Martin Geisler

Mersenne primtal

Marin Mersenne

3. årsopgave
Aalborghus Gymnasium
22.–29. januar 2001

Forord

Denne opgave skal handle om Mersenne primtal, men kommer også ind på meget andet. Da de forskellige grene af matematikken ofte vikler sig ind i hinanden på en uforudsigelig måde, må vi have fat i ting som f.eks. gruppeteori, for at kunne forstå argumenterne i forbindelse med beviset af Lucas-Lehmer sætningen.

Stilen

Jeg skrive i et tekstformateringssystem som hedder LaTeX. Denne rapport ser derfor ikke helt ud, som hvis den var lavet med f.eks. Word. Henvisninger til litteraturlisten bagerst står i teksten som f.eks "[1]", hvilket skal læses som "kilde 1".

I forhold til Word har mine sider en større margin, både i siderne og i top og bund. Det betyder naturligvis, at der ikke står så meget på hver linie, og at der ikke er så mange linier på hver side. Opsætningen er valgt sådan, fordi det er nemmere at læse en tekst, når linierne ikke er alt for lange.

Én side i LaTeX indeholder omkring 70% af hvad der kan stå på en side i Word, når vi snakker om ren tekst. Når det også er ligninger med på siden bliver forholdet endnu større, idet LaTeX bruger mere luft omkring ligningerne end Word vil gøre.

Tager man disse ting i betragtning, mener jeg, at opgaven har den rigtige størrelse.

Inddeling

Opgaven er inddelt i 6 kapitler plus 3 bilag. Her kommer en kort disposition af hvad hvert kapitel og bilag indeholder.

Kapitel 1 er den generel indføring i hvad vi forstår ved et primtal og en beskrivelse af deres egenskaber.

Kapitel 2 beskæftiger sig med kongruensbegrebet og introducerer modulusregning. Vi starter med det, da vi næsten uafbrudt kommer til at bruge kongruenser i resten af opgaven.

Kapitel 3 indeholder gruppeteori. Vi definerer grupper og en række af deres egenskaber. Vi skal bruge denne gruppeteori i næste kapitel til at bevise Lucas-Lehmer sætningen.

Kapitel 4 indeholder så endelig beviset for Lucas-Lehmer sætningen.

Kapitel 5 viser hvordan man så bruger Lucas-Lehmer sætningen konkret til at finde primtal i et projekt kaldet GIMPS.

Kapitel 6 er en opsummering og sammenfatning.

Bilag A er en tabel med samtlige 38 Mersenne primtal og de tilhørende perfekte tal. Tallene er ikke skrevet ud i deres fulde længde, da det ville kræve flere tusinde sider.

Bilag B samler de beviser fra afsnittet om kongruens, som det ikke var værd at bruge plads på i selve opgaven.

Bilag C indeholder ligeledes en række sætninger om regnereglerne med grupper (og beviser derfor), som ikke var så vigtige for hovedteksten.

Bilag D er en gennemgang af den algoritme som bruges ved division i `mprime`.

Bilag E er egentlig ikke et bilag, men blot en henvisning til de elektroniske kilder som findes på den vedlagte diskette.

Indhold

Kapitel 1

Primtal og deres kendetegn

Vi vil starte med at se generelt på primtal. Mersenne primtal er blot primtal som opfylder nogle yderligere krav, men derfor stadig også opfylder de generelle krav til primtal.

1.1 Generelt om primtal

Forskellige tal har forskellige divisorer. Ethvert helt tal a har de såkaldte *trivielle* divisorer 1, -1, a og $-a$. Andre divisorer kaldes *ægte* divisorer ifølge [13, s. 168].

Nogle tal har ikke andre divisorer end de trivielle — sådanne tal kaldes primtal. Vi kan formalisere definitionen:

DEFINITION 1.1 *Et tal a større end 1 som ikke har andre divisorer end 1, -1, a og $-a$ kaldes et* primtal.

De første primtal er den kendte talfølge $2, 3, 5, 7, 11, 13, \ldots$. Et tal som ikke er et primtal, kaldes et *sammensat* tal. Har vi to tal som ikke har nogle fælles, ægte divisorer, siger vi at de er *indbyrdes primiske*. Der gælder så følgende om et sammensat tal:

SÆTNING 1.2 *Ethvert sammensat tal større end 1 har et primtal som divisor, da den mindste divisor som er større end 1 er et primtal.*

Bevis af 1.2 Vi har et helt tal $a > 1$. Den mindste divisor i a som er større end 1, d er så et primtal, da d ikke har nogen ægte divisor. En ægte divisor i d ville også være divisor i a og samtidig være mindre end d, hvilket ikke kan lade sig gøre, da d er den mindste ægte divisor i a. ■

1.1.1 Uendelig mange primtal

Vi vil straks gå videre og vise den fundamentale sætning 1.3, som er taget fra [8, s. 14]:

SÆTNING 1.3 (EUCLID) *Der findes uendelig mange primtal.*

Bevis af 1.3 Vi vil vise at vi altid kan finde endnu et primtal. Hvis vi går ud fra, at der er et endeligt antal primtal, n, må vi kunne skrive dem op på en liste: $p_1, p_2, p_3, \ldots, p_n$. Ud fra denne liste, kan vi lave tallet

$$T = p_1 p_2 p_3 \cdots p_n + 1 \tag{1.1}$$

Nu har T ingen ægte divisorer blandt de allerede kendte primtal, da der ved division med et af $p_1, p_2, p_3, \ldots, p_n$ altid vil fremkomme en rest på 1.

Den mindste divisor i T som er større end 1, vil så ifølge sætning 1.2 på foregående side være et primtal, som vi ikke havde fundet endnu. ■

Med hensyn til Mersenne primtal, har man endnu ikke kunnet give noget bevis for, at der også er uendelig mange af dem[14, s. 80]. Man kan dog heller ikke give nogen god grund til, at det ikke skulle være tilfældet.

1.1.2 Faktorisering af sammensatte tal

En anden vigtig egenskab ved primtallene er, at de er alle sammensatte tals byggeklodser, forstået på den måde, at ethvert heltal kan skrives som et produkt bestående udelukkende af primtal:

SÆTNING 1.4 *Ethvert tal $a > 1$ kan skrives som et produkt af primtal. Skrives a som et sådant produkt, siger vi at a er opløst i dets* primfaktorer.

Bevis af 1.4 Sætning 1.2 på forrige side fortæller os at vi kan skrive a som $p_1 a_1$ hvor p_1 er et primtal, og a_1 er et heltal som er mindre end a. Hvis $a_1 = 1$ er $a = p_1$, altså et primtal. Vi er så færdige.

Hvis $a_1 > 1$, så kan vi skrive a_1 som $p_2 a_2$ hvor p_2 er et primtal. p_2 vil så også være en primfaktor i a, da $a = p_1 p_2 a_2$. Hvis nu $a_2 = 1$, er vi færdige, ellers fortsætter vi på samme måde ved at opløse a_2 i $p_3 a_3$.

Vi fortsætter indtil $a_n = 1$, hvilket vil ske på et tidspunkt, da vi har en aftagende følge af positive hele tal:

$$a > a_1 > a_2 > \cdots > a_{n-1} > a_n = 1 \tag{1.2}$$

Der kan højst være a tal i følgen, da de alle er mindre end a og positive.

Efter at have fundet n primtal, har vi fået opløst a i dets primfaktorer: $a = p_1 p_2 p_3 \cdots p_n$, hvilket var det vi skulle. ■

1.2 At vise at et tal er et primtal

Der er forskellige måder hvorpå man kan vise, at et givent tal er et primtal.

1.2.1 Den naive metode

Det simpleste er at prøve at finde en faktor til tallet n ved division. Sætning 1.2 på foregående side siger, at hvis vi kan finde en ægte divisor til tallet n, så er n ikke et primtal. Kan vi omvendt vise, at der ikke findes nogen ægte divisorer, så er tallet et primtal.

Så vi starter med at prøve at dele med 2, og hvis det ikke går op, prøver vi med 3, 4, 5 osv. Vi behøver kun at prøve indtil $i^2 \geq n$, hvor i er det tal vi

prøver med, da tal derover ikke vil kunne gå op i n. Hvis $ij = n$, hvor $i^2 \geq n$, må $j \leq i$, men så er j allerede testet.

Da man skal prøve med tal indtil $i^2 \geq n$, bliver beregningstiden meget stor, når vi arbejder med store tal. Allerede i antikken havde man derfor fundet en mere effektiv metode kaldet *Eratosthenes si*.

1.2.2 Eratosthenes si

Når man gerne vil finde alle primtal under en vis grænse g, kan man bruge en metode som går under navnet Eratosthenes si.

Man starter med at skrive alle tallene mindre end g og større end 1 op efter hinanden. Sætter vi $g = 20$ får vi følgende talrække:

$$2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16,\ 17,\ 18,\ 19,\ 20 \tag{1.3}$$

Første tal på listen kan ikke have nogen ægte divisor, så 2 er derfor et primtal. Alle tal som 2 går op i har nu 2 som divisor, og er derfor sammensatte. Disse tal fjernes fra listen:

$$2,\ 3,\ 5,\ 7,\ 9,\ 11,\ 13,\ 15,\ 17,\ 19 \tag{1.4}$$

Det næste tal i listen er 3, kan ikke have nogen ægte divisor. Hvis det havde, ville 3 ikke længere være i listen. Vi fjerner så alle tal som har 3 som divisor:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19 \tag{1.5}$$

Vi kommer så til tallet 5. Men da $5^2 = 25 > 20$, behøver vi ikke at fortsætte. Hvis der var flere sammensatte tal under 20, kunne det jo ikke have et primtal mindre end 5 som faktor. Det mindste sammensatte tal vi kunne "ramme" ville altså være 25. Fordelen ved denne metode er, at vi finder mange primtal på én gang, ved at udføre næsten de samme beregninger som ved det første metode.

