

Deling - primtal - kryptografi

Johan P. Hansen

14. november 2011

Indhold

1	Indledning	2
2	Primtal og heltalsdeling	3
2.1	Primtalsfaktorisering	4
2.1.1	Primtalsfaktoriseringens tidsforbrug	5
2.1.2	Om éntydhedsdelen af aritmetikkens fundamentalsætning	5
3	Uendelig mange primtal - Euklids sætning	6
3.1	Tre forskellige beviser for Euklids sætning	6
3.1.1	Euklids bevis	6
3.1.2	Bevis baseret på Fermat-tal	6
3.1.3	Eulers bevis	7
4	Optælling af primtal - primtalsætningen	8
4.1	Chebychevs sætning	9
4.1.1	Antal primtal med netop 100 cifre - estimat.	9
5	Landaus primtalsproblemer	9
5.1	Goldsbachs formodning	10
5.2	Formodningen om primtalstvillinger	10
5.2.1	Hardy-Littlewood formodningen	11
5.3	$N^2 + 1$ formodningen	11
5.4	Legendres formodning	11
6	Mersenne primtal - de størst kendte primtal	12
6.1	Mersenne primtal og perfekte tal	12
7	Kongruenser og potenser	13
7.1	Fermats lille sætning	14
7.2	Eulers sætning	15
7.2.1	Uddragning af rødder modulo m	16
7.3	Primtalstest	17

7.3.1	Pseudo-primtal	18
7.3.2	Rabin-Millers primtalstest - konstruktion af sandsynlige primtal	18
8	Offentlig nøgle kryptografi - RSA kryptografi - hemmelig kommunikation og digital underskrift	19
8.1	Offentlig-nøgle-kryptosystemet RSA	20
9	Appendiks	21
9.1	Gentagen kvadrering	21
9.2	Euklids algoritme og Bezouts identitet	22
	Litteratur	23
	Indeks	26

1 Indledning

Deling af tal er det overordnede tema. Tallet 60 kan deles i $60 = 4 \cdot 15$, som videredeles til:

$$60 = 2 \cdot 2 \cdot 3 \cdot 5 ,$$

hvorefter yderligere deling er umulig. Dette simple eksempel giver anledning til en række klassiske og forskningsaktuelle spørgsmål, hvis besvarelse også har stor praktisk betydning:

- Kan ethvert tal i lighed med 60 deles i et produkt af tal, der ikke kan yderligere deles? Kan en deling kun foretages på én måde? JA - aritmetikkens fundamental-sætning, der behandles i afsnit 2.1, præciserer og besvarer begge spørgsmål positivt.
- Er det hurtigt at dele et tal i sine faktorer? NÆPPE - men der er ikke et definitivt svar. Temaet, der behandles i afsnit 2.1.1, er helt centralt i moderne kryptografi, jvf. afsnit 8.1.
- Er der uendelig mange tal, der i lighed med 2,3 og 5 er udelelige? JA - bevises i afsnit 3.1 på tre forskellige måder.
- Kan man anslå, hvad chancen er for, at et tilfældigt valgt tal er udeleligt? JA - primtalssætningen, der behandles i afsnit 4, giver estimer. I nærheden af $n = 1.000$ er cirka hvert syvende tal udeleligt og i nærheden af $10.000.000.000$ er omkring 1 ud af 23 tal udeleligt.
- Kan man afgøre om et konkret tal er udeleligt, eller i det mindste med meget stor sandsynlighed er udeleligt? JA - i afsnit 7.3.2 beskrives en gennemførlig test, der med en fejl på mindre end 1 ud af $1.000.000.000.000.000.000$ afprøver om et givet tal er udeleligt.

- Ved man alt om tal, der ikke kan deles? NEJ - i afsnit 5 behandles fire klassiske og stadig uløste problemstillinger.
- Kan *delelighed* anvendes i praksis? JA - det er kernen bag sikkerheden i offentlig-nøgle-kryptosystemet RSA, jvf. afsnit 8.1.

Hensigten er at uddybe disse spørgsmål og give præcise svar, såvidt det er muligt, belyst såvel igennem den klassiske viden som ved aktuell matematisk forskning. Et yderligere sigte er anvendelsen i moderne kryptografi.

2 Primaltal og heltalsdeling

Talteori er grundlæggende studiet af de *naturlige* tal:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22,

Nogle af matematikkens vanskeligste og stadig uløste problemer knytter sig til dem.

I listen overfor er nogle tal fremhævet med rødt, det er primtallene, altså de udelelige tal.

Definition 1 (Primaltal). Et naturligt tal større end 1 kaldes et *primaltal*, hvis det ikke kan deles med andre naturlige tal end 1 og tallet selv.

Eratosthenes si er en antik græsk metode til at lave lister over primaltal. Ideen er at skrive de naturlige tal større end lig med 2 i en lang række, markere det mindste tal 2 og sies alle multipla af 2 væk. I restrækken markeres det mindste tal 3 og alle dets multipla sies bort. Sådan sies videre og tilbage i sien, er der kun primtallene:

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
2	3		5		7		9		11		13		15		17		19		21
2	3		5		7				11		13				17		19		

Et primaltal har en helt særlig egenskab - deler det et produkt, deler det en af faktorerne. Det samme er ikke tilfældet for alle tal, for eksempel deler 6 tallet $12 = 3 \cdot 4$; men det deler hverken 3 eller 4. Et primaltal er defineret udfra hvilke tal, der deler det - en påstået egenskab om det at dele andre tal kræver et matematisk bevis.

Sætning 2 (Primtalsegenskaben). *Lad p være et primaltal og lad m, n være naturlige tal. Antag at p går op i produktet $m \cdot n$, så går p op i enten m eller n . Mere generelt, hvis et primaltal går op i et produkt, så går det op i en af faktorerne.*

Bevis. Lad primtallet p dele produktet $m \cdot n$. Hvis p deler n , er vi færdige. Antag derfor, at p ikke deler n - så er 1 det eneste tal, der deler såvel n som p , hvorfor der ifølge Sætning 3 nedenfor findes hele tal x, y , så

$$nx + py = 1 .$$

Efter multiplikation af ligningen med m fås, at

$$mnx + mpy = m . \tag{1}$$

Tallet p deler ifølge antagelsen mn og dermed venstresiden af (1), altså også højresiden m , og vi er færdige. \square

Et meget nyttigt resultat, som vi allerede brugte ovenfor, om det største naturlige tal, der deler to tal, rummes i den følgende sætning, der vises i 9.2.

Sætning 3 (Største fælles deler (divisor), Euklids¹ algoritme og Bezouts² identitet). *Lad m, n være to naturlige tal og lad $\text{sfd}(m, n)$ betegne deres største fælles deler (divisor), altså det største naturlige tal, der deler såvel m som n . Der findes hele tal x, y , så*

$$mx + ny = \text{sfd}(m, n) .$$

Den største fælles deler (divisor) $\text{sfd}(m, n)$ og tallene x, y bestemmes effektivt med Euklids algoritme.

2.1 Primtalsfaktorisering

Sætning 4 (Aritmetikens fundamentalsætning). *Ethvert naturligt tal større end 1 kan skrives som et produkt³ af primtal på en entydig måde i den forstand at enhver primfaktor indgår et entydigt antal gange i faktoriseringen.*

Bevis. Sætningen rummer faktisk to dele - en eksistensdel og en entydighedsdel.

Eksistens. Antag modsætningsvis, at der findes et naturligt tal større end 1, der ikke kan skrives som et produkt af primtal. Lad n være det mindste sådanne tal. Tallet n kan ikke være et primtal, så ville det jo være faktoriseret i et produkt af primtal med kun én faktor. Derfor findes et d , forskellig fra 1 og n , som er en divisor i n .

$$n = q \cdot d . \tag{2}$$

Såvel d som q har imidlertid faktoriseringer i produkter af primtal, idet $1 < d < n$ og $1 < q < n$ og n er valgt minimal med den egenskab ikke at have primtalsfaktoriseringer. Af (2) følger, at også n kan primtalfaktoriseres ved at samle faktoriseringerne af q og d . Hermed er der opnået en modstrid. Konklusionen må være, at vores antagelse i udgangspunktet var forkert, der findes altså ikke naturlige tal større end 1, der ikke kan skrives som et produkt af primtal.

