MA1301 Tallteori — Høsten 2014

Richard Williamson

21. august 2015

Innhold

Forord

Pensumet

Disse notatene er pensumet for årets kurs. De er basert på tekstboka ≪Elementary number theory≫ av David M Burton, men er ofte ganske ulike. Når notatene skiller seg fra boka, er det notatene og ikke boka som bør følges.

Det er ingen plikt til å bruke tekstboka. Notatene har blitt skrevet i den hensikt at de skal være lett å lese og lære fra. Det kan være bedre å følge en fremstilling enn to[1].

Lenker til informasjon om de historiske skikkelsene som skapte tallteori kommer til å bli lagt ut på kursets hjemmeside. Disse vil dekke de fleste historiske notatene i tekstboka, men les gjerne dem også.

Guide

Notatene følger en struktur hvor diskusjon og utdypninger er skilt fra formelle definisjoner, proposisjoner, og andre typer påstander. For hver proposisjon eller annen type påstand, brukes alltid følgende mønster:

(1) Proposisjonen gis først;

(2) Etterfulgt av dens bevis;

(3) Eksempler på det som proposisjonen og dens bevis fastslår kommer så. Av og til er det i tillegg merknader til beviset eller proposisjonen.

Det kan være lurt å lese eksemplene rett etter å ha lest proposisjonen, og så gå tilbake og lese beviset. På denne måten blir proposisjonen litt mer konkret.

Det tar litt tid å bli fortrolig med den abstrakte og konsise måten matematikk skrives på. Ikke gi deg: det kommer etter hvert!

Oppgavene

Etter kapitlene finnes oppgaver, som er delt inn i to.

(1) *Oppgaver i eksamens still* er ≪vanlige matematiske oppgaver≫: de gir deg muligheten til å øve deg på å bruke teorien som ble introdusert i kapittelet, og dermed å vurdere din forståelse av kapittelets innhold.

[1] Likevel er det obligatorisk å ha en kopi av tekstboka! Siden jeg skriver notatene i år og bruker dem for første gang, kan det være greit å ha tekstboka som et sikkerhetsnett.

(2) *Oppgaver for å hjelpe med å forstå kapittelet* tar for seg teorien som ble introdusert i kapittelet. Noen ganger ser bevis og definisjoner litt avskrekkende ut til å begynne med: kanskje ser de litt for abstrakte ut, eller de benytter seg av notasjoner som man ikke føler seg fortrolig med. Målet med disse oppgavene er å hjelpe deg å få en god forståelse. Hvis du synes noe i kapittelet er vanskelig, se på oppgavene, og prøv å gjøre de som handler om det du sliter med.

Takk

Jeg takker den vidunderlige kona mi, Kari, så mye for all hjelpen med norsken. Jeg takker også Magnus Bakke Botnan, Truls Bakkejord Ræder, Gard Spreemann, og Marius Thaule for hjelpen med norsken, spesielt med ≪matematisk norsk≫.

Fremfor alt takker jeg Kari og lille Åsmund for å ha gjort dagene da disse notatene ble skrevet så lykkelige, fylt av latter, sang, og de gledelige smilene som bare en baby gir!

1 Induksjon og rekursjon

1.1 Naturlige tall og heltall

Definisjon 1.1.1. Et *naturlig tall* er et av tallene: 1, 2, ...

Merknad 1.1.2. Legg spesielt merke til at i dette kurset teller vi ikke 0 iblant de naturlige tallene. Allikevel er det noen som ser på 0 som et naturlig tall. Å inkludere det eller ikke er bare en konvensjon, og ikke noe å bekymre seg for. Noen ganger inkluderer jeg selv det, og noen ganger ikke!

Definisjon 1.1.3. Et *heltall* er et av tallene: $\ldots, -2, -1, 0, 1, 2, \ldots$.

Merknad 1.1.4. Alle naturlige tall er heltall. Men ikke alle heltall er naturlige tall: de negative heltallene er ikke naturlige tall. Ifølge Definisjon 1.1.1 er 0 heller ikke et naturlig tall.

Notasjon 1.1.5. La m og n være heltall. Vi skriver m ganger n som mn, $m \cdot n$, eller $m \times n$.

1.2 Bevis

Merknad 1.2.1. Matematikk er som et gigantisk byggverk i murstein. Det bygges opp på følgende måte.

(1) Matematiske påstander formuleres. Disse er mursteinene til byggverket.

(2) Disse påstandene bevises, ved hjelp av matematiske påstander som allerede har blitt bevist. Bevisene er sementen som binder mursteinene sammen.

Terminologi 1.2.2. Å *bevise* at en matematisk påstand er sann betyr å vise, ved å benytte gitte logiske prinsipper, at den er sann fra påstander som allerede har blitt bevist, og fra definisjonene av tingene påstanden handler om. Typisk blir et bevis bygd opp steg for steg i en rekke deduksjoner.

Eksempel 1.2.3. La n være et naturlig tall. Et eksempel på en matematisk påstand er:

$$n + 4 > n + 3.$$

At denne påstanden er sann følger logisk fra de følgende to påstandene:

(1) $4 > 3$.

(2) For hvilke som helst naturlige tall n, k, og l slik at $k > l$, er $n + k > n + l$.

Logikken er som følger: siden $4 > 3$ kan vi ta k som 4 og l som 3 i Påstand (2), og da får vi at $n + 4 > n + 3$, som vi ønsket å bevise.

Merknad 1.2.4. Hele kurset består av matematiske påstander og deres beviser, så vi ikke skal gi flere eksempler nå. De logiske prinsippene som står bak dem er stort sett så velkjente at vi ikke pleier å nevne dem. Imidlertid skal vi i dette kapittelet introdusere et logisk prinsipp som er svært viktig i matematikk, og som du sannsynligvis ikke kjenner til: «induksjon».

Merknad 1.2.5. Å bevise at en matematisk påstand er gal betyr helt enkelt å gi et eksempel hvor det ikke er sant. For eksempel se på påstanden: dersom n er et naturlig tall, er $2n > n + 1$. Denne påstanden er gal: når $n = 1$, er påstanden at $2 > 2$, noe som er galt.

Imidlertid er følgende påstand sann: dersom n er et naturlig tall slik at $n \geq 2$, er $2n > n + 1$. Den kan bevises ved hjelp av induksjon. Dette illustrerer hvor viktig det er at en matematisk påstand uttrykkes nøyaktig.

Terminologi 1.2.6. Et eksempel som beviser at en matematisk påstand er gal kalles noen ganger et *moteksempel*. Det tilsvarende engelske ordet er: «counterexample».

1.3 Teoremer, proposisjoner, lemmaer, og korollarer

Terminologi 1.3.1. Et matematisk utsagn som har blitt bevist kalles et *teorem*, en *proposisjon*, et *korollar*, eller et *lemma*. Forskjellige matematikere bruker disse betegnelsene på forskjellige måter, og noen bruker i tillegg andre betegnelser. Likevel finnes det noen hovedtrekk som går igjen.

(1) Et lemma betegner typisk et steg mot et teorem eller en proposisjon som i seg selv ikke er spesielt viktig. Ofte kan et lemma bevises ganske lett, men ikke alltid!

(2) Et teorem eller en proposisjon er et utsagn som er betydningsfult i seg selv. Et teorem er viktigere enn en proposisjon. Personlig bruker jeg «teorem» bare for de aller viktigste utsagnene.

(3) Et korollar betegner typisk et utsagn som er lett å dedusere fra et allerede bevist teorem, proposisjon, eller lemma.

1.4 Induksjon

Merknad 1.4.1. La n være et naturlig tall. Se på påstanden

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Hvordan kan vi bevise at dette er sant?

Vi kan sjekke om det er sant for gitte verdier av n. La for eksempel $n = 1$. Siden

$$\frac{1 \cdot (1+1)}{2} = \frac{1 \cdot 2}{2} = \frac{2}{2} = 1$$

er utsagnet sant i dette tilfellet.

La $n = 2$ istedenfor. Siden $1 + 2 = 3$ og

$$\frac{2 \cdot (2+1)}{2} = \frac{2 \cdot 3}{2} = \frac{6}{2} = 3,$$

er det sant at

$$1 + 2 = \frac{2 \cdot (2+1)}{2}.$$

Dermed er utsagnet sant i dette tilfellet også. Vi kan på en lignende måte sjekke om utsagnet er sant når $n = 3$, når $n = 4$, og så videre.

Likevel kan vi ikke sjekke om proposisjonen er sann for alle naturlig tall selv om vi brukte hele livet på kun det! Derfor regnes ikke å sjekke om det er sant i for enkelte verdier av n som et matematisk bevis.

Istedenfor benytter vi en type resonnement som kalles induksjon.

Terminologi 1.4.2. Anta at vi har et gitt matematisk utsagn for hvert heltall større enn eller likt et gitt heltall r. Anta dessuten at vi ønsker å bevise utsagnet for hvert av disse heltallene. *Induksjon* sier at vi kan gjøre det på følgende måte:

(1) Sjekk om utsagnet er sant for heltallet r.

(2) Hvis det antas at utsagnet har blitt bevist for et gitt heltall m som er større enn eller likt r, bevis at utsagnet er sant for heltallet $m + 1$.

Merknad 1.4.3. Idéen bak induksjon er at Steg (1) og Steg (2) gir oss en algoritme for å konstruere et bevis for utsagnet for et hvilket som helst heltall m større enn eller likt r:

(i) Steg (1) i Terminologi 1.4.2 fastslår at vi kan bevise utsagnet når $m = r$;

(ii) Steg (2) i Terminologi 1.4.2 fastslår at vi da kan bevise utsagnet når $m = r + 1$;

(iii) Steg (2) i Terminologi 1.4.2 fastslår at vi *da* kan bevise utsagnet når $m = r + 2$;

(iv) Steg (2) i Terminologi 1.4.2 fastslår at vi *da* kan bevise utsagnet når $m = r + 3$;

(v) Slik fortsetter vi til vi når heltallet vi er interessert i.

Merknad 1.4.4. Det er svært viktig å fremstille et bevis ved induksjon på en klar måte:

(1) Skriv tydelig at vi sjekker utsagnet for et gitt heltall r, for å gjennomføre Steg (1) i Terminologi 1.4.2.

(2) Skriv tydelig at vi antar at utsagnet har blitt bevist for et gitt heltall m større enn r. Skriv så et bevis for utsagnet for heltallet $m+1$, og redegjør for hvor du benytter antagelsen at utsagnet stemmer for heltallet m. Dermed har Steg (2) i Terminologi 1.4.2 blitt fullført.

(3) Avslutt fremstillingen ved å nevne at utsagnet stemmer for alle heltall større enn r ved induksjon. Det er også greit å begynne med å skrive at utsagnet skal bevises ved induksjon. Det viktigste er å nevne dette et eller annet sted.

Vi skal se på mange bevis ved induksjon i løpet av dette kurset, og du kommer sikkert til å bli fortrolig med det. La oss begynne med en gang ved å uttrykke formelt påstanden som vi tok for oss i Merknad 1.4.1, og å fremstille et bevis for det ved induksjon.

Proposisjon 1.4.5. La n være et naturlig tall. Da er

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. Dette gjorde vi i Merknad 1.4.1.

Anta nå at proposisjonen har blitt bevist for et gitt naturlig tall m større enn eller likt 1. Således har det blitt bevist at

$$1 + 2 + \cdots + m = \frac{m(m+1)}{2}.$$

Da er

$$\begin{aligned} 1 + 2 + \cdots + m + (m+1) &= \frac{m(m+1)}{2} + (m+1) \\ &= \frac{m(m+1) + 2(m+1)}{2} \\ &= \frac{(m+2)(m+1)}{2} \\ &= \frac{(m+1)(m+2)}{2}. \end{aligned}$$

Dermed er proposisjonen sann for det naturlige tallet $m+1$.

Ved induksjon konkluderer vi at proposisjonen er sann for alle naturlige tall. □

Eksempel 1.4.6. Når $n = 2$, fastslår Proposisjon 1.4.5 at

$$1 + 2 = \frac{2 \cdot 3}{2} = \frac{6}{2} = 3.$$

Eksempel 1.4.7. Når $n = 3$, fastslår Proposisjon 1.4.5 at

$$1 + 2 + 3 = \frac{3 \cdot 4}{2} = \frac{12}{2} = 6.$$

Eksempel 1.4.8. Når $n = 57$, fastslår Proposisjon 1.4.5 at

$$1 + 2 + \cdots + 57 = \frac{57 \cdot 58}{2} = \frac{3306}{2} = 1653.$$

Eksempel 1.4.9. Når $n = 100$, fastslår Proposisjon 1.4.5 at

$$1 + 2 + \cdots + 100 = \frac{100 \cdot 101}{2} = \frac{10100}{2} = 5050.$$

Merknad 1.4.10. Den viktigste delen av beviset for Proposisjon 1.4.5 er ligningen

$$1 + 2 + \cdots + m + (m + 1) = \frac{m(m + 1)}{2} + (m + 1).$$

Det er her vi benytter antakelsen at

$$1 + 2 + \cdots + m = \frac{m(m + 1)}{2}.$$

De andre linjene er bare algebraiske manipulasjoner.

Merknad 1.4.11. La oss se hvordan algoritmen i Merknad 1.4.3 ser ut for Proposisjon 1.4.5. Vi begynner med å sjekke om

$$1 = \frac{1 \cdot 2}{2}.$$

Så argumenterer vi som i beviset for Proposisjon 1.4.5, ved å erstatte m med 1:

$$\begin{aligned} 1 + 2 &= \frac{1 \cdot 2}{2} + 2 \\ &= \frac{1 \cdot 2 + 2 \cdot 2}{2} \\ &= \frac{(1 + 2) \cdot 2}{2} \\ &= \frac{2 \cdot (1 + 2)}{2} \\ &= \frac{2 \cdot 3}{2}. \end{aligned}$$

Dermed er

$$1 + 2 = \frac{2 \cdot 3}{2}.$$

Således har vi bevist at proposisjonen er sann når $n = 2$.

Så argumenterer vi som i beviset for Proposisjon 1.4.5, ved å erstatte m med 2:

$$\begin{aligned} 1+2+3 &= \frac{2\cdot 3}{2}+3 \\ &= \frac{2\cdot 3+2\cdot 3}{2} \\ &= \frac{(2+2)\cdot 3}{2} \\ &= \frac{3\cdot(2+2)}{2} \\ &= \frac{3\cdot 4}{2}. \end{aligned}$$

Dermed er

$$1+2+3=\frac{3\cdot 4}{2}.$$

Således har vi bevist at proposisjonen er sann når $n=3$.

Slik fortsetter vi til vi når heltallet vi er interessert i.

Merknad 1.4.12. Proposisjon 1.4.5 kan bevises på andre måter. Matematiske utsagn generelt kan typisk bevises på flere måter, og alle bevisene er like verdifulle. Ofte gir hvert bevis ny innsikt.

Likevel skal vi ikke her se på andre bevis for Proposisjon 1.4.5. Istedenfor skal vi øve oss litt mer på induksjon.

1.5 Flere eksempler på bevis ved induksjon

Proposisjon 1.5.1. La n være et naturlig tall. Da er

$$1+2+4+\cdots+2^{n-1}=2^n-1.$$

Bevis. Først sjekker vi om proposisjonen er sann når $n=1$. I dette tilfellet er utsagnet at $1=2^1-1$. Siden

$$2^1-1=2-1=1$$

er dette sant.

Anta nå at proposisjonen har blitt bevist for et gitt heltall m større enn eller likt 1. Således har det blitt bevist at

$$1+2+4+\cdots+2^{m-1}=2^m-1.$$

Da er

$$\begin{aligned} 1+2+4+\cdots+2^{m-1}+2^m &= (2^m-1)+2^m \\ &= (2^m+2^m)-1 \\ &= (2\cdot 2^m)-1 \\ &= 2^{m+1}-1. \end{aligned}$$

Dermed er proposisjonen sann for det naturlige tallet $m+1$.

Ved induksjon konkluderer vi at proposisjonen er sann for alle naturlige tall. □

Eksempel 1.5.2. Når $n = 2$, fastslår Proposisjon 1.5.1 at

$$1 + 2 = 2^2 - 1 = 4 - 1 = 3.$$

Eksempel 1.5.3. Når $n = 3$, fastslår Proposisjon 1.5.1 at

$$1 + 2 + 4 = 2^3 - 1 = 8 - 1 = 7.$$

Eksempel 1.5.4. Når $n = 6$, fastslår Proposisjon 1.5.1 at

$$1 + 2 + \cdots + 32 = 2^6 - 1 = 64 - 1 = 63.$$

Eksempel 1.5.5. Når $n = 57$, fastslår Proposisjon 1.5.1 at

$$1 + 2 + \cdots + 2^{56} = 2^{57} - 1 = 144115188075855872 - 1 = 144115188075855871.$$

Merknad 1.5.6. Den viktigste delen av beviset for Proposisjon 1.5.1 er ligningen

$$1 + 2 + 4 + \cdots + 2^{m-1} + 2^m = (2^m - 1) + 2^m.$$

Det er her vi benytter antakelsen at

$$1 + 2 + 4 + \cdots + 2^{m-1} = 2^m - 1.$$

De andre linjene er bare algebraiske manipulasjoner.

Proposisjon 1.5.7. La n være et naturlig tall. Da er

$$1 + 4 + 9 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. I dette tilfellet er utsagnet at

$$1 = \frac{1 \cdot (1+1) \cdot \big((2 \cdot 1) + 1\big)}{6}.$$

Siden

$$\frac{1 \cdot (1+1) \cdot \big((2 \cdot 1) + 1\big)}{6} = \frac{1 \cdot 2 \cdot 3}{6} = \frac{6}{6} = 1$$

er dette sant.

Anta nå at proposisjonen har blitt bevist for et gitt heltall m større enn eller likt 1. Således har det blitt bevist at

$$1 + 4 + 9 + \cdots + m^2 = \frac{m(m+1)(2m+1)}{6}.$$

Da er

$$\begin{aligned}
1+4+9+\cdots+m^2+(m+1)^2 &= \frac{m(m+1)(2m+1)}{6}+(m+1)^2 \\
&= \frac{m(m+1)(2m+1)+6(m+1)^2}{6} \\
&= \frac{(m+1)\cdot\big(m(2m+1)+6(m+1)\big)}{6} \\
&= \frac{(m+1)\cdot\big(2m^2+7m+6\big)}{6} \\
&= \frac{(m+1)\cdot\big((m+2)\cdot(2m+3)\big)}{6} \\
&= \frac{(m+1)\cdot\big((m+1)+1\big)\cdot\big(2(m+1)+1\big)}{6}.
\end{aligned}$$

Dermed er proposisjonen sann for det naturlige tallet $m+1$.

Ved induksjon konkluderer vi at proposisjonen er sann for alle naturlige tall. □

Eksempel 1.5.8. Når $n=2$, fastslår Proposisjon 1.5.7 at

$$1+4=\frac{2\cdot 3\cdot 5}{2}=\frac{30}{6}=5.$$

Eksempel 1.5.9. Når $n=3$, fastslår Proposisjon 1.5.7 at

$$1+4+9=\frac{3\cdot 4\cdot 7}{6}=\frac{84}{6}=14.$$

Eksempel 1.5.10. Når $n=6$, fastslår Proposisjon 1.5.7 at

$$1+4+\cdots+36=\frac{6\cdot 7\cdot 13}{6}=\frac{546}{6}=91.$$

Eksempel 1.5.11. Når $n=57$, fastslår Proposisjon 1.5.7 at

$$1+4+\cdots+3249=\frac{57\cdot 58\cdot 115}{6}=\frac{380190}{6}=63365.$$

Merknad 1.5.12. Den viktigste delen av beviset for Proposisjon 1.5.7 er ligningen

$$1+4+9+\cdots+m^2+(m+1)^2=\frac{m(m+1)(2m+1)}{6}+(m+1)^2.$$

Det er her vi benytter antakelsen at

$$1+4+9+\cdots+m^2=\frac{m(m+1)(2m+1)}{6}.$$

De andre linjene er bare algebraiske manipulasjoner.

Merknad 1.5.13. Alle proposisjonene vi har sett så langt er sanne for alle naturlige tall, altså alle heltall større enn eller like 1. Derfor begynte bevisene ved induksjon for alle disse proposisjonene med å sjekke om utsagnene er sanne når $n = 1$.

Neste skal vi bevise ved induksjon en proposisjon som er sann for alle naturlige tall større enn eller like 2. Derfor skal vi begynne beviset med å sjekke om proposisjonen er sann når $n = 2$.

Husk at induksjon kan brukes for å bevise en proposisjon for alle naturlige tall større enn eller like et hvilket som helst gitt heltall.

Proposisjon 1.5.14. La n være et naturlig tall som er større enn eller likt 2. Da er $n^2 > n + 1$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 2$. I dette tilfellet er utsagnet at

$$2^2 > 2 + 1.$$

Siden $2^2 = 4$ og $2 + 1 = 3$, er dette sant.

Anta nå at proposisjonen har blitt bevist for et gitt heltall m større enn eller likt 2. Således har det blitt bevist at

$$m^2 > m + 1.$$

Vi gjør følgende observasjoner.

(1) Vi har:

$$\begin{aligned}(m+1)^2 &= (m+1)\cdot(m+1)\\ &= m^2 + 2m + 1.\end{aligned}$$

(2) Siden $m > 0$, er $2m > 0$. Derfor er

$$m^2 + 2m + 1 > m^2 + 1.$$

(3) Fra antakelsen at

$$m^2 > m + 1,$$

følger det at

$$m^2 + 1 > (m + 1) + 1.$$

Fra (1) – (3) deduserer vi at

$$(m+1)^2 > (m+1) + 1.$$

Således er proposisjonen sann for det naturlige tallet $m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann for alle naturlige tall større enn eller like 2. □

Eksempel 1.5.15. Når $n = 3$, fastslår Proposisjon 1.5.14 at

$$9 > 4.$$

Eksempel 1.5.16. Når $n = 4$, fastslår Proposisjon 1.5.14 at

$$16 > 5.$$

Eksempel 1.5.17. Når $n = 57$, fastslår Proposisjon 1.5.14 at

$$3249 > 58.$$

Merknad 1.5.18. Observasjon (3), hvor vi benytter antakelsen at

$$m^2 > m + 1,$$

er den viktigste delen av beviset for Proposisjon 1.5.14.

1.6 Summetegnet

Notasjon 1.6.1. La k og l være heltall. For hvert heltall i slik at $k \leq i \leq l$, la z_i være et heltall. Noen ganger skriver vi summen

$$z_k + z_{k+1} + \cdots + z_l$$

som

$$\sum_{i=k}^{l} z_i.$$

Terminologi 1.6.2. Symbolet $\sum$ kalles *summetegn*.

Eksempel 1.6.3. La n være et naturlig tall. Summen

$$1 + 2 + \cdots + n,$$

som vi tok for oss i Proposisjon 1.4.5, kan skrives

$$\sum_{i=1}^{n} i.$$

Eksempel 1.6.4. La m være et naturlig tall. Summen

$$1 + 2 + \cdots + m,$$

som vi også tok for oss i Proposisjon 1.4.5, kan skrives

$$\sum_{i=1}^{m} i.$$

Eksempel 1.6.5. La m være et naturlig tall. Summen

$$1 + 2 + \cdots + (m + 1),$$

som vi igjen tok for oss i Proposisjon 1.4.5, kan skrives

$$\sum_{i=1}^{m+1} i.$$

Eksempel 1.6.6. La n være et naturlig tall. Summen

$$1 + 2 + 4 + \cdots + 2^{n-1},$$

som vi tok for oss i Proposisjon 1.5.1, kan skrives

$$\sum_{i=1}^{n} 2^{i-1}.$$

Den kan også skrives

$$\sum_{i=0}^{n-1} 2^i.$$

Eksempel 1.6.7. La m være et naturlig tall. Summen

$$1 + 2 + 4 + \cdots + 2^{m-1},$$

som vi også tok for oss i Proposisjon 1.5.1, kan skrives

$$\sum_{i=1}^{m} 2^{i-1}.$$

Den kan også skrives

$$\sum_{i=0}^{m-1} 2^i.$$

Eksempel 1.6.8. La m være et naturlig tall. Summen

$$1 + 2 + 4 + \cdots + 2^{m},$$

som vi igjen tok for oss i Proposisjon 1.5.1, kan skrives

$$\sum_{i=1}^{m+1} 2^{i-1}.$$

Den kan også skrives

$$\sum_{i=0}^{m} 2^i.$$

Eksempel 1.6.9. La n være et naturlig tall. Summen

$$1 + 4 + 9 + \cdots + n^2,$$

som vi tok for oss i Proposisjon 1.5.7, kan skrives

$$\sum_{i=1}^{n} i^2.$$

Eksempel 1.6.10. La m være et naturlig tall. Summen

$$1 + 4 + 9 + \cdots + m^2,$$

som vi også tok for oss i Proposisjon 1.5.7, kan skrives

$$\sum_{i=1}^{m} i^2.$$

Eksempel 1.6.11. La m være et naturlig tall. Summen

$$1 + 4 + 9 + \cdots + (m+1)^2,$$

som vi igjen tok for oss i Proposisjon 1.5.7, kan skrives

$$\sum_{i=1}^{m+1} i^2.$$

Eksempel 1.6.12. La n og k være naturlige tall. I den neste delen av kapittelet skal vi jobbe med summer som ligner på

$$\big(1 \times 2 \times \cdots \times k\big) + \big(2 \times 3 \times \cdots \times (k+1)\big) + \cdots + \big(n \times (n+1) \times \cdots \times (n+k-1)\big).$$

Denne summen kan skrives

$$\sum_{i=1}^{n} i \times (i+1) \times \cdots \times (i+k-1).$$

Eksempel 1.6.13. La m og k være naturlige tall. Summen

$$\big(1 \times 2 \times \cdots \times k\big) + \big(2 \times 3 \times \cdots \times (k+1)\big) + \cdots + \big(m \times (m+1) \times \cdots \times (m+k-1)\big)$$

kan skrives

$$\sum_{i=1}^{m} i \times (i+1) \times \cdots \times (i+k-1).$$

Eksempel 1.6.14. La m og k være naturlige tall. Summen

$$\big(1 \times 2 \times \cdots \times k\big) + \big(2 \times 3 \times \cdots \times (k+1)\big) + \cdots + \big((m+1) \times (m+2) \times \cdots \times (m+k)\big)$$

kan skrives

$$\sum_{i=1}^{m+1} i \times (i+1) \times \cdots \times (i+k-1).$$

1.7 Et eksempel til på bevis ved induksjon

Proposisjon 1.7.1. La n og k være naturlige tall. Da er

$$\sum_{i=1}^{n} i \times (i+1) \times \cdots \times (i+k-1) = \frac{n \times (n+1) \times \cdots \times (n+k)}{k+1}.$$

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. I dette tilfellet er utsagnet at

$$1 \times 2 \times \cdots \times k = \frac{1 \times (1+1) \times \cdots \times (1+k)}{k+1}.$$

Siden

$$\begin{aligned} \frac{1 \times (1+1) \times \cdots \times (1+k)}{k+1} &= \frac{1 \times 2 \times \cdots \times (k+1)}{k+1} \\ &= 1 \times 2 \times \cdots \times k \end{aligned}$$

er dette sant.

Anta nå at proposisjonen har blitt bevist når n er et gitt naturlig tall m. Således har det blitt bevist at

$$\sum_{i=1}^{m} i \times (i+1) \times \cdots \times (i+k-1) = \frac{m(m+1)\ldots(m+k)}{k+1}.$$

Da er

$$\begin{aligned} &\sum_{i=1}^{m+1} i \times (i+1) \times \cdots \times (i+k-1) \\ &= \left(\sum_{i=1}^{m} i \times (i+1) \times \cdots \times (i+k-1) \right) + (m+1) \times (m+2) \times \ldots (m+k) \\ &= \frac{m \times (m+1) \times \cdots \times (m+k)}{k+1} + (m+1) \times (m+2) \times \cdots \times (m+k) \\ &= \frac{\big(m \times (m+1) \times \cdots \times (m+k)\big) + \big((k+1) \times (m+1) \times (m+2) \times \cdots \times (m+k)\big)}{k+1} \\ &= \frac{\big((m+1) \times \cdots \times (m+k)\big)\big(m + (k+1)\big)}{k+1} \\ &= \frac{(m+1) \times (m+2) \times \cdots \times (m+k+1)}{k+1}. \end{aligned}$$

Dermed er proposisjonen sann når n er det naturlige tallet $m+1$.

Ved induksjon konkluderer vi at proposisjonen er sann for alle naturlige tall n og alle naturlige tall k. □

Eksempel 1.7.2. Når $n = 2$ og $k = 3$, fastslår Proposisjon 1.7.1 at

$$1 \times 2 \times 3 + 2 \times 3 \times 4 = \frac{2 \times 3 \times 4 \times 5}{4} = \frac{120}{4} = 30.$$

Eksempel 1.7.3. Når $n = 2$ og $k = 4$, fastslår Proposisjon 1.7.1 at

$$1 \times 2 \times 3 \times 4 + 2 \times 3 \times 4 \times 5 = \frac{2 \times 3 \times 4 \times 5 \times 6}{5} = \frac{720}{5} = 144.$$

Eksempel 1.7.4. Når $n = 2$ og $k = 6$, fastslår Proposisjon 1.7.1 at

$$1 \times 2 \times \cdots \times 6 + 2 \times 3 \times \cdots \times 7 = \frac{2 \times 3 \times \ldots 8}{7} = \frac{40320}{7} = 5760.$$

Eksempel 1.7.5. Når $n = 3$ og $k = 2$, fastslår Proposisjon 1.7.1 at

$$1 \times 2 + 2 \times 3 + 3 \times 4 = \frac{3 \times 4 \times 5}{3} = \frac{60}{3} = 20.$$

Eksempel 1.7.6. Når $n = 3$ og $k = 3$, fastslår Proposisjon 1.7.1 at

$$1 \times 2 \times 3 + 2 \times 3 \times 4 + 3 \times 4 \times 5 = \frac{3 \times 4 \times 5 \times 6}{4} = \frac{360}{4} = 90.$$

Eksempel 1.7.7. Når $n = 3$ og $k = 6$, fastslår Proposisjon 1.7.1 at

$$\begin{aligned} 1 \times 2 \times \cdots \times 6 + 2 \times 3 \times \cdots \times 7 + 3 \times 4 \times \cdots \times 8 &= \frac{3 \times 4 \times \cdots \times 9}{7} \\ &= \frac{181440}{7} \\ &= 25920. \end{aligned}$$

Eksempel 1.7.8. Når $n = 4$ og $k = 2$, fastslår Proposisjon 1.7.1 at

$$1 \times 2 + 2 \times 3 + 3 \times 4 + 4 \times 5 = \frac{4 \times 5 \times 6}{3} = \frac{120}{3} = 40.$$

Eksempel 1.7.9. Når $n = 4$ og $k = 3$, fastslår Proposisjon 1.7.1 at

$$\begin{aligned} 1 \times 2 \times 3 + 2 \times 3 \times 4 + 3 \times 4 \times 5 + 4 \times 5 \times 6 &= \frac{4 \times 5 \times 6 \times 7}{4} \\ &= \frac{840}{4} \\ &= 210. \end{aligned}$$

Eksempel 1.7.10. Når $n = 4$ og $k = 6$, fastslår Proposisjon 1.7.1 at

$$\begin{aligned} 1 \times 2 \times \cdots \times 6 + 2 \times 3 \times \cdots \times 7 + 3 \times 4 \times \cdots \times 8 + 4 \times 5 \times \cdots \times 9 &= \frac{4 \times 5 \times \cdots \times 10}{7} \\ &= \frac{604800}{7} \\ &= 86400. \end{aligned}$$

Eksempel 1.7.11. Når $n = 6$ og $k = 2$, fastslår Proposisjon 1.7.1 at

$$1 \times 2 + 2 \times 3 + \cdots + 6 \times 7 = \frac{6 \times 7 \times 8}{3} = \frac{336}{3} = 112.$$

Eksempel 1.7.12. Når $n = 6$ og $k = 3$, fastslår Proposisjon 1.7.1 at

$$\begin{aligned} 1 \times 2 \times 3 + 2 \times 3 \times 4 + \cdots + 6 \times 7 \times 8 &= \frac{6 \times 7 \times 8 \times 9}{4} \\ &= \frac{3024}{4} \\ &= 756. \end{aligned}$$

Eksempel 1.7.13. Når $n = 6$ og $k = 6$, fastslår Proposisjon 1.7.1 at

$$\begin{aligned} 1 \times 2 \times \cdots \times 6 + 2 \times 3 \times \cdots \times 7 + \cdots + 6 \times 7 \times \cdots \times 11 &= \frac{6 \times 7 \times \cdots \times 12}{7} \\ &= \frac{3991680}{7} \\ &= 570240. \end{aligned}$$

Merknad 1.7.14. Ligningen

$$\begin{aligned} &\left(\sum_{i=1}^{m} i \times (i+1) \times \cdots \times (i+k-1) \right) + (m+1) \times (m+2) \times \ldots (m+k) \\ &= \frac{m \times (m+1) \times \cdots \times (m+k)}{k+1} + (m+1) \times (m+2) \times \cdots \times (m+k) \end{aligned}$$

er den viktigste delen av beviset for Proposisjon 1.7.1. Det er her vi benytter antakelsen at

$$\sum_{i=1}^{m} i \times (i+1) \times \cdots \times (i+k-1) = \frac{m \times (m+1) \times \cdots \times (m+k)}{k+1}.$$

Merknad 1.7.15. Proposisjon 1.7.1 for tilfellet $k = 1$ er det samme som Proposisjon 1.4.5. Beviset på Proposisjon 1.7.1 generaliserer beviset for Proposisjon 1.4.5.

Merknad 1.7.16. Proposisjon 1.7.1 gjelder to variabler n og k, og bevis ved induksjon i slike tilfeller kan til å begynne med se litt forvirrende ut. La oss derfor se på logikken bak beviset for Proposisjon 1.7.1.

Da vi sjekket om Proposisjon 1.7.1 er sann når $n = 1$, var k et *hvilket som helst* naturlig tall. Da vi deretter antok at Proposisjon 1.7.1 er sann når n er et gitt naturlig tall m, og viste at den da er sann når $n = m+1$, var k også et *hvilket som helst* naturlig tall.

Dermed kan vi se på beviset for Proposisjon 1.7.1 på følgende måte. Først velger vi et naturlig tall k: la for eksempel k være 5. Da blir utsagnet:

$$\sum_{i=1}^{n} i \cdot (i+1) \cdot \cdots \cdot (i+4) = \frac{n(n+1) \cdots (n+5)}{6}.$$

Så beviser vi at dette er sant, ved å erstatte k med 5 i beviset for Proposisjon 1.7.1.

Først sjekker vi om utsagnet er sant når $n = 1$. Vi må altså sjekke om

$$1 \cdot 2 \cdot \cdots \cdot 5 = \frac{1 \cdot (1+1) \cdot \cdots \cdot (1+5)}{6}.$$

Siden

$$\begin{aligned}\frac{1 \cdot (1+1) \cdot \cdots \cdot (1+5)}{6} &= \frac{1 \cdot 2 \cdot \cdots \cdot 6}{6} \\ &= 1 \cdot 2 \cdot \cdots \cdot 5\end{aligned}$$

er dette sant.

Anta nå at det har blitt beviset at utsagnet er sant når n er et gitt naturlig tall m. Således har det blitt bevist at

$$\sum_{i=1}^{m} i \cdot (i+1) \cdot \cdots \cdot (i+4) = \frac{m(m+1)\cdots(m+5)}{6}.$$

Da er

$$\begin{aligned}&\sum_{i=1}^{m+1} i \cdot (i+1) \cdot \cdots \cdot (i+4) \\ &= \left(\sum_{i=1}^{m} i \cdot (i+1) \cdot \cdots \cdot (i+4)\right) + (m+1) \cdot (m+2) \cdot \ldots (m+5) \\ &= \frac{m(m+1)\cdots(m+5)}{6} + (m+1) \cdot (m+2) \cdot \cdots \cdot (m+5) \\ &= \frac{m(m+1)\cdots(m+5) + 6 \cdot (m+1) \cdot (m+2) \cdot \cdots \cdot (m+5)}{6} \\ &= \frac{\big((m+1) \cdot \cdots \cdot (m+5)\big)\big(m+6\big)}{6} \\ &= \frac{(m+1) \cdot (m+2) \cdot \cdots \cdot (m+6)}{6}.\end{aligned}$$

Dermed er utsagnet sant når n er det naturlige tallet $m + 1$.

Ved induksjon konkluderer vi at utsagnet er sant når n er et hvilket som helst naturlig tall.

Merknad 1.7.17. I prinsippet kan vi bytte om rollene til n og k i beviset for Proposisjon 1.7.1. Det vil si at vi i teorien kan gjøre følgende:

(1) Sjekke om Proposisjon 1.7.1 er sann når $k = 1$, og når n er et hvilket som helst naturlig tall.

(2) Anta så at Proposisjon 1.7.1 er sann når k er et gitt naturlig tall m, og når n er et hvilket som helst naturlig tall, og vis at den da er sann når $k = m + 1$, og når n igjen er et hvilket som helst naturlig tall.

Terminologi 1.7.18. Når vi beviser ved induksjon en proposisjon om heltall som involver to eller flere variabler, spiller alltid én variabel den rollen som n har i beviset for Proposisjon 1.7.1, og som k har i tilnærmingsmetoden beskrevet i Merknad 1.7.17. La oss anta at denne spesielle variabelen betegnes t. Da sier vi at proposisjonen har blitt bevist ved *induksjon på* t.

Eksempel 1.7.19. Vi sier at beviset vi ga for Proposisjon 1.7.1 er ved induksjon på n. Hadde vi et bevis for Proposisjon 1.7.1 med tilnærmingsmetoden beskrevet i Merknad 1.7.17, ville vi si at det er et bevis ved induksjon på k.

Merknad 1.7.20. For å bevise en proposisjon om heltall som involverer to eller flere variabler, er det typisk mye lettere å benytte induksjon på en av variablene enn induksjon på noen av de andre. Det er for eksempel ikke lett å bevise Proposisjon 1.7.1 ved induksjon på k, altså med tilnærmingsmetoden beskrevet i Merknad 1.7.17.

1.8 Fakultet

Definisjon 1.8.1. La n være et naturlig tall. Da er n *fakultet* produktet

$$1 \times 2 \times \cdots \times (n-1) \times n.$$

I tillegg definerer vi 0 *fakultet* til å være 1.

Notasjon 1.8.2. La n være et heltall slik at $n \geq 0$. Vi betegner n fakultet som $\ll n! \gg$.

Eksempel 1.8.3. Vi har: $1! = 1$.

Eksempel 1.8.4. Siden $1 \times 2 = 2$, er $2! = 2$.

Eksempel 1.8.5. Siden $1 \times 2 \times 3 = 6$, er $3! = 6$.

Eksempel 1.8.6. Siden $1 \times 2 \times 3 \times 4 = 24$, er $4! = 24$.

1.9 Binomialkoeffisienter og binomialteoremet

Merknad 1.9.1. Fra skolen kjenner du til ligningen

$$(x+y)^2 = x^2 + 2xy + y^2.$$

Nå skal vi se på en tilsvarende ligning for $(x+y)^n$, hvor n er et hvilket som helst naturlig tall. Først må vi gjøre noen forberedelser.

Definisjon 1.9.2. La n være et naturlig tall, og la k være et heltall slik at $0 \leq k \leq n$. Da er *binomialkoeffisienten av* n *og* k brøken

$$\frac{n!}{k! \cdot (n-k)!}.$$

Notasjon 1.9.3. Vi betegner binomialkoeffisienten av n og k som

$$\binom{n}{k}.$$

Merknad 1.9.4. Symbolet $\binom{n}{k}$ leses (temmelig ugrammatisk!) som «n velg k». Dette kommer av at det kan bevises at $\binom{n}{k}$ er antall muligheter for å velge ut k ting fra n ting. På grunn av denne tolkningen blir binomialkoeffisientene brukt mye i et område innen matematikken som kalles *kombinatorikk*.

Eksempel 1.9.5. Vi har:

$$\begin{aligned}\binom{4}{2} &= \frac{4!}{2! \cdot (4-2)!} \\ &= \frac{4!}{2! \cdot 2!} \\ &= \frac{24}{2 \cdot 2} \\ &= \frac{24}{4} \\ &= 6.\end{aligned}$$

Eksempel 1.9.6. Vi har:

$$\begin{aligned}\binom{5}{3} &= \frac{5!}{3! \cdot (5-3)!} \\ &= \frac{5!}{3! \cdot 2!} \\ &= \frac{120}{6 \cdot 2} \\ &= \frac{120}{12} \\ &= 10.\end{aligned}$$

Merknad 1.9.7. Bevisene av de følgende proposisjonene er enkle utregniner, og induksjon behøves ikke.

Proposisjon 1.9.8. La n være et naturlig tall. Da er $\binom{n}{0} = 1$.

Bevis. Vi regner som følger:

$$\begin{aligned}\binom{n}{0} &= \frac{n!}{0! \cdot (n-0)!} \\ &= \frac{n!}{0! \cdot n!} \\ &= \frac{n!}{1 \cdot n!} \\ &= \frac{n!}{n!} \\ &= 1.\end{aligned}$$

□

Proposisjon 1.9.9. La n være et naturlig tall. Da er $\binom{n}{1} = n$.

Bevis. Vi regner som følger:

$$\begin{aligned}\binom{n}{1} &= \frac{n!}{1! \cdot (n-1)!} \\ &= \frac{n!}{1 \cdot (n-1)!} \\ &= \frac{n!}{(n-1)!} \\ &= \frac{1 \times 2 \times \cdots \times (n-1) \times n}{1 \times 2 \times \cdots \times (n-2) \times (n-1)} \\ &= n.\end{aligned}$$

□

Proposisjon 1.9.10. La n være et naturlig tall, og la k være et heltall slik at $0 \leq k \leq n$. Da er $\binom{n}{k} = \binom{n}{n-k}$.

Bevis. Vi regner som følger:

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{k! \cdot (n-k)!} \\ &= \frac{n!}{(n-k)! \cdot k!} \\ &= \frac{n!}{(n-k)! \cdot \big(n-(n-k)\big)!} \\ &= \binom{n}{n-k}.\end{aligned}$$

□

Korollar 1.9.11. La n være et naturlig tall. Da er $\binom{n}{n} = 1$.

Bevis. På grunn av Proposisjon 1.9.10 er $\binom{n}{n} = \binom{n}{0}$. På grunn av Proposisjon 1.9.8 er $\binom{n}{0} = 1$. Således konkluderer vi at $\binom{n}{n} = 1$. □

Korollar 1.9.12. La n være et naturlig tall. Da er $\binom{n}{n-1} = n$.

Bevis. Ut ifra Proposisjon 1.9.10 er $\binom{n}{n-1} = \binom{n}{1}$. Ut ifra Proposisjon 1.9.9, er $\binom{n}{1} = n$. Således konkluderer vi at $\binom{n}{n-1} = n$. □

Eksempel 1.9.13. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 1.9.8 er $\binom{2}{0} = 1$.

(2) Ut ifra Proposisjon 1.9.9 er $\binom{2}{1} = 2$.

(3) Ut ifra Korollar 1.9.11 er $\binom{2}{2} = 1$.

Dermed har vi regnet ut $\binom{2}{k}$ for alle mulige verdier av k.

Eksempel 1.9.14. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 1.9.8 er $\binom{3}{0} = 1$.

(2) Ut ifra Korollar 1.9.11 er $\binom{3}{3} = 1$.

(3) Ut ifra Proposisjon 1.9.9 er $\binom{3}{1} = 3$.

(4) Fra (3) og Korollar 1.9.12, følger det at $\binom{3}{2} = 3$.

Dermed har vi regnet ut $\binom{3}{k}$ for alle mulige verdier av k.

Eksempel 1.9.15. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 1.9.8 er $\binom{4}{0} = 1$.

(2) Ut ifra Korollar 1.9.11 er $\binom{4}{4} = 1$.

(3) Ut ifra Proposisjon 1.9.9 er $\binom{4}{1} = 4$.

(4) Fra (3) og Korollar 1.9.12, følger det at $\binom{4}{3} = 4$.

(5) Fra Eksempel 1.9.5 har vi: $\binom{4}{2} = 6$.

Dermed har vi regnet ut $\binom{4}{k}$ for alle mulige verdier av k.

Eksempel 1.9.16. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 1.9.8 er $\binom{5}{0} = 1$.

(2) Ut ifra Korollar 1.9.11 er $\binom{5}{5} = 1$.

(3) Ut ifra Proposisjon 1.9.9 er $\binom{5}{1} = 5$.

(4) Fra (3) og Korollar 1.9.12, følger det at $\binom{5}{4} = 5$.

(5) Fra Eksempel 1.9.6 har vi: $\binom{5}{3} = 10$.

(6) Fra (5) og Proposisjon 1.9.10, følger det at $\binom{5}{2} = 10$.

Dermed har vi regnet ut $\binom{5}{k}$ for alle mulige verdier av k.

Merknad 1.9.17. I alle eksemplene vi har tatt for oss så langt, var $\binom{n}{k}$ er et naturlig tall. Vi skal snart bevise at dette er tilfelle for hvilke som helst n og k.

Proposisjon 1.9.18. La n og k være naturlige tall. Da er

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra definisjonen av $\binom{n}{k}$ og $\binom{n}{k-1}$ i Definisjon 1.9.2, er

$$\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k! \cdot (n-k)!} + \frac{n!}{(k-1)! \cdot (n-k+1)!}.$$

(2) Siden $k! = (k-1)! \cdot k$ og $(n-k+1)! = (n-k)! \cdot (n-k+1)$, er

$$\begin{aligned}\frac{n!}{k! \cdot (n-k)!} + \frac{n!}{(k-1)! \cdot (n-k+1)!} &= \frac{(n-k+1) \cdot n! + k \cdot n!}{k! \cdot (n-k+1)!} \\ &= \frac{n! \cdot (n-k+1+k)}{k! \cdot (n+1-k)!} \\ &= \frac{n! \cdot (n+1)}{k! \cdot (n+1-k)!}.\end{aligned}$$

(3) Siden $(n+1)! = n! \cdot (n+1)$, er

$$\frac{n! \cdot (n+1)}{k! \cdot (n+1-k)!} = \frac{(n+1)!}{k! \cdot (n+1-k)!}.$$

(4) Ut ifra definisjonen av $\binom{n+1}{k}$ i Definisjon 1.9.2, er

$$\binom{n+1}{k} = \frac{(n+1)!}{k! \cdot (n+1-k)!}.$$

Fra (1) – (4) konkluderer vi at

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

□

Eksempel 1.9.19. Når $n = 3$ og $k = 1$, fastslår Proposisjon 1.9.18 at

$$\binom{3}{1} + \binom{3}{0} = \binom{4}{1},$$

altså at

$$3 + 1 = 4.$$

Eksempel 1.9.20. Når $n = 3$ og $k = 2$, fastslår Proposisjon 1.9.18 at

$$\binom{3}{2} + \binom{3}{1} = \binom{4}{2},$$

altså at

$$3 + 3 = 6.$$

Eksempel 1.9.21. Når $n = 3$ og $k = 3$, fastslår Proposisjon 1.9.18 at

$$\binom{3}{3} + \binom{3}{2} = \binom{4}{3},$$

altså at

$$1 + 3 = 4.$$

Eksempel 1.9.22. Når $n = 5$ og $k = 1$, fastslår Proposisjon 1.9.18 at

$$\binom{5}{1} + \binom{5}{0} = \binom{6}{1},$$

altså at

$$5 + 1 = \binom{6}{1}.$$

Vi deduserer at $\binom{6}{1} = 6$.

Eksempel 1.9.23. Når $n = 5$ og $k = 2$, fastslår Proposisjon 1.9.18 at

$$\binom{5}{2} + \binom{5}{1} = \binom{6}{2},$$

altså at

$$10 + 5 = \binom{6}{2}.$$

Vi deduserer at $\binom{6}{2} = 15$.

Eksempel 1.9.24. Når $n = 5$ og $k = 3$, fastslår Proposisjon 1.9.18 at

$$\binom{5}{3} + \binom{5}{2} = \binom{6}{3},$$

altså at

$$10 + 10 = \binom{6}{3}.$$

Vi deduserer at $\binom{6}{3} = 20$.

Eksempel 1.9.25. Når $n = 5$ og $k = 4$, fastslår Proposisjon 1.9.18 at

$$\binom{5}{4} + \binom{5}{3} = \binom{6}{4},$$

altså at

$$5 + 10 = \binom{6}{4}.$$

Vi deduserer at $\binom{6}{4} = 15$.

Eksempel 1.9.26. Når $n = 5$ og $k = 5$, fastslår Proposisjon 1.9.18 at

$$\binom{5}{5} + \binom{5}{4} = \binom{6}{5},$$

altså at

$$1 + 5 = \binom{6}{5}.$$

Vi deduserer at $\binom{6}{5} = 6$.

Merknad 1.9.27. La oss sette opp binomialkoeffisientene på følgende måte. Det k-te tallet fra venstre, ved å telle k fra 0 til n, i den n-te raden fra toppen, ved å telle n fra 1, er binomialkoeffisienten $\binom{n}{k}$. For eksempel er det andre tallet fra venstre (ved å telle fra 0) i den fjerde raden fra toppen 6, som er binomialkoeffisienten $\binom{4}{2}$.

$$\begin{array}{ccccccccccc}
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

Proposisjonen 1.9.18 sier at når vi legger sammen to tall i en rad, får vi tallet mellom dem i den neste raden. For eksempel når vi legger sammen tallene 4 og 6 i den fjerde raden, får vi 10, som står mellom 4 og 6 i den femte raden.

Terminologi 1.9.28. Oppsettet av tallene i Merknad 1.9.27 kalles for *Pascals trekant*.

Proposisjon 1.9.29. La n være et naturlig tall, og la k være et heltall slik at $0 \leq k \leq n$. Da er $\binom{n}{k}$ et naturlig tall.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. I dette tilfellet er utsagnet at $\binom{1}{k}$ er et naturlig tall for hvert heltall k slik at $0 \leq k \leq 1$, altså når $k = 0$ og når $k = 1$. Ut ifra Proposisjon 1.9.8 er det sant at $\binom{1}{0}$ er et naturlig tall, og ut ifra Proposisjon 1.9.9 er det sant at $\binom{1}{1}$ er et naturlig tall.

Anta nå at proposisjonen har blitt bevist når n er et gitt naturlig tall m. Således har det blitt bevist at $\binom{m}{k}$ er et naturlig tall for alle heltallene k slik at $0 \leq k \leq m$. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 1.9.8 er $\binom{m+1}{0}$ et naturlig tall.

(2) La k være et naturlig tall. Fra antakelsen at $\binom{m}{k}$ er et naturlig tall for alle heltallene k slik at $0 \leq k \leq m$, er $\binom{m}{k}$ og $\binom{m}{k-1}$ naturlige tall. Derfor er

$$\binom{m}{k} + \binom{m}{k-1}$$

et naturlig tall. Ut ifra Proposisjon 1.9.18 vet vi dessuten at

$$\binom{m+1}{k} = \binom{m}{k} + \binom{m}{k-1}.$$

Vi deduserer at $\binom{m+1}{k}$ er et naturlig tall.

(3) Ut ifra Korollar 1.9.11 er $\binom{m+1}{m+1}$ et naturlig tall.

Dermed er $\binom{m+1}{k}$ et naturlig tall for alle naturlige tall k slik at $0 \leq k \leq m+1$. Således er proposisjonen sann når n er det naturlige tallet $m+1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall.

□

Proposisjon 1.9.30. La x og y være tall. La n være et heltall slik at $n \geq 0$. Da er

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i.$$

Bevis. Først sjekker vi om proposisjonen er sann når $n = 0$. I dette tilfellet er utsagnet at

$$(x+y)^0 = \sum_{i=0}^{0} \binom{0}{i} x^{0-i} y^i.$$

Siden $(x+y)^0 = 1$ og

$$\sum_{i=0}^{0} \binom{0}{i} x^{0-i} y^i = \binom{0}{0} x^{0-0} y^0 = 1 \cdot x^0 y^0 = 1,$$

er dette sant.

Anta nå at proposisjonen har blitt bevist når n er et gitt naturlig tall m. Således har det blitt bevist at

$$(x+y)^m = \sum_{i=0}^{m} \binom{m}{i} a^{m-i} b^i.$$

Vi gjør følgende observasjoner.

(1) Vi har:

$$\begin{aligned}(x+y)^{m+1} &= (x+y)^m \cdot (x+y) \\ &= \left(\sum_{i=0}^{m} \binom{m}{i} x^{m-i}y^i\right) \cdot (x+y) \\ &= \left(\sum_{i=0}^{m} \binom{m}{i} x^{m-i}y^i\right) \cdot x + \left(\sum_{i=0}^{m} \binom{m}{i} x^{m-i}y^i\right) \cdot y \\ &= \left(\sum_{i=0}^{m} \binom{m}{i} x^{m+1-i}y^i\right) + \left(\sum_{i=0}^{m} \binom{m}{i} x^{m-i}y^{i+1}\right)\end{aligned}$$

(2) Vi har:

$$\sum_{i=0}^{m} \binom{m}{i} x^{m+1-i}y^i = \binom{m}{0} x^{m+1-0}y^0 + \left(\sum_{i=1}^{m} \binom{m}{i} x^{m+1-i}y^i\right).$$

(3) Ut ifra Proposisjon 1.9.8 er $\binom{m}{0} = 1$. Derfor er

$$\binom{m}{0} x^{m+1-0}y^0 + \left(\sum_{i=1}^{m} \binom{m}{i} x^{m+1-i}y^i\right) = x^{m+1} + \left(\sum_{i=1}^{m} \binom{m}{i} x^{m+1-i}y^i\right).$$

(4) Vi har:

$$\begin{aligned}\sum_{i=0}^{m} \binom{m}{i} x^{m-i}y^{i+1} &= \sum_{i=1}^{m+1} \binom{m}{i-1} x^{m-(i-1)}y^{(i-1)+1} \\ &= \sum_{i=1}^{m+1} \binom{m}{i-1} x^{m+1-i)}y^i \\ &= \left(\sum_{i=1}^{m} \binom{m}{i-1} x^{m+1-i)}y^i\right) + \binom{m}{(m+1)-1} x^{m+1-(m+1)}y^{m+1} \\ &= \left(\sum_{i=1}^{m} \binom{m}{i-1} x^{m+1-i)}y^i\right) + \binom{m}{m} x^0 y^{m+1}.\end{aligned}$$

(5) Ut ifra Korollar 1.9.11 er $\binom{m}{m} = 1$. Derfor er:

$$\left(\sum_{i=1}^{m} \binom{m}{i-1} x^{m+1-i)}y^i\right) + \binom{m}{m} x^0 y^{m+1} = \left(\sum_{i=1}^{m} \binom{m}{i-1} x^{m+1-i)}y^i\right) + y^{m+1}.$$

(6) Vi har:

$$x^{m+1} + \left(\sum_{i=1}^{m} \binom{m}{i} x^{m+1-i} y^i\right) + \left(\sum_{i=1}^{m} \binom{m}{i-1} x^{m+1-i)} y^i\right) + y^{m+1}$$
$$= x^{m+1} + \left(\sum_{i=1}^{m} \left(\binom{m}{i} + \binom{m}{i-1}\right) x^{m+1-y} y^i\right) + y^{m+1}$$

(7) Ut ifra Proposisjon 1.9.18 er

$$\binom{m+1}{i} = \binom{m}{i} + \binom{m}{i-1}$$

for alle heltall i slik at $1 \leq i \leq m$. Vi deduserer at

$$x^{m+1} + \left(\sum_{i=1}^{m} \left(\binom{m}{i} + \binom{m}{i-1}\right) x^{m+1-y} y^i\right) + y^{m+1}$$
$$= x^{m+1} + \left(\sum_{i=1}^{m} \left(\binom{m}{i} + \binom{m}{i-1}\right) x^{m+1-y} y^i\right) y^{m+1}$$
$$= x^{m+1} + \left(\sum_{i=1}^{m} \binom{m+1}{i} x^{m+1-i} y^i\right) + y^{m+1}.$$

Vi deduserer fra (1) – (7) at

$$(x+y)^{m+1} = x^{m+1} + \left(\sum_{i=1}^{m} \binom{m+1}{i} x^{m+1-i} y^i\right) + y^{m+1}.$$

Nå gjør vi følgende observasjoner.

(1) Vi har:

$$\sum_{i=0}^{m+1} \binom{m+1}{i} x^{m+1-i} y^i$$
$$= \binom{m+1}{0} x^{m+1-0} y^0 + \left(\sum_{i=1}^{m} \binom{m+1}{i} x^{m+1-i} y^i\right) + \binom{m+1}{m+1} x^{m+1-(m+1)} y^{m+1}$$
$$= \binom{m+1}{0} x^{m+1} + \left(\sum_{i=1}^{m} \binom{m+1}{i} x^{m+1-i} y^i\right) + \binom{m+1}{m+1} y^{m+1}$$

(2) Ut ifra Proposisjon 1.9.8 er $\binom{m+1}{0} = 1$. Ut ifra Korollar 1.9.11 er $\binom{m+1}{m+1} = 1$. Derfor er

$$\binom{m+1}{0} x^{m+1} + \left(\sum_{i=1}^{m} \binom{m+1}{i} x^{m+1-i} y^i\right) + \binom{m+1}{m+1} y^{m+1}$$
$$= x^{m+1} + \left(\sum_{i=1}^{m} \binom{m+1}{i} x^{m+1-i} y^i\right) + y^{m+1}.$$

Vi deduserer fra (1) – (2) at

$$\sum_{i=0}^{m+1} \binom{m+1}{i} x^{m+1-i}y^i = x^{m+1} + \left(\sum_{i=1}^{m} \binom{m+1}{i} x^{m+1-i}y^i\right) + y^{m+1}.$$

For å oppsummere beviset så langt, har vi fastslått at

$$(x+y)^{m+1} = x^{m+1} + \left(\sum_{i=1}^{m} \binom{m+1}{i} x^{m+1-i}y^i\right) + y^{m+1}$$

og at

$$x^{m+1} + \left(\sum_{i=1}^{m} \binom{m+1}{i} x^{m+1-i}y^i\right) + y^{m+1} = \sum_{i=0}^{m+1} \binom{m+1}{i} x^{m+1-i}y^i.$$

Vi deduserer at

$$(x+y)^{m+1} = \sum_{i=0}^{m+1} \binom{m+1}{i} x^{m+1-i}y^i.$$

Dermed er proposisjonen sann når n er det naturlige tallet $m+1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall.

□

Eksempel 1.9.31. Når $n = 2$, fastslår Proposisjon 1.9.30 at

$$(x+y)^2 = x^2 + 2xy + y^2,$$

som forventet.

Eksempel 1.9.32. Når $n = 3$, fastslår Proposisjon 1.9.30 at

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

Eksempel 1.9.33. Når $n = 4$, fastslår Proposisjon 1.9.30 at

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4.$$

Merknad 1.9.34. Proposisjon 1.9.30 kalles noen ganger *binomialteoremet*.

Merknad 1.9.35. Den viktigste delen av beviset for Proposisjon 1.9.30 er ligningen

$$(x+y)^m \cdot (x+y) = \left(\sum_{i=0}^{m} \binom{m}{i} x^{m-i}y^i\right) \cdot (x+y).$$

Det er her vi benytter antakelsen at

$$(x+y)^m = \sum_{i=0}^{m} \binom{m}{i} a^{m-i}b^i.$$

Merknad 1.9.36. Til å begynne med kan manipulasjoner med summetegn som i beviset for Proposisjon 1.9.30 se litt forvirrende ut. I så fall skriv alle summene uten å bruke summetegnet. Skriv for eksempel

$$\sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

som

$$\binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \cdots + \binom{n}{n-1} x^1 y^{n-1} + \binom{n}{n} x^0 y^n.$$

1.10 Rekursjon

Merknad 1.10.1. Hvert tall i sekvensen

$$1, 2, 4, 8, 16, \ldots$$

er to ganger det foregående. Hvordan kan vi beskrive sekvensen formelt?

Vi kan ikke skrive ut hele sekvensen uansett hvor mye tid vi har: sammenlign med Merknad 1.4.1. Istedenfor benytter vi en type definisjon som kalles rekursjon.

Terminologi 1.10.2. Anta at vi ønsker å definere et heltall u_n for hvert naturlig tall n. *Rekursjon* sier at vi kan gjøre det på følgende måte:

(1) Definer u_1, u_2, …, u_r, hvor r er et gitt naturlig tall.

(2) La m være et naturlig tall som er større enn eller likt r. Hvis det antas at heltallet u_i har blitt definert for alle de naturlige tallene slik at $r \leq i \leq m$, definer heltallet u_{m+1}.

Merknad 1.10.3. I Merknad 1.4.3 så vi at induksjon gir en algoritme for å konstruere et bevis. På en lignende måte gir rekursjon en algoritme for å definere det n-te naturlige tallet i en sekvens, for et hvilket som helst naturlig tall n:

(i) Etter å ha fullført Steg (1) i Terminologi 1.10.2, har vi definert alle heltallene i sekvensen opp til det r-te;

(ii) Steg (2) i Terminologi 1.10.2 fastslår at vi da kan definere det $(r+1)$-te heltallet i sekvensen;

(iii) Steg (2) i Terminologi 1.10.2 fastslår at vi *da* kan definere det $(r+2)$-te heltallet i sekvensen;

(iv) Steg (2) i Terminologi 1.10.2 fastslår at vi *da* kan definere det $(r+3)$-te heltallet i sekvensen;

(v) Slik fortsetter vi til vi når det naturlige tallet vi er interessert i.

Eksempel 1.10.4. Følgende definerer en sekvens ved rekursjon.

(1) Det første heltallet i sekvensen er 1. Med andre ord er $u_1 = 1$. Ved å la r være 1, har vi dermed fullført Steg (1) i Terminologi 1.10.2.

(2) La m være et naturlig tall. Anta at det i-te heltallet i sekvensen, det vil si u_i, har blitt definert for alle de naturlige tallene i slik at $1 \leq i \leq m$. Da definerer vi heltallet u_{m+1} være $2u_m$. Ved å la r være 1, har vi dermed fullført Steg (2) i Terminologi 1.10.2.

La oss se hvordan algoritmen i Merknad 1.10.3 ser ut for denne sekvensen.

(i) Ut ifra (1) er 1 det første heltallet i sekvensen.

(ii) Fra (i) og (2) følger det at $2 \cdot 1 = 2$ er det andre heltallet i sekvensen.

(iii) Fra (ii) og (2) følger det at $2 \cdot 2 = 4$ er det tredje heltallet i sekvensen.

(iv) Fra (iii) og (2) følger det at $2 \cdot 4 = 8$ er det fjerde heltallet i sekvensen.

(v) Slik fortsetter vi.

Således ser vi at (1) og (2) formelt definerer sekvensen

$$1, 2, 4, 8, 16, \ldots$$

som vi tok for oss i Merknad 1.10.1.

Eksempel 1.10.5. Følgende definerer en sekvens ved rekursjon.

(1) Det første heltallet i sekvensen er -1. Med andre ord er $u_1 = -1$. Ved å la r være 1, har vi dermed fullført Steg (1) i Terminologi 1.10.2.

(2) La m være et naturlig tall. Anta at det i-te heltallet i sekvensen, det vil si u_i, har blitt definert for alle de naturlige tallene i slik at $1 \leq i \leq m$. Da definerer vi heltallet u_{m+1} til å være $u_m + 3$.

Dermed har vi formelt definert sekvensen:

$$-1, 2, 5, 8, 11, \ldots.$$

Merknad 1.10.6. I både Eksempel 1.10.4 og Eksempel 1.10.5 lot vi det naturlige tallet r i Terminologi 1.10.2 til å være 1. I den neste delen skal vi se på et eksempel hvor vi lar r være 2.

Merknad 1.10.7. Induksjon og rekursjon går hånd i hånd. For å bevise et matematisk utsagn som handler om en sekvens av heltall definert ved rekursjon, benytter vi typisk induksjon.

1.11 Fibonaccitall

Definisjon 1.11.1. Følgende definerer ved rekursjon *sekvensen av Fibonaccitall*.

(1) Det første heltallet i sekvensen er 1. Med andre ord er $u_1 = 1$.

(2) Det andre heltallet i sekvensen er 1. Med andre ord er $u_2 = 1$.

(3) La m være et naturlig tall slik at $m \geq 2$. Anta at det i-te heltallet i sekvensen, det vil si u_i, har blitt definert for alle de naturlige tallene i slik at $2 \leq i \leq m$. Da definerer vi heltallet u_{m+1} til å være $u_{m-1} + u_m$.

Merknad 1.11.2. Steg (1) og Steg (2) i Definisjon 1.11.1 fullfører, ved å la r være 2, Steg (1) i Terminologi 1.10.2. Steg (3) i Definisjon 1.11.1 fullfører, ved å la r være 2, Steg (2) i Terminologi 1.10.2.

Merknad 1.11.3. La oss se hvordan algoritmen i Merknad 1.10.3 ser ut for sekvensen av Fibonaccitall.

(i) Ut ifra Steg (1) i Definisjon 1.11.1 er 1 det første heltallet i sekvensen.

(ii) Ut ifra Steg (2) i Definisjon 1.11.1 er 1 det andre heltallet i sekvensen.

(iii) Fra (i), (ii) og Steg (3) i Definisjon 1.11.1, følger det at $1 + 1 = 2$ er det tredje heltallet i sekvensen.

(iv) Fra (ii), (iii) og Steg (3) i Definisjon 1.11.1, følger det at $1 + 2 = 3$ er det fjerde heltallet i sekvensen.

(iv) Fra (iii), (iv) og Steg (4) i Definisjon 1.11.1, følger det at $2 + 3 = 5$ er det femte heltallet i sekvensen.

(v) Slik fortsetter vi.

Dermed er sekvensen av Fibonaccitall:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots.$$

Terminologi 1.11.4. La n være et naturlig tall. Heltallet u_n i sekvensen av Fibonaccitall kalles det *n-te Fibonaccitallet*.

Notasjon 1.11.5. La n være et naturlig tall. I resten av dette kapittelet kommer alltid u_n til å betegne det n-te Fibonaccitallet.