1.3 Mersenne primtal

Da denne opgave skal handle om Mersenne primtal, må vi hellere slå fast hvad det er for primtal vi kalder Mersenne primtal, samt indføre en notation for dem:

DEFINITION 1.5 *Et Mersenne primtal, M_p, er et primtal som kan skrives som:*

$$M_p = 2^p - 1. \tag{1.6}$$

1.3.1 Den historisk udvikling

(Se tabel A.1 på side 22 for en komplet liste med alle kendte Mersenne primtal.)

Det var tidligere en normal misforståelse, at $2^p - 1$ altid ville være et primtal, bare p var det. Men i 1536 viste Hudalricus Regius[5], at det ikke var tilfældet, idet $2^{11} - 1 = 2047 = 23 \cdot 89$.

Pietro Cataldi fandt i 1588 ud af, at $M_{17} = 131071$ og $M_{19} = 524287$. Men han mente også at $M_{23} = 47 \cdot 178481$, $M_{29} = 233 \cdot 1103 \cdot 2089$ og $M_{37} = 233 \cdot 616318177$ var primtal.[1]

Det kendetegner disse første forsøg på et finde store primtal, at man ikke havde ret hver gang. Men det er ikke så underligt, for man skal jo huske at f.eks. $M_{31} = 2147483647$ jo har 10 cifre. Det er nogle enorme tal at arbejde med, hvis man ikke har elektroniske hjælpemidler.[2]

Man fortsatte med at lede efter endnu større primtal, og i 1644 påstod den franske munk Marin Mersenne (1588–1648) i sin bog *Cogitata Physica-Mathematica* at $2^p - 1$ var et primtal for

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 \text{ og } 257 \tag{1.7}$$

I denne liste var det kun tallene fra 31 og op efter, man var i tvivl om. Mersenne indrømmede endda at han ikke havde testet alle disse tal, men da tallene er så store, kunne ingen modbevise ham.

Først over 100 år senere kunne L. Euler (1707–1783) vise at M_{31} virkelig er et primtal, og 230 år senere viste E. Lucas (1842–1891) at M_{127} også er et primtal. M_{127} har 39 cifre og er det største primtal som er fundet ved håndkraft.

Senere fandt man ud af, at Mersenne havde glemt 3 tal, nemlig M_{61}, M_{89} og M_{107}. Han tog også fejl ved $M_{67} = 193707721 \cdot 761838257287$.[3] Men hans navn blev alligevel knyttet til disse primtal.

1.3.2 Sætninger om Mersenne primtal

Der gælder følgende sætning om M_p:

SÆTNING 1.6 *Hvis $M_p = 2^p - 1$ er et primtal, er p selv et primtal.*

Det beviser vi nu, beviset er fra [4].

Bevis af 1.6 Vi har $r, s \in \mathbb{Z}_+$. Vi kan så skrive $x^{rs} - 1$ som

$$x^{rs} - 1 = (x^s - 1)\left(x^{s(r-1)} + x^{s(r-2)} + \cdots + x^{2s} + x^s + 1\right) \tag{1.8}$$

Vi kan gøre prøve ved at gange $(x^s - 1)$ ind i parentesen. Resultatet bliver så:

$$\begin{aligned} &x^{sr} + x^{s(r-1)} + x^{s(r-2)} + \cdots + x^{3s} + x^{2s} + x^s \\ &\quad - x^{s(r-1)} - x^{s(r-2)} - \cdots - x^{3s} - x^{2s} - x^s - 1 = x^{sr} - 1 \end{aligned} \tag{1.9}$$

Vi har nu vist at $2^p - 1$ ikke kan være et primtal, hvis p ikke selv er et primtal. Vi har nemlig vist at tallet $2^s - 1$ går op i $2^p - 1$, hvis p kan skrives som $p = rs$. ■

[1] I [5] skriver de først at han tog fejl, da han mente at M_{31} var et primtal. Men dernæst skriver de at Euler viste at M_{31} virkelig *var* et primtal. Det kan godt være at Cataldi ikke kunne bevise at M_{31} er et primtal, men han tog ikke fejl da han påstod det.

[2] De faktoriseringer jeg har lavet her på siden, er alle lavet ved hjælp af min grafregner (en TI-89 fra TEXAS INSTRUMENTS). Det viser hvor langt den teknologiske udvikling er nået, når jeg kan sidde og teste Mersenne tal på en grafregner

[3] Den var en svær nød at knække for min grafregner. Men det er forståeligt, da primfaktorerne er meget store.

Sætning 1.6 på foregående side fortæller os, at vi nemt kan finde faktorer til $2^p - 1$, når p ikke er et primtal. F.eks. må $2^{100} - 1$ være en faktor i $2^{1000} - 1$, ligesom $2^{10} - 1$ må være det.

Hvis M_p *ikke* er et primtal, kan vi faktisk udtale os om formen af divisorerne:

SÆTNING 1.7 *Hvis p og q er ulige primtal, og q går op i M_p, så gælder der at*

$$p \equiv 1 \pmod{q} \quad og \quad p \equiv \pm 1 \pmod{8} \tag{1.10}$$

Det er det samme som at sige at en faktor q skal have formen $q = 2kp+1$, hvor k er et heltal.

Jeg giver ikke noget bevis for sætning 1.7, i stedet henvises til [6].

1.3.3 Mersenne primtals betydning

Som med det meste talteori, har Mersenne primtal ikke nogen særlig konkret betydning. Men man må dog nævne at Mersenne primtallene er knyttet sammen med de perfekte tal. Om et perfekt tal gælder

DEFINITION 1.8 *Et tal n er perfekt, hvis det er lig summen af dets (positive) divisorer, undtagen tallet selv. Derfor er 6 et perfekt tal, da $6 = 1 + 2 + 3$. Det samme er 28, da $28 = 1 + 2 + 4 + 7 + 14$.*

Perfekte tal er rimelig sjældne. Man kender også kun *lige* perfekte tal, men har endnu ikke kunne give noget bevis hverken for eller imod, at der skulle findes et ulige perfekt tal. Men man ved at et eventuelt ulige perfekt tal må være stort[11, s. 167], da man ved hjælp af computere har undersøgt alle tal op til 10^{600}!

Hvert Mersenne primtal vi finder, giver os samtidig et lige perfekt tal[14, s. 81] ifølge sætning 1.9:

SÆTNING 1.9 *For hvert Mersenne primtal $M_p = 2^p - 1$ gælder der at $P_p = 2^{p-1}(2^p - 1)$ er et lige perfekt tal.*

Før vi kan bevise sætning 1.9 må vi først introducere funktionen $\sigma(n)$, se [7]:

DEFINITION 1.10 *$\sigma(n)$ betegner summen af de positive divisorer til n. Vi har så for et primtal p at $\sigma(p) = p + 1$ og at $\sigma(m) = 2m$ hvis m er et perfekt tal. $\sigma(n)$ har den egenskab at $\sigma(nm) = \sigma(n) \cdot \sigma(m)$ når n og m er indbyrdes primiske.*

Der er lige en lille sætning vi også skal bruge, beviset for sætningen har jeg selv lavet:

SÆTNING 1.11 *Der gælder følgende om $\sigma(2^n)$:*

$$\sigma(2^n) = 2^{n+1} - 1 \tag{1.11}$$

Bevis af 1.11 Hvis vi opløser 2^n i dets primfaktorer, får vi naturligvis 2^n. Derfor kan f.eks. 3 eller 5 ikke gå op i 2^n. En divisor skal så selv have formen 2^m hvor $m \leq n$. Der må altså være n af disse divisorer, da 2^n er delelig med et hvert tal på formen 2^m:

$$\frac{2^n}{2^m} = 2^{n-m} \in \mathbb{Z} \tag{1.12}$$

Divisorerne er altså $\{1, 2, 2^2, 2^3, \ldots, 2^{n-1}, 2^n\}$. Deres sum er:

$$\sum_0^n 2^n = 2^{n+1} - 1 \tag{1.13}$$

Derved har vi vist at summen af divisorerne, $\sigma\left(2^n\right)$, er lig $2^{n+1} - 1$. ■

Vi kan så bevise sætning 1.9 på foregående side som i [3]:

Bevis af 1.9 Vi går ud fra at $M_p = 2^p - 1$ er et primtal, og skal vise at $n = 2^{p-1}(2^p - 1)$ er et (lige) perfekt tal, hvilket er det samme som at $\sigma(n) = 2n$.

