3.1. Formodninger om primtall.

(3.1.1) Mersenne, Godbach og primtallstvillinger. Vi skal her forklare noen av de mest kjente formodningene om primtall.

(3.1.2) Definition. Et *primtall* er et heltall p, større eller lik 2 som bare er delbart med ± 1 og $\pm p$.

De første primtallene er 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.

(3.1.2) Oppgave. Beskriv en metode for å finne alle primtall opp til et gitt tall n.

Hint: Skriv opp en liste 2, 3, 4, ... , $n-1$, n av tallene opp til n. Stryk alle tallene som er delbare med 2. Det minste tallet som gjenstår er da primtallet 3. Stryk deretter alle tall som er delbare med 3. Det minste gjenstående tallet er primtallet 5. Fortsett til alle tall er oppbrukt.

(3.1.3) Oppgave. Vis at det finnes uendelig mange primtall.

Hint: (Euclid $\sim 300 f.Kr$) Anta at det bare finnes et endelig antall primtall $p_1, p_2, \ldots, p_r$. Tallet $p_1, p_2, \cdots p_r + 1$ kan skrives som et produkt av primtall. Ingen av disse kan imidlertid være blandt $p_1, p_2, \ldots, p_r$ ettersom de da måtte dele 1. Dette strider mot antagelsen om at $p_1, p_2, \ldots, p_r$ er alle primtallene.

(3.1.4) Definition. *Mersenne tallene* er tallene $M_p = 2^p - 1$ der p er et primtall. Om tallet M_p er et primtall kaller vi det et *Mersenne primtall.*

Mersenne tallene er oppkalt etter Marin Mersenne (1588-1648) som var en sentral person i matematikken i begynnelsen på 16-hundretallet. De første Mersenne tallene er $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$. Tallene M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19} er Mersenne primtall mens $M_{11} = 23 \cdot 89$ og 47 deler M_{23}.

(3.1.4) Formodning. Det finnes uendelig mange Mersenne primtall.

(3.1.5) Bemerkning. Om M_p er et Mersenne primtall så vil $2M_p = 2(2^p - 1) = 2^{p+1} - 2$. Når p er odde får vi derfor at $2M_p = n^2 - 2$ der $n = 2^{\frac{p+1}{2}}$. Vi kan derfor gjøre en enklere formodning:

(3.1.5) Formodning. Det finnes uendelig mange tall n slik at $n^2 - 2$ er to ganger et primtall.

En liknende formodning er:

(3.1.6) Formodning. Det finnes uendelig mange tall n slik at $n^2 - 2$ er et primtall.

(3.1.7) Oppgave. Finn tall n slik at $n^2 - 2$ er et primtall, eller to ganger et primtall.

I en litt annen retning har vi formodningen:
kodertall

(3.1.7) Formodning. Det finnes uendelig mange primtall p slik at $q = 2p+1$ er primtall.

Denne formodningen er relatert til en formodning om primtallstvillinger, som er blandt de mest kjente i matematikken. *Primtallstvillinger* er par (p, q) av primtall slik at at $q-p = 2$. De første primtallstvillingene er (3.5), $(5, 7)$, $(11, 13)$, $(17, 19)$, $(29, 31)$. Vi vet at $(1706595 \cdot 2^{11235} - 1,\ 1706595 \cdot 2^{11235} + 1)$ er primtallstvillinger [R].

→ **(3.1.8) Oppgave.** Bruk primtallene fra Oppgave (3.1.2) til å finne primtallstvillinger.

(3.1.8) Formodning. Det finnes uendelig mange primtallstvillinger.

Vi vet (se e.g. [B] og [R]) at

$$B = \left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \left(\frac{1}{11} + \frac{1}{13}\right) + \left(\frac{1}{17} + \frac{1}{19}\right) + \left(\frac{1}{29} + \frac{1}{31}\right) + \cdots,$$

det vil si summen av de inverse av alle primtallstvillinger er lik $1.90216054\cdots$. Derimot vet vi at summen av de inverse av alle primtall $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{23} + \ldots$, divergerer. Dette skulle snarere tyde på at det bare finnes et endelig antall primtallstvillinger. Vi kjenner imidlertid så store primtallstvillinger at det er grunn til å tro formodningen om at det finnes uendelig mange primtall.

En annen berømt formodning som alle bør kjenne til er:

(3.1.9) Formodning. (Goldbach) Hvert like tall større enn 3 kan skrives som en sum av to primtall.

Christian Goldbach 1690-1764 formodet i et brev til Leonard Euler (1707-1783) i 1742 at hver tall $n > 5$ kan skrives som en sum av 3 primtall. Euler svarte at dette er ekvivalent med det vi i dag kaller Godbachs hypotese.