Proposisjon 1.11.6. La n være et naturlig tall. Da er

$$u_1 + u_2 + \cdots + u_n = u_{n+2} - 1.$$

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. I dette tilfellet er utsagnet at

$$u_1 = u_{1+2} - 1.$$

Siden $u_1 = 1$ og

$$u_{1+2} - 1 = u_3 - 1 = 2 - 1 = 1,$$

er dette sant.

Anta nå at proposisjonen har blitt bevist når n er et gitt naturlig tall m. Således har det blitt bevist at

$$u_1 + u_2 + \cdots + u_m = u_{m+2} - 1.$$

Vi gjør følgende observasjoner.

(1) Fra antakelsen at

$$u_1 + u_2 + \cdots + u_m = u_{m+2} - 1,$$

følger det at

$$\begin{aligned} u_1 + u_2 + \cdots + u_m + u_{m+1} &= (u_{m+2} - 1) + u_{m+1} \\ &= u_{m+2} + u_{m+1} - 1. \end{aligned}$$

(2) Ut ifra definisjonen til sekvensen av Fibonaccitall er

$$u_{m+3} = u_{m+2} + u_{m+1}.$$

Fra (1) – (2) deduserer vi at

$$u_1 + u_2 + \cdots + u_m + u_{m+1} = u_{m+3} - 1.$$

Dermed er proposisjonen sann når n er det naturlige tallet $m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall.

□

Eksempel 1.11.7. Når $n = 2$, fastslår Proposisjon 1.11.6 at

$$u_1 + u_2 = u_4 - 1,$$

altså at

$$1 + 1 = 3 - 1.$$

Eksempel 1.11.8. Når $n = 3$, fastslår Proposisjon 1.11.6 at

$$u_1 + u_2 + u_3 = u_5 - 1,$$

altså at

$$1 + 1 + 2 = 5 - 1.$$

Eksempel 1.11.9. Når $n = 4$, fastslår Proposisjon 1.11.6 at

$$u_1 + u_2 + u_3 + u_4 = u_6 - 1,$$

altså at

$$1 + 1 + 2 + 3 = 8 - 1.$$

Eksempel 1.11.10. Når $n = 9$, fastslår Proposisjon 1.11.6 at

$$u_1 + u_2 + \cdots + u_9 = u_{11} - 1,$$

altså at

$$1 + 1 + 2 + 3 + 5 + 8 + 13 + 21 + 34 = 89 - 1.$$

Merknad 1.11.11. Den viktigste delen av dette beviset er ligningen

$$u_1 + u_2 + \cdots + u_m + u_{m+1} = (u_{m+2} - 1) + u_{m+1}.$$

Det er her vi benytter antakelsen at

$$u_1 + u_2 + \cdots + u_m = u_{m+2} - 1.$$

Proposisjon 1.11.12. La n være et naturlig tall slik at $n \geq 2$. Da er

$$u_n^2 = u_{n+1}u_{n-1} + (-1)^{n-1}.$$

Bevis. Først sjekker vi om proposisjonen er sann når $n = 2$. I dette tilfellet er utsagnet at

$$u_2^2 = u_{2+1}u_{2-1} + (-1)^{2-1}.$$

Siden

$$u_2^2 = 1^2 = 1$$

og

$$\begin{aligned} u_{2+1}u_{2-1} + (-1)^{2-1} &= u_3u_1 - 1 \\ &= 2 \cdot 1 - 1 \\ &= 2 - 1 \\ &= 1, \end{aligned}$$

er dette sant.

Anta nå at proposisjonen har blitt bevist når n et gitt naturlig tall m slik at $m \geq 2$. Således har det blitt bevist at

$$u_m^2 = u_{m+1}u_{m-1} + (-1)^{m-1}.$$

Vi gjør følgende observasjoner.

(1) Ut ifra definisjonen til sekvensen av Fibonaccitall er

$$u_{m+1} = u_m + u_{m-1}.$$

Derfor er

$$\begin{aligned} u_{m+1}^2 - u_{m+2}u_m &= u_{m+1}\left(u_m + u_{m-1}\right) - u_{m+2}u_m \\ &= u_{m+1}u_m + u_{m+1}u_{m-1} - u_{m+2}u_m \\ &= u_m\left(u_{m+1} - u_{m+2}\right) + u_{m+1}u_{m-1}. \end{aligned}$$

(2) Ut ifra definisjonen til sekvensen av Fibonaccitall er

$$u_{m+2} = u_{m+1} + u_m.$$

Derfor er

$$u_{m+1} - u_{m+2} = -u_m.$$

Vi deduserer at

$$u_m\left(u_{m+1} - u_{m+2}\right) + u_{m+1}u_{m-1} = -u_m^2 + u_{m+1}u_{m-1}.$$

(3) Fra antakelsen at

$$u_m^2 = u_{m+1}u_{m-1} + (-1)^{m-1},$$

følger det at

$$\begin{aligned} -u_m^2 + u_{m+1}u_{m-1} &= -(-1)^{m-1} \\ &= (-1)\cdot(-1)^{m-1} \\ &= (-1)^{m-1+1} \\ &= (-1)^m. \end{aligned}$$

Fra (1) – (3) deduserer vi at

$$u_{m+1}^2 - u_{m+2}u_m = (-1)^m.$$

Derfor er

$$u_{m+1}^2 = u_{m+2}u_m + (-1)^m.$$

Dermed er proposisjonen sann når n er det naturlige tallet $m+1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall slik at $n \geq 2$.

□

Eksempel 1.11.13. Når $n = 3$, fastslår Proposisjon 1.11.12 at

$$2^2 = 3 \cdot 1 + 1.$$

Eksempel 1.11.14. Når $n = 4$, fastslår Proposisjon 1.11.12 at

$$3^2 = 5 \cdot 2 - 1.$$

Eksempel 1.11.15. Når $n = 9$, fastslår Proposisjon 1.11.12 at

$$34^2 = 55 \cdot 21 + 1.$$

Merknad 1.11.16. Den viktigste delen av beviset for Proposisjon 1.11.12 er Steg (3). Det er her vi benytter antakelsen at

$$u_m^2 = u_{m+1}u_{m-1} + (-1)^{m-1}.$$

1.12 Binets formel for Fibonaccitallene

Merknad 1.12.1. Nå skal vi finne en formel for det n-te Fibonaccitallet.

Proposisjon 1.12.2. La x være en løsning til ligningen

$$x^2 - x - 1 = 0.$$

La n være et naturlig tall slik at $n \geq 2$. Da er

$$x^n = xu_n + u_{n-1}.$$

Bevis. Først sjekker vi om proposisjonen er sann når $n = 2$. I dette tilfellet er utsagnet at

$$x^2 = xu_2 + u_1.$$

Siden $u_1 = 1$ og $u_2 = 1$, er

$$xu_2 + u_1 = x \cdot 1 + 1 = x + 1.$$

Ut ifra antakelsen at

$$x^2 - x - 1 = 0,$$

er

$$x^2 = x + 1.$$

Dermed er utsagnet sant.

Anta nå at proposisjonen har blitt bevist for et gitt heltall m slik at $m \geq 2$. Således har det blitt bevist at

$$x^m = xu_m + u_{m-1}.$$

Vi gjør følgende observasjoner.

(1) Fra antakelsen at

$$x^m = xu_m + u_{m-1}$$

følger det, ved å gange begge sidene i denne ligningen med x, at

$$x^{m+1} = x^2u_m + xu_{m-1}.$$

(2) Siden x er en løsning til ligningen

$$x^2 - x - 1 = 0,$$

er

$$x^2 = x + 1.$$

Fra (1) – (2) deduserer vi at

$$x^{m+1} = (x+1)u_m + xu_{m-1}.$$

Nå gjør vi følgende observajoner.

(1) Vi har:

$$\begin{aligned}(x+1)u_m + xu_{m-1} &= xu_m + u_m + xu_{m-1} \\ &= xu_m + xu_{m-1} + u_m \\ &= x(u_m + u_{m-1}) + u_m.\end{aligned}$$

(2) Ut ifra definisjonen til sekvensen av Fibonaccitall er

$$u_{m+1} = u_m + u_{m-1}.$$

Fra (1) – (2) deduserer vi at

$$(x+1)u_m + xu_{m-1} = xu_{m+1} + u_m.$$

For å oppsummere beviset så langt, har vi fastslått at

$$x^{m+1} = (x+1)u_m + xu_{m-1}$$

og at

$$(x+1)u_m + xu_{m-1} = xu_{m+1} + u_m.$$

Vi deduserer at

$$x^{m+1} = xu_{m+1} + u_m.$$

Dermed er proposisjonen sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann for alle naturlige tall n slik at $n \geq 2$.

□

Eksempel 1.12.3. La x være en løsning til ligningen

$$x^2 - x - 1 = 0.$$

Når $n = 3$, fastslår Proposisjon 1.12.2 at

$$\begin{aligned}x^3 &= u_3 x + u_2 \\ &= 2x + 1.\end{aligned}$$

Eksempel 1.12.4. La x være en løsning til ligningen

$$x^2 - x - 1 = 0.$$

Når $n = 5$, fastslår Proposisjon 1.12.2 at

$$\begin{aligned} x^5 &= u_5 x + u_5 \\ &= 5x + 3 \end{aligned}$$

Eksempel 1.12.5. La x være en løsning til ligningen

$$x^2 - x - 1 = 0.$$

Når $n = 7$, fastslår Proposisjon 1.12.2 at

$$\begin{aligned} x^7 &= u_7 x + u_6 \\ &= 13x + 8 \end{aligned}$$

Eksempel 1.12.6. La x være en løsning til ligningen

$$x^2 - x - 1 = 0.$$

Når $n = 9$, fastslår Proposisjon 1.12.2 at

$$\begin{aligned} x^9 &= u_9 x + u_8 \\ &= 34x + 21. \end{aligned}$$

Lemma 1.12.7. Tallene $\frac{1+\sqrt{5}}{2}$ og $\frac{1-\sqrt{5}}{2}$ er løsninger til ligningen

$$x^2 - x - 1 = 0.$$

Bevis. For å bevise at $\frac{1+\sqrt{5}}{2}$ er en løsning til ligningen

$$x^2 - x - 1 = 0,$$

regner vi som følger:

$$\begin{aligned} \left(\frac{1+\sqrt{5}}{2}\right)^2 - \frac{1+\sqrt{5}}{2} - 1 &= \frac{\left(1+\sqrt{5}\right)\cdot\left(1+\sqrt{5}\right)}{4} - \frac{1+\sqrt{5}}{2} - 1 \\ &= \frac{1+2\sqrt{5}+5}{4} - \frac{1+\sqrt{5}}{2} - 1 \\ &= \frac{1+2\sqrt{5}+5-2-2\sqrt{5}-4}{4} \\ &= \frac{0}{4} \\ &= 0. \end{aligned}$$

For å bevise at $\frac{1-\sqrt{5}}{2}$ er en løsning til ligningen

$$x^2 - x - 1 = 0,$$

regner vi som følger:

$$\begin{aligned}\left(\frac{1-\sqrt{5}}{2}\right)^2 - \frac{1-\sqrt{5}}{2} - 1 &= \frac{\left(1-\sqrt{5}\right)\cdot\left(1-\sqrt{5}\right)}{4} - \frac{1-\sqrt{5}}{2} - 1 \\ &= \frac{1-2\sqrt{5}+5}{4} - \frac{1-\sqrt{5}}{2} - 1 \\ &= \frac{1-2\sqrt{5}+5-2+2\sqrt{5}-4}{4} \\ &= \frac{0}{4} \\ &= 0.\end{aligned}$$

□

Merknad 1.12.8. Tallet $\frac{1+\sqrt{5}}{2}$ kalles noen ganger det gyldne snitt.

Proposisjon 1.12.9. La n være et naturlig tall. Da er

$$u_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Bevis. Fra Proposisjon 1.12.2 og Lemma 1.12.7 følger det at

$$\left(\frac{1+\sqrt{5}}{2}\right)^n = \left(\frac{1+\sqrt{5}}{2}\right)\cdot u_n + u_{n-1},$$

og at

$$\left(\frac{1-\sqrt{5}}{2}\right)^n = \left(\frac{1-\sqrt{5}}{2}\right)\cdot u_n + u_{n-1}.$$

Ved å benytte oss av disse faktaene, regner vi som følger:

$$\begin{aligned}
\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n &= \left(\frac{1+\sqrt{5}}{2}\right)\cdot u_n + u_{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)\cdot u_n - u_{n-1} \\
&= \left(\frac{1+\sqrt{5}}{2}\right)\cdot u_n - \left(\frac{1-\sqrt{5}}{2}\right)\cdot u_n \\
&= \left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right)\cdot u_n \\
&= \left(\frac{1+\sqrt{5}-1+\sqrt{5}}{2}\right)\cdot u_n \\
&= \frac{2\sqrt{5}}{2}\cdot u_n \\
&= \sqrt{5}\cdot u_n.
\end{aligned}$$

Dermed har vi bevist at

$$\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n = \sqrt{5}\cdot u_n.$$

Ved å dele begge sidene i denne ligningen med $\sqrt{5}$, deduserer vi at proposisjonen er sann.

□

Eksempel 1.12.10. Når $n = 2$, fastslår Proposisjon 1.12.9 at

$$1 = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right).$$

Eksempel 1.12.11. Når $n = 3$, fastslår Proposisjon 1.12.9 at

$$2 = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^3 - \left(\frac{1-\sqrt{5}}{2}\right)^3\right).$$

Eksempel 1.12.12. Når $n = 6$, fastslår Proposisjon 1.12.9 at

$$8 = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^6 - \left(\frac{1-\sqrt{5}}{2}\right)^6\right).$$

Eksempel 1.12.13. Når $n = 9$, fastslår Proposisjon 1.12.9 at

$$34 = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^9 - \left(\frac{1-\sqrt{5}}{2}\right)^9\right).$$

Terminologi 1.12.14. Ligningen i Proposisjon 1.12.9 kalles *Binets formel*.

Merknad 1.12.15. Flere fakta kan deduseres fra Proposisjon 1.12.9. Etter noen forberedelser skal se på et eksempel: Proposisjon 1.12.18.

Lemma 1.12.16. Vi har:

$$\left(\frac{1+\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right) = -1.$$

Bevis. Vi regner som følger:

$$\begin{aligned}\left(\frac{1+\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right) &= \frac{\left(1+\sqrt{5}\right)\left(1-\sqrt{5}\right)}{4} \\ &= \frac{1+\sqrt{5}-\sqrt{5}-5}{4} \\ &= \frac{-4}{4} \\ &= -1.\end{aligned}$$

□

Lemma 1.12.17. Vi har:

$$\frac{1}{5}\left(\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right) = \frac{1}{\sqrt{5}}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Eksempel 1.12.10 er

$$1 = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right).$$

Ved å gange begge sidene av denne ligningen med $\frac{1}{\sqrt{5}}$, følger det at

$$\frac{1}{\sqrt{5}} = \frac{1}{\sqrt{5}} \cdot \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right).$$

(2) Vi har:

$$\begin{aligned}
&\frac{1}{\sqrt{5}} \cdot \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^2 - \left(\frac{1-\sqrt{5}}{2} \right)^2 \right) \\
&= \frac{1}{\sqrt{5} \cdot \sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^2 - \left(\frac{1-\sqrt{5}}{2} \right)^2 \right) \\
&= \frac{1}{5} \left(\left(\frac{1+\sqrt{5}}{2} \right)^2 - \left(\frac{1-\sqrt{5}}{2} \right)^2 \right)
\end{aligned}$$

Fra (1) – (2) deduserer vi at

$$\frac{1}{\sqrt{5}} = \frac{1}{5} \left(\left(\frac{1+\sqrt{5}}{2} \right)^2 - \left(\frac{1-\sqrt{5}}{2} \right)^2 \right).$$

□

Proposisjon 1.12.18. La n være et naturlig tall. Da er

$$u_{n+2}^2 - u_n^2 = u_{2n+2}.$$

Bevis. For å gjøre beviset lettere å lese, la x være $\frac{1+\sqrt{5}}{2}$, og la y være $\frac{1-\sqrt{5}}{2}$. Vi gjør følgende observasjoner.

(1) La m være et naturlig tall. Ut ifra Proposisjon 1.12.9 er

$$u_m = \frac{1}{\sqrt{5}} \left(x^m - y^m \right).$$

Derfor er

$$\begin{aligned}
u_m^2 &= \left(\frac{1}{\sqrt{5}} \left(x^m - y^m \right) \right)^2 \\
&= \frac{1}{5} \left(x^m - y^m \right) \left(x^m - y^m \right) \\
&= \frac{1}{5} \left(x^{2m} - 2x^m y^m + y^{2m} \right) \\
&= \frac{1}{5} \left(x^{2m} - 2(xy)^m + y^{2m} \right).
\end{aligned}$$

(2) Ut ifra Lemma 1.12.16 er

$$2 \cdot (xy)^m = 2 \cdot (-1)^m.$$

Fra (1) – (2) deduserer vi at

$$u_m^2 = \frac{1}{5}\left(x^{2m} - 2\cdot(-1)^m + y^{2m}\right).$$

Dermed er

$$u_n^2 = \frac{1}{5}\left(x^{2n} - 2\cdot(-1)^n + y^{2n}\right)$$

og er

$$u_{n+2}^2 = \frac{1}{5}\left(x^{2(n+2)} - 2\cdot(-1)^{n+2} + y^{2(n+2)}\right).$$

Vi deduserer at

$$\begin{aligned}
&u_{n+2}^2 - u_n^2 \\
&= \frac{1}{5}\left(x^{2(n+2)} - 2\cdot(-1)^{n+2} + y^{2(n+2)}\right) - \frac{1}{5}\left(x^{2n} - 2\cdot(-1)^n + y^{2n}\right) \\
&= \frac{1}{5}\left(x^{2(n+2)} - 2\cdot(-1)^n\cdot(-1)^2 + y^{2(n+2)} - x^{2n} + 2\cdot(-1)^n - y^{2n}\right) \\
&= \frac{1}{5}\left(x^{2(n+2)} + y^{2(n+2)} - x^{2n} - y^{2n} - 2\cdot(-1)^n + 2\cdot(-1)^n\right) \\
&= \frac{1}{5}\left(x^{2(n+2)} + y^{2(n+2)} - x^{2n} - y^{2n}\right)
\end{aligned}$$

Dermed er

$$u_{n+2}^2 - u_n^2 = \frac{1}{5}\left(x^{2(n+2)} + y^{2(n+2)} - x^{2n} - y^{2n}\right).$$

Nå gjør vi følgende observasjoner.

(1) Ut ifra Lemma 1.12.16 er

$$x^2y^2 = (xy)^2 = (-1)^2 = 1.$$

Derfor er

$$\begin{aligned}
\frac{1}{5}\left(x^{2(n+2)} + y^{2(n+2)} - x^{2n} - y^{2n}\right) &= \frac{1}{5}\left(x^{2(n+2)} + y^{2(n+2)} - x^2y^2x^{2n} - x^2y^2y^{2n}\right) \\
&= \frac{1}{5}\left(x^{2n+4} + y^{2n+4} - y^2x^{2n+2} - x^2y^{2n+2}\right) \\
&= \frac{1}{5}\left(x^2 - y^2\right)\left(x^{2n+2} - y^{2n+2}\right)
\end{aligned}$$

(2) Ut ifra Lemma 1.12.17 er

$$\frac{1}{5}\left(x^2 - y^2\right) = \frac{1}{\sqrt{5}}.$$

Derfor er

$$\frac{1}{5}\left(x^2 - y^2\right)\left(x^{2n+2} - y^{2n+2}\right) = \frac{1}{\sqrt{5}}\left(x^{2n+2} - y^{2n+2}\right).$$

(3) Ut ifra Proposisjon 1.12.9 er

$$u_{2n+2} = \frac{1}{\sqrt{5}} \left(x^{2n+2} - y^{2n+2} \right).$$

Vi deduserer fra (1) – (3) at

$$\frac{1}{5} \left(x^{2(n+2)} + y^{2(n+2)} - x^{2n} - y^{2n} \right) = x_{2n+2}.$$

For å oppsummere beviset så langt, har vi fastslått at

$$u_{n+2}^2 - u_n^2 = \frac{1}{5} \left(x^{2(n+2)} + y^{2(n+2)} - x^{2n} - y^{2n} \right)$$

og at

$$\frac{1}{5} \left(x^{2(n+2)} + y^{2(n+2)} - x^{2n} - y^{2n} \right) = x_{2n+2}.$$

Vi deduserer at

$$u_{n+2}^2 - u_n^2 = u_{2n+2}.$$

□

Eksempel 1.12.19. Når $n = 2$, fastslår Proposisjon 1.12.18 at

$$3^2 - 1^2 = 8.$$

Eksempel 1.12.20. Når $n = 3$, fastslår Proposisjon 1.12.18 at

$$5^2 - 2^2 = 21.$$

Eksempel 1.12.21. Når $n = 5$, fastslår Proposisjon 1.12.18 at

$$13^2 - 5^2 = 144.$$

1.13 Varianter av induksjon

Merknad 1.13.1. Det finnes mange varianter av induksjon. Noen av disse kalles noen ganger «sterk induksjon», men vi skal ikke benytte denne terminologien. Nå skal vi se på de viktigste variantene for oss.

Terminologi 1.13.2. La c være et heltall slik at $c \geq 0$. Anta at vi har et gitt matematisk utsagn for hvert heltall større enn eller likt et gitt heltall r. Anta dessuten at vi ønsker å bevise utsagnet for hvert av disse heltallene. *Induksjon* sier at vi kan gjøre det på følgende måte:

(1) Sjekk om utsagnet er sant for alle heltallene r, $r + 1$, ..., $r + c$.

(2) Hvis det antas at utsagnet har blitt bevist for alle heltallene m, $m-1$, $\ldots$, $m-c$, hvor m er et gitt heltall som er større enn eller likt $r+c$, bevis at utsagnet er sant for heltallet $m+1$.

Merknad 1.13.3. Induksjon som beskrevet i Terminologi 1.4.2 er det samme som induksjon som beskrevet i Terminologi 1.13.2 for $c = 0$.

Merknad 1.13.4. Idéen bak induksjon som beskrevet i Terminologi 1.13.2 er at Steg (1) og Steg (2) gir oss følgende algoritmen for å konstruere et bevis for utsagnet for et hvilket som helst heltall m større enn r:

(i) Steg (1) i Terminologi 1.13.2 fastslår at vi kan bevise utsagnet for alle heltallene m slik at $r \leq m \leq r+c$;

(ii) Steg (2) i Terminologi 1.13.2 fastslår at vi da kan bevise utsagnet når $m = r+c+1$;

(iii) Steg (2) i Terminologi 1.13.2 fastslår at vi *da* kan bevise utsagnet når $m = r+c+2$;

(iv) Steg (2) i Terminologi 1.13.2 fastslår at vi *da* kan bevise utsagnet når $m = r+c+3$;

(v) Slik fortsetter til vi når heltallet vi er interessert i.

Merknad 1.13.5. Algoritmen i Merknad 1.4.3 er det samme som algoritmen i Merknad 1.13.4 for $c = 0$.

Proposisjon 1.13.6. La x være et heltall, og la n være et naturlig tall. Da er

$$x^n - 1 = (x-1) \cdot \left(x^{n-1} + x^{n-2} + \cdots + x + 1\right).$$

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$ og når $n = 2$.

(1) Når $n = 1$ er utsagnet at

$$x^1 - 1 = (x-1) \cdot 1.$$

Dette er sant.

(2) Når $n = 2$ er utsagnet at

$$x^2 - 1 = (x-1)(x+1).$$

Siden

$$(x+1)(x-1) = x^2 + x - x - 1 = x^2 - 1,$$

er dette sant.

Anta nå at proposisjonen har blitt bevist når $n = m$ og når $n = m-1$, hvor m er et naturlig tall slik at $m \geq 2$. Således har det blitt bevist at

$$x^m - 1 = (x-1) \cdot \left(x^{m-1} + x^{m-2} + \cdots + x + 1\right)$$

og at

$$x^{m-1} - 1 = (x-1) \cdot \left(x^{(m-1)-1} + x^{(m-1)-2} + \cdots + x + 1\right).$$

Vi gjør følgende observasjoner.

(1) Vi har:

$$\begin{aligned}(x+1)\left(x^m-1\right)-x\left(x^{m-1}-1\right) &= x^{m+1}-x+x^m-1-x^m+x\\ &= x^{m+1}-1.\end{aligned}$$

(2) Fra antakelsen at

$$\begin{aligned}x^m-1 &= (x-1)\cdot\left(x^{m-1}+x^{m-2}+\cdots+x+1\right)\\ &= (x-1)\cdot\left(\sum_{i=0}^{m-1}x^i\right),\end{aligned}$$

og antakelsen at

$$\begin{aligned}x^{m-1}-1 &= (x-1)\cdot\left(x^{(m-1)-1}+x^{(m-1)-2}+\cdots+x+1\right)\\ &= (x-1)\cdot\left(x^{m-2}+x^{m-3}+\cdots+x+1\right)\\ &= (x-1)\cdot\left(\sum_{i=0}^{m-2}x^i\right),\end{aligned}$$

følger det at

$$\begin{aligned}&(x+1)\left(x^m-1\right)-x\left(x^{m-1}-1\right)\\ &= (x+1)(x-1)\left(\sum_{i=0}^{m-1}x^i\right)-x(x-1)\left(\sum_{i=0}^{m-2}x^i\right)\\ &= (x-1)\left((x+1)\left(\sum_{i=0}^{m-1}x^i\right)-x\left(\sum_{i=0}^{m-2}x^i\right)\right)\\ &= (x-1)\left(x\left(\sum_{i=0}^{m-1}x^i\right)+\left(\sum_{i=0}^{m-1}x^i\right)-x\left(\sum_{i=0}^{m-2}x^i\right)\right)\\ &= (x-1)\left(\left(\sum_{i=1}^{m}x^i\right)+\left(\sum_{i=0}^{m-1}x^i\right)-\left(\sum_{i=1}^{m-1}x^i\right)\right)\\ &= (x-1)\left(\left(\sum_{i=1}^{m}x^i\right)+1+\left(\sum_{i=1}^{m-1}x^i\right)-\left(\sum_{i=1}^{m-1}x^i\right)\right)\\ &= (x-1)\left(\left(\sum_{i=1}^{m}x^i\right)+1\right)\\ &= (x-1)\left(x^m+x^{m-1}+\cdots+x+1\right)\end{aligned}$$

Fra (1) – (2) deduserer vi at

$$x^{m+1}-1=(x-1)\left(x^m+x^{m-1}+\cdots+x^2+x+1\right).$$

Dermed er proposisjonen sann når n er det naturlige tallet $m+1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall slik at $n \geq 2$. □

Eksempel 1.13.7. La x være et heltall. Når $n = 3$, fastslår Proposisjon 1.13.6 at

$$x^3 - 1 = (x-1)\left(x^2 + x + 1\right).$$

Når for eksempel $x = 5$, fastslår den at

$$124 = 4 \cdot (25 + 5 + 1).$$

Eksempel 1.13.8. La x være et heltall. Når $n = 5$, fastslår Proposisjon 1.13.6 at

$$x^5 - 1 = (x-1)\left(x^4 + x^3 + x^2 + x + 1\right).$$

Når for eksempel $x = -3$, fastslår den at

$$-244 = -4 \cdot (81 - 27 + 9 - 3 + 1).$$

Merknad 1.13.9. Det er lett å bevise Proposisjon 1.13.6 uten å benytte induksjon. Vi kan regne som følger:

$$\begin{aligned}
&(x-1)\left(x^{n-1} + x^{n-2} + \cdots + x + 1\right) \\
&= x\left(x^{n-1} + x^{n-2} + \cdots + x + 1\right) - \left(x^{n-1} + x^{n-2} + \cdots + x + 1\right) \\
&= \left(x^n + x^{n-1} + \cdots + x^2 + x\right) - \left(x^{n-1} + x^{n-2} + \cdots + x + 1\right) \\
&= x^n - 1.
\end{aligned}$$

Dette er et helt gyldig bevis! Vi benyttet lignende algebraiske manipulasjoner i beviset vi ga for 1.13.6.

Poenget med beviset vi ga for Proposisjon 1.13.6 er å forklare hvordan en gjennomfører et bevis som benytter varianten av induksjon hvor $c = 1$ og $r = 1$ i Terminologi 1.13.2.

Merknad 1.13.10. Den viktigste delen av beviset for Proposisjon 1.13.6 er ligningen

$$(x+1)\left(x^m - 1\right) - x\left(x^{m-1} - 1\right) = (x+1)(x-1)\left(\sum_{i=0}^{m-1} x^i\right) - x(x-1)\left(\sum_{i=0}^{m-2} x^i\right).$$

Det er her vi benytter både antakelsen at

$$x^m - 1 = (x-1) \cdot \left(\sum_{i=0}^{m-1} x^i\right)$$

og antakelsen at

$$x^{m-1} - 1 = (x-1) \cdot \left(\sum_{i=0}^{m-2} x^i\right).$$

Merknad 1.13.11. Kanskje ser det ut som Observasjon (1) i beviset for Proposisjon 1.13.6 har blitt tatt ut av løse luften. Det er sant at vi må være litt kreativ for å finne ligningen i denne observasjonen, og å skjønne at den har noe å si.

Vi kan se på ligningen i Observasjon (1) på følgende måte. Vi ønsker å bevise proposisjonen når $n = m + 1$. Da må vi jobbe med uttrykket $x^{m+1} - 1$. I tillegg har vi antatt at proposisjonen er sann når $n = m$ og $n = m - 1$, altså at

$$x^m - 1 = (x - 1) \cdot \left(\sum_{i=0}^{m-1} x^i \right)$$

og at

$$x^{m-1} - 1 = (x - 1) \cdot \left(\sum_{i=0}^{m-2} x^i \right).$$

Hvis vi finner en ligning med x^{m+1} på en side, og hvor både $x^m - 1$ og $x^{m-1} - 1$ dukker opp på den andre siden, kan vi benytte begge antakelsene for å si noe om x^{m+1}. Det er ingen generell oppskrift for å finne en slik ligning, men i Observasjon (1) klarte vi det.

Merknad 1.13.12. Hvis manipulasjonene med summetegn i beviset for Proposisjon 1.13.6 ser litt forvirrende ut, følg rådet gitt i Merknad 1.13.12. Skriv for eksempel

$$\sum_{i=1}^{m} x^i$$

som

$$x^m + x^{m-1} + \cdots + x^2 + x,$$

og skriv

$$\sum_{i=0}^{m-1} x^i$$

som

$$x^{m-1} + x^{m-2} + \cdots + x + 1.$$

Merknad 1.13.13. La oss se hvordan algoritmen i Merknad 1.13.4 ser ut for Proposisjon 1.13.6. Vi benytter varianten av induksjon hvor $c = 1$ og $r = 1$.

Vi begynner med å sjekke om proposisjonen er sann for alle de naturlige tallene r, $r + 1$, $\ldots$, $r + c$, det vil si når $n = 1$ og når $n = 2$. Vi sjekker altså at

$$x^1 - 1 = x - 1$$

og at

$$x^2 - 1 = (x - 1)(x + 1).$$

Så argumenterer vi som i beviset for Proposisjon 1.13.6, ved å erstatte m med 2. Vi gjør altså følgende observasjoner.

(1) Vi har:

$$\begin{aligned}(x+1)\left(x^2-1\right)-x\left(x^{2-1}-1\right) &= x^3-x+x^2-1-x^2+x\\ &= x^3-1\end{aligned}$$

(2) Vi vet at

$$x^2-1=(x-1)\cdot(x+1)$$

og at

$$x^1-1=(x-1)\cdot 1=x-1.$$

Det følger at

$$\begin{aligned}&(x+1)\left(x^2-1\right)-x\left(x^{2-1}-1\right)\\ &=(x+1)(x-1)(x+1)-x(x-1)\\ &=(x-1)\left((x+1)(x+1)-x\right)\\ &=(x-1)\left(x(x+1)+(x+1)-x\right)\\ &=(x-1)\left(x^2+x+(x+1)-x\right)\\ &=(x-1)\left((x^2+x)+1+x-x\right)\\ &=(x-1)\left((x^2+x)+1\right)\\ &=(x-1)\left(x^2+x^1+1\right)\end{aligned}$$

Fra (1) – (2) deduserer vi at

$$x^3-1=(x-1)\left(x^2+x+1\right).$$

Dermed er proposisjonen sann når $n=3$.

Så argumenterer vi som i beviset for Proposisjon 1.13.6, ved å erstatte m med 3. Vi gjør altså følgende observasjoner.

(1) Vi har:

$$\begin{aligned}(x+1)\left(x^3-1\right)-x\left(x^{3-1}-1\right) &= x^4-x+x^3-1-x^3+x\\ &= x^4-1.\end{aligned}$$

(2) Vi vet at

$$x^3-1=(x-1)\cdot(x^2+x+1)$$

og at

$$x^2-1=(x-1)\cdot(x+1).$$

Det følger at

$$\begin{aligned}
&(x+1)\left(x^3-1\right)-x\left(x^{3-1}-1\right)\\
&=(x+1)(x-1)(x^2+x+1)-x(x-1)(x+1)\\
&=(x-1)\left((x+1)(x^2+x+1)-x(x+1)\right)\\
&=(x-1)\left(x(x^2+x+1)+(x^2+x+1)-x(x+1)\right)\\
&=(x-1)\left((x^3+x^2+x)+(x^2+x+1)-(x^2+x)\right)\\
&=(x-1)\left((x^3+x^2+x)+1+(x^2+x)-(x^2+x)\right)\\
&=(x-1)\left((x^3+x^2+x)+1\right)\\
&=(x-1)\left(x^3+x^2+x^1+1\right)
\end{aligned}$$

Fra (1) – (2) deduserer vi at

$$x^4-1=(x-1)\left(x^3+x^2+x+1\right).$$

Dermed er proposisjonen sann når $n=4$.

Slik fortsetter vi til vi når heltallet vi er interessert i.

1.14 Litt mer om Fibonaccitallene

Proposisjon 1.14.1. La n være et heltall slik at $n \geq 0$, og la k være et naturlig tall slik at $k \geq 3$. Da er

$$u_{n+k}=u_{k-1}\cdot u_{n+2}+u_{k-2}\cdot u_{n+1}.$$

Bevis. Først sjekker vi om proposisjonen er sann når $k=3$ og når $k=4$.

(1) Når $k=3$, er utsagnet at

$$u_{n+3}=u_2\cdot u_{n+2}+u_1\cdot u_{n+1}.$$

Vi gjør følgende observasjoner.

(i) Siden $u_1=1$ og $u_1=1$, er

$$u_2\cdot u_{n+2}+u_1\cdot u_{n+1}=u_{n+2}+u_{n+1}.$$

(ii) Ut ifra definisjonen til sekvensen av Fibonaccitall er

$$u_{n+3}=u_{n+2}+u_{n+1}.$$

Fra (i) – (ii) deduserer vi at utsagnet er sant.

(2) Når $k=4$, er utsagnet at

$$u_{n+4}=u_3\cdot u_{n+2}+u_2\cdot u_{n+1}.$$

Vi gjør følgende obsvervasjoner.

(i) Siden $u_2 = 1$ og $u_3 = 2$, er

$$u_3 \cdot u_{n+2} + u_2 \cdot u_{n+1} = 2u_{n+2} + u_{n+1}.$$

(ii) Fra definisjonen til sekvensen av Fibonaccitall har vi:

$$u_{n+4} = u_{n+3} + u_{n+2}$$

og

$$u_{n+3} = u_{n+2} + u_{n+1}.$$

Derfor er

$$\begin{aligned} u_{n+4} &= (u_{n+2} + u_{n+1}) + u_{n+2} \\ &= 2u_{n+2} + u_{n+1}. \end{aligned}$$

Fra (i) – (ii) deduserer vi at utsagnet er sant.

Anta nå at proposisjonen har blitt bevist når $k = m$ og når $k = m - 1$, hvor m er et gitt heltall større enn eller likt 4. Således har det blitt bevist at

$$u_{n+m} = u_{m-1} \cdot u_{n+2} + u_{m-2} \cdot u_{n+1}$$

og at

$$u_{n+m-1} = u_{m-2} \cdot u_{n+2} + u_{m-3} \cdot u_{n+1}.$$

Vi gjør følgende observasjoner.

(1) Ut ifra definisjonen til sekvensen av Fibonaccitall er

$$u_{n+m+1} = u_{n+m} + u_{n+m-1}.$$

(2) Fra antakelsen at

$$u_{n+m} = u_{m-1} \cdot u_{n+2} + u_{m-2} \cdot u_{n+1}$$

og antakelsen at

$$u_{n+m-1} = u_{m-2} \cdot u_{n+2} + u_{m-3} \cdot u_{n+1}$$

følger det at

$$\begin{aligned} &u_{n+m} + u_{n+m-1} \\ &= (u_{m-1} \cdot u_{n+2} + u_{m-2} \cdot u_{n+1}) + (u_{m-2} \cdot u_{n+2} + u_{m-3} \cdot u_{n+1}) \\ &= (u_{m-1} + u_{m-2})\, u_{n+2} + (u_{m-2} + u_{m-3})\, u_{n+1} \end{aligned}$$

(3) Ut ifra definisjonen til sekvensen av Fibonaccitall har vi:

$$u_m = u_{m-1} + u_{m-2}$$

og

$$u_{m-1} = u_{m-2} + u_{m-3}.$$

Fra (1) – (3) deduserer vi at

$$u_{n+m+1} = u_m \cdot u_{n+2} + u_{m-1} \cdot u_{n+1}.$$

Dermed er proposisjonen sann når k er det naturlige tallet $m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann når k er et hvilket som helst naturlig tall større enn eller likt 3.

□

Eksempel 1.14.2. Når $n = 2$ og $k = 3$, fastslår Proposisjon 1.14.1 at

$$u_5 = u_2u_4 + u_1u_3,$$

altså at

$$5 = 1 \cdot 3 + 1 \cdot 2.$$

Eksempel 1.14.3. Når $n = 2$ og $k = 4$, fastslår Proposisjon 1.14.1 at

$$u_6 = u_3u_4 + u_2u_3,$$

altså at

$$8 = 2 \cdot 3 + 1 \cdot 2.$$

Eksempel 1.14.4. Når $n = 2$ og $k = 7$, fastslår Proposisjon 1.14.1 at

$$u_9 = u_6u_4 + u_5u_3,$$

altså at

$$34 = 28 \cdot 3 + 5 \cdot 2.$$

Eksempel 1.14.5. Når $n = 3$ og $k = 3$, fastslår Proposisjon 1.14.1 at

$$u_6 = u_2u_5 + u_1u_4,$$

altså at

$$8 = 1 \cdot 5 + 1 \cdot 3.$$

Eksempel 1.14.6. Når $n = 3$ og $k = 4$, fastslår Proposisjon 1.14.1 at

$$u_7 = u_3u_5 + u_2u_4,$$

altså at

$$13 = 2 \cdot 5 + 1 \cdot 3.$$

Eksempel 1.14.7. Når $n = 3$ og $k = 7$, fastslår Proposisjon 1.14.1 at

$$u_{10} = u_6u_5 + u_5u_4,$$

altså at

$$55 = 8 \cdot 5 + 5 \cdot 3.$$

Eksempel 1.14.8. Når $n = 6$ og $k = 5$, fastslår Proposisjon 1.14.1 at

$$u_{11} = u_4u_8 + u_3u_7,$$

altså at

$$89 = 3 \cdot 21 + 2 \cdot 13.$$

Merknad 1.14.9. I beviset for Proposisjon 1.14.1 benyttet vi varianten av induksjon hvor $c = 1$ og $r = 3$. Vi kan se på beviset for følgende måte. Først velger vi et heltall n slik at $n \geq 0$: la for eksempel n være 7. Da blir utsagnet:

$$u_{7+k} = u_{k-1} \cdot u_9 + u_{k-2} \cdot u_8.$$

Så beviser vi at dette er sant, ved å erstatte n med 7 i beviset for Proposisjon 1.14.1.

Vi begynner med å sjekke om utsagnet er sant for alle de naturlige tallene r, $r + 1$, $\ldots$, $r + c$, det vil si når $k = 3$ og når $k = 4$. Vi sjekker altså at

$$u_{10} = u_2 \cdot u_9 + u_1 \cdot u_8$$

og at

$$u_{11} = u_3u_9 + u_2u_8.$$

Anta nå at det har blitt bevist at utsagnet er sant når $k = m$ og når $k = m - 1$, hvor m er et gitt heltall større enn eller likt 4. Således har det blitt bevist at

$$u_{7+m} = u_{m-1} \cdot u_9 + u_{m-2} \cdot u_8$$

og at

$$u_{7+m-1} = u_{m-2} \cdot u_9 + u_{m-3} \cdot u_8.$$

Vi gjør følgende observasjoner.

(1) Ut ifra definisjonen til sekvensen av Fibonaccitall er

$$u_{7+m+1} = u_{7+m} + u_{6+m}.$$

(2) Fra antakelsen at

$$u_{7+m} = u_{m-1} \cdot u_9 + u_{m-2} \cdot u_8$$

og antakelsen at

$$u_{6+m} = u_{m-2} \cdot u_9 + u_{m-3} \cdot u_8$$

følger det at

$$\begin{aligned} &u_{7+m} + u_{6+m} \\ &= (u_{m-1} \cdot u_9 + u_{m-2} \cdot u_8) + (u_{m-2} \cdot u_9 + u_{m-3} \cdot u_8) \\ &= (u_{m-1} + u_{m-2})\, u_9 + (u_{m-2} + u_{m-3})\, u_8 \end{aligned}$$

(3) Ut ifra definisjonen til sekvensen av Fibonaccitall har vi:

$$u_m = u_{m-1} + u_{m-2}$$

og

$$u_{m-1} = u_{m-2} + u_{m-3}.$$

Fra (1) – (3) deduserer vi at

$$u_{8+m} = u_m \cdot u_9 + u_{m-1} \cdot u_8.$$

Dermed er proposisjonen sann når k er det naturlige tallet $m + 1$.

Ved induksjon konkluderer vi at utsagnet er sant når k er et hvilket som helst naturlig tall større enn eller likt 3.

Merknad 1.14.10. Siden ligningen

$$u_n = u_{n-1} + u_{n-2}$$

som definerer det n-te Fibonaccitallene inneholder *to* av Fibonaccitallene som allerede har blitt definert, benytter vi typisk varianten av induksjon hvor $c = 1$ for å bevise påstander om Fibonaccitallene:

(1) For å gjennomføre Steg (1) i Terminologi 1.13.2, sjekker vi om påstanden er sann for *to* heltall.

(2) For å gjennomføre Steg (2) i Terminologi 1.13.2, antar vi at påstanden har blitt bevist for de *to* heltallene m og $m - 1$, hvor m er et gitt heltall.

Rekursjon og induksjon henger generelt sett sammen slik.

Proposisjon 1.14.11. La n være et naturlig tall. Da er $u_{5n+2} > 10^n$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. I dette tilfellet er utsagnet at $u_7 > 10$. Siden $u_7 = 13$ er dette sant.

Anta nå at proposisjonen har blitt bevist når n er et gitt naturlig tall m. Således har det blitt bevist at $u_{5m+2} > 10^m$. Vi gjør følgende observasjoner.

(1) Vi har:

$$u_{5(m+1)+2} = u_{5m+5+2} = u_{5m+7}.$$

(2) Ut ifra Proposisjon 1.14.1, ved å la n være $5m$, er

$$u_{5m+7} = u_6 u_{5m+2} + u_5 u_{5m+1}.$$

Siden $u_5 = 5$ og $u_6 = 8$, deduserer vi at

$$u_{5m+7} = 8u_{5m+2} + 5u_{5m+1}.$$

(3) Siden $u_{5m} < u_{5m+1}$, er

$$\begin{aligned} u_{5m} + u_{5m+1} &< u_{5m+1} + u_{5m+1} \\ &= 2u_{5m+1}. \end{aligned}$$

Derfor er

$$\begin{aligned} 2(u_{5m} + u_{5m+1}) &< 2 \cdot 2u_{5m+1} \\ &= 4u_{5m+1}. \end{aligned}$$

(4) Siden u_{5m+1}, som alle Fibonnacitallene, er større enn 0, er

$$4u_{5m+1} < 5u_{5m+1}.$$

(5) Fra (3) – (4), følger det at

$$2(u_{5m} + u_{5m+1}) < 5u_{5m+1}.$$

(6) Ut ifra definisjonen til sekvensen av Fibonaccitall, er

$$u_{5m} + u_{5m+1} = u_{5m+2}.$$

(7) Fra (5) – (6), følger det at

$$2u_{5m+2} < 5u_{5m+1}.$$

Derfor er

$$\begin{aligned} 8u_{5m+2} + 5u_{5m+1} &> 8u_{5m+2} + 2u_{5m+2} \\ &= 10u_{5m+2}. \end{aligned}$$

Fra (1), (2), og (7), følger det at

$$u_{5(m+1)+2} > 10u_{5m+2}.$$

Fra antakelsen at $u_{5m+2} > 10^m$, deduserer vi at

$$\begin{aligned} u_{5(m+1)+2} &> 10 \cdot 10^m \\ &= 10^{m+1}. \end{aligned}$$

Dermed er proposisjonen sann når n er det naturlige tallet $m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall. □

Eksempel 1.14.12. Når $n = 2$, fastslår Proposisjon 1.14.11 at $u_{12} > 10^2 = 100$. Faktisk er $u_{12} = 144$.

Eksempel 1.14.13. Når $n = 3$, fastslår Proposisjon 1.14.11 at $u_{17} > 10^3 = 1000$.

Eksempel 1.14.14. Når $n = 7$, fastslår Proposisjon 1.14.11 at $u_{37} > 10^7 = 10000000$.

O1 Oppgaver – induksjon og rekursjon

O1.1 Oppgaver i eksamens stil

Oppgave O1.1.1. La n være et naturlig tall slik at $n \geq 2$. Bevis at $2n > n + 1$.

Oppgave O1.1.2. La n være et naturlig tall. Bevis at

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Oppgave O1.1.3. La n være et naturlig tall. Bevis at

$$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Oppgave O1.1.4. La x og n være naturlige tall. Bevis at

$$(1 + x)^n \geq 1 + nx.$$

Oppgave O1.1.5. Bevis at begge utsagnene nedenfor er gale:

(1) For alle naturlige tall m og n er $(mn)! = m! \cdot n!$.

(2) For alle naturlige tall m og n er $(m + n)! = m! + n!$.

Oppgave O1.1.6. La n være et naturlig tall slik at $n \geq 4$. Bevis at $n! > n^2$. *Tips*: Benytt Proposisjon 1.5.14 i beviset.

Oppgave O1.1.7. La n, k, og l være heltall slik at $n \geq k \geq l \geq 0$. Bevis at

$$\binom{n}{k} \cdot \binom{k}{l} = \binom{n}{l} \cdot \binom{n-l}{k-l}.$$

Tips: Induksjon behøves ikke! På hver side av ligningen, erstatt binomnialkoeffisientene med deres definisjonene, og vis at begge sidene blir like.

Oppgave O1.1.8. La n være et naturlig tall.

(1) Bevis at

$$1^2 + 3^2 + 5^2 + \cdots + (2n - 1)^2 = \frac{n(2n-1)(2n+1)}{3}.$$

(2) Deduser at

$$1^2 + 3^2 + 5^2 + \cdots + (2n - 1)^2 = \binom{2n+1}{3}.$$

Oppgave O1.1.9. La n være et naturlig tall slik at $n \geq 2$. Bevis at

$$\sum_{i=2}^{n} \binom{i}{2} = \binom{n+1}{3}.$$

Tips: Benytt Proposisjon 1.9.18 i beviset.

Oppgave O1.1.10. La n være et naturlig tall. La u_{n+1} være det $(n+1)$-te Fibonaccitallet. Bevis at

$$u_1 + u_3 + \cdots + u_{2n-1} = u_{2n}.$$

Oppgave O1.1.11. La n være et naturlig tall. La u_k være det k-te Fibonnacitallet, hvor k er et hvilket som helst naturlig tall. Bevis at

$$\sum_{i=1}^{n} \binom{n}{i} u_i = u_{2n}.$$

Tips: Gjør følgende:

(1) La r være

$$\frac{1+\sqrt{5}}{2}$$

og la s være

$$\frac{1-\sqrt{5}}{2}.$$

Bevis at

$$\frac{1}{\sqrt{5}}\left(r^n - s^n\right) = \frac{r^n - s^n}{r-s}.$$

Fra Proposisjon 1.12.9, deduser at

$$u_n = \frac{r^n - s^n}{r-s}.$$

(2) Bevis at

$$(1+r)^n - (1+s)^n = \left(\sum_{i=0}^{n} \binom{n}{i} r^i\right) - \left(\sum_{i=0}^{n} \binom{n}{i} s^i\right).$$

Tips: Benytt formelen i Proposisjon 1.9.30 to ganger:

(i) Ved å la x være 1 og å la y være r.

(ii) Ved å la x være 1 og å la y være s.

(3) Deduser fra (1), (2) og Proposisjon 1.12.9 at

$$\frac{(1+r)^n - (1+s)^n}{r-s} = \sum_{i=1}^{n} \binom{n}{i} u_i.$$

(4) Fra Lemma 1.12.7 vet vi at $r^2 = r + 1$ og at $s^2 = s + 1$. Deduser at
$$r^{2n} - s^{2n} = (1 + r)^n - (1 + s)^n.$$

(5) Deduser fra (1) og (4) at
$$u_{2n} = \frac{(1 + r)^n - (1 + s)^n}{r - s}.$$

(6) Konkluder fra (3) og (5) at
$$\sum_{i=1}^{n} \binom{n}{i} u_i = u_{2n}.$$

Oppgave O1.1.12. Følgende definerer ved rekursjon *sekvensen av Lucastall*.

(1) Det første heltallet i sekvensen er 1.

(2) Det andre heltallet i sekvensen er 3.

(3) La m være et naturlig tall slik at $m \geq 2$. Anta at det i-te heltallet i sekvensen har blitt definert for alle de naturlige tallene i slik at $2 \leq i \leq m$. Betegn det m-te heltallet i sekvensen som v_m, og betegn det $(m - 1)$-te heltallet i sekvensen som v_{m-1}. Da definerer vi det $(m + 1)$-te heltallet i sekvensen til å være $v_{m-1} + v_m$.

Skriv de første ti heltallene i sekvensen.

Oppgave O1.1.13. La v_n betegne det n-te heltallet i sekvensen av Lucastall. Bevis at
$$v_1 + \cdots + v_n = v_{n+2} - 3.$$

Oppgave O1.1.14. La u_r betegne det r-te heltallet i sekvensen av Fibonaccitall. La v_r betegne det r-te heltallet i sekvensen av Lucastall.

(1) La n være et naturlig tall slik at $n \geq 3$. Bevis at
$$v_{n+2} + v_n = (v_{n+1} + v_{n-1}) + (v_n + v_{n-2}).$$
Tips: Induksjon behøves ikke!

(2) La n være et naturlig tall slik at $n \geq 2$. Bevis at
$$v_{n+1} + v_{n-1} = 5u_n.$$

Oppgave O1.1.15. La n være et naturlig tall slik at $n \geq 2$. La u_n være det n-te Fibonaccitallet. Bevis at u_n er lik
$$\binom{n-1}{0} + \binom{n-2}{1} + \cdots + \binom{\frac{n-1}{2}}{\frac{n-1}{2}}$$
dersom n er et oddetall, og er lik
$$\binom{n-1}{0} + \binom{n-2}{1} + \cdots + \binom{\frac{n}{2}}{\frac{n-2}{2}}$$
dersom n er et partall. *Tips*: Benytt en variant av induksjon, og benytt Proposisjon 1.9.18.

O1.2 Oppgaver for å hjelpe med å forstå kapittelet

Oppgave O1.2.1. Er følgende utsagn riktige eller gale ifølge Definisjon 1.1.1 og Definisjon 1.1.3?

(1) -3 er et naturlig tall.

(2) $\sqrt{9}$ er et heltall.

(3) $\frac{4}{3}$ er et heltall.

(4) $1 - 1$ er et naturlig tall.

(5) $(-3) \cdot (-4)$ er et naturlig tall.

Oppgave O1.2.2. Hva fastslår Proposisjon 1.4.5 når $n = 4$?

Oppgave O1.2.3. Fortsett med Merknad 1.4.11 ved å vise at Proposisjon 1.4.5 er sann når $n = 4$.

Oppgave O1.2.4. Hva fastslår Proposisjon 1.5.1 når $n = 4$?

Oppgave O1.2.5. Gjør det samme som i Merknad 1.4.11 for Proposisjon 1.5.1. Med andre ord, beskriv hvordan algoritmen i Merknad 1.4.3 ser ut for Proposisjon 1.5.1.

Oppgave O1.2.6. Hva fastslår Proposisjon 1.5.7 når $n = 4$?

Oppgave O1.2.7. Gjør det samme som i Merknad 1.4.11 for Proposisjon 1.5.7. Med andre ord, beskriv hvordan algoritmen i Merknad 1.4.3 ser ut for Proposisjon 1.5.7.

Oppgave O1.2.8. Hva fastslår Proposisjon 1.5.14 når $n = 5$?

Oppgave O1.2.9. Gjør det samme som i Merknad 1.4.11 for Proposisjon 1.5.14. Med andre ord, beskriv hvordan algoritmen i Bemarking 1.4.3 ser ut for Proposisjon 1.5.14.

Oppgave O1.2.10. Skriv følgende summene ved å bruke summetegnet.

(1) -9 -6 -3 + 0 + 3 + 6 + 9 + 12 + 15.

(2) $1 + 5 + 9 + 13 + \ldots + 53$.

Oppgave O1.2.11. Skriv summene

$$\sum_{i=3}^{9} 4i$$

og

$$\sum_{i=0}^{7} \left(3^i + i\right)$$

uten å bruke summetegnet.

Oppgave O1.2.12. Hva fastslår Proposisjon 1.7.1 når $n = 5$ og $k = 3$? Hva fastslår den når $n = 5$ og $k = 5$?

Oppgave O1.2.13. Skriv utsagnet i Proposisjon 1.7.1 når $k = 3$ uten å bruke summetegnet. Skriv så et bevis for dette utsagnet ved å erstatte k med 3 i beviset for Proposisjon 1.7.1, uten å bruke summetegnet. *Tips*: Se på Merknad 1.7.16.

Oppgave O1.2.14. Regn ut følgende tall.

(1) 5!

(2) 6!

Oppgave O1.2.15. Regn ut $\binom{7}{k}$ for alle heltallene k slik at $0 \leq k \leq 7$, uten å benytte Proposisjon 1.9.18.

Oppgave O1.2.16. Regn ut $\binom{7}{k}$ for alle heltallene k slik at $0 \leq k \leq 7$, uten å benytte Proposisjon 1.9.18.

Oppgave O1.2.17. Regn ut $\binom{8}{k}$ for alle heltall k slik at $0 \leq k \leq 7$, ved å benytte Proposisjon 1.9.18 og til Oppgave O1.2.16.

Oppgave O1.2.18. Gjør det samme som i Merknad 1.4.11 for Proposisjon 1.9.29. Med andre ord, beskriv hvordan algoritmen i Merknad 1.4.3 ser ut for Proposisjon 1.9.29.

Oppgave O1.2.19. Hva fastslår Proposisjon 1.9.30 når $n = 5$?

Oppgave O1.2.20. Skriv utsagnet i Proposisjon 1.9.30 når $n = 4$ uten å bruke summetegnet. Skriv så beviset for dette utsagnet uten å bruke summetegnet, ved å ertsatte m med 3 i beviset for Proposisjon 1.9.30. *Tips*: Se Merknad 1.9.36.

Oppgave O1.2.21. La n være et naturlig tall. Ved å la x være 1 og y være 1 i Proposisjon 1.9.30, bevis at

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$

Oppgave O1.2.22. La n være et naturlig tall. Følgende ligning kan også deduseres fra Proposisjon 1.9.30:

$$\binom{n}{0} - \binom{n}{1} + \cdots + (-1)^n \binom{n}{n} = 0.$$

Hvilke heltall bør vi la x og y være?

Oppgave O1.2.23. Hva er det 15-te Fibonaccitallet?

Oppgave O1.2.24. Hva fastslår Proposisjon 1.11.6 når $n = 5$?

Oppgave O1.2.25. Gjør det samme som i Merknad 1.4.11 for Proposisjon 1.11.6. Med andre ord, beskriv hvordan algoritmen i Bemarking 1.4.3 ser ut for Proposisjon 1.11.6.

Oppgave O1.2.26. Hva fastslår Proposisjon 1.11.12 når $n = 5$?

Oppgave O1.2.27. Gjør det samme som i Merknad 1.4.11 for Proposisjon 1.11.12. Med andre ord, beskriv hvordan algoritmen i Bemarking 1.4.3 ser ut for Proposisjon 1.11.12.

Oppgave O1.2.28. Hva fastslår Proposisjon 1.12.2 når $n = 6$?

Oppgave O1.2.29. Gjør det samme som i Merknad 1.4.11 for Proposisjon 1.12.2. Med andre ord, beskriv hvordan algoritmen i Bemarking 1.4.3 ser ut for Proposisjon 1.12.2.

Oppgave O1.2.30. Hva fastslår Proposisjon 1.12.9 når $n = 7$?

Oppgave O1.2.31. Hva fastslår Proposisjon 1.12.18 når $n = 7$?

Oppgave O1.2.32. Gi et alternativt bevis for Proposisjon 1.12.9 ved å benytte varianten av induksjon hvor $c = 1$ i Terminologi 1.13.2.

Oppgave O1.2.33. La v_n være det n-te heltallet i sekvensen av Lucastall. Bevis at

$$v_n = \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Tips: Benytt varianten av induksjon hvor $c = 1$ i Terminologi 1.13.2.

Oppgave O1.2.34. La u_n være det n-te Fibonaccitallet, og la v_n være det n-te heltallet i sekvensen av Lucastall. Bevis at

$$v_n^2 - 5u_n^2 = 4 \cdot (-1)^n,$$

ved å benytte Proposisjon 1.12.9 og Oppgave O1.2.33.

Oppgave O1.2.35. La x være et heltall. Hva fastslår Proposisjon 1.13.6 når $n = 7$? Hva fastslår den når $n = 7$ og $x = -2$?

Oppgave O1.2.36. Fortsett med Merknad 1.13.13 ved å vise at Proposisjon 1.4.5 er sann når $n = 4$.

Oppgave O1.2.37. La x være et heltall. Hva fastslår Proposisjon 1.14.1 når $n = 4$ og $k = 6$? Hva fastslår den når $n = 5$ og $k = 4$?

Oppgave O1.2.38. Skriv utsagnet i Proposisjon 1.14.1 når $n = 9$. Skriv så et bevis for dette utsagnet ved å erstatte k med 9 i beviset for Proposisjon 1.14.1. *Tips*: Se Merknad 1.14.9.

Oppgave O1.2.39. Gjør det samme som i Merknad 1.13.13 for Proposisjon 1.14.1. Med andre ord, beskriv hvordan algoritmen i Bemarking 1.13.4 ser ut for Proposisjon 1.14.1.

Oppgave O1.2.40. La n være et heltall slik at $n \geq 0$, la k være et naturlig tall slik at $k \geq 3$, og la l være et naturlig tall slik at $l \leq k - 2$. Da er

$$u_{n+k} = u_{k-l} \cdot u_{n+l+1} + u_{k-l-1} \cdot u_{n+l}.$$

Tips: Omarbeid beviset for Proposisjon 1.14.1. HUsk å sjekke om proposisjonen er sann når $k = 3$ og når $k = 4$ for alle de naturlige tallene l slik at $l \leq k - 2$. Det er ikke så mange!

Oppgave O1.2.41. Hva fastslår Proposisjon 1.14.11 når $n = 5$?

Oppgave O1.2.42. Gjør det samme som i Merknad 1.4.11 for Proposisjon 1.14.11. Med andre ord, beskriv hvordan algoritmen i Merknad 1.4.3 ser ut for Proposisjon 1.14.11.

Oppgave O1.2.43. Gi et eksempel på et naturlig tall n slik at $u_n > 1000000000000000$. Her er u_n det n-te Fibonaccitallet.

2 Delbarhet

2.1 Absoluttverdien

Definisjon 2.1.1. La n være et heltall. Da er *absoluttverdien til* n:

(1) n dersom $n \geq 0$;

(2) $-n$ dersom $n < 0$.

Merknad 2.1.2. Med andre ord får vi absoluttverdien til n ved å fjerne minustegnet hvis $n < 0$, og ved å gjøre ingenting hvis $n > 0$.

Notasjon 2.1.3. La n være et heltall. Vi betegner absoluttverdien til n som $|n|$.

Eksempel 2.1.4. Vi har: $|3| = 3$.

Eksempel 2.1.5. Vi har: $|-3| = 3$.

Eksempel 2.1.6. Vi har: $|0| = 0$.

Eksempel 2.1.7. Vi har: $|-7| = 7$.

Eksempel 2.1.8. Vi har: $|151| = 151$.

2.2 Divisjonsalgoritmen

Merknad 2.2.1. La l og n være naturlige tall. Fra barneskolen kjenner du til at vi alltid kan finne et naturlig tall k og et naturlig tall r slik at:

(1) $n = kl + r$,

(2) $0 \leq r < l$.

Det naturlige tallet k kalles *kvotient*, og det naturlige tallet r kalles *rest*.

Eksempel 2.2.2. La n være 5, og la l være 3. Da er $k = 1$ og $r = 2$, siden vi har:

(1) $5 = 1 \cdot 3 + 2$,

(2) $0 \leq 2 < 3$.

Eksempel 2.2.3. La n være 18, og la l være 5. Da er $k = 3$ og $r = 3$, siden vi har:

(1) $18 = 3 \cdot 5 + 3$,

(2) $0 \leq 3 < 5$.

Merknad 2.2.4. På barneskolen lærte du en metode for å finne k og r. Men hvordan vet vi at metoden alltid virker? Med andre ord, hvordan vet vi at vi alltid kan finne naturlige tall k og r som oppfyller kravene (1) og (2) i Merknad 2.2.1?

I denne delen av kapittelet skal vi *bevise* ved induskjon at det finnes, for alle naturlige tall n og l, naturlige tall k og r slik at (1) og (2) i Merknad 2.2.1 er sanne. Det følgende lemmaet er kjernen i beviset for Proposisjon 2.2.6.

Lemma 2.2.5. La n være et heltall slik at $n \geq 0$. La l være et naturlig tall. Anta at det finnes et heltall k og et heltall r slik at:

(1) $n = kl + r$,

(2) $0 \leq r < l$,

(3) $k \geq 0$.

Da finnes det et heltall k' og et heltall r' slik at:

(I) $n + 1 = k'l + r'$,

(II) $0 \leq r' < l$.

(III) $k' \geq 0$.

Bevis. Siden $0 \leq r < l$, er et av de følgende utsagnene sant:

(A) $r < l - 1$;

(B) $r = l - 1$.

Vi skal gjennomføre beviset i disse to tilfellene hver for seg.

Anta først at (A) er tilfellet. La da k' være k, og la r' være $r + 1$. Vi gjør følgende observasjoner.

(i) Fra (1) har vi:

$$n + 1 = (kl + r) + 1.$$

Derfor er:

$$\begin{aligned} n + 1 &= (kl + r) + 1 \\ &= kl + (r + 1) \\ &= k'l + r'. \end{aligned}$$

Dermed oppfyller k' og r' kravet (I).

(ii) Fra (2) har vi:

$$0 \leq r.$$

Derfor er

$$\begin{aligned} 0 &\leq r \\ &\leq r+1 \\ &= r'. \end{aligned}$$

Siden vi har antatt at (A) er sant, vet vi også at

$$r < l - 1.$$

Det følger at

$$r + 1 < l,$$

altså at

$$r' < l.$$

Dermed har vi bevist at

$$0 \leq r' < l.$$

Således oppfyller r' kravet (II).

(iii) Fra (3) har vi:

$$k \geq 0.$$

Siden $k' = k$, har vi altså:

$$k' \geq 0.$$

Dermed oppfyller k' kravet (III).

Fra (i) – (iii) konkluderer vi at lemmaet er sant i tilfellet (A).

Anta nå at (B) er tilfellet. La da k' være $k + 1$, og la r' være 0. Vi gjør følgende observasjoner.

(i) Fra (1) har vi:

$$n + 1 = (kl + r) + 1.$$

Siden vi har antatt at (B) er sant, er $r = l - 1$. Derfor er

$$\begin{aligned} n + 1 &= (kl + r) + 1 \\ &= \big(kl + (l - 1)\big) + 1 \\ &= kl + l - 1 + 1 \\ &= (k + 1)l + 0 \\ &= k'l + r'. \end{aligned}$$

Dermed oppfyller k' og r' kravet (I).

(ii) Siden l er et naturlig tall, er $0 < l$. Siden $r' = 0$, er derfor $r' < l$. I tillegg er $0 \leq 0$, altså $0 \leq r'$. Dermed er

$$0 \leq r' < l.$$

Således oppfyller r' kravet (II).

(iii) Fra (3) har vi:

$$k \geq 0.$$

Siden $k' = k + 1$, deduserer vi at

$$k' \geq 0.$$

Dermed oppfyller k' kravet (III).

Fra (i) – (iii) konkluderer vi at lemmaet er sant i tilfellet (B).

□

Proposisjon 2.2.6. La n være et heltall slik at $n \geq 0$. La l være et naturlig tall. Da finnes det et heltall k og et heltall r slik at:

(I) $n = kl + r$,

(II) $0 \leq r < l$,

(III) $k \geq 0$.

Bevis. Først sjekker vi at proposisjonen er sann når $n = 0$. I dette tilfellet er utsagnet at det finnes, for et hvilket som helst naturlig tall l, et heltall k og et heltall r slik at:

(1) $0 = kl + r$

(2) $0 \leq r < l$,

(3) $k \geq 0$.

La k være 0, og la r være 0. Vi gjør følgende observasjoner.

(i) Vi har:

$$\begin{aligned} kl + r &= 0 \cdot l + 0 \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

Dermed oppfyller k og r kravet (1).