Entydighed. Lad

$$p_1 \cdot p_2 \cdot \dots \cdot p_i = q_1 \cdot q_2 \cdot \dots \cdot q_j \tag{3}$$

være to primtalsfaktoriseringer. Primtallet p_1 er divisor i venstresiden af (3) og dermed også i højresiden, ifølge Sætning 2 derfor også divisor i en af primfaktorerne i højresiden.

¹Selvom Euklid er den mest berømte matematiker nogensinde, og hans navn var synonymt med geometri indtil midten af det 20. århundrede er kun to forhold kendt om ham. Det ene er, at han levede mellem Platon (død ca. 347 f. kr.) og Archimedes (født ca. 287 f. kr.). Det andet er, at han underviste i Alexandria. Euklids berømmelse hviler i særdeleshed på *Elementerne*, som han skrev i 13 bøger.

²É. Bézout (1730 – 1783)

³et produkt kan blot bestå af en faktor

Da et primtal kun har 1 og sig selv som divisor, må p_1 være lig med denne primfaktor i højresiden af (3). Denne fælles primfaktor forkorter vi væk og gentager derpå argumentet med p_2, p_3, \dots, p_i . Konklusionen er, at primfaktorerne i venstresiden af (3) optræder i højreside mindst det samme antal gange.

Foretager vi det tilsvarende argument med udgangspunkt i højresiden af (3) kan vi samlet konkludere, at faktoriseringen er entydig i den forstand, at en primfaktor indgår et entydigt antal gange i faktoriseringen. \square

Man bemærker, at beviset ikke giver en effektiv metode til at bestemme en primtalsfaktorisering.

2.1.1 Primtalsfaktoriseringens tidsforbrug

For at få en fornemmelse af hvor tidskrævende det formentlig er at primtalsfaktorisere, forestiller vi os, at m er et helt tal med 200 cifre, dvs. $m \sim 10^{200}$. Det vil være oplagt at eftersøge en faktor i m ved at prøve sig frem nedenfra, denne metode virker ganske overbevisende for små værdier af m ; men for store værdier er det ikke en farbar vej. Lad os antage, at vi kan afgøre om et helt tal er divisor i m i løbet af 1 million'te del af et sekund (10^{-6} sek.). I alt vil efterprøvning af de første $\sqrt{m} \sim 10^{100}$ tal tage så mange år:

$$10^{100} \cdot 10^{-6} = 10^{94} \frac{1}{60 \cdot 60 \cdot 24 \cdot 365} \sim 3,2 \cdot 10^{86} .$$

Til sammenligning er universets alder blot $13,75 \cdot 10^9$ år.

De to hurtigste metoder til at håndtere såkaldt svære faktoriseringer - faktoriseringer af tal, der er produktet af to næsten lige store primtal - er den *kvadratisk si* og *tallegemesien*, hvor den sidste er den hurtigste for ekstremt store tal, jvf. iøvrigt [Pom96].

Den erfaring, at primtalsfaktorisering er meget tidskrævende, er det bærende element bag sikkerheden i det vidt udbredte RSA kryptosystem, som vi behandler i afsnit 8.1. Virksomheden RSA har netop derfor nogle faktoreringsudfordringer. I 2009 lykkedes det et hold fra 6 institutioner at faktorisere RSA-768 - et tal på 768 bits svarende til 232 decimale cifre - ved hjælp af af tallegemesien. Det tog angiveligt næsten 2000 2.2GHz-Opteron-CPU år over knap 3 kalenderår ved parallel beregning på mange maskiner. Tallet RSA-896 med 270 decimale cifre er stadig ikke faktoreret.

2.1.2 Om éntydighedsdelen af aritmetikkens fundamentalsætning

Harald Bohr holdt den 6. februar 1930 et foredrag ved Den polytekniske Lærestalts årsfest med titlen *Matematikkens ideale Elementer*, jvf. [Boh87]. Foredraget indeholder en interessant kommentar til éntydighedsdelen af aritmetikkens fundamentalsætning:

”Vi betragter i Stedet for alle de sædvanlige positive Tal kun Tallene af Formen $4n + 1$, altsaa 1, 5, 9, 13, ..., og tænker os et øjeblik, at vi, om jeg saa maa sige, slet ikke kender andre Tal. Vi betegner disse Tal, lige som før de sædvanlige Tal, med Bogstaverne a, b, c, \dots . Ved Produktet af to Tal a og b skal forstaas det Tal c , vi kommer til ved sædvanlig Multiplikation af a og b ; dette har en Mening, fordi Produktet af to Tal af

Formen $4n + 1$ igen er et Tal af denne Form. Et Tal a siges naturligvis at gaa op i et Tal b eller være en Divisor i b , hvis der findes et Tal c , saaledes at $ac = b$. Alle de sædvanlige Regler for Multiplikation og Division af hele Tal gælder ogsaa for vores nye Tal, saaledes f.Eks., at hvis a gaar op i b , og b gaar op i c , da gaar a op i c . Ethvert Tal a har som før kun et endeligt Antal Divisorer, og to Tal a og b har altid fælles Divisorer, nemlig i hvert Fald Tallet 1; følgelig kan vi ogsaa her tale om den største fælles Divisor for to Tal a og b . Et *Primtal* defineres naturligvis ogsaa her som et Tal > 1 , der ikke har andre Divisorer end 1 og Tallet selv; de første Primtal er 5, 9, 13, 17, 21, 29, . . . [. . .]

Det er klart, at ogsaa indenfor vores nye Talteori kan ethvert Tal a opløses i Primfaktorer; thi Beviset for denne Sætning indenfor den sædvanlige Talteori [. . .] kan jo ordret anvendes paa vores nye Tal.

Men der gælder ikke her nogen almenlydig Sætning om, at Primtalsopløsningen er éntydig. Et Eksempel herpaa har vi i tallet 441, der paa to forskellige Maader kan opløses i Primtalsfaktorer, nemlig dels skrives som $9 \cdot 49$ og dels som $21 \cdot 21$."

3 Uendelig mange primtal - Euklids sætning

Sætning 5 (Euklids sætning). *Der er uendelig mange primtal.*

3.1 Tre forskellige beviser for Euklids sætning

En matematisk sætning behøver kun ét matematisk bevis - flere beviser gør ikke sætningen mere sand. Her præsenteres imidlertid tre forskellige beviser for sætningen for derved at illustrere forskellige metoder.

3.1.1 Euklids bevis

Bevis. Lad p_1, p_2, \dots, p_j være primtal. Så er

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_j + 1$$

et tal, der ikke kan divideres af noget p_i - kunne det det, ville p_i gå op i 1, hvilket ikke er tilfældet. Primdivisorerne i n , som jo findes ifølge Sætning 4, kan altså ikke være blandt p_1, p_2, \dots, p_j - de er altså andre og nye primtal. Heraf følger umiddelbart, at der må være uendelig mange primtal. \square

3.1.2 Bevis baseret på Fermat-tal

Et Fermat⁴-tal er et tal på formen:

$$F_n := 2^{2^n} + 1, \quad n \text{ et naturligt tal .}$$

⁴Pierre de Fermat (1601-1665). Fermats arbejder indenfor talteori blev først forstået og værdsat da Euler (1707-1783) genoplyvede dem og startede den sammenhængende forskning, der kulminerede i Gauss's og Kummers arbejder i begyndelsen af det nittende århundrede.

De første Fermat-tal⁵ ⁶ er $F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537, F_5 = 641 \cdot 6700417$. I [Pom96] er der en status over faktorisering af de første 20 Fermat-tal.