Vi har altså:

$$\sigma(n) = \sigma\left(2^{p-1}(2^p - 1)\right) = \sigma\left(2^{p-1}\right) \cdot \sigma\left(2^p - 1\right) = (2^p - 1)2^p = 2n \tag{1.14}$$

Vi benyttede undervejs at 2^{p-1} og $2^p - 1$ er indbyrdes primiske, da $2^p - 1$ er et primtal som i hvert tilfælde *ikke* går op i 2^{p-1}. Det viser at n er et perfekt tal og at det må have formen $n = 2^{p-1}\left(2^p - 1\right)$.

Vi kan også vise at det omvendte gælder, nemlig at hvis n er et lige perfekt tal, så vil det kunne skrives som $n = 2^{p-1}\left(2^p - 1\right)$.

Vi har altså et lige perfekt tal, n. Det må vi kunne skrive som $2^{k-1}m$ hvor $k \geq 2$ og m er et ulige heltal. Vi regner nu på $\sigma(n)$:

$$\sigma(n) = \sigma\left(2^{k-1}m\right) = \sigma\left(2^{k-1}\right) \cdot \sigma(m) \tag{1.15}$$

Det giver os at

$$\sigma(n) = \left(2^k - 1\right) \cdot \sigma(m) \tag{1.16}$$

Vi benyttede at 2^{k-1} og m må være indbyrdes primiske, da 2^{k-1} kun har primtalsdivisoren 2 og m er ulige og derfor ikke delelig med 2.

Vi ved også at n er et perfekt tal:

$$\sigma(n) = 2n = 2\left(2^{k-1}m\right) = 2^k m \tag{1.17}$$

Kombinerer vi de to sidste ligninger får vi

$$2^k m = \left(2^k - 1\right) \cdot \sigma(m) \tag{1.18}$$

hvilket betyder at $2^k - 1$ går op i $2^k m$. Men $2^k - 1$ kan ikke gå op i 2^k, og må derfor gå op i m. Vi kan altså skrive m som

$$m = \left(2^k - 1\right) M \Leftrightarrow m + M = 2^k M \tag{1.19}$$

hvor $M \in \mathbb{Z}$. Sætter vi $m = \left(2^k - 1\right) M$ ind i (1.18), får vi:

$$\begin{gathered} 2^k\left(2^k - 1\right) M = \left(2^k - 1\right) \cdot \sigma(m) \Leftrightarrow \\ 2^k M = \sigma(m) \end{gathered} \tag{1.20}$$

Både m og M er divisorer i m. Da $\sigma(m)$ netop er summen af divisorerne i m (som der godt kan være flere af ud over m og M), må $\sigma(m)$ være større end eller lig $m + M$. Men da $m + M$ samtidig er lig $2^k M$ ifølge (1.19), har vi at

$$\sigma(m) = m + M \tag{1.21}$$

Det viser at der kun kan være to divisorer i m. Hvis nu M var lig ab, skulle vi have fået $\sigma(m) = m + M + a + b$. m må så være et primtal, og M må være lig 1.

Vi har altså at $m = 2^k - 1$ er et primtal. Tallet n får så formen $2^{k-1}\left(2^k - 1\right)$, hvilket var det vi skulle vise. ■

Som et eksempel på brugen af sætning 1.9 på side 5, kan vi se at tallet $2^{12}\left(2^{13} - 1\right) = 33550336$ er et perfekt tal, da $M_{13} = 2^{13} - 1$ er et primtal.

Kapitel 2

Kongruens og modulusregning

Jeg har medtaget dette afsnit, da det er nødvendigt for beviset af Lucas-Lehmer sætningen senere.

Når man regner med kongruenser, regner man faktisk med rester efter divisioner. Derfor er kongruensbegrebet uhyre vigtigt i forbindelse med primtal, da man netop i denne sammenhæng ofte beskæftiger sig med brøker, rester og tals delelighed generelt.

2.1 Kongruens

Vi starter med at definere kongruens:

DEFINITION 2.1 *Hvis differencen mellem to tal a og b er delelig af et andet tal m, siger vi at a er kongruent med b modulus m, og det skrives således:*

$$a \equiv b \pmod{m} \tag{2.1}$$

Vi kan også skrive det som en almindelig ligning i stedet:

$$\frac{a-b}{m} = n \Leftrightarrow a = nm + b, \quad n \in \mathbb{Z} \tag{2.2}$$

Det var C. F. Gauss (1777–1855) som opfandt denne notation[11, s. 69]. Notationen ligner den vi bruger til almindelige ligninger, og det viser sig at man kan regne på kongruenserne efter nogle specielle regler. Det var et stort fremskridt, da man nu havde fået et værktøj til at beskrive de ting, der sker når tal går op i hinanden.

Da de fleste af de følgende sætninger er ret trivielle at bevise, har jeg flyttet beviserne over i bilaget, se side 24.

SÆTNING 2.2 *Følgende kongruenser er altid sande: $a \equiv b \pmod{1}$ og $a \equiv 0 \pmod{a}$.*

Sætning 2.3 *Vi kan gange både a og b med det samme tal: $a \equiv b \pmod{m} \Leftrightarrow ad \equiv bd \pmod{m}$. Som et specialtilfælde har vi at $a \equiv 0 \pmod{m} \Leftrightarrow an \equiv 0 \pmod{m}$.*

Sætning 2.4 *Kongruenser modulus det samme tal kan lægges sammen og trækkes fra hinanden: Hvis $a \equiv b$ og $c \equiv d \pmod{m}$ så gælder der at $a + c \equiv b + d \pmod{m}$.*

Sætning 2.5 *Kongruenser modulus det samme tal kan også ganges sammen: Hvis $a \equiv b$ og $c \equiv d \pmod{m}$ så gælder der at $ac \equiv bd \pmod{m}$. Hvis vi gentager processen får vi at der også gælder at: $a^k \equiv b^k \pmod{m}$.*

Sætning 2.6 *Hvis $a \equiv b$ og $b \equiv c \pmod{m}$ så gælder der at $a \equiv c \pmod{m}$.*

Sætning 2.7 *Vi kan lægge et helt antal m til eller trække det fra a, og vil stadig få samme rest: $a \pm nm \equiv b \pmod{m}$.*

Sætning 2.8 *Kongruensen $a \equiv b \pmod{m}$ er kun sandt, hvis der samtidig gælder at $ac \equiv bc \pmod{mc}$.*

Sætning 2.9 *Hvis $ac \equiv bc \pmod{m}$ og største fælles divisor for c og m er d, så gælder der at $a \equiv b \pmod{\frac{m}{d}}$. Hvis c og m er indbyrdes primiske ($d = 1$), og vi får så at $a \equiv b \pmod{m}$.*

Bevis af 2.9 $ac \equiv bc \pmod{m}$ kan skrives om til $ac = jm + bc$. Den største fælles divisor for c og m er d, så der gælder så også at $a\frac{c}{d} = j\frac{m}{d} + b\frac{c}{d}$. Her er alle brøkerne heltal, da d går op i både c og m.

Vi kan så gange igennem med $\frac{d}{c}$, og får så at $a = \frac{m}{c} + b \Leftrightarrow a$ hvilket viser at a er kongruent med b modulus $\frac{m}{c}$. ■

Som et eksempel kan vi se på kongruensen $6 \cdot 6 \equiv 1 \cdot 6 \pmod{15}$. Her har vi at største fælles divisor for 6 og 15 lig 3. Vi kan derfor omskrive kongruensen til $6 \equiv 1 \pmod{5}$, hvilket tydeligvis også er sandt.

2.2 Restklasser

Har vi en ligning som $a \equiv b \pmod{m} \Leftrightarrow a = nm + b$ får vi en hel række løsninger, da $n \in \mathbb{Z}$. Det at vi får en hel *klasse* af løsninger, fører os over i begrebet *restklasser*:

Definition 2.10 *Tal som giver samme rest r ved division med et tal t, siges at tilhøre samme* restklasse. *Vi får t klasser, som kaldes restklasserne modulus t.*

Ud fra definitionen og det vi ved om kongruens, kan vi skrive at a og b ligger i samme restklasse modulus t sådan her:

$$\begin{aligned} a &\equiv k \pmod{t} \Leftrightarrow a = n_1 t + k \\ b &\equiv k \pmod{t} \Leftrightarrow b = n_2 t + k \end{aligned} \tag{2.3}$$

Det medfører faktisk at $a \equiv b$ og at $b \equiv a \pmod{t}$ da:

$$\begin{aligned} a - b = (n_1 - n_2)t \Leftrightarrow a \equiv b \pmod{t} \\ b - a = (n_2 - n_1)t \Leftrightarrow b \equiv a \pmod{t} \end{aligned} \tag{2.4}$$

hvor både $n_1 - n_2$ og $n_2 - n_1$ er heltal.

Kapitel 3

Grupper

Gruppeteorien beskæftiger sig med forskellige mængder af objekter, som er knyttet sammen af kompositioner, som opfylder nogle bestemte krav. Da der ikke er nogle bestemte krav til typen af objekter, er gruppeteori altså en del af det man vil kalde *abstrakt algabra*.