(ii) Siden l er et naturlig tall, er $0 < l$. Siden $r = 0$, er derfor $r < l$. I tillegg er $0 \leq 0$, altså $0 \leq r$. Dermed er

$$0 \leq r < l.$$

Således oppfyller r kravet (2).

(iii) Vi har: $0 \geq 0$. Siden $k = 0$, er derfor $k \geq 0$. Dermed oppfyller k kravet (3).

Fra (i) – (iii) konkluderer vi at utsagnet er sant.

Anta nå at proposisjonen har blitt bevist når n er et gitt helltall m slik at $m \geq 0$. Således har det blitt bevist at det finnes, for et hvilket som helst naturlig tall l, et heltall k og et heltall r slik at:

(1) $m = kl + r$,

(2) $0 \leq r < l$,

(3) $k \geq 0$.

Da følger det fra Lemma 2.2.5 at det finnes et heltall k' og et heltall r' slik at:

(1) $m + 1 = k'l + r'$,

(2) $0 \leq r' < l$,

(3) $k' \geq 0$.

Dermed er proposisjonen sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall. □

Terminologi 2.2.7. I Merknad 1.4.3 så vi at induksjon gir en algoritme for å konstruere et bevis for en matematisk påstand. Således gir beviset for Proposisjon 2.2.6 en algoritme for å finne k og r. Denne algoritmen kalles noen ganger *divisjonsalgoritmen.*

Eksempel 2.2.8. La oss se hvordan divisjonsalgoritmen ser ut når $n = 3$ og $l = 2$.

(1) Vi begynner med å observere at:

$$0 = 0 \cdot 2 + 0.$$

(2) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$1 = 0 \cdot 2 + 1.$$

(3) Som i beviset for Lemma 2.2.5 i tilfellet (B), observerer vi at det følger at

$$2 = 1 \cdot 2 + 0.$$

(4) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$3 = 1 \cdot 2 + 1.$$

Dermed er $k = 1$ og $r = 1$.

Eksempel 2.2.9. La oss se hvordan divisjonsalgoritmen ser ut når $n = 6$ og $l = 4$.

(1) Vi begynner med å observere at:

$$0 = 0 \cdot 4 + 0.$$

(2) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$1 = 0 \cdot 4 + 1.$$

(3) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$2 = 0 \cdot 4 + 2.$$

(4) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$3 = 0 \cdot 4 + 3.$$

(5) Som i beviset for Lemma 2.2.5 i tilfellet (B), observerer vi at det følger at

$$4 = 1 \cdot 4 + 0.$$

(6) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$5 = 1 \cdot 4 + 1.$$

(7) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$6 = 1 \cdot 4 + 2.$$

Dermed er $k = 1$ og $r = 2$.

Eksempel 2.2.10. La oss se hvordan divisjonsalgoritmen ser ut når $n = 7$ og $l = 3$.

(1) Vi begynner med å observere at:

$$0 = 0 \cdot 3 + 0.$$

(2) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$1 = 0 \cdot 3 + 1.$$

(3) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$2 = 0 \cdot 3 + 2.$$

(4) Som i beviset for Lemma 2.2.5 i tilfellet (B), observerer vi at det følger at

$$3 = 1 \cdot 3 + 0.$$

(5) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$4 = 1 \cdot 3 + 1.$$

(6) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$5 = 1 \cdot 3 + 2.$$

(7) Som i beviset for Lemma 2.2.5 i tilfellet (B), observerer vi at det følger at

$$6 = 2 \cdot 3 + 0.$$

(8) Som i beviset for Lemma 2.2.5 i tilfellet (A), observerer vi at det følger at

$$7 = 2 \cdot 3 + 1.$$

Dermed er $k = 2$ og $r = 1$.

Korollar 2.2.11. La n være et heltall. La l være et heltall slik at $l \neq 0$. Da finnes det et heltall k og et heltall r slik at:

(I) $n = kl + r$,

(II) $0 \leq r < |l|$.

Bevis. Ett av følgende utsagn er sant:

(A) $l > 0$ og $n \geq 0$;

(B) $l < 0$ og $n \geq 0$;

(C) $l > 0$ og $n < 0$;

(D) $l < 0$ og $n < 0$;

Anta først at (A) er tilfellet. Da er l et naturlig tall. Det følger fra Proposisjon 2.2.6 at det finnes et heltall k' og et heltall r' slik at:

(i) $n = k'l + r'$,

(ii) $0 \leq r' < l$.

Siden $|l| = l$, deduserer vi at proposisjonen er sann i dette tilfellet, ved å la k være k' og å la r være r'.

Anta nå at (B) er tilfellet. Da er $-l$ et naturlig tall. Det følger fra Proposisjon 2.2.6 at det finnes et heltall k' og et heltall r' slik at:

(i) $n = k' \cdot (-l) + r'$,

(ii) $0 \leq r' < -l$.

Vi gjør følgende observasjoner.

(1) Det følger fra (i) at

$$n = (-k') \cdot l + r'.$$

(2) Vi har: $|l| = -l$. Derfor følger det fra (ii) at

$$0 \leq r' < |l|\,.$$

Dermed er proposisjonen sann i dette tilfellet også, ved å la k være $-k'$ og å la r være r'.

Anta nå at (C) er tilfellet. Da er $-n \geq 0$. Det følger fra Proposisjon 2.2.6 at det finnes et heltall k' og et heltall r' slik at:

(i) $-n = k' \cdot l + r'$,

(ii) $0 \leq r' < l$.

Ett av følgende utsagn er sant.

(a) $r' = 0$.

(b) $0 < r' < l$.

Anta først at $r' = 0$. Det følger fra (i) at

$$n = (-k') \cdot l.$$

Dermed er proposisjonen sann i dette tilfellet, ved å la k være k', og å la r være 0.

Anta nå at $0 < r' < l$. Vi gjør følgende observasjoner.

(1) Det følger fra (i) at

$$\begin{aligned} n &= -k' \cdot l - r' \\ &= -k' \cdot l - l + l - r' \\ &= (-k' - 1) \cdot l + (l - r'). \end{aligned}$$

(2) Siden $0 < r' < l$, er $0 < l - r' < l$.

Dermed er proposisjonen sann i dette tilfellet også, ved å la k være $-k' - 1$, og å la r være $l - r'$. Således har vi bevist at proposisjonen er sann i tilfellet (C).

Anta nå at (D) er tilfellet. Da er $-n \geq 0$. I tillegg er $-l$ et naturlig tall. Det følger fra Proposisjon 2.2.6 at det finnes et heltall k' og et heltall r' slik at:

(i) $-n = k' \cdot (-l) + r'$,

(ii) $0 \leq r' < -l$.

Ett av følgende utsagn er sant.

(a) $r' = 0$.

(b) $0 < r' < -l$.

Anta først at $r' = 0$. Det følger fra (i) at

$$n = k' \cdot l.$$

I tillegg har vi: $|l| = -l$. Dermed er proposisjonen sann i dette tilfellet, ved å la k være k', og å la r være 0.

Anta nå at $0 < r' < -l$. Vi gjør følgende observasjoner.

(1) Det følger fra (i) at

$$\begin{aligned} n &= k' \cdot l - r' \\ &= k' \cdot l + l - l - r' \\ &= (k' + 1) \cdot l + (-l - r'). \end{aligned}$$

(2) Siden $0 < r' < -l$, er $0 < -l - r' < -l$.

(3) Vi har: $|l| = -l$. Derfor følger det fra (2) at

$$0 < -l - r' < |l|.$$

Fra (1) og (3) konkluderer vi at proposisjonen er sann i dette tilfellet også, ved å la k være $k' + 1$, og å la r være $-l - r'$. Således har vi bevist at proposisjonen er sann i tilfellet (D).

□

Eksempel 2.2.12. La $n = -5$, og la l være 2. For å få heltall k og r slik at

$$-5 = k \cdot 2 + r$$

og $0 \leq r < 2$, fastslår beviset for Korollar 2.2.11 at vi kan gjøre følgende.

(1) Benytt divisjonsalgoritmen i tilfellet $n = 5$ og $l = 2$. Vi hopper over detaljene. Resultatet er:

$$5 = 2 \cdot 2 + 1.$$

(2) Observer at det følger fra (1) at

$$\begin{aligned} -5 &= -2 \cdot 2 - 1 \\ &= -2 \cdot 2 - 2 + 2 - 1 \\ &= (-2 - 1) \cdot 2 + (2 - 1) \\ &= (-3) \cdot 2 + 1. \end{aligned}$$

Dermed er

$$-5 = (-3) \cdot 2 + 1,$$

og $0 \leq 1 < 2$. Således er $k = -3$ og $r = 1$.

Eksempel 2.2.13. La $n = 8$, og la l være -3. For å få heltall k og r slik at

$$8 = k \cdot (-3) + r$$

og $0 \leq r < 3$, fastslår beviset for Korollar 2.2.11 at vi kan gjøre følgende.

(1) Benytt divisjonsalgoritmen i tilfellet $n = 8$ og $l = 3$. Vi hopper over detaljene. Resultatet er:

$$8 = 2 \cdot 3 + 2.$$

(2) Observer at det følger fra (1) at

$$8 = (-2) \cdot (-3) + 2.$$

I tillegg er $0 \leq 2 < 3$. Således er $k = -2$ og $r = 2$.

Eksempel 2.2.14. La $n = -7$, og la l være -4. For å få heltall k og r slik at

$$-7 = k \cdot (-4) + r$$

og $0 \leq r < 4$, fastslår beviset for Korollar 2.2.11 at vi kan gjøre følgende.

(1) Benytt divisjonsalgoritmen i tilfellet $n = 7$ og $l = 4$. Vi hopper over detaljene. Resultatet er:

$$7 = 1 \cdot 4 + 3.$$

(2) Observer at det følger fra (1) at

$$\begin{aligned} -7 &= 1 \cdot (-4) - 3 \\ &= 1 \cdot (-4) + (-4) - (-4) - 3 \\ &= (1 + 1) \cdot (-4) + (4 - 3) \\ &= 2 \cdot (-4) + 1. \end{aligned}$$

Dermed er

$$-7 = 2 \cdot (-4) + 1,$$

og $0 \leq 1 < 4$. Således er $k = 2$ og $r = 1$.

Proposisjon 2.2.15. La n være et heltall. La l være et naturlig tall. La k og r være heltall slik at:

(I) $n = kl + r$,

(II) $0 \leq r < l$.

La k' og r' også være heltall slik at:

(III) $n = k'l + r'$,

(IV) $0 \leq r' < l$.

Da er $k = k'$ og $r = r'$.

Bevis. Anta først at $k \geq k'$. Vi gjør følgende observasjoner.

(1) Fra (I) og (III) har vi:

$$\begin{aligned} r' - r &= (n - k'l) - (n - kl) \\ &= n - n - k'l + kl \\ &= kl - k'l \\ &= (k - k')l. \end{aligned}$$

(2) Fra (II) har vi: $0 \leq r$. Derfor er $-r \leq 0$. Det følger at $r' - r \leq r'$.

(3) Fra (IV) har vi: $r' < l$.

(4) Det følger fra (2) og (3) at

$$\begin{aligned} r' - r &\leq r' \\ &< l. \end{aligned}$$

Dermed er $r' - r < l$.

(5) Fra (1) og (4) har vi:

$$\begin{aligned} (k - k')l &= r' - r \\ &< l. \end{aligned}$$

Dermed er $(k - k')l < l$. Derfor er $k - k' < 1$.

(6) Siden $k \geq k'$, er $k - k' \geq 0$.

(7) Siden k og k' er heltall, er $k - k'$ et heltall.

(8) Fra (5) – (7) har vi: $k - k'$ er et heltall og

$$0 \leq k - k' < 1.$$

Derfor er $k - k' = 0$. Vi deduserer at $k = k'$.

(9) Det følger fra (1) og (8) at

$$\begin{aligned} r' - r &= (k - k')l \\ &= 0 \cdot l \\ &= 0. \end{aligned}$$

Vi deduserer at $r = r'$.

Anta nå at $k < k'$, altså at $k' \geq k$. Da gjennomfører vi akkurat det samme argumentet ved å bytte om k og k' og å bytte om r og r'.

□

Merknad 2.2.16. La k og r være de heltallene vi får ved å benytte divisjonsalgoritmen. Proposisjon 2.2.15 fastslår at k og r er de *entydige* heltallene, det vil si de *eneste* heltallene, som oppfyller kravene (I) – (II) i Proposisjon 2.2.6.

Merknad 2.2.17. I praksis *må* vi ikke benytte divisjonsalgoritmen for å finne k og r. Faktisk kommer vi fortere til k og r ved å benytte metoden du lærte på barneskolen! Vi kan også godt prøve å gjette k og r, og sjekke om gjetningen er riktig. Proposisjon 2.2.15 fastslår at uansett hvordan vi kommer fram til k og r, får vi de samme heltallene som ved å benytte divisjonsalgoritmen.

Dette er et avgjørende poeng. Proposisjon 2.2.6 sier noe om *eksistensen* av heltallene k og r, mens Proposisjon 2.2.15 sier noe om *entydigheten* av k og r. Den beste måten å bevise teoretisk at en matematisk påstand er sann er ikke nødvendigvis den beste å gjennomføre i praksis. Den beste situasjonen er at vi har, som her, en proposisjon som garanterer at alle metoder er like verdige.

Eksempel 2.2.18. La n være 64, og la l være 17. Siden

$$64 = 3 \cdot 17 + 13,$$

fastslår Proposisjon 2.2.15 at vi får $k = 3$ og $r = 13$ ved å bruke divisjonsalgoritmen som i Eksempel 2.2.8 – Eksempel 2.2.10.

Eksempel 2.2.19. La n være 127, og la l være 23. Siden

$$127 = 5 \cdot 23 + 12,$$

fastslår Proposisjon 2.2.15 at vi får $k = 5$ og $r = 12$ ved å bruke divisjonsalgoritmen som i Eksempel 2.2.8 – Eksempel 2.2.10.

Korollar 2.2.20. La n være et heltall. La l være et heltall slik at $l \neq 0$. La k og r være heltall slik at:

(I) $n = kl + r$,

(II) $0 \leq r < |l|$,

La k' og r' også være heltall slik at:

(III) $n = k'l + r'$,

(IV) $0 \leq r' < |l|$.

Da er $k = k'$ og $r = r'$.

Bevis. Ett av følgende utsagn er sant:

(1) $l > 0$;

(2) $l < 0$.

Anta først at $l > 0$. Da er l et naturlig tall, og $|l| = l$. Derfor følger det fra Proposisjon 2.2.15 at $k = k'$ og $r = r'$.

Anta nå at $l < 0$. Da er $-l$ et naturlig tall, og $|l| = -l$. Derfor følger det fra Proposisjon 2.2.15 for heltallet n og det naturlige tallet $-l$ at $k = k'$ og $r = r'$.

□

Merknad 2.2.21. Korollar 2.2.20 fastslår at uansett hvordan vi kommer fram til k og r, får vi de samme heltallene som ved å benytte tilnærmingsmetoden i Eksempel 2.2.12 – 2.2.14. Sammenlign med Merknad 2.2.17.

Eksempel 2.2.22. La n være -33, og la l være 12. Siden

$$-33 = -3 \cdot 12 + 3,$$

fastslår Korollar 2.2.20 at vi får $k = -33$ og $r = 3$ ved å bruke tilsnærmingsmetoden i Eksempel 2.2.12 – 2.2.14.

Eksempel 2.2.23. La n være 25, og la l være -7. Siden

$$25 = -3 \cdot -7 + 4,$$

fastslår Korollar 2.2.20 at vi får $k = -3$ og $r = 4$ ved å bruke tilsnærmingsmetoden i Eksempel 2.2.12 – 2.2.14.

Eksempel 2.2.24. La n være -156, og la l være -38. Siden

$$-156 = 5 \cdot -38 + 34,$$

fastslår Korollar 2.2.20 at vi får $k = 5$ og $r = 34$ ved å bruke tilsnærmingsmetoden i Eksempel 2.2.12 – 2.2.14.

Proposisjon 2.2.25. La m og n være heltall. La l være et heltall slik at $l \neq 0$. Anta at $lm = ln$. Da er $m = n$.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $lm = ln$, er

$$0 = lm - ln,$$

altså

$$0 = (m - n) \cdot l$$

(2) Vi har:

$$0 = 0 \cdot l.$$

Fra (1), (2), og Korollar 2.2.20 følger det at

$$m - n = 0,$$

altså at $m = n$.

□

Merknad 2.2.26. Vi er vant til å kunne fjerne l fra begge sider av ligningen

$$lm = ln.$$

Proposisjon 2.2.25 fastslår formelt at dette er en gyldig algebraisk manipulasjon.

Er det ikke nok å si: ≪vi deler begge sider av ligningen med l≫? Jo, men hva mener vi egentlig med dette? Poenget med Proposisjon 2.2.25 er at Korollar 2.2.20 gir oss muligheten til formelt å gjennomføre argumentene vi hadde kommet fram til om vi funderte på dette spørsmålet.

2.3 Partall og oddetall

Terminologi 2.3.1. Ved å la l være 2 i Korollar 2.2.11, får vi at, for et hvilket som helst heltall n, det finnes et heltall k slik at enten $n = 2k$ eller $n = 2k + 1$.

(1) Dersom $n = 2k$, sier vi at n er et *partall*.

(2) Dersom $n = 2k + 1$, sier vi at n er et *oddetall*.

Merknad 2.3.2. Det følger fra Proposisjon 2.2.15 at et heltall ikke kan være både et partall og et oddetall!

Eksempel 2.3.3. Siden $57 = 2 \cdot 28 + 1$, er 57 et oddetall.

Eksempel 2.3.4. Siden $26 = 2 \cdot 13$, er 26 et partall.

Eksempel 2.3.5. Siden $-3 = 2 \cdot (-2) + 1$, er -3 et oddetall.

2.4 Eksempler på bevis som benytter divisjonsalgoritmen

Merknad 2.4.1. La n være et heltall, og la l være heltall slik at $l \neq 0$. Korollar 2.2.11 sier at det finnes et heltall k slik at n er lik et av de følgende heltallene: kl, $kl+1$, $kl+2$, $\ldots$, $kl+|l|-1$. Når l er for eksempel 5, fastslår korollaret at, for alle heltall n, det finnes et heltall k slik at n er lik et av de følgende heltallene: $5k$, $5k+1$, $5k+2$, $5k+3$, $5k+4$.

For å bevise en matematisk påstand om heltall, kan vi derfor:

(1) velge et heltall l;

(2) sjekke om påstanden er sann, for alle heltall k, i hvert av de følgende tilfellene: $n = kl$, $n = kl+1$, $n = kl+2$, $\ldots$, $n = kl+|l|-1$.

Vi skal nå se på noen eksempler hvor denne tilnærmingsmetoden benyttes.

Proposisjon 2.4.2. La n være et heltall. Da finnes det et heltall m slik at enten $n^2 = 4m$ eller $n^2 = 4m+1$.

Bevis. Ved å la l være 2 i Korollar 2.2.11, får vi at det finnes et heltall k slik at ett av følgende utsagn er sant:

(1) $n = 2k$,

(2) $n = 2k+1$.

Anta først at (1) er sant. La m være k^2. Da er

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 4k^2 \\ &= 4m. \end{aligned}$$

Dermed er proposisjonen sann i dette tilfellet.

Anta nå at (2) er sant. La m være k^2+k. Da er

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2+4k+1 \\ &= 4(k^2+k)+1 \\ &= 4m+1. \end{aligned}$$

Dermed er proposisjonen sann i dette tilfellet også.

□

Eksempel 2.4.3. Når $n = 3$, fastslår Proposisjon 2.4.2 at det finnes et heltall m slik at enten $3^2 = 4m$ eller $3^2 = 4m+1$, altså slik at enten $9 = 4m$ eller $9 = 4m+1$. Det er nemlig sant at $9 = 4 \cdot 2 + 1$.

Eksempel 2.4.4. Når $n = 6$, fastslår Proposisjon 2.4.2 at det finnes et heltall m slik at enten $6^2 = 4m$ eller $6^2 = 4m + 1$, altså slik at enten $36 = 4m$ eller $36 = 4m + 1$. Det er nemlig sant at $36 = 4 \cdot 9$.

Eksempel 2.4.5. Når $n = 57$, fastslår Proposisjon 2.4.2 at det finnes et heltall m slik at enten $57^2 = 4m$ eller $57^2 = 4m+1$, altså slik at enten $3249 = 4m$ eller $3249 = 4m+1$. Det er nemlig sant at $3249 = 4 \cdot 812 + 1$.

Eksempel 2.4.6. Når $n = -6$, faststlår Proposisjon 2.4.2 at det finnes et heltall m slik at enten $(-6)^2 = 4m$ eller $(-6)^2 = 4m+1$, altså slik at enten $36 = 4m$ eller $36 = 4m+1$. Det er nemlig sant at $36 = 4 \cdot 9$.

Eksempel 2.4.7. Når $n = -7$, faststlår Proposisjon 2.4.2 at det finnes et heltall m slik at enten $(-7)^2 = 4m$ eller $(-7)^2 = 4m+1$, altså slik at enten $49 = 4m$ eller $49 = 4m+1$. Det er nemlig sant at $49 = 4 \cdot 12 + 1$.

Merknad 2.4.8. For å oppsummere beviset for Proposisjon 2.4.2, delte vi det opp i to tilfeller:

(1) hvor n er et partall;

(2) hvor n er et oddetall.

Vi beviste at Proposisjon 2.4.2 er sann i disse to tilfellene hver for seg.

Proposisjon 2.4.9. La n være et oddetall. Da finnes det et heltall m slik at $n^2 = 8m+1$.

Bevis. Ved å la l være 4 i Korollar 2.2.11, får vi at det finnes et heltall k slik at ett av følgende utsagn er sant:

(1) $n = 4k$,

(2) $n = 4k + 1$,

(3) $n = 4k + 2$,

(4) $n = 4k + 3$.

Siden n er et oddetall, må faktisk enten (2) eller (4) være sant.

Anta først at (2) er sant. La m være $2k^2 + k$. Da er

$$\begin{aligned} n^2 &= (4k + 1)^2 \\ &= 16k^2 + 8k + 1 \\ &= 8\left(2k^2 + k\right) + 1 \\ &= 8m + 1. \end{aligned}$$

Dermed er proposisjonen sann i dette tilfellet.

Anta nå at (4) er sant. La m være $2k^2 + 3k + 1$. Da er

$$\begin{aligned} n^2 &= (4k+3)^2 \\ &= 16k^2 + 24k + 9 \\ &= \left(16k^2 + 24k + 8\right) + 1 \\ &= 8\left(2k^2 + 3k + 1\right) + 1 \\ &= 8m + 1. \end{aligned}$$

Dermed er proposisjonen sann i dette tilfellet også.

□

Eksempel 2.4.10. Når $n = 5$, fastslår Proposisjon 2.4.9 at det finnes et heltall m slik at $5^2 = 8m + 1$, altså slik at $25 = 8m + 1$. Det er nemlig sant at $25 = 8 \cdot 3 + 1$.

Eksempel 2.4.11. Når $n = 9$, fastslår Proposisjon 2.4.9 at det finnes et heltall m slik at $9^2 = 8m + 1$, altså slik at $81 = 8m + 1$. Det er nemlig sant at $81 = 8 \cdot 10 + 1$.

Eksempel 2.4.12. Når $n = 57$, fastslår Proposisjon 2.4.9 at det finnes et heltall m slik at $57^2 = 8m + 1$, altså slik at $3249 = 8m + 1$. Det er nemlig sant at $3249 = 8 \cdot 406 + 1$.

Eksempel 2.4.13. Når $n = -7$, fastslår Proposisjon 2.4.9 at det finnes et heltall m slik at $(-7)^2 = 8m + 1$, altså slik at $49 = 8m + 1$. Det er nemlig sant at $49 = 8 \cdot 6 + 1$.

Eksempel 2.4.14. Når $n = -11$, fastslår Proposisjon 2.4.9 at det finnes et heltall m slik at $(-11)^2 = 8m+1$, altså slik at enten $121 = 8m+1$. Det er nemlig sant at $121 = 8 \cdot 15+1$.

Merknad 2.4.15. Utsagnet i Proposisjon 2.4.9 er gal når n er et partall, siden n^2 er et partall om n er et partall, men $8m + 1$ er et oddetall for alle heltall m. Et riktig utsagn er at det finnes et heltall m slik at enten $n^2 = 8m$ eller $n^2 = 8m + 4$ når n er et partall.

Proposisjon 2.4.16. La n være et heltall. Da finnes det et heltall m slik at ett av følgende utsagn er sant:

(1) $n^3 = 9m$

(2) $n^3 = 9m + 1$

(3) $n^3 = 9m + 8$.

Bevis. Ved å la l være 3 i Korollar 2.2.11, får vi at det finnes et heltall q slik at ett av følgende utsagn er sant:

(1) $n = 3k$,

(2) $n = 3k + 1$,

(3) $n = 3k + 2$.

Anta først at (1) er sant. La m være $3k^3$. Da er

$$\begin{aligned} n^3 &= (3k)^3 \\ &= 27k^3 \\ &= 9 \cdot (3k^3) \\ &= 9m. \end{aligned}$$

Dermed er proposisjonen sann i dette tilfellet.

Anta nå at (2) er sant. La m være $3k^3 + 3k^2 + k$. Ut ifra Proposisjon 1.9.30 er

$$\begin{aligned} (3k+1)^3 &= \binom{3}{0} \cdot (3k)^3 \cdot 1^0 + \binom{3}{1} \cdot (3k)^2 \cdot 1^1 + \binom{3}{2} \cdot (3k)^1 \cdot 1^2 + \binom{3}{3} \cdot (3k)^0 \cdot 1^3 \\ &= (3k)^3 + 3 \cdot (3k)^2 + 3 \cdot (3k) + 1 \\ &= 3^3 \cdot k^3 + 3^3 \cdot k^2 + 3^2 \cdot k + 1. \end{aligned}$$

Derfor er

$$\begin{aligned} n^3 &= (3k+1)^3 \\ &= 3^3 \cdot k^3 + 3^3 \cdot k^2 + 3^2 \cdot k + 1 \\ &= (3^2) \cdot \left(3k^3 + 3k^2 + k\right) + 1 \\ &= 9m + 1. \end{aligned}$$

Dermed er proposisjonen sann i dette tilfellet.

Anta nå at (3) er sant. La m være $3k^3 + 6k^2 + 4k$. Ut ifra Proposisjon 1.9.30 er

$$\begin{aligned} (3k+2)^3 &= \binom{3}{0} \cdot (3k)^3 \cdot 2^0 + \binom{3}{1} \cdot (3k)^2 \cdot 2^1 + \binom{3}{2} \cdot (3k)^1 \cdot 2^2 + \binom{3}{3} \cdot (3k)^0 \cdot 2^3 \\ &= (3k)^3 + 3 \cdot (3k)^2 \cdot 2 + 3 \cdot (3k) \cdot 2^2 + 2^3 \\ &= 3^3 \cdot k^3 + 3^3 \cdot 2 \cdot k^2 + 3^2 \cdot 4 \cdot k + 8. \end{aligned}$$

Derfor er

$$\begin{aligned} n^3 &= (3k+2)^3 \\ &= 3^3 \cdot k^3 + 3^3 \cdot 2 \cdot k^2 + 3^2 \cdot 4 \cdot k + 8 \\ &= (3^2) \cdot \left(3k^3 + 3 \cdot 2 \cdot k^2 + 4k\right) + 8 \\ &= 9\left(3k^3 + 6k^2 + 4k\right) + 8 \\ &= 9m + 8. \end{aligned}$$

Dermed er proposisjonen sann i dette tilfellet også.

□

Eksempel 2.4.17. Når $n = 4$, fastslår Proposisjon 2.4.16 at det finnes et heltall m slik at ett av følgende utsagn er sant:

(1) $4^3 = 9m$, altså $64 = 9m$;

(2) $4^3 = 9m + 1$, altså $64 = 9m + 1$;

(3) $4^3 = 9m + 8$, altså $64 = 9m + 8$;

Det er nemlig sant at $84 = 9 \cdot 7 + 1$.

Eksempel 2.4.18. Når $n = 11$, fastslår Proposisjon 2.4.16 at det finnes et heltall m slik at ett av følgende utsagn er sant:

(1) $11^3 = 9m$, altså $1331 = 9m$;

(2) $11^3 = 9m + 1$, altså $1331 = 9m + 1$;

(3) $11^3 = 9m + 8$, altså $1331 = 9m + 8$.

Det er nemlig sant at $1331 = 9 \cdot 147 + 8$.

Eksempel 2.4.19. Når $n = 57$, fastslår Proposisjon 2.4.16 at det finnes et heltall m slik at ett av følgende utsagn er sant:

(1) $57^3 = 9m$, altså $185193 = 9m$;

(2) $57^3 = 9m + 1$, altså $185193 = 9m + 1$;

(3) $57^3 = 9m + 8$, altså $185193 = 9m + 8$.

Det er nemlig sant at $185193 = 9 \cdot 20557$.

Eksempel 2.4.20. Når $n = -7$, fastslår Proposisjon 2.4.16 at det finnes et heltall m slik at ett av følgende utsagn er sant:

(1) $(-7)^3 = 9m$, altså $-343 = 9m$;

(2) $(-7)^3 = 9m + 1$, altså $-343 = 9m + 1$;

(3) $(-7)^3 = 9m + 8$, altså $-343 = 9m + 8$;

Det er nemlig sant at $-343 = 9 \cdot (-39) + 8$.

Eksempel 2.4.21. Når $n = -8$, fastslår Proposisjon 2.4.16 at det finnes et heltall m slik at ett av følgende utsagn er sant:

(1) $(-8)^3 = 9m$, altså $-512 = 9m$;

(2) $(-8)^3 = 9m + 1$, altså $-512 = 9m + 1$;

(3) $(-8)^3 = 9m + 8$, altså $-512 = 9m + 8$.

Det er nemlig sant at $-512 = 9 \cdot (-57) + 1$.

Eksempel 2.4.22. Når $n = -12$, fastslår Proposisjon 2.4.16 at det finnes et heltall m slik at ett av følgende utsagn er sant:

(1) $(-12)^3 = 9m$, altså $-1728 = 9m$;

(2) $(-12)^3 = 9m + 1$, altså $-1728 = 9m + 1$;

(3) $(-12)^3 = 9m + 8$, altså $-1728 = 9m + 8$.

Det er nemlig sant at $-1728 = 9 \cdot (-192)$.

2.5 Grunnleggende proposisjoner om delbarhet

Definisjon 2.5.1. La l og n være heltall. Da er n *delelig med* l dersom det finnes et heltall k slik at $n = kl$.

Notasjon 2.5.2. La l og n være heltall. Dersom n er delelig med l, skriver vi $l \mid n$.

Terminologi 2.5.3. La l og n være heltall. Dersom n er delelig med l, sier vi at l er en *divisor* til n.

Eksempel 2.5.4. Siden $6 = 3 \cdot 2$, er 6 delelig med 2. Derfor skriver vi: $2 \mid 6$.

Eksempel 2.5.5. Siden $16 = 4 \cdot 4$, er 16 delelig med 4. Derfor skriver vi: $4 \mid 16$.

Eksempel 2.5.6. Siden $-15 = (-5) \cdot 3$, er -15 delelig med 3. Derfor skriver vi: $3 \mid -15$.

Eksempel 2.5.7. La n være et hvilket som helst naturlig tall. Siden $n = n \cdot 1$, er n delelig med 1. Derfor skriver vi: $1 \mid n$.

Merknad 2.5.8. La l og n være heltall. Fra Korollar 2.2.11 vet vi at det alltid er et heltall k og et heltall r slik at:

(I) $n = kl + r$,

(II) $0 \leq r < |l|$.

Anta at n er delelig med l, altså at det finnes et heltall k' slik at $n = k'l$. Da følger det fra Proposisjon 2.2.15 at $k = k'$ og at $r = 0$.

Hvis på en annen side $r > 0$, følger det fra Proposisjon 2.2.15 at n ikke er delelig med l.

Proposisjon 2.5.9. La l og n være heltall. Anta at $l \mid n$. Da er $-l \mid n$.

Bevis. Siden $l \mid n$, finnes det et heltall k slik at $n = kl$. Da er $n = (-k) \cdot (-l)$. Siden k er et heltall, er $-k$ et heltall. Vi konkluderer at $-l \mid n$. □

Eksempel 2.5.10. Siden $6 = 2 \cdot 3$, er $3 \mid 6$. Derfor er $-3 \mid 6$. Vi har: $6 = (-2) \cdot (-3)$.

Eksempel 2.5.11. Siden $-14 = 2 \cdot -7$, er $-7 \mid -14$. Derfor er $7 \mid -14$. Vi har: $-14 = (-2) \cdot 7$.

Proposisjon 2.5.12. La l og n være heltall. Anta at $l \mid n$. Da er $l \mid -n$.

Bevis. Oppgave O2.1.5. □

Eksempel 2.5.13. Siden $20 = 4 \cdot 5$, er $5 \mid 20$. Derfor er $5 \mid -20$. Vi har: $-20 = (-4) \cdot 5$.

Eksempel 2.5.14. Siden $-33 = (-11) \cdot 3$, er $3 \mid -33$. Derfor er $3 \mid 33$. Vi har: $33 = 11 \cdot 3$.

Proposisjon 2.5.15. La l, l', n, og n' være heltall. Anta at $l \mid n$ og $l' \mid n'$. Da er $l \cdot l' \mid n \cdot n'$.

Bevis. Oppgave O2.1.6. □

Eksempel 2.5.16. Siden $18 = 3 \cdot 6$ er $6 \mid 18$. Siden $56 = 14 \cdot 4$ er $4 \mid 56$. Derfor er $6 \cdot 4 \mid 18 \cdot 56$, altså $24 \mid 1008$. Vi har: $1008 = 42 \cdot 24$.

Eksempel 2.5.17. Siden $-15 = 5 \cdot (-3)$ er $-3 \mid -15$. Siden $-100 = (-10) \cdot 10$ er $10 \mid -100$. Derfor er $-3 \cdot 10 \mid (-15) \cdot (-100)$, altså $-30 \mid 1500$. Vi har: $1500 = (-50) \cdot (-30)$.

Korollar 2.5.18. La l', n, og n' være heltall. Anta at $l' \mid n'$. Da er $l' \mid n \cdot n'$.

Bevis. Følger umiddelbart fra Proposisjon 2.5.15 ved å la l være 1. □

Eksempel 2.5.19. Siden $72 = 8 \cdot 9$ er $9 \mid 72$. Derfor er $9 \mid 4 \cdot 72$, altså $9 \mid 288$. Vi har: $288 = 32 \cdot 9$.

Eksempel 2.5.20. Siden $-12 = (-2) \cdot 6$ er $6 \mid -12$. Derfor er $6 \mid 63 \cdot (-12)$, altså $6 \mid -756$. Vi har: $-756 = (-126) \cdot 6$.

Korollar 2.5.21. La l, l', og n' være heltall. Anta at $l' \mid n'$. Da er $ll' \mid ln'$.

Bevis. Siden $l = 1 \cdot l$, har vi: $l \mid l$. Derfor følger utsagnet umiddelbart fra Proposisjon 2.5.15 ved å la n være l. □

Eksempel 2.5.22. Siden $42 = 6 \cdot 7$ er $7 \mid 42$. Derfor er $8 \cdot 7 \mid 8 \cdot 42$, altså $56 \mid 336$. Vi har: $336 = 6 \cdot 56$.

Eksempel 2.5.23. Siden $-32 = 4 \cdot (-8)$ er $-8 \mid -32$. Derfor er $(-6) \cdot (-8) \mid (-6) \cdot (-32)$, altså $48 \mid 192$. Vi har: $192 = 4 \cdot 48$.

Proposisjon 2.5.24. La l, m, og n være heltall. Anta at $l \mid m$ og $l \mid n$. Da er $l \mid m + n$.

Bevis. Siden $l \mid m$, finnes det et heltall k slik at $m = kl$. Siden $l \mid n$, finnes det et heltall k' slik at $n = k'l$. Da er

$$\begin{aligned} m + n &= kl + k'l \\ &= (k + k')l. \end{aligned}$$

Siden k og k' er heltall, er $k + k'$ et heltall. Vi konkluderer at $l \mid m + n$. □

Eksempel 2.5.25. Siden $14 = 2 \cdot 7$ er $7 \mid 14$. Siden $63 = 9 \cdot 7$ er $7 \mid 63$. Derfor er $7 \mid 14 + 63$, altså $7 \mid 77$. Vi har: $77 = 11 \cdot 7$.

Eksempel 2.5.26. Siden $-16 = (-4) \cdot 4$ er $4 \mid -16$. Siden $-32 = (-8) \cdot 4$ er $4 \mid -32$. Derfor er $4 \mid (-16) + (-32)$, altså $4 \mid -48$. Vi har: $-48 = (-12) \cdot 4$.

Proposisjon 2.5.27. La l, m, og n være heltall. Anta at $l \mid m$ og at $m \mid n$. Da er $l \mid n$.

Bevis. Siden $l \mid m$, finnes det et heltall k slik at $m = kl$. Siden $m \mid n$, finnes det et heltall k' slik at $n = k'm$. Da er

$$\begin{aligned} n &= k'm \\ &= k'(kl) \\ &= (k'k)l. \end{aligned}$$

Siden k og k' er heltall, er kk' et heltall. Vi konkluderer at $l \mid n$.

□

Eksempel 2.5.28. Siden $24 = 3 \cdot 8$ er $8 \mid 24$. Siden $72 = 3 \cdot 24$ er $24 \mid 72$. Derfor er $7 \mid 8 \mid 72$. Vi har: $72 = 9 \cdot 8$.

Eksempel 2.5.29. Siden $-21 = 3 \cdot (-7)$ er $-7 \mid -21$. Siden $63 = (-3) \cdot (-21)$ er $63 \mid -21$. Derfor er $-7 \mid 63$. Vi har: $63 = (-9) \cdot (-7)$.

Proposisjon 2.5.30. La l og n være naturlige tall. Anta at $l \mid n$. Da er $l \leq n$.

Bevis. Siden $l \mid n$ og både l og n er naturlige tall, finnes det et naturlig tall m slik at $n = ml$. Siden m er et naturlig tall, er $1 \leq m$. Derfor er

$$\begin{aligned} l &\leq ml \\ &= n. \end{aligned}$$

□

Eksempel 2.5.31. Siden $27 = 3 \cdot 9$, er $9 \mid 27$. Vi har: $9 \leq 27$.

Korollar 2.5.32. La l være et heltall, og la n være et heltall slik at $n \neq 0$. Anta at $l \mid n$. Da er $|l| \leq |n|$.

Bevis. Oppgave O2.1.7. □

Eksempel 2.5.33. Siden $-4 = 2 \cdot (-2)$, er $-2 \mid -4$. Vi har: $2 \leq 4$, altså $|-2| \leq |-4|$.

Eksempel 2.5.34. Siden $9 = (-3) \cdot (-3)$, er $-3 \mid 9$. Vi har: $3 \leq 9$, altså $|-3| \leq |9|$.

2.6 Største felles divisor

Definisjon 2.6.1. La l og n være heltall. Et naturlig tall d er den *største felles divisoren* til l og n dersom følgende er sanne.

(1) Vi har: $d \mid l$ og $d \mid n$, altså d er en divisor til både l og n.

(2) La c være et naturlig tall slik at $c \mid l$ og $c \mid n$, altså c er en divisor til både l og n. Da er $c \leq d$.

Notasjon 2.6.2. La l og n være heltall. Dersom det finnes naturlig tall som er den største felles divisoren til l og n, betegner vi det som $\mathsf{sfd}(l, n)$.

Merknad 2.6.3. La l og n være heltall. I Definisjon 2.6.1 kan vi bytte rekkefølgen på l og n uten å endre kravene (1) og (2). Dersom det finnes naturlig tall d som er den største felles divisoren til l og n, følger det at d er også den største felles divisoren til n og l. Med andre ord er $\mathsf{sfd}(l, n) = \mathsf{sfd}(n, l)$.

Eksempel 2.6.4. Divisorene til 6 som er naturlige tall er: 1, 2, 3, og 6. Divisorene til 8 som er naturlige tall er: 1, 2, 4, og 8. Dermed ser vi at de eneste naturlige tallene som deler både 6 og 8 er 1 og 2. Siden $1 \leq 2$, er $\mathsf{sfd}(6, 8) = 2$.

Eksempel 2.6.5. Divisorene til 9 som er naturlige tall er: 1, 3, 9. Divisorene til 12 som er naturlige tall er: 1, 2, 3, 4, 6, og 12. Dermed ser vi at de eneste naturlige tallene som deler både 9 og 12 er 1 og 3. Siden $1 \leq 3$, er $\mathsf{sfd}(9, 12) = 3$.

Eksempel 2.6.6. Divisorene til 30 som er naturlige tall er: 1, 2, 3, 5, 6, 10, 15, og 30. Divisorene til 105 som er naturlige tall er: 1, 3, 5, 7, 15, 21, 35, og 105. Dermed ser vi at de eneste naturlige tallene som deler både 30 og 105 er 1, 3, 5, og 15. Siden 15 er den største av disse fire naturlige tallene, er $\mathsf{sfd}(30, 105) = 15$.

Eksempel 2.6.7. Divisorene til 5 som er naturlige tall er: 1 og 5. Divisorene til 7 som er naturlige tall er: 1 og 7. Dermed ser vi at det eneste naturlige tallet som deler både 5 og 7 er 1. Derfor er $\mathsf{sfd}(5, 7) = 1$.

Eksempel 2.6.8. Divisorene til -10 som er naturlige tall er: 1, 2, 5, 10. Divisorene til 18 som er naturlige tall er: 1, 2, 3, 6, 9, 18. Dermed ser vi at de eneste naturlige tallene som deler både -10 og 18 er 1 og 2. Siden $1 \leq 2$, er $\mathsf{sfd}(-10, 18) = 2$.

Eksempel 2.6.9. Divisorene til -21 som er naturlige tall er: 1, 3, 7, 21. Divisorene til -24 som er naturlige tall er: 1, 2, 3, 4, 6, 8, 12, og 24. Dermed ser vi at de eneste naturlige tallene som deler både -21 og -24 er 1 og 3. Siden $1 \leq 3$, er $\mathsf{sfd}(-21, -24) = 3$.

Eksempel 2.6.10. La n være et heltall slik at $n \neq 0$. Siden n er delelig med n, og siden alle andre divisorer til n er mindre enn n, er $\mathsf{sfd}(n, n) = n$.

Merknad 2.6.11. Alle naturlige tall er divisorer til 0. Derfor finnes det ikke et naturlig tall som er den største felles divisoren til 0 og 0. Med andre ord har 0 og 0 ikke en største felles divisor.

Proposisjon 2.6.12. La l og n være heltall. Anta at det finnes et naturlig tall d slik at d er den største felles divisoren til l og n. Da er d den største felles divisoren til $-l$ og n.

Bevis. Siden $\mathsf{sfd}(l, n) = d$, har vi:

(1) $d \mid l$;

(2) $d \mid n$;

(3) dersom c er et naturlig tall slik at $c \mid l$ og $c \mid n$, er $c \leq d$.

Vi gjør følgende observasjoner.

(4) Fra (1) og Proposisjon 2.5.12 følger det at $d \mid -l$.

(5) La c være et naturlig tall slik at $c \mid -l$ og $c \mid n$. Siden $c \mid -l$, følger det fra Proposisjon 2.5.12 at $c \mid l$. Derfor har vi: $c \mid l$ og $c \mid n$. Fra (3) deduserer vi at $c \leq d$.

Fra (4), (2), og (5) konkluderer vi at $\mathsf{sfd}(-l, n) = d$.

□

Eksempel 2.6.13. I Eksempel 2.6.4 fant vi at $\mathsf{sfd}(6, 8) = 2$. Derfor fastslår Proposisjon 2.6.12 at $\mathsf{sfd}(-6, 8) = 2$.

Eksempel 2.6.14. I Eksempel 2.6.9 fant vi at $\mathsf{sfd}(-21, -24) = 3$. Derfor fastslår Proposisjon 2.6.12 at $\mathsf{sfd}(21, -24) = 3$.

Korollar 2.6.15. La l og n være heltall. Anta at det finnes et naturlig tall d slik at d er den største felles divisoren til l og n. Da er d den største felles divisoren til l og $-n$.

Bevis. Utsagnet følger umiddelbart fra Merknad 2.6.3 og Proposisjon 2.6.12. □

Eksempel 2.6.16. I Eksempel 2.6.4 fant vi at $\mathsf{sfd}(6, 8) = 2$. Derfor fastslår Korollar 2.6.15 at $\mathsf{sfd}(6, -8) = 2$.

Eksempel 2.6.17. I Eksempel 2.6.9 fant vi at $\mathsf{sfd}(-21, -24) = 3$. Derfor fastslår Korollar 2.6.15 at $\mathsf{sfd}(-21, 24) = 3$.

Korollar 2.6.18. La l og n være heltall. Anta at det finnes et naturlig tall d slik at d er den største felles divisoren til l og n. Da er d den største felles divisoren til $-l$ og $-n$.

Bevis. Siden d er den største felles divisoren til l og n, følger det fra Proposisjon 2.6.12 at d er den største felles divisoren til $-l$ og n. Da følger det fra Korollar 2.6.15 at d er den største felles divisoren til $-l$ og $-n$. □

Eksempel 2.6.19. I Eksempel 2.6.4 fant vi at $\mathsf{sfd}(6, 8) = 2$. Derfor fastslår Korollar 2.6.18 at $\mathsf{sfd}(-6, -8) = 2$.

Eksempel 2.6.20. I Eksempel 2.6.9 fant vi at $\mathsf{sfd}(-21, -24) = 3$. Derfor fastslår Korollar 2.6.18 at $\mathsf{sfd}(21, 24) = 3$.

Proposisjon 2.6.21. La n være et heltall, og la l være et naturlig tall. Anta at $l \mid n$. Da er l den største felles divisoren til l og n.

Bevis. Vi gjør følgende observasjoner.

(1) Vi har: $l \mid n$;

(2) Siden $l = 1 \cdot l$, har vi: $l \mid l$.

(3) La c være et naturlig tall slik at $c \mid l$ og $c \mid n$. Siden $c \mid l$, følger det fra Proposisjon 2.5.30 at $c \leq l$.

Fra (1) – (3) konkluderer vi at l er den største felles divisoren til l og n.

□

Eksempel 2.6.22. Siden $21 = 7 \cdot 3$, har vi: $3 \mid 21$. Derfor fastslår Proposisjon 2.6.21 at $\mathsf{sfd}(3, 21) = 3$.

Eksempel 2.6.23. Siden $-50 = -2 \cdot 25$, har vi: $25 \mid -50$. Derfor fastslår Proposisjon 2.6.21 at $\mathsf{sfd}(25, -50) = 25$.

Korollar 2.6.24. La l og n være heltall. Anta at $l \mid n$, og at $l \neq 0$. Da er $|l|$ den største felles divisoren til l og n.

Bevis. Ett av følgende utsagn er sant:

(i) $l > 0$;

(ii) $l < 0$.

Anta først at $l > 0$. Da er l et naturlig tall. Ut ifra Proposisjon 2.6.21 er l den største felles divisoren til l og n. I tillegg er $|l| = l$. Dermed er det sant at $|l|$ er den største felles divisoren til l og n.

Anta nå at $l < 0$. Da er $-l$ et naturlig tall. Derfor følger det fra Proposisjon 2.6.21 at $-l$ er den største felles divisoren til $-l$ og n. Vi gjør følgende observasjoner.

(1) Det følger fra Proposisjon 2.6.12, at $-l$ er den største felles divisoren til l og n.

(3) Siden $l < 0$, har vi: $|l| = -l$.

Dermed er det sant at $|l|$ er den største felles divisoren til l og n.

□

Eksempel 2.6.25. Siden $15 = (-5) \cdot (-3)$, har vi: $-3 \mid 15$. Derfor fastslår Korollar 2.6.24 at $\mathsf{sfd}(-3, 15) = 3$.

Eksempel 2.6.26. Siden $-27 = 9 \cdot (-3)$, har vi: $-3 \mid -27$. Derfor fastslår Korollar 2.6.24 at $\mathsf{sfd}(-3, -27) = 3$.

Proposisjon 2.6.27. La l, m, og n være heltall. La d være et naturlig tall slik at d er den største felles divisoren til l og n. Anta at $n \mid m$. Da er d den største felles divisoren til $l + m$ og n.

Bevis. Oppgave O2.1.8. □

Merknad 2.6.28. Dersom $n \mid m$, er med andre ord $\mathsf{sfd}(l + m, n) = \mathsf{sfd}(l, n)$.

Eksempel 2.6.29. Vi har: $\mathsf{sfd}(12, 21) = 3$. I tilleg har vi: $21 \mid 105$. Proposisjon 2.6.27 fastslår at 3 er den største felles divisoren til $12 + 105$ og 21, altså til 117 og 21.

Eksempel 2.6.30. Vi har: $\mathsf{sfd}(-24, 32) = 8$. I tilleg har vi: $32 \mid -192$. Proposisjon 2.6.27 fastslår at 8 er den største felles divisoren til $-24 - 192$ og 32, altså til -216 og 32.

2.7 Euklids algoritme

Merknad 2.7.1. La l og n være heltall, slik at det ikke er sant at både $l = 0$ og $n = 0$. Det ser kanskje opplagt ut at det finnes et naturlig tall d som er den største felles divisoren til l og n: for å finne d, kan vi bare liste alle heltallene som er divisorer til både l og n, og finne den største av disse.

Imidlertid er dette en ineffektiv algoritme. Vi skal nå gi et bevis ved induksjon for at det finnes et naturlig tall som er den største felles divisoren til l og n. Beviset gir oss en mer effektiv algoritme for å finne den største divisoren til l og n.

I tillegg gir beviset en algoritme for å finne heltall u og v slik at

$$\mathsf{sfd}(l, n) = ul + vn.$$

Vi kommer til å se at det er svært viktig fra et teoretisk synspunkt at vi kan finne heltall x og y slik at denne ligningen er sann.

Merknad 2.7.2. Kjernen av beviset, og dermed av de to algoritmene det fører til, er det følgende lemmaet.

Lemma 2.7.3. La k, l, n, og r være heltall slik at $n = kl + r$. Anta at det finnes et naturlig tall som er den største felles divisoren til n og l, og at det finnes et naturlig tall som er den største felles divisoren til l og r. Da er $\mathsf{sfd}(n, l) = \mathsf{sfd}(l, r)$.

Bevis. La d være $\mathsf{sfd}(n, l)$. Fra definisjonen til $\mathsf{sfd}(n, l)$ har vi:

(i) $d \mid n$;

(ii) $d \mid l$;

(iii) dersom c er et naturlig tall slik at $c \mid n$ og $c \mid l$, er $c \leq d$.

Vi gjør følgende observasjoner.

(1) Fra (ii) og Korollar 2.5.18 følger det at $d \mid (-k) \cdot l$.

(2) Siden

$$n = kl + r,$$

er

$$r = n + (-k) \cdot l.$$

Fra (i), (2), og Proposisjon 2.5.24, følger det at $d \mid r$.

La c være et naturlig tall slik at:

(iv) $c \mid l$;

(v) $c \mid r$.

Vi gjør følgende observasjoner.

(3) Det følger fra (iv) og Korollar 2.5.18 at $c \mid kl$.

(4) Siden

$$n = kl + r,$$

følger det fra (3), (v) og Proposisjon 2.5.24 at $c \mid n$.

Fra (4), (iv), og (iii), følger det at $c \leq d$.

Således har vi:

(A) $d \mid l$;

(B) $d \mid r$;

(C) dersom $c \mid l$ og $c \mid r$, er $c \leq d$.

Dermed er d den største felles divisoren til l og r.

□

Merknad 2.7.4. Målet vårt er Korollar 2.7.6. Imidlertid skal vi først bevise Proposisjon 2.7.5. Da skal vi observere at Korollar 2.7.6 følger fra Proposisjon 2.7.5.

Kanskje ser Proposisjon 2.7.5 litt rar ut. For hvert par naturlige tall l og s slik at $s < l$, beviser vi på en måte at (I) og (II) er sanne mange ganger: en gang for hvert naturlig tall større enn eller likt l.

Likevel viser det seg at påstanden i Proposisjon 2.7.5 er bedre for å gjennomføre et bevis ved induksjon enn påstanden i Korollar 2.7.6, i det minste for de variantene av induksjon som vi så på i Kapittel 1.

Proposisjon 2.7.5. La n være et naturlig tall slik at $n \geq 2$. La l og s være naturlige tall slik at $s < l \leq n$. Da finnes det et naturlig tall d slik at:

(I) d er den største felles divisoren til l og s;

(II) det finnes heltall u og v slik at $d = ul + vs$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. La l og s være naturlige tall slik at $s < l \leq 2$. Vi må sjekke om det finnes et naturlig tall d slik at:

(I) d er den største felles divisoren til l og s;

(II) det finnes heltall u og v slik at $d = ul + vs$.

Et par naturlige tall l og s oppfyller kravet $s < l \leq 2$ hvis og bare hvis $s = 1$ og $l = 2$. Derfor emå vi sjekke om det finnes et naturlig tall d slik at:

(A) d er den største felles divisoren til 1 og 2;

(B) det finnes heltall u og v slik at $d = 2u + v$.

Vi gjør følgende observasjoner:

(1) 1 er den største felles divisoren til 1 og 2;

(2) $1 = 0 \cdot 2 + 1 \cdot 1$.

Dermed er (A) og (B) sanne ved å la d være 1, u være 0, og v være 1. Således er proposisjonen sann når $n = 1$.

Anta nå at det har blitt bevist at proposisjonen er sann når n er et gitt naturlig tall m. La l og s være naturlige tall slik at $s < l \leq m + 1$. Vi ønsker å bevise at det finnes et naturlig tall d slik at:

(I) d er den største felles divisoren til l og s;

(II) det finnes heltall u og v slik at $d = ul + vs$.

Ut ifra Proposisjon 2.2.6 finnes det et naturlig tall k og et naturlig tall r slik at:

(i) $l = ks + r$;

(ii) $0 \leq r < s$.

Ett av følgende utsagn er sant:

(A) $r = 0$;

(B) $0 < r < s$.

Anta først at (A) er tilfellet. Vi gjør følgende observasjoner.

(1) Siden $r = 0$, er $l = ks$. Dermed er $s \mid l$. Det følger fra Proposisjon 2.6.21 at s er den største felles divisoren til l og s.

(2) Vi har:

$$s = 0 \cdot l + 1 \cdot s.$$

Dermed er (I) og (II) sanne ved å la d være s', u være 0, og v være 1. Således er proposisjonen sann når $n = m + 1$.

Anta nå at (B) er tilfellet. Siden

$$s < l \leq m + 1,$$

er $s \leq m$. Dermed er $r < s \leq m$. Fra antakelsen at proposisjonen har blitt bevist når $n = m$, følger det at det finnes et naturlig tall d' slik at:

(iii) d' er den største felles divisoren til s og r;

(iv) det finnes heltall u' og v' slik at $d' = u's + v'r$.

Vi gjør følgende observasjoner.

(1) Det følger fra (i), (iii), og Lemma 2.7.3 at d' er den største felles divisoren til l og s.

(2) Fra (i) og (iv) er

$$\begin{aligned} d' &= u's + v'r \\ &= u's - v'(l - ks) \\ &= (-v') \cdot l + (u' + kv')s. \end{aligned}$$

Dermed er (A) og (B) sanne ved å la d være d', u være v', og v være $u' + kv'$. Således er proposisjon sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall.

□

Korollar 2.7.6. La n være et naturlig tall. La l være et naturlig tall slik at $l \leq n$. Da finnes det et naturlig tall d slik at:

(I) d er den største felles divisoren til l og n;

(II) det finnes heltall u og v slik at $d = ul + vn$.

Bevis. Ett av følgende utsagn er sant:

(1) $l < n$;

(2) $l = n$.

Anta først at (1) er sant. Siden l er et naturlig tall, er $1 \leq l$. Derfor er $n \geq 2$. Da følger det umiddelbart fra Proposisjon 2.7.5, ved å la l i proposisjonen være n og s i proposisjonen være l, at det finnes et naturlig tall d slik at (I) og (II) er sanne.

Anta nå at (2) er sant. Vi gjør følgende observasjoner.

(1) Som fastslått i Eksempel 2.6.10, er n den største felles divisoren til n og n.

(2) Vi har:

$$n = 1 \cdot n + 0 \cdot n.$$

Dermed er (I) og (II) sanne ved å la d være n, u være 1, og v være 0.

□

Korollar 2.7.7. La n være et naturlig tall. La l være et naturlig tall. Da finnes det et naturlig tall d slik at:

(I) d er den største felles divisoren til l og n;

(II) det finnes heltall u og v slik at $d = ul + vn$.

Bevis. Ett av følgende utsagn er sant:

(1) $l \leq n$;

(2) $l > n$.

Anta først at (1) er sant. Da følger det fra Korollar 2.7.6 at det finnes et naturlig tall d slik at (I) og (II) er sanne.

Anta nå at (2) er sant. Da følger det fra Korollar 2.7.6 at det finnes et naturlig tall d' og heltall u' og v' slik at:

(A) d' er den største felles divisoren til n og l;

(B) $d' = u'n + v'l$.

La d være d'. Da følger det fra (A) og Merknad 2.6.3 at (I) er sant. La u være v', og v være u'. Da følger det fra (B) at (II) er sant.

□

Merknad 2.7.8. La n være et naturlig tall, og la l være et naturlig tall slik at $l < n$. I Merknad 1.4.3 så vi at induksjon gir en algoritme for å konstruere et bevis for en matematisk påstand. Således gir beviset for Proposisjon 2.7.5 en algoritme for å få den største felles divisoren til l og n. Denne algoritmen kan fremstilles som følger.

(1) Benytt divisjonsalgoritmen for å få heltall k_0 og r_0 slik at

$$n = k_0 l + r_0.$$

Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(l, n) = \mathsf{sfd}(r_0, l)$.

(2) Benytt divisjonsalgoritmen for å få heltall k_1 og r_1 slik at

$$l = k_1 r_0 + r_1.$$

Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(r_0, l) = \mathsf{sfd}(r_1, r_0)$.

(3) Benytt divisjonsalgoritmen for å få heltall k_2 og r_2 slik at

$$r_0 = k_2 r_1 + r_2.$$

Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(r_1, r_0) = \mathsf{sfd}(r_2, r_1)$.

(4) Benytt divisjonsalgoritmen for å få heltall k_3 og r_3 slik at

$$r_1 = k_3 r_2 + r_3.$$

Ut ifra Lemma 2.7.3, er $\mathsf{sfd}(r_2, r_1) = \mathsf{sfd}(r_1, r_0)$.

(5) Slik fortsetter vi.

La oss betegne n som r_{-2} og l som r_{-1}. Til slutt finnes det et heltall i og et heltall k_i slik at vi får

$$r_{i-2} = k_i r_{i-1} + 0$$

når vi benytter divisjonsalgoritmen, altså $r_{i-1} \mid r_{i-2}$. Fra Proposisjon 2.6.21 deduserer vi at $\mathsf{sfd}(r_{i-1}, r_{i-2}) = r_{i-1}$. Dermed er

$$\mathsf{sfd}(l, n) = \mathsf{sfd}(r_0, l) = \mathsf{sfd}(r_1, r_0) = \mathsf{sfd}(r_2, r_1) = \cdots = \mathsf{sfd}(r_{i-1}, r_{i-2}) = r_{i-1}.$$

Således er $\mathsf{sfd}(l, n) = r_{i-1}$.

Terminologi 2.7.9. Algoritmen i Merknad 2.7.8 kalles *Euklids algoritme*.

Merknad 2.7.10. Strengt tatt er algoritmen som vi får fra beviset for Proposisjon 2.7.5 ikke *helt* den samme som algoritmen i Merknad 2.7.8. I hvert steg av algoritmen vi får fra beviset for Proposisjon 2.7.5 beviser vi flere fakta enn vi trenger for å finne den største felles divisoren til et bestemt par naturlige tall.

Alle disse faktaene behøves derimot for å gjennomføre beviset for Proposisjon 2.7.5 betraktet i sin helhet, men når vi ønsker å finne den største felles divisoren til et bestemt par naturlige tall, kan vi plukke ut de faktaene som behøves. Da får vi algoritmen i Merknad 2.7.8.

Eksempel 2.7.11. La oss se hvordan Euklids algoritme ser ut når $n = 6$ og $l = 4$.

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$6 = 1 \cdot 4 + 2.$$

Fra Lemma 2.7.3 deduserer vi at

$$\mathsf{sfd}(6, 4) = \mathsf{sfd}(4, 2).$$

(2) Da benytter vi divisjonsalgoritmen for å få:

$$4 = 2 \cdot 2 + 0,$$

altså $2 \mid 4$. Fra Proposisjon 2.6.21 deduserer vi at $\mathsf{sfd}(4, 2) = 2$.

Dermed er

$$\mathsf{sfd}(6,4) = \mathsf{sfd}(4,2) = 2.$$

Eksempel 2.7.12. La oss se hvordan Euklids algoritme ser ut når $n = 20$ og $l = 8$.

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$20 = 2 \cdot 8 + 4.$$

Fra Lemma 2.7.3 deduserer vi at

$$\mathsf{sfd}(20,8) = \mathsf{sfd}(8,4).$$

(2) Da benytter vi divisjonsalgoritmen for å få:

$$8 = 2 \cdot 4 + 0,$$

altså $4 \mid 8$. Fra Proposisjon 2.6.21 deduserer vi at $\mathsf{sfd}(8,4) = 4$.

Dermed er

$$\mathsf{sfd}(20,8) = \mathsf{sfd}(8,4) = 4.$$

Eksempel 2.7.13. La oss se hvordan Euklids algoritme ser ut når $n = 18$ og $l = 10$.

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$18 = 1 \cdot 10 + 8.$$

Fra Lemma 2.7.3 deduserer vi at

$$\mathsf{sfd}(18,10) = \mathsf{sfd}(10,8).$$

(2) Da benytter vi divisjonsalgoritmen for å få:

$$10 = 1 \cdot 8 + 2.$$

Fra Lemma 2.7.3 deduserer vi at $\mathsf{sfd}(10,8) = \mathsf{sfd}(8,2)$.

(3) Da benytter vi divisjonsalgoritmen for å få:

$$8 = 4 \cdot 2 + 0,$$

altså $2 \mid 8$. Fra Proposisjon 2.6.21 deduserer vi at $\mathsf{sfd}(8,2) = 2$.

Dermed er

$$\mathsf{sfd}(18,10) = \mathsf{sfd}(10,8) = \mathsf{sfd}(8,2) = 2.$$

Eksempel 2.7.14. La oss se hvordan Euklids algoritme ser ut når $n = 54$ og $l = 15$.

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$54 = 3 \cdot 15 + 9.$$

Fra Lemma 2.7.3 deduserer vi at

$$\mathsf{sfd}(54, 15) = \mathsf{sfd}(15, 9).$$

(2) Da benytter vi divisjonsalgoritmen for å få:

$$15 = 1 \cdot 9 + 6.$$

Fra Lemma 2.7.3 deduserer vi at $\mathsf{sfd}(15, 9) = \mathsf{sfd}(9, 6)$.

(3) Da benytter vi divisjonsalgoritmen for å få:

$$9 = 1 \cdot 6 + 3.$$

Fra Lemma 2.7.3 deduserer vi at $\mathsf{sfd}(9, 6) = \mathsf{sfd}(6, 3)$.

(4) Da benytter vi divisjonsalgoritmen for å få:

$$6 = 2 \cdot 3 + 0.$$

Fra Proposisjon 2.6.21 deduserer vi at $\mathsf{sfd}(6, 3) = 3$.

Dermed er

$$\mathsf{sfd}(54, 15) = \mathsf{sfd}(15, 9) = \mathsf{sfd}(9, 6) = \mathsf{sfd}(6, 3) = 3.$$

Merknad 2.7.15. La n være et naturlig tall, og la l være et naturlig tall slik at $l < n$. Som vi har sett, gir Euklids algoritme oss den største felles divisoren til l og n. La oss betegne $\mathsf{sfd}(l, n)$ som d.

Proposisjon 2.7.5 gir oss i tillegg en algoritme for å finne heltall x og y slik at

$$d = ul + vn.$$

Igjen beviser i hvert steg av denne algoritmen flere fakta enn vi trenger. Ved å plukke ut bare de faktaene som behøves, kan algoritmen fremstilles som følger.

(1) Benytt divisjonsalgoritmen for å få heltall k_0 og r_0 slik at

$$n = k_0 l + r_0.$$

Da er

$$r_0 = -k_0 l + n.$$

La u_0 være $-k_0$, og la v_0 være 1.

(2) Benytt divisjonsalgoritmen for å få heltall k_1 og r_1 slik at

$$l = k_1 r_0 + r_1.$$

Da er

$$\begin{aligned} r_1 &= l - k_1 r_0 \\ &= l - k_1(u_0 l + v_0 n) \\ &= (1 - u_0 k_1)l - (v_0 k_1)n. \end{aligned}$$

La u_1 være $1 - u_0 k_1$, og la v_1 være $-v_0 k_1$.

(3) Benytt divisjonsalgoritmen for å få heltall k_2 og r_2 slik at

$$r_0 = k_2 r_1 + r_2.$$

Da er

$$\begin{aligned} r_2 &= r_0 - k_2 r_1 \\ &= (u_0 l + v_0 n) - k_2(u_1 l + v_1 n) \\ &= (u_0 - u_1 k_2)l + (v_0 - v_1 k_2)n. \end{aligned}$$

La u_2 være $u_0 - u_1 k_2$, og la v_2 være $v_0 - v_1 k_2$.

(4) Benytt divisjonsalgoritmen for å få heltall k_3 og r_3 slik at

$$r_1 = k_3 r_2 + r_3.$$

Da er

$$\begin{aligned} r_3 &= r_1 - k_3 r_2 \\ &= (u_1 l + v_1 n) - k_3(u_2 l + v_2 n) \\ &= (u_1 - u_2 k_3)l + (v_1 - v_2 k_3)n. \end{aligned}$$

La u_3 være $u_1 - u_2 k_3$, og la v_3 være $v_1 - v_2 k_3$.

(5) Slik fortsetter vi.