Bevis. Følger umiddelbart af følgende lemma - ethvert Fermat-tal har mindst en primdivisor, der ikke er divisor i noget andet Fermat-tal. \square

Lemma 6. *To Forskellige Fermat-tal har ingen fælles divisorer på nær 1.*

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

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k-1} - x^{2^k-2} + x^{2^k-3} - x^{2^k-4} + \dots - 1$$

et helt tal, altså er F_n en divisor i $F_{n+k} - 2$. En fælles divisor i F_n og F_{n+k} er dermed en divisor i 2 - en fælles divisor er altså enten 1 eller 2; men Fermat-tallene er ulige, så en fælles divisor må være 1. \square

3.1.3 Eulers bevis

Bevis. Antag modsætningsvis, at der kun er endelig mange primtal p_1, p_2, \dots, p_j .

Lad x, n være naturlige tal med $n \leq x$. Ifølge Sætning 4 kan n faktoreres i et produkt af primtal, heri udtager vi netop et eksemplar af hvert af de primtal, der optræder et ulige antal gange, og samler dem i et delprodukt, der er på formen:

$$m = 2^{b_1} \cdot 3^{b_2} \cdot \dots \cdot p_j^{b_j}, \quad b_j \in \{0, 1\} .$$

Tallet n kan altså skrives:

$$n = n_1^2 \cdot m.$$

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

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

Dette er imidlertid ikke sandt for store x . Vi har dermed opnået en modstrid - udgangspunktet om, at der kun er endelig mange primtal, må derfor være forkert. \square

Remark 7 (Euler). Essensen ovenfor i Eulers⁷ bevis kan anvendes til at vise, at

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \dots$$

kan gøres lige så stor som ønskelig ved blot at medtage led nok.

⁵Fermat troede, at alle Fermat-tal F_n er primtal. Deri havde han ikke ret; Euler fandt, at $F_5 = 641 \cdot 6700417$.

⁶Gauss viste, at hvis F_n er et primtal, så kan en regulær F_n -kant konstrueres med passer og lineal.

⁷L. Euler (1707-1783) bidrog til flere matematiske discipliner. Han lagde det videnskabelige fundament for talteorien. Euler var den første til at formulere en variant af algebraens fundamentalsætning.

Tabel 1: Forholdet $\frac{\pi(n)}{n}$ bliver mindre med voksende n

n	10	25	50	100	200	500	1000	5000
$\pi(n)$	4	9	15	25	46	95	168	669
$\frac{\pi(n)}{n}$	0,400	0,360	0,300	0,250	0,230	0,190	0,168	0,134

Tabel 2: Primaltalssætningen - forholdet $\frac{\pi(n)}{\ln(n)}$ er tæt på 1.

n	10	10^2	10^3	10^4	10^6	10^9
$\pi(n)$	4	25	168	1229	78498	50847534
$\frac{n}{\ln(n)}$	4,34	21,71	144,76	1085,74	72382,41	48254942,43
$\frac{\pi(n)}{\ln(n)}$	0,921	1,151	1,131	1,161	1,084	1,054

4 Optælling af primtal - primaltalssætningen

I og med at der er uendelig mange primtal, giver det ikke mening at tælle dem, imidlertid kan vi tælle antallet af primtal, der er mindre end et givet naturligt tal n - dette antal benævnes $\pi(n)$, altså

$$\pi(n) = \#\{p \mid p \leq n, p \text{ et primtal}\}.$$

I tabel 1 er der angivet sammenhørende værdier for n , $\pi(n)$ og forholdet $\frac{\pi(n)}{n}$, der synes at blive mindre med voksende n . Fortsætter dette mønster vil det være rimeligt at sige at *kun de færreste tal er primtal*.

I tabel 2 sammenligner vi i stedet $\pi(n)$ med $\frac{n}{\ln(n)}$, hvor $\ln(n)$ betegner den naturlige logaritme af n . Vi ser, at forholdet mellem de to tal ligger tæt på 1. Dette præciseres i Sætning 8.

Sætning 8 (Primaltalssætningen). *For store naturlige tal n gælder, at*

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

i den forstand, at forholdet mellem $\pi(n)$ og $\frac{n}{\ln n}$ for store værdier af n nærmer sig 1.

Man kan også sige, at vælger vi et stort tal n , så er sandsynligheden for at et tal i nærheden af n er et primtal lig med $\frac{1}{\ln(n)}$. I nærheden af $n = 1000$ er hvert syvende tal et primtal og i nærheden af 10.000.000.000 er omkring 1 ud af 23 tal primtal.

Omkring 1800 fremsatte Gauss⁸ og Legendre uafhængigt af hinanden og alene på baggrund af eksperimenter formodningen om primtalsfordelingen.

⁸C. F. Gauss (1777-1855). I 1801 (24 år gammel) udgav Gauss bogen *Disquisitiones arithmeticae*, hvori han systematisk opsummerede den indtil da spredte viden om talteori, løste nogle af de vanskeligst udestående problemer og formulerede begreber og problemstillinger, der udgjorde mønstret for et århundredes forskning og stadig er af stor betydning i dag.

Der skulle gå næsten 100 år før det lykkedes Hadamard og CH. de la Vallée Poussin hver for sig at bevise sætningen med såkaldt kompleks analytiske metoder. Det var B. Riemann der grundlagde anvendelse af kompleks analyse indenfor talteori i notatet *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse* i november 1859 udgaven af "Monatsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin", hvis ideer stadig er til inspiration og er helt fundamentale for analytisk talteori.

I 1948 fandt Erdős og Selberg et "elementært" bevis for primtalssætningen - et bevis der ikke bruger kompleks analyse.

Det nok simpleste analytiske bevis blev givet i 1980 af D. J. Newman [New80], se også [Zag97].

4.1 Chebychevs sætning

Endnu før primtalssætningen var vist opnåede P. L. Chebyshev i 1848 og 1850 resultater, der indebærer følgende.

Sætning 9. *For store naturlige tal n er*

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

Se [Nai82] og [Per85], hvor et 2 sider elementært bevis af sætningen findes.

4.1.1 Antal primtal med netop 100 cifre - estimat.

For at estimere antallet af primtal med 100 cifre anvender vi Sætning 9.

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

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

Herved kan vi anslå, 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.

5 Landaus primtalsproblemer

Ved *International Congress of Mathematicians* i 1912 opregnede Edmund Landau fire basale problemer i forbindelse med primtal - problemer som han i sit foredrag beskrev som: "*unattackable at the present state of science*":

- Goldbachs formodning⁹
- Formodningen om primtalstvillinger

⁹C. Goldbach (1690 –1764) fremsatte formodningen i et brev af 7. juni 1742 til L. Euler.

- $N^2 + 1$ formodningen
- Legendres¹⁰ formodning

Her i 2011, snart 100 år senere, er Landaus fire problemer stadig uløste!

5.1 Goldsbachs formodning

Formodning 10 (Goldbach). *Ethvert lige helt tal (pånær 2) er summen af to primtal.*

Goldbach fremsatte formodningen i et brev til Euler dateret den 7. juni 1742. Formodningen er let at verificere for små lige hele tal:

$$4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 3 + 7, 12 = 5 + 7,$$

$$14 = 3 + 11, 16 = 3 + 13, 18 = 5 + 13, 20 = 7 + 13$$

og ved brug af computere er den verificeret for meget store lige hele tal. Formodningen er åben - altså ubevist - men, at den er sand, underbygges af, at matematikere har været i stand til at vise tilsvarende resultater. I 1937 vistes således, at alle (tilpas store) ulige hele tal er summen af 3 primtal og i 1966 vistes, at alle (tilpas store) lige hele tal er summen af et primtal og et andet tal, der enten er et primtal eller produktet af 2 primtal.