3.1 Algebraisk struktur

Vi starter med at se på en komposition[13, s. 133]:

DEFINITION 3.1 *En komposition $*$ i en mængde M er en forskrift, som knytter et hvert ordnet par af elementer fra M til et element i M. $*$ definerer en afbildning af M ind i M.*

Man skal lægge mærke til at symbolet $*$ ikke er brugt som et gangetegn. $*$ angiver blot en vilkårlig forskrift, som f.eks. kunne være givet ved

$$a * b = \frac{a+b}{3} \tag{3.1}$$

Ud fra en komposition får vi så en *algebraisk struktur*:

DEFINITION 3.2 *En algebraisk struktur er en mængde, M, hvortil der er knyttet en komposition, $*$. Dette skrives som $(M, *)$.*

Vi kan nu se, at vi allerede kender mange algebraiske strukturer. F.eks. har vi at $(\mathbb{Z}, +)$ er en algebraisk struktur, da der gælder

$$\forall a, b \in \mathbb{Z}: \quad a + b \in \mathbb{Z} \tag{3.2}$$

Næste skridt ville så være at fastlægge, hvordan vi ville regne med elementerne i en algebraisk struktur. Men da disse regler blot er udtryk for en mere formel beskrivelse af de regler vi allerede kender, er de flyttet til bilaget, se afsnit C.1 på side 25. Vi vil dog lige ridse definitionerne op:

For at den *associative lov* er opfyldt for kompositionen $*$, skal der gælde følgende

Definition 3.3 *En komposition $*$ i en mængde M er associativ, hvis den opfylder*

$$\forall a, b, c \in M: \quad (a * b) * c = a * (b * c) \tag{3.3}$$

En algebraisk struktur med en associativ kompositon $(M, *)$ kaldes en semigruppe.

Vi har også den kommutative lov:

Definition 3.4 *En komposition $*$ i en mængde M er kommutativ hvis den opfylder at*

$$\forall a, b \in M: \quad a * b = b * a \tag{3.4}$$

Er $(M, *)$ er semigruppe, og er $*$ kommutativ, har vi en kommutativ semigruppe.

I nogle algebraiske strukturer findes et element som er *neutralt.*

Definition 3.5 *I en algebraisk struktur $(M, *)$ er elementet e neutralt hvis der gælder at*

$$\forall a \in M: \quad a * e = e * a = a \tag{3.5}$$

Ved addition kaldes det neutrale element for et nul-element *mens det kaldes et* et-element *ved multiplikation.*

Når vi så har en vilkårlig semigruppe med et neutralt element, kan vi definere et omvendt element:

Definition 3.6 *Når a er element i semigruppen $(M, *)$ med det neutrale element e, og ligningssystemet*

$$x * a = e, \qquad a * x = e \tag{3.6}$$

har en løsning, er a invertibelt. Løsningen kaldes det inverse element til a og betegnes med a^{-1*}.

3.2 Grupper

Nu da vi har defineret en komposition, en algebraisk struktur, en semigruppe, et neutralt element og et inverst element, er vi endelig klart til at definere hvad vi forstår ved en gruppe (se [13, s. 148], [12, s. 27] eller [1, s. 186]):

Definition 3.7 *En gruppe er en algebraisk struktur G med en komposition $*$, som opfylder følgende:*

- *$*$ opererer på to elementer og der gælder at $a, b \in G \Rightarrow a * b \in G$,*
- *$*$ er associativ,*
- *Der findes et neutralt element i G,*
- *Alle elementer i G har et inverst element.*

Hvis kompositionen $*$ også er kommutativ, siges gruppen at være kommutativ. En kommutativ gruppe kaldes også en abelsk gruppe.[1]

Vi ser nu hvorfor man kalder en associativ algebraisk struktur for en *semigruppe*, idet en semigruppe kun mangler at opfylde de to sidste punkter.

3.2.1 Orden på sagerne

Både de enkelte elementer i en gruppe og gruppen selv kan have det vi betegner med orden. Vi definerer et elements orden således:

DEFINITION 3.8 *I en endelig gruppe med kompositionen $*$ er et elements orden n det* mindste *tal større end 0 som opfylder at:*

$$a^{n*} = e \tag{3.7}$$

hvor e er det neutrale element i gruppen. Vi skriver det også som $n = \operatorname{ord} a$.

Vi vil nu bevise at ethvert element i en endelig gruppe har en orden

Bevis af 3.8 Vi skal vise at man før eller siden vil komme til det neutrale element:

$$\exists n \in \mathbb{Z} : \quad a^{n*} = e \tag{3.8}$$

Vi går ud fra at det ikke er muligt. For at undgå at komme til det neutrale element, må man altså kunne cykle i ring blandt gruppens elementer. Da gruppen indeholder et endeligt antal elementer, vil man før eller siden komme tilbage til et element, man har været ved før.

Dette element må endvidere være det oprindelige element a. Hvis ikke, skulle der være to forskellige løsninger til ligningen $a^{(m-1)*}$, hvor a^{m*} er det første element, vi har været ved før.

Vi har altså at $a = a^{m*} = a^{2m*}$. Det er lovligt at tilføje a^{-1*} på hver side af lighedstegnet, så det gør vi. Det giver os at $a * a^{-1} = a^{(m-1)*} \Leftrightarrow e = a^{(m-1)*}$. Vi ser nu at vi alligevel når til det neutrale element, nemlig efter $m-1$ gange.■

En gruppe har også en orden:

DEFINITION 3.9 *En gruppes orden n er lig antallet af elementer i G.*

SÆTNING 3.10 *Hvis G er en endelig gruppe, er et elements orden højst lig gruppens orden:*

$$\operatorname{ord} x \leq \operatorname{ord} G \tag{3.9}$$

Beviset kommer fra [11, s. 173]:

Bevis af 3.10 En gruppe G med ordnen n og kompositionen $*$ består af n elementer. Følgende mængde $\{e, x, x^{2*}, x^{3*}, \ldots, x^{n*}\}$ hvor $x \in G$ består af $n+1$ elementer, så mindst to af dem må være ens. Vi har så at $x^{u*} = x^{v*}$ hvor $0 \leq u < v \leq n$. Det giver os at $x^{(v-u)*} = x^{0*} = e$, hvor $1 \leq v - u \leq n$.

Ifølge definitionen ef et elements orden (sætning 3.8) må $\operatorname{ord} x$ nu være mindre end eller ligmed $v - u$, som selv er mindre end eller lig med n: $\operatorname{ord} x \leq v - u \leq n$. Det giver os at $\operatorname{ord} x \leq n$. ■

[1] Opkaldt efter den norske matematiker N. H. Abel, der bl.a. beskæftigede sig med kommutative grupper.

SÆTNING 3.11 *Vi har en endelig gruppe G hvor $a \in G$. Der gælder nu at*

$$a^r = e \Rightarrow \operatorname{ord} a \equiv 0 \pmod{r} \tag{3.10}$$

Dette bevis stammer også fra [11, s. 173]:

Bevis af 3.11 Vi sætter $s = \operatorname{ord} x$, og går ud fra at $x^{r*} = e$, hvor der gælder at $r \equiv b \pmod{s} \Leftrightarrow r = as + b$ hvor $a \in \mathbb{Z}$ og $0 \leq b < s$.[2] Hvis $b > 0$ går r altså ikke om i s, der er b til rest. Vi får så at:

$$e = x^{r*} = x^{(as+b)*} = (x^{s*})^{a*} * x^{b*} = e^{a*} * x^{b*} = x^{b*} \tag{3.11}$$

Ved næstsidste omskrivning brugte vi definitionen på et elements orden, som siger at $x^{s*} = e$.

Hvis nu $b > 0$ har vi fundet en mindre eksponent end s som giver os det neutrale element, da $b < s$. Dette strider imod definitionen af et elements orden, som jo siger at $s > 0$ er den mindste eksponent for hvilken det gælder at $a^{s*} = e$. Derfor kan b kun være 0, hvilket giver os at

$$r \equiv 0 \pmod{s} \tag{3.12}$$

hvilket fortæller os at r går op i s. ■

Følgende sætning bruges i beviset af Lucas-Lehmer sætningen.

SÆTNING 3.12 *Lad X være en mængde med en binær og associativ operator, som indeholder et neutralt element. Mængden X^* af alle de invertible elementer i X udgør så en gruppe.*

Bevis af 3.12 Det neutrale element i X er invertibelt, så X^* er ikke en tom mængde. Det er også klart at alle elementer i X^* er invertible, da det netop er en betingelse for at være med i X^*.

Vi mangler så blot at vise, $\forall a, b \in X^* : a * b \in X^*$. Vi tager to elementer fra X, a og b, som er invertible, med de inverse elementer a^{-1} og b^{-1}. Det inverse element til $a * b$ er så $b^{-1} * a^{-1}$, hvilket vi kan vise ved brug af den associative lov:

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e, \tag{3.13}$$

Dette inverse element findes, da både a^{-1} og b^{-1} tilhører X^*. Dermed opfylder X^* kravene for at være en gruppe. ■

[2] I [11] har de at $0 \leq b < r$. De ender så med at konstatere, at vi finder en eksponent b som er mindre end r. De skriver at det strider imod definitionen af x's orden, men det kan jeg ikke forstå, da den kun fortæller os at $b \geq s$ og ikke at $b > r$.

Kapitel 4

Lucas-Lehmer sætningen

Lucas-Lehmer sætningen bruges til at bevise at et givent Mersenne tal er et primtal. Derfor omtaler jeg den også sommetider som Lucas-Lehmer testen.

4.1 Lucas-Lehmer

Det følgende bevis for Lucas-Lehmer sætningen er taget fra [11, s. 170–173], som har det fra [2]. Oprindeligt stammer beviset fra [15].