La oss betegne n som r_{-2} og l som r_{-1}. Til slutt finnes det et heltall i og et heltall k_i slik at vi får

$$r_{i-2} = k_i r_{i-1} + 0$$

når vi benytter divisjonsalgoritmen. Fra Euklids algoritme vet vi at $d = r_{i-1}$. Vi gjør følgende.

(1) Hvis $i = 0$, er $d = l$. I dette tilfellet er $u = 1$ og $v = 0$, altså

$$d = 1 \cdot l + 0 \cdot n.$$

(2) Ellers er

$$r_{i-1} = u_{i-1}l + v_{i-1}r,$$

altså

$$d = u_{i-1}l + v_{i-1}r.$$

I dette tilfellet er $u = u_{i-1}$ og $v = v_{i-1}$.

Eksempel 2.7.16. La oss se hvordan algoritmen i Merknad 2.7.15 ser ut når $n = 6$ og $l = 4$. Fra Eksempel 2.7.11 vet vi at $\mathsf{sfd}(6, 4) = 2$. Derfor bør algoritmen gi oss heltall u og v slik at

$$2 = u \cdot 6 + v \cdot 4.$$

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$6 = 1 \cdot 4 + 2.$$

Da er

$$2 = -1 \cdot 4 + 6.$$

Vi lar u_0 være -1, og lar v_0 være 1.

(2) Da benytter vi divisjonsalgoritmen for å få:

$$4 = 2 \cdot 2 + 0,$$

altså $2 \mid 4$.

Fra Euklids algoritme deduserer vi at $\mathsf{sfd}(6, 4) = 2$. Dermed er $u = u_0$ og $v = v_0$, altså $u = -1$ og $v = 1$. For å oppsummere, har vi:

$$2 = (-1) \cdot 4 + 1 \cdot 6.$$

Eksempel 2.7.17. La oss se hvordan algoritmen i Merknad 2.7.15 ser ut når $n = 20$ og $l = 8$. Fra Eksempel 2.7.12 vet vi at $\mathsf{sfd}(20, 8) = 4$. Derfor bør algoritmen gi oss heltall u og v slik at

$$4 = u \cdot 8 + v \cdot 20.$$

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$20 = 2 \cdot 8 + 4.$$

Da er

$$4 = -2 \cdot 8 + 1 \cdot 20.$$

Vi lar u_0 være -2, og lar v_0 være 1.

(2) Da benytter vi divisjonsalgoritmen for å få:

$$8 = 2 \cdot 4 + 0.$$

Fra Euklids algoritme deduserer vi at $\mathsf{sfd}(20, 8) = 4$. Dermed er $u = u_0$ og $v = v_0$, altså $u = -2$ og $v = 1$. For å oppsummere, har vi:

$$4 = (-2) \cdot 8 + 1 \cdot 20.$$

Eksempel 2.7.18. La oss se hvordan algoritmen i Merknad 2.7.15 ser ut når $n = 18$ og $l = 10$. Fra Eksempel 2.7.13 vet vi at $\mathsf{sfd}(18, 10) = 2$. Derfor bør algoritmen gi oss heltall u og v slik at

$$2 = u \cdot 10 + v \cdot 18.$$

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$18 = 1 \cdot 10 + 8.$$

Da er

$$8 = -1 \cdot 10 + 1 \cdot 18.$$

Vi lar u_0 være -1, og lar v_0 være 1.

(2) Da benytter vi divisjonsalgoritmen for å få:

$$10 = 1 \cdot 8 + 1 \cdot 2.$$

Da er

$$\begin{aligned} 2 &= -1 \cdot 8 + 10 \\ &= -1 \cdot (-1 \cdot 10 + 18) + 10 \\ &= 2 \cdot 10 + (-1) \cdot 18. \end{aligned}$$

Vi lar u_1 være 2, og lar v_1 være -1.

(3) Da benytter vi divisjonsalgoritmen for å få:

$$8 = 4 \cdot 2 + 0.$$

Fra Euklids algoritme deduserer vi at $\mathsf{sfd}(18, 10) = 2$. Dermed er $u = u_1$ og $v = v_1$, altså $u = 2$ og $v = -1$. For å oppsummere, har vi:

$$2 = 2 \cdot 10 + (-1) \cdot 18.$$

Eksempel 2.7.19. La oss se hvordan algoritmen i Merknad 2.7.15 ser ut når $n = 54$ og $l = 15$. Fra Eksempel 2.7.14 vet vi at $\mathsf{sfd}(54, 15) = 3$. Derfor bør algoritmen gi oss heltall u og v slik at

$$3 = u \cdot 15 + v \cdot 54.$$

(1) Vi begynner med å benytte divisjonsalgoritmen for å få:

$$54 = 3 \cdot 15 + 9.$$

Da er

$$9 = -3 \cdot 15 + 1 \cdot 54.$$

Vi lar u_0 være -3, og lar v_0 være 1.

(2) Da benytter vi divisjonsalgoritmen for å få:

$$15 = 1 \cdot 9 + 1 \cdot 6.$$

Da er

$$\begin{aligned} 6 &= -1 \cdot 9 + 15 \\ &= -1 \cdot (-3 \cdot 15 + 54) + 15 \\ &= 4 \cdot 15 + (-1) \cdot 54. \end{aligned}$$

Vi lar u_1 være 4, og lar v_1 være -1.

(3) Da benytter vi divisjonsalgoritmen for å få:

$$9 = 1 \cdot 6 + 1 \cdot 3.$$

Da er

$$\begin{aligned} 3 &= -1 \cdot 6 + 9 \\ &= -1 \cdot (4 \cdot 15 - 54) + (-3 \cdot 15 + 54) \\ &= (-7) \cdot 15 + 2 \cdot 54. \end{aligned}$$

Vi lar u_2 være -7, og lar v_2 være 2.

(4) Da benytter vi divisjonsalgoritmen for å få:

$$6 = 2 \cdot 3 + 0.$$

Fra Euklids algoritme deduserer vi at $\mathsf{sfd}(54, 15) = 3$. Dermed er $u = u_2$ og $v = v_2$, altså $u = -7$ og $v = -2$. For å oppsummere, har vi:

$$3 = (-7) \cdot 15 + 2 \cdot 54.$$

Korollar 2.7.20. La n og l være heltall. Anta at det ikke er sant at både n og l er lik 0. Da finnes det et naturlig tall d slik at:

(I) d er den største felles divisoren til l og n;

(II) det finnes heltall u og v slik at $d = ul + vn$.

Bevis. Ett av følgende utsagn er sant:

(1) $l > 0$ og $n > 0$;

(2) $l > 0$ og $n < 0$;

(3) $l < 0$ og $n > 0$;

(4) $l < 0$ og $n < 0$;

(5) $l \neq 0$ og $n = 0$.

(6) $l = 0$ og $n \neq 0$.

Anta først at (1) er sant. Da er l og n naturlige tall. Det følger fra Korollar 2.7.7 at det finnes et naturlig tall d slik at (I) og (II) er sanne.

Anta nå at (2) er sant. Da er l og $-n$ naturlige tall. Det følger fra Korollar 2.7.7 at det finnes et naturlig tall d' slik at:

(A) d' er den største felles divisoren til l og $-n$;

(B) det finnes heltall u' og v' slik at $d' = u'l + v'(-n)$.

La d være d'. Det følger fra (A) og Korollar 2.6.15 at d er den største felles divisoren til l og $-(-n)$, altså til l og n. Dermed er (I) sant.

La u være u', og la v være $-v'$. Ut ifra (B) er

$$\begin{aligned} d &= u'l + v'(-n) \\ &= u'l + (-v')n \\ &= ul + vn. \end{aligned}$$

Dermed er (II) sant.

Anta nå at (3) er sant. Da er $-l$ og n naturlige tall. Det følger fra Korollar 2.7.7 at det finnes et naturlig tall d' slik at:

(A) d' er den største felles divisoren til $-l$ og n;

(B) det finnes heltall u' og v' slik at $d' = u'(-l) + v'n$.

La d være d'. Det følger fra (A) og Proposisjon 2.6.12 at d er den største felles divisoren til $-(-l)$ og n, altså til l og n. Dermed er (I) sant.

La u være $-u'$, og la v være v'. Ut ifra (B) er

$$\begin{aligned} d &= u'(-l) + v'n \\ &= (-u')l + v'n \\ &= ul + vn. \end{aligned}$$

Dermed er (II) sant.

Anta nå at (4) er sant. Da er $-l$ og $-n$ naturlige tall. Det følger fra Korollar 2.7.7 at det finnes et naturlig tall d' slik at:

(A) d' er den største felles divisoren til $-l$ og $-n$;

(B) det finnes heltall u' og v' slik at $d' = u'(-l) + v'(-n)$.

La d være d'. Det følger fra (A) og Korollar 2.6.18 at d er den største felles divisoren til $-(-l)$ og $-(-n)$, altså til l og n. Dermed er (I) sant.

La u være $-u'$, og la v være $-v'$. Ut ifra (B) er

$$\begin{aligned} d &= u'(-l) + v'(-n) \\ &= (-u')l + (-v')n \\ &= ul + vn. \end{aligned}$$

Dermed er (II) sant.

Anta nå at (5) er sant. Alle heltall er divisorer til 0. Den største divisoren til l er l. Derfor er l den største felles divisoren til l og 0. La d være l, la x være 1, og la y være 0. Da er

$$l = 1 \cdot l + 0 \cdot 0.$$

Dermed er (I) og (II) sanne.

Anta nå at (6) er sant. Alle heltall er divisorer til 0. Den største divisoren til n er n. Derfor er n den største felles divisoren til 0 og n. La d være n, la x være 0, og la y være 1. Da er

$$n = 0 \cdot 0 + 1 \cdot n.$$

Dermed er (I) og (II) sanne.

□

Eksempel 2.7.21. Beviset for Korollar 2.7.20 fastslår at $\mathsf{sfd}(20, -8)$ kan finnes ved å benytte Euklids algoritme når $n = 20$ og $l = 8$. Vi gjorde dette i Eksempel 2.7.12. Vi har:

$$\mathsf{sfd}(20, -8) = \mathsf{sfd}(20, 8) = 4.$$

I tilleg fastslår beviset for Korollar 2.7.20 at vi kan finne heltall u og v slik at

$$4 = u \cdot (-8) + v \cdot 20$$

på følgende måte.

(1) Benytt algoritmen i Merknad 2.7.15 for å få heltall u' og v' slik at

$$4 = u' \cdot 8 + v' \cdot 20.$$

Vi gjorde dette i Eksempel 2.7.17. Vi har:

$$4 = (-2) \cdot 8 + 1 \cdot 20.$$

(2) La u være 2, og la v være 1.

Da er

$$\begin{aligned} u \cdot (-8) + v \cdot 20 &= 2 \cdot (-8) + 1 \cdot 20 \\ &= (-2) \cdot 8 + 1 \cdot 20 \\ &= 4. \end{aligned}$$

Eksempel 2.7.22. Beviset for Korollar 2.7.20 fastslår at $\mathsf{sfd}(-18, 10)$ kan finnes ved å benytte Euklids algoritme når $n = 18$ og $l = 10$. Vi gjorde dette i Eksempel 2.7.13. Vi har:

$$\mathsf{sfd}(-18, 10) = \mathsf{sfd}(18, 10) = 2.$$

I tilleg fastslår beviset for Korollar 2.7.20 at vi kan finne heltall u og v slik at

$$2 = u \cdot 10 + v \cdot (-18)$$

på følgende måte.

(1) Benytt algoritmen i Merknad 2.7.15 for å få heltall u' og v' slik at

$$2 = u' \cdot 10 + v' \cdot 18.$$

Vi gjorde dette i Eksempel 2.7.18. Vi har:

$$2 = 2 \cdot 10 + (-1) \cdot 18.$$

(2) La u være 2, og la v være 1.

Da er

$$\begin{aligned} u \cdot 10 + v \cdot (-18) &= 2 \cdot 10 + 1 \cdot (-18) \\ &= 2 \cdot 10 + (-1) \cdot 18 \\ &= 2. \end{aligned}$$

Eksempel 2.7.23. Beviset for Korollar 2.7.20 fastslår at $\mathsf{sfd}(-15, -54)$ kan finnes ved å benytte Euklids algoritme når $n = 54$ og $l = 15$. Vi gjorde dette i Eksempel 2.7.14. Vi har:

$$\mathsf{sfd}(-15, -54) = \mathsf{sfd}(54, 15) = 3.$$

I tilleg fastslår beviset for Korollar 2.7.20 at vi kan finne heltall u og v slik at

$$3 = u \cdot (-54) + v \cdot (-15)$$

på følgende måte.

(1) Benytt algoritmen i Merknad 2.7.15 for å få heltall u' og v' slik at

$$3 = u' \cdot 15 + v' \cdot 54.$$

Vi gjorde dette i Eksempel 2.7.19. Vi har:

$$3 = (-7) \cdot 15 + 2 \cdot 54.$$

(2) La u være -2, og la v være 7.

Da er

$$\begin{aligned} u \cdot (-54) + v \cdot (-15) &= (-2) \cdot (-54) + 7 \cdot (-15) \\ &= 2 \cdot 54 + (-7) \cdot 15 \\ &= (-7) \cdot 15 + 2 \cdot 54 \\ &= 3. \end{aligned}$$

2.8 Relativt primiske heltall og Euklids lemma

Merknad 2.8.1. Korollar 2.7.20 er et svært viktig teoretisk verktøy. I denne og neste del av kapittelet skal vi se på noen eksempler som kan hjelpe oss å få en følelse for hvordan Korollar 2.7.20 kan benyttes.

Proposisjon 2.8.2. La l og n være heltall. La k være et naturlig tall. La d være et naturlig tall slik at d er den største felles divisoren til l og n. Da er kd den største felles divisoren til kl og kn.

Bevis. Siden d er den største felles divisoren til l og n, har vi:

(1) $d \mid l$;

(2) $d \mid n$.

Fra (1) og Korollar 2.5.21 deduserer vi at $kd \mid kl$. Fra (2) og Korollar 2.5.21 deduserer vi at $kd \mid kn$.

La c være et naturlig tall slik at:

(i) $c \mid kl$;

(ii) $c \mid kn$.

Vi gjør følgende observasjoner.

(1) Ut ifra Korollar 2.7.20 finnes det heltall u og v slik at

$$d = ul + vn.$$

Det følger at

$$kd = ukl + ukn.$$

(2) Fra (i) og Korollar 2.5.18 følger det at $c \mid ukl$.

(3) Fra (ii) og Korollar 2.5.18 følger det at $c \mid vkn$.

(4) Fra (2), (3), og Proposisjon 2.5.24 følger det at $c \mid ukl + ukn$.

(5) Fra (1) og (4) følger det at

$$c \mid kd.$$

(6) Siden k og d er naturlige tall, er kd et naturlig tall.

(7) Siden c er et naturlig tall, følger det fra (5), (6), og Proposisjon 2.5.30 at $c \leq kd$.

For å oppsummere beviset så langt, har vi bevist at:

(1) $kd \mid kl$;

(2) $kd \mid kn$;

(3) dersom $c \mid kl$ og $c \mid kn$, er $c \leq kd$.

Dersom er kd den største felles divisoren til kl og kn.

□

Eksempel 2.8.3. Vi har: $\mathsf{sfd}(18, 24) = 6$. Siden $90 = 5 \cdot 18$ og $120 = 5 \cdot 24$, følger det fra Proposisjon 2.8.2 at

$$\mathsf{sfd}(90, 120) = 5 \cdot \mathsf{sfd}(18, 24) = 5 \cdot 6 = 30.$$

Eksempel 2.8.4. Vi har: $\mathsf{sfd}(13, -21) = 1$. Siden $91 = 7 \cdot 13$ og $-147 = 7 \cdot -21$, følger det fra Proposisjon 2.8.2 at

$$\mathsf{sfd}(91, -147) = 7 \cdot \mathsf{sfd}(13, -21) = 7 \cdot 1 = 7.$$

Korollar 2.8.5. La l og n være heltall. La k være et heltall slik at $k \neq 0$. La d være et naturlig tall slik at d er den største felles divisoren til l og n. Da er $|k| \cdot d$ den største felles divisoren til kl og kn.

Bevis. Ett av følgende utsagn er sant:

(1) $k > 0$;

(2) $k < 0$.

Anta først at (1) er sant. Da er k et naturlig tall, og $|k|\, k$. Dermed følger utsagnet fra Proposisjon 2.8.2.

Anta nå at (2) er sant. Da er $-k$ et naturlig tall, og $|k| = -k$. Det følger fra Proposisjon 2.8.2 at $|k| \cdot d$ er den største felles divisoren til $(-k) \cdot l$ og $(-k) \cdot n$. Fra Korollar 2.6.18 følger det at $|k|$ er den største felles divisoren til $-(-k) \cdot l$ og $-(-k) \cdot n$, altså til l og n.

□

Eksempel 2.8.6. Vi har: $\mathsf{sfd}(14, 63) = 7$. Det følger fra Korollar 2.8.5 at

$$\mathsf{sfd}(-154, -693) = |-11| \cdot 7 = 11 \cdot 7 = 77.$$

Eksempel 2.8.7. Vi har: $\mathsf{sfd}(-76, 20) = 4$. Det følger fra Korollar 2.8.5 at

$$\mathsf{sfd}(380, -100) = |-5| \cdot 4 = 5 \cdot 4 = 20.$$

Proposisjon 2.8.8. La l og n være heltall. Da er $\mathsf{sfd}(l, n) = 1$ hvis og bare hvis det finnes heltall u og v slik at

$$1 = ul + vn.$$

Bevis. Anta først at $\mathsf{sfd}(l, n) = 1$. Da følger det fra Korollar 2.7.20 at det finnes heltall u og v slik at

$$1 = ul + vn.$$

Anta istedenfor at det finnes heltall u og v slik at

$$1 = ul + vn.$$

La c være et naturlig tall slik at:

(i) $c \mid l$;

(ii) $c \mid n$.

Vi gjør følgende observasjoner.

(1) Det følger fra (1) og Korollar 2.5.18 at $c \mid ul$.

(2) Det følger fra (2) og Korollar 2.5.18 at $c \mid vn$.

(3) Det følger fra (1), (2), og Proposisjon 2.5.24 at $c \mid ul + vn$.

Det følger fra (3) og ligningen $1 = ul + vn$ at $c \mid 1$.

Dermed har vi bevist at $c \mid 1$ dersom $c \mid l$ og $c \mid n$. I tillegg har vi: $1 \mid l$ og at $1 \mid n$. Vi konkluderer at $\mathsf{sfd}(l, n) = 1$.

□

Eksempel 2.8.9. Vi har:

$$1 = (-2) \cdot 14 + 29.$$

Derfor fastslår Proposisjon 2.8.8 at $\mathsf{sfd}(14, 29) = 1$.

Eksempel 2.8.10. Vi har:

$$1 = 5 \cdot 13 - 8 \cdot 8.$$

Derfor fastslår Proposisjon 2.8.8 at $\mathsf{sfd}(13, 8) = 1$.

Merknad 2.8.11. Proposisjon 2.8.8 stemmer ikke om vi bytter 1 med et annet heltall. For eksempel er

$$2 = 3 \cdot 3 + (-1) \cdot 7,$$

men $\mathsf{sfd}(3, 7) \neq 2$. Faktisk er $\mathsf{sfd}(3, 7) = 1$.

Terminologi 2.8.12. La l og n være heltall slik at $\mathsf{sfd}(l, n) = 1$. Da sier vi at l og n er *relativt primiske*.

Proposisjon 2.8.13. La l og n være heltall, og la d være et heltall slik at $\mathsf{sfd}(l, n) = d$. La k_l være heltallet slik at $l = k_l d$, og la k_n være heltallet slik at $n = k_n d$. Da er $\mathsf{sfd}(k_l, k_n) = 1$.

Bevis. Ut ifra Korollar 2.7.20, finnes det heltall u og v slik at

$$d = ul + vn.$$

Derfor er

$$d = uk_l d + uk_n n,$$

altså

$$d = d(uk_l + uk_n).$$

Det følger fra Proposisjon 2.2.25 at

$$1 = uk_l + uk_n.$$

Fra Proposisjon 2.8.8 konkluderer vi at $\mathsf{sfd}(k_l, k_n) = 1$. □

Merknad 2.8.14. Fra definisjonen til $\mathsf{sfd}(l, n)$ vet vi at $d \mid l$ og at $d \mid r$. Derfor finnes det heltall k_l og k_n slik at ligningene i Proposisjon 2.8.13 er sanne. Ut ifra Korollar 2.2.20 er dessutten k_l og k_n de eneste heltallene slik at disse to ligningene er sanne.

Eksempel 2.8.15. Vi har:

$$\mathsf{sfd}(108, 45) = 9.$$

Derfor fastslår Proposisjon 2.8.13 at

$$\mathsf{sfd}(12, 5) = 1.$$

Eksempel 2.8.16. Vi har:

$$\mathsf{sfd}(-48, 27) = 3.$$

Derfor fastslår Proposisjon 2.8.13 at

$$\mathsf{sfd}(-16, 9) = 1.$$

Proposisjon 2.8.17. La l, l', og n være heltall. Anta at $l \mid n$ og at $l' \mid n$. Dersom $\mathsf{sfd}(l, l') = 1$, har vi: $l \cdot l' \mid n$.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $l \mid n$, finnes det et heltall k_l slik at $n = k_l l$.

(2) Siden $l' \mid n$, finnes det et heltall $k_{l'}$ slik at $n = k_{l'} l'$.

(3) Ut ifra Korollar 2.7.20 finnes det heltall u og v slik at

$$1 = ul + vl'.$$

Det følger fra (1) – (3) at

$$\begin{aligned} n &= uln + vl'n \\ &= ulk_{l'}l' + vl'k_l l \\ &= (uk_{l'} + vk_l)ll'. \end{aligned}$$

Dermed har vi: $ll' \mid n$.

□

Eksempel 2.8.18. Vi har: $5 \mid 80$ og $8 \mid 80$. Siden $\mathsf{sfd}(5, 8) = 1$, fastslår Proposisjon 2.8.17 at $5 \cdot 8 \mid 40$, altså at $40 \mid 80$.

Eksempel 2.8.19. Vi har: $-9 \mid 882$ og $-14 \mid 882$. Siden $\mathsf{sfd}(-9, -14) = 1$, fastslår Proposisjon 2.8.17 at $-9 \cdot -14 \mid 882$, altså at $126 \mid 882$.

Merknad 2.8.20. Proposisjon 2.8.17 stemmer ikke om $\mathsf{sfd}(l, n) \neq 1$. For eksempel er $\mathsf{sfd}(9, 15) = 3$, og vi har: $9 \mid 45$ og $15 \mid 45$. Men $9 \cdot 15 = 135$, og det er ikke sant at $135 \mid 45$.

Merknad 2.8.21. Den følgende proposisjonen er kjernen til et teorem vi kommer til å bevise i det neste kapitelet. Det kalles noen ganger *Euklids lemma*.

Proposisjon 2.8.22. La l, n, og n' være heltall slik at $l \mid n \cdot n'$. Dersom $\mathsf{sfd}(l, n) = 1$, har vi: $l \mid n'$.

Bevis. Siden $\mathsf{sfd}(l, n) = 1$, fastslår Korollar 2.7.20 at det finnes heltall u og v slik at

$$1 = ul + vn.$$

Derfor er

$$n' = (u \cdot l) \cdot n' + (v \cdot n) \cdot n') = (u \cdot n') \cdot l + v \cdot (n \cdot n').$$

Vi gjør følgende observasjoner.

(1) Siden $l \mid l$, følger det fra Korollar 2.5.18 at $l \mid (u \cdot n') \cdot l$.

(2) Fra Korollar 2.5.18 og antakelsen at $l \mid n \cdot n'$, har vi: $l \mid v \cdot (n \cdot n')$.

Fra (1), (2), og Proposisjon 2.5.24, følger det at $l \mid l \cdot (u \cdot n') + v \cdot (n \cdot n')$. Dermed har vi: $l \mid n'$.

□

Eksempel 2.8.23. Vi har: $\mathsf{sfd}(9, 25) = 1$. I tillegg har vi: $9 \mid 1125$. Siden $1125 = 25 \cdot 45$, fastslår Proposisjon 2.8.22 at

$$9 \mid 45.$$

Eksempel 2.8.24. Vi har: $\mathsf{sfd}(-17, 24) = 1$. I tillegg har vi: $-17 \mid 2248$. Siden $2248 = 24 \cdot 102$, fastslår Proposisjon 2.8.22 at

$$-17 \mid 102.$$

Merknad 2.8.25. Proposisjon 2.8.22 stemmer ikke om $\mathsf{sfd}(l, n) \neq 1$. For eksempel er $\mathsf{sfd}(2, 4) = 2$, og $2 \mid 28$. Vi har: $28 = 4 \cdot 7$, men det er ikke sant at $2 \mid 7$.

Proposisjon 2.8.26. La l, m, og n være heltall. La d være et naturlig tall slik at d er den største felles divisoren til l og m. Anta at $1 = \mathsf{sfd}(l, n)$. Da er d den største felles divisoren til l og mn.

Bevis. Oppgave O2.1.10. □

Merknad 2.8.27. Dersom $1 = \mathsf{sfd}(l, n)$, er med andre ord $\mathsf{sfd}(l, m) = \mathsf{sfd}(l, mn)$.

Eksempel 2.8.28. Vi har: $\mathsf{sfd}(33, 44) = 11$. I tilleg har vi: $\mathsf{sfd}(33, 50) = 1$. Proposisjon 2.8.26 fastslår at $\mathsf{sfd}(33, 44 \cdot 50) = \mathsf{sfd}(33, 44)$, altså at $\mathsf{sfd}(33, 2200) = 11$.

Eksempel 2.8.29. Vi har: $\mathsf{sfd}(18, -27) = 9$. I tilleg har vi: $\mathsf{sfd}(18, 29) = 1$. Proposisjon 2.8.26 fastslår at $\mathsf{sfd}(18, -27 \cdot 29) = \mathsf{sfd}(18, -27)$, altså at $\mathsf{sfd}(18, -783) = 9$.

Proposisjon 2.8.30. La x, y, og z være heltall. Da er $\mathsf{sfd}(x, yz) = 1$ om og bare om $\mathsf{sfd}(x, y) = 1$ og $\mathsf{sfd}(x, z) = 1$.

Bevis. Anta først at $\mathsf{sfd}(x, y) = 1$ og $\mathsf{sfd}(x, z) = 1$. Siden $\mathsf{sfd}(x, y) = 1$, følger det fra Proposisjon 2.8.26 at $\mathsf{sfd}(x, yz) = \mathsf{sfd}(x, z)$. Siden $\mathsf{sfd}(x, z) = 1$, konkluderer vi at $\mathsf{sfd}(x, yz) = 1$.

Anta istedenfor at $\mathsf{sfd}(x, yz) = 1$. La w være et naturlig tall slik at $w \mid x$ og $w \mid y$. Vi gjør følgende observasjoner.

(1) Siden $w \mid y$, følger det fra Korollar **??** at $w \mid yz$.

(2) Siden $w \mid x$ og $w \mid yz$, følger det fra antakelsen $\mathsf{sfd}(x, yz) = 1$ at $w = 1$.

Således har vi bevist at, dersom w er et naturlig tall slik at $w \mid x$ og $w \mid y$, er $w = 1$. Dermed er $\mathsf{sfd}(x, y) = 1$.

Et lignende argument fastslår at, dersom w er et naturlig tall slik at $w \mid x$ og $w \mid z$, er $w = 1$. Dermed er $\mathsf{sfd}(x, z) = 1$.

□

Eksempel 2.8.31. Ved å benytte Euklids algoritme, finner vi at $\mathsf{sfd}(8, 1155) = 1$. Siden $1155 = 33 \cdot 35$, fastslår da Proposisjon 2.8.30 at $\mathsf{sfd}(8, 33) = 1$ og $\mathsf{sfd}(8, 35) = 1$. Dette er riktignok sant.

Eksempel 2.8.32. Siden $\mathsf{sfd}(9, -26) = 1$ og $\mathsf{sfd}(9, 77) = 1$, fastslår Proposisjon 2.8.30 at $\mathsf{sfd}(9, (-26) \cdot 77) = 1$, altså at $\mathsf{sfd}(9, -2002) = 1$. Ved å benytte Euklids algoritme, finner vi at dette riktignok er sant.

2.9 Lineære diofantiske ligninger

Merknad 2.9.1. La oss se på ligningen

$$x + 2y = 0.$$

Det er lett å finne alle heltallene x og y slik at denne ligningen er sann. For hvert heltall z, er $x = -2z$ og $y = z$ en løsning. Disse er de eneste løsningene. Således har vi for eksempel de følgende løsningene:

(1) $x = 2$ og $y = 1$;

(2) $x = 8$ og $y = 4$;

(3) $x = -18$, $y = -9$.

La oss se istedenfor på ligningen

$$2x + 4y = 3.$$

Det finnes ikke noe heltall x og y slik at denne ligningen er sann. For alle heltall x og y er $2x + 4y$ et partall, mens 3 er et oddetall. Derfor er det umulig at $2x + 4y$ kan være lik 3.

La nå a, b, og c være heltall. Ved hjelp av begrepet «største felles divisor», skal vi i denne delen av kapittelet se på hvordan vi kan finne alle heltallsløsningene til en hvilken som helst ligning

$$ax + by = c.$$

Terminologi 2.9.2. La a, b, og c være heltall. Når vi er interessert i heltall x og y slik at

$$ax + by = c,$$

kalles denne ligningen en *lineær diofantisk ligning.*

Merknad 2.9.3. En stor del av tallteori handler om heltallsløsninger til ligninger. Generelt sett er det veldig vanskelig å finne alle heltallsløsningene til en gitt ligningen: i dagens forskning innen tallteori benytter matematikere svært sofistikerte og abstrakte verktøy for å få en forståelse. Likevel er i mange tilfeller løsningene fremdeles et mysterium.

Proposisjon 2.9.4. La a, b, c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a, b) = d$. Fra Korollar 2.7.20 vet vi at det finnes heltall u og v slik at $d = ua + vb$. Anta at $d \mid c$, altså at det finnes et heltall k slik at $c = kd$. Da er $x = ku$ og $y = kv$ en løsning til ligningen

$$ax + by = c.$$

Bevis. Vi regner som følger:

$$\begin{aligned} ax + by &= a(ku) + b(kv) \\ &= k(au + bv) \\ &= kd \\ &= c. \end{aligned}$$

□

Merknad 2.9.5. Dette beviset er lett. Imidlertid er proposisjonen langt fra triviell. Det er Korollar 2.7.20, altså Euklids algoritme, som gir oss muligheten til å løse ligningen

$$ax + by = c$$

når $d \mid c$, ved å fastslå at vi kan finne heltall u og v slik at $d = ua + bv$.

Eksempel 2.9.6. Ved å benytte Euklids algoritme og algoritmen i Merknad 2.7.15, får vi:

(1) $\mathsf{sfd}(63, 49) = 7$;

(2) $7 = (-3) \cdot 63 + 4 \cdot 49$.

Siden $252 = 36 \cdot 7$, har vi i tillegg: $7 \mid 252$. Derfor fastslår Proposisjon 2.9.4 at $x = 36 \cdot (-3)$ og $y = 36 \cdot 4$, altså $x = -108$ og $y = 144$, er en løsning til ligningen

$$63x + 49y = 252.$$

Eksempel 2.9.7. Ved å benytte Euklids algoritme og algoritmen i Merknad 2.7.15, får vi:

(1) $\mathsf{sfd}(286, 455) = 13$;

(2) $13 = 8 \cdot 286 + (-5) \cdot 455$.

Siden

$$-429 = (-33) \cdot 13,$$

har vi i tillegg: $13 \mid -429$. Derfor fastslår Proposisjon 2.9.4 at $x = (-33) \cdot 8$ og $y = (-33) \cdot (-5)$, altså $x = -264$ og $y = 165$, er en løsning til ligningen

$$286x + 455y = -429.$$

Eksempel 2.9.8. Ved å benytte Euklids algoritme og algoritmen i Merknad 2.7.15, får vi:

(1) $\mathsf{sfd}(-24, 136) = 8$;

(2) $8 = (-6) \cdot (-24) + (-1) \cdot 136$.

Siden $1072 = 134 \cdot 8$, har vi i tillegg: $8 \mid 1072$. Derfor fastslår Proposisjon 2.9.4 at $x = 134 \cdot (-6)$ og $y = 134 \cdot (-1)$, altså $x = -804$ og $y = -134$, er en løsning til ligningen

$$-24x + 136y = 1072.$$

Proposisjon 2.9.9. La a, b, c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a, b) = d$. La x og y være heltall slik at

$$ax + by = c.$$

Da er $d \mid c$.

Bevis. Ut ifra definisjonen til $\mathsf{sfd}(a, b)$ er $d \mid a$ og $d \mid b$. Derfor finnes det et heltall k_a slik at $a = k_a d$, og et heltall k_b slik at $b = k_b d$. Nå regner vi som følger:

$$\begin{aligned} c &= ax + by \\ &= k_a dx + k_b dy \\ &= (k_a x + k_b y)d. \end{aligned}$$

Dermed er $d \mid c$.

□

Eksempel 2.9.10. Ved å benytte Euklids algoritme får vi: $\mathsf{sfd}(57, 133) = 19$. Siden det ikke er sant at $19 \mid 36$, følger det fra Proposisjon 2.9.9 at ligningen

$$57x + 133y = 36$$

har ingen heltallsløsning.

Eksempel 2.9.11. Vi har: $\mathsf{sfd}(-12, -18) = 6$. Siden det ikke er sant at $6 \mid 10$, følger det fra Proposisjon 2.9.9 at ligningen

$$-12x - 18y = 10$$

har ingen heltallsløsning.

Korollar 2.9.12. La a, b, c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a, b) = d$. Ligningen

$$ax + by = c$$

har en heltallsløsning hvis og bare hvis $d \mid c$.

Bevis. Følger umiddelbart fra Proposisjon 2.9.4 og Proposisjon 2.9.9. □

Proposisjon 2.9.13. La a, b, c, x, og y være heltall. Anta at

$$ax + by = c.$$

La d være et naturlig tall slik at $\mathsf{sfd}(a, b) = d$. Ut ifra definisjonen til $\mathsf{sfd}(a, b)$ vet vi at $d \mid a$ og $d \mid b$, altså at det finnes heltall k_a slik at $a = k_a d$, og at det finnes et heltall k_b slik at $b = k_b d$. La x' og y' være heltall slik at

$$ax' + by' = c.$$

Da finnes det et heltall t slik at

$$x' = x + k_b t$$

og

$$y' = y - k_a t.$$

Bevis. Vi gjør følgende observasjoner.

(1) Siden

$$ax + by = c$$

og

$$ax' + by' = c,$$

er

$$ax + by = ax' + by'.$$

Derfor er

$$by - by' = ax' - ax,$$

altså er

$$b(y - y') = a(x' - x).$$

(2) Siden $a = k_a d$ og $b = k_b d$, følger det fra (1) at

$$(k_b d)(y - y') = (k_a d)(x' - x),$$

altså at

$$d\big(k_b(y - y')\big) = d\big(k_a(x' - x)\big).$$

(3) Det følger fra (2) og Proposisjon 2.2.25 at

$$k_b(y - y') = k_a(x' - x).$$

Dermed er $k_a \mid k_b(y - y')$.

(4) Ut ifra Proposisjon 2.8.13 er $\mathsf{sfd}(k_a, k_b) = 1$.

(5) Det følger fra (3), (4), og Proposisjon 2.8.22 at $k_a \mid y - y'$. Dermed finnes det et heltall t slik at $y - y' = tk_a$.

(6) Det følger fra (3) og (5) at

$$k_a(x' - x) = k_b t k_a,$$

altså

$$k_a(x' - x) = k_a k_b t.$$

(7) Det følger fra (6) og Proposisjon 2.2.25 at $x' - x = k_b t$.

Fra (5) og (7) deduserer vi at

$$x' = x + tk_b$$

og

$$y' = y - tk_a.$$

□

Eksempel 2.9.14. Vi har: $x = 5$ og $y = 3$ er en løsning til ligningen

$$4x - 6y = 2.$$

I tillegg er

$$\mathsf{sfd}(4, -6) = 2.$$

Siden $4 = 2 \cdot 2$, er $k_a = 2$. Siden $-6 = (-3) \cdot 2$, er $k_b = -3$. La x' og y' være heltall slik at

$$4x' - 6y' = 2.$$

Proposisjon 2.9.13 fastsår at det finnes et heltall t slik at $x' = 5 + (-3)t$ og $y' = 3 - 2t$, altså $x' = 5 - 3t$ og $y' = 3 - 2t$.

For eksempel er $x = 68$ og $y = 45$ en løsning til ligningen

$$4x - 6y = 2.$$

Ved å la $t = 21$, er det rikignok sant at $x = 5 - 3t$ og $y = 3 - 2t$.

Eksempel 2.9.15. Vi har: $x = -2$ og $y = 1$ er en løsning til ligningen

$$-9x - 6y = 12.$$

I tillegg er

$$\mathsf{sfd}(-9, -6) = 3.$$

Siden $-9 = (-3) \cdot 3$, er $k_a = -3$. Siden $-6 = (-2) \cdot 3$, er $k_b = -2$. La x' og y' være heltall slik at

$$-9x' - 6y' = 12.$$

Proposisjon 2.9.13 fastsår at det finnes et heltall t slik at $x' = -2+(-2)t$ og $y' = 1-(-3)t$, altså $x' = -2 - 2t$ og $y' = 1 + 3t$.

For eksempel er $x = 30$ og $y = -47$ en løsning til ligningen

$$-9x - 6y = 12.$$

Ved å la $t = -15$, er det rikignok sant at $x = -2 - 2t$ og $y = 1 + 3t$.

Korollar 2.9.16. La a, b, c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a, b) = d$. Fra Korollar 2.7.20 vet vi at det finnes heltall u og v slik at $d = ua + vb$. Ut ifra definisjonen til $\mathsf{sfd}(a, b)$ vet vi at $d \mid a$ og $d \mid b$, altså at det finnes heltall k_a slik at $a = k_a d$, og at det finnes et heltall k_b slik at $b = k_b d$. Anta at $d \mid c$, altså at det et heltall k slik at $c = kd$. La x og y være heltall slik at

$$ax + by = c.$$

Da finnes det et heltall t slik at

$$x = ku + k_b t$$

og

$$y = kv - k_a t.$$

Bevis. Ut ifra Proposisjon 2.9.4 er

$$a(ku) + b(kv) = c.$$

Dermed følger utsagnet umiddelbart fra Proposisjon 2.9.13. □

Eksempel 2.9.17. La oss se på ligningen

$$63x + 49y = 252.$$

Som i Eksempel 2.9.6, har vi

(1) $\mathsf{sfd}(63, 49) = 7$;

(2) $7 = (-3) \cdot 63 + 4 \cdot 49$.

Siden $252 = 36 \cdot 7$, har vi i tillegg: $7 \mid 252$ og $k = 36$. Siden $63 = 9 \cdot 7$, er $k_a = 9$. Siden $49 = 7 \cdot 7$, er $k_b = 7$. Dersom x og y er heltall slik at

$$63x + 49y = 252,$$

fastslår Korollar 2.9.16 at det finnes et heltall t slik at $x = 36 \cdot (-3) + 7t$ og $y = 36 \cdot 4 - 9t$, altså $x = -108 + 7t$ og $y = 144 - 9t$.

For eksempel er $x = 39$ og $y = -45$ en løsning til ligningen. Ved å la $t = 21$, er det riktignok sant at $x = -108 + 7t$ og $y = 144 - 9t$.

Eksempel 2.9.18. La oss se på ligningen

$$286x + 455y = -429.$$

Som i Eksempel 2.9.7, har vi

(1) $\mathsf{sfd}(286, 455) = 13$;

(2) $13 = 8 \cdot 286 + (-5) \cdot 455$.

Siden

$$-429 = (-33) \cdot 13,$$

har vi i tillegg: $13 \mid -429$ og $k = -33$.. Siden $286 = 22 \cdot 13$, er $k_a = 13$. Siden $455 = 35 \cdot 13$, er $k_b = 35$. Dersom x og y er heltall slik at

$$286x + 455y = -429,$$

fastslår Korollar 2.9.16 at det finnes et heltall t slik at $x = (-33) \cdot 8 + 35t$ og $y = (-33) \cdot (-5) - 22t$, altså $x = -264 + 35t$ og $y = 165 - 22t$.

For eksempel er $x = 366$ og $y = -231$ en løsning til ligningen. Ved å la $t = 18$, er det riktignok sant at $x = -264 + 35t$ og $y = 165 - 22t$.

Eksempel 2.9.19. La oss se på ligningen

$$-24x + 136y = 1072.$$

Ved å benytte Euklids algoritme og algoritmen i Merknad 2.7.15, får vi:

(1) $\mathsf{sfd}(-24, 136) = 8$;

(2) $8 = (-6) \cdot (-24) + (-1) \cdot 136$.

Siden $1072 = 134 \cdot 8$, har vi i tillegg: $8 \mid 1072$ og $k = 134$. Dersom x og y er heltall slik at

$$-24x + 136y = 1072,$$

fastslår Korollar 2.9.16 at det finnes et heltall t slik at $x = 134 \cdot (-6) + 17t$ og $y = 134 \cdot (-1) + 3t$, altså $x = -804 + 17t$ og $y = -134 + 3t$.

For eksempel er $x = -1025$ og $y = -173$ en løsning til ligningen. Ved å la $t = -13$, er det riktignok sant at $x = -804 + 17t$ og $y = -134 + 3t$.

Proposisjon 2.9.20. La a, b, c, x, og y være heltall. Anta at

$$ax + by = c.$$

La d være et naturlig tall slik at $\mathsf{sfd}(a, b) = d$. Ut ifra definisjonen til $\mathsf{sfd}(a, b)$ vet vi at $d \mid a$ og $d \mid b$, altså at det finnes heltall k_a slik at $a = k_a d$, og at det finnes et heltall k_b slik at $b = k_b d$. For hvert heltall t, er da

$$x' = x + k_b t$$

og

$$y' = y - k_a t$$

en løsning til ligningen

$$ax' + by' = c.$$

Bevis. Vi regner som følger:

$$\begin{aligned} ax' + by' &= a(x + k_b t) + b(y - k_a t) \\ &= ax + by + ak_b t - bk_a t \\ &= ax + by + (ak_b - bk_a)t \\ &= ax + by + \big((k_a d)k_b - (k_b d)k_a\big)t \\ &= ax + by + (k_a k_b d - k_a k_b d)t \\ &= ax + by + 0 \cdot t \\ &= ax + by \\ &= c \end{aligned}$$

□

Eksempel 2.9.21. Som i Eksempel 2.9.14, har vi:

(1) $x = 5$ og $y = 3$ er en løsning til ligningen

$$4x - 6y = 2;$$

(2) $\mathsf{sfd}(4, -6) = 2$;

(3) $k_a = 2$ og $k_b = -3$.

For hvert heltall t, fastslår Proposisjon 2.9.20 at $x = 5 - 3t$ og $y = 3 - 2t$ er en løsning til ligningen

$$63x + 49y = 252.$$

For eksempel er $x = 5 - 3 \cdot 68$ og $y = 3 - 2 \cdot 68$, altså $x = -199$ og $y = -133$, en løsning til ligningen.

Korollar 2.9.22. La a, b, c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a,b) = d$. Fra Korollar 2.7.20 vet vi at det finnes heltall u og v slik at $d = ua + vb$. Ut ifra definisjonen til $\mathsf{sfd}(a,b)$ vet vi at $d \mid a$ og $d \mid b$, altså at det finnes heltall k_a slik at $a = k_a d$, og at det finnes et heltall k_b slik at $b = k_b d$. Anta at $d \mid c$, altså at det et heltall k slik at $c = kd$. For hvert heltall t, er da

$$x = ku + k_b t$$

og

$$y = kv - k_a t$$

en løsning til ligningen

$$ax + by = c.$$

Bevis. Ut ifra Proposisjon 2.9.4 er

$$aku + bkv = c.$$

Dermed følger utsagnet umiddelbart fra Proposisjon 2.9.20. □

Eksempel 2.9.23. La oss se på ligingen

$$63x + 49y = 252.$$

Som i Eksempel 2.9.6, har vi:

(1) $\mathsf{sfd}(63, 49) = 7$;

(2) $x = -3$ og $y = 4$ er en løsning til ligningen

$$63x + 49y = 7;$$

(3) $k = 36$;

(4) $k_a = 9$ og $k_b = 7$.

For hvert heltall t, fastslår Korollar 2.9.22 at $x = 36 \cdot (-3) + 7t$ og $y = 36 \cdot 4 + 9t$, altså $x = -108 + 7t$ og $y = 144 - 9t$, er en løsning til ligningen

$$63x + 49y = 252.$$

For eksempel er $x = -108 + 7 \cdot 51$ og $y = 144 - 9 \cdot 51$, altså $x = 249$ og $y = -315$, en løsning til ligningen.

Korollar 2.9.24. La a, b, c, x, og y være heltall. Anta at

$$ax + by = c.$$

La d være et naturlig tall slik at $\mathsf{sfd}(a,b) = d$. Ut ifra definisjonen til $\mathsf{sfd}(a,b)$ vet vi at $d \mid a$ og $d \mid b$, altså at det finnes heltall k_a slik at $a = k_a d$, og at det finnes et heltall k_b slik at $b = k_b d$. Da er heltall x' og y' en løsning til ligningen

$$ax' + by' = c$$

hvis og bare hvis det finnes et heltall t slik at

$$x' = x + k_b t$$

og

$$y' = y - k_a t.$$

Bevis. Følger umiddelbart fra Proposisjon 2.9.13 og Proposisjon 2.9.20. □

Korollar 2.9.25. La a, b, c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a,b) = d$. Fra Korollar 2.7.20 vet vi at det finnes heltall u og v slik at $d = ua + vb$. Ut ifra definisjonen til $\mathsf{sfd}(a,b)$ vet vi at $d \mid a$ og $d \mid b$, altså at det finnes heltall k_a slik at $a = k_a d$, og at det finnes et heltall k_b slik at $b = k_b d$. Anta at $d \mid c$, altså at det et heltall k slik at $c = kd$. Da er heltall x og y en løsning til ligningen

$$ax + by = c$$

hvis og bare hvis det finnes et heltall t slik at

$$x = ku + k_b t$$

og

$$y = kv - k_a t.$$

Bevis. Følger umiddelbart fra Korollar 2.9.16 og Korollar 2.9.22. □

Merknad 2.9.26. Ved å ha gitt et bevis for Korollar 2.9.25, har vi rukket en komplett forståelse for løsningene til en hvilken som helst lineær diofantisk ligning.

2.10 Delbarhet og Fibonaccitallene

Merknad 2.10.1. Nå skal vi benytte teorien vi har sett på i dette kapittelet for å utforske Fibonaccitallene videre.

Notasjon 2.10.2. La n være et naturlig tall. I resten av dette kapittelet kommer alltid u_n til å betegne det n-te Fibonaccitallet.

Proposisjon 2.10.3. La n være et naturlig tall. Da er $\mathsf{sfd}(u_n, u_{n+1}) = 1$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. I dette tilfellet er utsagnet at $\mathsf{sfd}(u_1, u_2) = 1$. Siden $u_1 = 1$ og $u_2 = 1$, er dette sant.

Anta nå at proposisjonen har blitt bevist for et gitt naturlig tall m. Således har det blitt bevist at $\mathsf{sfd}(u_m, u_{m+1}) = 1$. La c være et naturlig tall slik at:

(i) $c \mid u_{m+1}$;

(ii) $c \mid u_{m+2}$.

Vi gjør følgende observasjoner.

(1) Fra (i) og Proposisjon 2.5.12 følger det at $c \mid -u_{m+1}$.

(2) Ut ifra definisjonen til Fibonaccitallene er $u_{m+2} = u_m + u_{m+1}$. Derfor er $u_m = u_{m+2} - u_{m+1}$.

(3) Fra (ii), (1), (2), og Proposisjon 2.5.24, følger det at $c \mid u_m$.

Fra (3), (i), og antakelsen at $\mathsf{sfd}(u_m, u_{m+1}) = 1$, følger det at $c = 1$.

Dersom $c \mid u_{m+1}$ og $c \mid u_{m+2}$, har vi dermed bevist at $c = 1$. Vi deduserer at $\mathsf{sfd}(u_{m+1}, u_{m+2}) = 1$. Således er proposisjonen sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann for alle naturlige tall.

□

Eksempel 2.10.4. La n være 5. Da fastslår Proposisjon 2.10.3 at $\mathsf{sfd}(u_5, u_6) = 1$, altså at $\mathsf{sfd}(5, 8) = 1$.

Eksempel 2.10.5. La n være 7. Da fastslår Proposisjon 2.10.3 at $\mathsf{sfd}(u_7, u_8) = 1$, altså at $\mathsf{sfd}(13, 21) = 1$.

Lemma 2.10.6. La n være et naturlig tall. La l være et naturlig tall slik at $l \geq 2$. Da er

$$u_{l+n} = u_{l-1}u_n + u_l u_{n+1}.$$

Bevis. Siden $n \geq 1$, er $n-1 \geq 0$. Siden $l \geq 2$, er $l+1 \geq 3$.Derfor følger det fra Proposisjon 1.14.1 at

$$\begin{aligned} u_{(n-1)+(l+1)} &= u_{(l+1)-1}u_{(n-1)+2} + u_{(l+1)-2}u_{(n-1)+1} \\ &= u_l u_{n+1} + u_{l-1}u_n \\ &= u_{l-1}u_n + u_l u_{n+1}. \end{aligned}$$

Dermed er

$$\begin{aligned} u_{l+n} &= u_{n+l} \\ &= u_{(n-1)+(l+1)} \\ &= u_{l-1}u_n + u_l u_{n+1}. \end{aligned}$$

□

Eksempel 2.10.7. Når $n = 3$ og $l = 7$, fastslår Proposisjon 1.14.1 at

$$u_{10} = u_6 u_3 + u_7 u_4,$$

altså at

$$55 = 8 \cdot 2 + 13 \cdot 3.$$

Eksempel 2.10.8. Når $n = 6$ og $l = 5$, fastslår Proposisjon 1.14.1 at

$$u_{11} = u_4u_6 + u_5u_7,$$

altså at

$$89 = 3 \cdot 8 + 5 \cdot 13.$$

Proposisjon 2.10.9. La l og n være naturlige tall. Da har vi: $u_l \mid u_{ln}$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. I dette tilfellet er utsagnet at

$$u_l \mid u_l.$$

Siden $u_l = 1 \cdot u_l$, er dette sant.

Anta nå at proposisjonen har blitt bevist når n er et gitt naturlig tall m. Således har det blitt bevist at

$$u_l \mid u_{lm}.$$

Ett av følgende utsagn er sant.

(A) $l = 1$;

(B) $l \geq 2$.

Anta først at (A) er tilfellet. Siden $u_1 = 1$, er det sant at $u_1 \mid u_{m+1}$, altså at $u_1 \mid u_{1\cdot(m+1)}$. Dermed er proposisjonen sann når $n = m + 1$ i dette tilfellet.

Anta nå at (B) er tilfellet. Vi gjør følgende observasjoner.

(1) Vi har:

$$u_{l(m+1)} = u_{lm+l}.$$

(2) Siden $l \geq 2$, følger det fra Lemma 2.10.6 at

$$u_{lm+l} = u_{lm-1}u_l + u_{lm}u_{l+1}.$$

(3) Ut ifra antakelsen at $u_l \mid u_{lm}$ finnes det et heltall k slik at $u_{lm} = k \cdot u_l$.

(4) Det følger fra (2) og (3) at

$$\begin{aligned} u_{lm+l} &= u_{lm-1}u_l + ku_lu_{l+1} \\ &= (u_{lm-1} + ku_{l+1})\, u_l. \end{aligned}$$

(5) Siden hvert Fibonaccitall er et naturlig tall og k er et heltall, er $u_{lm-1} + ku_{l+1}$ et heltall.

(6) Det følger fra (4) og (5) at $u_l \mid u_{lm+l}$.

Dermed har vi bevist at $u_l \mid u_{l(m+1)}$. Således er proposisjonen sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall.

□

Eksempel 2.10.10. Når $l = 3$ og $n = 5$, fastslår Proposisjon 2.10.9 at $u_3 \mid u_{15}$, altså at $2 \mid 610$.

Eksempel 2.10.11. Når $l = 4$ og $n = 3$, fastslår Proposisjon 2.10.9 at $u_4 \mid u_{12}$, altså at $3 \mid 144$.

Korollar 2.10.12. La l og k være naturlige tall slik at $l \mid n$. Da er $u_l \mid u_n$.

Bevis. Siden l og n er naturlige tall, finnes det da et naturlig tall k slik at $n = kl$. Det fra Proposisjon 2.10.9 at $u_l \mid u_{kl}$, altså at $u_l \mid u_n$. □

Eksempel 2.10.13. Vi har: $3 \mid 9$. Derfor er $u_3 \mid u_9$, altså $2 \mid 34$.

Eksempel 2.10.14. Vi har: $6 \mid 12$. Derfor er $u_6 \mid u_{12}$, altså $8 \mid 144$.

Lemma 2.10.15. La k, l, n, og r være naturlige tall slik at $n = kl+r$. Da er $\mathsf{sfd}(u_n, u_l) = \mathsf{sfd}(u_r, u_l)$.

Bevis. Ett av følgende utsagn er sant:

(A) $k = 1$ og $l = 1$;

(B) $kl \geq 2$.

Anta først at (A) er tilfellet. Da er utsagnet at $\mathsf{sfd}(u_n, u_1) = \mathsf{sfd}(u_r, u_1)$. Siden $u_1 = 1$, har vi:

$$\mathsf{sfd}(u_n, u_1) = \mathsf{sfd}(u_n, 1) = 1$$

og

$$\mathsf{sfd}(u_r, u_1) = \mathsf{sfd}(u_r, 1) = 1.$$

Dermed er proposisjonen sann i dette tilfellet.

Anta nå at (B) er tilfellet. Vi skal først bevise at $\mathsf{sfd}(u_{kl-1}, u_l) = 1$. La c være et naturlig tall slik at:

(i) $c \mid u_{kl-1}$;

(ii) $c \mid u_l$.

Vi gjør følgende observasjoner.

(1) Fra Proposisjon 2.10.9 har vi: $u_l \mid u_{kl}$.

(2) Det følger fra (ii), (1), og Proposisjon 2.5.27 at $c \mid u_{kl}$.

(3) Fra (i), (2), og Proposisjon 2.10.3 følger det at $c = 1$.

Dersom $c \mid u_{kl-1}$ og $c \mid u_l$, har vi dermed bevist at $c = 1$. Derfor er $\mathsf{sfd}(u_{kl-1}, u_l) = 1$.

Nå gjør vi følgende observasjoner.

(1) Siden $kl \geq 2$, følger det fra Lemma 2.10.6 at

$$u_{kl+r} = u_{kl-1}u_r + u_{kl}u_{r+1}.$$

(2) Ut ifra Proposisjon 2.10.9 er $u_l \mid u_{kl}$.

(3) Det følger fra (2) og Korollar 2.5.18 at $u_l \mid u_{r+1}u_{kl}$, altså at $u_l \mid u_{kl}u_{r+1}$.

(4) Det følger fra (3) og Proposisjon 2.6.27 at

$$\mathsf{sfd}(u_{kl-1}u_r + u_{kl}u_{r+1}, u_l) = \mathsf{sfd}(u_{kl-1}u_r, u_l).$$

(5) Vi vet at $\mathsf{sfd}(u_{kl-1}, u_l) = 1$, altså at $\mathsf{sfd}(u_l, u_{kl-1}) = 1$. Det følger fra Proposisjon 2.8.26 at $\mathsf{sfd}(u_l, u_{kl-1}u_r) = \mathsf{sfd}(u_l, u_r)$, altså at $\mathsf{sfd}(u_{kl-1}u_r, u_l) = \mathsf{sfd}(u_r, u_l)$.

Fra (1), (4), og (5) følger det at $\mathsf{sfd}(u_{kl+r}, u_l) = \mathsf{sfd}(u_r, u_l)$, altså at $\mathsf{sfd}(u_n, u_l) = \mathsf{sfd}(u_r, u_l)$.

□

Eksempel 2.10.16. Vi har: $7 = 2 \cdot 3 + 1$. Lemma 2.10.15 fastslår at $\mathsf{sfd}(u_7, u_3) = \mathsf{sfd}(u_3, u_1)$, altså at $\mathsf{sfd}(13, 2) = \mathsf{sfd}(2, 1)$.

Eksempel 2.10.17. Vi har: $13 = 2 \cdot 5 + 3$. Lemma 2.10.15 fastslår at $\mathsf{sfd}(u_{13}, u_5) = \mathsf{sfd}(u_5, u_3)$, altså at $\mathsf{sfd}(233, 5) = \mathsf{sfd}(5, 2)$.

Merknad 2.10.18. Målet vårt er Korollar 2.10.20. Imidlertid skal vi først bevise Proposisjon 2.10.19. Da skal vi observere at Korollar 2.10.20 følger fra Proposisjon 2.10.19.

Sammenlign med Merknad 2.7.4. For hvert par naturlige tall l og s slik at $s < l$, beviser vi på en måte at $\mathsf{sfd}(u_l, u_s) = u_d$ mange ganger: en gang for hvert naturlig tall større enn eller likt l.

Likevel viser det seg at påstanden i Proposisjon 2.10.19 er bedre for å gjennomføre et bevis ved induksjon enn påstanden i Korollar 2.10.20.

Proposisjon 2.10.19. La n være et naturlig tall slik at $n \geq 2$. La s og l være naturlige tall slik at $s < l \leq n$. La $d = \mathsf{sfd}(l, s)$. Da er $\mathsf{sfd}(u_l, u_s) = u_d$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 2$. La l og s være naturlige tall slik at $s < l \leq 2$. La $d = \mathsf{sfd}(l, s)$. Vi må sjekke om

$$\mathsf{sfd}(u_l, u_s) = u_d.$$

Et par naturlige tall l og s oppfyller kravet $s < l \leq 2$ hvis og bare hvis $s = 1$ og $l = 2$. Derfor må vi sjekke om

$$\mathsf{sfd}(u_2, u_1) = u_{\mathsf{sfd}(2,1)}.$$

Vi har: $\mathsf{sfd}(2,1) = 1$. Siden $u_1 = 1$ og $u_2 = 1$, har vi i tillegg: $\mathsf{sfd}(u_2, u_1) = \mathsf{sfd}(1,1) = 1$. Dermed er utasgnet sant.

Anta nå at proposisjonen har blitt bevist når n er et gitt naturlig tall m slik at $m \geq 2$. La s og l være naturlige tall slik at $s < l \leq m+1$. Ut ifra Proposisjon 2.2.6 finnes det heltall k og r slik at $l = ks + r$, $k \geq 0$, og $0 \leq r < s$. Siden $r < s$ og $s < l$, er $r < l$. Derfor er det faktisk ikke sant at $k = 0$, altså k er et naturlig tall. Ett av følgende utsagn er sant:

(A) $r = 0$;

(B) r er et naturlig tall.

Anta først at (A) er tilfellet. Da er $l = ks$, altså $s \mid l$. Vi gjør følgende observasjoner.

(1) Det følger fra Proposisjon 2.6.21 at $\mathsf{sfd}(l, s) = s$.

(2) I tillegg følger det fra Korollar 2.10.12 at $u_l \mid u_s$.

(3) Det følger fra (2) og Proposisjon 2.6.21 at $\mathsf{sfd}(u_l, u_s) = u_s$.

Det følger fra (1) og (3) at $\mathsf{sfd}(u_l, u_s) = \mathsf{sfd}(l, s)$. Dermed er proposisjonen sann i dette tilfellet.

Anta nå at (B) er tilfellet. Vi gjør følgende observasjoner.

(1) Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(l, s) = \mathsf{sfd}(s, r)$.

(2) Siden $s < l \leq m+1$, er $s < m$. La $d = \mathsf{sfd}(s, r)$. Ut ifra antakelsen at proposisjonen er sann når $n = m$, følger det at $\mathsf{sfd}(u_s, u_r) = u_d$.

(3) Ut ifra Lemma 2.10.15 er $\mathsf{sfd}(u_l, u_s) = \mathsf{sfd}(u_s, u_r)$.

Det følger fra (1), (2), og (3) at $\mathsf{sfd}(u_l, u_s) = \mathsf{sfd}(l, s)$. Dermed er proposisjonen sann i dette tilfellet.

□

Korollar 2.10.20. La l og n være naturlige tall. La $d = \mathsf{sfd}(l, n)$. Da er $\mathsf{sfd}(u_l, u_n) = u_d$.

Bevis. Ett av følgende utsagn er sant:

(1) $n = 1$;

(2) $n \geq 2$.

Anta først at $n = 1$. Da er utsagnet at $\mathsf{sfd}(u_l, u_1) = u_{\mathsf{sfd}(l,1)}$. Siden $u_1 = 1$, har vi:

$$\mathsf{sfd}(u_l, u_1) = \mathsf{sfd}(u_l, 1) = 1.$$

I tilleg har vi:

$$u_{\mathsf{sfd}(l,1)} = u_1 = 1.$$

Dermed er proposisjonen sann i dette tilfellet.

Anta nå at $n \geq 2$. Da følger det umiddelbart fra Proposisjon 2.10.19, ved å la l i proposisjonen være n og s i proposisjonen være l, at utsagnet er sant. □

Merknad 2.10.21. La d være den største felles divisoren til det l-te Fibonaccitallet og det n-te Fibonaccitallet. Proposisjon 2.10.19 fastlår at d er også et Fibonaccitall, nemlig det d-te!

Eksempel 2.10.22. Vi har: $\mathsf{sfd}(6, 9) = 3$. Korollar 2.10.20 fastslår at $\mathsf{sfd}(u_6, u_9) = u_3$, altså at $\mathsf{sfd}(8, 34) = 2$.

Eksempel 2.10.23. Vi har: $\mathsf{sfd}(8, 12) = 4$. Korollar 2.10.20 fastslår at $\mathsf{sfd}(u_8, u_{12}) = u_4$, altså at $\mathsf{sfd}(21, 144) = 3$.

Korollar 2.10.24. La l og n være naturlige tall slik at $l \geq 3$ Da er u_n delelig med u_l hvis og bare hvis n er delelig med l.

Bevis. Anta først at u_n er delelig med u_l. Vi gjør følgende observasjoner.

(1) Siden u_n er delelig med u_l, følger det fra Proposisjon 2.6.21 at $\mathsf{sfd}(u_l, u_n) = u_l$.

(2) Ut ifra Korollar 2.10.20 er $\mathsf{sfd}(u_l, u_n) = u_{\mathsf{sfd}(l,n)}$.

(3) Det følger fra $u_l = u_{\mathsf{sfd}(l,n)}$.

(4) De eneste naturlige tallene $i \neq j$ slik at $u_i = u_j$ er $i = 1$ og $j = 2$.

(5) Siden $l \geq 3$, følger det fra (3) og (4) at $l = \mathsf{sfd}(l, n)$.

Fra definisjonen til $\mathsf{sfd}(l, n)$ har vi: $\mathsf{sfd}(l, n) \mid n$. Dermed har vi: $l \mid n$.

Anta istedenfor at $l \mid n$. Korollar 2.10.12 fastslår at $u_l \mid u_n$.

□

Eksempel 2.10.25. Siden 10 er ikke delelig med 4, følger det fra Korollar 2.10.24 er u_{10} er ikke delelig med u_4, altså er 55 ikke delelig med 3.

Eksempel 2.10.26. Siden 54 er ikke delelig med 23, følger det fra Korollar 2.10.24 er u_{54} er ikke delelig med u_{23}.

O2 Oppgaver – Delbarhet

O2.1 Oppgaver i eksamens stil

Oppgave O2.1.1. La n være et partall. Bevis at det er et heltall m slik at enten $n^2 = 8m$ eller $n^2 = 8m + 4$.

Oppgave O2.1.2. La n være et heltall. Bevis at det er et heltall m slik at enten $n^4 = 5m$ eller $n^4 = 5m + 1$. *Tips*: Benytt Proposisjon 1.9.30 i løpet av svaret ditt.

Oppgave O2.1.3. La n være et heltall. Anta at det er heltall s slik at $n = s^3$. Anta i tillegg at det er et heltall t slik at $n = t^2$. Bevis at det er et heltall m slik at enten $n = 7m$ eller $n = 7m + 1$. *Tips*: Gjør følgende.

(1) Bevis at det er et heltall m slik at et av de følgende utsagnene er sant:
   (i) $n = 7m$;
   (ii) $n = 7m + 1$;
   (iii) $n = 7m + 6$.

   Benytt Proposisjon 1.9.30 og antakelsen at $n = s^3$ i løpet av svaret ditt.

(2) Bevis at det er et heltall m' slik at et av de følgende utsagnene er sant:
   (i) $n = 7m'$;
   (ii) $n = 7m' + 1$;
   (iii) $n = 7m' + 2$;
   (iv) $n = 7m' + 4$;

   Benytt antakelsen at $n = t^2$ i løpet av svaret ditt.

(3 Benytt Korollar 2.2.20 ved å la l være 7.

Oppgave O2.1.4. La n være et naturlig tall.

(1) Bevis at $7n^2 + 7n + 4$ er et partall.

(2) Bevis at $n(7n^2 + 5)$ er delelig med 6.

Tips: Benytt induksjon i beviset for (2). Sjekk i tillegg om ligningen

$$(m + 1)(7m^2 + 14m + 12) = m(7m^2 + 5) + (21m^2 + 21m + 12)$$

er sann for et hvilket som helst naturlig tall, og benytt denne ligningen i løpet av svaret ditt.

Oppgave O2.1.5. La l og n være heltall. Anta at $l \mid n$. Bevis at $l \mid -n$.

Oppgave O2.1.6. La l, l', n, og n' være heltall. Anta at $l \mid n$ og $l' \mid n'$. Bevis at $l \cdot l' \mid n \cdot n'$.

Oppgave O2.1.7. La l være et heltall, og la n være et heltall slik at $n \neq 0$. Anta at $l \mid n$. Ved å benytte Proposisjon 2.5.30, bevis at $|l| \leq |n|$.