5.2 Formodningen om primtalstvillinger

Formodning 11 (Primtalstvillinger). *Der er uendelige mange primtal p , så $p + 2$ også er et primtal.*

Er p og $p + 2$ begge primtal, kaldes tallene primtalstvillinger, der er 35 primtalstvillinger mindre end 1000:

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), (197, 199), (227, 229), (239, 241), (269, 271), (281, 283), (311, 313), (347, 349), (419, 421), (431, 433), (461, 463), (521, 523), (569, 571), (599, 601), (617, 619), (641, 643), (659, 661), (809, 811), (821, 823), (827, 829), (857, 859), (881, 883).

Ved computeres hjælp kan der produceres lange lister af primtalstvillinger.

De størst kendte primtalstvillinger pr. 15. jan. 2007 er:

$$2003663613 * 2^{195000} - 1, \quad 2003663613 * 2^{195000} + 1.$$

Det er tal med 58.711 cifre.

At formodningen er sand underbygges af, at der i 1966 vistes, at der er uendelige mange primtal p , så $p + 2$ enten er et primtal eller et produkt af 2 primtal.

¹⁰A-M Legendre (1752 – 1833) ydede vigtige bidrag til statistik, talteori, abstrakt algebra og matematisk analyse.

5.2.1 Hardy-Littlewood formodningen

Hardy-Littlewood formodningen, der er en stærkere form af formodningen, postulerer en fordelingen af primtalstvillinger i lighed med Sætning 8 (Primtalssætningen). Mere præcist, lad $\pi_2(n)$ være antallet af primtal mindre end lig med n , så $p + 2$ også er et primtal, altså

$$T(n) = \#\{p \mid p \leq n \text{ og } p, p + 2 \text{ begge primtal}\} .$$

Så er den stadig ubeviste formodning, at

$$\pi_2(n) \sim \text{konstant} \times \frac{n}{(\ln n)^2}$$

i den forstand, at forholdet mellem $\pi_2(n)$ og $\frac{n}{(\ln n)^2}$ for store værdier af n , nærmer sig en konstant.

5.3 $N^2 + 1$ formodningen

For et lige tal N er $N^2 + 1$ ofte et primtal. De første primtal på denne form er:

$$2^2 + 1 = 5, \quad 4^2 + 1 = 17, \quad 6^2 + 1 = 37, \quad 10^2 + 1 = 101, \quad 14^2 + 1 = 197, \quad 16^2 + 1 = 257, \\ 20^2 + 1 = 401, \quad 24^2 + 1 = 577, \quad 26^2 + 1 = 677, \quad 36^2 + 1 = 1297, \quad 40^2 + 1 = 1601.$$

Formodning 12 ($N^2 + 1$ formodningen). *Der er uendelig mange primtal på formen $N^2 + 1$.*

Det aktuelt bedste resultat i den retning er fra 1978, hvor det blev vist, at der er uendelig mange hele tal N for hvilke $N^2 + 1$ er et primtal eller et produkt af to primtal. En stærkere form af formodningen, postulerer fordelingen af sådanne primtal i lighed med Sætning 8 (Primtalssætningen). Mere præcist, lad $S(n)$ være antallet af primtal mindre end lig med n og på formen $N^2 + 1$, altså

$$S(n) = \#\{p \mid p \leq n \text{ og } p = N^2 + 1 \text{ for et helt tal } N\}.$$

Så er den ubeviste formodning, at

$$S(n) \sim \text{konstant} \times \frac{\sqrt{n}}{\ln n}$$

i den forstand, at forholdet mellem $S(n)$ og $\frac{\sqrt{n}}{\ln n}$ for store værdier af n nærmer sig en konstant.

5.4 Legendres formodning

Formodning 13 (Legendres formodning). *For ethvert helt tal n findes der mindst et primtal mellem n^2 og $(n + 1)^2$.*

Formodningen følger, hvis man kan vise, at afstanden til det næste primtal fra et givet primtal p er mindre end $2\sqrt{p}$. En tabel over maksimale afstande mellem primtal viser således, at formodningen er sand for n mindre end 10^{18} .

Man har vist, at for alle tilpas store n er der mindst et primtal mellem n^3 og $(n + 1)^3$.

6 Mersenne primtal - de størst kendte primtal

Et primtal på formen

$$2^p - 1, \quad p \text{ et primtal}$$

kaldes et Mersenne¹¹ primtal. De første er

$$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 31, \quad 2^7 - 1 = 127, \quad 2^{13} - 1 = 8191.$$

Ikke alle tal på formen $2^p - 1$ er primtal, eksempelvis har vi følgende faktoriseringer

$$2^{11} - 1 = 2047 = 23 \cdot 89, \quad 2^{29} - 1 = 536870911 = 233 \cdot 1103 \cdot 2089.$$

I 1876 viste E. Lucas, at $2^{127} - 1$ er et primtal og dette tal var faktisk indtil 1950'erne det størst kendte primtal. Med computerens hjælp er det muligt at finde større Mersenne primtal. Der er et projekt Great Internet Mersenne Prime Search (GIMPS) på www.mersenne.org/prime.htm, der omhandler dette. Rekordens er, at $2^{43112609} - 1$ er Mersenne primtal nummer 47 og det er det størst kendte primtal¹².

Åben problemstilling 14. Er der uendelig mange Mersenne primtal?

6.1 Mersenne primtal og perfekte tal

Tallet 6 har en særlig egenskab

$$1 + 2 + 3 = 6,$$

det er altså summen af dets egentlige divisorer 1, 2, 3. Det samme gør sig gældende for $496 = 16 \cdot 31 = 2^4 \cdot 31$, der har de egentlige divisorer

$$1, 2, 2^2, 2^3, 2^4 \text{ og } 31, 2 \cdot 31, 2^2 \cdot 31, 2^3 \cdot 31,$$

som adderes til

$$\begin{aligned} (1 + 2 + 2^2 + 2^3 + 2^4) + (31 + 2 \cdot 31 + 2^2 \cdot 31 + 2^3 \cdot 31) &= \\ (1 + 2 + 2^2 + 2^3 + 2^4) + (1 + 2 + 2^2 + 2^3) \cdot 31 &= 31 + 15 \cdot 31 = \\ 16 \cdot 31 &= 496. \end{aligned}$$

Sådanne tal kaldes *perfekte tal*. Allerede i det antikke Grækenland vidste man, hvordan man konstruerede perfekte tal. I Euklids elementer (bog IX) [Euk85] optræder, hvad der svarer til denne sætning.

Sætning 15 (Euklids formel for perfekte tal). *Hvis $2^p - 1$ er et Mersenne primtal, så er*

$$2^{p-1}(2^p - 1)$$

et perfekt tal.

¹¹Marin Mersenne (1588 – 1648) var fransk teolog, filosof, matematiker og musikteoretiker - refereres til som: "Father of acoustics".

¹²Det vil kræve 3 461 sider at skrive dette tal med 75 decimale cifre pr. linie og 50 linier pr. side

De perfekte tal 6 og 496 ovenfor fremkommer netop ved at bruge Euklids formel med p lig med 2 og 5. Formlen bevises ved et argument, der er en kopi af udregningen for 496,

Bevis. (Euklids formel). De egentlige divisorer i $2^{p-1}(2^p - 1)$ er

$$1, 2, 2^2, \dots, 2^{p-1} \quad \text{og} \quad (2^p - 1), 2 \cdot (2^p - 1) \cdot \dots \cdot 2^{p-2} \cdot (2^p - 1) ,$$

som adderes til

$$\begin{aligned} & (1 + 2 + 2^2 + \dots + 2^{p-1}) + (1 + 2 + 2^2 + \dots + 2^{p-2})(2^p - 1) = \\ & (2^p - 1) + (2^{p-1} - 1)(2^p - 1) = \\ & 2^{p-1}(2^p - 1) , \end{aligned}$$

hvor vi et par gange anvender, at $1 + 2 + 2^2 + \dots + 2^{n-1} = 2^n - 1$ for ethvert $n > 0$. \square

Et oplagt spørgsmål er nu, om der findes andre perfekte tal. Omkring 2000 år efter Euklid viste Euler, at samtlige lige perfekte tal fremkommer ved Euklids formel.