For eksempel har vi $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7 = 5 + 5$, $12 = 5 + 7$. *Goldbachs formodning* har blitt vist for alle tall mindre eller lik 10^8 (se e.g. [S] eller [R]). Jing-run Chen [C] viste i 1973 at hvert like tall større enn 3 kan skrives på formen $p + q \cdot r$ der p, q og r er primtall.

(3.1.10) Oppgave. Verifiser at Godbachs hypotese holder for så mange like tall som mulig.

Alle disse formodningene er gamle og en rekke tidenes fremste matematikere har arbeidet med dem. De er også kontrollert opp til astronomiske tall. Mye er kjent om tallteori, og det finnes et stort antall meget kraftfulle metoder (se e.g. [HW]). Til tross for dette er det ingen som har en god ide om hvordan disse formodningene skal vises, eller hvilke metoder som skal brukes.

3.2. Litt elementær tallteori.

(3.2.1) Fermats Lille Sats og Carmichaeltall. Tallteorien består ikke bare av formodninger. Den er også full av vakre og dype resultater og teorier. Vi skal kikke på et par elementære resultater som vi vil bruke i neste seksjon.

La N være et helt tall. Om a og b er to heltall slik at n deler $a-b$ skriver vi

$$a \equiv b \pmod{n}$$

og sier at *a er kongruent med b modulo n.* Dette kan virke som en komplisert måte å uttrykke saken på, men er en genial terminologi, som viler på fundamentale prinsipper i matematikken.

(3.2.2) Oppgave. Vis at om $a \equiv b \pmod{n}$ og $c \equiv d \pmod{n}$ så vil $b \equiv a \pmod{n}$, $a-c \equiv b-d \pmod{n}$ og $ac \equiv bd \pmod{n}$.

(3.2.3) Oppgave. La n være et helt positivt tall. Vis at for hvert tall a så finnes et tall r slik at $0 \leq r \leq n-1$ og $a \equiv r \pmod{n}$. Overbevis deg selv om at det for hvert e er lett å finne r slik at $a^e \equiv r \pmod{n}$ med $0 \leq r \leq n-1$, til tross for at a^e er altfor stor for å kunne beregnes.

(3.2.4) Theorem. (Fermats Lille Sats) *La p være et primtall. For hvert heltall a som ikke er delbart med p har vi*

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

(3.2.5) Oppgave. Bevis Fermats Lille Sats.

Hint: Vi at om $a \equiv r_1, 2a \equiv r_2, \ldots, (p-1)a \equiv r_{p-1} \pmod{n}$ med $0 \leq r_i \leq p-1$ så vil $r_1, r_2, \ldots, r_{p-1}$ være ulike. Ta produktene av høyre og venstre sidene i de $p-1$ kongruensene vi har skrevet opp. Da får vi at $(1 \cdot 2 \cdots (p-1))a^{p-1} \equiv (1 \cdot 2 \cdots (p-1)) \pmod{n}$. Dette medfører Fermats Lille Sats fordi p ikke deler $1 \cdot 2 \cdots (p-1)$.

(3.2.6) Oppgave. Vis at det følger av Fermats Lille Sats at om p og q er ulike primtall, og a og b er tall som ikke er delbare med p respektive q så har vi at $a^{p-1}b^{q-1} \equiv 1 \pmod{p} \cdot q$.

Vi kan spørre i hvilken omfatning Fermats Lille Sats holder for andre tall enn primtall, det vil si om det er mulig at følgende:

$$a^{n-1} \equiv 1 \pmod{n} \text{ for alle tall } a \text{ som er primiske med } n$$

kan holde for et sammensatte tall n.

Merk at for tall a og n som ikke er primiske er det umulig at $a^{n-1} \equiv 1 \pmod{n}$ holder fordi hver divisor i a og n må da dele 1.

(3.2.7) Definition. Vi sier at et sammensatt tall n slik at $a^{n-1} \equiv 1 \pmod{n}$ for alle heltall a som er primiske med n er et *Carmichaeltall*.

Det viser seg at det er veldig få Carmichaeltall [Cl]. De første er 561, 1105, 1729, 1905, 2465, 2821, 6601. Til tross for dette var det ikke før i 1974 at W. Alford, A. Granville og C. Pomerance viste [AGP] at det finnes uendelig mange Carmichaeltall.

(3.2.8) Oppgave. Sjekk at vi skjelden har at $a^{n-1} \equiv 1 \pmod{n}$ for alle heltall a primiske med n når n er et sammensatt tall. Det vil si, fortsett listen $3^3 \equiv 3 \not\equiv 1 \pmod{4}$, $5^5 \equiv 5 \not\equiv 1 \pmod{6}$, $3^7 \equiv 3 \not\equiv 1 \pmod{8}$, $3^9 \equiv 3 \not\equiv 1 \pmod{10}$, $5^{11} \equiv 5 \not\equiv 1 \pmod{12}$.