Oppgave O2.1.8. La l, m, og n være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(l, n) = d$. Anta at $n \mid m$. Bevis at $\mathsf{sfd}(l + m, n) = d$. *Tips*: Benytt ligningen $l = (l + m) - m$ i løpet av beviset ditt.

Oppgave O2.1.9. For hvert av de følgende heltallene l og n, finn $\mathsf{sfd}(l, n)$, og finn heltall u og v slik at $\mathsf{sfd}(l, n) = ul + vn$. Benytt Euklids algoritme i løpet av svarene dine.

(1) $l = 231$, $n = 616$.

(2) $l = -153$, $n = 391$.

(3) $l = -168$, $n = -420$,

Oppgave O2.1.10. La l, m, og n være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(l, m) = d$. Anta at $\mathsf{sfd}(l, n) = 1$. Bevis at $\mathsf{sfd}(l, mn) = d$. *Tips*: Gjør først følgende, og benytt da (3) i løpet av beviset ditt.

(1) La c være et heltall slik at $c \mid l$, og la s være et heltall. Bevis at $\mathsf{sfd}(c, s) \leq \mathsf{sfd}(l, s)$.

(2) La c være et heltall slik at $c \mid l$. Deduser fra (1) og antakelsen at $\mathsf{sfd}(l, n) = 1$ at $\mathsf{sfd}(c, n) = 1$.

(3) Dersom c er et naturlig tall slik at $c \mid mn$, deduser fra (2) og Proposisjon 2.8.22 at $c \mid m$.

Oppgave O2.1.11. For hver av de følgende ligningene, finn en heltallsløsning dersom det er mulig. Hvis det ikke er mulig, forklar hvorfor.

(1) $396x - 165y = 462$.

(2) $-546x + 312y = -317$.

(3) $288x + 186y = 6138$.

Oppgave O2.1.12. Finn alle heltallsløsningene til de følgende ligningene.

(1) $-371x + 28y = 119$.

(2) $15x - 33y = 28$.

(3) $1126x + 441y = -135$.

Oppgave O2.1.13. For et hvilket som helst naturlig tall r, la u_r betegne det r-te Fibonaccitallet. Finn $\mathsf{sfd}(u_{2793}, u_{462})$.

Oppgave O2.1.14. For et hvilket som helst naturlig tall r, la u_r betegne det r-te Fibonaccitallet. La l og n være naturlige tall. Anta at $\mathsf{sfd}(l, n) = 1$. Bevis at $u_l u_n \mid u_{ln}$.

O2.2 Oppgaver for å hjelpe med å forstå kapittelet

Oppgave O2.2.1. Hva er absoluttverdiene til de følgende heltallene:

(1) -83;

(2) 45;

(3) 6;

(4) -1257.

Oppgave O2.2.2. Beskriv hvordan divisjonsalgoritmen ser ut i de følgende tilfellene:

(1) $n = 8$ og $l = 5$;

(2) $n = 11$ og $l = 3$;

(3) $n = 10$ og $l = 5$.

Tips: Se Eksempel 2.2.8 – Eksempel 2.2.10.

Oppgave O2.2.3. Beskriv hvordan beviset for Korollar 2.2.11 ser ut i de følgende tilfellene:

(1) $n = -9$ og $l = 4$.

(2) $n = 8$ og $l = -3$.

(3) $n = -13$ og $l = -5$.

(4) $n = -10$ og $l = 2$.

Tips: Se Eksempel 2.2.12 – 2.2.14.

Oppgave O2.2.4. Hvilke heltall k og r får vi ved å bruke divisjonsalgoritmen når:

(1) $n = 348$ og $l = 39$,

(2) $n = 179$ og $l = 7$?

Tips: Se Merknad 2.2.17 og eksemplene som følger den.

Oppgave O2.2.5. Hvilke heltall k og r får vi ved å bruke divisjonsalgoritmen når:

(1) $n = 79$ og $l = -12$,

(2) $n = -87$ og $l = -11$,

(3) $n = -134$ og $l = -46$?

Tips: Se Merknad 2.2.21 og eksemplene som følger den.

Oppgave O2.2.6. Hvilke av de følgende heltallene er partall, og hvilke er oddetall? Som i Eksempel 2.3.3 – Eksempel 2.3.5, begrunn svaret ditt ved å referere til Terminologi 2.3.1.

(1) 46.

(2) -53

(3) -4.

(4) 16.

Oppgave O2.2.7. Hva fastslår Proposisjon 2.4.2 når $n = 15$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med 15. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.8. Hva fastslår Proposisjon 2.4.2 når $n = 20$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med 20. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.9. Hva fastslår Proposisjon 2.4.2 når $n = -10$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med -10. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.10. Hva fastslår Proposisjon 2.4.2 når $n = -5$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med -5. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.11. Hva fastslår Proposisjon 2.4.9 når $n = 7$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med 7. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.12. Hva fastslår Proposisjon 2.4.9 når $n = 13$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med 13. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.13. Hva fastslår Proposisjon 2.4.9 når $n = -5$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med -5. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.14. Hva fastslår Proposisjon 2.4.9 når $n = -9$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med -9. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.15. Hva fastslår Proposisjon 2.4.16 når $n = 5$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med 5. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.16. Hva fastslår Proposisjon 2.4.16 når $n = 10$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med 10. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.17. Hva fastslår Proposisjon 2.4.16 når $n = -12$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med -12. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.18. Hva fastslår Proposisjon 2.4.16 når $n = -5$? Hva er m i dette tilfellet? Gå gjennom beviset for Proposisjon 2.4.2 ved å erstatte n med -5. Hvilket at utsagnene (1) og (2) stemmer? Hva er k i dette tilfellet?

Oppgave O2.2.19. For hvert av de de følgende heltallene l og n, vis at $l \mid n$.

(1) $l = 19$, $n = 57$.

(2) $l = 6$, $n = -48$.

(3) $l = -21$, $n = 42$.

(4) $l = -26$, $n = -78$.

Oppgave O2.2.20. Hvilket steg i beviset for Proposisjon 2.6.21 ikke stemmer om vi antar at l er et heltall heller enn et naturlig tall?

Oppgave O2.2.21. Gi et eksempel for å vise at Proposisjon 2.8.8 ikke stemmer om vi bytter 1 med 3.

Oppgave O2.2.22. Gi et eksempel for å vise at Proposisjon 2.8.22 ikke stemmer om vi antar at $\mathsf{sfd}(l, n) = 3$.

3 Modulær aritmetikk

3.1 Kongruens

Merknad 3.1.1. Hva er klokka sju timer etter kl. 20? Selvfølgelig er den kl. 3. Vi sier ikke at den er kl. 27!

Etter 24 timer, begynner klokka på 0 igjen: midnatt er både kl. 24 og kl. 0. På en måte er derfor 24 «lik» 0 når vi ser på klokka. Ved å utvide dette litt, kan vi si at 3 er «lik» 27 når vi ser på ei klokke.

Denne måten å telle på kalles «aritmetikk modulo 24». Istedenfor å si at 3 er «lik» 27 når vi teller timene, sier vi at 3 er «kongruent til 27 modulo 24».

Vi kan telle på lignende vis ved å erstatte 24 med et hvilket som helst heltall. I dette kapittelet kommer vi til å studere disse måtene å telle på. Teorien er svært viktig i alle deler av tallteori, og i mange andre områder innen matematikk.

Definisjon 3.1.2. La n være et heltall slik at $n \neq 0$. La x og y være heltall. Da er x og y *kongruent modulo* n dersom $n \mid x - y$.

Merknad 3.1.3. Ut ifra Definisjon 2.5.1 er x og y kongruent modulo n hvis og bare hvis det finnes et heltall k slik at $x - y = kn$.

Terminologi 3.1.4. Hvis x og y er kongruent modulo n, sier vi ofte at x er *kongruent til* y *modulo* n.

Terminologi 3.1.5. «Modulo» forkortes ofte til «mod».

Notasjon 3.1.6. Hvis x og y er kongruent modulo n, skriver vi:

$$x \equiv y \pmod{n}.$$

Eksempel 3.1.7. Siden

$$27 - 3 = 24$$

og $24 \mid 24$, er

$$27 \equiv 3 \pmod{24}.$$

Eksempel 3.1.8. Siden

$$24 - 0 = 24$$

og $24 \mid 24$, er

$$24 \equiv 0 \pmod{24}.$$

Eksempel 3.1.9. Siden

$$53 - 5 = 48$$

og $24 \mid 48$, er

$$53 \equiv 5 \pmod{24}.$$

Eksempel 3.1.10. Siden

$$5 - 3 = 2$$

og $2 \mid 2$ er

$$5 \equiv 3 \pmod{2}.$$

Eksempel 3.1.11. Siden

$$57 - 13 = 44$$

og $2 \mid 44$, er

$$57 \equiv 13 \pmod{2}.$$

Eksempel 3.1.12. Siden

$$21 - 35 = -14$$

og $2 \mid -14$, er

$$21 \equiv 35 \pmod{2}.$$

Eksempel 3.1.13. Siden

$$40 - 124 = -84$$

og $2 \mid -84$, er

$$40 \equiv 124 \pmod{2}.$$

Eksempel 3.1.14. Siden

$$-17 - 21 = -38$$

og $2 \mid -38$, er

$$-17 \equiv 21 \pmod{2}.$$

Eksempel 3.1.15. Siden

$$-22 - (-108) = -22 + 108 = 86$$

og $2 \mid 86$, er

$$-22 \equiv -108 \pmod{2}.$$

Eksempel 3.1.16. Siden

$$-12 - (-4) = -12 + 4 = -8$$

og $2 \mid -8$, er

$$-12 \equiv -4 \pmod{2}.$$

Eksempel 3.1.17. Siden

$$11 - 5 = 6$$

og $3 \mid 6$, er

$$11 \equiv 5 \pmod{3}.$$

Eksempel 3.1.18. Siden

$$0 - 27 = -27$$

og $3 \mid -27$, er

$$0 \equiv 27 \pmod{3}.$$

Eksempel 3.1.19. Siden

$$14 - 17 = -3$$

og $3 \mid -3$, er

$$14 \equiv 17 \pmod{3}.$$

Eksempel 3.1.20. Siden

$$14 - 17 = -3$$

og $3 \mid -3$, er

$$14 \equiv 17 \pmod{3}.$$

Eksempel 3.1.21. Siden

$$-32 - 25 = -57$$

og $3 \mid -57$, er

$$-32 \equiv 25 \pmod{3}.$$

Eksempel 3.1.22. Siden

$$19 - (-59) = 19 + 59 = 78$$

og $3 \mid 78$, er

$$19 \equiv -59 \pmod{3}.$$

Eksempel 3.1.23. Siden

$$-23 - (-11) = -23 + 11 = -12$$

og $3 \mid -12$, er

$$-23 \equiv -11 \pmod{3}.$$

Eksempel 3.1.24. Siden

$$89 - 17 = 72$$

og $-8 \mid 72$, er

$$89 \equiv 17 \pmod{-8}.$$

Eksempel 3.1.25. Siden

$$33 - 25 = 8$$

og $-8 \mid 8$, er

$$33 \equiv 25 \pmod{-8}.$$

Eksempel 3.1.26. Siden

$$14 - 54 = -40$$

og $-8 \mid -40$, er

$$14 \equiv 54 \pmod{-8}.$$

Eksempel 3.1.27. Siden

$$-12 - 36 = -48$$

og $-8 \mid -48$, er

$$-12 \equiv 36 \pmod{-8}.$$

Eksempel 3.1.28. Siden

$$-17 - (-49) = 32$$

og $-8 \mid 32$, er

$$-17 \equiv -49 \pmod{-8}.$$

3.2 Grunnleggende proposisjoner om kongruens

Proposisjon 3.2.1. La n være et naturlig tall. La x være et heltall. Da finnes det et heltall r slik at de følgende er sanne:

(I) $x \equiv r \pmod{n}$;

(II) $0 \leq r < n$.

Bevis. Ut ifra Korollar 2.2.11 finnes det heltall k og r slik at:

(1) $x = kn + r$;

(2) $0 \leq r < n$.

Det følger fra (1) at

$$x - r = kn,$$

altså at

$$n \mid x - r.$$

Dermed er $x \equiv r \pmod{n}$.

□

Merknad 3.2.2. Proposisjon 3.2.1 fastslår at hvert heltall er kongruent modulo n til ett av heltallene 0, 1, 2, ..., $n - 1$.

Merknad 3.2.3. Gitt et naturlig tall n og et heltall x, fastlår beviset for Proposisjon 3.2.1 at vi kan finne r ved å benytte divisjonsalgoritmen: r er resten vi får ved å dele x med n.

Eksempel 3.2.4. Vi har:

$$22 = 7 \cdot 3 + 1,$$

altså $3 \mid 22 - 1$. Dermed er $22 \equiv 1 \pmod{3}$.

Eksempel 3.2.5. Vi har:

$$124 = 7 \cdot 17 + 8,$$

altså $17 \mid 124 - 8$. Dermed er $124 \equiv 8 \pmod{17}$.

Eksempel 3.2.6. Vi har

$$48 = 8 \cdot 6,$$

altså $6 \mid 48 - 0$. Dermed er $48 \equiv 0 \pmod{6}$.

Eksempel 3.2.7. Vi har:

$$-17 = (-4) \cdot 5 + 3,$$

altså $5 \mid -17 - 3$. Dermed er $-17 \equiv 3 \pmod{5}$.

Eksempel 3.2.8. Vi har:

$$-23 = (-6) \cdot 4 + 1,$$

altså $4 \mid -23 - 1$. Dermed er $-23 \equiv 1 \pmod{4}$.

Eksempel 3.2.9. Vi har:

$$-63 = (-9) \cdot 7,$$

altså $7 \mid -63 + 0$. Dermed er $-63 \equiv 0 \pmod{7}$.

Korollar 3.2.10. La n være et heltall slik at $n \neq 0$. La x være et heltall. Da finnes det et heltall r slik at de følgende er sanne:

(I) $x \equiv r \pmod{n}$;

(II) $0 \leq r < |n|$.

Bevis. Ett av følgende utsagn er sant:

(A) $n > 0$;

(B) $n < 0$.

Anta først at (A) er sant. Da følger utsagnet umiddelbart fra Proposisjon 3.2.1.

Anta nå at (B) er sant. Da er $-n$ et naturlig tall. Det følger fra Proposisjon 3.2.1 at det finnes et heltall r slik at:

(1) $x \equiv r \pmod{-n}$;

(2) $0 \leq r < -n$.

Det følger fra (1) og Proposisjon 3.2.19 at

$$x \equiv r \pmod{n}.$$

Siden $n < 0$, er i tillegg $|n| = -n$. Dermed er

$$0 \leq r < |n|.$$

□

Proposisjon 3.2.11. La n være et heltall slik at $n \neq 0$. La r og s være heltall sik at $0 \leq r < |n|$ og $0 \leq s < |n|$. Dersom $r \equiv s \pmod{n}$, er $r = s$.

Bevis. Siden $r \equiv s \pmod{n}$, har vi $n \mid r - s$. Dermed finnes det et heltall k slik at

$$r - s = kn,$$

altså

$$r = kn + s.$$

I tillegg er

$$r = 0 \cdot k + r.$$

Det følger fra Korollar 2.2.20 at $r = s$. □

Merknad 3.2.12. Vi ønsker å manipulere kongruenser på en lignende måte som vi manipulere likheter. I resten av denne delen av kapittelet skal vi bevise at dette er gyldig. Når du leser bevisene, la merke til at vi bygger på de grunnleggende proposisjonene i §2.5 av Kapittel 2.

Proposisjon 3.2.13. La n være et heltall slik at $n \neq 0$. La x være et heltall. Da er $x \equiv 0 \pmod{n}$ hvis og bare hvis $n \mid x$.

Bevis. Vi har: $x \equiv 0 \pmod{n}$ hvis og bare hvis $n \mid x - 0$, altså hvis og bare hvis $n \mid x$. □

Eksempel 3.2.14. Siden $3 \mid 18$, er $18 \equiv 0 \pmod{3}$.

Eksempel 3.2.15. Siden $5 \mid -20$, er $-20 \equiv 0 \pmod{5}$.

Proposisjon 3.2.16. La n være et heltall slik at $n \neq 0$. La x være et heltall. Da er $x \equiv x \pmod{n}$.

Bevis. Siden $x - x = 0$ og $n \mid 0$, er $x \equiv x \pmod{n}$. □

Eksempel 3.2.17. Vi har: $3 \equiv 3 \pmod{5}$.

Eksempel 3.2.18. Vi har: $-11 \equiv -11 \pmod{7}$.

Proposisjon 3.2.19. La n være et heltall slik at $n \neq 0$. La x og y være heltall. Anta at $x \equiv y \pmod{n}$. Da er $x \equiv y \pmod{-n}$.

Bevis. Siden $x \equiv y \pmod{n}$, har vi: $n \mid x - y$. Det følger fra Proposisjon 2.5.9 at $-n \mid x - y$. Dermed er $x \equiv y \pmod{-n}$.

□

Eksempel 3.2.20. Siden

$$32 - 17 = 15$$

og $5 \mid 15$, er

$$32 \equiv 17 \pmod{5}.$$

Derfor fastslår Proposisjon 3.2.19 at

$$32 \equiv 17 \pmod{-5}.$$

Eksempel 3.2.21. Siden

$$-6 - (-36) = 30$$

og $-5 \mid 30$, er

$$-6 \equiv -36 \pmod{-5}.$$

Derfor fastslår Proposisjon 3.2.19 at

$$-6 \equiv -36 \pmod{5}.$$

Korollar 3.2.22. La n være et heltall slik at $n \neq 0$. La x og y være heltall. Da er $x \equiv y \pmod{n}$ hvis og bare hvis $x \equiv y \pmod{-n}$.

Bevis. Følger umiddelbart fra Proposisjon 3.2.19. □

Merknad 3.2.23. Siden Korollar 3.2.22 stemmer, kommer n i de aller fleste eksemplene videre til å bli et naturlig tall.

Proposisjon 3.2.24. La n være et heltall slik at $n \neq 0$. La x og y være heltall. Anta at $x \equiv y \pmod{n}$. Da er $y \equiv x \pmod{n}$.

Bevis. Siden $x \equiv y \pmod{n}$, er $n \mid x-y$. Det følger fra Proposisjon 2.5.12 at $n \mid -(x-y)$, altså at $n \mid y - x$. □

Eksempel 3.2.25. Siden

$$32 - 18 = 14$$

og $7 \mid 14$, er

$$32 \equiv 18 \pmod{7}.$$

Derfor fastslår Proposisjon 3.2.24 at

$$18 \equiv 32 \pmod{7}.$$

Eksempel 3.2.26. Siden

$$3 - 7 = -4$$

og $4 \mid -4$, er

$$3 \equiv 7 \pmod{4}.$$

Derfor fastslår Proposisjon 3.2.24 at

$$7 \equiv 3 \pmod{4}.$$

Eksempel 3.2.27. Siden

$$-8 - 24 = -32$$

og $16 \mid -32$, er

$$-8 \equiv 24 \pmod{16}.$$

Derfor fastslår Proposisjon 3.2.24 at

$$24 \equiv -8 \pmod{16}.$$

Eksempel 3.2.28. Siden

$$9 - (-11) = 9 + 11 = 20$$

og $5 \mid 20$, er

$$9 \equiv -11 \pmod{5}.$$

Derfor fastslår Proposisjon 3.2.24 at

$$-11 \equiv 9 \pmod{5}.$$

Eksempel 3.2.29. Siden

$$-5 - (-9) = -5 + 9 = 4$$

og $2 \mid 4$, er

$$-5 \equiv -9 \pmod{2}.$$

Derfor fastslår Proposisjon 3.2.24 at

$$-9 \equiv -5 \pmod{2}.$$

Korollar 3.2.30. La n være et heltall slik at $n \neq 0$. La x være et heltall. Da er $0 \equiv x \pmod{n}$ hvis og bare hvis $n \mid x$.

Bevis. Følger umiddelbart fra Proposisjon 3.2.13 og Proposisjon 3.2.24. □

Eksempel 3.2.31. Siden $7 \mid 21$, er $0 \equiv 21 \pmod{7}$.

Eksempel 3.2.32. Siden $6 \mid -48$, er $0 \equiv -48 \pmod{6}$.

Proposisjon 3.2.33. La n være et heltall slik at $n \neq 0$. La x, y, og z være heltall. Anta at $x \equiv y \pmod{n}$, og at $y \equiv z \pmod{n}$. Da er $x \equiv z \pmod{n}$.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $x \equiv y \pmod{n}$, er $n \mid x - y$.

(2) Siden $y \equiv z \pmod{n}$, er $n \mid y - z$.

Det følger fra (1), (2), og Proposisjon 2.5.24 at $n \mid (x - y) + (y - z)$, altså at $n \mid x - z$. Dermed er $x \equiv z \pmod{n}$. □

Eksempel 3.2.34. Siden

$$19 - (-8) = 27$$

og $3 \mid 27$, er $19 \equiv -8 \pmod{3}$. Siden

$$(-8) - 64 = -72$$

og $3 \mid 72$, er $-8 \equiv 64 \pmod{3}$. Derfor fastslår Proposisjon 3.2.33 at $19 \equiv 64 \pmod{3}$.

Eksempel 3.2.35. Siden

$$-9 - (-59) = 50$$

og $5 \mid 50$, er $-9 \equiv -59 \pmod{5}$. Siden

$$(-59) - 61 = -120$$

og $5 \mid 120$, er $-59 \equiv 61 \pmod{5}$. Derfor fastslår Proposisjon 3.2.33 at $-9 \equiv 61 \pmod{5}$.

Proposisjon 3.2.36. La n være et heltall slik at $n \neq 0$. La x, y, x', og y' være heltall. Anta at $x \equiv y \pmod{n}$, og at $x' \equiv y' \pmod{n}$. Da er $x + x' \equiv y + y' \pmod{n}$.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $x \equiv y \pmod{n}$, er $n \mid x - y$.

(2) Siden $x' \equiv y' \pmod{n}$, er $n \mid x' - y'$.

Det følger fra (1), (2), og Proposisjon 2.5.24 at

$$n \mid (x - y) + (x' - y'),$$

altså at

$$n \mid (x + x') - (y + y').$$

Dermed er $x + x' \equiv y + y' \pmod{n}$. □

Eksempel 3.2.37. Siden

$$13 - 5 = 8$$

og $4 \mid 8$, er $13 \equiv 5 \pmod{4}$. Siden

$$23 - (-17) = 40$$

og $4 \mid 40$, er $23 \equiv -17 \pmod{4}$. Derfor fastslår Proposisjon 3.2.36 at

$$13 + 23 \equiv 5 + (-17) \pmod{4},$$

altså at

$$36 \equiv -12 \pmod{4}.$$

Eksempel 3.2.38. Siden

$$(-16) - 17 = -33$$

og $11 \mid -33$, er $-16 \equiv 17 \pmod{11}$. Siden

$$(-34) - (-56) = 22$$

og $11 \mid 22$, er $-34 \equiv -56 \pmod{11}$. Derfor fastslår Proposisjon 3.2.36 at

$$(-16) + (-34) \equiv 17 + (-56) \pmod{5},$$

altså at

$$-50 \equiv -39 \pmod{11}.$$

Korollar 3.2.39. La n være et heltall slik at $n \neq 0$. La x, y, og z være heltall. Anta at $x \equiv y \pmod{n}$. Da er $x + z \equiv y + z \pmod{n}$.

Bevis. Ut ifra Proposisjon 3.2.16 er $z \equiv z \pmod{n}$. Ved å la både x' og y' være z, følger dermed utsagnet umiddelbart fra Proposisjon 3.2.36. □

Eksempel 3.2.40. Siden

$$18 - 12 = 6$$

og $2 \mid 6$, er $18 \equiv 12 \pmod{2}$. Derfor fastslår Korollar 3.2.39 at

$$18 + 15 \equiv 12 + 15 \pmod{2},$$

altså at

$$33 \equiv 27 \pmod{2}.$$

Eksempel 3.2.41. Siden

$$(-8) - (-23) = 15$$

og $5 \mid 15$, er $-8 \equiv -23 \pmod{5}$. Derfor fastslår Korollar 3.2.39 at

$$-8 + 13 \equiv -23 + 13 \pmod{5},$$

altså at

$$5 \equiv -10 \pmod{5}.$$

Proposisjon 3.2.42. La n være et heltall slik at $n \neq 0$. La x, y, x', og y' være heltall. Anta at $x \equiv y \pmod{n}$, og at $x' \equiv y' \pmod{n}$. Da er $x \cdot x' \equiv y \cdot y' \pmod{n}$.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $x \equiv y \pmod{n}$, er $n \mid x - y$. Dermed finnes det et heltall k slik at $x - y = kn$, altså $x = y + kn$.

(2) Siden $x' \equiv y' \pmod{n}$, er $n \mid x' - y'$. Dermed finnes det et heltall k' slik at $x' - y' = k'n$, altså $x' = y' + k'n$.

Det følger fra (1) og (2) at

$$\begin{aligned} x \cdot x' &= (y + kn) \cdot (y' + k'n) \\ &= y \cdot y' + k \cdot k' \cdot n + k' \cdot y \cdot n + k \cdot y' \cdot n \\ &= y \cdot y' + (k \cdot k' + k' \cdot y + k' \cdot y)n. \end{aligned}$$

Dermed er

$$x \cdot x' - y \cdot y' = (k \cdot k' + k' \cdot y + k' \cdot y)n.$$

Siden k, k', y, og y' er heltall, er $k \cdot k' + k' \cdot y + k' \cdot y$ et heltall. Således har vi beviset at

$$n \mid x \cdot x' + y \cdot y'.$$

Vi konkluderer at

$$x \cdot x' \equiv y \cdot y' \pmod{n}.$$

□

Eksempel 3.2.43. Siden

$$20 - (-16) = 36$$

og $3 \mid 36$, er $20 \equiv -16 \pmod{3}$. Siden

$$(-41) - 4 = -45$$

og $3 \mid -45$, er $-41 \equiv 4 \pmod{3}$. Derfor fastslår Proposisjon 3.2.42 at

$$20 \cdot (-41) \equiv (-16) \cdot 4 \pmod{3},$$

altså at

$$-820 \equiv -64 \pmod{3}.$$

Eksempel 3.2.44. Siden

$$(-38) - (-17) = -21$$

og $7 \mid -21$, er $-38 \equiv -17 \pmod{7}$. Siden

$$3 - 10 = -7$$

og $7 \mid -7$, er $3 \equiv 10 \pmod{7}$. Derfor fastslår Proposisjon 3.2.42 at

$$(-38) \cdot 3 \equiv (-17) \cdot 10 \pmod{7},$$

altså at

$$-114 \equiv -170 \pmod{7}.$$

Korollar 3.2.45. La n være et heltall slik at $n \neq 0$. La x, y, og z være heltall. Anta at $x \equiv y \pmod{n}$. Da er $x \cdot z \equiv y \cdot z \pmod{n}$.

Bevis. Ut ifra Proposisjon 3.2.16 er $z \equiv z \pmod{n}$. Ved å la både x' og y' være z, følger dermed utsagnet umiddelbart fra Proposisjon 3.2.42. □

Eksempel 3.2.46. Siden

$$13 - 24 = -11$$

og $11 \mid -11$, er $13 \equiv 24 \pmod{11}$. Derfor fastslår Korollar 3.2.45 at

$$13 \cdot (-3) \equiv 24 \cdot (-3) \pmod{11},$$

altså at

$$-39 \equiv -72 \pmod{11}.$$

Eksempel 3.2.47. Siden

$$17 - (-7) = 24$$

og $6 \mid 24$, er $17 \equiv -7 \pmod{6}$. Derfor fastslår Korollar 3.2.45 at

$$17 \cdot 3 \equiv (-7) \cdot 3 \pmod{6},$$

altså at

$$51 \equiv -21 \pmod{6}.$$

Proposisjon 3.2.48. La n være et heltall slik at $n \neq 0$. La x være et heltall, og la t være et naturlig tall. Anta at $x \equiv y \pmod{n}$. Da er $x^t \equiv y^t \pmod{n}$.

Bevis. Først sjekker vi om proposisjonen er sann når $t = 1$. Ut ifra antakelsen at

$$x \equiv y \pmod{n},$$

er dette sant.

Anta nå at proposisjonen har blitt bevist når $t = m$, hvor m er et gitt naturlig tall. Således har det blitt bevist at

$$x^m \equiv y^m \pmod{n}.$$

Det følger fra dette, antakelsen at

$$x \equiv y \pmod{n},$$

og Proposisjon 3.2.42, at

$$x^m \cdot x \equiv y^m \cdot y \pmod{n},$$

altså at

$$x^{m+1} \equiv y^{m+1} \pmod{n}.$$

Dermed er proposisjonen sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann for et hvilket som helst naturlig tall n. □

Eksempel 3.2.49. Siden $3 - 5 = -2$ og $2 \mid -2$, er $3 \equiv 5 \pmod 3$. Derfor fastslår Proposisjon 3.2.48 at

$$3^4 \equiv 5^4 \pmod 2,$$

altså at

$$81 \equiv 625 \pmod 2.$$

Eksempel 3.2.50. Siden $(-8) - (-5) = -3$ og $3 \mid -3$, er $-8 \equiv -5 \pmod 3$. Derfor fastslår Proposisjon 3.2.48 at

$$(-8)^2 \equiv (-5)^2 \pmod 3,$$

altså at

$$64 \equiv 25 \pmod 3.$$

Proposisjon 3.2.51. La n være et heltall slik at $n \neq 0$. La x og y være heltall. La l være et heltall slik at $l \neq 0$. Anta at $x \equiv y \pmod n$. Da er $lx \equiv ly \pmod{ln}$.

Bevis. Siden $x \equiv y \pmod n$, har vi: $n \mid x - y$. Dermed finnes det et heltall k slik at $x - y = kn$. Da er

$$l(x - y) = lkn,$$

altså

$$lx - ly = k(ln).$$

Således har vi: $ln \mid lx - ly$. Derfor er

$$lx \equiv ly \pmod{ln}.$$

□

Eksempel 3.2.52. Siden $9 - 23 = -14$ og $7 \mid -14$, er $9 \equiv 23 \pmod 7$. Derfor fastslår Proposisjon 3.2.51 at

$$3 \cdot 9 \equiv 3 \cdot 23 \pmod{3 \cdot 7},$$

altså

$$27 \equiv 69 \pmod{21}.$$

Eksempel 3.2.53. Siden $-11 - (-21) = 20$ og $5 \mid 20$, er $-11 \equiv -21 \pmod 5$. Derfor fastslår Proposisjon 3.2.51 at

$$8 \cdot (-11) \cdot 8 \cdot (-21) \equiv 8 \cdot (-21) \pmod{8 \cdot 5},$$

altså

$$-88 \equiv -168 \pmod{40}.$$

Proposisjon 3.2.54. La n være et heltall slik at $n \neq 0$. La x og y være heltall. La l være et heltall slik at $l \neq 0$, $l \mid y$, og $l \mid n$. Anta at $x \equiv y \pmod n$. Da er $x \equiv 0 \pmod l$.

Bevis. Siden $l \mid y$, finnes det et heltall k slik at $y = kl$. Siden $l \mid n$, finnes det et heltall k' slik at $n = k'l$. Siden $x \equiv y \pmod{n}$, har vi: $n \mid x - y$. Dermed finnes det et heltall k'' slik at $x - y = k''n$. Vi har:

$$\begin{aligned} x &= y + k''n \\ &= kl + k''k'l \\ &= (k + k''k')l. \end{aligned}$$

Siden k, k', og k'' er heltall, er $k+k''k'$ et heltall. Dermed har vi: $l \mid x$. Ut ifra Proposisjon 3.2.13, følger det at $x \equiv 0 \pmod{l}$.

□

Eksempel 3.2.55. Siden $18 - 6 = 12$ og $12 \mid 12$, er $18 \equiv 6 \pmod{12}$. I tillegg har vi: $12 = 4 \cdot 3$ og $6 = 2 \cdot 3$. Derfor fastslår Proposisjon 3.2.54 at $18 \equiv 0 \pmod{3}$, som er riktignok sant.

Eksempel 3.2.56. Siden $-42 - 6 = -48$ og $24 \mid -48$, er $-42 \equiv 6 \pmod{24}$. I tillegg har vi: $24 = 12 \cdot 2$ og $6 = 3 \cdot 2$. Derfor fastslår Proposisjon 3.2.54 at $-42 \equiv 0 \pmod{2}$, som er riktignok sant.

Proposisjon 3.2.57. La m og n være heltall slik at $m \neq 0$ og $n \neq 0$. Anta at $m \mid n$. La x og y være heltall slik at

$$x \equiv y \pmod{n}.$$

Da er

$$x \equiv y \pmod{m}.$$

Bevis. Siden

$$x \equiv z \pmod{n},$$

har vi: $n \mid x - z$. Siden $m \mid n$, følger det fra Proposisjon 2.5.27 at

$$m \mid x - z.$$

Vi konkluderer at

$$x \equiv z \pmod{m}.$$

□

Eksempel 3.2.58. Siden $64 - 12 = 52$ og $26 \mid 52$, er

$$64 \equiv 12 \pmod{26}.$$

Siden $13 \mid 26$, fastslår Proposisjon 3.2.57 at

$$64 \equiv 12 \mod 13.$$

Siden $64 - 12 = 52$ og $13 \mid 52$, er dette riktignok sant.

Eksempel 3.2.59. Siden $-7-(-19)=12$ og $4 \mid 12$, er

$$-7 \equiv -19 \pmod{4}.$$

Siden $2 \mid 4$, fastslår Proposisjon 3.2.57 at

$$-7 \equiv -19 \mod 2.$$

Siden $-7-(-19)=12$ og $2 \mid 12$, er dette riktignok sant.

Proposisjon 3.2.60. La m og n være heltall slik at $m \neq 0$ og $n \neq 0$. Anta at $m \mid n$. La x, y, og z være heltall. Anta at

$$x \equiv y \pmod{m}.$$

Dersom

$$x \equiv z \pmod{n},$$

finnes det et heltall i slik at

$$z = y + im \pmod{n}.$$

Bevis. Ut ifra Proposisjon 3.2.57 er

$$x \equiv z \pmod{m}.$$

Det følger fra Proposisjon 3.2.24 at

$$z \equiv x \pmod{m}.$$

Siden i tillegg

$$x \equiv y \pmod{m},$$

følger det fra Proposisjon 3.2.33 at

$$z \equiv y \pmod{m}.$$

Da har vi: $m \mid z-y$. Således finnes det et heltall i slik at $z-y=im$, altså slik at $z=y+im$. □

Eksempel 3.2.61. Siden $13-4=9$ og $3 \mid 9$, er

$$13 \equiv 4 \pmod{3}.$$

Siden $13-25=-12$ og $6 \mid -12$, er

$$13 \equiv 25 \pmod{6}.$$

Siden $3 \mid 6$, fastslår Proposisjon 3.2.60 at det er et heltall i slik at $25=4+3i$. Det er riktignok sant at $25=4+3\cdot 7$.

Eksempel 3.2.62. Siden $17 - (-13) = 30$ og $5 \mid 30$, er

$$17 \equiv -13 \pmod{5}.$$

Siden $17 - 67 = -40$ og $20 \mid -40$, er

$$17 \equiv 67 \pmod{20}.$$

Siden $5 \mid 20$, fastslår Proposisjon 3.2.60 at det er et heltall i slik at $67 = -13 + 5i$. Det er riktignok sant at $67 = -13 + 5 \cdot 16$.

Korollar 3.2.63. La m og n være heltall slik at $m \neq 0$ og $n \neq 0$. Anta at $m \mid n$. La x, y, og z være heltall. Anta at

$$x \equiv y \pmod{m}.$$

Dersom

$$x \equiv z \pmod{n},$$

finnes det et heltall i slik at $0 \leq y + im < n$ og

$$z \equiv y + im \pmod{n}.$$

Bevis. Følger umiddelbart fra Proposisjon 3.2.60 og Proposisjon 3.2.1. □

Eksempel 3.2.64. La z være et heltall slik at

$$z \equiv 2 \pmod{5}.$$

Korollar 3.2.63 fastslår at enten

$$z \equiv 2 \pmod{10}$$

eller

$$z \equiv 7 \pmod{10},$$

siden 2 og 7 er de eneste heltallene som er større enn eller like 0, mindre enn 10 og like $2 + 5i$ for noen heltall i. For eksempel er

$$12 \equiv 2 \pmod{5},$$

og

$$12 \equiv 2 \pmod{10}.$$

På en annen side er

$$17 \equiv 2 \pmod{5},$$

og

$$17 \equiv 7 \pmod{10}.$$

Eksempel 3.2.65. La z være et heltall slik at

$$z \equiv 3 \pmod 4.$$

Korollar 3.2.63 fastslår at ett av følgende er sant:

(1) $z \equiv 3 \pmod{16}$;

(2) $z \equiv 7 \pmod{16}$;

(3) $z \equiv 11 \pmod{16}$;

(4) $z \equiv 15 \pmod{16}$.

Heltallene 3, 7, 11, og 15 er nemlig de eneste heltallene som er større enn eller like 0, mindre enn 16 og like $3 + 4i$ for noen heltall i. For eksempel har vi:

(1) $19 \equiv 3 \pmod 4$ og $19 \equiv 3 \pmod{16}$;

(2) $55 \equiv 3 \pmod 4$ og $55 \equiv 7 \pmod{16}$;

(3) $91 \equiv 3 \pmod 4$ og $91 \equiv 11 \pmod{16}$;

(4) $31 \equiv 3 \pmod 4$ og $31 \equiv 15 \pmod{16}$.

Proposisjon 3.2.66. La n være et heltall. La k være et naturlig tall. La x være et heltall slik at

$$x \equiv 0 \pmod n.$$

Da er

$$x^k \equiv 0 \pmod{n^k}.$$

Bevis. Siden

$$x \equiv 0 \pmod n,$$

har vi: $n \mid x$. Det følger fra Proposisjon 2.5.15 at

$$n^k \mid x^k,$$

altså at

$$x^k \equiv 0 \pmod{n^k}.$$

□

Eksempel 3.2.67. Siden

$$12 \equiv 0 \pmod 3,$$

fastlår Proposisjon 3.2.66 at

$$12^2 \equiv 0 \pmod{3^2},$$

altså at

$$144 \equiv 0 \pmod 9.$$

Siden $144 = 16 \cdot 9$ er dette riktignok sant.

Eksempel 3.2.68. Siden

$$-10 \equiv 0 \pmod 5,$$

fastlår Proposisjon 3.2.66 at

$$-10^3 \equiv 0 \pmod{5^3},$$

altså at

$$-1000 \equiv 0 \pmod{125}.$$

Siden $-1000 = -8 \cdot 125$ er dette riktignok sant.

Proposisjon 3.2.69. La n være et heltall. La x og y være heltall slik at

$$x \equiv y \pmod n.$$

La z være et heltall. Da er $\mathsf{sfd}(x, n) = \mathsf{sfd}(y, n)$.

Bevis. Siden

$$x \equiv y \pmod n,$$

har vi: $n \mid x - y.$. Dermed finnes det et heltall k slik at $x - y = kn$, altså $y = kn + x$. Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(y, n) = \mathsf{sfd}(n, x)$, altså $\mathsf{sfd}(y, n) = \mathsf{sfd}(x, n)$. □

Eksempel 3.2.70. Siden

$$18 \equiv 10 \pmod 8,$$

fastslår Proposisjon 3.2.69 at $\mathsf{sfd}(18, 8) = \mathsf{sfd}(10, 8)$. Siden $\mathsf{sfd}(18, 8) = 2$ og $\mathsf{sfd}(10, 8) = 2$, er dette riktignok sant.

Eksempel 3.2.71. Siden

$$56 \equiv -98 \pmod{77},$$

fastslår Proposisjon 3.2.69 at $\mathsf{sfd}(56, 77) = \mathsf{sfd}(-98, 77)$. Siden $\mathsf{sfd}(56, 77) = 7$ og $\mathsf{sfd}(-98, 77) = 7$, er dette riktignok sant.

3.3 Utregning ved hjelp av kongruenser

Merknad 3.3.1. Vi skal nå se at de algebraiske manipulasjonene med kongruenser, som vi nå har hevist er gyldige, kan hjelpe oss å vise at utsagner om store heltall er sanne uten å kruke en kalkulator eller en datamaskin.

Proposisjon 3.3.2. Heltallet $2^{20} - 1$ er delelig med 41.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $32 - (-9) = 41$, og siden $41 \mid 41$, er $32 \equiv -9 \pmod{41}$. Siden $32 = 2^5$, har vi dermed:

$$2^5 \equiv -9 \pmod{41}.$$

(2) Det følger fra (1) og Proposisjon 3.2.48 at

$$\left(2^5\right)^4 \equiv (-9)^4 \pmod{41}.$$

Siden

$$(-9)^4 = 9^4 = (9)^2 \cdot (9)^2 = 81 \cdot 81,$$

har vi dermed:

$$2^{20} \equiv 81 \cdot 81 \pmod{41}.$$

(3) Siden $81 - (-1) = 82$, og siden $41 \mid 82$, er $81 \equiv -1 \pmod{41}$.

(4) Det følger fra (3) og Proposisjon 3.2.42 at $81 \cdot 81 \pmod{}() - 1) \cdot (-1) \pmod{41}$¸ altså at $81 \cdot 81 = 1 \pmod{41}$.

(5) Det følger fra (2), (3), og Proposisjon 3.2.33 at $2^{20} \equiv 1 \pmod{41}$.

(6) Det følger fra (5) og Korollar 3.2.39 at

$$2^{20} - 1 \equiv 1 - 1 \pmod{41},$$

altså at

$$2^{20} - 1 \equiv 0 \pmod{41}.$$

Det følger fra (6) og Proposisjon 3.2.13 at $41 \mid 2^{20} - 1$. □

Proposisjon 3.3.3. Heltallet $111^{333} + 333^{111}$ er delelig med 7.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $111 - (-1) = 112$, og siden $7 \mid 112$, er $111 \equiv -1 \pmod{7}$.

(2) Det følger fra (1) og Proposisjon 3.2.48 at

$$111^{333} \equiv (-1)^{333} \pmod{7},$$

altså at

$$111^{333} \equiv -1 \pmod{7}.$$

(3) Det følger fra (1) og Korollar 3.2.45 at

$$3 \cdot 111 \equiv 3 \cdot (-1) \pmod{7},$$

altså at

$$333 \equiv -3 \pmod{7}.$$

(4) Det følger fra (3) og Proposisjon 3.2.48 at

$$(333)^3 \equiv (-3)^3 \pmod{7},$$

altså at

$$(333)^3 \equiv -27 \pmod{7}.$$

(5) Siden

$$-27 - 1 = -28,$$

og siden $7 \mid 28$, er

$$-27 \equiv 1 \pmod{7}.$$

(6) Det følger fra (4), (5), og Proposisjon 3.2.33 at

$$(333)^3 \equiv 1 \pmod{7}.$$

(7) Det følger fra (7) og Proposisjon 3.2.48 at

$$\left((333)^3\right)^{37} \equiv 1^{37} \pmod{7},$$

altså at

$$333^{111} \equiv 1 \pmod{7}.$$

(8) Det følger fra (2), (7), og Proposisjon 3.2.36 at

$$111^{333} + 333^{111} \equiv (-1) + 1 \pmod{7},$$

altså at

$$111^{333} + 333^{111} \equiv 0 \pmod{7}.$$

Det følger fra (8) og Proposisjon 3.2.13 at $7 \mid 111^{333} + 333^{111}$. □

Proposisjon 3.3.4. Summen

$$1! + 2! + \cdots + 99! + 100!$$

er kongruent til 9 mod 12.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $4! = 4 \times 3 \times 2 \times 1 = 24$, og siden $12 \mid 24$, er $4! \equiv 0 \pmod{12}$.

(2) For hvert naturlig tall m slik at $4 < m \leq 100$, følger det fra (1) og Korollar 3.2.45 at

$$4! \cdot (5 \times \cdots \times m) \equiv 0 \cdot (5 \times \cdots \times m) \pmod{12},$$

altså at

$$m! \equiv 0 \pmod{12}.$$

(3) Fra (2) og Proposisjon 3.2.36 følger det at

$$1! + 2! + 3! + 4! + 5! + \cdots + 99! + 100! \equiv 1! + 2! + 3! + 0 + 0 + \cdots + 0 + 0 \pmod{12},$$

altså at

$$1! + 2! + \cdots + 99! + 100! \equiv 1! + 2! + 3! \pmod{12}.$$

(4) Siden

$$1! + 2! + 3! = 1 + 2 + 6 = 9$$

følger det fra (3) at

$$1! + 2! + \cdots + 99! + 100! \equiv 9 \pmod{12}.$$

□

Proposisjon 3.3.5. La t være et naturlig tall. Da er $3^{t+2} + 4^{2t+1}$ delelig med 13.

Bevis. Vi gjør følgende observasjoner.

(1) Vi har:

$$\begin{aligned} 3^{t+2} + 4^{2t+1} &= 3^t \cdot 9 + 4^{2t} \cdot 4 \\ &= 3^t \cdot 9 + \left(4^2\right)^t \cdot 4 \\ &= 3^t \cdot 9 + 16^t \cdot 4. \end{aligned}$$

(2) Siden $16 - 3 = 13$ og $13 \mid 13$, er $16 \equiv 3 \pmod{13}$.

(3) Det følger fra (2) og Proposisjon 3.2.48 at

$$16^t \equiv 3^t \pmod{13}.$$

(4) Det følger fra (3) og Korollar 3.2.45 at

$$16^t \cdot 4 \equiv 3^t \cdot 4 \pmod{13}.$$

(5) Det følger fra (4) og Korollar 3.2.39 at

$$3^t \cdot 9 + 16^t \cdot 4 \equiv 3^t \cdot 9 + 3^t \cdot 4 \pmod{13},$$

altså at

$$3^t \cdot 9 + 16^t \cdot 4 \equiv 3^t \cdot 13 \pmod{13}.$$

(6) Siden $13 \mid 3^t \cdot 13$, følger det fra Proposisjon 3.2.13 at $3^t \cdot 13 \equiv 0 \pmod{13}$.

(7) Det følger fra (5), (6), og Proposisjon 3.2.33 at

$$3^t \cdot 9 + 16^t \cdot 4 \equiv 0 \pmod{13}.$$

Det følger fra (1) og (7) at

$$3^{t+2} + 4^{2t+1} \equiv 0 \pmod{13}.$$

Det følger fra Proposisjon 3.2.13 at $13 \mid 3^{t+2} + 4^{2t+1}$.

□

Proposisjon 3.3.6. La x være et naturlig tall. Anta at det finnes et heltall n slik at $n \geq 0$ og

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0,$$

hvor, for hvert heltall i slik at $0 \leq i \leq n$, er x_i et heltall slik at $x_i \geq 0$. Da er x delelig med 9 hvis og bare hvis summen

$$x_0 + x_1 + \cdots + x_{n-1} + x_n$$

er delelig med 9.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $10 - 1 = 9$ og $9 \mid 9$, er $10 \equiv 1 \pmod 9$.

(2) La i være et heltall slik at $0 \leq i \leq n$. Det følger fra (1) og Proposisjon 3.2.48 at $10^i \equiv 1^i \pmod 9$, altså at
$$10^i \equiv 1 \pmod 9.$$

(3) Det følger fra (2) og Korollar 3.2.45 at $x_i \cdot 10^i \equiv x_i \cdot 1 \pmod 9$, altså at
$$x_i \cdot 10^i \equiv x_i \pmod 9.$$

(4) Det følger fra (3) og Proposisjon 3.2.36 at
$$\begin{aligned} &x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0 \\ &\equiv x_n + x_{n-1} + \cdots + x_1 + x_0 \pmod 9, \end{aligned}$$
altså at
$$x \equiv x_0 + x_1 + \cdots + x_{n-1} + x_n \pmod 9.$$

Anta at $9 \mid x$. Det følger fra Korollar 3.2.30 at $0 \equiv x \pmod 9$. Da følger det fra (4) og Proposisjon 3.2.33 at

$$0 \equiv x_0 + x_1 + \cdots + x_{n-1} + x_n \pmod 9.$$

Fra Proposisjon 3.2.13 deduserer vi at

$$9 \mid x_0 + x_1 + \cdots + x_{n-1} + x_n.$$

Dersom $9 \mid x$, har vi dermed bevist at

$$9 \mid x_0 + x_1 + \cdots + x_{n-1} + x_n.$$

Anta istedenfor at
$$9 \mid x_0 + x_1 + \cdots + x_{n-1} + x_n.$$

Det følger fra Proposisjon 3.2.13 at

$$x_0 + x_1 + \cdots + x_{n-1} + x_n \equiv 0 \pmod 9.$$

Da følger det fra (4) og Proposisjon 3.2.33 at

$$x \equiv 0 \pmod 9.$$

Fra Korollar 3.2.30 deduserer vi at $9 \mid x$. Dersom

$$9 \mid x_0 + x_1 + \cdots + x_{n-1} + x_n,$$

har vi dermed bevist at $9 \mid x$.

□

Merknad 3.3.7. Når vi skriver et heltall, skriver vi akkurat heltall x_0, …, x_n for noe heltall n, slik at ligningen i Proposisjon 3.3.6 stemmer. For eksempel har vi:

$$1354 = 1 \cdot 1000 + 3 \cdot 100 + 5 \cdot 10 + 4 \cdot 1,$$

altså

$$1354 = 1 \cdot 10^3 + 3 \cdot 10^2 + 5 \cdot 10^1 + 4 \cdot 10^0.$$

Med andre ord er x_i det i-te heltallet fra høyre, ved å telle fra 0.

Merknad 3.3.8. Ved å benytte divisjonsalgoritmen, kan det bevises formelt at, for hvert heltall x, finnes det et heltall n slik at $n \geq 0$ og

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0,$$

hvor, for hvert heltall i slik at $0 \leq i \leq n$, er x_i et heltall slik at $0 \leq x_i \leq 9$. Med andre ord, gjelder Proposisjon 3.3.6 for et hvilket som helst heltall x.

Det kan også bevises at heltallene n og x_0, x_1, …, x_n er de *eneste* slik at ligningen i Proposisjon 3.3.6 stemmer, og slik at $0 \leq x_i \leq 9$ for hvert i.

Imidlertid er disse bevisene ikke spesielt viktige fra et teoretisk synspunkt. Derfor skal vi hoppe over dem, og nøye oss med Proposisjon 3.3.6.

Terminologi 3.3.9. La x være et heltall. La n være et heltall slik at $n \geq 0$ og

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0,$$

hvor, for hvert heltall i slik at $0 \leq i \leq n$, er x_i et heltall slik at $0 \leq x_i \leq 9$. La i være et heltall slik at $0 \leq i \leq n$. Vi sier at x_i er et *siffer* av x.

Eksempel 3.3.10. Siden summen av sifrene i 72 er

$$7 + 2 = 9,$$

og siden $9 \mid 9$, fastslår Proposisjon 3.3.6 at $9 \mid 72$.

Eksempel 3.3.11. Siden summen av sifrene i 154872 er

$$1 + 5 + 4 + 8 + 7 + 2 = 27,$$

og siden $9 \mid 27$, fastslår Proposisjon 3.3.6 at $9 \mid 154872$.

Eksempel 3.3.12. Siden summen av sifrene i 76253 er

$$7 + 6 + 2 + 5 + 3 = 23,$$

og siden det ikke er sant at $9 \mid 23$, fastslår Proposisjon 3.3.6 at det ikke er sant at $9 \mid 76253$.

Eksempel 3.3.13. Siden summen av sifrene i 849 er

$$8 + 4 + 9 = 21,$$

og siden det ikke er sant at $9 \mid 21$, fastslår Proposisjon 3.3.6 at det ikke er sant at $9 \mid 849$.

Proposisjon 3.3.14. La x være et naturlig tall. Anta at det finnes et heltall n slik at $n \geq 0$ og

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0,$$

hvor, for hvert heltall i slik at $0 \leq i \leq n$, er x_i et heltall slik at $x_i \geq 0$. Da er x delelig med 11 hvis og bare hvis summen

$$x_0 - x_1 + \cdots + (-1)^{n-1} \cdot x_{n-1} + (-1)^n x_n$$

er delelig med 11.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $10 - (-1) = 11$ og $11 \mid 11$, er $10 \equiv -1 \pmod{11}$.

(2) La i være et heltall slik at $0 \leq i \leq n$. Det følger fra (1) og Proposisjon 3.2.48 at $10^i \equiv (-1)^i \pmod{11}$.

(3) Det følger fra (2) og Korollar 3.2.45 at $x_i \cdot 10^i \equiv x_i \cdot (-1)^i \pmod{11}$, altså at

$$x_i \cdot 10^i \equiv (-1)^i \cdot x_i \pmod{11}.$$

(4) Det følger fra (3) og Proposisjon 3.2.36 at

$$\begin{aligned} &x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0 \\ &\equiv (-1)^n \cdot x_n + (-1)^{n-1} x_{n-1} + \cdots + (-1)^1 \cdot x_1 + (-1)^0 \cdot x_0 \pmod{11}, \end{aligned}$$

altså at

$$x \equiv x_0 - x_1 + \cdots + (-1)^{n-1} x_{n-1} + (-1)^n x_n \pmod{11}.$$

Anta at $11 \mid x$. Det følger fra Korollar 3.2.30 at $0 \equiv x \pmod{11}$. Da følger det fra (4) og Proposisjon 3.2.33 at

$$0 \equiv x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n \pmod{11}.$$

Fra Proposisjon 3.2.13 deduserer vi at

$$11 \mid x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n.$$

Dersom $11 \mid x$, har vi dermed bevist at

$$11 \mid x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n.$$

Anta istedenfor at

$$11 \mid x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n.$$

Det følger fra Proposisjon 3.2.13 at

$$x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n \equiv 0 \pmod{11}.$$

Da følger det fra (4) og Proposisjon 3.2.33 at

$$x \equiv 0 \pmod{11}.$$

Fra Korollar 3.2.30 deduserer vi at $11 \mid x$. Dersom

$$11 \mid x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n,$$

har vi dermed bevist at $11 \mid x$.

□

Eksempel 3.3.15. Siden

$$1 - 2 + 1 = 0,$$

og siden $11 \mid 0$, fastslår Proposisjon 3.3.6 at $11 \mid 121$.

Eksempel 3.3.16. Siden

$$3 - 5 + 7 - 0 + 6 = 11,$$

og siden $11 \mid 11$, fastslår Proposisjon 3.3.6 at $11 \mid 60753$.

Eksempel 3.3.17. Siden

$$2 - 1 + 8 - 2 + 9 - 1 + 7 = 22,$$

og siden $11 \mid 22$, fastslår Proposisjon 3.3.6 at $11 \mid 7192812$.

Eksempel 3.3.18. Siden

$$9 - 1 + 3 - 7 + 4 = 8,$$

og siden det ikke er sant at $11 \mid 8$, fastslår Proposisjon 3.3.6 at det ikke er sant at $11 \mid 47319$.

Eksempel 3.3.19. Siden

$$7 - 3 + 8 = 12,$$

og siden det ikke er sant at $11 \mid 12$, fastslår Proposisjon 3.3.6 at det ikke er sant at $11 \mid 837$.

3.4 Lineære kongruenser

Terminologi 3.4.1. La n være et heltall slik at $n \neq 0$. La a og c være heltall. La x være et heltall slik at

$$ax \equiv c \pmod{n}.$$

Da sier vi at x er en *løsning* til denne kongruensen.

Terminologi 3.4.2. La n være et heltall slik at $n \neq 0$. La a og c være heltall. Når vi er interessert i heltall x som er løsninger til kongruensen

$$ax \equiv c \pmod{n},$$

kalles

$$ax \equiv c \pmod{n}$$

en *lineær kongruens*.

Eksempel 3.4.3. Siden

$$6 \cdot 3 - 8 = 18 - 8 = 10$$

og $5 \mid 10$, er

$$6 \cdot 3 \equiv 8 \pmod{5}.$$

Dermed er 3 en løsning til kongruensen

$$6x \equiv 8 \pmod{5}.$$

Eksempel 3.4.4. Siden

$$(-8) \cdot (-5) - 12 = 40 - 12 = 28$$

og $7 \mid 28$, er

$$(-8) \cdot (-5) \equiv 12 \pmod{7}.$$

Dermed er -5 en løsning til kongruensen

$$-8x \equiv 12 \pmod{7}.$$

Proposisjon 3.4.5. La n være et heltall slik at $n \neq 0$. La a, c, og x være heltall. Da er x en løsning til kongruensen

$$ax \equiv c \pmod{n}$$

hvis og bare hvis det finnes et heltall y slik at x og y er en løsning til ligningen

$$ax - ny = c.$$

Bevis. Anta først at x er en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Da har vi: $n \mid ax - c$. Dermed finnes det et heltall y slik at

$$ax - c = yn.$$

Således er

$$ax - yn = c.$$

Anta istedenfor at det finnes et heltall y slik at

$$ax - yn = c.$$

Da er

$$ax - c = yn,$$

altså $n \mid ax - c$. Vi deduserer at $ax \equiv c \pmod{n}$. □

Eksempel 3.4.6. Fra Eksempel 3.4.3 vet vi at 3 er en løsning til kongruensen

$$6x \equiv 8 \pmod{5}.$$

Derfor fastslår Proposisjon 3.4.5 at det finnes et heltall y slik at $x = 3$ og y er en løsning til ligningen

$$6x - 5y = 8.$$

Vi har nemlig at $x = 3$ og $y = 2$ er en løsning til ligningen

$$6x - 5y = 8.$$

Eksempel 3.4.7. Fra Eksempel 3.4.4 vet vi at -5 er en løsning til kongruensen

$$-8x \equiv 12 \pmod{7}.$$

Derfor fastslår Proposisjon 3.4.5 at det finnes et heltall y slik at $x = -5$ og y er en løsning til ligningen

$$-8x - 7y = 12.$$

Vi har nemlig at $x = -5$ og $y = 4$ er en løsning til ligningen

$$-8x - 7y = 12.$$

Merknad 3.4.8. La n være et heltall slik at $n \neq 0$. La a og c være heltall. Proposisjon 3.4.5 fastslår at det finnes et nært forhold mellom heltallsløsninger til lineære kongruenser og løsninger til lineære diofantiske ligninger.

Dermed kan vi bygge på den gode forståelsen vår for lineære diofantiske ligninger for å få en like god forståelse for heltallsløsninger til lineære kongruenser, som vi nå kommer til å se.

Proposisjon 3.4.9. La n være et heltall slik at $n \neq 0$. La a og c være heltall. Da har kongruesen

$$ax \equiv c \pmod{n}$$

en løsning hvis og bare hvis $\mathsf{sfd}(a, n) \mid c$.

Bevis. Følger umiddelbart fra Proposisjon 3.4.5 og Korollar 2.9.12. □

Eksempel 3.4.10. Vi har: $\mathsf{sfd}(12, 15) = 3$. Siden $3 \mid 6$, fastslår Proposisjon 3.4.9 at kongruensen

$$12x \equiv 6 \pmod{15}$$

har en løsning.

Proposisjon 3.4.9 sier ikke hvordan man finner den, men det kan sjekkes at for eksempel $x = 13$ er en løsning.

Eksempel 3.4.11. Vi har: $\mathsf{sfd}(-14, 21) = 7$. Siden $7 \mid 35$, fastslår Proposisjon 3.4.9 at kongruensen

$$-14x \equiv 35 \pmod{21}$$

har en løsning.

Proposisjon 3.4.9 sier ikke hvordan man finner den, men det kan sjekkes at for eksempel $x = 5$ er en løsning.

Merknad 3.4.12. Etter å ha gjort noen forbedredelser, skal vi nå se på *hvordan* man finner en løsning til en kongruens

$$ax \equiv c \pmod{n}.$$

Proposisjon 3.4.13. La n være et heltall slik at $n \neq 0$. La a, x, og y være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a, n) = d$. Siden $d \mid n$, finnes det et heltall k_n slik at $n = k_n d$. Vi har:

$$ax \equiv ay \pmod{n}$$

hvis og bare hvis

$$x \equiv y \pmod{k_n}.$$

Bevis. Anta først at

$$ax \equiv ay \pmod{n}.$$

Vi gjør følgende observasjoner.

(1) Siden

$$ax \equiv ay \pmod{n},$$

har vi: $n \mid ax - ay$, altså $n \mid a(x - y)$. Dermed finnes det et heltall k slik at

$$a(x - y) = kn.$$

(2) Siden $\mathsf{sfd}(a, n) = d$, har vi: $d \mid a$. Dermed finnes det et heltall k_a slik at $a = k_a a$.

(3) Fra (1), (2), og antakelsen at $n = k_n d$, følger det at

$$k_a d(x - y) = k k_n d,$$

altså at

$$d k_a (x - y) = d k k_n.$$

(4) Fra (3) og Proposisjon 2.2.25 følger det at

$$k_a (x - y) = k k_n.$$

Dermed har vi:

$$k_n \mid k_a (x - y).$$

(5) Ut ifra Proposisjon 2.8.13 er

$$\mathsf{sfd}(k_a, k_n) = 1,$$

altså

$$\mathsf{sfd}(k_n, k_a) = 1.$$

(6) Fra (4), (5), og Proposisjon 2.8.22 følger det at

$$k_n \mid x - y.$$

Dermed er

$$x \equiv y \pmod{k_n}.$$

Således har vi bevist at, dersom

$$ax \equiv ay \pmod{n},$$

er

$$x \equiv y \pmod{k_n}.$$

Anta istedenfor at

$$x \equiv y \pmod{k_n}.$$

Da følger det fra Proposisjon 3.2.51 at

$$ax \equiv ay \pmod{n}.$$

□

Eksempel 3.4.14. Siden $6 \cdot 14 - 6 \cdot 23 = -54$, og siden $9 \mid -54$, er

$$6 \cdot 14 \equiv 6 \cdot 23 \pmod{9}.$$

Vi har: $\mathsf{sfd}(6, 9) = 3$, og $9 = 3 \cdot 3$. Derfor fastslår Proposisjon 3.4.13 at

$$14 \equiv 23 \pmod{3}.$$

Eksempel 3.4.15. Siden $8 \cdot 12 - 8 \cdot 5 = 56$, og siden $28 \mid 56$, er

$$8 \cdot 12 \equiv 8 \cdot 5 \pmod{28}.$$

Vi har: $\mathsf{sfd}(8, 28) = 4$, og $28 = 7 \cdot 4$. Derfor fastslår Proposisjon 3.4.13 at

$$12 \equiv 5 \pmod{7}.$$

Proposisjon 3.4.16. La n være et heltall slik at $n \neq 0$. La a, c, og x være heltall. Anta at

$$ax \equiv c \pmod{n}.$$

La d være et naturlig tall slik at $\mathsf{sfd}(a, n) = d$. Ut ifra definisjonen til $\mathsf{sfd}(a, n)$ vet vi at $d \mid n$, altså at det finnes heltall k_n slik at $n = k_n d$. Da er følgende sanne.

(I) For hvert heltall r slik at $0 \leq r < d$, er

$$x' = x + k_n r$$

en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

(II) La x' være et heltall slik at

$$ax' \equiv c \pmod{n}.$$

Da finnes det et heltall r, hvor $0 \leq r < d$, slik at

$$x' \equiv x + k_n r \pmod{n}.$$

(III) La r og s være heltall slik at $0 \leq r < d$ og $0 \leq s < d$. La

$$x' = x + k_n r$$

og

$$x'' = x + k_n s$$

Hvis

$$x' \equiv x'' \pmod{n}$$

er $r = s$.

Bevis. La oss først bevise at (I) er sant. La t være et heltall slik at $0 \leq t < d$, Fra definisjonen til $\mathsf{sfd}(a, n)$ vet vi at $d \mid a$, altså at det finnes heltall k_a slik at $a = k_a d$. Ut ifra Korollar 2.9.24 er

$$x' = x + k_n t$$

og

$$y' = x - k_a t$$

en løsning til ligningen

$$ax + ny = c.$$

Derfor er

$$x' = x + k_n t$$

og

$$y' = -(x - k_a t) = k_a t - x$$

en løsning til ligningen

$$ax - ny = c.$$

Fra Proposisjon 3.4.5 deduserer vi at

$$x' = x + k_n t$$

er en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

La oss nå bevise at (II) er sant. La x' være et heltall slik at

$$ax' \equiv c \pmod{n}.$$

Fra Proposisjon 3.4.5 følger det at det finnes et heltall y' slik at

$$ax' - ny' = c.$$

Da er

$$ax' + n(-y') = c.$$

Det følger fra Korollar 2.9.25 at det da er et heltall t slik at

$$x' = x + k_n t.$$

Ut ifra Korollar 2.2.11 finnes det heltall k_t og r slik at:

(1) $t = k_t d + r$;

(2) $0 \leq r < d$;

Da er

$$\begin{aligned} x' &= x + k_n t \\ &= x + k_n \left(k_t d + r\right) \\ &= x + k_n r + (k_n d) k_t \\ &= x + k_n r + n k_t. \end{aligned}$$

Derfor er

$$x' - (x + k_n r) = k_t n,$$

altså $n \mid x' - (x + k_n r)$. Dermed er

$$x' \equiv x + k_n r \pmod{n}.$$

La oss nå bevise at (III) er sant. Anta at

$$x' \equiv x'' \pmod{n},$$

altså at

$$x + k_n r \equiv x + k_n s \pmod{n}.$$

Vi gjør følgende observasjoner.

(1) Det følger fra Korollar 3.2.39 at

$$x + k_n r - x \equiv x + k_n s - x \pmod{n},$$

altså at

$$k_n r \equiv k_n s \pmod{n}.$$

(2) Siden $k_n \mid n$, følger det fra Proposisjon 2.6.21 at $\mathsf{sfd}(k_n, n) = k_n$.

Fra (1), (2), og Proposisjon 3.4.13 følger det at

$$r \equiv s \pmod{d}.$$

Siden $0 \leq r < d$ og $0 \leq s < d$, følger det fra Proposisjon 3.2.11 at $r = s$.

□

Merknad 3.4.17. La a og c være heltall, og la $d = \mathsf{sfd}(a, c)$. Proposisjon 3.4.16 fastslår at kongruensen

$$ax \equiv c \pmod{n}$$

har akkurat d løsninger slik at ikke noe par av disse er kongruent modulo n. Gitt én løsning x, er disse løsningene: x, $x + k_n$, $x + 2k_n$, $x + 3k_n$, …, $x + (d-1)k_n$.