Der er altså en komplet forståelse af de lige perfekte tal, derimod ved man absolut intet om ulige perfekte tal.

Åben problemstilling 16. Findes der ulige perfekte tal?

Intet er fundet og man ved, at findes der et, er det større end 10^{300} .

7 Kongruenser og potenser

Deling af hele tal er et centralt begreb og for at gøre det mere håndterbart indfører vi efter Gauss [Gau01] begrebet *kongruens*. Om to hele tal a, b siger vi, at de er *kongruente modulo m* , hvis det naturlige tal m går op i $a - b$, og vi skriver

$$a \equiv b \pmod{m} .$$

For eksempel er $12 \equiv 5 \pmod{7}$ og $21 \equiv 0 \pmod{3}$. En anden måde at sige det på, er at a og b har samme rest ved division med m .

Kongruens opfører sig på mange måder som det sædvanlige lighedstegn, hvis

$$\begin{aligned} a_1 & \equiv b_1 \pmod{m} , \\ a_2 & \equiv b_2 \pmod{m} , \end{aligned}$$

så er

$$\begin{aligned} a_1 \pm a_2 & \equiv b_1 \pm b_2 \pmod{m} , \\ a_1 a_2 & \equiv b_1 b_2 \pmod{m} . \end{aligned}$$

Man skal dog være meget varsom med forkortning, når man regner modulo m . For eksempel kan man ikke forkorte med **2** i kongruensen:

$$15 \cdot \mathbf{2} \equiv 20 \cdot \mathbf{2} \pmod{10} ,$$

idet 15 jo ikke er kongruent med 20 modulo 10.

7.1 Fermats lille sætning

For et helt tal a , vil vi nu se på dets potenser a, a^2, a^3, \dots modulo et primtal p . Vi starter med tilfældet $p = 7$ og får tabel 3. hvor vi bemærker, at for $a = 1, 2, 3, 4, 5, 6$ er

Tabel 3: Potenserne a^k mod 7

a	a^2	a^3	a^4	a^5	a^6	a^7
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	4	1	2	4	1	2
3	2	6	4	5	1	3
4	2	1	4	2	1	4
5	4	6	2	3	1	5
6	1	6	1	6	1	6

$a^6 \equiv 1 \pmod{7}$, hvilket er fremhævet med rødt. Det er et tilfælde af Fermats lille sætning.

Sætning 17 (Fermats lille sætning). *Lad p være et primtal og lad a være et helt tal, som ikke kan deles med p . Så er*

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

Vi illustrerer beviset ved eksemplet $p = 7, a = 5$ og betragter tabellen nedenfor, hvor vi ser, at tallene i tredje række og første række er ens, blot rækkefølgen er ændret.

x	1	2	3	4	5	6
$5 \cdot x$	5	10	15	20	25	30
$5 \cdot x \pmod{7}$	5	3	1	6	4	2

derfor er

$$(5 \cdot 1) \cdot (5 \cdot 2) \cdot (5 \cdot 3) \cdot (5 \cdot 4) \cdot (5 \cdot 5) \cdot (5 \cdot 6) \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7} \Rightarrow$$

$$5^6 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7},$$

hvorfor 7 er en divisor i produktet

$$(5^6 - 1) \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6.$$

Da primtallet 7 ikke er en divisor i de sidste 6 faktorer, må 7 i medfør af Sætning 2 være en divisor i den første faktor $(5^6 - 1)$ og vi har, at $5^6 \equiv 1 \pmod{7}$. Denne illustration bruges som forlæg til et egentligt bevis for Fermats lille sætning.

Bevis. (Fermats lille sætning) Lad p være et primtal, som ikke går op i a , og betragt de to rækker af tal

$$\begin{array}{c|cccc} x & 1 & 2 & 3 & \dots & (p-1) \\ a \cdot x & a \cdot 1 & a \cdot 2 & a \cdot 3 & \dots & a \cdot (p-1) \end{array}$$

To forskellige tal i den anden række kan ikke være kongruente modulo p . Hvis det faktisk var tilfældet, at

$$a \cdot j \equiv a \cdot i \pmod{p}, \quad 1 \leq i < j \leq p-1,$$

så ville p være en divisor i produktet $a \cdot (j - i)$, hvilket er jo er umuligt ifølge Sætning 2, da p ikke går op i nogen af faktorerne a eller $(j - i)$. Der er altså præcis de samme rester modulo p , der optræder i anden som i første række, blot i en anden orden. Derfor har vi, at produkterne af tallene i første og anden række er ens modulo m .

$$\begin{aligned} (a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdot \dots \cdot (a \cdot (p-1)) &\equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p} \Rightarrow \\ a^{p-1} (1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)) &\equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}, \end{aligned}$$

hvorfor p er en divisor i produktet

$$(a^{p-1} - 1) \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1).$$

Da primtallet p ikke er en divisor i de sidste $p-1$ faktorer, må p i medfør af Sætning 2 være en divisor i den første faktor $(a^{p-1} - 1)$ og vi slutter, at $a^{p-1} \equiv 1 \pmod{p}$. \square

7.2 Eulers sætning

For et helt tal a , vil vi nu se på dets potenser a, a^2, a^3, \dots modulo det naturlige tal m , der ikke er et primtal. I tilfældet $m = 15$ fås tabel 4. hvor vi ikke ser helt det samme

Tabel 4: Potenserne a^k mod 15

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	1	2	4	8	1	2	4	8	1	2	4
3	9	12	6	3	9	12	6	3	9	12	6	3	9
4	1	4	1	4	1	4	1	4	1	4	1	4	1
5	10	5	10	5	10	5	10	5	10	5	10	5	10
6	6	6	6	6	6	6	6	6	6	6	6	6	6
7	4	13	1	7	4	13	1	7	4	13	1	7	4
8	4	2	1	8	4	2	1	8	4	2	1	8	4
9	6	9	6	9	6	9	6	9	6	9	6	9	6
10	10	10	10	10	10	10	10	10	10	10	10	10	10
11	1	11	1	11	1	11	1	11	1	11	1	11	1
12	9	3	6	12	9	3	6	12	9	3	6	12	9
13	4	7	1	13	4	7	1	13	4	7	1	13	4
14	1	14	1	14	1	14	1	14	1	14	1	14	1

mønster, som i tilfældet med Fermats lille sætning jvf. tabel 3; men i stedet bemærker, at for $a = 1, 2, 4, 7, 8, 11, 14$ er $a^8 \equiv 1 \pmod{15}$, hvilket er fremhævet med rødt.

Det er et tilfælde af Eulers sætning, som udtrykkes ved hjælp af Eulers ϕ -funktion. For et naturligt tal m er $\phi(m)$ antallet af naturlige tal blandt $1, 2, \dots, m$, der er primiske med m , altså tal hvis største fælles divisor med m er 1.

Man ser let, at $\phi(7) = 6$ og $\phi(15) = 8$; men det er generelt særdeles tidskrævende og i praksis umuligt (uden særlig viden) at bestemme $\phi(m)$. Har vi imidlertid en primtalsfaktorisering af m , så er beregningen ligetil i henhold til følgende sætning.

Sætning 18. *Lad p, q være primtal med $p \neq q$. Så er*

$$\phi(p) = p - 1, \quad (4)$$

$$\phi(p \cdot q) = (p - 1) \cdot (q - 1). \quad (5)$$

Bevis. Den første påstand er triviell, så lad os betragte tilfældet $m = p \cdot q$. Tallene mindre end m , der ikke er primiske med m , er netop de tal, der har p eller q som primfaktor, altså de $q - 1$ tal $p \cdot 1, p \cdot 2, \dots, p \cdot (q - 1)$ og de $p - 1$ tal $1 \cdot q, 2 \cdot q, \dots, (p - 1) \cdot q$. Antallet af tal mindre end $m = p \cdot q$, der er primiske med m , er således

$$(p \cdot q - 1) - (q - 1) - (p - 1) = (p - 1) \cdot (q - 1).$$

□

Vi kan nu formulere Eulers sætning, som kan bevises efter den samme tankegang, der ligger til grund for beviset af Sætning 17 (Fermats lille sætning).

