antage at et divisionscheck tager 10^{-6} sek. Et fuldstændigt gennemløb af alle tal op til \sqrt{m} tager så

$$10^{100} \cdot 10^{-6} \text{sek.} \sim 3 \cdot 10^{86} \text{år}$$

Det er lang tid, universets alder anslås at være $18 \cdot 10^{12}$ år med en usikkerhed på $3 \cdot 10^{12}$ år.

Generelt er der $\log m$ cifre i tallet m og under den samme antagelse om regnetid som ovenfor vil et fuldstændigt gennemløb af alle tal op til \sqrt{m} tage

$$10^{\frac{\log m}{2}} \cdot 10^{-6} \text{sek.}$$

Regnetiden vokser altså **eksponentielt** i antallet af cifre $\log m$.

Er det svært at afgøre om et tal er et primtal?

Eratosthenes si.

Metode ovenfor er i raffineret form Eratosthenes si (240 f. kr.).

I talrækken:

$$2, 3, \hat{4}, 5, \hat{6}, 7, \hat{8}, 9, \dots, m$$

udtages det mindste tal 2 og alle egentlige multipla af 2 bortsies:

$$3, 5, 7, \hat{9}, 11, \dots, m$$

dernæst udtages 3 i listen og alle egentlige multipla af det 3 bortsies:

$$5, 7, 11, \dots, m$$

Således fortsættes succesivt med at udtage det mindste tal i listen og bortsi egentlige multipla heraf. Når processen stander, har vi udtaget alle primtal mindre end eller lig m .

Fermats lille sætning giver en primtalstest.

Gauss indførte i [3] *modulus* begrebet, altså regning med kongruenser og rester. I [5] behandles det i kapitel 3. Fermats lille sætning behandles side 35.

Sætning 2. Fermats lille sætning. *Lad p være et primtal. Så gælder, at*

$$a^p \equiv a \pmod{p},$$

altså a^p og a har sammen rest ved division med p . Hvis p ikke går op i a gælder, at

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

Bevis. For $a \neq 0$, se på produkterne

$$1 \cdot \dots \cdot (p-1) \quad , \quad (a \cdot 1) \cdot \dots \cdot (a \cdot (p-1)).$$

Da de modulo p blot adskiller sig ved en permutation af faktorerne, må de være ens og resultatet følger ved forkortning. For $a = 0$ er påstanden trivielt. □

Fermats lille sætning giver en primtalstest - men den er ikke sikker.

Testen er imidlertid ikke sikker! Der er såkaldte **pseudoprimaltal**, altså tal, for hvilke Fermats lille sætning er sand for $a = 2$.

$$2^{341} = (2^{10})^{34} \cdot 2 \equiv 2 \pmod{341},$$

idet

$$2^{10} = 1024 \equiv 1 \pmod{341}.$$

MEN 341 er ikke et primtal

$$341 = 11 \cdot 31.$$

Bemærk, at

$$n \text{ pseudoprimaltal} \Rightarrow 2^n - 1 \text{ pseudoprimaltal}.$$

Der er altså uendelig mange pseudoprimaltal.

Et tal, der ikke er et primtal, for hvilket Fermats lille sætning er sand for alle valg af a kaldes et **Carmichael tal**. Eksempler er 561, 1729 og 2821. Først så sent som i 1992 blev der vist, at der er uendelig mange Carmichael tal.

Er det svært at afgøre om et tal er et primtal?

I 2002 viste Agrawal, Kayal og Saxena fra Indien, at det kan gøres i polynomiell tid, se [1].

Første del er en generalisering af Fermats lille sætning og tilhørende test. Nu fås et helt sikkert kriterium for om et givet tal er et primtal.

Sætning 3. *Lad a være indbyrdes primisk med n . Så er n et primtal, hvis og kun hvis*

$$(X - a)^n \equiv (X^n - a^n) \pmod{n}, \quad (1)$$

i polynomiumsringen $\mathbb{Z}[X]$. Altså hvis og kun hvis polynomierne $(X - a)^n$ og $X^n - a^n$ har samme rest modulo n .