Eksempel 3.4.18. La oss se på kongruensen

$$4x \equiv 6 \pmod{10}.$$

Siden

$$4 \cdot 4 - 6 = 10$$

og $10 \mid 10$, er

$$4 \cdot 4 \equiv 6 \pmod{10}.$$

Dermed er $x = 4$ en løsning til kongruensen. Vi har: $\mathsf{sfd}(4, 10) = 2$. Siden $10 = 5 \cdot 2$, er $k_n = 5$. Proposisjon 3.4.16 fastslår at:

(I) $x = 4 + 5 \cdot 0$ og $x = 4 + 5 \cdot 1$, altså $x = 4$ og $x = 9$ er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 10 til én av disse to;

(III) disse to løsningene er ikke kongruent modulo 10 til hverandre.

Eksempel 3.4.19. La oss se på kongruensen

$$12x \equiv 51 \pmod{21}.$$

Siden

$$12 \cdot 6 - 51 = 21$$

og $21 \mid 21$, er

$$12 \cdot 6 \equiv 51 \pmod{21}.$$

Dermed er $x = 6$ en løsning til kongruensen. Vi har: $\mathsf{sfd}(12, 21) = 3$. Siden $21 = 7 \cdot 3$, er $k_n = 7$. Proposisjon 3.4.16 fastslår at:

(I) $x = 6 + 7 \cdot 0$, $x = 6 + 7 \cdot 1$, og $x = 6 + 7 \cdot 2$, altså $x = 6$, $x = 13$, og $x = 20$, er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 21 til én av disse to;

(III) ikke noe par av disse tre løsningene er kongruent modulo 21 til hverandre.

Merknad 3.4.20. La merke til at (II) i Proposisjon 3.4.16 sier ikke at hver løsning til kongruensen

$$ax \equiv c \pmod{n}$$

er *lik* $x + k_n r$ for et heltall r slik at $0 \leq r < d$. På lignende vis sier ikke (II) i Eksempel 3.4.18 at hver løsning x til kongruensen

$$4x \equiv 6 \pmod{10}$$

er *lik* enten 4 eller 9. For eksempel er $x = 14$ en løsning: siden

$$4 \cdot 14 - 6 = 50$$

og $10 \mid 50$, er

$$4 \cdot 14 \equiv 6 \pmod{10}.$$

For et annet eksempel er $x = -1$ en løsning: siden

$$4 \cdot (-1) - 6 = -10$$

og $10 \mid -10$, er

$$4 \cdot (-1) \equiv 6 \pmod{10}.$$

Merknad 3.4.21. Imidlertid sier Proposisjon 3.4.16 at, dersom kongruensen

$$ax \equiv c \pmod{n}$$

har én løsning, finnes det akkurat d løsninger slik at ikke noe par av disse er kongruent modulo n til hverandre. Det er ikke viktig at vi beskriver disse d løsningene som i (I) i Proposisjon 3.4.16. Hver liste over d løsninger, slik at ikke noe par av disse er kongruent modulo n, er like verdifull.

For eksempel i Eksempel 3.4.18, etter å ha observert at $x = 4$ er en løsning til kongruensen

$$4x \equiv 6 \pmod{10},$$

fikk vi lista $x = 4$ og $x = 9$ ved å benytte (I) i Proposisjon 3.4.16. Følgende lister er like verdifulle:

(1) $x = 14$ og $x = 9$;

(2) $x = 4$ og $x = -1$;

(3) $x = 14$ og $x = -1$.

Det finnes uendelig mange andre lister som er like verdifulle!

Merknad 3.4.22. Likevel beskriver skriver vi oftest ei liste hvor alle løsningene x til kongruensen

$$ax \equiv c \pmod{n}$$

oppfyller: $0 \leq x < n$. Proposisjon 3.2.1 fastslår at det alltid er mulig å finne ei slik liste.

For eksempel skriver vi oftest $x = 4$ og $x = 9$ som lista over løsningene til kongruensen

$$4x \equiv 6 \pmod{10}$$

vi så på i Eksempel 3.4.18.

Merknad 3.4.23. For å finne løsningene til kongruensen

$$ax \equiv c \pmod{n},$$

følger det fra Proposisjon 3.4.16 at det viktigste er å finne én løsning. Som vi snart kommer til å se, kan dette alltid gjøres, om det *er* en løsning, ved å benytte Euklids algoritme,

Imidlertid kan en løsning ofte finnes fortere i prakis ved å benytte andre metoder. For å hjelpe oss med dette, er følgende proposisjon svært nyttig.

Proposisjon 3.4.24. La n være et heltall slik at $n \neq 0$. La a, c, og x være heltall. Anta at

$$ax \equiv c \pmod{n}.$$

Ut ifra Proposisjon 3.2.1 finnes det et heltall r slik at:

(1) $x \equiv r \pmod{n}$;

(2) $0 \leq r < n$.

Vi har:

$$ar \equiv c \pmod{n}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Proposisjon 3.2.1 fastslår at det finnes et heltall r slik at:
   (i) $x \equiv r \pmod{n}$;
   (ii) $0 \leq r < n$.

(2) Det følger fra (i) og Korollar 3.2.45 at

$$ax \equiv ar \pmod{n}.$$

(3) Fra (2) og Proposisjon 3.2.24 følger det at

$$ar \equiv ax \pmod{n}.$$

(4) Fra (3), antakelsen at

$$ax \equiv c \pmod{n},$$

og Proposisjon 3.2.33, følger det at

$$ar \equiv c \pmod{n}.$$

□

Eksempel 3.4.25. La oss se på kongruensen

$$6x \equiv -27 \pmod{15}.$$

Siden

$$6 \cdot 53 - (-27) = 345$$

og $15 \mid 345$, er

$$6 \cdot 53 \equiv -27 \pmod{15}.$$

Proposisjon 3.4.24 fastslår at det finnes en løsning r til kongruensen slik at:

(1) $53 \equiv r \pmod{15}$;

(2) $0 \leq r < 15$.

Beviset for Proposisjon 3.4.24 fastslår at r er resten vi får når vi deler 53 med 15, altså $r = 8$. Siden

$$6 \cdot 8 - (-27) = 75$$

og $15 \mid 75$, er det riktignok sant at

$$6 \cdot 8 \equiv -27 \pmod{15}.$$

Eksempel 3.4.26. La oss se på kongruensen

$$4x \equiv 18 \pmod{14}.$$

Siden

$$4 \cdot (-69) - 18 = -294$$

og $14 \mid -294$, er

$$4 \cdot (-69) \equiv 18 \pmod{14}.$$

Proposisjon 3.4.24 fastslår at det finnes en løsning r til kongruensen slik at:

(1) $-69 \equiv r \pmod{15}$;

(2) $0 \leq r < 14$.

Beviset for Proposisjon 3.4.24 fastslår at r er resten vi får når vi deler -69 med 14, altså $r = 1$. Siden

$$4 \cdot 1 - 18 = -14$$

og $14 \mid -14$, er det riktignok sant at

$$4 \cdot 1 \equiv 18 \pmod{14}.$$

Merknad 3.4.27. Dersom det finnes en løsning til kongruensen

$$ax = c \pmod{n},$$

følger det fra Proposisjon 3.4.24 at det finnes en løsning x slik at $0 \leq x < n$. For å finne én løsning til kongruensen, kan vi derfor ganske enkelt sjekke om

$$ar \equiv c \pmod{n}$$

for heltallene r slik at $0 \leq x < n$. Da kan vi benytte (I) i Proposisjon 3.4.16 for å finne de andre løsningene.

Eksempel 3.4.28. La oss se på kongruensen

$$8x \equiv -12 \pmod{20}.$$

For å finne én løsning, er det nok å sjekke om kongruensen stemmer når $x = 0$, $x = 1$, $x = 2$, ..., $x = 19$.

(1) Det er ikke sant at

$$8 \cdot 0 \equiv -12 \pmod{20},$$

siden det ikke er sant at

$$0 \equiv 3 \pmod{20}.$$

(2) Det er sant at

$$8 \cdot 1 \equiv -12 \pmod{20},$$

siden

$$8 - (-12) = 20$$

og $20 \mid 20$.

Siden vi nå har funnet én løsning, er det ikke nødvendig å se på $x = 2$, $x = 3$, ..., $x = 19$.

Nå benytter vi (I) i Proposisjon 3.4.16 for å finne de andre løsningene. Vi har: $\mathsf{sfd}(8, 20) = 4$, og $20 = 5 \cdot 4$. Derfor fastslår Proposisjon 3.4.16 at:

(I) $x = 1 + 5r$ er en løsning for alle heltallene r slik at $0 \leq r < 4$, altså $x = 1$, $x = 6$, $x = 11$, og $x = 16$ er løsninger;

(II) enhver annen løsning er kongruent modulo 20 til én av disse;

(III) ikke noe par av disse fire løsningene er kongruent modulo 20 til hverandre.

Eksempel 3.4.29. La oss se på kongruensen

$$14x \equiv 7 \pmod{63}.$$

For å finne én løsning, er det nok å sjekke om kongruensen stemmer når $x = 0$, $x = 1$, $x = 2$, ..., $x = 62$.

(1) Det er ikke sant at

$$14 \cdot 0 \equiv 7 \pmod{63},$$

siden det ikke er sant at

$$0 \equiv 7 \pmod{63}.$$

(2) Det er ikke sant at

$$14 \cdot 1 \equiv 7 \pmod{63},$$

siden det ikke er sant at

$$14 \equiv 7 \pmod{63}.$$

(3) Det er ikke sant at

$$14 \cdot 2 \equiv 7 \pmod{63},$$

siden det ikke er sant at

$$28 \equiv 7 \pmod{63}.$$

(4) Det er ikke sant at

$$14 \cdot 3 \equiv 7 \pmod{63},$$

siden det ikke er sant at

$$42 \equiv 7 \pmod{63}.$$

(5) Det er ikke sant at

$$14 \cdot 4 \equiv 7 \pmod{63},$$

siden det ikke er sant at

$$56 \equiv 21 \pmod{63}.$$

(6) Det er sant at

$$14 \cdot 5 \equiv 7 \pmod{63},$$

siden

$$14 \cdot 5 - 7 = 63$$

og $63 \mid 63$.

Siden vi nå har funnet én løsning, er det ikke nødvendig å se på tilfellet når $x = 6$, $x = 7$, ..., $x = 62$.

Nå benytter vi (I) i Proposisjon 3.4.16 for å finne de andre løsningene. Vi har: $\mathsf{sfd}(14, 63) = 7$ og $63 = 9 \cdot 7$. Derfor fastslår Proposisjon 3.4.16 at:

(I) $x = 5 + 9r$ er en løsning for alle heltallene r slik at $0 \leq r < 7$, altså $x = 5$, $x = 14$, $x = 23$, $x = 32$, $x = 41$, $x = 50$, og $x = 59$ er løsninger;

(II) enhver annen løsning er kongruent modulo 63 til én av disse;

(III) ikke noe par av disse fire løsningene er kongruent modulo 63 til hverandre.

Merknad 3.4.30. Proposisjon 3.4.13 kan også være til stor hjelp når vi ønsker å finne en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

La $d = \mathsf{sfd}(a, n)$. Anta at $d \mid c$. Proposisjon 3.4.13 fastslår at x er en løsning til kongruensen hvis og bare hvis x er en løsning til kongruensen

$$k_a x \equiv k_c \pmod{k_n},$$

hvor:

(1) k_a er heltallet slik at $a = k_a \cdot d$;

(2) k_c er heltallet slik at $c = k_c \cdot d$;

(3) k_n er heltallet slik at $n = k_n \cdot d$.

Det kan være mange færre tilfeller å se på når vi gjennomfører metoden i Merknad 3.4.27 for kongruensen

$$k_a x \equiv k_c \pmod{k_n},$$

sammenlignet med når vi gjennomfører denne metoden for kongruensen

$$ax \equiv c \pmod{n}.$$

Med andre ord, kan vi ofte finne en løsning til kongruensen

$$k_a x \equiv k_c \pmod{k_n}$$

mye fortere enn en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Eksempel 3.4.31. La oss se igjen på kongruensen

$$8x \equiv -12 \pmod{20}$$

fra Eksempel 3.4.28. Vi har: $\mathsf{sfd}(8, 20) = 4$. Derfor er $k_a = 2$, $k_c = -3$, og $k_n = 5$. Proposisjon 3.4.13 fastslår at x er en løsning til kongruensen hvis og bare hvis x er en løsning til kongruensen

$$2x \equiv -3 \pmod{5}.$$

For å finne en løsning til denne kongruensen, er det nok å sjekke om den stemmer når $x = 0$, $x = 1$, $x = 2$, ..., $x = 4$.

(1) Det er ikke sant at

$$2 \cdot 0 \equiv -3 \pmod{5},$$

siden det ikke er sant at

$$0 \equiv -3 \pmod{5}.$$

(2) Det er sant at

$$2 \cdot 1 \equiv -3 \pmod{5},$$

siden

$$2 \cdot 1 - (-3) = 5$$

og $5 \mid 5$.

Nå kan vi fortsette som i Eksempel 3.4.28, ved å benytte løsningen $x = 1$ for å finne de andre løsningene til kongruensen

$$8x \equiv -12 \pmod{20}.$$

Eksempel 3.4.32. La oss se igjen på kongruensen

$$14x \equiv 7 \pmod{63}$$

fra Eksempel 3.4.29. Vi har: $\mathsf{sfd}(14, 63) = 7$. Derfor er $k_a = 2$, $k_c = 1$, og $k_n = 9$. Proposisjon 3.4.13 fastslår at x er en løsning til kongruensen hvis og bare hvis x er en løsning til kongruensen

$$2x \equiv 1 \pmod{9}.$$

For å finne en løsning til denne kongruensen, er det nok å sjekke om den stemmer når $x = 0$, $x = 1$, $x = 2$, …, $x = 8$.

(1) Det er ikke sant at

$$2 \cdot 0 \equiv 1 \pmod{9},$$

siden det ikke er sant at

$$0 \equiv 1 \pmod{9}.$$

(2) Det er ikke sant at

$$2 \cdot 1 \equiv 1 \pmod{9},$$

siden det ikke er sant at

$$2 \equiv 1 \pmod{9}.$$

(3) Det er ikke sant at

$$2 \cdot 2 \equiv 1 \pmod{9},$$

siden det ikke er sant at

$$4 \equiv 1 \pmod{9}.$$

(4) Det er ikke sant at

$$2 \cdot 3 \equiv 1 \pmod{9},$$

siden det ikke er sant at

$$6 \equiv 1 \pmod{9}.$$

(5) Det er ikke sant at

$$2 \cdot 4 \equiv 1 \pmod{9},$$

siden det ikke er sant at

$$8 \equiv 1 \pmod{9}.$$

(6) Det er sant at

$$2 \cdot 5 \equiv 1 \pmod{9},$$

siden

$$2 \cdot 5 - 1 = 9$$

og $9 \mid 9$.

Nå kan vi fortsette som i Eksempel 3.4.29, ved å benytte løsningen $x = 5$ for å finne de andre løsningene til kongruensen

$$14x \equiv 7 \pmod{63}.$$

Proposisjon 3.4.33. La n være et heltall slik at $n \neq 0$. La a og c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a, n) = d$. Fra Korollar 2.7.20 vet vi at det finnes heltall u og v slik at $d = ua + vn$. Ut ifra definisjonen til $\mathsf{sfd}(a, n)$ vet vi at $d \mid n$, altså at det finnes heltall k_n slik at $n = k_n d$. Anta at $d \mid c$, altså at det et heltall k slik at $c = kd$. Da er

$$x = ku$$

en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Bevis. Ut ifra Proposisjon 2.9.4 er

$$a(ku) + n(kv) = c.$$

Dermed er

$$a(ku) - n \cdot (-kv) = c.$$

Fra Proposisjon 3.4.5 deduserer vi at

$$a(ku) \equiv c \pmod{n}.$$

□

Eksempel 3.4.34. La oss se på kongruensen

$$12x \equiv 57 \pmod{21}.$$

Vi har: $\mathsf{sfd}(12, 21) = 3$. Siden $3 \mid 57$, vet vi fra Proposisjon 3.4.9 at kongruensen har en løsning. Ved å benytte algoritmen i Merknad 2.7.15, får vi:

$$3 = 2 \cdot 12 + (-1) \cdot 21.$$

Siden $57 = 19 \cdot 3$, er $k = 19$. Derfor fastslår Korollar 3.4.36 at $x = 19 \cdot 2$ er en løsning til kongruensen, altså at $x = 38$ er en løsning til kongruensen.

Når vi deler 38 med 21 får vi 17 som resten. Det følger fra Proposisjon 3.4.24 at $x = 17$ er en løsning til kongruensen.

Eksempel 3.4.35. La oss se på kongruensen

$$-8x \equiv 20 \pmod{44}.$$

Vi har: $\mathsf{sfd}(-8, 44) = 4$. Siden $4 \mid 20$, vet vi fra Proposisjon 3.4.9 at kongruensen har en løsning. Ved å benytte algoritmen i Merknad 2.7.15, får vi:

$$4 = 5 \cdot (-8) + 1 \cdot 44.$$

Siden $20 = 5 \cdot 4$, er $k = 4$. Derfor fastslår Korollar 3.4.36 at $x = 5 \cdot 5$ er en løsning til kongruensen, altså at $x = 25$ er en løsning til kongruensen.

Korollar 3.4.36. La n være et heltall slik at $n \neq 0$. La a og c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a, n) = d$. Fra Korollar 2.7.20 vet vi at det finnes heltall u og v slik at $d = ua + vn$. Ut ifra definisjonen til $\mathsf{sfd}(a, n)$ vet vi at $d \mid n$, altså at det finnes heltall k_n slik at $n = k_n d$. Anta at $d \mid c$, altså at det et heltall k slik at $c = kd$. Da er følgende sanne.

(I) For hvert heltall r slik at $0 \leq r < d$, er

$$x = ku + k_n r$$

en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

(II) La x være et heltall som er en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Da finnes det et heltall r, hvor $0 \leq r < d$, slik at

$$x \equiv ku + k_n r \pmod{n}.$$

(III) La r og s være heltall slik at $0 \leq r < d$ og $0 \leq s < d$. La

$$x = ku + k_n r$$

og

$$x' = ku + k_n s$$

være to av løsningene i (I) til kongruensen

$$ax \equiv c \pmod{n}.$$

Dersom

$$x \equiv x' \pmod{n},$$

er $r = s$.

Bevis. Følger umiddelbart fra Proposisjon 3.4.33 og Proposisjon 3.4.16. □

Eksempel 3.4.37. La oss se på kongruensen

$$12x \equiv 57 \pmod{21}.$$

Som i Eksempel 3.4.34, er $\mathsf{sfd}(12, 57) = 3$ og $ku = 38$. Siden $21 = 7 \cdot 3$, er $k_n = 7$. Derfor fastslår Korollar 3.4.36 at:

(I) $x = 38 + 7r$ er en løsning til kongruensen for alle heltallene r slik at $0 \leq r < 3$, altså $x = 38$, $x = 45$, og $x = 52$ er løsninger til kongruensen.

(II) Enhver løsning til kongruensen er kongruent modulo 21 til én av disse løsningene.

(III) Ikke noe par av disse tre løsningene er kongruent til hverandre modulo 21.

Når vi deler 38, 45, og 52 med 21, får vi restene 17, 3, og 10. Dermed følger det fra Proposisjon 3.4.24, (I) – (III) ovenfor, Proposisjon 3.2.24, og Proposisjon 3.2.33 at:

(I) $x = 3$, $x = 10$, og $x = 17$ er løsninger til kongruensen.

(II) enhver annen løsning til kongruensen er kongruent modulo 21 til én av disse løsningene.

(III) ikke noe par av disse fire løsningene er kongruent til hverandre modulo 21.

Etter at vi fant løsningen $x = 38$, kunne vi alternativt hatt først dedusert, som i Eksempel 3.4.34, at $x = 17$ er en løsning. Da kan vi benytte Proposisjon 3.4.16 for å få:

(I) $x = 17 + 7r$ er en løsning til kongruensen for alle heltallene r slik at $0 \leq r < 3$, altså $x = 17$, $x = 24$, og $x = 31$ er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 21 til én av disse løsningene.

(III) ikke noe par av disse tre løsningene er kongruent til hverandre modulo 21.

Når vi deler 24 og 31 med 21, får vi restene 3 og 10. Dermed følger det fra Proposisjon 3.4.24, (I) – (III) ovenfor, Proposisjon 3.2.24, og Proposisjon 3.2.33 at:

(I) $x = 3$, $x = 10$, og $x = 17$ er løsninger til kongruensen.

(II) enhver annen løsning til kongruensen er kongruent modulo 21 til én av disse løsningene.

(III) ikke noe par av disse fire løsningene er kongruent til hverandre modulo 21.

Eksempel 3.4.38. La oss se på kongruensen

$$-8x \equiv 20 \pmod{44}.$$

Som i Eksempel 3.4.35, er $\mathsf{sfd}(-8, 44) = 4$ og $ku = 25$. Siden $44 = 11 \cdot 4$, er $k_n = 11$. Derfor fastslår Korollar 3.4.36 at:

(I) $x = 25 + 11r$ er en løsning til kongruensen for alle heltallene r slik at $0 \leq r < 4$, altså $x = 25$, $x = 36$, $x = 47$, og $x = 58$ er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 44 til én av disse løsningene.

(III) ikke noe par av disse fire løsningene er kongruent til hverandre modulo 44.

Når vi deler 25, 36, 47, og 58 med 44, får vi restene 25, 36, 3, og 14. Dermed følger det fra Proposisjon 3.4.24, (I) – (III) ovenfor, Proposisjon 3.2.24, og Proposisjon 3.2.33 at:

(I) $x = 3$, $x = 14$, $x = 25$, og 36 er løsninger til kongruensen.

(II) enhver annen løsning til kongruensen er kongruent modulo 44 til én av disse løsningene.

(III) ikke noe par av disse fire løsningene er kongruent til hverandre modulo 44.

Korollar 3.4.39. La n være et heltall slik at $n \neq 0$. La a og c være heltall. Anta at $\mathsf{sfd}(a, n) = 1$. Fra Korollar 2.7.20 vet vi at det finnes heltall u og v slik at $d = ua + vn$. Da er $x = cu$ en løsning til kongruensen

$$ax \equiv c \pmod{n},$$

og enhver annen løsning er kongruent modulo n til denne løsningen.

Bevis. Følger umiddelbart fra Korollar 3.4.36. □

Eksempel 3.4.40. La oss se på kongruensen

$$7x \equiv 16 \pmod{23}.$$

Vi har: $\mathsf{sfd}(7, 23) = 1$. Siden $1 \mid 16$, vet vi fra Proposisjon 3.4.9 at kongruensen har en løsning. Ved å benytte algoritmen i Merknad 2.7.15, får vi:

$$1 = 10 \cdot 7 + (-3) \cdot 23.$$

Derfor fastslår Korollar 3.4.36 at:

(1) $x = 16 \cdot 10$ er en løsning til kongruensen, altså $x = 160$ er en løsning til kongruensen;

(2) enhver annen løsning til kongruensen er kongruent modulo 23 til denne løsningen.

Når vi deler 160 med 23, får vi 22 som resten. Det følger fra Proposisjon 3.4.24 at $x = 22$ er en løsning til kongruensen. Da fastslår (II) i Proposisjon 3.4.16 at enhver annen løsning er kongruent til denne modulo 23.

Merknad 3.4.41. I Merknad 3.4.27 og Merknad 3.4.30 har vi sett to metoder som kan hjelpe oss å finne en løsning til kongruensen

$$ax \equiv c \pmod{n}$$

fortere i praksis enn å benytte Euklids algoritme og Merknad 2.7.15. Følgende proposisjon kan også være til hjelp.

Proposisjon 3.4.42. La n være et heltall slik at $n \neq 0$. La a og c være heltall. La y være et heltall slik at

$$ay \equiv 1 \pmod{n}.$$

Da er $x = yc$ en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Bevis. Siden

$$ay \equiv 1 \pmod{n},$$

følger det fra Korollar 3.2.45 at

$$ayc \equiv c \pmod{n}.$$

□

Eksempel 3.4.43. La oss se på kongruensen

$$5x \equiv 17 \pmod{19}.$$

Siden

$$5 \cdot 4 - 1 = 19$$

og $19 \mid 19$, er $y = 4$ en løsning til kongruensen

$$5y = 1 \pmod{19}.$$

Da fastslår Proposisjon 3.4.42 at

$$x = 4 \cdot 17,$$

altså $x = 68$, er en løsning til kongruensen.

Når vi deler 68 med 19 får vi resten 11. Det følger fra Proposisjon 3.4.24 at $x = 11$ er en løsning til kongruensen. Siden $\mathsf{sfd}(5, 19) = 1$, er alle andre løsninger kongruent modulo 19 til denne løsningen.

Eksempel 3.4.44. La oss se på kongruensen

$$6x \equiv -24 \pmod{9}.$$

Vi har: $\mathsf{sfd}(6, 9) = 3$. Da fastslår Proposisjon 3.4.13 at et heltall x er en løsning til denne kongruensen hvis og bare hvis det finnes en løsning til kongruensen

$$2x \equiv -8 \pmod{3}.$$

Siden

$$2 \cdot 2 - 1 = 3$$

og $3 \mid 3$, er $x = 2$ en løsning til kongruensen

$$2x \equiv 1 \pmod{3}.$$

Da fastslår Proposisjon 3.4.42 at

$$x = 2 \cdot (-8),$$

altså $x = -16$, er en løsning til kongruensen

$$2x \equiv -8 \pmod{3},$$

altså til kongruensen

$$6x \equiv -24 \pmod{9}.$$

Nå kan vi benytte Proposisjon 3.4.16 for å finne de andre løsningene. Siden $9 = 3 \cdot 3$, er $k_n = 3$. Da fastslår Proposisjon 3.4.16 at:

(I) $x = -16 + 3r$ er en løsning til kongruensen

$$6x \equiv -24 \pmod 9$$

for alle heltallene r slik at $0 \leq r < 3$, altså $x = -16$, $x = -13$, og $x = -10$, er løsninger til denne kongruensen.

(II) Enhver løsning til kongruensen er kongruent modulo 9 til én av disse løsningene.

(III) Ikke noe par av disse tre løsningene er kongruent til hverandre modulo 9.

Når vi deler -16, -13, og -10 med 9, får vi restene 2, 5, og 8. Da følger det fra Proposisjon 3.4.24, (I) – (III) ovenfor, Proposisjon 3.2.24, og Proposisjon 3.2.33 at:

(I) $x = 2$, $x = 5$, og $x = 8$ er løsninger til kongruensen

$$6x \equiv -24 \pmod 9.$$

(II) Enhver løsning til kongruensen er kongruent modulo 9 til én av disse løsningene.

(III) Ikke noe par av disse tre løsningene er kongruent til hverandre modulo 9.

Merknad 3.4.45. Følgende proposisjon kan spare oss litt arbeid når vi ønsker å finne løsningene til en kongruens.

Proposisjon 3.4.46. La n være et heltall slik at $n \neq 0$. La a, c, og x være heltall. Ut ifra Proposisjon 3.2.1 finnes det et heltall r slik at:

(1) $c \equiv r \pmod n$;

(2) $0 \leq r < n$.

Da er

$$ax \equiv c \pmod n$$

hvis og bare hvis

$$ax \equiv r \pmod n.$$

Bevis. Anta først at

$$ax \equiv c \pmod n.$$

Siden

$$c \equiv r \pmod n,$$

følger det fra Proposisjon 3.2.33 at

$$ax \equiv r \pmod n.$$

Anta istedenfor at

$$ax \equiv r \pmod n.$$

Siden $c \equiv r \pmod{n}$, følger det fra Proposisjon 3.2.24 at

$$r \equiv c \pmod{n}.$$

Da følger det fra Proposisjon 3.2.33 at

$$ax \equiv c \pmod{n}.$$

□

Eksempel 3.4.47. Vi har: $87 \equiv 3 \pmod{12}$. Da fastslår Proposisjon 3.4.46 at x er en løsning til kongruensen

$$9x \equiv 87 \pmod{12}$$

hvis og bare hvis x er en løsning til kongruensen

$$9x \equiv 3 \pmod{12}.$$

Eksempel 3.4.48. Vi har: $-102 \equiv 18 \pmod{20}$. Da fastslår Proposisjon 3.4.46 at x er en løsning til kongruensen

$$12x \equiv -102 \pmod{20}$$

hvis og bare hvis x er en løsning til kongruensen

$$12x \equiv 18 \pmod{20}.$$

Merknad 3.4.49. La n være et heltall slik at $n \neq 0$. La a og c være heltall. Vi har nå rukket en komplett forståelse for kongruensen

$$ax \equiv c \pmod{n},$$

og har i tillegg sett flere metoder for å finne fort dens løsninger. For å oppsummere, har vi følgende oppskrift.

(1) Regn ut $\mathsf{sfd}(a, n)$. La oss betegne $\mathsf{sfd}(a, n)$ som d. Dersom $d \mid c$, har kongruensen en løsning: gå da videre til (3), eller valgfritt til (2). Ellers har kongruensen ikke en løsning.

(2) Dersom $c > n$, finn et heltall r slik at $c \equiv r \pmod{n}$ og $0 \leq r < n$. Gå da videre til (3) ved å erstatte c med r.

(3) Prøv å finne én løsning. For å gjøre dette, kan vi gå videre til ett av (4), (5), (6), eller (7). Dersom $\mathsf{sfd}(a, n) > 1$, er det typisk best å gå videre til (5).

(4) Ved å benytte algoritmen i Merknad 2.7.15, finn heltall u og v slik at $d = ua + vn$. Finn heltallet k slik at $c = kd$. Da er $x = ku$ en løsning. Gå videre til (8).

(5) Dersom $\mathsf{sfd}(a, n) > 1$, finn heltallet k_a slik at $a = k_a \cdot d$, heltallet k_c slik at $c = k_c d$, og heltallet k_n slik at $n = k_n \cdot d$. Prøv å finne én løsning til kongruensen

$$k_a \equiv k_c \pmod{k_n}$$

ved å gå videre til (4), (6) eller (7), og ved å erstatte a med k_a, c med k_c, og n med k_n. Ofte er det i praksis best å gå videre til (6) eller (7).

(6) Sjekk om x er en løsning til kongruensen for alle heltallene x slik at $0 \leq x < n$. Stopp når en løsning er blitt funnet. Gå videre til (8).

(7) Finn en løsning til kongruensen

$$ay \equiv 1 \pmod{n}.$$

Da er yc en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Gå videre til (8).

(8) Etter at vi har funnet én løsning, benytt Proposisjon 3.4.16 for å finne de andre. Gå valgfritt videre til (8).

(9) Benytt Proposisjon 3.4.24, Proposisjon 3.2.24, og Proposisjon 3.2.33, for å finne alle løsningene x slik at $0 \leq x < n$.

Eksempel 3.4.50. La oss se på kongruensen

$$16x \equiv 56 \pmod{24}.$$

Vi gjør følgende.

(1) Først regner vi ut $\mathsf{sfd}(16, 24)$. Vi får: $\mathsf{sfd}(16, 24) = 8$. Siden $8 \mid 56$, fastslår Proposisjon 3.4.9 at kongruensen har en løsning. Da har vi fullført Steg (1) i Merknad 3.4.49.

(2) Siden $56 - 8 = 48$ og $24 \mid 48$, er $56 \equiv 8 \pmod{24}$. Da fastslår Proposisjon 3.4.46 at x er en løsning til kongruensen

$$16x \equiv 56 \pmod{24}$$

hvis og bare hvis x er en løsning til kongruensen

$$16x \equiv 8 \pmod{24}.$$

Nå skal vi prøve å finne løsningene til denne kongruensen. Dette fullfører Steg (2) i Merknad 3.4.49.

(3) For å finne løsningene til kongruensen

$$16x \equiv 8 \pmod{24},$$

skal vi først prøve å finne én løsning. Dette fullfører Steg (3) i Merknad 3.4.49.

(4) Ut ifra Proposisjon 3.4.30, er x en løsning til kongruensen

$$16x \equiv 8 \pmod{24}$$

hvis og bare hvis x er en løsning til kongruensen

$$2x \equiv 1 \pmod{3}.$$

Nå skal vi prøve å finne én løsning til denne kongruensen. Dette fullfører Steg (5) i Merknad 3.4.49.

(5) Nå sjekker vi om x er en løsning til kongruensen

$$2x \equiv 1 \pmod{3}$$

for hvert heltall x slik at $0 \leq x < 3$. Siden

$$2 \cdot 2 - 1 = 3$$

og $3 \mid 3$, får vi at $x = 2$ er en løsning. Dette fullfører Steg (6) i Merknad 3.4.49.

(6) Vi har:

$$24 = 3 \cdot 8.$$

Da fastslår Proposisjon 3.4.16 at:

(I) $x = 2 + 3r$ er en løsning til kongruensen

$$16x \equiv 56 \pmod{24}$$

for alle heltallene r slik at $0 \leq r < 8$, altså $x = 2$, $x = 5$, $x = 8$, $x = 11$, $x = 14$, $x = 15$, $x = 18$, $x = 21$ er løsninger til denne kongruensen.

(II) Enhver løsning til kongruensen er kongruent modulo 24 til én av disse løsningene.

(III) Ikke noe par av disse åtte løsningene er kongruent til hverandre modulo 24.

Dette fullfører Steg (8) i Merknad 3.4.49.

(7) Siden alle løsningene x i (7) oppfyller $0 \leq x < 24$, er det ikke noe å gjøre i Steg (9) i Merknad 3.4.49.

Vi kunne alternativt har gjort ett av følgende.

(1) Vi kunne har benyttet algoritmen i Merknad 2.7.15 for å finne en løsning til kongruensen

$$16x \equiv 56 \pmod{24}$$

og da benyttet Proposisjon 3.4.16 for å finne de andre løsningene. Dermed hadde vi gått fra Steg (1) til Steg (3) til Steg (4) til Steg (8) i Merknad 3.4.49.

(2) Vi kunne har benyttet algoritmen i Merknad 2.7.15 for å finne en løsning til kongruensen

$$16x \equiv 8 \pmod{24}$$

og da benyttet Proposisjon 3.4.16 for å finne de andre løsningene. Dermed hadde vi gått fra Steg (1) til Steg (2) til Steg (3) til Steg (4) til Steg (8) i Merknad 3.4.49.]

(3) Vi kunne har benyttet algoritmen i Merknad 2.7.15 for å finne en løsning til kongruensen

$$2x \equiv 1 \pmod{3}$$

og da benyttet Proposisjon 3.4.16 for å finne de andre løsningene. Dermed hadde vi gått fra Steg (1) til Steg (2) til Steg (3) til Steg (5) til Steg (4) til Steg (8) i Merknad 3.4.49.

I tillegg kunne vi har benyttet metoden i (7) i Merknad 3.4.49 på flere steder. For eksempel kunne vi har funnet en løsning til kongruensen

$$16x \equiv 1 \pmod{24},$$

og benyttet dette heltallet for å finne en løsning til kongruensen

$$16x \equiv 8 \pmod{24}.$$

Imidlertid rekker vi en løsning fortere ved å følge stegene (1) – (7) ovenfor.

Eksempel 3.4.51. La oss se på kongruensen

$$-27x \equiv -99 \pmod{45}.$$

Vi gjør følgende.

(1) Først regner vi ut $\mathsf{sfd}(-27, 45)$. Vi får: $\mathsf{sfd}(-27, 45) = 9$. Siden $9 \mid -99$, fastslår Proposisjon 3.4.9 at kongruensen har en løsning. Da har vi fullført Steg (1) i Merknad 3.4.49.

(2) Siden $-99 - 36 = -135$ og $45 \mid -135$, er $-99 \equiv 36 \pmod{45}$. Da fastslår Proposisjon 3.4.46 at x er en løsning til kongruensen

$$-27x \equiv -99 \pmod{45}$$

hvis og bare hvis x er en løsning til kongruensen

$$-27x \equiv 36 \pmod{45}.$$

Nå skal vi prøve å finne løsningene til denne kongruensen. Dette fullfører Steg (2) i Merknad 3.4.49.

(3) For å finne løsningene til kongruensen

$$-27x \equiv 36 \pmod{45},$$

skal vi først prøve å finne én løsning. Dette fullfører Steg (3) i Merknad 3.4.49.

(4) Ut ifra Proposisjon 3.4.30, er x en løsning til kongruensen

$$-27x \equiv 36 \pmod{45}$$

hvis og bare hvis x er en løsning til kongruensen

$$-3x \equiv 4 \pmod{5}.$$

Nå skal vi prøve å finne én løsning til denne kongruensen. Dette fullfører Steg (5) i Merknad 3.4.49.

(5) Nå prøver vi å finne en løsning til kongruensen

$$-3y \equiv 1 \pmod{5}.$$

Siden

$$(-3) \cdot (-2) - 1 = 5$$

og $5 \mid 5$, er $y = -2$ en løsning til denne kongruensen. Da fastslår Proposisjon 3.4.42 at $x = (-2) \cdot 4$, altså $x = -8$ er en løsning til kongruensen

$$-3x \equiv 4 \pmod{5}.$$

Dette fullfører Steg (7) i Merknad 3.4.49.

(6) Vi har:

$$45 = 5 \cdot 9.$$

Da fastslår Proposisjon 3.4.16 at:

(I) $x = -8 + 5r$ er en løsning til kongruensen

$$-18x \equiv -99 \pmod{45}$$

for alle heltallene r slik at $0 \leq r < 9$, altså $x = -8$, $x = -3$, $x = 2$, $x = 7$, $x = 12$, $x = 17$, $x = 22$, $x = 27$, og $x = 32$ er løsninger til denne kongruensen.

(II) Enhver løsning til kongruensen er kongruent modulo 45 til én av disse løsningene.

(III) Ikke noe par av disse ni løsningene er kongruent til hverandre modulo 45.

Dette fullfører Steg (8) i Merknad 3.4.49.

(7) Når vi deler $x = -8$ og $x = -3$ med 45, får vi restene 37 og 42. Derfor fastslår Proposisjon 3.4.24, Proposisjon 3.2.24, og Proposisjon 3.2.33 at:

(I) $x = 2$, $x = 7$, $x = 12$, $x = 17$, $x = 22$, $x = 27$, $x = 32$, $x = 37$, og $x = 42$ er løsninger til denne kongruensen.

(II) Enhver løsning til kongruensen er kongruent modulo 45 til én av disse løsningene.

(III) Ikke noe par av disse ni løsningene er kongruent til hverandre modulo 45.

Dette fullfører Steg (9) i Merknad 3.4.49.

Alternativt kunne vi har gjort følgende.

(1) For å finne en løsning til kongruensen

$$-3x \equiv 4 \pmod{5},$$

kunne vi har sjekket om x er en løsning for hvert heltall x slik at $0 \leq x < 4$. Siden

$$(-3) \cdot 2 - 4 = -10$$

og $5 \mid --10$, får vi at $x = 2$ er en løsning. Dette fullfører Steg (6) i Merknad 3.4.49. Da hadde vi gått videre til Steg (8) i Merknad 3.4.49.

(2) Som i Eksempel 3.4.50, kunne vi har benyttet algoritmen i Merknad 2.7.15 istedenfor ett av (2), (4), eller (5) ovenfor, og så gått videre til Steg (8) i Merknad 3.4.49.

I tillegg, som i Eksempel 3.4.50, kunne vi har benyttet metoden i (7) i Merknad 3.4.49 på flere steder. Imidlertid rekker vi en løsning fortere ved å følge stegene (1) – (7) ovenfor.

Merknad 3.4.52. Generelt sett er det best å benytte algoritmen i Merknad 2.7.15 for å finne en løsning til kongruensen

$$ax \equiv c \pmod{n}$$

når n er ganske stort, og det er ikke mulig å benytte Proposisjon 3.4.30 for å se istedenfor på en kongruens hvor n er mindre.

Merknad 3.4.53. Mange andre gyldige metoder kan benyttes for å finne én løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

For eksempel kan vi argumentere på en lignende måte som i Proposisjon 3.4.42, med for eksempel -1 istedenfor 1, og $-yc$ istedenfor yc. Vær kreativ!

O3 Oppgaver – Modulær aritmetikk

O3.1 Oppgaver i eksamens stil

Oppgave O3.1.1. Hvilke av de følgende er sanne?

(1) $123 \equiv 155 \pmod 4$?

(2) $-5 \equiv 18 \pmod 7$?

(3) $36 \equiv -8 \pmod{11}$?

Begrunn svarene dine.

Oppgave O3.1.2. Gjør følgende.

(1) Vis at $53 \equiv 14 \pmod{39}$ og at $196 \equiv 1 \pmod{39}$. Deduser at

$$53^2 \equiv 1 \pmod{39}.$$

(2) Vis at $103 \equiv -14 \pmod{39}$. Deduser fra dette og kongruensen $196 \equiv 1 \pmod{39}$ at $103^2 \equiv 1 \pmod{39}$.

(3) Benytt (1) og (2) for å vise at

$$53^{103} + 103^{53}$$

er delelig med 39.

Oppgave O3.1.3. Gjør følgende.

(1) Vis at $32 \equiv 5 \pmod{27}$.

(2) La t være et naturlig tall. Benytt (1) for å vise at

$$2^{5t+1} + 5^{t+2}$$

er delelig med 27. *Tips*: Observer at $2^{5t} = 32^t$.

Oppgave O3.1.4. La x være et naturlig tall. Anta at det er et heltall n slik at $n \geq 0$ og

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0,$$

hvor, for hvert heltall i slik at $0 \leq i \leq n$, er x_i et heltall slik at $x_i \geq 0$. Gjør følgende.

(1) Vis at $10 \equiv 4 \pmod 6$.

(2) La i være et naturlig tall. Vis at $10^i \equiv 4 \pmod 6$. *Tips*: Benytt (1) og induksjon.

(3) Benytt (2) for å vise at x er delelig med 6 hvis og bare hvis summen

$$x_0 + 4x_1 + 4x_2 + \cdots + 4x_{n-1} + 4x_n$$

er delelig med 6.

(4) Er 1321473 delelig med 6? Benytt (3) i løpet av svaret ditt.

Oppgave O3.1.5. Benytt algoritmen i Merknad 2.7.15 i minst én del av oppgaven, men ikke i alle de tre delene.

(1) Finn løsninger til kongruensen

$$-6x \equiv 15 \pmod{27}$$

slik at alle løsningene til denne kongruensen er kongruent modulo 27 til ett av heltallene i lista di, og slik at ikke noe par av heltallene i lista di er kongruent til hverandre modulo 27.

(2) Finn løsninger til kongruensen

$$104x \equiv -56 \pmod{128}$$

slik at alle løsningene til denne kongruensen er kongruent modulo 128 til ett av heltallene i lista di, og slik at ikke noe par av heltallene i lista di er kongruent til hverandre modulo 128.

(3) Finn løsninger til kongruensen

$$7x \equiv 2 \pmod{50}$$

slik at alle løsningene til denne kongruensen er kongruent modulo 50 til ett av heltallene i lista di, og slik at ikke noe par av heltallene i lista di er kongruent til hverandre modulo 50.

4 Primtall

4.1 Primtall

Definisjon 4.1.1. La n være et naturlig tall. Da er n et *primtall* om:

(1) $n \geq 2$;

(2) de eneste naturlige tallene som er divisorer til n er 1 og n.

Eksempel 4.1.2. Siden det ikke er sant at $1 \geq 2$, er 1 ikke et primtall.

Eksempel 4.1.3. De eneste naturlige tallene som er divisorer til 2 er 1 og 2. Derfor er 2 et primtall.

Eksempel 4.1.4. De eneste naturlige tallene som er divisorer til 3 er 1 og 3. Derfor er 3 et primtall.

Eksempel 4.1.5. Siden 2 er en divisor til 4, er 1 og 4 ikke de eneste divisorene til 4. Derfor er 4 ikke et primtall.

Eksempel 4.1.6. De eneste naturlige tallene som er divisorer til 5 er 1 og 5. Derfor er 5 et primtall.

Eksempel 4.1.7. Siden 2 og 3 er divisorer til 6, er 1 og 6 ikke de eneste divisorene til 6. Derfor er 6 ikke et primtall.

Eksempel 4.1.8. De eneste naturlige tallene som er divisorer til 7 er 1 og 7. Derfor er 7 et primtall.

Eksempel 4.1.9. Siden 2 og 4 er divisorer til 8, er 1 og 8 ikke de eneste divisorene til 8. Derfor er 8 ikke et primtall.

Eksempel 4.1.10. Siden 3 er en divisor til 9, er 1 og 9 ikke de eneste divisorene til 9. Derfor er 9 ikke et primtall.

Eksempel 4.1.11. Siden 2 og 45 er divisorer til 10, er 1 og 10 ikke de eneste divisorene til 10. Derfor er 10 ikke et primtall.

Merknad 4.1.12. De første ti primtallene er: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. Sjekk om du er enig om dette!

4.2 Grunnleggende proposisjoner om primtall

Proposisjon 4.2.1. La x være et heltall. La p være et primtall. Da er enten $\mathsf{sfd}(p, x) = 1$ eller $\mathsf{sfd}(p, x) = p$.

Bevis. Vi gjør følgende observasjoner:

(1) siden p er et primtall, er 1 og p de eneste divisorene til p;

(2) $\mathsf{sfd}(p, x)$ er en divisor til p.

Det følger fra (1) og (2) at enten $\mathsf{sfd}(p, x) = 1$ eller $\mathsf{sfd}(p, x) = p$.

□

Eksempel 4.2.2. La x være 12, og la p være 5. Da er $\mathsf{sfd}(5, 12) = 1$.

Eksempel 4.2.3. La x være 15, og la p være 5. Da er $\mathsf{sfd}(5, 15) = 5$.

Merknad 4.2.4. Proposisjon 4.2.1 er selvfølgelig ikke sann om vi ikke antar at p er et primtall: ellers hadde begrepet «største felles divisor» ikke vært veldig nyttig! Hvis for eksempel $x = 12$ og $p = 8$, er $\mathsf{sfd}(8, 12) = 4$. Dermed er det ikke sant at $\mathsf{sfd}(8, 12) = 1$ eller $\mathsf{sfd}(8, 12) = 12$.

Korollar 4.2.5. La x være et heltall. La p være et primtall. Hvis $p \mid x$ er $\mathsf{sfd}(p, x) = p$. Ellers er $\mathsf{sfd}(p, x) = 1$.

Bevis. Anta først at det ikke er sant at $p \mid x$. Vi gjør følgende observasjoner:

(1) ut ifra Proposisjon 4.2.1 er enten $\mathsf{sfd}(p, x) = 1$ eller $\mathsf{sfd}(p, x) = p$;

(2) $\mathsf{sfd}(p, x)$ er en divisor til x.

Fra (1), (2), og antakelsen at det ikke er sant at $p \mid x$, følger det at $\mathsf{sfd}(p, x) = 1$.

Anta istedenfor at $p \mid x$. Da følger det fra Proposisjon 2.6.21 at $\mathsf{sfd}(p, x) = p$.

□

Eksempel 4.2.6. La x være 14, og la p være 3. Det er ikke sant at $3 \mid 14$. Da fastslår Korollar 4.2.5 at $\mathsf{sfd}(3, 14) = 1$, som riktignok er sant.

Eksempel 4.2.7. La x være 18, og la p være 3. Det er sant at $3 \mid 18$. Da fastslår Korollar 4.2.5 at $\mathsf{sfd}(3, 18) = 3$, som riktignok er sant.

Merknad 4.2.8. Korollar 4.2.5 er ikke sant om vi ikke antar at p er et primtall. Hvis for eksempel $x = 15$ og $p = 9$, er det ikke sant at $9 \mid 15$. Imidlertid er $\mathsf{sfd}(9, 15) = 3$, altså er det ikke sant $\mathsf{sfd}(9, 15) = 1$.

Korollar 4.2.9. La p og q være primtall slik at $p \neq q$. La m og n være naturlige tall. Da er $\mathsf{sfd}(p^m, q^n) = 1$.

Bevis. Ut ifra Korollar 4.2.5 er $\mathsf{sfd}(p, q) = 1$. Ved å benytte Proposisjon 2.8.30 og Merknad 2.6.3 gjentatte ganger, følger det at $\mathsf{sfd}(p^m, q^n) = 1$. □

Eksempel 4.2.10. Korollar 4.2.9 fastslår at $\mathsf{sfd}(3^3, 5^2) = 1$, altså at $\mathsf{sfd}(27, 25) = 1$. Dette er riktignok sant.

Eksempel 4.2.11. Korollar 4.2.9 fastslår at $\mathsf{sfd}(2^6, 7^3) = 1$, altså at $\mathsf{sfd}(64, 343) = 1$. Ved å benytte Euklids algoritme, finner vi at dette riktignok er sant.

Proposisjon 4.2.12. La x og y være heltall. La p være et primtall. Anta at $p \mid xy$. Da har vi: $p \mid x$ eller $p \mid y$.

Bevis. Anta at det ikke er sant at $p \mid x$. Fra Korollar 4.2.5 følger det at $\mathsf{sfd}(p, x) = 1$. Fra Proposisjon 2.8.22 deduserer vi at $p \mid y$. □

Eksempel 4.2.13. La p være 3. Vi har: $3 \mid 48$, og $48 = 6 \cdot 8$. Proposisjon 4.2.12 fastslår at enten $3 \mid 6$ eller $3 \mid 8$. Det er riktignok sant at $3 \mid 6$.

Eksempel 4.2.14. La p være 11. Vi har: $11 \mid 66$, og $66 = 3 \cdot 33$. Proposisjon 4.2.12 fastslår at enten $11 \mid 3$ eller $11 \mid 33$. Det er riktignok sant at $11 \mid 33$.

Eksempel 4.2.15. La p være 7. Vi har: $7 \mid 294$, og $294 = 14 \cdot 21$. Proposisjon 4.2.12 fastslår at enten $7 \mid 14$ eller $7 \mid 21$. Det er riktignok sant at $7 \mid 14$, og faktisk også sant at $7 \mid 21$.

Merknad 4.2.16. Proposisjon 4.2.12 er ikke sant om vi ikke antar at p er et primtall. Hvis for eksempel $x = 4$, $y = 6$, og $p = 12$, har vi: $12 \mid 24$. Imidlertid er det ikke sant at $12 \mid 4$, og heller ikke sant at $12 \mid 6$.

Merknad 4.2.17. Eksempel 4.2.15 viser at det er helt mulig at både $p \mid x$ og $p \mid y$ i Proposisjon 4.2.12.

Merknad 4.2.18. Proposisjon 4.2.12 er avgjørende. Den er kjernen til aritmetikkens fundamentalteoremet, som vi kommer til å se på snart.

Kanskje ser beviset for Proposisjon 4.2.12 lett ut, men Euklids lemma ligger bak det. Euklids lemma var langt fra lett å bevise: vi måtte studere inngående begrepet «største felles divisor» og komme fram til Korollar 2.7.6.

Korollar 4.2.19. La n være et naturlig tall. For hvert naturlig tall i slik at $1 \leq i \leq n$, la x_i være et heltall. La p være et primtall. Dersom $p \mid x_1 \cdots x_n$, finnes det et naturlig tall i slik at $1 \leq i \leq n$ og $p \mid x_i$.

Bevis. Først sjekker vi om korollaret er sant når $n = 1$. Dette er tautologisk!

Anta nå at korollaret har blitt bevist når $n = m$, hvor m er et gitt naturlig tall. For hvert naturlig tall i slik at $1 \leq i \leq m + 1$, la x_i være et heltall. Anta at $p \mid x_1 \cdots x_{m+1}$. Vi ønsker å bevise at det finnes et naturlig tall i slik at $1 \leq i \leq m + 1$ og $p \mid x_i$.

La $x = x_1 \cdots x_m$, og la $y = x_{m+1}$. Ut ifra Proposisjon 4.2.12 er ett av følgende sant:

(1) $p \mid x$;

(2) $p \mid y$, altså $p \mid x_{m+1}$.

Anta først at (2) er sant. Da stemmer utsagnet vi ønsker å bevise, ved å la $i = m + 1$.

Anta istedenfor at (1) er sant. Ut ifra antakelsen at korollaret har blitt bevist når $n = m$, finnes det da et naturlig tall i slik at $1 \leq i \leq m$ og $p \mid x_i$. Siden $1 \leq i \leq m$, er $1 \leq i \leq m + 1$. Dermed stemmer utsagnet vi ønsker å bevise.

Således er korollaret sant når $n = m + 1$. Ved induksjon konkluderer vi at korollaret er sant for alle naturlige tall. □

Eksempel 4.2.20. Vi har: $5 \mid 180$ og $180 = 2 \cdot 15 \cdot 6$. Korollar 4.2.19 fastslår at et av følgende er sant: $5 \mid 2$, $5 \mid 15$, $5 \mid 6$. Det er riktignok sant at $5 \mid 15$.

Eksempel 4.2.21. Vi har: $3 \mid 540$ og $540 = 6 \cdot 10 \cdot 9$. Korollar 4.2.19 fastslår at et av følgende er sant: $3 \mid 6$, $3 \mid 10$, $3 \mid 9$. Det er riktignok sant at $3 \mid 6$, og faktisk også sant at $3 \mid 9$.

Merknad 4.2.22. Korollar 4.2.19 er ikke sant om vi ikke antar at p er et primtall. Hvis for eksempel $x_1 = 8$, $x_2 = 9$, $x_3 = 11$, og $p = 6$, har vi: $6 \mid 792$. Imidlertid er ikke noe av følgende sant: $6 \mid 8$, $6 \mid 9$, eller $6 \mid 11$.

Korollar 4.2.23. La n være et naturlig tall. For hvert naturlig tall i slik at $1 \leq i \leq n$, la p_i være et primtall. La p være et primtall. Dersom $p \mid p_1 \cdots p_n$, finnes det et naturlig tall i slik at $1 \leq i \leq n$ og $p = p_i$.

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Korollar 4.2.19 finnes det et naturlig tall i slik at $1 \leq i \leq n$ og $p \mid p_i$.

(2) Siden p_i er et primtall, er 1 og p_i de eneste divisorene til p_i.

Det følger fra (1) og (2) at enten $p = 1$ eller $p = p_i$. Siden p er et primtall, er $p \geq 2$. Vi konkluderer at $p = p_i$.

□

Eksempel 4.2.24. Vi har: $30 = 2 \cdot 3 \cdot 5$. Dersom p er et primtall og $p \mid 30$, fastslår Korollar 4.2.23 at p er lik ett av 2, 3, eller 5.

Eksempel 4.2.25. Vi har: $441 = 3 \cdot 3 \cdot 7 \cdot 7$. Dersom p er et primtall og $p \mid 441$, fastslår Korollar 4.2.23 at p er lik enten 3 eller 7.

Merknad 4.2.26. Korollar 4.2.23 er ikke sant om vi ikke antar at p_i er et primtall for hvert naturlig tall i slik at $1 \leq i \leq n$. Hvis for eksempel $x_1 = 7$, $x_2 = 15$, og $p = 5$, har vi: $7 \cdot 15 = 105$ og $5 \mid 105$. Imidlertid er verken $5 = 7$ eller $5 = 15$.

Merknad 4.2.27. Korollar 4.2.23 er heller ikke sant om vi ikke antar at p er et primtall. Hvis for eksempel $x_1 = 3$, $x_2 = 23$, $x_3 = 5$, og $p = 15$, har vi: $3 \cdot 23 \cdot 5 = 345$ og $15 \mid 345$. Imidlertid er ikke noe av følgende sant: $15 = 3$, $15 = 23$, eller $15 = 5$.

Proposisjon 4.2.28. La p være et primtall. La a og c være heltall. Anta at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da her kongruensen

$$ax \equiv c \pmod{p}$$

en løsning, og alle løsningene til denne kongruensen er kongruent til hverandre modulo p.

Bevis. Siden det ikke er sant at $a \equiv 0 \pmod{p}$, følger det fra Proposisjon 3.2.13 at det ikke er sant at $p \mid a$. Siden p er et primtall, følger det fra Korollar 4.2.5 at $\mathsf{sfd}(a, p) = 1$. Da følger utsagnet fra Korollar 3.4.39. □

Eksempel 4.2.29. Siden 7 er et primtall og det ikke er sant at

$$4 \equiv 0 \pmod{7},$$

fastslår Proposisjon 4.2.28 at kongruensen

$$4x \equiv 6 \pmod{7}$$

har en løsning. Dette er riktignok sant: $x = 5$ er en løsning. Proposisjon 4.2.28 fastslår i tillegg at enhver annen løsning til kongruensen er kongruent til 5 modulo 7.

Eksempel 4.2.30. Siden 37 er et primtall og det ikke er sant at

$$12 \equiv 0 \pmod{37},$$

fastslår Proposisjon 4.2.28 at kongruensen

$$12x \equiv 28 \pmod{37}$$

har en løsning. Dette er riktignok sant: $x = 27$ er en løsning. Proposisjon 4.2.28 fastslår i tillegg at enhver annen løsning til kongruensen er kongruent til 27 modulo 37.

Proposisjon 4.2.31. La p være et primtall slik at $p > 2$. Da finnes det et naturlig tall k slik at $p - 1 = 2k$.

Bevis. Ut ifra Proposisjon 3.2.1 er ett av følgende utsagn sant:

(A) $p \equiv 0 \pmod{2}$;

(B) $p \equiv 1 \pmod{2}$.

Anta først at (A) er sant. Da har vi: $2 \mid p$. Siden p er et primtall, er 1 og p de eneste divisorene til p. Vi deduserer at $p = 2$. Imidlertid har vi antatt at $p > 2$. Siden antakelsen at (A) er sant fører til motsigelsen at både $p = 2$ og $p > 2$, konkluderer vi at (A) ikke er sant.

Derfor er (B) sant. Da følger det fra Korollar 3.2.39 at

$$p - 1 \equiv 0 \pmod 2,$$

altså

$$2 \mid p - 1.$$

Dermed finnes det et heltall k slik at $p - 1 = 2k$. Siden både 2 og $p - 1$ er naturlige tall, er k et naturlig tall. □

Eksempel 4.2.32. Siden 11 er et primtall og $11 > 2$, fastslår Proposisjon 4.2.31 at det finnes et naturlig tall k slik at $10 = 2k$. Dette er riktignok sant: vi kan la k være 5.

Eksempel 4.2.33. Siden 23 er et primtall og $23 > 2$, fastslår Proposisjon 4.2.31 at det finnes et naturlig tall k slik at $22 = 2k$. Dette er riktignok sant: vi kan la k være 11.

4.3 Aritmetikkens fundamentalteorem I

Merknad 4.3.1. Målet vårt i denne delen av kapittelet er å gi et bevis for Teorem 4.3.3. For å gjøre dette, må vi først endre påstanden i Teorem 4.3.3, for å kunne gjennomføre et bevis ved induksjon. Vi gjorde noe lignende da vi ga et bevis for Korollar 2.7.6 og et bevis for Korollar 2.10.20: se Merknad 2.7.4 og Merknad 2.10.18.

Proposisjon 4.3.2. La n være et naturlig tall slik at $n \geq 2$. La l være et naturlig tall slik at $2 \leq l \leq n$. Da finnes det et naturlig tall t og, for hvert naturlig tall i slik at $i \leq t$, et primtall p_i, slik at $l = p_1 p_2 \cdots p_t$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 2$. Da er $l = 2$, og utsagnet er: det finnes et naturlig tall t og, for hvert naturlig tall i slik at $i \leq t$, et primtall p_i, slik at

$$2 = p_1 p_2 \cdots p_t.$$

Siden 2 er et primtall, er dette sant: vi lar $t = 1$, og lar $p_1 = 2$.

Anta nå at proposisjonen har blitt bevist når $n = m$, hvor m er et gitt naturlig tall slik at $m \geq 2$. La l være et naturlig tall slik at $2 \leq l \leq m + 1$. Vi ønsker å bevise at det finnes et naturlig tall t og primtall p_i, for hvert naturlig tall i slik at $i \leq t$, slik at $l = p_1 p_2 \cdots p_t$.

Ut ifra definisjonen til et primtall, er ett av følgende sant:

(1) l er et primtall;

(2) det finnes et naturlig tall a slik at $1 < a < l$ og $a \mid l$.

Anta først at (1) er sant. Da rekker vi målet ved å la t være 1 og p_1 være l.

Anta istedenfor at (2) er sant. Da finnes det et naturlig tall k slik at $1 < k < l$ og $l = a \cdot k$. Vi gjør følgende observasjoner.

(1) Siden $l \leq m + 1$ og $a < l$, er $a < m + 1$, altså $a \leq m$.

(2) Siden $l \leq m+1$ og $k < l$, er $k < m+1$, altså $k \leq m$.

(3) Ut ifra antakelsen at proposisjonen er sann når $n = m$, følger det fra (1) at det finnes et naturlig tall s og primtall q_i, for hvert naturlig tall i slik at $i \leq s$, slik at $a = q_1 q_2 \cdots q_s$.

(4) Ut ifra antakelsen at proposisjonen er sann når $n = m$, følger det fra (2) at det finnes et naturlig tall s' og primtall q'_i, for hvert naturlig tall i slik at $i \leq s'$, slik at $k = q'_1 q'_2 \cdots q'_{s'}$.

(5) Det følger fra (4) at:

$$\begin{aligned} n &= ak \\ &= (q_1 \dots q_s)\left(q'_1 \cdots q'_{s'}\right) \\ &= q_1 \dots q_s q'_1 \dots q'_{s'}. \end{aligned}$$

Derfor rekker vi målet ved å la $t = s + s'$ og

$$p_i = \begin{cases} q_i & \text{if } 1 \leq i \leq s, \\ q'_{i-s} & \text{if } s+1 \leq i \leq t. \end{cases}$$

Dermed er proposisjonen sann når $n = m+1$. Ved induksjon konkluderer vi at den er sann for alle de naturlige tallene n slik at $n \geq 2$.

□

Teorem 4.3.3. La n være et naturlig tall slik at $n \geq 2$. Da finnes det et naturlig tall t og primtall p_i, for hvert naturlig tall i slik at $i \leq t$, slik at $n = p_1 p_2 \cdots p_t$.

Bevis. Følger umiddelbart fra Proposisjon 4.3.3 ved å la $l = n$. □

Terminologi 4.3.4. Teorem 4.3.3 og Teorem 4.7.2 kalles *aritmetikkens fundamentalteorem.*

Merknad 4.3.5. Aritmetikkens fundamentalteorem er ett av de vikigste teoremene i hele matematikken. Det er spesielt viktig i tallteori og algebra, og andre deler av matematikk som bygger på disse to, men det dukker opp overalt: til og med i knuteteori!

Eksempel 4.3.6. La n være 24. Teorem 4.3.3 fastslår at det finnes et naturlig tall t og primtall $p_1, \dots, p_t$ slik at $24 = p_1 \cdots p_t$. Det er riktignok sant at

$$24 = 2 \cdot 2 \cdot 2 \cdot 4.$$

Her er $t = 4$, $p_1 = p_2 = p_3 = 2$, og $p_4 = 3$.

Eksempel 4.3.7. La n være 63. Teorem 4.3.3 fastslår at det finnes et naturlig tall t og primtall $p_1, \dots, p_t$ slik at $63 = p_1 \cdots p_t$. Det er riktignok sant at

$$63 = 3 \cdot 3 \cdot 7.$$

Her er $t = 3$, $p_1 = p_2 = 3$, og $p_3 = 7$.

Eksempel 4.3.8. La n være 143. Teorem 4.3.3 fastslår at det finnes et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at $143 = p_1 \cdots p_t$. Det er riktignok sant at

$$143 = 11 \cdot 13.$$

Her er $t = 2$, $p_1 = 11$, og $p_2 = 13$.

Eksempel 4.3.9. La n være 125. Teorem 4.3.3 fastslår at det finnes et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at $125 = p_1 \cdots p_t$. Det er riktignok sant at

$$125 = 5 \cdot 5 \cdot 5.$$

Her er $t = 3$, og $p_1 = p_2 = p_3 = 5$.

Eksempel 4.3.10. La n være 7623. Teorem 4.3.3 fastslår at det finnes et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at $7623 = p_1 \cdots p_t$. Det er riktignok sant at

$$7623 = 3 \cdot 3 \cdot 7 \cdot 11 \cdot 11.$$

Her er $t = 5$, $p_1 = p_2 = 3$, $p_3 = 7$, og $p_4 = p_5 = 11$.

Terminologi 4.3.11. La n være et naturlig tall slik at $n \geq 2$. La t være et naturlig tall. For hvert naturlig tall i slik at $1 \leq i \leq t$, la p_i være et primtall. Anta at

$$n = p_1 \cdots p_t.$$

Vi sier at produktet $p_1 \cdots p_n$ er en *primtallsfaktorisering* av n.

Merknad 4.3.12. Ved å benytte denne terminologien, fastslår Teorem 4.3.3 at hvert naturlig tall har en primtallsfakorisering.

Merknad 4.3.13. Idéen bak beviset for Proposisjon 4.3.2, og dermed beviset for Teorem 4.3.3, er ganske enkel, og fører til en fin metode for å finne en primtallsfaktorisering til et naturlig tall i praksis. For å forklare dette, la oss se igjen på Eksempel 4.3.6.

(1) Vi kan begynne med å observere at $24 = 2 \cdot 12$. Siden 12 er ikke er primtall, har vi ikke rukket en primtallsfaktorisering av 24 ennå.

(2) Vi observerer at $12 = 2 \cdot 6$. Derfor er

$$24 = 2 \cdot 2 \cdot 6.$$

Siden 6 er ikke er primtall, har vi fremdeles rukket en primtallsfaktorisering av 24..

(3) Vi observerer at $6 = 2 \cdot 3$. Derfor er

$$24 = 2 \cdot 2 \cdot 2 \cdot 3.$$

Både 2 og 3 er primtall. Dermed har vi rukket en primtallsfaktorisering av 24: vi kan la t være 4, p_1 være 2, p_2 være 2, p_3 være 2, og p_4 være 3.

Dette er ikke det eneste gyldige argumentet. Istedenfor kan vi gjør følgende.

(1) Begynn med å observere at $24 = 6 \cdot 4$. Siden 6 og 4 ikke er primtall, har vi ikke rukket en primtallsfaktorisering av 24 ennå.