(3.2.9) Oppgave. La n være et sammensatt tall som ikke er et Carmichaeltall. Da finnes et tall b primisk med n slik at $b^{n-1} \not\equiv 1 \pmod{n}$. La $r_1, r_2, \ldots, r_m$ være alle tallene blandt $1, 2, \ldots, n-1$ som er primiske med n, og som er slik at $r_i^{n-1} \equiv 1 \pmod{n}$. Videre la $br_1 \equiv s_1, \ldots, br_m \equiv s_m \pmod{n}$, der $0 \leq s_i \leq n-1$. Vis at tallene s_i er primiske med n og at $s_i^{n-1} \not\equiv 1 \pmod{n}$. Derfor utgjør tallene $r_1, r_2, \ldots, r_m$ høyst halvparten av tallene $1, 2, \ldots, n-1$ som er primiske med n. Med andre ord, om n er et sammensatt tall som ikke er et Carmichaeltall, og om vi velger et vilkårlig tall a blandt $1, 2, \ldots, n-1$ som er primisk med n så er sjansen høst $\frac{1}{2}$ for at $a^{n-1} \equiv 1 \pmod{n}$.

3.3. Offentlig kryptering.

(3.3.1) RSA. Om to personer vil sende hemmelige meddelelser til hverandre kan de skaffe seg en kodebok som de bruker til å kryptere og avkryptere meddelelser med. Om de bare er passe smarte kan de gjøre dette slik at ingen andre, som ikke har kodeboken, kan avkryptere en kryptert meddelelse. Slike metoder er ofte upraktiske, og forsøker man å gjøre dem mer anvendbare åpner de seg for personer som vil avkryptere uten kodebok.

Ofte er det ikke to personer som vil sende hemmelige meddelelser til hverandre, men mange personer som vil sende en hemmelig meddelelse til en eneste person. Slik er det for eksempel når vi vil bruke kontokort og vil kryptere kontonummer og beløp slik at bare banken kan avkryptere informasjonen. Lenge filosoferte man på om dette var mulig. Slike koder ble kalt *offentlig krypteringskoder* ettersom alle har nøkkelen til krypteringen. I 1979 konstruerte tre matematikere R. Rivest, A. Shamir og L. Adleman en slik kode [RSA] (see e.g. [H]). Koden kalles *RSA-koden.* Ideen er enkel. De som skal kryptere en meddelelse bruker et stort tall n, som alle kjenner og som er et produkt av to store primtall, men de kjenner ikke disse primtallene. For å avkryptere meddelelsen må man kjenne til disse primtallene, og det gjør bare mottakeren. Metoden bygger på at selvom man kjenner et tall og vet at det er et produkt av to primtall tar det uhyggelig lang tid å finne disse primtallene om tallet er stort.

Vi skal forklare hvordan RSA krypterer og avkrypterer meddelelser:

For dette velger vi et tall n som er et produkt $n = p \cdot q$ av to primtall p og q. Vi tenker oss at alle meddelelser representeres av et tall som er mindre enn n. Dette er lett gjort. Består meddelelsen av bokstaver kan vi for eksempel representere a ved tallet 01, b ved tallet 02 og så videre. Er meddelelsen så lang at tallet som representerer meddelelsen blir større enn n kan vi dele opp tallet i deler som er mindre enn n og sende hver del for seg.

Før vi kan begynne å kode finner vi minste felles multiplum m av tallene $p-1$ og $q-1$. Ettersom $p-1$ og $q-1$ er ulike tall har vi att $m \leq (p-1)(q-1)/2$. Det er nu lett å finne heltall r og s slik at

$$rs \equiv 1 \pmod{m}.$$

Vi gir tallene r og n til alle som vil kryptere. En meddelse M krypteres til meddelelsen c_M bestemt ved at

$$c_M \equiv M^r \pmod{n}$$

der $0 \leq c_M \leq n-1$.

Den som kjenner til tallet s kan lett avkryptere meddelelsen fordi:

$$M \equiv c_M^s \pmod{n}.$$

For å vise at den siste likheten gjelder bruker vi først at ved definisjonen av minste felles multiplum så finnes det et tall e slik at $m = e(p-1)(q-1)$. Videre følger det av at $rs \equiv 1 \pmod{m}$ at det finnes et helt tall d slik at $rs = 1 + dm$. Derfor
→ følger det av Oppgave (3.2.6) at $M^m \equiv M^{e(p-1)(q-1)} \equiv (M^{(p-1)(q-1)})^e \equiv 1^e \equiv 1 \pmod{n}$. Derfor får vi at $c_M^s \equiv M^{rs} \equiv M^{1+dm} \equiv M(M^m)^d \equiv M \cdot 1 \equiv M \pmod{n}$, som vi ville vise.