Sætning 19 (Eulers sætning). *Lad m være et naturligt tal og lad a være et helt tal, som er primisk med m , altså hvis største fælles divisor med m er 1. Så er*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Ser vi på tilfældet $m = 15 = 3 \cdot 5$, hvor $\phi(m) = (3 - 1) \cdot (5 - 1) = 8$ ifølge (5), fås for $a = 1, 2, 4, 7, 8, 11, 13, 14$, der er de primiske rester modulo 15, at

$$a^8 \equiv 1 \pmod{15},$$

jvf. tabel 4, hvori resultaterne er fremhævet med rød skrift.

7.2.1 Uddragning af rødder modulo m

Lad k, b, m være naturlige tal. Udfordring er, at løse kongruensen

$$x^k \equiv b \pmod{m}. \quad (6)$$

Vi vil her beskrive en metode, der forudsætter, at vi kender værdien $\phi(m)$ af Eulers ϕ -funktion. Det er værd at bemærke, at vi kan beregne denne værdi, hvis vi kan primtalsfaktorisere m , jvf. sætning 18, hvorimod værdien i almindelighed er uberegnelig for store værdier af m .

Antag, at k og $\phi(m)$ er indbyrdes primiske, altså at deres største fælles divisor er 1. Bestem i henhold til Sætning 3 og ved brug af Euklids udvidede algoritme, jvf. 9.2 og (14), hele tal $u > 0$ og $v < 0$, så

$$ku + \phi(m)v = 1 \Rightarrow ku = 1 - \phi(m)v \Rightarrow ku = 1 + \phi(m)w, \quad (7)$$

hvor $w = -v > 0$. Antag, at b i (6) er primisk med m . Vi får, at $x = b^u$ er en løsning til (6), thi fra (7) fås, at

$$b^u \equiv (x^k)^u \equiv x^{ku} \equiv x^{1+\phi(m)w} \equiv x \underbrace{(x \cdots x)^{\phi(m)} \cdots (x \cdots x)^{\phi(m)}}_{\phi(m)w} \equiv x \pmod{m},$$

idet de med rødt markerede produkter er kongruente til 1 modulo m ifølge Sætning 7.2 (Eulers sætning). Løsningen x er entydigt bestemt modulo m .

Roduddragning opnås altså ved en passende potensopløftning, som vi kan gøre effektivt med gentagen kvadrering, jvf. 9.1.

Som illustration vil vi løse kongruensen

$$x^{17} \equiv 13 \pmod{77}. \quad (8)$$

Vi noterer, at $77 = 7 \cdot 11$ og $\phi(77) = (7-1)(11-1) = 60$, jvf. (5). Vi bestemmer dernæst u, v , ved hjælp af metoden i 9.2, så

$$17u + 60v = 1 \Rightarrow ku = 1 - \phi(m)v.$$

Et sæt løsninger til denne ligning er $u = 53, v = -15$ og vi får, at

$$x = b^u = (13)^{53} \equiv 41 \pmod{77},$$

er løsningen til (8) modulo 77.

7.3 Primalstest

Fermats lille sætning giver grundlaget for en metode til at afsløre, om et tal n er et primtal. Metoden går ud på at afgøre om

$$a^{n-1} \equiv 1 \pmod{n}. \quad (9)$$

for et eller flere a med $\text{sfd}(a, n) = 1$.

Selvom (9) er sand, når n et primtal (Fermats lille sætning), kan vi ikke omvendt slutte, at n er primtal, hvis (9) er sand for et eller for alle a .

Det mindste tal, hvor der kommer en falsk positiv, er $n = 341 = 11 \cdot 31$ med $a = 2$. Der gælder nemlig, at

$$2^{341-1} \equiv 1 \pmod{341}.$$

Et tal, der er falsk positiv, kaldes et *pseudo-primtal*.

7.3.1 Pseudo-primtal

Definition 20. Lad n være et naturligt tal og lad a være primisk med n , altså $\text{sfd}(a, n) = 1$. Hvis

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

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 tal - de såkaldte Carmichael tal - der er pseudo-primtal for alle a , der er primiske med n . Det mindste Carmichael tal er $561 = 3 \cdot 11 \cdot 17$. Først i 1994 vistes, at der er uendelig mange - for store n er der mindst $n^{\frac{2}{7}}$ Carmichael tal mellem 1 og n .

7.3.2 Rabin-Millers primtalstest - konstruktion af sandsynlige primtal

I og med at Carmichael tal findes, må der udvikles bedre metoder til primtalstest. Rabin-Miller testen tager afsæt i følgende egenskab ved primtal, der vises ved anvendelse af Sætning 17 (Fermats lille sætning).

Sætning 21. Lad p være et primtal og lad a være et tal, der ikke er deleligt med p . Lad $p - 1 = 2^s d$, hvor $1 \leq s$ og d ulige. Så gælder enten, at

$$a^d \equiv 1 \pmod{p}$$

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

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

Carmichael tallet $n = 561$ afsløres som værende sammensat ved at bruge "vidnet" $a = 2$. Vi har, at $n - 1 = 560 = 2^4 \cdot 35$ og, at

$$\begin{aligned} 2^{35} &\equiv 263 \pmod{561}, \\ 2^{2 \cdot 35} &\equiv 263^2 \equiv 166 \pmod{561}, \\ 2^{4 \cdot 35} &\equiv 166^2 \equiv 67 \pmod{561}, \\ 2^{8 \cdot 35} &\equiv 67^2 \equiv 1 \pmod{561}. \end{aligned}$$

Resultatet $2^{35} \pmod{561}$ i den første række er hverken 1 eller -1 og ingen af tallene i de tre sidste rækker er -1 , hvorfor $a = 2$ er et vidne på, at 561 ikke er et primtal.

Definition 22. Lad $n \neq 2$ være et naturligt tal, der ikke er et primtal, og lad a være primisk med n , altså $\text{sfd}(a, n) = 1$.

Lad $n - 1 = 2^s d$, hvor $1 \leq s$ og d ulige. Hvis enten

$$a^d \equiv 1 \pmod{n}$$

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

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

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

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

For et ikke-primtal er sandsynligheden for, at det er et pseudo-primtal for et stigende antal baser a , mindre og mindre - faktisk er der en øvre grænse. G. Miller [Mil76] og M. Rabin [Rab80] lagde med den følgende sætning grundlaget for en probabilistisk primtalstest.

Sætning 23 (Rabin-Miller). *Antag at n ikke er et primtal. Antallet af baser a , hvori n er et stærkt pseudo-primtal, er højst*

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

Sandsynligheden er i gennemsnit betydeligt lavere, I. Damgård, P. Landrock og C. Pomerance [DLP93] har bestemt meget bedre eksplicitte grænser.

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

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

Konstruktion af store (sandsynlige) primtal Rabin-Millers primtalstest kan anvendes til at producere store (med for eksempel 100 cifre), der med meget stor sandsynlighed er primtal. Vælges $k = 30$ tilfældigt valgte baser a er risikoen for en falsk positiv af en test af et tilfældigt tal højst

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

hvilket er mindre end 1 ud af 1.000.000.000.000.000 gange.

8 Offentlig nøgle kryptografi - RSA kryptografi - hemmelig kommunikation og digital underskrift

Det er dokumenteret, at kryptografisk teknikker er anvendt siden det antikke Ægypten og af Julius Cæsars regime, hvilket endda har givet navn til en krypteringsmetode, hvor man blot forskyder alfabetets bogstaver 3 pladser, jvf.[Sin01].

Oprindeligt kendte man blot *symmetrisk kryptografi*, hvor de to partnere, der skulle kommunikere delte en fælles hemmelig krypteringsnøgle, der blev anvendt ved både kryptering og dekryptering. Sådanne symmetriske krypteringssystemer anvendes stadig i stor udstrækning; men de lider af en stor praktisk svaghed, nemlig kravet til sikker udveksling af den fælles hemmelige nøgle.