Bemærkning. Det er her vigtigt, at fremhæve at beregningen foregår i polynomiumsringen $\mathbb{Z}[X]$ og at de to polynomier i (1) er ens \pmod{n} , hvis og kun hvis de har de samme koefficienter \pmod{n} .

Eksempel 1. For primtallet $p = 23$ får vi:

$$\begin{aligned}(X - 1)^{23} &= \\ &X^{23} - 23 X^{22} + 253 X^{21} - 1771 X^{20} + 8855 X^{19} - 33649 X^{18} \\ &+ 100947 X^{17} - 245157 X^{16} + 490314 X^{15} \\ &- 817190 X^{14} + 1144066 X^{13} - 1352078 X^{12} + 1352078 X^{11} \\ &- 1144066 X^{10} + 817190 X^9 - 490314 X^8 + 245157 X^7 \\ &- 100947 X^6 + 33649 X^5 - 8855 X^4 + 1771 X^3 - 253 X^2 + 23 X - 1 \\ &\equiv X - 1 \pmod{23}\end{aligned}$$

Eksempel 2. For det sammensatte tal $n = 24 = 2^3 \cdot 3$ får vi:

$$(X - 1)^{24} =$$

$$\begin{aligned} & 1 - 24 X + 276 X^2 - 2024 X^3 + 10626 X^4 - 42504 X^5 + 134596 X^6 \\ & - 346104 X^7 + 735471 X^8 - 1307504 X^9 + 1961256 X^{10} - 2496144 X^{11} \\ & + 2704156 X^{12} - 2496144 X^{13} + 1961256 X^{14} - 1307504 X^{15} \\ & + 735471 X^{16} - 346104 X^{17} + 134596 X^{18} - 42504 X^{19} + 10626 X^{20} \\ & - 2024 X^{21} + 276 X^{22} - 24 X^{23} + X^{24} \end{aligned}$$

\equiv

$$\begin{aligned} & 1 + 12 X^2 + 16 X^3 + 18 X^4 + 4 X^6 + 15 X^8 + 16 X^9 + 4 X^{12} \\ & + 16 X^{15} + 15 X^{16} + 4 X^{18} + 18 X^{20} + 16 X^{21} + 12 X^{22} + X^{24} \end{aligned}$$

mod 24

Bevis. Med binomialformlen fås:

$$(X - a)^n - (X^n - a^n) = \sum_{i=1}^{n-1} (-1)^i \binom{n}{i} a^{n-i} x^i = \sum_{i=1}^{n-1} (-1)^i \frac{(i+1) \cdots n}{1 \cdots (n-i)} a^{n-i} x^i.$$

Hvis n er et primtal, er n en divisor i alle koefficienterne på højresiden og vi er færdige. Antag omvendt at $n = q^k \cdot d$ er sammensat, hvor q er et primtal og ikke en divisor i d .

Se nu på koefficienten

$$\binom{n}{q} = \frac{(q^k d - q + 1) \cdots q^k d}{1 \cdots (q)}.$$

Heraf ses, at q^k ikke går op i $\binom{n}{q}$ og da q^k er indbyrdes primisk med a^{n-q} er koefficienten til X^q

$$(-1)^q \binom{n}{q} a^{n-q} \not\equiv 0 \pmod{q^k}$$

□

Ovenstående elegante primtals kriterium er næppe til umiddelbar nytte. For store n er det umuligt at beregne $(X - a)^n$, faktisk kræver det mere tid end Erathostenes si beregningen.

Ideen er nu istedet

- a) i polynomiell tid at beregne resten af $(X - a)^n$ ved polynomiers division med polynomiet $X^r - 1$ for et passende r , altså at undersøge om

$$(X - a)^n \equiv (X^n - a^n) \pmod{(n, X^r - 1)}$$

- b) at undersøge om sætningen ovenfor overlever i en eller anden form i termer af ovenstående noget svagere kriterium.