SÆTNING 4.1 (LUCAS-LEHMER) *$M_p = 2^p - 1$ er kun et primtal hvis det går op i S_{p-1}:*

$$S_{p-1} \equiv 0 \pmod{M_p} \tag{4.1}$$

hvor serien S defineres således:

$$\begin{aligned} S_1 &= 4 \\ S_n &= S_{n-1}^2 - 2 \end{aligned} \tag{4.2}$$

Bevis af 4.1 Vi starter med at indføre to symboler $\omega = 2+\sqrt{3}$ og $\overline{\omega} = 2-\sqrt{3}$. Vi ser at $\omega\overline{\omega} = 1$.

Der gælder nu følgende om serien S, ω og $\overline{\omega}$:

SÆTNING 4.2 *Det m-te element i serien S er givet ved*

$$S_m = \omega^{2^{m-1}} + \overline{\omega}^{2^{m-1}}. \tag{4.3}$$

Bevis af 4.2 Vi bruger et induktionsbevis, som i [9, s. 273–275]. Der skal altså gælde to ting om (4.3):

1. S_1 skal være sand,
2. Hvis S_m er sand, skal S_{m+1} også være det. Vi kender S_{m+1} fra (4.2).

Ifølge (4.2) er $S_1 = 4$. Vi ser at $\omega^{2^{1-1}} + \overline{\omega}^{2^{1-1}}$ også er lig 4.

Vi viser så, at *hvis* (4.3) er sand for m, *så* er den også sand for $m+1$. S_{m+1} skal så være lig $\omega^{2^n} + \overline{\omega}^{2^n}$:

$$\begin{aligned} S_{m+1} &= S_m^2 - 2 \\ &= \left(\omega^{2^{m-1}} + \overline{\omega}^{2^{m-1}}\right)^2 - 2 \\ &= \left(\omega^{2^{m-1}}\right)^2 + \left(\overline{\omega}^{2^{m-1}}\right)^2 + 2\left(\omega\overline{\omega}\right)^{2^{m-1}} - 2 \\ &= \omega^{2^m} + \overline{\omega}^{2^m} \end{aligned} \tag{4.4}$$

Vi har nu vist at (4.3) gælder for både $m = 1$ og for $m = m + 1$, derfor gælder den for alle $m \in \mathbb{Z}$. ■

Vi går nu ud fra at M_p går op i S_{p-1}, og ud fra sætning 4.2 på foregående side får vi at det må betyde følgende:

$$\begin{aligned} S_{p-1} &\equiv 0 \pmod{M_p} \Leftrightarrow \\ \omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} &\equiv 0 \pmod{M_p} \Leftrightarrow \\ \omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} &= RM_p, \qquad R \in \mathbb{Z} \end{aligned} \tag{4.5}$$

I sidste linie skrev vi kongruensen som en normal ligning. Denne arbejder vi videre på, først ganger vi igennem med $\omega^{2^{p-2}}$ og vi flytter 1 over på højresiden:

$$\omega^{2^{p-1}} = RM_p\omega^{2^{p-2}} - 1 \tag{4.6}$$

Vi kvadrerer:

$$\omega^{2^p} = \left(RM_p\omega^{2^{p-2}} - 1\right)^2 \tag{4.7}$$

Vi får brug for (4.6) og (4.7) lidt senere.

Vi vil gå ud fra at M_p *ikke* er et primtal, og vil vise at dette medfører en modstrid. Hvis M_p ikke er et primtal, vil der være en primfakter q som opfylder at $q^2 \leq M_p$.

Vi lader nu $\mathbb{Z}_q$ betegne mængden af heltal modulus q og X betegne mængden $\{a_1 + a_2\sqrt{3} : a_1, a_2 \in \mathbb{Z}_q\}$. Vi definerer to kompositioner på mængden X, addition og multiplikation. I begge tilfælde reducerer vi koefficienterne med *modulus* q.

Addition defineres på normal vis:

$$(a_1 + a_2\sqrt{3}) + (b_1 + b_2\sqrt{3}) = (a_1 + b_1) + (a_2 + b_2)\sqrt{3} \tag{4.8}$$

På samme måde defineres multiplikation som:

$$(a_1 + a_2\sqrt{3}) \times (b_1 + b_2\sqrt{3}) = (a_1b_1 + 3a_2b_2) + (a_1b_2 + b_1a_2)\sqrt{3} \tag{4.9}$$

Vi ser at $(X, +, \times)$ er en algebraisk struktur, da kompositionerne opfylder kravet om at de afbilder mængden X ind i X.

Det neutrale element i X med hensyn til multiplikation er $1 + 0\sqrt{3}$. Da der ifølge sætning C.6 på side 27 højst findes ét neutralt element, er det nok at gøre prøve med $1 + 0\sqrt{3}$ for at vise at det virkeligt er det neutrale element:

$$(a_1 + a_2\sqrt{3}) \times (1 + 0\sqrt{3}) = (1a_1 + 0a_2) + (0a_1 + 1a_2)\sqrt{3} = a_1 + a_2\sqrt{3} \tag{4.10}$$

Vi lader X^* betegne gruppen af invertible elementer i X. Ved at bruge sætning 3.12 på side 14 ser vi at X^* er en gruppe.

Vi ser nu på $\omega = 2 + \sqrt{3}$ som et element i X. ω er også et element i X^* da det er invertibelt: $\omega\overline{\omega} = 1$. Hvis man tænker nærmere over det, vil det først se ud som om at $\overline{\omega} = 2 - \sqrt{3}$ *ikke* er et element i X. Alle elementerne i X har jo formen $a + b\sqrt{3}$ hvor $a, b \in \mathbb{Z}_q = \{0, 1, \ldots q - 1\}$. Koefficienterne skulle altså ikke være negative.

Men da koefficienterne bliver reduceret modulus q, kan de i virkeligheden have denne form:

$$X = \{(a + nq) + (b + nq)\sqrt{3} : a, b \in \mathbb{Z}_q, n \in \mathbb{Z}\} \tag{4.11}$$

I tilfældet med $\overline{\omega} = 2 - \sqrt{3}$, kan vi også skrive $\overline{\omega}$ som $2 + (q-1)\sqrt{3}$ da $q - 1$ også er kongruent med -1 modulus q. Derfor er det faktisk i orden når de i beviserne skriver $\overline{\omega} = 2 - \sqrt{3}$.

Vi valgte q så det gik op i M_p. Derfor gælder der at

$$RM_p\omega^{2^{p-2}} \equiv 0 \pmod{q} \tag{4.12}$$

Set som et element i X er $RM_p\omega^{2^{p-2}}$ altså lig 0, da koefficienterne reduceres modulus q. Ud fra det kan vi omskrive ligningerne (4.6) og (4.7) til:

$$\begin{aligned} \omega^{2^{p-1}} &= RM_p\omega^{2^{p-2}} - 1 \equiv -1 \pmod{q} \\ \omega^{2^p} &= \left(RM_p\omega^{2^{p-2}} - 1\right)^2 \equiv 1 \pmod{q} \end{aligned} \tag{4.13}$$

Set som et element i X får vi altså at

$$\omega^{2^{p-1}} = -1 \qquad \text{og} \qquad \omega^{2^p} = 1 \tag{4.14}$$

Da $\omega^{2^p} = 1 = e$ har vi ifølge sætning 3.11 på side 14 at $\operatorname{ord}\omega$ går op i 2^p. Vi har altså at $\operatorname{ord}\omega = 2^k$ hvor $k \leq p$. Hvis vi kvadrerer $\omega^{2^k} = 1$ får vi $\omega^{2^{k+1}} = 1^2$. Bliver vi ved med at kvadrere får vi til sidst at $\omega^{2^{p-1}} = 1$, hvilket er falsk i følge (4.14). Derfor kan k ikke være mindre end p, hvilket giver os at $\operatorname{ord}\omega = 2^p$.

Da X^* består af alle de invertible elementer fra X, får vi at $\operatorname{ord} X^* \leq q^2 - 1$. Der er nemlig q elementer i $\mathbb{Z}_q$, og vi bruger 2 elementer til hvert element i X. Det giver os at der er q^2 elementer i X. Men da elementet $0 + 0\sqrt{3}$ ikke er invertibelt, findes der højst $q^2 - 1$ elementer i X^*.

ω er et element i X, da $\omega\overline{\omega} = 1$. Her er det at $\overline{\omega} = 2 + (q-1)\sqrt{3}$, så der gælder at både 2 og $q - 1$ er elementer i $\mathbb{Z}_q$. Vi får så ifølge sætning 3.10 på side 13 at

$$\begin{aligned} &\operatorname{ord}\omega \leq \operatorname{ord} X^* \Leftrightarrow \\ &2^p \leq q^2 - 1 \end{aligned} \tag{4.15}$$

Vi har samtidig valgt q sådan at $q^2 \leq M_p$, hvilket giver os at

$$q^2 - 1 \leq M_p - 1 \Leftrightarrow q^2 - 1 \leq 2^p - 2 \tag{4.16}$$

Sætter vi nu (4.15) sammen med (4.16) får vi følgende modstrid:

$$2^p \leq q^2 - 1 \leq 2^p - 2 \tag{4.17}$$

Vi har nu vist at q ikke kan være en primfaktor i M_p. Da vi netop valgte q, så det ville være primfaktor, må det betyde at M_p ikke har nogen primfaktorer overhoved — M_p må derfor være et primtal. ■

Kapitel 5

Lucas-Lehmer sætningen i brug

Nu da vi har vist at Lucas-Lehmer sætningen kan bruges til at afgøre om et givent tal på formen $2^p - 1$ er et primtal, ville det være oplagt at benytte testen i et computerprogram.