Det var et gennembrud, at man indså, at man kan lave hemmelig kommunikation selvom transmissionen overvåges omhyggeligt og selvom der ikke forinden var udvekslet en fælles hemmelig nøgle. Denne ved første tanke helt umulige opgave løses ved *asymmetrisk kryptografi* - et begreb, der opbygges omkring ikke blot én nøgle men et *nøglepar*. I nøgleparret er den ene nøgle offentlig og udveksles i fuld offentlighed, hvorimod den

anden er privat (hemmelig) og den skal ikke udveksles. De to nøgler i parret har asymmetriske funktioner - *låses der med en nøgle kan den anden nøgle (og kun den) låse op og vise versa.*

Hemmelig kommunikation foretages ved, at afsender låser dokumentet med den offentlige nøgle i modtagerens nøglepar. Modtageren kan nu låse dokumentet op ved at anvende den modsvarende private (hemmelige) nøgle i sit nøglepar. Han og kun han kan låse dokumentet op, for blot han besidder den hemmelige nøgle i nøgleparret, der matcher den offentlige nøgle.

Digital underskrift af et dokument laves ved at afsender låser dokumentet med sin private (hemmelige) nøgle. Enhver kan nu låse dokumentet op med afsenders offentlige nøgle og derved overbevise sig om, at afsender besidder den tilsvarende hemmelige nøgle og dermed er den, han udgiver sig for.

Man kan næppe overvurdere betydningen af offentlig-nøgle-kryptosystemer og de tilknyttede digitale underskrifter i den moderne verden, hvor enorme informationsmængder udveksles og bindende aftaler indgås over store afstande på elektronisk vis uden at partnerne nogensinde mødes.

Offentlig nøgle kryptering blev opfundet i 1969 af J. Ellis, M. Williamson og C. Cocks, der arbejdede ved British Government Communications Headquarters, deres opfindelser blev imidlertid hemmeligholdt af den britiske regering indtil 1997. I mellemtiden blev de genopfundet af W. Diffie samt R. Rivest, A. Shamir og L. Adleman, der i 1978 skabte offentlig-nøgle-kryptosystemet RSA. Disse opfindelser er virkelig banebrydende i den lange historie om hemmelig kommunikation, jvf. [Ell69],[Dif96], [RSA82] og [Sin01].

Kunsten ved at lave et offentligt nøgle kryptosystem er altså at give en metode til at konstruere nøglepar, således at kendskab til den offentlige nøgle ikke gør det muligt at bestemme den tilhørende private (hemmelige) nøgle. RSA-kryptosystemet er en sådan metode, hvor sikkerheden hviler på den erfaring, at det er umuligt effektivt at faktorisere et helt tal i et produkt af primtal, jvf. 2.1.1.

8.1 Offentlig-nøgle-kryptosystemet RSA

Eulers sætning og umuligheden af at beregne Eulers ϕ -funktion uden kendskab til primtalsfaktoriseringen er kernen i sikkerheden i offentlig-nøgle-kryptosystemet RSA.

Vi konstruerer et nøglepar ved at vælge to store forskellige primtal p, q og beregner $m = pq$ og $\phi(m) = (p - 1)(q - 1)$ i henhold til Sætning 18, idet vi kender og udnytter faktorisering af $m = pq$. Vælg et k primisk med $\phi(m)$:

$$\text{Offentlig nøgle : } m, k \tag{10}$$

$$\text{Privat nøgle : } \phi(m) \tag{11}$$

En klartekst kan let omskrives til en stribe af tal ud fra en i forvejen fastlagt tabel, der sammenknytter tal og bogstaver. Vi krypterer og dekrypterer altså blot tal.

Tallet a krypteres til

$$b \equiv a^k \pmod{m},$$

hvilket kan gøres effektivt ved at anvende metoden med gentagen kvadrering, jvf. 9.1. Dekryptering svarer til at genfinde a ud fra b , altså løse kongruensen:

$$x^k \equiv b \pmod{m} .$$

Det kan gøres effektivt ved metoden i 7.2.1, der forudsætter, at vi kender $\phi(m)$, hvilket vi gør - det er jo vores hemmelige nøgle.

En fjende, der vil bryde krypteringen, skal beregne $\phi(m)$, hvilket er uhyre tidskrævende - når man ikke kender faktoriseringen $m = p \cdot q$. I afsnit 2.1.1 anskueliggjorde vi netop primtalsfaktoriserings enorme tidsforbrug.

Bag NemID anvendes RSA-nøglepar med mindst 1024 bits altså med over 300 decimale cifre.

9 Appendiks

9.1 Gentagen kvadrering

Ved at anvende det ældgamle trick *gentagen kvadrering* og Fermats lille sætning kan man meget effektivt alene med papir og blyant beregne resten ved division med primtal p af meget store potenser af hele tal.

Lad os først beregne, at

$$35^{157} \equiv 155 \pmod{167} . \tag{12}$$

For at anvende gentagen kvadrering opstiller vi en hjælpetabel, hvor det sidste tal i en række fås ved kvadrering af det tilsvarende tal i den foregående, og vi konsekvent regner modulo 167.

n	2^n	$35^{2^n} \pmod{167}$
0	1	35
1	2	1225 \equiv 56
2	4	3136 \equiv 130
3	8	16900 \equiv 33
4	16	1089 \equiv 87
5	32	7569 \equiv 54
6	64	2916 \equiv 77
7	128	5929 \equiv 84

Da $157 = 1+4+8+16+128$, fås ved anvendelse af hjælpetabellen og potensregnerreglerne, at

$$35^{157} = 35^{1+4+8+16+128} = 35^1 \cdot 35^4 \cdot 35^8 \cdot 35^{16} \cdot 35^{128} \equiv 35 \cdot 130 \cdot 33 \cdot 87 \cdot 84 \equiv 155 \pmod{167} ,$$

hvilket er det søgte resultat.

Styrken i ovenstående kombineret med Sætning 17 (Fermats lille sætning) eller Sætning 19 (Eulers sætning) illustreres med regneeksemplet

$$20112012^{20122013} \pmod{167}$$

Da $20112012 \equiv 35 \pmod{167}$ er

$$20112012^{20122013} \equiv 35^{20122013} \pmod{167} .$$

Vi noterer, at

$$20122013 = 121216 \cdot (167 - 1) + 157$$

og ved hjælp af potensregnerreglerne og Fermats lille sætning (167 er et primtal) fås, at

$$\begin{aligned} 35^{20122013} &\equiv 35^{121216 \cdot (167-1) + 157} \equiv \\ &(\mathbf{35^{(167-1)}})^{121216} \cdot 35^{157} \equiv 35^{157} \equiv 155 \pmod{167}, \end{aligned}$$

ifølge den tidligere udregning (12), da det med rødt markerede er kongruent til 1 modulo 167 ifølge Sætning 17 (Fermats lille sætning).

9.2 Euklids algoritme og Bezouts identitet

Dette afsnit beskriver en metode til effektivt at håndtere Sætning 3. Beviser og gennemregnede eksempler findes i [HS02].