Kriteriet overlever i følgende form,

Sætning 4 (Agrawal-Kayal-Saxena). *Antag $s \leq n$. Vælg primtal q og r så $q|(r-1)$, $n^{(r-1)/q} \not\equiv 0, 1 \pmod{r}$ og*

$$\binom{q+s-1}{s} \geq n^{2\lfloor\sqrt{r}\rfloor}.$$

Hvis vi for alle $1 \leq a < s$ har, at

- *a er indbyrdes primisk med n , og*
- $(X - a)^n \equiv (X^n - a) \pmod{(n, X^r - 1)}$,

så er n en primtalspotens.

Polynomiel tid: der findes et tal k og en algoritme, der for ethvert naturligt tal n i $O(\log^k n)$ trin afgør om tallet er et primtal eller ej. AKS-algoritmen og efterfølgende forfininger afgør det i $O(\log^{7,5} n)$ trin, se http://www.cse.iitk.ac.in/news/primality_v3.pdf

Offentlig nøgle kryptering

Cæsars udviklede et krypteringssystem, hvor man erstattede hvert bogstav i den oprindelige tekst med det bogstav, der står 3 pladser længere fremme i alfabetet. Der dekrypteres ved at forskyde 3 pladser til venstre. Der er altså ingen principiel forskel på at kryptere og dekryptere. Det er et **1-nøglesystem**.

I 1976 lancerede Diffie og *Hellman* et nyt koncept - et **2-nøglesystem**:

Alice fremstiller to nøgler:

- en hemmelig som kun hun kender, den kalder vi S_A ,
- en offentlig, som alle kender, den kalder vi P_A .

De to nøgler spiller sammen således, at S_A låser og P_A låser op igen - og omvendt. Tilsvarende har Bob lavet sig et nøglepar (P_B, S_B) .

Hemmeligholdelse

Alice sender en hemmelig meddelelse M til Bob ved at kryptere meddelelsen med Bobs offentlige nøgle og sende

$$P_B(M).$$

Bob anvender sin hemmelige nøgle S_B på det modtage

$$S_B(P_B(M)) = M$$

og får M ud, da nøglerne ophæver hinanden.

Bob kan imidlertid ikke vide, hvem afsenderen er, alle kender jo hans offentlige nøgle.

Dette kan vi sikre ved **digital signatur**, som 2-nøglesystemmet også giver.

Digital Signatur

Hvis Alice sender

$$S_A(M)$$

til Bob, kan Bob være sikker på, at meddelelsen kommer fra Alice, hvis han kan få M ud ved at udregne

$$P_A(S_A(M)).$$

Det er nemlig kun Alice, der har den hemmelige nøgle S_A , der passer med den offentlige nøgle P_A . Alice har altså fået sat sin underskrift på M .

Hemmeligholdelse og Digital Signatur

Skal M samtidig holdes hemmelig, sender Alice blot

$$P_B(S_A(M)).$$

Bob er den eneste, der kan finde M ved at udregne

$$P_A(S_B(P_B(S_A(M)))).$$

RSA

Diffie og *Hellman* gav ikke noget svar på om det er muligt konkret at lave et 2-nøglesystem.

Kravet er, at det skal være (så godt som) umuligt at bestemme den hemmelige nøgle ud fra den offentlige.

De tre matematikere *Rivest*, *Shamir* og *Adleman* konstruerede i 1977 et 2-nøglesystem, hvis sikkerhed beror på at det er (så godt som) umuligt at faktorisere et helt tal i et produkt af primtal.

Lad $\mathbb{Z}/m\mathbb{Z}$ være de m restklasser mod m . Afbildningen

$$\begin{aligned}\mathbb{Z}/m\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \\ a &\mapsto a^k \pmod{m}\end{aligned}$$

er udgangspunktet. Dens **inverse afbildning?**

Eulers $\varphi(m)$ -funktion:

$$\varphi(m) = \#\{k \mid 1 \leq k < m, \text{ hvor } k \text{ og } m \text{ indbyrdes primiske}\}$$

Centrale bemærkninger:

- $\varphi(pq) = (p - 1)(q - 1)$, hvis p, q er to forskellige primtal.
- $\varphi(m)$ kan ikke beregnes uden at kende en **primtalsfaktorisering** af m .

Sætning 5. Eulers sætning. *Antag, at a er primisk med m . Der gælder, at*

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

altså, at $a^{\varphi(m)}$ har rest 1 ved division med m .