5.1 GIMPS-projektet

Der er i øjeblikket en koordineret jagt igang efter meget store Mersenne primtal, kaldet GIMPS. GIMPS er en forkortelse for "The Great Internet Mersenne Prime Search", og som navnet siger foregår eftersøgninger på tværs af Internettet. Omkring 35.000 maskiner hjælper med i projektet[10].

Det foregår sådan, at der kører et program på hver computer der er tilmeldt projektet. Dette program aftaler med en central server, at det undersøger en bestemt eksponent. Den centrale server holder styr på, hvilke eksponenter der stadig er ledige, hvilke der allerede er tjekket én gang osv. På den måde arbejder de mange computere sig efterhånden gennem større og større eksponenter.

Min egen computer har netop afsluttet en test af $M_{10632613}$, som ikke var et primtal. Den er nu igang med $M_{10934279}$. Selv om Lucas-Lehmer testen er meget effektiv i forhold til andre metoder, tager det alligevel omkring en måned at teste bare én eksponent. Og det er endda på en hurtig maskine.

Men GIMPS har alligevel testet omkring 225.000 eksponenter igennem de 4 år projektet har været igang. Alle eksponenter mindre end 3.210.800 er nu dobbelttjekket, og alle under 5.558.700 er tjekket mindst én gang[17].

5.2 Programmet `mprime`

Det program som leder efter Mersenne primtallene hedder `mprime`. Da det trods alt er en tidskrævende proces at gennemføre en Lucas-Lehmer test, prøver man på at undgå den. Man starter derfor med at prøve at finde en faktor ved division[16]. Man bruger en modificeret udgave af Eratosthenes si (se afsnit 1.2.2 på side 3), hvor alle potentielle faktorer på formen $2kp + 1$ bliver

repræsenteret. Man prøver derefter at dividere Mersenne tallet med de divisorer som ikke blev siet fra.

Man laver ikke bare en "normal" division, men bruger en meget hurtig algoritme. Da selve algoritmen blot er en beskrivelse af implementeringen i computeren, har jeg lagt den om i bilaget, se bilag D på side 28.

5.2.1 Lucas-Lehmer testen

Hvis man ikke finder nogen divisorer, må man lave en Lucas-Lehmer test. Sætning 4.1 på side 15 siger at tallet M_p er et primtal hvis det går op i S_{p-1}.

Vi skal altså finde ud af om $S_{p-1} \equiv 0 \pmod{2^p - 1}$. Men hvis vi bare begynder at regne S_{p-1} ud, får vi hurtigt nogle *meget* store tal ($S_5 = 1537110438$), hvilket vi ikke er interesseret i, da disse er langsomme at arbejde med.[1]

Derfor regner vi modulus $2^p - 1$, sådan at vi efter hvert trin reducerer S_n modulus $2^p - 1$. Det kan vi gøre, fordi hvis

$$S_n \equiv k \pmod{2^p - 1} \Leftrightarrow \tag{5.1}$$

så har vi ifølge sætning 2.5 på side 9 at

$$S_n^2 \equiv k^2 \pmod{2^p - 1} \Leftrightarrow \tag{5.2}$$

og vi kan så trække 2 fra på begge sider

$$S_{n+1} = S_n^2 - 2 \equiv k^2 - 2 \pmod{2^p - 1} \tag{5.3}$$

Vi kan altså lige så godt regne videre med et tal som er kongruent med det "rigtige" og alt for store tal S_n. Resten, k i eksemplet, holder sig så hele tiden under $2^p - 1$, hvilket sikre at tallene ikke løber løbsk og bliver alt for store.

Hvis vi efter sidste trin får resten 0, ved vi at $2^p - 1$ er et primtal. Vi demonstrere det ved at vise at $2^{17} - 1$ virkeligt er et primtal. Processen skal så igennem $p - 1 = 16$ trin. Ved hvert trin bruger man resten fra sidste trin, kvadrerer den og trækker 2 fra, og finder en ny rest:

$$\begin{aligned}
S_1 &= 4 \\
S_2 &= 4^2 - 2 &&\equiv 14 &&\pmod{2^{17} - 1} \\
S_3 &= 14^2 - 2 &&\equiv 194 &&\pmod{2^{17} - 1} \\
S_4 &= 194^2 - 2 &&\equiv 37634 &&\pmod{2^{17} - 1} \\
S_5 &\equiv 37634^2 - 2 &&\equiv 95799 &&\pmod{2^{17} - 1} \\
&&&\dots \\
S_{13} &\equiv 69559^2 - 2 &&\equiv 99585 &&\pmod{2^{17} - 1} \\
S_{14} &\equiv 99585^2 - 2 &&\equiv 78221 &&\pmod{2^{17} - 1} \\
S_{15} &\equiv 78221^2 - 2 &&\equiv 130559 &&\pmod{2^{17} - 1} \\
S_{16} &\equiv 130559^2 - 2 &&\equiv 0 &&\pmod{2^{17} - 1}
\end{aligned}$$

[1] Da det er store tal, ganger `mprime` dem ikke sammen på normal vis, men bruger i stedet en hurtigere metode kaldet *irrational base discrete weighted transform*, som involverer en *Fast Fourier Transform* (FFT), en kvadrering og en invers FFT, se [16].

Efter det 4. trin ændrede jeg lignedstegnet (=) til et $\equiv$ da S_5 ikke er lig 37634, men blot er kongruent med det, modulus $2^{17} - 1$. Resten 0 efter det 16. trin, sådan som den skulle, da $2^{17} - 1$ er et primtal.

5.2.2 Dobbelttjek

Alle eksponenter bliver dobbelttjekket for at sikre sig mod fejl, som kan opstå undervejs i den lange Lucas-Lehmer test. Det er ikke selve algoritmen som fejler noget, men i stedet de moderne processorer. Man bruger kommatal (*floating points* på engelsk) til beregningerne, da processorerne er hurtigere til disse beregninger, end til heltalsberegninger. Men der kan så opstå afrundingsfejl undervejs.

Derfor gemmer man de sidste 64 bit af S_{p-1} efter en test, og når så dobbelttjekket er færdigt, sammenligner man disse bit fra de to test. Hvis disse to tal er ens, er begge programmer altså nået frem til det samme tal for S_{p-1}, og eksponenten bliver så erklæret for testet. Det sker sommetider at de to tal ikke stemmer, og så må man igang med en tredje test. Fejlraten på en Lucas-Lehmer test er ifølge [16] lidt over 1%.

Kapitel 6

Konklusion

Vi er nået vidt omkring i denne opgave, men har alligevel hele tiden arbejdet imod målet: at forstå beviset for Lucas-Lehmer sætningen, som jo bygger på snedige argumenter taget fra gruppeteorien, kombineret med modulusregning.

Vi startede med en gennemgang af Mersenne primtallenes historie, og kom i den forbindelse ind på hvor svært det var dengang at afgøre om Marin Mersenne havde ret eller ej.

Jeg har vist hvordan man kan bruge forskellige metoder til at vise at et givent tal er et primtal. Vi så hvordan de fleste metoder er besværlige at bruge, da der skal udføres mange beregninger med store tal.

De nødvendige forudsætninger for beviset af Lucas-Lehmer sætningen blev gennemgået, og sætningen blev da også bevist.

Endelig blev der givet et eksempel på, hvordan man bruger Lucas-Lehmer sætningen i vore dage til at finde meget store primtal.

Jeg synes, at det er lykkedes at vise, hvordan tingene hænger sammen på kryds og tværs af matematikkens grene. Mange spændende aspekter ved kongruenser og grupper er blevet vist og forklaret. Gruppeteori er et interessant emne, da argumenterne ofte bygger på små og i sig selv simple ting, selv deres resultater kan være vidtgående.

Det samme gælder for kongruenser. Med modulusregning har vi et værktøj, hvormed vi nu kan beskrive en masse af det vi allerede viste om tal og deres indbyrdes forhold. Vi kan beskrive det på en fornuftig måde så man kan arbejde systematisk videre med det.

Vi har også set hvor svært det er at finde meget store primtal — og alligevel har man fundet et tal med over 2 millioner cifre ved at bruge Lucas-Lehmer testen.

Bilag A

Tabel over M_p

Tabel A.1 indeholder en komplet list over de 38 Mersenne primtal man har fundet hidtil. Tabellen er hentet fra [5]. Grunden til at det 38. tal står på listen som "??" er, at man endnu ikke har tjekket alle tal mellem $M_{3021377}$ og $M_{6972593}$. Det kan godt tænkes at der gemmer sig endnu et tal i intervallet.

Tabellen indeholder også antallet af cifre i Mersenne primtallet $M_p = 2^n - 1$, så man kan se hvor imponerende store de er. Det perfekte tal $P_p = 2^{p-1}(2^p - 1)$ er også taget med.