Lad m, n være to naturlige tal og lad $\text{sfd}(m, n)$ betegne deres største fælles divisor. Der findes hele tal x, y , så

$$mx + ny = \text{sfd}(m, n) . \tag{13}$$

Den største fælles divisor $\text{sfd}(m, n)$ og et løsningssæt x, y bestemmes effektivt med Euklids algoritme, der beskrives nedenfor. Har vi bestemt et løsningssæt (x, y) til (13), så er samtlige løsninger bestemt ved formlerne

$$\left(x + c \frac{n}{\text{sfd}(m, n)}, y - c \frac{m}{\text{sfd}(m, n)} \right), \tag{14}$$

hvor $c = \dots, -2, -1, 0, 1, 2, 3, \dots$

Euklids algoritme Sæt $r_0 = m, r_1 = n$ og divider successivt indtil resten er 0:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2, & 0 \leq r_2 < r_1, \\ r_1 &= q_2 r_2 + r_3, & 0 \leq r_3 < r_2, \\ &\dots \\ r_{k-2} &= q_{k-1} r_{k-1} + r_k, & 0 \leq r_k < r_{k-1}, \\ &\dots \\ r_{n-3} &= q_{n-2} r_{n-2} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2}, \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n, & 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= q_n r_n + 0 . \end{aligned}$$

Så er

$$\text{sfd}(m, n) = r_n .$$

Algoritmen er hurtig, vi bemærker, at for hver to trin er resten mindst halveret, altså

$$r_{k+2} < \frac{1}{2}r_k .$$

Heraf beregner man for eksempel, at selv for tal med 100 cifre skal der højst foretages 666 divisioner.

For at bestemme et løsningsæt x og y i (13) defines to talrækker x_0, \dots, x_n og y_0, \dots, y_n ved

$$\begin{aligned} x_0 &= 1, & y_0 &= 0, \\ x_1 &= 0, & y_1 &= 1, \\ x_k &= x_{k-2} - q_{k-1}x_{k-1}, & y_k &= y_{k-2} - q_{k-1}y_{k-1} \quad \text{for } 2 \leq k \leq n, \end{aligned}$$

hvor kvotienterne q_i stammer fra udregningen ovenfor.

Så er

$$\begin{aligned} r_k &= mx_k + ny_k \quad \text{for } 2 \leq k \leq n, \\ \text{sfd}(m, n) &= r_n = mx_n + ny_n . \end{aligned}$$

Tabeller

1	Forholdet $\frac{\pi(n)}{n}$ bliver mindre med voksende n	8
2	Primtalssætningen - forholdet $\frac{\pi(n)}{\ln(n)}$ er tæt på 1.	8
3	Potenserne $a^k \bmod 7$	14
4	Potenserne $a^k \bmod 15$	15

Litteratur

- [Boh87] Harald Bohr. *Matematiske arbejder med pædagogisk sigte*. Dansk Matematisk Forening, København, second edition, 1987.
- [Dav08] H. Davenport. *The higher arithmetic*. Cambridge University Press, Cambridge, eighth edition, 2008. An introduction to the theory of numbers, With editing and additional material by James H. Davenport.
- [Dif96] Whitfield Diffie. The national security establishment and the development of public-key cryptography. *Des. Codes Cryptogr.*, 7(1-2):9–11, 1996. Special issue dedicated to Gustavus J. Simmons.
- [DLP93] Ivan Damgård, Peter Landrock, and Carl Pomerance. Average case error estimates for the strong probable prime test. *Math. Comp.*, 61(203):177–194, 1993.

- [Ell69] J Ellis. The story of non-secret encryption. 1969. Released by CSEG in 1997, <http://www.cesg.gov.ellisdox.ps>.
- [Euk85] Euklid. *Elementerne*. Gyldendal 1897-1900, optrykt af Trip, 1985.
- [Eul85] L Euler. *Elements of Algebra*. Springer Verlag, 1985. Translated by J. Hewlett. Longman, Orme and Co., London 1840. Reprinted.
- [Gau01] C. F. Gauss. *Disquisitiones arithmeticae. Oprindelig 1801. Werke, Königliche Gesellschaft der Wissenschaften zu Göttingen, Leipzig-Berlin, 1863-1933*, 1801.
- [Hea] T. Heath. *Diophantus of Alexandria*. Second Edition, Cambridge University Press, Cambridge (1910). Reprint by Dover Books, New York (1964).
- [HPS08] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An introduction to mathematical cryptography*. Undergraduate Texts in Mathematics. Springer, New York, 2008.
- [HS02] J. P. Hansen and H. Spalk. *Algebra og talteori*. Gyldendal, 2002.
- [IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.
- [LN97] P. Landrock and K. Nissen. *Kryptologi - fra viden til videnskab*. Abacus, 1997.
- [Mil76] Gary L. Miller. Riemann's hypothesis and tests for primality. *J. Comput. System Sci.*, 13(3):300–317, 1976. Working papers presented at the ACM-SIGACT Symposium on the Theory of Computing (Albuquerque, N.M., 1975).
- [Nai82] M. Nair. On Chebyshev-type inequalities for primes. *Amer. Math. Monthly*, 89(2):126–129, 1982.
- [New80] D. J. Newman. Simple analytic proof of the prime number theorem. *Amer. Math. Monthly*, 87(9):693–696, 1980.
- [NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons Inc., New York, fifth edition, 1991.
- [Per85] N. Costa Pereira. A short proof of Chebyshev's theorem. *Amer. Math. Monthly*, 92(7):494–495, 1985.
- [Pom96] Carl Pomerance. A tale of two sieves. *Notices Amer. Math. Soc.*, 43(12):1473–1485, 1996.
- [Rab80] Michael O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, 12(1):128–138, 1980.

- [Rib04] Paulo Ribenboim. *The little book of bigger primes*. Springer-Verlag, New York, second edition, 2004.
- [Ros94] H. E. Rose. *A course in number theory*. Oxford Science Publications. The Clarendon Press Oxford University Press, New York, second edition, 1994.
- [RSA82] Ronald Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public key cryptosystems. In *Secure communications and asymmetric cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, pages 217–239. Westview, Boulder, CO, 1982.
- [Sin01] Simon Singh. *Kodebogen - Videnskaben om hemmelige budskaber - fra oldtidens Ægypten til kvantekryptering*. Gyldendal, 2001.
- [Zag97] D. Zagier. Newman’s short proof of the prime number theorem. *Amer. Math. Monthly*, 104(8):705–708, 1997.

DRAFT

Indeks

- $N^2 + 1$ formodningen, 11
- Bezouts identitet, 4, 22
- Carmichael tal, 18
- CH. de la Vallée Poussin, 9
- Chebychev, 9
- digital underskrift, 19
- Eratosthenes si, 3
- Erdős, 9
- Euklid, 4
 - Euklids algoritme, 4
 - perfekte tal, 12
 - udvidede algoritme, 17
 - uendelig mange primtal, 6
- Euklids algoritme, 4, 22
- Euler, 7, 15
- Euler sætning, 16
- Eulers ϕ -funktion, 16
- Eulers sætning, 16
- Fermat, 6
- Fermat-tal, 6
- Fermats lille sætning, 14
 - bevis, 14
 - illustration af beviset for $p = 7$, 14
- Gauss, 8, 13
- gentagen kvadrering, 21
- Goldbachs formodning, 10
- Hadamard, 9
- Hardy-Littlewood formodningen, 11
- kongruens, 13
- kvadratisk si, 5
- Landaus primtalsproblemer, 9
- Legendre, 8
 - Legendres formodning, 11
- Mersenne primtal, 12
 - perfekte tal, 13
- nøglepar, 19
- Offentlig nøgle kryptografi, 19
- perfekte tal, 12
 - lige, 13
 - ulige?, 13
- primtal, 3
 - definition, 3
 - divisor i et produkt, 3
 - primtalstest, 17
 - pseudo-primtal, 18
 - uendelig mange, 6
 - bevis baseret på Fermat-tal, 6
 - Euklids bevis, 6
 - Eulers bevis, 7
 - primtalsfaktorisering, 4
 - tidsforbrug, 5
 - primtalsætningen, 8
 - primtalstest, 17
 - primtalstvillinger, 10
 - pseudo-primtal, 18
 - stærke pseudo-primtal, 19
- Rabin-Miller primtalstest, 18
- RSA
 - RSA-768, 5
 - RSA kryptografi, 19
- sandsynlige primtal, 18
- Selberg, 9
- si
 - Eratosthenes si, 3
 - kvadratisk si, 5
 - tallegeme-sien, 5
 - største fælles deler, 4
- tallegeme-sien, 5
- uddragning af rødder modulo m , 16