Bevis. Efter samme ide som beviset for Fermats lille sætning. Se f.eks. [5],
Kap. 5. □

Vi kan nu bestemme den inverse til $a \mapsto a^k \pmod{m}$

- bestem ved hjælp af Euklids algoritme tal u, v , således at

$$ku - \varphi(m)v = 1, \text{ Bezouts identitet, jvf. [5], side 15,}$$

idet det er forudsat, at k og $\varphi(m)$ er indbyrdes primiske.

- noter, at

$$(a^k)^u = a^{\varphi(m)v+1} = \left(a^{\varphi(m)}\right)^v \cdot a \equiv a \pmod{m}$$

ifølge Eulers sætning.

Konklusionen er, at afbildningerne

-

$$\mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$$

$$a \mapsto a^k \pmod{m}$$

$$b \mapsto b^u \pmod{m}$$

er hinandens inverse,

- MEN bestemmelse af den inverse forudsætter kendskab til primtalsfaktoriseringen af m .

RSA nøglerne.

I notationen ovenfor lader vi

- Offentlige nøgle være : (k, m) og
- Private nøgle være: u

Eksempel.

$p = 3, q = 11$ giver $m = 33$ og $\varphi(3 \cdot 11) = 20$. Med $k = 3$, løser $u = 7$ ligningen:

$$3 \cdot u - 20 \cdot v = 1.$$

Meddelelsen 9 krypteres til $9^3 = 729 \equiv 3 \pmod{33}$, som dekrypteres til $3^7 = 2187 \equiv 9 \pmod{33}$.

I praksis bruges store primtal så m er af størrelsesordenen mindst 2^{512} eller har mere end 154 cifre.

Når du benytter dit DANKORT, skal du først indtaste din 4-cifrede PIN-kode, der herefter verificeres. Det sker ikke i de enkelte terminaler, men centralt. Dette kræver, at PIN-koden holdes hemmelig under hele processen. Det sker gennem RSA.

Faktoriseringsteori

Vi har lige set og udnyttet, at de hele tal \mathbb{Z} har entydig faktorisering.

Det samme er tilfældet for den Gaussiske talring $\mathbb{Z}[i]$ og $\mathbb{Z}[\xi]$, hvor $\xi^3 = 1$, jvf. [5], Kap. 11 og 13.

Imidlertid har ikke alle ringe entydig faktorisering. I $\mathbb{Z}[i\sqrt{5}]$ gælder således, at

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

I $\mathbb{Z}[\xi]$, hvor $\xi^p = 1$, er der ikke generelt entydig faktorisering. Antaget ”Entydighed” af faktoriseringen:

$$z^p = x^p + y^p = (x + y)(x + \xi y) \cdots (x + \xi^{p-1}y),$$

var fejlen i Lames bevis i 1847 for Fermats sidste sætning. (Der er faktisk ikke entydig faktorisering for uendelig mange primtal p , det første er $p = 23$, jvf. Kummer).

Faktoriseringsteori er via klasselegemesteori indlejret i det såkaldte **Langlands program**, jvf. [4], som L. Lafforque, IHES, Paris i 2000 fik Fields medaljen for at have gennemført væsentlige dele af.

Litteratur

- [1] M. Agrawal, N. Kayal and N. Saxena, “PRIMES is in P,” Preprint Indian Institute of Technology Kanpur, INDIA, Aug. 2001.
- [2] F. Bornemann, “PRIMES is in P: A Breakthrough for ”Everyman”,” Preprint Indian Institute of Technology Kanpur, INDIA, Aug. 2001.
- [3] C. F. Gauss, “Disquisitiones arithmeticae,” 1801. Optrykt i *Werke*, Königl. Gesellsch. d. Wissensch. zu Göttingen (Leipzig-Berlin, 1863-1933).
- [4] S. Gelbart, “An elementary Introduction to the Langlands Program,” *Bulletin of the American Mathematical Society*, 10 (1984), 177-218.
- [5] Johan P. Hansen og Henrik G. Spalk, “Algebra og talteori,” Aspekt Serien, Gyldendal, 2002