(2) Observer at $6 = 2 \cdot 3$ og at $4 = 2 \cdot 2$. Derfor er

$$24 = 2 \cdot 3 \cdot 2 \cdot 3.$$

Både 2 og 3 er primtall. Dermed har vi rukket en primtallsfaktorisering av 24: vi kan la t være 4, p_1 være 2, p_2 være 3, p_3 være 2, og p_4 være 3.

La merke til at primtallene $p_1, \ldots, p_t$ er de samme som vi fikk tidligere. Det er kun rekkefølgene som er annerledes.

Det er dessuten mulig å begynne med å observere at

$$24 = 8 \cdot 3.$$

Da kan vi fortsette som ovenfor.

La oss oppsummere.

(1) Siden 24 ikke er et primtall, finnes det minst ett par naturlige tall a og k slik at $24 = ak$, $1 < a < 24$, og $1 < k < 24$. For å finne en primtallsfakorisering av 24, er det nok å finne en primtallsfaktorisering av a og en primtallsfaktorisering av b.

(2) Hvis både a og b er primtall, har vi rukket målet. Ellers kan vi uttrykke a eller b, eller begge to, som et produkt av naturlige tall som er større enn 1. Det er nok å finne en primtallsfaktorisering av disse naturlige tallene.

(3) Slik fortsetter vi.

Uansett hvilket produkt $24 = ab$ vi begynner med, viser det seg at vi får den samme primstallsfaktoriseringen til 24, bortsett fra rekkefølgen av primtallene. Den andre delen av aritmetikkens fundamentalteorem, som vi kommer til å gi et bevis for senere, fastslår at dette er tilfellet for et hvilket som helst naturlig tall, ikke kun 24.

Eksempel 4.3.14. La oss gjennomføre metoden i Merknad 4.3.13 for å finne en primtallsfaktorisering til 600. For eksempel kan vi regne som følger:

$$\begin{aligned} 600 &= 50 \cdot 12 \\ &= (10 \cdot 5) \cdot (2 \cdot 6) \\ &= 10 \cdot 5 \cdot 2 \cdot 6 \\ &= (5 \cdot 2) \cdot 5 \cdot 2 \cdot (2 \cdot 3) \\ &= 5 \cdot 2 \cdot 5 \cdot 2 \cdot 2 \cdot 3. \end{aligned}$$

Dermed er

$$5 \cdot 2 \cdot 5 \cdot 2 \cdot 2 \cdot 3$$

en primtallsfaktorisering av 600. Ved å endre rekkefølgen av primtallene i denne faktoriseringen litt, får vi

$$2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5.$$

Vi kan gjennomføre metoden i Merknad 4.3.13 på mange andre måter. For eksempel kan vi regne som følger:

$$\begin{aligned} 600 &= 6 \cdot 100 \\ &= (3 \cdot 2) \cdot (10 \cdot 10) \\ &= 3 \cdot 2 \cdot 10 \cdot 10 \\ &= 3 \cdot 2 \cdot (2 \cdot 5) \cdot (5 \cdot 2) \\ &= 3 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 2. \end{aligned}$$

Ved å endre rekkefølgen av primtallene i denne faktoriseringen litt, ser vi at vi har rukket den samme primtallsfaktoriseringen som ovenfor, nemlig

$$2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5.$$

Eksempel 4.3.15. La oss gjennomføre metoden i Merknad 4.3.13 for å finne en primtallsfaktorisering til 126. Vi kan regne som følger:

$$\begin{aligned} 126 &= 2 \cdot 63 \\ &= 2 \cdot (9 \cdot 7) \\ &= 2 \cdot 9 \cdot 7 \\ &= 2 \cdot (3 \cdot 3) \cdot 7 \\ &= 2 \cdot 3 \cdot 3 \cdot 7 \end{aligned}$$

Dermed er

$$2 \cdot 3 \cdot 3 \cdot 7$$

en primtallsfaktorisering av 126.

Alternativt kan vi for eksempel regne som følger:

$$\begin{aligned} 126 &= 3 \cdot 42 \\ &= 3 \cdot (21 \cdot 2) \\ &= 3 \cdot 21 \cdot 2 \\ &= 3 \cdot (7 \cdot 3) \cdot 2 \\ &= 3 \cdot 7 \cdot 3 \cdot 2. \end{aligned}$$

Dermed er

$$3 \cdot 7 \cdot 3 \cdot 2$$

en primtallsfaktorisering av 126. Ved å endre rekkefølgen av primtallene i denne faktoriseringen litt, ser vi at vi har rukket den sammen primtallsfaktoriseringen som ovenfor, nemlig

$$2 \cdot 3 \cdot 3 \cdot 7.$$

For å gjennomføre metoden i Merknad 4.3.13, må vi finne først et naturlig tall som deler 126. I praksis er det sannsynlig at vi hadde først lagt merke til at $2 \mid 126$, og deretter regnet som ovenfor, ved å begynne med produktet

$$126 = 2 \cdot 63.$$

Likevel er alle andre måter å gjennomføre metoden i Merknad 4.3.13 like verdifulle. For eksempel er det usannsynlig at vi først kommer fram til produktet

$$126 = 14 \cdot 9,$$

men om det er tilfellet, kan vi godt regne som følger:

$$\begin{aligned} 126 &= 14 \cdot 9 \\ &= (7 \cdot 2) \cdot (3 \cdot 3) \\ &= 7 \cdot 2 \cdot 3 \cdot 3. \end{aligned}$$

Dermed er

$$7 \cdot 2 \cdot 2 \cdot 3$$

en primtallsfaktorisering av 126. Ved å endre rekkefølgen av primtallene i denne faktoriseringen litt, ser vi at vi har rukket den sammen primtallsfaktoriseringen som ovenfor, nemlig

$$2 \cdot 3 \cdot 3 \cdot 7.$$

Korollar 4.3.16. La n være et naturlig tall. Da finnes det et naturlig tall t, primtall $p_1, p_2, \ldots, p_t$, og naturlige tall $k_1, k_2, \ldots, k_t$ slik at

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_t^{k_t},$$

og slik at $p_i \neq p_j$ om $i \neq j$.

Bevis. Ut ifra Teorem 4.3.3, finnes det et naturlig tall s og primtall $q_1, q_2, \ldots, q_s$ slik at

$$n = q_1 \cdots q_s.$$

La $p_1, p_2, \ldots, p_t$ være de primtallene blant $q_1, q_2, \ldots, q_s$ som forblir etter å ha hevde alle repetisjoner. Da er $q_i \neq q_j$ dersom $i \neq j$.

For hvert naturlig tall i slik at $i \leq t$, la k_i være antall primtall blant $q_1, q_2, \ldots, q_s$ som er like p_i, altså antall ledd i produktet $q_1 \cdots q_s$ som er like p_i. Ved å bytte om rekkefølgen av primtallene i produktet, er da

$$n = \underbrace{p_1 p_1 \cdots p_1}_{k_1 \text{ ganger}} \cdot \underbrace{p_2 p_2 \cdots p_2}_{k_2 \text{ ganger}} \cdots \underbrace{p_s p_s \cdots p_s}_{k_s \text{ ganger}}.$$

Dermed er

$$n = p_1^{k_1} \cdots p_t^{k_t}.$$

□

Eksempel 4.3.17. Ut ifra Eksempel 4.3.14 er $2^3 \cdot 3 \cdot 5^2$ en primtallsfaktorisering til 600.

Eksempel 4.3.18. Ut ifra Eksempel 4.3.15 er $2 \cdot 3^2 \cdot 7$ en primtallsfaktorisering til 126.

Korollar 4.3.19. La n være et naturlig tall slik at $n > 1$. Da finnes det et primtall p slik at $p \mid n$.

Bevis. Ut ifra Teorem 4.3.3, finnes det et naturlig tall t og primtall $p_1, p_2, \ldots, p_t$ slik at

$$n = p_1 \cdots p_t.$$

Dersom $t = 1$, er n et primtall. Siden $n \mid n$, er korollaret i dette tilfellet.
Dersom $t > 1$, er

$$n = (p_1 \cdots p_{t-1}) \cdot p_t,$$

altså $p_t \mid n$. □

Merknad 4.3.20. Et hvilket som helst av primtallene $p_1, p_2, \ldots, p_t$ kan benyttes istedenfor p_t i beviset for Korollary 4.3.19.

Eksempel 4.3.21. Korollar 4.3.19 fastslår at det naturlige tallet 231 er delelig med et primtall. Siden $231 = 21 \cdot 11$, har vi riktignok: $11 \mid 231$.

Eksempel 4.3.22. Korollar 4.3.19 fastslår at det naturlige tallet 24843 er delelig med et primtall. Siden $24843 = 1911 \cdot 13$, har vi riktignok: $13 \mid 24843$.

4.4 Det finnes uendelig mange primtall

Merknad 4.4.1. Ved hjelp av aritmetikkens fundamentalteorem kan vi nå bevise et teorem går helt tilbake til Antikkens Hellas, og er ett av de meste berømte teoremene i hele matematikken.

Teorem 4.4.2. La n være et naturlig tall. Da finnes det et primtall p slik at $p > n$.

Bevis. La q være produktet av alle primtallene som er mindre enn eller like n. Ut ifra Teorem 4.3.3, finnes det et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at

$$q + 1 = p_1 \cdots p_t.$$

Anta at $p_1 \leq n$. Vi gjør følgende observasjoner.

(1) Ut ifra definisjonen til q og antakelsen at $p_1 \leq n$, følger det at $p_1 \mid q$.

(2) Siden

$$q + 1 = p_1 \cdot (p_2 \cdots p_t),$$

har vi: $p_1 \mid q + 1$.

(3) Det følger fra (1) og Proposisjon 2.5.12 at $p_1 \mid -q$.

(4) Det følger fra (2), (3), og Proposisjon 2.5.24 at $p_1 \mid (q+1) - q$, altså at $p_1 \mid 1$.

Siden p_1 er et primtall, er $p_1 \geq 2$. Det kan ikke være sant at både $p_1 \mid 1$ og $p_1 \geq 2$. Siden antakelsen at $p_1 \leq n$ fører til denne motsigelsen, deduserer vi at det ikke er sant at $p_1 \leq n$. Derfor er $p_1 > n$.

□

Merknad 4.4.3. Det er ikke noe spesielt med p_1 i beviset for Teorem 4.4.2. Det samme argumentet viser at $p_i > n$ for alle primtallene p_1, p_2, ..., p_t som dukker opp i primtallsfaktorisingen til $q+1$ i beviset.

Merknad 4.4.4. Teorem 4.4.2 fastslår at det finnes uendelig mange primtall: uansett hvor stort et naturlig tall er, kan vi alltid finne et større primtall.

Eksempel 4.4.5. La oss gå gjennom beviset for Teorem 4.4.2 når $n = 14$. Det finnes seks primtall som er mindre enn eller likt 14, nemlig 2, 3, 5, 7, 11, og 13. La q være produktet av disse primtallene, altså

$$q = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13.$$

Dette produktet er likt 30030. Beviset for Teorem 4.4.2 fastslår at hvert primtall i en primtallsfaktorisering av $q+1$, altså av 30031, er større enn 14. Vi har:

$$30031 = 59 \cdot 509,$$

og både 59 og 509 er primtall. Med andre ord, er primtallet p_1 i beviset for Teorem 4.4.2 likt 59 i dette tilfellet: det er riktignok at $59 > 14$.

Merknad 4.4.6. Ofte er beviset for Teorem 4.4.2 misforstått: det fastslår *ikke* at $q+1$ er et primtall som er større enn n, hvor q er produktet av de primtallene som er mindre enn eller likt n. Det er sant at $q+1 > n$, men det er *ikke* nødvendigvis sant at $q+1$ er et primtall. Som vi så i Eksempel 4.4.5, er $q+1$ ikke et primtall når $n = 14$. Med andre ord, er

$$(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) + 1$$

ikke et primtall: det er delelig med 59 og med 509.

Som vi har sett, fastslår Teorem 4.4.2 heller at hvert primtall i en primtallsfaktorisering av $q+1$ er større enn n.

Eksempel 4.4.7. Noen ganger er imidlertid $q+1$ selv et primtall. La oss gå for eksempel gjennom beviset for Teorem 4.4.2 når $n = 8$. Det finnes fire primtall som er mindre enn eller likt 8, nemlig 2, 3, 5, og 7. La q være produktet av disse primtallene, altså

$$q = 2 \cdot 3 \cdot 5 \cdot 7.$$

Dette produktet er lik 210. Beviset for Teorem 4.4.2 fastslår at hvert primtallene i en primtallsfaktorisering av $q+1$, altså av 211, er større enn 8. Faktisk er 211 et primtall, og derfor er 211 selv en primtallsfaktorisering, med ett ledd i produktet, av 211. Med andre ord, er primtallet p_1 i beviset for Teorem 4.4.2 lik 211 i dette tilfellet: det er riktignok at $211 > 8$.

Merknad 4.4.8. Argumentet bak beviset for Teorem 4.4.2 kan tilpasses for å bevise at andre lignende påstander sanne. La oss se på et eksempel.

Proposisjon 4.4.9. La n være et heltall slik at $n \geq 0$. Da finnes det et primtall p slik at $p \equiv 3 \pmod 4$ og $p > n$.

Bevis. La q være produktet av alle primtallene som er mindre enn eller like n, og som er kongruent til 3 modulo 4. Ut ifra Teorem 4.3.3 finnes det et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at

$$4q - 1 = p_1 \cdots p_t.$$

Ut ifra Proposisjon 3.2.1 er, for hvert naturlig tall i slik at $i \leq t$, ett av følgende sant:

(1) $p_i \equiv 0 \pmod 4$;

(2) $p_i \equiv 1 \pmod 4$;

(3) $p_i \equiv 2 \pmod 4$;

(4) $p_i \equiv 3 \pmod 4$;

Anta først at (1) er sant for et naturlig tall $i \leq t$.. Da følger det fra Korollar 3.2.45 at

$$(p_1 \cdots p_{i-1}) \cdot p_i \cdot (p_{i+1} \cdots p_t) \equiv (p_1 \cdots p_{i-1}) \cdot 0 \cdot (p_{i+1} \cdots p_t) \pmod 4,$$

altså at

$$4q - 1 \equiv 0 \pmod 4.$$

Imidlertid er

$$4q - 1 \equiv 3 \pmod 4.$$

Siden $0 \neq 3$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$4q - 1 \equiv 0 \pmod 4$$

og

$$4q - 1 \equiv 3 \pmod 4.$$

Siden antakelsen at (1) er sant fører til denne motigelsen, konkluderer vi at (1) ikke er sant.

Anta nå at (3) er sant for et naturlig tall $i \leq t$. Siden $2 \mid 4$, følger det da fra Proposisjon 3.2.54 at $p_i \equiv 0 \pmod 2$. Da følger det fra Korollar 3.2.45 at

$$(p_1 \cdots p_{i-1}) \cdot p_i \cdot (p_{i+1} \cdots p_t) \equiv (p_1 \cdots p_{i-1}) \cdot 0 \cdot (p_{i+1} \cdots p_t) \pmod 2,$$

altså at

$$4q - 1 \equiv 0 \pmod 2.$$

Imidlertid er

$$4q - 1 \equiv 1 \pmod 2.$$

Siden $0 \neq 1$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$4q - 1 \equiv 0 \pmod{2}$$

og

$$4q - 1 \equiv 1 \pmod{4}.$$

Siden antakelsen at (3) er sant fører til denne motigelsen, konkluderer vi at (3) ikke er sant.

Anta nå at (2) er sant for alle de naturlige tallene i slik at $i \leq t$. Da følger det fra Proposisjon 3.2.42 at

$$p_1 \cdots p_t \equiv 1^t \pmod{4},$$

altså at

$$4q - 1 \equiv 1 \pmod{4}.$$

Imidlertid er

$$4q - 1 \equiv 3 \pmod{4}.$$

Siden $1 \neq 3$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$4q - 1 \equiv 1 \pmod{4}$$

og

$$4q - 1 \equiv 3 \pmod{4}.$$

Siden antakelsen at (2) er sant fører til denne motigelsen, konkluderer vi at (2) ikke er sant for alle de naturlige tallene i slik at $i \leq t$.

Derfor finnes det et naturlig tall i, hvor $i \leq t$, slik at (4) er sant, altså at $p_i \equiv 3 \pmod{4}$. Anta at $p_i \leq n$. Vi gjør følgende observasjoner.

(1) Siden $p_i \equiv 3 \pmod{4}$, følger det fra definisjonen til q og antakelsen at $p_i \leq n$ at $p_i \mid q$.

(2) Siden

$$4q - 1 = p_i \cdot (p_1 \cdots p_{i-1} p_{i+1} \cdots p_t),$$

har vi: $p_i \mid 4q - 1$.

(3) Det følger fra (1) og Korollar 2.5.18 at $p_i \mid 4q$.

(4) Det følger fra (2) og Korollar 2.5.18 at $p_i \mid -(4q - 1)$.

(5) Det følger fra (3), (4), og Proposisjon 2.5.24 at $p_i \mid 4q - (4q - 1)$, altså at $p_i \mid 1$.

Siden p_i er et primtall, er $p_i \geq 2$. Det kan ikke være sant at både $p_i \mid 1$ og $p_i \geq 2$. Siden antakelsen at $p_i \leq n$ fører til denne motsigelsen, deduserer vi at det ikke er sant at $p_i \leq n$. Derfor er $p_i > n$.

□

Merknad 4.4.10. De første 10 primtallene som er kongruent til 3 modulo 4 er: 3, 7, 11, 19, 23, 31, 43, 47, 59, og 67. Proposisjon 4.4.9 fastslår at det finnes uendelig mange slike primtall: uansett hvor stort et naturlig tall er, finnes det alltid et primtall kongruent til 3 modulo 4 som er større.

Merknad 4.4.11. Beviset for Proposisjon 4.4.9 gir oss en metode for å finne et primtall kongruent til 3 modulo 4 som er større enn et bestemt naturlig tall n: ett av primtallene i en primtallsfaktorisering av $4q - 1$ er et primtall kongruent til 3 modulo 4, hvor q er produktet av alle de primtallene mindre enn eller likt n som er kongruent til 3 modulo 4.

Eksempel 4.4.12. La n være 22. Primtallene som er mindre enn eller likt 22, og som er kongruent til 3 modulo 4, er 3, 7, 11, og 19. La $q = 3 \cdot 7 \cdot 11 \cdot 19$, altså $q = 4389$. Da er $4q - 1 = 17555$. En primtallsfakorisering av 17555 er $5 \cdot 3511$. Beviset for Proposisjon 4.4.9 fastslår at enten 5 eller 3511 er større enn 22 og kongruent til 3 modulo 4. Det er riktignok sant at $3511 > 22$ og $3511 \equiv 3 \pmod 4$.

4.5 Eksempler på bevis for utsagn om primtall hvor kongruenser benyttes

Merknad 4.5.1. I §2.4 av Kapittel 2, så vi at vi kan benytte divisjonsalgoritmen for å dele i tilfeller et bevis for et utsagn om heltallene. I denne delen av kapittelet skal vi se på et par eksempler hvor vi benytter den samme tilnærmingsmetoden, men hvor vi benytter kongruenser istedenfor å benytte divisjonsalgoritmen direkte. Da blir tilnærmingsmetoden mer elegant, og fortere å gjennomføre. I tillegg skal vi se på hvordan en antakelse om primtall kan benyttes når vi gjennomføre et slikt bevis.

Proposisjon 4.5.2. La n være et heltall slik at $n \geq 0$. Da finnes det et heltall $m \geq 0$ slik at $3m + 2$ er et primtall, og $3m + 2 \mid 3n + 2$.

Bevis. Ut ifra Teorem 4.3.3 finnes det et naturlig tall t og, for hvert naturlig tall i slik at $i \leq t$, et primtall p_i, slik at

$$3n + 2 = p_1 \cdots p_t.$$

Ut ifra Proposisjon 3.2.1 er, for hvert naturlig tall i slik at $i \leq t$, ett av følgende sant:

(A) $p_i \equiv 0 \pmod 3$;

(B) $p_i \equiv 1 \pmod 3$;

(C) $p_i \equiv 2 \pmod 3$.

Vi skal gjennomføre beviset i hvert tilfelle hvert for seg.

Anta først at (A) er sant for et naturlig tall i slik at $i \leq t$. Fra Korollar 3.2.45, har vi da:

$$(p_1 \cdots p_{i-1}) \cdot p_i \cdot (p_{i+1} \cdots p_t) \equiv (p_1 \cdots p_{i-1}) \cdot 0 \cdot (p_{i+1} \cdots p_t) \pmod 3,$$

altså

$$(p_1 \cdots p_{i-1}) \cdot p_i \cdot (p_{i+1} \cdots p_t) \equiv 0 \pmod 3.$$

Dermed er

$$3n + 2 \equiv 0 \pmod 3.$$

Imidlertid er

$$3n + 2 \equiv 2 \pmod 3.$$

Siden $0 \neq 2$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$3n + 2 \equiv 0 \pmod 3$$

og

$$3n + 2 \equiv 2 \pmod 3.$$

Siden antakelsen at (A) er sant fører til denne motigelsen, konkluderer vi at (A) ikke er sant.

Anta nå at (B) er sant for alle de naturlige tallene $i \leq t$. Fra Proposisjon 3.2.42 har vi da:

$$p_1 \cdots p_n \equiv 1^i \pmod 3,$$

altså

$$3n + 2 \equiv 1 \pmod 3.$$

Imidlertid er

$$3n + 2 \equiv 2 \pmod 3.$$

Siden $1 \neq 2$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$3n + 2 \equiv 1 \pmod 3$$

og

$$3n + 2 \equiv 2 \pmod 3.$$

Siden antakelsen at (B) er sant fører til denne motigelsen, konkluderer vi at (B) ikke er sant for alle de naturlige tallene i slik at $i \leq t$.

Derfor finnes det et naturlig tall i, hvor $i \leq t$, slik at (C) er sant, altså at

$$p_i \equiv 2 \pmod 3.$$

Ut ifra definisjonen til denne kongruensen, har vi da: $3 \mid p_i - 2$. Dermed finnes det et heltall m slik at $m \geq 0$ og $p_i = 3m + 2$. Siden

$$3n + 2 = p_i \cdot (p_1 \cdots p_{i-1} p_{i+1} \cdots p_t),$$

har vi i tillegg:

$$p_i \mid 3n + 2.$$

Således er $3m + 2$ et primtall som deler $3n + 2$.

□

Merknad 4.5.3. Med andre ord, fastslår Proposisjon 4.5.2 at hvert naturlig tall som er lik $3n + 2$ for noen heltall $n \geq 0$, er delelig med et primtall som er lik $3m + 2$ for noen heltall $m \geq 0$.

Eksempel 4.5.4. Siden $119 = 3 \cdot 39 + 2$, fastslår Proposisjon 4.5.2 at det finnes et primtall som både deler 119 og er lik $3m + 2$ for noen heltall $m \geq 0$. Riktignok har vi:

(1) $17 \mid 119$;

(2) 17 er et primtall;

(3) $17 = 3 \cdot 5 + 2$.

Med andre ord, kan vi la $m = 5$.

Eksempel 4.5.5. Siden $32 = 3 \cdot 10 + 2$, fastslår Proposisjon 4.5.2 at det finnes et primtall som både deler 32 og er lik $3m + 2$ for noen heltall $m \geq 0$. Riktignok har vi:

(1) $2 \mid 32$;

(2) 2 er et primtall;

(3) $2 = 3 \cdot 0 + 2$.

Med andre ord, kan vi la $m = 0$.

Eksempel 4.5.6. Siden $47 = 3 \cdot 15 + 2$, fastslår Proposisjon 4.5.2 at det finnes et primtall som både deler 47 og er lik $3m + 2$ for noen heltall $m \geq 0$. Faktisk er 47 selv et primtall: vi kan la $m = 15$.

Proposisjon 4.5.7. La p være et primtall slik at $p \geq 5$. Da er $p^2 + 2$ delelig med 3.

Bevis. Ut ifra Proposisjon 3.2.1 er ett av følgende sant:

(A) $p \equiv 0 \pmod 6$;

(B) $p \equiv 1 \pmod 6$;

(C) $p \equiv 2 \pmod 6$;

(D) $p \equiv 3 \pmod 6$;

(E) $p \equiv 4 \pmod 6$;

(F) $p \equiv 5 \pmod 6$.

Anta først at (A) er sant. Fra Proposisjon 3.2.13 har vi da: $6 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Derfor er $p = 6$. Imidlertid er 6 ikke et primtall. Siden antakelsen at (A) er sant fører til motsigelsen at p både er og er ikke et primtall, konkluderer vi at (A) ikke er sant.

Anta nå at (C) er sant. Ut ifra Proposisjon 3.2.54 er da $p \equiv 0 \pmod 2$. Fra Proposisjon 3.2.13 følger det at: $2 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Derfor er $p = 2$. Imidlertid er $2 < 5$. Siden antakelsen at (C) er sant fører til motsigelsen at både $p \geq 5$ og $p < 5$, konkluderer vi at (C) ikke er sant.

Anta nå at (D) er sant. Ut ifra Proposisjon 3.2.54 er da $p \equiv 0 \pmod 3$. Fra Proposisjon 3.2.13 følger det at: $3 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Derfor er $p = 3$. Imidlertid er $3 < 5$. Siden antakelsen at (D) er sant fører til motsigelsen at både $p \geq 5$ og $p < 5$, konkluderer vi at (D) ikke er sant.

Anta nå at (E) er sant. Vi har: $4 \equiv -2 \pmod 6$. Ut ifra Proposisjon 3.2.33 er da

$$p \equiv -2 \pmod 6.$$

Fra Proposisjon 3.2.54 følger det at $p \equiv 0 \pmod{-2}$. Fra Korollar 3.2.22 deduserer vi at $p \equiv 0 \pmod 2$. Ut ifra Proposisjon 3.2.13 har vi da: $2 \mid p$. Som i tilfellet hvor vi antok at (C) var sant, konkluderer vi at (E) ikke er sant.

Anta nå at (B) er sant. Fra Proposisjon 3.2.48 følger det at

$$p^2 \equiv 1^2 \pmod 6,$$

altså at

$$p^2 \equiv 1 \pmod 6.$$

Da følger det fra Korollar 3.2.39 at

$$p^2 + 2 \equiv 1 + 2 \pmod 6,$$

altså at

$$p^2 + 2 \equiv 3 \pmod 6.$$

Ut ifra Proposisjon 3.2.54 er da

$$p^2 + 2 \equiv 0 \mod 3.$$

Fra Proposisjon 3.2.13 har vi da: $3 \mid p^2 + 2$.

Anta nå at (F) er sant. Vi har: $5 \equiv -1 \pmod 6$. Ut ifra Proposisjon 3.2.33 er da

$$p \equiv -1 \pmod 6.$$

Fra Proposisjon 3.2.48 følger det at

$$p^2 \equiv (-1)^2 \pmod 6,$$

altså at

$$p^2 \equiv 1 \pmod 6.$$

Som i tilfellet hvor vi antok at (B) var sant, følger det at: $3 \mid p^2 + 2$.

□

Merknad 4.5.8. Det følger fra Proposisjon 4.5.7 at, dersom $p \geq 5$ er et primtall, er $p^2 + 2$ ikke et primtall.

Eksempel 4.5.9. La $p = 11$. Proposisjon 4.5.7 fastslår at $11^2 + 2$, altså 123, er delelig med 3. Dette er riktignok sant: $123 = 41 \cdot 3$.

Eksempel 4.5.10. La $p = 17$. Proposisjon 4.5.7 fastslår at $17^2 + 2$, altså 291, er delelig med 3. Dette er riktignok sant: $291 = 97 \cdot 3$.

4.6 Primtallsfaktoriseringer og største felles divisor

Proposisjon 4.6.1. La n og n' være naturlige tall. Anta at

$$n = p_1 \cdots p_t,$$

hvor t er et naturlig tall og, for hvert naturlig tall i slik at $i \leq t$, p_i er et primtall. Anta dessuten at

$$n' = p'_1 \cdots p'_{t'},$$

hvor t' er et naturlig tall og, for hvert naturlig tall i' slik at $i' \leq t'$, $p_{i'}$ er et primtall. La q_1, q_2, …, q_s være alle primtallene slik at, for hvert naturlig tall j slik at $j \leq s$, finnes det naturlige tall i og i' slik at $q_j = p_i$ og $q_j = p'_i$, hvor $i \leq t$ og $i' \leq t'$. Da er

$$\mathsf{sfd}(n, n') = q_1 \cdots q_s.$$

Bevis. La k være produktet av alle primtallene blant p_1, …, p_t som ikke er like q_j for noen naturlig tall j slik at $j \leq s$. Da er

$$n = k \cdot (q_1 \cdots q_s),$$

altså

$$q_1 \cdots q_s \mid n.$$

La k' være produktet av alle primtallene blant p'_1, …, $p'_{t'}$ som ikke er like q_j for noen naturlig tall j slik at $j \leq s$. Da er

$$n' = k' \cdot (q_1 \cdots q_s),$$

altså

$$q_1 \cdots q_s \mid n'.$$

La c være et naturlig tall slik at $c \mid n$ og $c \mid n'$. Ut ifra Teorem 4.3.3, finnes det et naturlig tall u og, for hvert naturlig tall l slik at $l \leq u$, et primtall p_l, slik at

$$c = p_1 \cdots p_u.$$

Vi gjør følgende observasjoner.

(1) For hvert naturlig tall l slik at $l \leq u$, er

$$c = (p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_u) \cdot p_l.$$

Dermed har vi: $p_l \mid c$.

(2) Siden $c \mid n$, følger det fra (1) og Proposisjon 2.5.27 at $p_l \mid n$ for hvert naturlig tall l slik at $l \leq u$.

(3) Det følger fra (2) og Korollar 4.2.23 at, for hvert naturlig tall l slik at $l \leq u$, finnes det et naturlig tall i slik at $i \leq t$ og $p_l = p_i$.

(4) Siden $c \mid n'$, følger det fra (1) og Proposisjon 2.5.27 at $p_l \mid n'$ for hvert naturlig tall l slik at $l \leq u$.

(5) Det følger fra (4) og Korollar 4.2.23 at, for hvert naturlig tall l slik at $l \leq u$, finnes det et naturlig tall i' slik at $i' \leq t'$ og $p_l = p_{i'}$.

(6) Det følger fra (3) og (5) at, for hvert naturlig tall l slik at $l \leq u$, finnes det et naturlig tall j slik at $j \leq s$ og $p_l = q_s$.

La m være produktet av alle primtallene blant $q_1, \ldots, q_s$ som ikke er like p_l for noen naturlig tall l slik at $l \leq u$. Da er

$$q_1 \cdots q_s = m \cdot (p_1 \cdots p_u),$$

altså

$$q_1 \cdots q_s = m \cdot c.$$

Dermed har vi:

$$c \mid q_1 \cdots q_s.$$

Det følger fra Proposisjon 2.5.30 at $c \leq q_1 \cdots q_s$. Således har vi bevist at:

(I) $q_1 \cdots q_s \mid n$;

(II) $q_1 \cdots q_s \mid n'$;

(III) dersom c er et naturlig tall slik at $c \mid n$ og $c \mid n'$, er

$$c \leq q_1 \cdots q_s.$$

Vi konkluderer at

$$\mathsf{sfd}(n, n') = q_1 \cdots q_s.$$

□

Merknad 4.6.2. Proposisjon 4.6.1 gir oss en ny tilnærmingsmetode for å finne den største felles divisoren til et par naturlig tall n og n':

(1) finn en primtallsfaktorisering av n og en primtallsfaktorisering av n';

(2) da er $\mathsf{sfd}(n, n')$ lik produktet av alle primtallene som dukker opp i begge primtallsfaktoriseringene.

Eksempel 4.6.3. La oss benytte oss av denne tilnærmingsmetoden for å finne $\mathsf{sfd}(105, 30)$. En primtallsfaktorisering av 105 er

$$3 \cdot 5 \cdot 7.$$

En primtallsfaktorisering av 30 er

$$2 \cdot 3 \cdot 5.$$

Primtallene som dukker opp i begge primtallsfaktoriseringene er 3 og 5. Proposisjon 4.6.1 fastslår at

$$\mathsf{sfd}(105, 30) = 3 \cdot 5,$$

altså at

$$\mathsf{sfd}(105, 30) = 15.$$

Eksempel 4.6.4. La oss benytte oss av denne tilnærmingsmetoden for å finne $\mathsf{sfd}(180, 216)$. En primtallsfaktorisering av 180 er

$$2 \cdot 2 \cdot 3 \cdot 3 \cdot 5.$$

En primtallsfaktorisering av 216 er

$$2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3.$$

Primtallene som dukker opp i begge primtallsfaktoriseringene er 2 (to ganger) og 3 (to ganger). Proposisjon 4.6.1 fastslår at

$$\mathsf{sfd}(180, 216) = 2 \cdot 2 \cdot 3 \cdot 3,$$

altså at

$$\mathsf{sfd}(180, 216) = 36.$$

Eksempel 4.6.5. La oss benytte oss av denne tilnærmingsmetoden for å finne

$$\mathsf{sfd}(254163, 4952038).$$

En primtallsfaktorisering av 254163 er

$$3 \cdot 7 \cdot 7 \cdot 7 \cdot 13 \cdot 19.$$

En primtallsfaktorisering av 4952038 er

$$2 \cdot 7 \cdot 7 \cdot 13 \cdot 13 \cdot 13 \cdot 23.$$

Primtallene som dukker opp i begge primtallsfaktoriseringene er 7 (to ganger) og 13. Proposisjon 4.6.1 fastslår at

$$\mathsf{sfd}(254163, 4952038) = 7 \cdot 7 \cdot 13,$$

altså i at

$$\mathsf{sfd}(254163, 4952038) = 637.$$

4.7 Aritmetikkens fundamentalteorem II

Merknad 4.7.1. Teorem 4.7.2 fastslår at hvert naturlig tall har en primtallsfaktorisering. I Merknad 4.3.13, Eksempel 4.3.14, og Eksempel 4.3.15, så vi på en metode for å finne en primtallsfaktorisering til et naturlig tall i praksis. Denne metoden kan typisk gjennomføres på flere måter, men vi så at vi alltid får den samme primtallsfaktoriseringen.

Nå skal vi bevise at dette er nødvendigvis sant: hvert naturlig tall har kun én primtallsfaktorisering. Det er kun rekkefølgen av primtallene i faktoriseringen som kan være ulik. Med andre ord, har hvert naturlig tall kun én primtallsfaktorisering slik at primtallene i faktoriseringen går fra lavest på venstre side til høyest på høyre side.

Teorem 4.7.2. La n være et naturlig tall. La s og t være naturlige tall. Anta at det finnes, for hvert naturlig tall i slik at $i \leq s$, og hvert naturlig tall j slik at $j \leq t$, primtall p_i og p'_j slik at

$$n = p_1 \cdots p_s$$

og

$$n = p'_1 \cdots p'_t.$$

Anta dessuten at

$$p_1 \leq p_2 \leq \cdots \leq p_s$$

og at

$$p'_1 \leq p'_2 \leq \cdots \leq p'_t.$$

Da har vi:

(I) $s = t$;

(II) $p_i = p'_i$ for hvert naturlig tall i slik at $i \leq s$.

Bevis. Først sjekker vi om proposisjonen er sann når $s = 1$. Da er $n = p_1$, hvor p_1 er et primtall. La t være et naturlig tall. Anta at det finnes, for hvert naturlig tall j slik at $j \leq t$, primtall p'_j slik at

$$p_1 = p'_1 \cdots p'_t,$$

hvor

$$p'_1 \leq p'_2 \leq p'_t.$$

Vi ønsker å bevise at vi da har: $t = 1$ og $p_1 = p'_1$. Siden

$$p_1 = p'_1 \cdots p'_t,$$

har vi: $p'_1 \mid p_1$. Siden p_1 er et primtall, følger det fra Korollar 4.2.23 at $p'_1 = p_1$. Anta at $t > 1$. Da har vi:

$$p_1 = p_1 \cdot \left(p'_2 \cdots p'_t\right).$$

Det følger fra Proposisjon 2.2.25 at

$$1 = p'_2 \cdots p'_t.$$

Siden p'_j er, for hvert naturlig tall j slik at $j \leq t$, et primtall, er $p'_j \geq 2$. Derfor er

$$p'_2 \cdots p'_t \geq 2.$$

Det kan ikke være sant at både

$$p'_2 \cdots p'_t = 1$$

og

$$p'_2 \cdots p'_t \geq 2.$$

Siden antakelsen at $t > 1$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $t > 2$. Dermed er $t = 1$. Således har vi bevist at proposisjonen er sann når $s = 1$.

Anta nå at proposisjonen har blitt bevist når $s = m$, hvor m er et gitt naturlig tall. Vi ønsker å bevise at det følger at proposisjonen er sann når $s = m + 1$. Anta at det finnes et naturlig tall t slik at, for hvert naturlig tall slik at $i \leq m + 1$, og hvert naturlig tall j slik at $j \leq t$, primtall p_i og p_j slik at

$$n = p_1 \cdots p_s$$

og

$$n = p'_1 \cdots p'_t.$$

Anta dessuten at

$$p_1 \leq p_2 \leq \cdots \leq p_{m+1}$$

og at

$$p'_1 \leq p'_2 \leq \cdots \leq p'_t.$$

Vi gjør følgende observasjoner.

(1) Siden

$$p'_1 \ldots p'_t = (p_1 \cdots p_m) \cdot p_{m+1},$$

har vi:

$$p_{m+1} \mid p'_1 \cdots p'_t.$$

Siden p_{m+1} er et primtall, følger det fra Korollar 4.2.23 at det finnes et naturlig tall j slik at $j \leq t$ og $p_{m+1} = p'_j$. Siden $p'_j \leq p'_t$, deduserer vi at $p_{m+1} \leq p'_t$.

(2) Siden

$$p_1 \ldots p_{m+1} = \left(p'_1 \cdots p'_{t-1}\right) \cdot p'_t,$$

har vi:

$$p'_t \mid p_1 \cdots p_{m+1}.$$

Siden p'_t er et primtall, følger det fra Korollar 4.2.23 at det finnes et naturlig tall i slik at $i \leq m + 1$ og $p'_t = p_i$. Siden $p_i \leq p_{m+1}$, deduserer vi at $p'_t \leq p_{m+1}$.

(3) Fra (1) og (2) har vi: $p_{m+1} \leq p'_t$ og $p'_t \leq p_{m+1}$. Det følger at $p_{m+1} = p'_t$.

(4) Ut ifra (3) og ligningen

$$p_1 \cdots p_{m+1} = p'_1 \cdots p'_t$$

er

$$(p_1 \cdots p_m) \cdot p_{m+1} = \left(p'_1 \cdots p'_{t-1}\right) \cdot p_{m+1}.$$

Det følger fra Proposisjon 2.2.25 at

$$p_1 \cdots p_m = p'_1 \cdots p'_{t-1}.$$

Fra antakelsen at proposisjonen er sann når $n = m$, følger det fra (4) at:

(I) $m = t - 1$;

(II) $p_i = p'_i$ for hvert naturlig tall i slik at $1 \leq i \leq m$.

Ut ifra (I) er $m + 1 = t$. Ut ifra (3) og (II) er $p_i = p'_i$ for hvert naturlig tall i slik at $1 \leq i \leq m + 1$. Således er proposisjonen sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann for alle naturlige tall.

□

Merknad 4.7.3. Teorem 4.7.2 er ikke sant om vi ikke antar at p_i er et primtall for hvert naturlig tall i slik at $i \leq s$, og at p'_j er et primtall for hvert naturlig tall j slik at $j \leq t$. For eksempel har vi: $12 = 3 \cdot 4$ og $12 = 2 \cdot 6$. Det er ikke sant at $3 = 2$ og at $4 = 6$.

Merknad 4.7.4. Antakelsen at

$$p_1 \leq p_2 \leq \cdots \leq p_s$$

og

$$p'_1 \leq p'_2 \leq \cdots \leq p'_t$$

er harmløs: vi kan bytte om rekkefølgen av primtallene i en hvilken som helst primtallsfaktorisering for å oppfylle dette kravet. Dermed kan Teorem 4.7.2 formuleres som i det andre avsnittet av Merknad 4.7.1.

Merknad 4.7.5. Når vi så på divisjonsalgoritmen i §2.2, var det både en proposisjon som sa noe om eksistens (Proposisjon 2.2.6) og en proposisjon sa noe om entydighet (Proposisjon 2.2.15): se Merknad 2.2.17. På lignende vis er Teorem 4.3.3 et teorem om *eksistensen* av en primtallsfaktorisering til et naturlig tall, mens Teorem 4.7.2 er et teorem om *entydigheten* av primtallsfakoriseringene til et naturlig tall.

4.8 Inverser modulo et primtall

Merknad 4.8.1. Fra skolen kjenner du godt til at ligningen

$$3x = 1$$

har en løsning: $x = \frac{1}{3}$. Vi skriver ofte $\frac{1}{3}$ som 3^{-1}. For et hvilket som helst heltall a slik at $a \neq 0$, er $x = \frac{1}{a}$, altså $x = a^{-1}$, en løsning til ligningen

$$ax = 1.$$

Brøkene a^{-1} er svært viktige. De gir oss muligheten til å definere begrepet «dele med a»: gang med a^{-1}.

Bortsett fra når $a = 1$ eller $a = -1$, er a^{-1} aldri et heltall. Det vil si ligningen

$$ax = 1$$

har en heltallsløsning kun når a er lik enten 1 eller -1. Vi kan ikke dele i verdenen av heltall: vi må jobbe i den større verdenen av brøk.

La n være et naturlig tall. Hva om vi istedenfor ser på kongruensen

$$ax \equiv 1 \pmod{n}?$$

Når n er et primtall p, følger det resultater om linære kongruenser som vi har sett på at denne kongruensen har en heltallsløsning for et hvilket som helst a som ikke delelig med p.

Når vi jobber modulo et primtall, finnes det dermed et heltall som spiller rollen av brøket a^{-1}. Dette heltallet gir oss muligheten til å dele i aritmetikk modulo et primtall.

Således finnes det et forhold mellom aritmetikk modulo p og aritmetikk med brøk. Dette forholdet er på mange måter nærere enn forholdet mellom aritmetikk modulo p og aritmetikk med heltall.

At vi kan dele i aritmetikk modulo et primtall er svært viktig. Vi kommer til å benytte oss av dette ofte!

Definisjon 4.8.2. La p være et primtall. La a være et heltall slik at det ikke er sant at $a \equiv 0 \pmod{p}$. En *invers* til a modulo p er et heltall x slik at $ax \equiv 1 \pmod{p}$.

Notasjon 4.8.3. Vi betegner en invers x til a modulo p slik at $0 \leq x < p$ som a^{-1}.

Eksempel 4.8.4. Siden $2 \cdot 3 = 6$ og $6 \equiv 1 \pmod{5}$, er 3 en invers til 2 modulo 5. Med andre ord er $2^{-1} = 3$ i aritmetikk modulo 5.

Eksempel 4.8.5. Siden $3 \cdot 5 = 15$ og $15 \equiv 1 \pmod{7}$, er 5 en invers til 3 modulo 7. Med andre ord er $3^{-1} = 5$ i aritmetikk modulo 7.

Eksempel 4.8.6. Siden $2 \cdot 2 = 4$ og $4 \equiv 1 \pmod{3}$, er 2 en invers til 2 modulo 3. Med andre ord er $2^{-1} = 2$ i aritmetikk modulo 3.

Merknad 4.8.7. Eksempel 4.8.4 og Eksempel 4.8.6 viser at inversen til et heltall modulo et primtall p avhenger av p. Hvis vi med andre ord har to ulike primtall p og q, kan en invers til et heltall a modulo p være ulik en invers til a modulo q.

Proposisjon 4.8.8. La p være et primtall. La a være et heltall slik at det ikke er sant at $a \equiv 0 \pmod{p}$. Ut ifra Proposisjon 3.2.1 finnes det at heltall r slik at:

(1) $a \equiv r \pmod{p}$.

(2) $0 \leq r < p$;

Da er et heltall x en invers til a modulo p hvis og bare hvis x er en invers til r modulo p.

Bevis. Ut ifra (1) og Korollar 3.2.45 er

$$ax \equiv rx \pmod{p}.$$

Ut ifra Proposisjon 3.2.24 og Proposisjon 3.2.33 er da

$$rx \equiv 1 \pmod{p}$$

hvis og bare hvis

$$ax \equiv 1 \pmod{p}.$$

□

Eksempel 4.8.9. Siden $12 \cdot 3 = 36$ og

$$36 \equiv 1 \pmod{5},$$

er 3 en invers til 12 modulo 5. Vi har:

$$12 \equiv 2 \pmod{5}.$$

Proposisjon 4.8.8 fastslår at 3 er da en invers til 2 modulo 5. Fra Eksempel 4.8.4 vet vi at dette er riktignok sant.

Eksempel 4.8.10. Siden $38 \cdot 5 = 190$ og

$$190 \equiv 1 \pmod{7},$$

er 5 en invers til 38 modulo 7. Vi har:

$$38 \equiv 3 \pmod{7}.$$

Proposisjon 4.8.8 fastslår at 5 er da en invers til 3 modulo 7. Fra Eksempel 4.8.5 vet vi at dette er riktignok sant.

Proposisjon 4.8.11. La p være et primtall. La a være et heltall slik at det ikke er sant at $a \equiv 0 \pmod{p}$. La x være en invers til a modulo p. Da finnes det et heltall r slik at:

(1) r er en invers til a modulo p;

(2) $0 \leq r < p$;

(3) $x \equiv r \pmod{p}$.

Bevis. Ut ifra Proposisjon 3.2.1 finnes det et heltall r slik at:

(I) $x \equiv r \pmod{p}$;

(II) $0 \leq r < p$.

Vi gjør følgende observasjoner.

(1) Det følger fra (I) og Korollar 3.2.45 at

$$ax \equiv ar \pmod{p}.$$

Fra Proposisjon 3.2.24 følger det at

$$ar \equiv ax \pmod{p}.$$

(2) Siden x er en invers til a modulo p, er

$$ax \equiv 1 \pmod{p}.$$

Fra (1), (2), og Proposisjon 3.2.33 følger det at

$$ar \equiv 1 \pmod{p},$$

altså at r er en invers til a modulo p.

□

Eksempel 4.8.12. Siden $3 \cdot 7 = 21$ og

$$21 \equiv 1 \pmod{5},$$

er 7 en invers til 3 modulo 5. Siden $3 \cdot 2 = 6$ og

$$6 \equiv 1 \pmod{5},$$

er 2 i tillegg en invers til 3 modulo 5. Proposisjon 4.8.11 fastslår at

$$7 \equiv 2 \pmod{5}.$$

Dette er riktignok sant.

Eksempel 4.8.13. Siden $4 \cdot 25 = 100$ og

$$100 \equiv 1 \pmod{11},$$

er 25 en invers til 4 modulo 11. Siden $4 \cdot 3 = 12$ og

$$12 \equiv 1 \pmod{11},$$

er 3 i tillegg en invers til 4 modulo 11. Proposisjon 4.8.11 fastslår at

$$25 \equiv 3 \pmod{11}.$$

Dette er riktignok sant.

Proposisjon 4.8.14. La p være et primtall. La a være et heltall slik at det ikke er sant at $a \equiv 0 \pmod{p}$. Da finnes det et heltall x som er en invers til a modulo p, og enhver annet heltall som er en invers til a er kongruent til x modulo p.

Bevis. Følger umiddelbart fra Proposisjon 4.2.28, ved å la c være 1. □

Korollar 4.8.15. La p være et primtall. La a være et heltall slik at det ikke er sant at $a \equiv 0 \pmod{p}$. Da finnes det et heltall r slik at:

(1) r er en invers til a modulo p;

(2) $0 \leq r < p$;

(3) enhver annet heltall som er en invers til a er kongruent til r modulo p.

Bevis. Følger umiddelbart fra Proposisjon 4.8.14, Proposisjon 4.8.11, Proposisjon 3.2.33, og Proposisjon 3.2.24. □

Merknad 4.8.16. Korollar 4.8.15 fastslår at, for et hvilket som helst heltall a, finnes det et heltall x som kan betegnes a^{-1} ifølge Notasjon 4.8.3. Dessuten er x det eneste heltallet som kan betegnes slikt.

Eksempel 4.8.17. La p være 2. Siden $1 \cdot 1 = 1$ og

$$1 \equiv 1 \pmod{2},$$

er $1^{-1} = 1$ modulo 2. Ut ifra Proposisjon 4.8.8 er inversen til 1 nok å konstatere en invers modulo 2 til et hvilket som helst heltall som ikke er kongruent til 0 modulo 2.

Eksempel 4.8.18. La p være 3. Siden $1 \cdot 1 = 1$ og

$$1 \equiv 1 \pmod{3},$$

er $1^{-1} = 1$ modulo 3. Siden $2 \cdot 2 = 4$ og

$$4 \equiv 1 \pmod{3},$$

er $2^{-1} = 2$ modulo 3. Ut ifra Proposisjon 4.8.8 er inversene til 1 og 2 nok å konstatere en invers modulo 3 til et hvilket som helst heltall som ikke er kongruent til 0 modulo 3.

Eksempel 4.8.19. La p være 5. Ut ifra Proposisjon 4.8.8 er inversene til de naturlige tallene 1, 2, 3, og 4 nok å konstatere en invers modulo 5 til et hvilket som helst heltall som ikke er kongruent til 0 modulo 5. Disse inversene vises i tabellene.

Naturlig tall	Invers modulo 5
1	1
2	3
3	2
4	4

For eksempel er $4^{-1} = 4$ modulo 5, siden $4 \cdot 4 = 16$ og

$$16 \equiv 1 \pmod{5}.$$

Eksempel 4.8.20. La p være 7. Ut ifra Proposisjon 4.8.8 er inversene til de naturlige tallene 1, 2, ..., 6 nok å konstatere en invers modulo 7 til et hvilket som helst heltall som ikke er kongruent til 0 modulo 7. Disse inversene vises i tabellene.

Naturlig tall	Invers modulo 7
1	1
2	4
3	5
4	2
5	3
6	6

For eksempel er $2^{-1} = 4$ modulo 7, siden $2 \cdot 4 = 8$ og

$$8 \equiv 1 \pmod{7}.$$

Eksempel 4.8.21. La p være 11. Ut ifra Proposisjon 4.8.8 er inversene til de naturlige tallene 1, 2, ..., 10 nok å konstatere en invers modulo 7 til et hvilket som helst heltall som ikke er kongruent til 0 modulo 11. Disse inversene vises i tabellene.

Naturlig tall	Invers modulo 11
1	1
2	6
3	4
4	3
5	9
6	2
7	8
8	7
9	5
10	10

For eksempel er $7^{-1} = 8$ modulo 11, siden $7 \cdot 8 = 56$ og

$$56 \equiv 1 \pmod{11}.$$

Proposisjon 4.8.22. La p være et primtall. Da er $(p-1)^{-1} = p - 1$.

Bevis. Siden $p - 1 \equiv -1 \pmod{p}$, følger det fra Proposisjon 3.2.42 at

$$(p-1) \cdot (p-1) \equiv (-1) \cdot (-1) \pmod{p}.$$

Dermed er

$$(p-1)\cdot(p-1) \equiv 1 \pmod{p}.$$

□

Eksempel 4.8.23. Proposisjon 4.8.22 fastlår at $12^{-1} = 12$ modulo 13. Siden

$$12 \cdot 12 = 144$$

og

$$144 \equiv 1 \pmod{13},$$

er dette riktignok sant.

Eksempel 4.8.24. Proposisjon 4.8.22 fastlår at $16^{-1} = 16$ modulo 17. Siden

$$16 \cdot 16 = 256$$

og

$$256 \equiv 1 \pmod{17},$$

er dette riktignok sant.

Merknad 4.8.25. La p være et primtall. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Ut ifra Proposisjon 3.2.13 er det da ikke sant at $p \mid a$. Fra Korollar 4.2.5 følger det at $\mathsf{sfd}(a, p) = 1$.

Korollar 3.4.39 gir oss derfor en tilnærmingsmetode for å finne a^{-1} modulo p. Ved å benytte algoritmen i Merknad 2.7.15, får vi heltall u og v slik at $1 = au + vp$. Da fastslår Korollar 3.4.39 at $x = u$ er en løsning til kongruensen

$$ax \equiv 1 \pmod{p}.$$

Eksempel 4.8.26. Ved å benytte algoritmen i Merknad 2.7.15, får vi at

$$1 = 9 \cdot 17 + (-8) \cdot 19.$$

Da fastslår Korollar 3.4.39 at $x = 9$ er en løsning til kongruensen

$$17x \equiv 1 \pmod{19},$$

altså at $17^{-1} = 9$ modulo 19.

Eksempel 4.8.27. Ved å benytte algoritmen i Merknad 2.7.15, får vi at

$$1 = (-10) \cdot 26 + 9 \cdot 29.$$

Da fastslår Korollar 3.4.39 at $x = -10$ er en løsning til kongruensen

$$26x \equiv 1 \pmod{29},$$

altså at -10 er en invers til 26 modulo 29. Siden

$$-10 \equiv 19 \mod 29,$$

konkluderer vi at $26^{-1} = 19$ modulo 29.

Proposisjon 4.8.28. La p være et primtall. La x, y, og z være heltall slik at

$$xz \equiv yz \pmod{p}.$$

Anta at det ikke er sant at

$$z \equiv 0 \pmod{p}.$$

Da er

$$x \equiv y \pmod{p}.$$

Bevis. Siden p er et primtall og det ikke er sant at

$$z \equiv 0 \pmod{p},$$

fastslår Korollar 4.8.15 at det finnes et heltall z^{-1} som er en invers til z modulo p. Dermed er

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

Vi gjør følgende observasjoner.

(1) Fra Korollar 3.2.45 og kongruensen

$$zz^{-1} \equiv 1 \pmod{p}$$

følger det at

$$xzz^{-1} \equiv x \pmod{p}.$$

Fra Proposisjon 3.2.24 følger det at

$$x \equiv xzz^{-1} \pmod{p}.$$

(2) Fra Korollar 3.2.45 og kongruensen

$$zz^{-1} \equiv 1 \pmod{p}$$

følger det at

$$yzz^{-1} \equiv y \pmod{p}.$$

(3) Fra Korollar 3.2.45 og kongruensen

$$xz \equiv yz \pmod{p},$$

følger det at

$$xzz^{-1} \equiv yzz^{-1} \pmod{p}.$$

Fra (1) – (3) og Proposisjon 3.2.33, følger det at

$$x \equiv y \pmod{p}.$$

□

Eksempel 4.8.29. Vi har:

$$42 \equiv 72 \pmod{5},$$

altså

$$3 \cdot 14 \equiv 8 \cdot 14 \pmod{5}.$$

Proposisjon 4.8.28 fastslår da at

$$3 \equiv 8 \pmod{5},$$

som er riktignok sant.

Eksempel 4.8.30. Vi har:

$$30 \equiv 96 \pmod{11},$$

altså

$$5 \cdot 6 \equiv 16 \cdot 6 \pmod{11}.$$

Proposisjon 4.8.28 fastslår da at

$$5 \equiv 16 \pmod{11},$$

som er riktignok sant.

Merknad 4.8.31. Siden det ikke er sant at

$$z \equiv 0 \pmod{p},$$

er det ikke sant at $p \mid z$. Ut ifra Korollar 4.2.5 er da $\mathsf{sfd}(z, p) = 1$. Derfor kan Proposisjon 4.8.28 også bevises ved å benytte Proposisjon 3.4.13.

4.9 Binomialteoremet modulo et primtall

Merknad 4.9.1. La n være et naturlig tall. La k være et heltall slik at $0 \leq k \leq n$. Ut ifra Proposisjon 1.9.29, er $\binom{n}{k}$ et naturlig tall. Ut ifra Proposisjon 3.2.1, er $\binom{n}{k}$ kongruent modulo n til et heltall r slik at $0 \leq r < n$. Hva er r? Når n er et primtall, sier følgende proposisjon at r er alltid lik 0. Denne observasjonen er veldig nyttig, som vi kommer til å se.

Proposisjon 4.9.2. La p være et primtall. La k være et heltall slik at $0 < k < p$. Da er

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Bevis. Ut ifra definisjonen til $\binom{p}{k}$, er

$$p! = \binom{p}{k} \cdot \big(k! \cdot (p-k)!\big).$$

Ut ifra definisjonen til $p!$ er dermed

$$\binom{p}{k} \cdot k! \cdot (p-k)! = (p-1)! \cdot p,$$

altså

$$\binom{p}{k} \cdot k! \cdot (p-k)!$$

er delelig med p. Siden p er et primtall, følger det fra Korollar 4.2.19 at ett av følgende er sant.

(A) Vi har:

$$p \mid \binom{p}{k}.$$

(B) Vi har:

$$p \mid k!.$$

(C) Vi har:

$$p \mid (p-k)!.$$

Anta først at (C) er sant. Ut ifra Korollar 4.2.19 og definisjonen til $(p-k)!$, finnes det da et naturlig tall i slik at $p \mid i$ og $i \leq p-k$. Siden $k > 0$, er $p-k < p$. Dermed er $i < p$. Siden $p \mid i$, følger det imidlertid fra Proposisjon 2.5.30 at $p \leq i$. Det kan ikke være sant at både $i < p$ og $p \leq i$. Siden antakelsen at (C) er sant fører til denne motsigelsen, deduserer vi at (C) ikke er sant.

Anta nå at (B) er sant. Ut ifra Korollar 4.2.19 og definisjonen til $k!$, finnes det da et naturlig tall i slik at $p \mid i$ og $i \leq k$. Siden $k < p$, er da $i < p$. Siden $p \mid i$, følger det imidlertid fra Proposisjon 2.5.30 at $p \leq i$. Dermed har vi: $p < p$. Dette kan ikke være sant! Siden antakelsen at (B) er sant fører til denne motsigelsen, deduserer vi at (B) ikke er sant.

Således er (A) sant. Ut ifra Proposisjon 3.2.13, er da

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

□

Eksempel 4.9.3. La p være 5. Proposisjon 4.9.2 fastslår at

$$\binom{5}{k} \equiv 0 \pmod{5}$$

for hvert naturlig tall k slik at $k < 5$. Tabellen viser $\binom{5}{k}$ for hvert naturlig tall k slik at $k < 5$.

k	$\binom{5}{k}$
1	5
2	10
3	10
4	5

Det er riktignok sant at hvert naturlig tall i den andre kolonnen er kongruent til 0 modulo 5.

Eksempel 4.9.4. La p være 7. Proposisjon 4.9.2 fastslår at

$$\binom{7}{k} \equiv 0 \pmod{7}$$

for hvert naturlig tall k slik at $k < 7$. Tabellen viser $\binom{5}{k}$ for hvert naturlig tall k slik at $k < 5$.

k	$\binom{7}{k}$
1	7
2	21
3	35
4	35
5	21
6	7

Det er riktignok sant at hvert naturlig tall i den andre kolonnen er kongruent til 0 modulo 7.

Merknad 4.9.5. Proposisjon 4.9.2 er ikke nødvendigvis sant om vi ikke antar at p er et primtall. For eksempel er $\binom{4}{2} = 2$, og det er ikke sant at $2 \equiv 0 \pmod{4}$.

Proposisjon 4.9.6. La p være et primtall. La x og y være heltall. Da er

$$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 1.9.30 er

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i.$$

(2) Ut ifra Proposisjon 4.9.2 er $\binom{p}{i} \equiv 0 \pmod{p}$ når $1 \leq i \leq p - 1$.

(3) Det følger fra (2) og Korollar 3.2.45 at

$$\binom{p}{i} x^{p-i} y^i \equiv 0 \pmod{p}$$

når $1 \leq i \leq n$.

(4) Det følger fra (3), Proposisjon 3.2.36, og Proposisjon 3.2.16 at

$$\sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i \equiv x^p + y^p \pmod{p}.$$

Fra (1) og (4) konkluderer vi at

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

□

Eksempel 4.9.7. La p være 2. Da fastslår Proposisjon 4.9.6 at

$$(3+8)^2 \equiv 3^2 + 8^2 \pmod{2}.$$

Vi gjør følgende observasjoner.

(1) Vi har:

$$(3+8)^2 = 11^2 = 121$$

og

$$121 \equiv 1 \pmod{2}.$$

(2) Vi har:

$$3^2 + 8^2 = 9 + 64 = 73$$

og

$$73 \equiv 1 \pmod{2}.$$

Dermed er

$$121 \equiv 73 \pmod{2},$$

altså Proposisjon 4.9.6 riktignok stemmer.

Eksempel 4.9.8. La p være 3. Da fastslår Proposisjon 4.9.6 at

$$(6+2)^3 \equiv 6^3 + 2^3 \pmod{3}.$$

Vi gjør følgende observasjoner.

(1) Vi har:

$$(6+2)^3 = 8^3 = 512$$

og

$$512 \equiv 2 \pmod{3}.$$

(2) Vi har:

$$6^3 + 2^3 = 216 + 8 = 224$$

og

$$224 \equiv 2 \pmod 3.$$

Dermed er

$$512 \equiv 224 \pmod 2,$$

altså Proposisjon 4.9.6 riktignok stemmer.

Merknad 4.9.9. Proposisjon 4.9.6 er binomialteoremet i aritmetikk modulo et primtall. Det har blitt mye enklere! Alle de elevene i årenes løp som har gjort feilen at $(x+y)^2 = x^2 + y^2$ hadde hatt det riktig om de hadde sagt at de jobber modulo 2!

Proposisjon 4.9.6 er svært nyttig. Vi kommer ummidelbart til å benytte oss av det for å bevise Proposisjon 4.10.1, som er svært viktig: vi skal benytte oss av denne proposisjonen igjen og igjen.

4.10 Fermats lille teorem

Proposisjon 4.10.1. La p være et primtall. La x være et heltall slik at $x \geq 0$. Da er

$$x^p \equiv x \pmod p.$$

Bevis. Siden $0^p \equiv 0 \pmod p$, er proposisjonen sann når $x = 0$. Anta at proposisjonen har blitt bevist når $x = m$, hvor m er et gitt heltall slik at $m \geq 0$. Ut ifra Proposisjon 4.9.6 er

$$(m+1)^p \equiv m^p + 1^p \pmod p,$$

altså

$$(m+1)^p \equiv m^p + 1 \pmod p.$$

Ut ifra antakelsen at proposisjonen er sann når $x = m$, er

$$m^p \equiv m \pmod p.$$

Da følger det fra Korollar 3.2.39 og Proposisjon 3.2.33 at

$$(m+1)^p \equiv m + 1 \pmod p.$$

Dermed er proposisjonen sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann for et hvilket som helst naturlig tall x. □

Eksempel 4.10.2. Proposisjon 4.10.1 fastslår at

$$9^2 \equiv 9 \pmod 2.$$

Vi gjør følgende observasjoner.

(1) Vi har: $9^2 = 81$, og

$$81 \equiv 1 \pmod{2}.$$

(2) Vi har:

$$9 \equiv 1 \pmod{2}.$$

Dermed er utsagnet riktignok sant.

Eksempel 4.10.3. Proposisjon 4.10.1 fastslår at

$$4^3 \equiv 4 \pmod{3}.$$

Vi gjør følgende observasjoner.

(1) Vi har: $4^3 = 64$ og

$$64 \equiv 1 \pmod{3}.$$

(2) Vi har:

$$4 \equiv 1 \pmod{3}.$$

Dermed er utsagnet riktignok sant.

Eksempel 4.10.4. Proposisjon 4.10.1 fastslår at

$$3^5 \equiv 3 \pmod{5}.$$

Siden $3^5 = 243$ og $243 \equiv 3 \pmod{5}$, er dette riktignok sant.

Korollar 4.10.5. La p være et primtall. La x være et heltall. Da er

$$x^p \equiv x \pmod{p}.$$

Bevis. Ett av følgende er sant:

(A) $x \geq 0$;

(B) $x < 0$.

Anta først at (A) er sant. Da følger korollaret umiddelbart fra Proposisjon 4.10.1.
Anta istedenfor at (B) er sant. Ut ifra Korollar 2.2.11 er ett av følgende sant.

(I) $p = 2$;

(II) p er et oddetall.

Anta først at (I) er sant. Ut ifra Proposisjon 3.2.1 er da enten

$$-x \equiv 0 \pmod 2$$

eller

$$-x \equiv 1 \pmod 2.$$

Anta først at

$$-x \equiv 0 \pmod 2.$$

Ut ifra Proposisjon 3.2.48 er da $(-x)^p \equiv 0 \pmod 2$. Dermed er

$$(-x)^p \equiv -x \pmod 2.$$

Anta istedenfor at

$$-x \equiv 1 \pmod 2.$$

Ut ifra Proposisjon 3.2.48 er da $(-x)^p \equiv 1 \pmod 2$. Dermed er

$$(-x)^p \equiv -x \pmod 2.$$

Således er korollaret sant når (I) stemmer.

Anta nå at (II) er sant. Da er $-x \geq 0$. Ut ifra Proposisjon 4.10.1 er da

$$(-x)^p \equiv -x \pmod p.$$

Siden p er et oddetall, er $(-1)^p = -1$. Dermed er $(-x)^p = -x^p$. Siden

$$(-x)^p \equiv -x \pmod p,$$

følger det at

$$-x^p \equiv -x \pmod p.$$

Ut ifra Korollar 3.2.45 følger det at

$$(-1) \cdot -x^p \equiv (-1) \cdot -x \pmod p,$$

altså at

$$x^p \equiv x \pmod p.$$

Således er korollaret sant når (II) stemmer.

□

Eksempel 4.10.6. Proposisjon 4.10.1 fastslår at

$$(-7)^2 \equiv -7 \pmod 2.$$

Vi gjør følgende observasjoner.

(1) Vi har: $(-7)^2 = 49$, og

$$49 \equiv 1 \pmod 2.$$

(2) Vi har:

$$-7 \equiv 1 \pmod{2}.$$

Dermed er utsagnet riktignok sant.

Eksempel 4.10.7. Proposisjon 4.10.1 fastslår at

$$(-5)^3 \equiv -5 \pmod{3}.$$

Vi gjør følgende observasjoner.