Man kan f.eks. lægge mærke til hvor mange cifre der er i M_{127}, som blev fundet i 1876 af Lucas, ved håndkraft. De efterfølgende Mersenne primtal er alle fundet ved brug af elektroniske hjælpemidler.

Tabel A.1: Komplet list over Mersenne primtallene

Nr.	p	Cifre i M_p	Cifre i P_p	År	Opdager
1	2	1	1	—	—
2	3	1	2	—	—
3	5	2	3	—	—
4	7	3	4	—	—
5	13	4	8	1456	Anonym
6	17	6	10	1588	Cataldi
7	19	6	12	1588	Cataldi
8	31	10	19	1772	Euler
9	61	19	37	1883	Pervushin
10	89	27	54	1911	Powers
11	107	33	65	1914	Powers
12	127	39	77	1876	Lucas
13	521	157	314	1952	Robinson
14	607	183	366	1952	Robinson
15	1279	386	770	1952	Robinson
16	2203	664	1327	1952	Robinson
17	2281	687	1373	1952	Robinson
18	3217	969	1937	1957	Riesel
19	4253	1281	2561	1961	Hurwitz

Fortsættes på næste side

Fortsat fra forrige side

Nr.	p	Cifre i M_p	Cifre i P_p	År	Opdager
20	4423	1332	2663	1961	Hurwitz
21	9689	2917	5834	1963	Gillies
22	9941	2993	5985	1963	Gillies
23	11213	3376	6751	1963	Gillies
24	19937	6002	12003	1971	Tuckerman
25	21701	6533	13066	1978	Noll & Nickel
26	23209	6987	13973	1979	Noll
27	44497	13395	26790	1979	Nelson & Slowinski
28	86243	25962	51924	1982	Slowinski
29	110503	33265	66530	1988	Colquitt & Welsh
30	132049	39751	79502	1983	Slowinski
31	216091	65050	130100	1985	Slowinski
32	756839	227832	455663	1992	Slowinski & Gage
33	859433	258716	517430	1994	Slowinski & Gage
34	1257787	378632	757263	1996	Slowinski & Gage
35	1398269	420921	841842	1996	Armengaud og GIMPS
36	2976221	895932	1791864	1997	Spence og GIMPS
37	3021377	909526	1819050	1998	Clarkson og GIMPS
??	6972593	2098960	4197919	1999	Hajratwala og GIMPS

Bilag B

Kongruens

Her er beviser til sætningerne 2.2 til 2.8 på side 8–9.

Bevis af 2.2 Det er klart at 1 altid vil gå op i differencen mellem to heltal. Det er også klart at tallet a går også altid op i sig selv med 0 til rest. ■

Bevis af 2.3 Hvis $a \equiv b \pmod{m}$, gælder der at $\frac{a-b}{m}$ har en heltallig løsning. Men så vil $\frac{d(a-b)}{m}$ også have det, hvormed sætningen er bevist. ■

Bevis af 2.4 Har vi at $a \equiv b \pmod{m}$ og at $c \equiv d \pmod{m}$ betyder det at $a = jm + b$ og at $c = km + d$. Derfor har vi også at $a + c = m(j + k) + b + d$. Derfor er $a + c \equiv b + d \pmod{m}$ da m går op i $m(j + k)$. ■

Bevis af 2.5 Vi har at $a \equiv b \pmod{m}$ og $c \equiv d \pmod{m}$. Bruger vi så sætning 2.3 på side 9 får vi at $ac \equiv bc \pmod{m}$ og $bc \equiv bd \pmod{m}$ Sætter vi det sammen får vi at $ac \equiv bc \equiv bd \pmod{m} \Leftrightarrow ac \equiv bd \pmod{m}$. ■

Bevis af 2.6 $a \equiv b \pmod{m}$ betyder at $a = jm + b$ hvor $j \in \mathbb{Z}$. Ligeledes har vi at $b \equiv c \pmod{m} \Leftrightarrow b = km + c$, hvor $k \in \mathbb{Z}$.

Vi kan derfor lave følgende omskrivning $a \equiv c \pmod{m} \Leftrightarrow jm + b \equiv b - km \pmod{m} \Leftrightarrow m(j + k) + b \equiv b \pmod{m}$. Sidste kongruens er sand, da m selvfølgelig går op i $m(j + k) + b$ til sidst med b som rest. ■

Bevis af 2.7 Hvis $a \equiv b \pmod{m}$ har vi at $a = jm + b \Leftrightarrow a + km = m(j + k) + b$. Det giver os at $a + km \equiv b \pmod{m}$. Sætningen gælder selvfølgelig også hvis vi trækker et antal m fra a. ■

Bevis af 2.8 For at $a \equiv b \pmod{m}$ skal være sand, skal vi som bekendt kunne finde en heltallig løsning til ligningen $\frac{a-b}{m} = n$. Hvis vi forlænger brøken med c får vi at $\frac{ac-bc}{mc} = n$, hvilket også er sandt. ■

Bilag C

Grupper

Som omtalt på side 11, vil vi her definere de regneregler som gælder for algebraiske strukturer og derved også for grupper.

C.1 Regneregler

Vi vil nu fastlægge de normale regneregler i forbindelse med algebraiske strukturer og deres kompositioner. Vi starter med at definere at

DEFINITION C.1 *Udtrykket $a*b*c$ skal forstår som $(a*b)*c$. På samme måde definerer vi en komposition mellem f.eks. 6 elementer som:*

$$a_1 * a_2 * a_3 * a_4 * a_5 * a_6 = \Big(\Big(\big((a_1 * a_2) * a_3\big) * a_4\Big) * a_5\Big) * a_6 \tag{C.1}$$

Ved n elementer får vi $n-2$ parenteser foran første led.

Vi vil gerne have en kortere måde at skrive $a * a * a * a * \cdots * a$ på, og introducerer derfor skrivemåde

DEFINITION C.2 *$a * a * a * a * \cdots * a$, hvor a optræder n gange skrives som:*

$$a * a * a * a * \cdots * a = a^{n*} \tag{C.2}$$

Det medfører at

$$a = a^{1*} \tag{C.3}$$

C.2 Den associative lov

Den associative lov, se definition 3.3 på side 12, siger, at vi kan sætte og hæve parenteser i et udtryk med 3 led, uden at værdien af udtrykket ændrer sig. Følgende sætning, som er taget fra [13, s. 137], udtaler sig om tilfældet hvor der er n led

SÆTNING C.3 *Hvis $a_1, a_2, a_3, \ldots a_n$ alle er elementer i semigruppen $(M, *)$, ændres udtrykket*

$$a_1 * a_2 * a_3 \ldots a_n \tag{C.4}$$

sig ikke ved at sætte parenteser omkring nogle af leddene.

Bevis af C.3 Hvis vi skriver udtrykket med alle de underforståede parenteser ser vi

$$\Big(\big(\ldots\big((a_1 * a_2) * a_3\big) * \cdots * a_{n-2}\big) * a_{n-1}\Big) * a_n \tag{C.5}$$

at vi kan flytte den yderste parentes hen omkring a_{n-1} og a_n, ved at gøre brug af den associative lov.

Vi kan sætte parenteser omkring to vilkårlige naboled a_p og a_{p+1} på denne måde, da der altid vil være en underforstået parentes, som slutter mellem a_p og a_{p+1}. Denne parentes kan fjernes, samtidig med at vi sætter en parentes omkring a_p og a_{p+1}. ■

Nu da vi har vist at vi kan sætte parenteser som vi vil i forbindelse med en associativ komposition, kan vi hurtigt bevise de regler, som ligger til grund for regning med potenser[13, s. 137]:

SÆTNING C.4 *Har vi en semigruppe $(M, *)$ med et element a, og to tal $m, n \in \mathbb{Z}$, gælder der at*

$$a^{m*} * a^{n*} = a^{(n+m)*} \qquad og \qquad (a^{m*})^{n*} = a^{(nm)*} \tag{C.6}$$

Bevis af C.4 Beviset er trivielt, da vi bare skal flytte parenteser. Vi skriver først $a^{m*} * a^{n*} = a^{(n+m)*}$ ud med de underforståede parenteser:

$$\underbrace{\Big(\big(\ldots\big((a * a) * a\big) * \cdots * a\big) * a\Big)}_{\text{ialt } n \text{ } a\text{'er}} * \underbrace{\big(\ldots\big((a * a) * a\big) * \cdots * a\big)}_{\text{ialt } m \text{ } a\text{'er}} \tag{C.7}$$

Hæver vi alle parenteserne, får vi som ønsket

$$\underbrace{a * a * a * \cdots * a * a}_{\text{i alt } n+n \text{ } a\text{'er}} = a^{(n+m)*} \tag{C.8}$$

På samme måde kan det nemt vises at $(a^{m*})^{n*} = a^{(nm)*}$. ■

Sætning C.4 kan direkte overføres til vores normale potensregler, da $(R, \times)$ udgør en semigruppe idet multiplikation er associativ: $(a \times b) \times c = a \times (b \times c)$.

C.3 Den kommutative lov

Når både den associative og den kommutative lov (se definition 3.4 på side 12) er opfyldt, gælder der følgende sætning:

SÆTNING C.5 *Hvis $a_n, a_2, a_3, \ldots, a_{n-1}, a_n$ er elementer i en kommutativ semigruppe $(M, *)$, ændres værdien af udtrykket*

$$a_n * a_2 * a_3 * \cdots * a_{n-1} * a_n \tag{C.9}$$

ikke, hvis man ændrer leddenes rækkefølge.