(3.3.3) Bemerkning. Det er klart at vi ikke, på noen lett måte, kan rekonstruere tallene p og q fra r og n. Kjenner vi derimot r, s og n er det mye raskere å finne p og q fordi m er en divisor i $rs - 1$ og kjenner vi m så er vi nære ved å finne $(p-1)(q-1)$ og dermed p og q.

3.4. Store Primtall.

(3.4.1) Store Primtall. Som vi har sett må vi for å konstruere bra offentlig kryperingskoder kunne konstruere store primtall. Takket være at det finnes så få Carmichaeltall er dette lett, ialfall med stor sannsynlighet (see e.g. [P] og [W]).

Vi vil teste om et gitt tall n er primtall. Velg først et vilkårlig tall a_1 blandt $2, 3, \ldots, n-1$. Test om a_1 er primiske med n. Er den ikke det kan ikke n være et primtall, og vi er ferdige. Om a_1 er primisk med n prøver vi om vi har $a_1 \equiv 1$
→ (mod n). Holder ikke dette, hvilket det på grunn av (3.2.9) ikke gjør med en sannsynlighet av minst $\frac{1}{2}$ om n er sammensatt og ikke et Carmichaeltall, følger det av Fermats Lille Sats at n ikke er et primtall og vi er ferdige. Om vi har at $a_1 \equiv 1 \pmod{n}$ så velger vi et nytt vilkårlig tall a_2 blandt $2, 3, \ldots, n-1$. Test om a_2 er primiske med n. Er den ikke det kan ikke n være et primtall, og vi er ferdige. Om a_2 er primisk med n prøver vi om vi har $a_2 \equiv 1 \pmod{n}$. Holder ikke dette,
→ hvilket det på grunn av (3.2.9) ikke gjør med en sannsynlighet av minst $\frac{1}{2}$ om n er sammensatt og ikke et Carmichaeltall, følger det av Fermats Lille Sats at n ikke er et primtall og vi er ferdige. Den sammensatte sannsynligheten for at $a_i^{n-1} \equiv 1 \pmod{n}$ ikke holder for $i = 1$ og $i = 2$ om n er et sammensatt tall som ikke er et Carmichaeltall er større enn $1 - \frac{1}{2^2}$. Om vi har at $a_2 \equiv 1 \pmod{n}$ så velger vi et nytt vilkårlig tall a_3 blandt $2, 3, \ldots, n-1$, og fortsetter prosessen. Etter r steg har vi enten funnet at n ikke er et primtall, eller at $a_i^{n-1} \equiv 1 \pmod{n}$ for $i = 1, 2, \ldots, r$. Det vil si, vi har at n er et primtall *med en sannsynlighet av* $1 - \frac{1}{2^r}$. Dette er en meget rask metode for å finne store primtall, med *stor sannsynlighet.*

(3.4.3) Oppgave. Bruk metoden ovenfor til å bestemme om tall du selv velger er primtall.

3.4. Referenser.

[AGP] W.R. Alford, A. Granville, & C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (1994), no. 139, 703-722.

[B] V. Brun, *La série* $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ *où les dénominaterurs sont 'nombres primes jumeaux' est convergente ou finie*, Bull.Sci. Math. (1919), no. 43, 101-204, 124-128.

[Cl] R.D. Carmichael, *On composite numbers P which satisfy the Fermat congruence* $a^{p-1} \equiv 1 \pmod{P}$, Amer. Math. Monthly (1912), no. 19, 22-27.

[C] H. Chen, *On the representation of large even integers as the sum of a prime and the product of at most two primes*, Sci. Sinica (1973), no. 16, 157-176.

[H] J. Håstad, *Offentlig kryptering*, Välj specialarbete i matematik (Dan Laksov, ed.), ISBN: 91-7170-851-0, THD AB, BANDHAGEN 1989, 1989.

[HW] G.H. Hardy & E.M. Wright, *An introduction to the theory of numbers*, Fith edtion, Oxford Univ. Press, Oxford 1979, 1979.

[P] C. Pomerance, *Recent developments in primality testing*, Mathematical intelligenser **3** (1981), 97-105.

[R] P. Ribenboim, *The little book of big primes*, ISBN 0-387-97508-X, Springer Verlag, New Your, 1991.

[RSA] R. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of ACM **21** (1979), 120-126.

[S] D. Shanks, *Solved and Unsolved Problems in Number Theory*, Fourth Edition, ISBN 0-8284-1297-9, Chelsea Publishing Company, New York, 1993.

[W] S. Wagon, *Primality testing*, Mathematical intelligenser **8:3** (1986), 58-61.