Bevis af C.5 Da kompositionen er associativ kan vi sætte parenteser hvor vi vil. Vi sætter så parenteser rundt om et led a_p og a_{p+1}. Da den kommutative lov også gælder, kan vi bytte disse to led. Når vi så hæver parenteserne igen, har vi byttet rundt på leddene.

Ved gentagne gange at bytte rundt på leddene, kan vi altså ændre rækkefølgen af leddene til en hvilken som helst rækkefølge vi er interesseret i, *uden* at ændre på værdien af udtrykket. ■

C.4 Neutralt og inverst element

Når man snakker om et neutralt element, se definition 3.5 på side 12, kan man vise at

SÆTNING C.6 *Der er højst ét neutralt element i en algebraisk struktur.*

Dette bevis kommer fra[13, s. 140]:

Bevis af C.6 Hvis både e og f er neutrale elementer, så gælder der at

$$f = e * f = f * e = e \Leftrightarrow f = e \tag{C.10}$$

Derved har vi vist, at der højst findes ét unikt neutralt element i en algebraisk struktur. ■

Det viser sig, at der ligesom ved det neutrale element, højst findes ét inverst element, se definition 3.6 på side 12, til et givent a:

SÆTNING C.7 *Der findes højst ét inverst element til a som opfylder ligningssystemet*

$$x * a = e, \qquad a * x = e \tag{C.11}$$

Bevis af C.7 Som i beviset af det unikke neutrale element, vil vi vise at to løsninger til ligningssystemet, i virkeligheden er den samme.

Hvis der finde to løsninger, a_1 og a_2, må der gælde følgende om dem:

$$a_1 = a_1 * e = a_1 * (a * a_2) = a_1 * a * a_2 = (a_1 * a) * a_2 = e * a_2 = a_2 \tag{C.12}$$

Vi har her kun brugt den associative lov,[1] som giver os mulighed for frit at hæve og sætte parenteser. Det viste sig, at de to løsninger var ens. ■

[1] Vi arbejder i en semigruppe, hvor kompositionen per definition er associativ.

Bilag D

Hurtig division

Her kommer en beskrivelse af den algoritme man bruger i `mprime` til at dividere af $2^p - 1$ med de potentielle divisorer, som ikk er blevet siet fra i den indledende sortering.

D.1 Algoritmen

Trinnene i algoritmen er:

1. En potentiel faktor til $2^p - 1$ vælges, kald den q.
2. Eksponenten, p, skrives så som et binært tal, kaldet p_2
3. Vi starter med at se på den mest betydende bit i p_2 (den længst mod venstre), og sætter resten lig 1.
4. Resten kvadreres.
5. Hvis den aktuelle bit er lig 1, ganges resten med 2, ellers forbliver den uændret. Vi ser så på næste bit i p_2.
6. Resultatet reduceres modulus $2^p - 1$ hvorved der fremkommer en rest.
7. Trinnene 4 til 6 gentages indtil man har været igennem alle bits i p_2.

D.2 Eksempel

Hvis man f.eks. gerne vil finde en faktor til M_{29} (som ikke er et primtal), skal den have formen $q = 2 \cdot 29k + 1$, og der skal også gælde at $q \equiv \pm 1 \pmod 8$. Det giver os alt i alt at der skal gælder følgende om divisoren q:

$$q = 58k + 1 \equiv \pm 1 \pmod 8 \tag{D.1}$$

Vi prøver os frem og finder at $p = 58 \cdot 3 + 1 = 175$ og $q = 58 \cdot 4 + 1 = 233$ er mulige divisorer, da der gælder at $175 \equiv 7 \pmod 8$ og $233 \equiv 1 \pmod 8$. Vi starter med $p = 175$.

Første trin i algoritmen er at skrive eksponenten som et binært tal: $29_{10} = 11101_2$. De små mærker forneden angiver talsystemet. Vi starter med 1 som vi

kvadrerer. Vi ser så på den mest betydende bit i eksponenten som er 1, hvilket betyder at vi skal gange med 2 og finder resten ved division med 175. Resten bliver så 2.

Vi gentager proceduren, og får denne gang at $2^2 \cdot 2 \equiv 4 \pmod{175}$. Vi ganger med 2, da den næste bit også er 1. Fortsætter vi, kan vi udfylde et skema som det i tabel D.1.

Kvadrering	Bit	Gange med 2	Rest
$1^2 = 1$	1	$1 \cdot 2 = 2$	2
$2^2 = 4$	1	$4 \cdot 2 = 8$	8
$8^2 = 64$	1	$64 \cdot 2 = 128$	128
$128^2 = 16384$	0	Nej	109
$109^2 = 11881$	1	$11881 \cdot 2 = 23762$	137

Tabel D.1: Trinene i division af $2^{29} - 1$ med 175.

Tabel D.1 fortæller os at den sidste rest blev 137. Det betyder at $2^{29} \equiv 137 \pmod{175}$. Trækker vi en fra på begge sider, får vi at $2^{29} - 1 \equiv 136 \pmod{175}$. 175 er altså ikke en faktor i M_{29}. Prøver vi så i stedet med den mulige divisor 233, får vi de udregninger som findes i tabel D.2.

Kvadrering	Bit	Gange med 2	Rest
$1^2 = 1$	1	$1 \cdot 2 = 2$	2
$2^2 = 4$	1	$4 \cdot 2 = 8$	8
$8^2 = 64$	1	$64 \cdot 2 = 128$	128
$128^2 = 16384$	0	Nej	74
$74^2 = 5476$	1	$5476 \cdot 2 = 10952$	1

Tabel D.2: Trinene i division af $2^{29} - 1$ med 233.

Så fortæller tabel D.2 os at $2^{29} \equiv 1 \pmod{233} \Leftrightarrow 2^{29} - 1 \equiv 0 \pmod{233}$. Vi kan altså nu konstatere at 233 er en faktor i M_{29}, som så ikke kan være et primtal.

Bilag E

Elektroniske kilder

Der er i opgaven brugt en række elektroniske kilder i form af sider fra Internettet. Følgende kilder findes derfor på den vedlagte diskette: [3], [4], [5], [6], [7], [10], [16] og [17].

Kilderne er navngivet med samme nummer som her i opgaven, f.eks har [3] fået filnavnet `kilde3.html` på disketten.

Litteratur

[1] R. B. J. T. Allenby. *Rings, Fields and Groups*. Hodder Headline PLC, 338 Euston Road, London NW1 3BH, 1991, anden udgave. ISBN 0-7131-3476-3.

[2] J. W. Bruce. A really trivial proof of the Lucas-Lehmer test. *American Math Monthly*, 100, 370–371, 1993.

[3] Chris K. Caldwell. All even perfect numbers are a power of two times a mersenne prime. *Prime Pages' list of proofs*. URL http://www.utm.edu/research/primes/notes/proofs/EvenPerfect.html

[4] Chris K. Caldwell. If 2^n-1 is prime, then so is n. *Prime Pages' list of proofs*. URL http://www.utm.edu/research/primes/notes/proofs/Theorem2.html

[5] Chris K. Caldwell. Mersenne Primes: History, Theorems and Lists. *Prime Pages' list of proofs*. URL http://www.utm.edu/research/primes/mersenne.shtml

[6] Chris K. Caldwell. Modular restrictions mersenne divisors. *Prime Pages' list of proofs*. URL http://www.utm.edu/research/primes/notes/proofs/MerDiv.html

[7] Chris K. Caldwell. Sigma function $\sigma(n)$. *The Prime Glossary*. URL http://www.utm.edu/research/primes/glossary/SigmaFunction.html

[8] Peter J. Cameron. *Introduction to Algebra*. Oxford University Press, Great Clarendon Street, Oxford OX2 6DP, 1998. ISBN 0-19-580195-1.

[9] Jens Carstensen og Jesper Frandsen. *Mat 3A*. Systime, Skt. Pauls Gade 25, DK-8000 Århus C, 1999. ISBN 87 616-0053-9.

[10] Entropia. Current internet primenet server world test status. *Internet PrimeNet Server*, 2001. URL http://www.mersenne.org/primenet/status.shtml#status

[11] Peter Giblin. *Primes and Programming*. Cambridge University Press, The Pitt Building, Trumpington Street, Cambridge CB2 1RP, 1993. ISBN 0-521-40182-8.

[12] I. N. Herstein. *Topics in Algebra*. Wiley International Editions, 605 Third Avenue New York, New York 10016, 1975, anden udgave. ISBN 0-471-02371-X.

[13] Erik Kristensen og Ole Rindung. *Matematik 2.2*. G. E. C. Gad, København, 1977, tredie udgave. ISBN 87-18-47785-0.

[14] Paulo Ribenboim. *The Book of Prime Number Records*. Springer-Verlag, 175 Fifth Avenue, New York, 1988. ISBN 0-387-96573-4.

[15] M. I. Rosen. A proof of the Lucas-Lehmer test. *American Math Monthly*, 95, 855–856, 1988.

[16] George Woltman. The math. *Mersenne.org*, Januar 2001. URL http://www.mersenne.org/math.htm

[17] George Woltman. Search status. *Mersenne.org*, Januar 2001. URL http://www.mersenne.org/status.htm