(1) Vi har: $(-5)^3 = -125$ og

$$-125 \equiv 1 \pmod{3}.$$

(2) Vi har:

$$-5 \equiv 1 \pmod{3}.$$

Dermed er utsagnet riktignok sant.

Korollar 4.10.8. La p være et primtall. La x være et heltall slik at det ikke er sant at

$$x \equiv 0 \pmod{p}.$$

Da er

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

Bevis. Ut ifra Korollar 4.10.5 er

$$x^p \equiv x \pmod{p}.$$

Siden det ikke er sant at

$$x \equiv 0 \pmod{p},$$

følger det fra Proposisjon 4.8.28 at

$$x^p \cdot x^{-1} \equiv x \cdot x^{-1} \pmod{p},$$

altså at

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

□

Terminologi 4.10.9. Både Korollar 4.10.5 og Korollar 4.10.8 kalles *Fermats lille teorem.*

Merknad 4.10.10. Flere andre bevis for Korollar 4.10.8 kan gis. Disse bevisene er typisk av kombinatorisk art: vi finner to forskjellige måter å navngi heltallene r slik at $0 \leq r \leq p-1$. Slike «telleargumentene» er ikke enkle å uttrykke rigorøst kun ved hjelp av de begrepene vi utforsker i dette kurset.

Hvis vi først hadde gitt et bevis for Korollar 4.10.8, kunne vi ha dedusert at Korollar 4.10.5 er sant ved å gange begge sidene av kongruensen

$$x^{p-1} \equiv 1 \pmod{p}$$

med x.

Eksempel 4.10.11. Korollar 4.10.8 fastslår at

$$4^4 \equiv 1 \pmod{5}.$$

Siden $4^4 = 256$ og

$$256 \equiv 1 \pmod{5},$$

er dette riktignok sant.

Eksempel 4.10.12. Korollar 4.10.8 fastslår at

$$2^6 \equiv 1 \pmod{7}.$$

Siden $2^6 = 64$ og

$$64 \equiv 1 \pmod{7},$$

er dette riktignok sant.

Merknad 4.10.13. En formodning som ikke ble besvart i flere hundreår var at den motsatte til Korollar 4.10.8 stemmer: dersom det finnes et heltall x slik at

$$x^{n-1} \equiv 1 \pmod{n},$$

er n et primtall. Denne formodningen er faktisk gal! La oss se på at moteksempel.

La x være 2, og la n være 341. Vi har: $2^{10} = 1024$. Siden $1023 = 3 \cdot 341$, er

$$341 \mid 1023.$$

Derfor er

$$1024 \equiv 1 \pmod{341},$$

altså

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

Ut ifra Proposisjon 3.2.48, er da

$$\left(2^{10}\right)^{34} \equiv 1^{34} \pmod{341},$$

altså

$$2^{340} \equiv 1 \pmod{341}.$$

Imidlertid er $341 = 11 \cdot 31$, det vil si er 341 ikke et primtall.

4.11 Eksempler på bevis hvor Fermats lille teorem benyttes

Proposisjon 4.11.1. Det naturlige tallet $7^{104} + 1$ er delelig med 17.

Bevis. Vi har:

$$104 = 6 \cdot 16 + 8.$$

Dermed er

$$7^{104} = 7^{6 \cdot 16 + 8} = 7^{6 \cdot 16} \cdot 7^8 = \left(7^{16}\right)^6 \cdot 7^8.$$

Siden 17 er et primtall, følger det fra Korollar 4.10.8 at

$$7^{16} \equiv 1 \pmod{17}.$$

Ut ifra Proposisjon 3.2.48 er da

$$\left(7^{16}\right)^6 \equiv 1^6 \pmod{17},$$

altså

$$\left(7^{16}\right)^6 \equiv 1 \pmod{17}.$$

Siden $49 + 2 = 51$, og $17 \mid 51$, har vi i tillegg:

$$7^2 \equiv -2 \pmod{17}.$$

Ut ifra Proposisjon 3.2.48 er da

$$\left(7^2\right)^4 \equiv (-2)^4 \pmod{17},$$

altså

$$7^8 \equiv 16 \pmod{17}.$$

Siden

$$16 \equiv -1 \pmod{17},$$

er dermed

$$7^8 \equiv -1 \pmod{17}.$$

Det følger fra Proposisjon 3.2.42 at

$$\left(7^{16}\right)^6 \cdot 7^8 \equiv 1 \cdot (-1) \pmod{17},$$

altså at

$$7^{104} \equiv -1 \pmod{17}.$$

Således er $7^{104} + 1$ delelig med 17.

□

Merknad 4.11.2. Følgende proposisjon behøves i løpet av vårt neste eksempel på et bevis hvor Fermats lille teorem benyttes. Proposisjonen er viktig i seg selv.

Proposisjon 4.11.3. La x og r være heltall. La m og n være heltall. Anta at $m \neq 0$, $n \neq 0$, og $\mathsf{sfd}(m, n) = 1$. Anta at

$$x \equiv r \pmod{m}$$

og at

$$x \equiv r \pmod{n}.$$

Da er

$$x \equiv r \pmod{mn}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Siden

$$x \equiv r \pmod{m},$$

har vi:

$$m \mid x - r.$$

(2) Siden

$$x \equiv r \pmod{n},$$

har vi:

$$n \mid x - r.$$

Siden $\mathsf{sfd}(m, n) = 1$, følger det fra Proposisjon 2.8.17 at $mn \mid x - r$. Dermed er

$$n \equiv r \pmod{pq}.$$

□

Eksempel 4.11.4. Vi har:

$$49 \equiv 1 \pmod{3}$$

og

$$49 \equiv 1 \pmod{4}.$$

Siden $\mathsf{sfd}(3, 4) = 1$, fastlsår Proposisjon 4.11.3 at

$$49 \equiv 1 \pmod{3 \cdot 4},$$

altså

$$49 \equiv 1 \pmod{12}.$$

Dette er riktignok sant.

Eksempel 4.11.5. Vi har:

$$89 \equiv 5 \pmod{7}$$

og

$$89 \equiv 5 \pmod{6}.$$

Siden $\mathsf{sfd}(7, 6) = 1$, fastlsår Proposisjon 4.11.3 at

$$89 \equiv 5 \pmod{7 \cdot 6},$$

altså

$$89 \equiv 5 \pmod{42}.$$

Dette er riktignok sant.

Korollar 4.11.6. La x og r være heltall. La p og q være et primtall slik at $p \neq q$. Anta at

$$x \equiv r \pmod{p}$$

og at

$$x \equiv r \pmod{q}.$$

Da er

$$x \equiv r \pmod{pq}.$$

Bevis. Siden q er et primtall, er 1 og q de eneste divisorene til q. Siden $p \neq q$, følger det at q ikke er delelig med p. Det følger fra Korollar 4.2.5 at $\mathsf{sfd}(p, q) = 1$. Da følger korollaret umiddelbart fra Proposisjon 4.11.3. □

Eksempel 4.11.7. Vi har:

$$32 \equiv 2 \pmod{3}$$

og

$$32 \equiv 2 \pmod{5}.$$

Korollar 4.11.6 fastslår at

$$32 \equiv 2 \pmod{3 \cdot 5},$$

altså

$$32 \equiv 2 \pmod{15}.$$

Dette er riktignok sant.

Eksempel 4.11.8. Vi har:

$$237 \equiv 6 \pmod{11}$$

og

$$237 \equiv 6 \pmod{7}.$$

Korollar 4.11.6 fastslår at

$$237 \equiv 6 \pmod{7 \cdot 11},$$

altså

$$237 \equiv 6 \pmod{77}.$$

Dette er riktignok sant.

Merknad 4.11.9. Utsagnet i Proposisjon 4.11.3 er ikke nødvendigvis sant om vi ikke antar at p er et primtall. La for eksempel p være 4, og la q være 6. Vi har:

$$14 \equiv 2 \pmod{4}$$

og

$$14 \equiv 2 \pmod{6}.$$

Imidlertid er det ikke sant at

$$14 \equiv 2 \pmod{24}.$$

Utsagnet i Proposisjon 4.11.3 er heller ikke nødvendigvis sant om $p \mid q$. La for eksempel p være 3, og la q være 6. Vi har:

$$8 \equiv 2 \pmod{3}$$

og

$$8 \equiv 2 \pmod{6}.$$

Imidlertid er det ikke sant at

$$8 \equiv 3 \pmod{18}.$$

Proposisjon 4.11.10. La x være et heltall. Anta at $\mathsf{sfd}(x, 30) = 1$. Da er $x^4 + 59$ delelig med 60.

Bevis. Siden $\mathsf{sfd}(x, 30) = 1$, er x ikke delelig med 2, 3, eller 5. Da fastslår Korollar 4.10.8 at alle de tre følgende utsagnene er sanne:

(A) $x \equiv 1 \pmod{2}$;

(B) $x^2 \equiv 1 \pmod{3}$;

(C) $x^4 \equiv 1 \pmod{5}$.

Det følger fra (A) og Korollar 3.2.63 at enten

$$x \equiv 1 \pmod{4}$$

eller

$$x \equiv 3 \pmod{4}.$$

Hvis

$$x \equiv 1 \pmod{4},$$

følger det fra Proposisjon 3.2.48 at

$$x^4 \equiv 1^4 \pmod{4},$$

altså at

$$x^4 \equiv 1 \pmod{4}.$$

Hvis

$$x \equiv 3 \pmod 4,$$

følger det fra Proposisjon 3.2.48 at

$$x^2 \equiv 3^2 \pmod 4,$$

altså at

$$x^2 \equiv 9 \pmod 4.$$

Siden

$$9 \equiv 1 \pmod 4,$$

følger det fra Proposisjon 3.2.33 at

$$x^2 \equiv 1 \pmod 4.$$

Da følger det fra Proposisjon 3.2.48 at

$$\left(x^2\right)^2 \equiv 1^2 \pmod 4,$$

altså at

$$x^4 \equiv 1 \pmod 4.$$

Således er

$$x^4 \equiv 1 \pmod 4$$

både om

$$x \equiv 1 \pmod 4$$

og om

$$x \equiv 3 \pmod 4,$$

altså i begge de mulige tilfellene.

I tillegg følger det fra (B) og Proposisjon 3.2.48 at

$$\left(x^2\right)^2 \equiv 1^2 \pmod 3,$$

altså at

$$x^4 \equiv 1 \pmod 3.$$

Dermed er følgende sanne.

(1) $x^4 \equiv 1 \pmod 4$;

(2) $x^4 \equiv 1 \pmod 3$;

(3) $x^4 \equiv 1 \pmod 5$.

Ved å la p være 3 og q være 4, følger det fra (1), (2), og Proposisjon 4.11.3 at

$$x^4 \equiv 1 \pmod{3 \cdot 4},$$

altså at

$$x^4 \equiv 1 \pmod{12}.$$

Ved å la p være 5 og q være 12, følger det fra denne kongruensen, (3), og Proposisjon 4.11.3 at

$$x^4 \equiv 1 \pmod{5 \cdot 12},$$

altså at

$$x^4 \equiv 1 \pmod{60}.$$

Da følger det fra Korollar 3.2.39 at

$$x^4 + 59 \equiv 1 + 59 \pmod{60},$$

altså at

$$x^4 \equiv 60 \pmod{60}.$$

Siden

$$60 \equiv 0 \pmod{60},$$

følger det fra Proposisjon 3.2.33 at

$$x^4 + 59 \equiv 0 \pmod{60}.$$

Fra Proposisjon 3.2.13 konkluderer vi at

$$x^4 + 59$$

er delelig med 60.

□

Eksempel 4.11.11. Proposisjon 4.11.10 fastslår at

$$7^4 + 59$$

er delelig med 60. Siden $7^4 + 59 = 2460$ og $2460 = 41 \cdot 60$ er dette riktignok sant.

Eksempel 4.11.12. Proposisjon 4.11.10 fastslår at

$$11^4 + 59$$

er delelig med 60. Siden $11^4 + 59 = 14700$ og $14700 = 245 \cdot 60$ er dette riktignok sant.

Proposisjon 4.11.13. La p være et primtall. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da er

$$x = a^{p-2}c$$

en løsning til kongruensen

$$ax \equiv c \pmod{p}.$$

Enhver annen løsning til denne kongruensen er kongruent til x modulo p.

Bevis. Siden det ikke er sant at

$$a \equiv 0 \pmod{p},$$

følger det fra Korollar 4.10.8 at

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

Ut ifra Korollar 3.2.45 er da

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

Siden

$$a \cdot \left(a^{p-2}c\right) = a^{p-1}c,$$

deduserer vi at

$$a \cdot \left(a^{p-2}c\right) \equiv c \pmod{p}.$$

Med andre ord er $x = a^{p-2}c$ en løsning til kongruensen

$$ax \equiv c \pmod{p}.$$

Siden det ikke er sant at

$$a \equiv 0 \pmod{p},$$

er det ikke sant at $p \mid a$. Siden p er et primtall, følger det fra Korollar 4.2.5 at $\mathsf{sfd}(a, p) = 1$. Ut ifra Korollar 3.4.39, Proposisjon 3.2.33, og Proposisjon 3.2.24, er da en hvilken som helst løsning x til kongruensen

$$ax \equiv 0 \pmod{p}$$

kongruent modulo p til $a^{p-2}c$. □

Eksempel 4.11.14. Proposisjon 4.11.13 fastslår at $x = 3^3 \cdot 2$, altså $x = 54$, er en løsning til kongruensen

$$3x \equiv 2 \pmod{5}.$$

Siden

$$162 \equiv 2 \pmod{5},$$

er dette riktignok sant.

Eksempel 4.11.15. Proposisjon 4.11.13 fastslår at $x = 2^5 \cdot 5$, altså $x = 160$, er en løsning til kongruensen

$$2x \equiv 5 \pmod{7}.$$

Siden

$$320 \equiv 5 \pmod{7},$$

er dette riktignok sant.

4.12 Orden modulo et primtall

Definisjon 4.12.1. La p være et primtall. La x være et heltall slik at det ikke er sant at

$$x \equiv 0 \pmod{p}.$$

Et naturlig tall t er *ordenen* til a modulo p dersom t er det minste naturlige tallet slik at:

(1) $x^t \equiv 1 \pmod{p}$;

(2) $0 \leq t < p$.

Merknad 4.12.2. La x være et heltall slik at det ikke er sant at

$$x \equiv 0 \pmod{p}.$$

Ut ifra Korollar 4.10.8 er

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

Derfor har x en orden, og denne ordenen er mindre enn eller likt $p - 1$.

Merknad 4.12.3. For å finne ordenen til et heltall x modulo et primtall p, kan vi gå gjennom heltallene x, x^2, x^3, ..., x^{p-1}. Den første potensen i slik at

$$x^i \equiv 1 \pmod{p}$$

er ordenen til x modulo p.

Notasjon 4.12.4. La p være et primtall. La x være et heltall slik at det ikke er sant at $x \equiv 0 \pmod{p}$. Vi betegner ordenen til x modulo p som $\mathsf{ord}_p(x)$.

Eksempel 4.12.5. Siden $1^1 = 1$, er ordenen til 1 lik 1 for et hvilket som helst primtall p.

Eksempel 4.12.6. For å finne ordenen til 2 modulo 3, gjør vi følgende. Kongruensen i den andre raden er modulo 3.

i	2^i
1	2
2	$4 \equiv 1$

Dermed er ordenen til 2 modulo 3 lik 2.

Således har vi følgende ordener modulo 3.

x	Ordenen til x modulo 3
1	1
2	2

Eksempel 4.12.7. Alle kongruenser i dette eksempelet er modulo 5. For å finne ordenen til 2 modulo 5, gjør vi følgende.

i	2^i
1	2
2	4
3	$8 \equiv 3$
4	$2^4 = 2^2 \cdot 2^2 \equiv 4 \cdot 4 = 16 \equiv 1$

Dermed er ordenen til 2 modulo 5 lik 4.

For å finne ordenen til 3 modulo 5, gjør vi følgende.

i	3^i
1	3
2	$9 \equiv 4$
3	$3^3 = 3^2 \cdot 3^1 \equiv 4 \cdot 3 = 12 \equiv 2$
4	$3^4 = 3^3 \cdot 3^1 \equiv 2 \cdot 3 = 6 \equiv 1$

Dermed er ordenen til 3 modulo 5 lik 4.

For å finne ordenen til 4 modulo 5, gjør vi følgende.

i	4^i
1	4
2	$16 \equiv 1$

Dermed er ordenen til 4 modulo 5 lik 2.

Således har vi følgende ordener modulo 5.

x	Ordenen til x modulo 5
1	1
2	4
3	4
4	2

Merknad 4.12.8. Utregningene i Eksempel 4.12.7 er ikke de eneste mulige. For å vise at

$$2^4 \equiv 1 \pmod 5,$$

kan vi også for eksempel regne som følger:

$$2^4 = 2^3 \cdot 2^1 \equiv 3 \cdot 2 = 6 \equiv 1 \pmod 5.$$

Alternativt følger det fra Korollar 4.10.8.

Det samme gjelder i neste eksempel.

Eksempel 4.12.9. Alle kongruenser i dette eksempelet er modulo 7. For å finne ordenen til 2 modulo 7, gjør vi følgende.

i	2^i
1	2
2	4
3	$8 \equiv 1$

Dermed er ordenen til 2 modulo 7 lik 3.

For å finne ordenen til 3 modulo 7, gjør vi følgende.

i	3^i
1	3
2	$9 \equiv 2$
3	$3^3 = 3^2 \cdot 3^1 \equiv 2 \cdot 3 = 6$
4	$3^4 = 3^2 \cdot 3^2 \equiv 2 \cdot 2 = 4$
5	$3^5 = 3^3 \cdot 3^2 \equiv 6 \cdot 2 = 12 \equiv 5$
6	$3^6 = 3^4 \cdot 3^2 \equiv 4 \cdot 2 = 8 \equiv 1$

Dermed er ordenen til 4 modulo 7 lik 6.

For å finne ordenen til 4 modulo 7, gjør vi følgende.

i	4^i
1	4
2	$16 \equiv 2$
3	$4^3 = 4^2 \cdot 4^1 \equiv 2 \cdot 4 = 8 \equiv 1$

Dermed er ordenen til 4 modulo 7 lik 3.

For å finne ordenen til 5 modulo 7, gjør vi følgende.

i	5^i
1	5
2	$25 \equiv 4$
3	$5^3 = 5^2 \cdot 5^1 \equiv 4 \cdot 5 = 20 \equiv -1$
4	$5^4 = 5^3 \cdot 5^1 \equiv (-1) \cdot 5 = -5 \equiv 2$
5	$5^5 = 5^3 \cdot 5^2 \equiv (-1) \cdot 4 = -4 \equiv 3$
6	$5^6 = 5^3 \cdot 5^3 \equiv (-1) \cdot (-1) = 1$

Dermed er ordenen til 5 modulo 7 lik 6.

For å finne ordenen til 6 modulo 7, gjør vi følgende.

i	6^i
1	6
2	$36 \equiv 1$

Dermed er ordenen til 6 modulo 7 lik 2.

Således har vi følgende ordener modulo 7.

x	Ordenen til x modulo 7
1	1
2	3
3	6
4	3
5	6
6	2

Proposisjon 4.12.10. La p være et primtall. La x være et heltall slik at x det ikke er sant at

$$x \equiv 0 \pmod{p}.$$

La s være ordenen til x. La t være et naturlig tall. Da er

$$x^t \equiv 1 \pmod{p}$$

hvis og bare hvis $s \mid t$.

Bevis. Anta først at $x^t \equiv 1 \pmod{p}$. Ut ifra Proposisjon 2.2.6 finnes det naturlige tall k og r slik at $t = ks + r$. Da er:

$$\begin{aligned} x^t &= x^{ks+r} \\ &= x^{ks} x^r \\ &= (x^s)^k \, x^r. \end{aligned}$$

Ut ifra definisjonen til s er

$$x^s \equiv 1 \pmod{p}.$$

Dermed er

$$x^t \equiv 1^k \cdot x^r,$$

alts

$$x^t \equiv x^r \pmod{p}.$$

Ut ifra antakelsen at

$$x^t \equiv 1 \pmod{p}$$

og Proposisjon 3.2.24, er da

$$x^r \equiv 1 \pmod{p}.$$

Ut ifra definisjonen til s, er s det minste naturlige tallet slik at $x^s \equiv 1 \pmod{p}$. Siden $0 \leq r < s$ og

$$x^r \equiv 1 \pmod{p},$$

følger det at $r = 0$. Dermed er $t = ks$. Vi konkluderer at $s \mid t$.

Anta istedenfor at $s \mid t$. Da finnes det et naturlig tall k slik at $t = ks$. Ut ifra definisjonen til s, er $x^s \equiv 1 \pmod{p}$. Derfor er

$$(x^s)^k \equiv 1^k \pmod{p},$$

altså er

$$x^{sk} \equiv 1 \pmod{p}.$$

Siden

$$sk = ks = t,$$

konkluderer vi at

$$x^t \equiv 1 \pmod{p}.$$

□

Eksempel 4.12.11. Siden $2^6 = 64$ og

$$64 \equiv 1 \pmod{7},$$

fastslår Proposisjon 4.12.10 at ordenen til 2 modulo 7 deler 6. Ut ifra Eksempel 4.12.9 er ordenen til 2 modulo 7 lik 3. Det er riktignok sant at $3 \mid 6$.

Eksempel 4.12.12. Siden $3^8 = 6561$ og

$$6561 \equiv 1 \pmod{5},$$

fastslår Proposisjon 4.12.10 at ordenen til 3 modulo 4 deler 8. Ut ifra Eksempel 4.12.7 er ordenen til 3 modulo 5 lik 4. Det er riktignok sant at $4 \mid 8$.

4.13 Primitive røtter modulo et primtall

Definisjon 4.13.1. La p være et primtall. La x være et heltall slik at det ikke er sant at

$$x \equiv 0 \pmod{p}.$$

Da er x en *primitiv rot* modulo p dersom ordenen til x modulo p er $p - 1$.

Eksempel 4.13.2. Siden ordenen til 1 er $2 - 1 = 1$, er 1 en primitiv rot modulo 2.

Eksempel 4.13.3. Ut ifra tabellen på slutten av Eksempel 4.12.6 har vi følgende.

x	Primitiv rot modulo 3?
1	✗
2	✓

Eksempel 4.13.4. Ut ifra tabellen på slutten av Eksempel 4.12.7 har vi følgende.

x	Primitiv rot modulo 5?
1	✗
2	✓
3	✓
4	✗

Eksempel 4.13.5. Ut ifra tabellen på slutten av Eksempel 4.12.9 har vi følgende.

x	Primitiv rot modulo 7?
1	✗
2	✗
3	✓
4	✗
5	✓
6	✗

Proposisjon 4.13.6. La p være et primtall. La x være en primitiv rot modulo p. La a være et heltall. Da finnes det et heltall r slik at $0 \leq r < p$ og

$$x^r \equiv a \pmod{p}.$$

Bevis. Kommer snart! □

Merknad 4.13.7. Proposisjon 4.13.6 er grunnen for at primitive røtter er viktige. Å kunne uttrykke et hvilket som helst heltall modulo p som en potens av ett heltall er noe er spesielt med aritmetikk modulo p, og svært viktig fra et teoretisk synspunkt. Det er langt fra tilfellet at det finnes et heltall x slik at hvert naturlig tall er *likt* x opphøyd i noe. Når $x = 2$, får vi for eksempel heltallene 2, 4, 8, 16, ..., men får vi ikke de negative heltallene, og heller ikke de naturlige tallene 1, 3, 5, 6, 7, 9, ...

4.14 Lagranges teorem

Merknad 4.14.1. Fra skolen kjenner du til at en ligning

$$ax^2 + bx + c = 0$$

har maksimum to løsninger. Se Merknad 5.1.1 for mer om dette. Kanskje kjenner du dessuten til noe som er mer generell: en ligning

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$$

har maksimum n løsninger. I denne delen av kapittelet skal vi bevise at det samme er tilfellet i modulær aritmetikk: en kongruens

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$$

har maksimum n løsninger slik at ikke noe par av disse er kongruent til hverandre modulo p.

Proposisjon 4.14.2. La m være et heltall. La n være et naturlig tall. For hvert heltall i slik at $0 \leq i \leq n$, la a_i være et heltall. La x være et heltall slik at

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{m}.$$

Ut ifra Proposisjon 3.2.1 finnes det et heltall r slik at:

(1) $0 \leq r < m - 1$;

(2) $x \equiv r \pmod{m}$.

Vi har:

$$a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \equiv 0 \pmod{m}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 3.2.48 er

$$x^i \equiv r^i \pmod{m}$$

for hvert naturlig tall i slik at $i \leq n$.

(2) Det følger fra (1) og Korollar 3.2.45 at

$$a_i x^i \equiv a_i r^i \pmod{m}$$

for hvert naturlig tall i slik at $i \leq n$.

(3) Det følger fra (2) og Korollar 3.2.36 at

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x \\ &\equiv a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r \pmod{m} \end{aligned}$$

(4) Det følger fra (3) og Korollar 3.2.39 at

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \\ &\equiv a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \pmod{m}. \end{aligned}$$

Ut ifra Proposisjon 3.2.24 er da

$$\begin{aligned} &a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \\ &\equiv a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{m} \end{aligned}$$

Det følger fra (4), antakelsen at

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{m}$$

og Proposisjon 3.2.33 at

$$a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \equiv 0 \pmod{m}.$$

□

Eksempel 4.14.3. Det kan regnes ut at

$$16^2 + 3 \cdot 16 + 4 = 308$$

og at $308 = 44 \cdot 7$, altså at

$$308 \equiv 0 \pmod{7}.$$

Dermed er $x = 16$ en løsning til kongruensen

$$x^2 + 3x + 4 \equiv 0 \pmod{7}.$$

Siden

$$16 \equiv 2 \pmod{7},$$

fastslår Proposisjon 4.14.2 at $x = 2$ er også en løsning til kongruensen. Dette er riktignok sant.

Eksempel 4.14.4. Det kan regnes ut at

$$9^3 + 3 \cdot 9^2 - 16 \cdot 9 + 2 = 830$$

og at $830 = 166 \cdot 5$, altså at

$$830 \equiv 0 \pmod{5}.$$

Dermed er $x = 9$ en løsning til kongruensen

$$x^3 + 3x^2 + -16x + 2 \equiv 0 \pmod{5}.$$

Siden

$$9 \equiv 4 \pmod{5},$$

fastslår Proposisjon 4.14.2 at $x = 4$ er også en løsning til kongruensen. Dette er riktignok sant.

Lemma 4.14.5. La p være et primtall. La n være et naturlig tall. For hvert heltall i slik at $0 \leq i \leq n$, la a_i være et heltall. La y være et heltall. Da finnes det et heltall r og, for hvert heltall i slik at $0 \leq i \leq n-1$, et heltall b_i, slik at

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \\ &= (x-y)\left(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r \end{aligned}$$

for hvert heltall x.

Bevis. Først sjekker vi om lemmaet er sant når $n = 1$. La b_0 være a_1, og la r være $a_1 y + a_0$. Da er:

$$\begin{aligned} (x-y)b_0 + r &= a_1(x-y) + (a_1 y + a_0) \\ &= a_1 x - a_1 y + a_1 y + a_0 \\ &= a_1 x + a_0. \end{aligned}$$

Dermed er lemmaet sant når $n = 1$.

Anta nå at proposisjonen har blitt bevist når $n = m$, hvor m er et gitt naturlig tall. Vi gjør følgende observasjoner.

(1) Vi har:

$$\begin{aligned} &a_{m+1}x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \\ &= x\left(a_{m+1}x^m + a_m x^{m-1} + \cdots + a_2 x + a_1\right) + a_0. \end{aligned}$$

(2) Ut ifra antakelsen at lemmaet er sant når $n = m$, finnes det et heltall r' og, for hvert heltall i slik at $0 \leq i \leq m-1$, et heltall b'_i, slik at

$$\begin{aligned} &a_{m+1}x^m + a_m x^{m-1} + \cdots + a_2 x + a_1 \\ &= (x-y)\left(b'_{m-1}x^{m-1} + b'_{m-2}x^{m-2} + \cdots + b'_1 x + b'_0\right) + r'. \end{aligned}$$

(3) La b_0 være r'. For hvert heltall i slik at $1 \leq i \leq m$, la b_i være b'_{i-1}. La r være $yr' + a_0$. Da er

$$\begin{aligned} &(x-y)\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r \\ &= (x-y)\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x\right) + (x-y)b_0 + r \\ &= x(x-y)\left(b_m x^{m-1} + b_{m-1}x^{m-2} + \cdots + b_2 x + b_1\right) + xb_0 - yb_0 + r \\ &= x\Big((x-y)\left(b_m x^{m-1} + b_{m-1}x^{m-2} + \cdots + b_2 x + b_1\right) + b_0\Big) - yb_0 + r \\ &= x\Big((x-y)\left(b'_{m-1}x^{m-1} + b'_{m-2}x^{m-2} + \cdots + b'_1 x + b'_0\right) + r'\Big) - yr' + \left(yr' + a_0\right) \\ &= x\Big((x-y)\left(b'_{m-1}x^{m-1} + b'_{m-2}x^{m-2} + \cdots + b'_1 x + b'_0\right) + r'\Big) + a_0. \end{aligned}$$

(4) Det følger fra (2) at

$$\begin{aligned} &x\Big((x-y)\left(b'_{m-1}x^{m-1}+b'_{m-2}x^{m-2}+\cdots+b'_1x+b'_0\right)+r'\Big)+a_0\\ &=x\left(a_{m+1}x^m+a_mx^{m-1}+\cdots+a_2x+a_1\right)+a_0. \end{aligned}$$

Det følger fra (1), (3), og (4) at

$$\begin{aligned} &a_{m+1}x^{m+1}+a_mx^m+\cdots+a_2x^2+a_1x+a_0\\ &=(x-y)\left(b_mx^m+b_{m-1}x^{m-1}+\cdots+b_2x^2+b_1x+b_0\right)+r. \end{aligned}$$

Dermed er lemmaet sant når $n=m+1$.

Ved induksjon konkluderer vi at lemmaet er sant når n er et hvilket som helst naturlig tall.

□

Eksempel 4.14.6. La y være 3. Da fastslår Lemma 4.14.5 at det finnes et heltall r og et heltall b_0 slik at

$$11x+8=(x-3)\cdot b_0+r,$$

for hvert heltall x. Dette er riktigknok sant, ved å la b_0 være 11, og r være 41: det stemmer at

$$11x+8=(x-3)\cdot 11+41.$$

Eksempel 4.14.7. La y være -7. Lemma 4.14.5 fastslår at det finnes et heltall r og heltall b_0 og b_1 slik at

$$5x^2+2x-3=\big(x-(-7)\big)\left(b_1x+b_0\right)+r,$$

altså at

$$5x^2+2x-3=(x+7)\left(b_1x+b_0\right)+r,$$

for hvert heltall x. Dette er riktigknok sant, ved å la b_0 være -33, b_1 være 5, og r være 228: det stemmer at

$$5x^2+2x-3=(x+7)\left(5x-33x\right)+228.$$

Eksempel 4.14.8. La y være 6. Lemma 4.14.5 fastslår at det finnes et heltall r og heltall b_0, b_1, og b_2 slik at

$$2x^3-8x^2+5x-7=(x-6)\left(b_2x^2+b_1x+b_0\right)+r$$

for hvert heltall x. Dette er riktigknok sant, ved å la b_0 være 2, b_1 være 4, b_2 være 29, og r være 167: det stemmer at

$$2x^3-8x^2+5x-7=(x-6)\left(2x^2+4x+29\right)+167.$$

Merknad 4.14.9. Utsagnet i Lemma 4.14.5 er: det finnes et heltall r og, for hvert heltall i slik at $0 \leq i \leq n$, et heltall b_i, slik at

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \\ &= (x - y)\left(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r \end{aligned}$$

for *hvert* heltall x. Dette er ikke det samme som å si: gitt et heltall x, finnes det et heltall r og, for hvert heltall i slik at $0 \leq i \leq n$, et heltall b_i, slik at denne ligningen stemmer.

Den andre påstanden holder muligheten åpen for at heltallet r og heltallene b_i varierer avhengig av x. Heltallet r og heltallene b_i i Lemma 4.14.5 varierer ikke avhengig av x.

Gitt et heltall x, er for eksempel

$$2x^2 + x - 1 = (x - 1)(2x + 1) + 2x.$$

Ved å la b_0 være 1, b_1 være 2, og r være $2x$, får vi med andre ord at

$$2x^2 + x - 1 = (x - 1)\left(b_1 x + b_0\right) + r.$$

Imidlertid varierer da r avhengig av x. Hvis for eksempel $x = 1$, er $r = 2$, og vi har:

$$2x^2 + x - 1 = (x - 1)(2x + 1) + 2.$$

Hvis $x = 2$, er $r = 4$, og vi har:

$$2x^2 + x - 1 = (x - 1)(2x + 1) + 4.$$

Istedenfor kan vi la b_0 være 1, b_1 være 2, og r være 3: da har vi

$$2x^2 + x - 1 = (x - 1)(2x + 3) + 2.$$

I dette tilfellet varierer r ikke avhengig av x: uansett hvilket heltall x vi velger, er $r = 3$.

Merknad 4.14.10. Lemma 4.14.5 kan generaliseres. Et uttrkk

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

hvor a_i er et heltall for hvert heltall i slik at $0 \leq i \leq n$, og x er en variabel, kalles et *polynom*. Det finnes en divisjonsalgoritme for polynom som bygger på divisjonsalgoritmen for heltall: vi kan dele et polynom med et annet polynom, og får en kvotient som er et polynom og en rest som er et heltall. Lemma 4.14.5 følger umiddelbart fra dette.

Imidlertid kommer vi ikke til å trenge et annet sted divisjonsalgoritmen for polynom. Dessuten må begrepet ≪ ≪polynom≫ defineres formelt, og dette er heller ikke noe vi kommer et annet sted til å trenge. Derfor skal vi nøye oss med det direkte beviset vi ga for Lemma 4.14.5.

Proposisjon 4.14.11. La p være et primtall. La n være et naturlig tall. For hvert heltall i slik at $0 \leq i \leq n$, la a_i være et heltall. Anta at det ikke er sant at

$$a_n \equiv 0 \pmod{p}.$$

Enten har kongruensen

$$a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}$$

ingen løsning, eller så er der et naturlig tall l slik at $l \leq n$, og heltall x_1, x_2, …, x_l, slik at følgende er sanne.

(I) For hvert naturlig tall i slik at $i \leq l$, er

$$a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}.$$

(II) La z være et heltall slik at

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_2 z^2 + a_1 z + a_0 \equiv 0 \pmod{p}.$$

Da finnes det et naturlig tall i slik at $i \leq l$ og $z \equiv x_i \pmod{p}$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. La a_0 og a_1 være heltall. Siden p er et primtall og det ikke er sant at

$$a_1 \equiv 0 \pmod{p},$$

følger det fra Proposisjon 4.2.28 at det finnes et heltall x slik at følgende er sanne.

(1) Vi har: $a_1 x \equiv -a_0 \pmod{p}$.

(2) La y være et heltall slik at $a_1 y \equiv -a_0 \pmod{p}$. Da er $x \equiv y \pmod{p}$.

Det følger fra (1) og Korollar 3.2.39 at

$$a_1 x + a_0 \equiv 0 \pmod{p}.$$

Således er proposisjonen sann når $n = 1$, ved å la $l = 1$ og $x_1 = x$.

Anta nå at proposisjonen har blitt bevist når $n = m$, hvor m er et gitt naturlig tall. For hvert heltall i slik at $0 \leq i \leq m + 1$, la a_i være et heltall. Hvis kongruensen

$$a_{m+1} x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

har ingen løsning, er proposisjonen sann. Ellers finnes det et heltall y slik at

$$a_{m+1} y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 \equiv 0 \pmod{p}.$$

Ut ifra Lemma 4.14.5 finnes det et heltall r og, for hvert naturlig tall i slik at $0 \leq i \leq m$, et heltall b_i, slik at

$$\begin{aligned} &a_{m+1} x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \\ &= (x - y)\left(b_m x^m + b_{m-1} x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r \end{aligned}$$

for hvert heltall x. Ved å la $x = y$, får vi:

$$a_{m+1}y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 = r.$$

Siden

$$a_{m+1}y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 \equiv 0 \pmod{p},$$

følger det at

$$r \equiv 0 \pmod{p}.$$

Ut ifra Korollar 3.2.39 er dermed

$$\begin{aligned} &a_{m+1}x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \\ &\equiv (x - y)\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0\right) \pmod{p} \end{aligned}$$

for hvert heltall x.

Anta først at kongruensen

$$b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0 \equiv 0 \pmod{p}$$

har ingen løsning. Da er proposisjonen sann når $n = m + 1$, ved å la l være 1 og x_1 være y.

Anta istedenfor at kongruensen

$$b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0 \equiv 0 \pmod{p}$$

har minst én løsning. Siden det ikke er sant at

$$a_{m+1} \equiv 0 \pmod{p},$$

er det ikke sant at

$$b_m \equiv 0 \pmod{p}.$$

Ut ifra antakelsen at proposisjonen er sann når $n = m$, finnes det derfor et naturlig tall l' og, for hvert naturlig tall i slik at $i \leq l'$, et heltall y_i, slik at følgende er sanne.

(A) For hvert naturlig tall i slik at $i \leq l'$, er

$$b_m y_i^m + b_{m-1}y_i^{m-1} + \cdots + b_2 y_i^2 + b_1 y_i + b_0 \equiv 0 \pmod{p}.$$

(B) La z være et heltall slik at

$$b_m z^m + b_{m-1}z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0 \equiv 0 \pmod{p}.$$

Da finnes det et naturlig tall i slik at $i \leq l'$ og $z \equiv y_i \pmod{p}$.

La da l være $l' + 1$. For hvert naturlig tall i slik at $i \leq l'$, la x_i være y_i. La x_l være y. Vi gjør følgende observasjoner.

(1) Det følger fra (A) og Korollar 3.2.45 at, for hvert naturlig tall i slik at $i \leq l'$, er

$$(y_i - y)\left(b_m y_i^m + b_{m-1} y_i^{m-1} + \cdots + b_2 y_i^2 + b_1 y_i + b_0\right) \equiv (x - y) \cdot 0 \pmod{p},$$

altså

$$(y_i - y)\left(b_m y_i^m + b_{m-1} y_i^{m-1} + \cdots + b_2 y_i^2 + b_1 y_i + b_0\right) \equiv 0 \pmod{p}.$$

Dermed er

$$(x_i - y)\left(b_m x_i^m + b_{m-1} x_i^{m-1} + \cdots + b_2 x_i^2 + b_1 x_i + b_0\right) \equiv 0 \pmod{p}$$

for hvert naturlig tall i slik at $i \leq l - 1$. Siden

$$\begin{aligned} &a_{m+1} x_i^{m+1} + a_m x_i^m + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \\ &\equiv (x_i - y)\left(b_m x_i^m + b_{m-1} x_i^{m-1} + \cdots + b_2 x_i^2 + b_1 x_i + b_0\right) \pmod{p}, \end{aligned}$$

følger det fra Korollar 3.2.33 at

$$a_{m+1} x_i^{m+1} + a_m x_i^m + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}$$

for hvert naturlig tall i slik at $i \leq l - 1$.

(2) Siden

$$a_{m+1} y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 \equiv 0 \pmod{p},$$

er

$$a_{m+1} x_l^{m+1} + a_m x_l^m + \cdots + a_2 x_l^2 + a_1 x_l + a_0 \equiv 0 \pmod{p}.$$

For hvert naturlig tall i slik at $i \leq l$, er således

$$a_{m+1} x_i^{m+1} + a_m x_i^m + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}.$$

Dermed er (I) sant.

La nå z være et heltall slik at

$$a_{m+1} z^{m+1} + a_m z^m + \cdots + a_2 z^2 + a_1 x + a_0 \equiv 0 \pmod{p}.$$

Siden

$$\begin{aligned} &a_{m+1} z^{m+1} + a_m z^m + \cdots + a_2 z^2 + a_1 x + a_0 \\ &= (z - y)\left(b_m z^m + b_{m-1} z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0\right) \end{aligned}$$

er da

$$(z - y)\left(b_m z^m + b_{m-1} z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0\right) \equiv 0 \pmod{p}.$$

Anta at det ikke er sant at

$$z \equiv y \pmod{p}.$$

Ut ifra Korollar 3.2.39 er det da ikke sant at

$$z - y \equiv 0 \pmod{p}.$$

Det følger da fra Proposisjon 4.8.28 at

$$b_m z^m + b_{m-1} z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0 \equiv 0 \pmod{p}.$$

Fra denne kongruensen og (B) deduserer vi at det finnes et naturlig tall i slik at $i \leq l'$ og

$$z \equiv y_i \pmod{p},$$

altså slik at $i \leq l - 1$ og

$$z \equiv x_i \pmod{p}.$$

Vi har således bevist: dersom

$$a_{m+1} z^{m+1} + a_m z^m + \cdots + a_2 z^2 + a_1 x + a_0 \equiv 0 \pmod{p},$$

er enten

$$z \equiv y \pmod{p},$$

altså

$$z \equiv x_l \pmod{p},$$

eller så finnes det et naturlig tall i slik at $i \leq l - 1$ og

$$z \equiv x_i \pmod{p}.$$

Dermed er (II) er sant.

Således er proposisjonen sann når $n = m + 1$. Ved induksjon konkluderer vi at proposisjonen er sann for et hvilket som helst naturlig tall n.

□

Terminologi 4.14.12. Proposisjon 4.14.11 kalles *Lagranges teorem.*

Merknad 4.14.13. Med andre ord fastslår Proposisjon 4.14.11 at, dersom det ikke er sant at

$$a_n \equiv 0 \pmod{p},$$

finnes det maksimum n løsninger til kongruensen

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

slik at ikke noe par av disse løsningene er kongruent til hverandre modulo p, og slik at enhver annen løsning er kongruent modulo p til én av disse løsningene.

Terminologi 4.14.14. Anta at kongruensen

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

har m løsninger, hvor m er et heltall slik at $0 \leq m \leq n$, slik at ikke noe par av disse m løsningene er kongruent til hverandre modulo p, og slik at enhver annen løsning er kongruent modulo p til én av disse m løsningene. Da sier vi at kongruensen

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

har *m løsninger modulo p.*

Merknad 4.14.15. Ved å benytte denne terminologien, fastslår Proposisjon 4.14.11 at, dersom det ikke er sant at

$$a_n \equiv 0 \pmod{p},$$

finnes det maksimum n løsninger modulo p til kongruensen

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}.$$

Eksempel 4.14.16. Proposisjon 4.14.11 fastslår at kongruensen

$$-3x^2 + 7x - 17 \equiv 0 \pmod{5}$$

har maksimum to løsninger p. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 4 er løsninger.

Vi har følgende. Alle kongruensene er modulo 5.

x	$-3x^2 + 7x - 17$	Løsning modulo 5?
1	$-13 \equiv 2$	✗
2	$-15 \equiv 0$	✓
3	$-23 \equiv 2$	✗
4	$-37 \equiv 3$	✗

Således har kongruensen

$$-3x^2 + 7x - 17 \equiv 0 \pmod{5}$$

én løsning modulo 5.

Eksempel 4.14.17. Proposisjon 4.14.11 fastslår at kongruensen

$$2x^2 + 3x + 5 \equiv 0 \pmod{7}$$

har maksimum to løsninger. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 6 er løsninger. Vi har følgende. Alle kongruensene er modulo 7.

x	$2x^2+3x+5$	Løsning modulo 7?
1	$10 \equiv 3$	✗
2	$19 \equiv 5$	✗
3	$32 \equiv 4$	✗
4	$49 \equiv 0$	✓
5	$70 \equiv 0$	✓
6	$95 \equiv 4$	✗

Således har kongruensen

$$2x^2+3x+5 \equiv 0 \pmod 7$$

to løsninger modulo 7.

Eksempel 4.14.18. Proposisjon 4.14.11 fastslår at kongruensen

$$5x^2+7x+6 \equiv 0 \pmod{13}$$

har maksimum to løsninger. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 12 er løsninger.

Vi har følgende. Alle kongruensene er modulo 13.

x	$5x^2+7x+6$	Løsning modulo 13?
1	$18 \equiv 5$	✗
2	$40 \equiv 1$	✗
3	$72 \equiv 7$	✗
4	$114 \equiv 10$	✗
5	$166 \equiv 10$	✗
6	$228 \equiv 7$	✗
7	$300 \equiv 1$	✗
8	$382 \equiv 5$	✗
9	$474 \equiv 6$	✗
10	$576 \equiv 4$	✗
11	$688 \equiv 12$	✗
12	$810 \equiv 4$	✗

Således har kongruensen

$$5x^2+7x+6 \equiv 0 \pmod{13}$$

ingen løsning modulo 13.

Eksempel 4.14.19. Proposisjon 4.14.11 fastslår at kongruensen

$$x^3-x^2+x+1 \equiv 0 \pmod{11}$$

har maksimum tre løsninger. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 10 er løsninger.

Vi har følgende. Alle kongruensene er modulo 11.

x	$x^3 - x^2 + x + 1$	Løsning modulo 11?
1	2	✗
2	7	✗
3	$22 \equiv 0$	✓
4	$53 \equiv 9$	✗
5	$106 \equiv 7$	✗
6	$187 \equiv 0$	✓
7	$302 \equiv 5$	✗
8	$457 \equiv 6$	✗
9	$658 \equiv 9$	✗
10	$911 \equiv 7$	✗

Således har kongruensen

$$x^3 - x^2 + x + 1 \equiv 0 \pmod{11}$$

to løsninger modulo 11.

Merknad 4.14.20. Hvis vi ikke jobber modulo p, og se istedenfor på ligningen

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0,$$

fører akkurat det samme argumentet som i beviset for Proposisjon 4.14.11 til et bevis for faktumet nevnt i Merknad 4.14.1: at denne ligningen har maksimum n løsninger.

Merknad 4.14.21. Proposisjon 4.14.11 er ikke nødvendigvis sann om vi ikke antar at p er et primtall. La oss se for eksempel på kongruensen

$$x^2 + x - 2 \equiv 0 \pmod{10}.$$

Vi har følgende. Alle kongruensene er modulo 10.

x	$x^2 + x - 2$	Løsning modulo 10?
1	0	✓
2	4	✗
3	$10 \equiv 0$	✓
4	$18 \equiv 8$	✗
5	$28 \equiv 8$	✗
6	$40 \equiv 0$	✓
7	$54 \equiv 4$	✗
8	$70 \equiv 0$	✓
9	$88 \equiv 8$	✗

Således har kongruensen

$$x^2 + x - 2 \equiv 0 \pmod{10}$$

fire løsninger modulo 10.

4.15 Wilsons teorem

Merknad 4.15.1. Kanskje ser Lagranges teorem temmelig unøyaktig ut. Det sier ikke hvor mange løsninger kongruensen

$$a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}$$

har, og sier ikke hvordan eventuelle løsninger kan finnes.

Derfor er det lett å tro at Lagranges teorem derfor ikke er så nyttig. Imidlertid kommer vi nå til å se at Lagranges teorem kan benyttes for å gi et bevis for Proposisjon 4.15.8, som er både konkret og eksakt. Beviset for Proposisjon 4.15.8 benytter altså, på en interessant måte, et overslag vi får ved å benytte Lagranges teorem som et steg mot å fastslå at den nøyaktige kongruensen i proposisjonen stemmer.

Først må vi gjøre noen forberedelser.

Lemma 4.15.2. La n være et naturlig tall slik at $n \geq 2$. La x være et heltall. Det finnes heltall a_0, a_1, …, a_{n-2} slik at:

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)\\&= x^{n-1} + a_{n-2}x^{n-2} + a_{n-3}x^{n-3} + \cdots + a_2x^2 + a_1x + a_0.\end{aligned}$$

Bevis. Først sjekker vi om lemmaet er sant når $n = 2$. I dette tilfellet er utsagnet at det finnes et heltall a_0 slik at

$$x - 1 = x - a_0.$$

Ved å la a_0 være 1, ser vi at dette riktignok er sant.

Anta nå at lemmaet har blitt bevist når $n = m$, hvor m er et gitt naturlig tall slik at $m \geq 2$. Således har det blitt bevist at det finnes heltall b_0, b_1, …, b_{m-2} slik at:

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(m-1)\big)\\&= x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0.\end{aligned}$$

Da er

$$\begin{aligned}&(x-1)(x-2)\cdots(x-m)\\&= \Big((x-1)(x-2)\cdots\big(x-(m-1)\big)\Big)\cdot(x-m)\\&= \big(x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0\big)\cdot(x-m).\end{aligned}$$

Produktet

$$\big(x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0\big)\cdot(x-m)$$

er likt summen av

$$x\left(x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0\right)$$

og

$$-m\left(x^{m-1}+b_{m-2}x^{m-2}+b_{m-3}x^{m-3}+\cdots+b_2x^2+b_1x+b_0\right),$$

altså summen av

$$\left(x^m+b_{m-2}x^{m-1}+b_{m-3}x^{m-2}+\cdots+b_2x^3+b_1x^2+b_0x\right)$$

og

$$-\left(mx^{m-1}+mb_{m-2}x^{m-2}+mb_{m-3}x^{m-3}+\cdots+mb_2x^2+mb_1x+mb_0\right).$$

Denne summen er lik

$$x^m+(b_{m-2}+m)\,x^{m-1}+(b_{m-3}+mb_{m-2})\,x^{m-2}+\cdots+(b_1+mb_2)\,x^2+(b_0+mb_1)\,x+mb_0.$$

Dermed har vi vist at

$$\begin{aligned}&(x-1)(x-2)\cdots(x-m)\\&=x^m+(b_{m-2}+m)\,x^{m-1}+(b_{m-3}+mb_{m-2})\,x^{m-2}+\cdots+(b_1+mb_2)\,x^2+(b_0+mb_1)\,x+mb_0.\end{aligned}$$

La a_0 være mb_0. For hvert naturlig tall i slik at $i\leq m-2$, la a_i være $b_{i-1}+mb_i$. La a_{m-1} være $b_{m-2}+m$. Da er

$$\begin{aligned}&(x-1)(x-2)\cdots(x-m)\\&=x^m+a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_2x^2+a_1x+a_0.\end{aligned}$$

Dermed er lemmaet sant når $n=m+1$.

Ved induksjon konkluderer vi at lemmaet er sant for alle de naturlige tallene n slik at $n\geq 2$.

□

Eksempel 4.15.3. Lemma 4.15.2 fastslår at det finnes heltall a_0 og a_1 slik at

$$(x-1)(x-2)=x^2+a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)=x^2-3x+2,$$

altså kan vi la a_0 være 2 og a_1 være -3.

Eksempel 4.15.4. Lemma 4.15.2 fastslår at det finnes heltall a_0, a_1, a_2 slik at

$$(x-1)(x-2)(x-3)=x^3+a_2x^2+a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)(x-3)=x^3-6x^2+11x-6,$$

altså kan vi la a_0 være -6, a_1 være 11, og a_2 være -6.

Korollar 4.15.5. La n være et naturlig tall slik at $n \geq 2$. La x være et heltall. Det finnes heltall a_0, a_1, …, a_{n-2} slik at:

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)-\big(x^{n-1}-1\big)\\&=a_{n-2}x^{n-2}+a_{n-3}x^{n-3}+\cdots+a_2x^2+a_1x+a_0.\end{aligned}$$

Bevis. Ut ifra Lemma 4.15.2 finnes det heltall b_0, b_1, …, b_{n-1} slik at

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)\\&=x^{n-1}+b_{n-2}x^{n-2}+b_{n-3}x^{n-3}+\cdots+b_2x^2+b_1x+b_0.\end{aligned}$$

Da er

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)-\big(x^{n-1}-1\big)\\&=\big(x^{n-1}+b_{n-2}x^{n-2}+b_{n-3}x^{n-3}+\cdots+b_2x^2+b_1x+b_0\big)-x^{n-1}+1\\&=b_{n-2}x^{n-2}+b_{n-3}x^{n-3}+\cdots+b_2x^2+b_1x+b_0+1.\end{aligned}$$

La $a_0 = b_0 + 1$. For hvert naturlig tall i slik at $i \leq n-2$, la $a_i = b_i$. Da er

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)-\big(x^{n-1}-1\big)\\&=a_{n-2}x^{n-2}+a_{n-3}x^{n-3}+\cdots+a_2x^2+a_1x+a_0.\end{aligned}$$

□

Eksempel 4.15.6. Korollar 4.15.5 fastslår at det finnes heltall a_0 og a_1 slik at

$$(x-1)(x-2)-\big(x^2-1\big)=a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)-\big(x^2-1\big)=-3x+3,$$

altså kan vi la a_0 være -3 og a_1 være 3.

Eksempel 4.15.7. Korollar 4.15.5 fastslår at det finnes heltall a_0, a_1, a_2 slik at

$$(x-1)(x-2)(x-3)-\big(x^3-1\big)=a_2x^2+a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)(x-3)=-6x^2+11x-5,$$

altså kan vi la a_0 være -6, a_1 være 11, og a_2 være -5.

Proposisjon 4.15.8. La p være et primtall. Da er

$$(p-1)!\equiv -1 \pmod{p}.$$

Bevis. Anta først at $p = 2$. Vi har:

$$(2-1)! - (-1) = 1! - (-1) = 1 + 1 = 2.$$

Siden $2 \mid 2$, deduserer vi at

$$(2-1)! \equiv -1 \pmod{2}.$$

Dermed er proposisjonen sann i dette tilfellet.

Anta nå at $p > 2$. La x være et heltall. Ut ifra Korollar 4.15.5 finnes det heltall a_0, a_1, …, a_{p-2} slik at

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big)\\ &= a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_2x^2 + a_1x + a_0.\end{aligned}$$

Anta at det ikke er sant at

$$a_i \equiv 0 \pmod{p}$$

for alle heltallene i slik at $0 \leq i \leq p-2$. La da m være det største heltallet slik at:

(i) $0 \leq m \leq p-2$;

(ii) det ikke er sant at

$$a_m \equiv 0 \pmod{p}.$$

Da er

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big)\\ &= a_mx^m + a_{m-1}x^{m-1} + \cdots + a_2x^2 + a_1x + a_0.\end{aligned}$$

For hvert naturlig tall r slik at $r \leq p-1$ er følgende sanne.

(1) Siden $(r-r) = 0$, er

$$(x-1)(x-2)\cdots\big(x-(p-1)\big) = 0.$$

(2) Ut ifra Korollar 4.10.8 er

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

Dermed er

$$r^{p-1} - 1 \equiv 1 - 1 \pmod{p},$$

altså

$$r^{p-1} - 1 \equiv 0 \pmod{p}.$$

(3) Det følger fra (1) og (2) at

$$(r-1)(r-2)\cdots\big(r-(p-1)\big) - \big(r^{p-1}-1\big) \equiv 0 \pmod{p}.$$

For hvert naturlig tall r slik at $r \leq p-1$, er dermed $x = r$ en løsning til kongruensen

$$(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big) \equiv 0 \pmod{p},$$

altså til kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}.$$

Således har kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

minst $p-1$ løsninger.

Siden det ikke er sant at

$$a_m \equiv 0 \pmod{p},$$

følger det på en annen side fra Proposisjon 4.14.11 at kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

har maksimum m løsninger. Vi har: $m \leq p-2$. Dermed har vi en motsigelse: kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

kan ikke ha både minst $p-1$ løsninger og maksimum $p-2$ løsninger.

Vi har således bevist at antakelsen at det ikke er sant at

$$a_i \equiv 0 \pmod{p}$$

for alle heltallene i slik at $0 \leq i \leq p-2$ fører til en motsigelse. Derfor er

$$a_i \equiv 0 \pmod{p}$$

for alle heltallene i slik at $0 \leq i \leq p-2$.

Det følger fra Korollar 3.2.45 og Proposisjon 3.2.36 at, for et hvilket som helst heltall x, er da

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big)\\ &\equiv 0\cdot x^{p-2} + 0\cdot x^{p-3} + \cdots + 0\cdot x^2 + 0\cdot x + 0 \pmod{p},\end{aligned}$$

altså

$$(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big) \equiv 0 \pmod{p}.$$

La $x = 0$. Ut ifra den foregående proposisjonen er

$$(0-1)(0-2)\cdots\big(0-(p-1)\big) - \big({}^{p-1}-1\big) \equiv 0 \pmod{p},$$

altså

$$(-1)^{p-1}\big(1\cdot 2\cdots(p-1)\big) + 1 \equiv 0 \pmod{p}.$$

Ut ifra Korollar 3.2.39 er dermed

$$(-1)^{p-1}(p-1)! \equiv -1 \pmod{p}.$$

Ut ifra Proposisjon 4.2.31, finnes det et naturlig tall k slik at $p-1=2k$. Derfor er

$$(-1)^{p-1} = (-1)^{2k} = \left((-1)^2\right)^k = 1^k = 1.$$

Vi konkluderer at

$$(p-1)! \equiv -1 \pmod{p}.$$

□

Terminologi 4.15.9. Proposisjon 4.15.8 kalles *Wilsons teorem.*

Eksempel 4.15.10. Siden 3 er et primtall og $3 > 2$, fastslår Proposisjon 4.15.8 at

$$(3-1)! \equiv -1 \pmod{3}.$$

Siden $(3-1)! = 2! = 2$ og

$$2 \equiv -1 \pmod{3},$$

er dette riktignok sant.

Eksempel 4.15.11. Siden 5 er et primtall og $5 > 2$, fastslår Proposisjon 4.15.8 at

$$(5-1)! \equiv -1 \pmod{5}.$$

Siden $(5-1)! = 4! = 24$ og

$$24 \equiv -1 \pmod{5},$$

er dette riktignok sant.

Eksempel 4.15.12. Siden 7 er et primtall og $7 > 2$, fastslår Proposisjon 4.15.8 at

$$(7-1)! \equiv -1 \pmod{7}.$$

Siden $(7-1)! = 6! = 720$ og

$$720 \equiv -1 \pmod{7},$$

er dette riktignok sant.

Proposisjon 4.15.13. Det naturlige tallet

$$2 \cdot (26!) + 1$$

er delelig med 29.

Bevis. Vi gjør følgende observasjoner.

(1) Vi har: $2 = (-1) \cdot (-2)$. Derfor er

$$2 \cdot (26!) = (-1) \cdot (-2) \cdot (26!).$$

(2) Vi har:

$$-1 \equiv 28 \pmod{29}$$

og

$$-2 \equiv 27 \pmod{29}.$$

(3) Det følger fra (2) og Proposisjon 3.2.42 at

$$(-1) \cdot (-2) \equiv 28 \cdot 27 \pmod{29}.$$

(4) Det følger fra (3) og Korollar 3.2.45 at

$$(-1) \cdot (-2) \cdot (26!) \equiv 28 \cdot 27 \cdot 26! \pmod{29}.$$

Siden $28 \cdot 27 \cdot (26!) = 28!$, er dermed

$$(-1) \cdot (-2) \cdot (26!) \equiv 28! \pmod{29}.$$

(5) Siden 29 er et primtall, følger det fra Proposisjon 4.15.8 at

$$28! \equiv -1 \pmod{29}.$$

(6) Det følger fra (4), (5), og Proposisjon 3.2.33 at

$$(-1) \cdot (-2) \cdot (26!) \equiv -1 \pmod{29}.$$

Det følger fra (1) og (6) at

$$2 \cdot (26!) \equiv -1 \pmod{29}.$$

Ut ifra Korollar 3.2.39 er da

$$2 \cdot (26!) + 1 \equiv -1 + 1 \pmod{29},$$

altså

$$2 \cdot (26!) + 1 \equiv 0 \pmod{29}.$$

Vi konkluderer at $29 \mid 2 \cdot (26!) + 1$. □

Merknad 4.15.14. Det er naturlig å se først på Wilsons teorem som er artig, men ikke så viktig fra et teoretisk synspunkt. Imidlertid kommer til å benytte Wilsons teorem i løpet av vårt bevis for det dypeste teoremet i kurset, Teorem 5.8.30!

O4 Oppgaver – Primtall

O4.1 Oppgaver i eksamens stil

Oppgave O4.1.1. Hvilke naturlige tall x slik at $30 \leq x \leq 45$ er primtall?

Oppgave O4.1.2. La p være et primtall slik at $p > 2$ og $p \neq 5$. Gjør følgende.

(1) Dersom $p \equiv 7 \pmod{10}$, vis at $p^2 \equiv -1 \pmod{10}$.

(2) Vis at det ikke er sant at $p \equiv 4 \pmod{10}$. *Tips*: Benytt Proposisjon 3.2.54.

(3) Vis at enten $p^2 - 1$ er delelig med 10 eller $p^2 + 1$ er delelig med 10.

Oppgave O4.1.3. Gjør følgende.

(1) Skriv ned de første 10 primtallene p slik at $p \equiv 5 \pmod{6}$.

(2) La n være et naturlig tall. Bevis at det er et primtall p slik at $p \equiv 5 \pmod{6}$ og $p > n$. Med andre ord, bevis at det er uendelig mange primtall som er kongruent til 5 modulo 6. *Tips*: Se på $6q - 1$, hvor q er produktet av alle primtallene som er mindre enn eller like n og som er kongruent til 5 modulo 6.

Oppgave O4.1.4. Løs Oppgave 2 i Øving 4 ved å benytte kongruenser istedenfor å benytte divisjonsalgoritmen direkte.

Oppgave O4.1.5. Gjør følgende.

(1) Finn en primtallsfaktorisering til 7623.

(2) Finn en primtallsfaktorisering til 2352.

(3) Benytt (1) og (2) for å finne den største felles divisoren til 7623 og 2352.

Oppgave O4.1.6. Finn en invers til 6 modulo 13.

Oppgave O4.1.7. Benytt Fermats lille teorem for å vise at $6^{146} + 2$ er delelig med 19.

Oppgave O4.1.8. La x være et heltall. Anta at $\mathsf{sfd}(x, 21) = 1$. Vis at $8x^6 + 55$ er delelig med 63.

Oppgave O4.1.9. Finn uten å benytte Euklids algoritme og uten gå gjennom alle heltallene 0, 1, ..., 28 en løsning x til kongruensen

$$3x \equiv 8 \pmod{29},$$

slik at $0 \leq x < 29$. Forklar hvorfor enhver annen løsning er kongruent modulo 29 til løsningen du har funnet.

Oppgave O4.1.10. Skriv ned ordenene modulo 11 til alle de naturlige tallene 1, 2, ..., 10. Hvilke av 1, 2, ..., 10 er primitive røtter modulo 11?

Oppgave O4.1.11. Vis uten å regne ut at $18 \cdot (33!) - 3$ er delelig med 37.

O4.2 Oppgaver for å hjelpe med å forstå kapittelet

Oppgave O4.2.1. Gå gjennom beviset for Teorem 4.3.3 når $n = 18$. Hva er det minste primetall større enn 18 som vi får? *Tips*: 510511 er delelig med 277 og 97, og både 277 og 97 er primtall.

Oppgave O4.2.2. La p være 11. Regn ut de første ti naturlige tallene i sekvensen i Definisjon **??**. Ved å benytte svaret ditt på Oppgave O4.1.10, sjekk om det tiende naturlige tallet i sekvensen er en primitiv rot modulo 11.

5 Kvadratisk gjensidighet

5.1 Kvadratiske kongruenser

Merknad 5.1.1. Fra skolen vet du at en ligning

$$ax^2 + bx + c = 0$$

har 0, 1, eller 2 løsningner. Hvis $\sqrt{b^2 - 4ac} < 0$, har ligningen 0 løsninger. Hvis $\sqrt{b^2 - 4ac} = 0$, har ligningen 1 løsning. Hvis $\sqrt{b^2 - 4ac} > 0$, har ligningen 2 løsninger.

Hvis $\sqrt{b^2 - 4ac} \geq 0$, vet dessuten en formell for å finne disse løsningene:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Imidlertid er disse ligningne ofte ikke heltall. Løsningene til ligningen

$$x^2 - 2 = 0$$

er for eksempel $x = \pm\sqrt{2}$.

I dette kapittelet kommer vi til å se på heltallsløsninger til kongruenser

$$ax^2 + bx + c \equiv 0 \pmod{n}.$$

Terminologi 5.1.2. La n være et heltall slik at $n \neq 0$. La a, b, og c være heltall. La x være et heltall slik at

$$ax^2 + bx + c \equiv 0 \pmod{n}.$$

Da sier vi at x er en *løsning* til denne kongruensen.

Terminologi 5.1.3. La n være et heltall slik at $n \neq 0$. La a, b, og c være heltall. Når vi er interessert i heltall x som er løsninger til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{n},$$

kalles

$$ax^2 + bx + c \equiv 0 \pmod{n}$$

en *kvadratisk kongruens*.

Merknad 5.1.4. Vi skal fokusere på kongruenser

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

hvor p er et primtall og $p > 2$.

Merknad 5.1.5. Nå har vi blitt fortrolig med algebraiske manipulasjoner med kongruenser. Heretter skal vi derfor gi referansen til proposisjonen eller korollaret i §3.2 som fastslår at en algebraisk manipulasjon vi benytter er gydlig kun når dette er uklart.

Lemma 5.1.6. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da er det ikke sant at

$$2a \equiv 0 \pmod{p}.$$

Bevis. Anta at

$$2a \equiv 0 \pmod{p}.$$

Fra Proposisjon 3.2.13 har vi da: $p \mid 2a$. Siden p er et primtall, følger det fra Proposisjon 4.2.12 at enten $p \mid 2$ eller $p \mid a$. Imidlertid fastslår følgende observasjoner at verken $p \mid 2$ eller $p \mid a$ er sant.

(1) Siden det ikke er sant at

$$a \equiv 0 \pmod{p},$$

følger det fra Proposisjon 3.2.13 at det ikke er sant at $p \mid a$.

(2) Det eneste primtallet som deler 2 er 2. Siden $p > 2$, er det derfor ikke sant at $p \mid 2$.

Således fører antakelsen at $2a \equiv 0 \pmod{p}$ til en motsigelse. Vi konkluderer at det ikke er sant $2a \equiv 0 \pmod{p}$. □

Lemma 5.1.7. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da er det ikke sant at

$$4a \equiv 0 \pmod{p}.$$

Bevis. Siden det ikke er sant at

$$a \equiv 0 \pmod{p},$$

følger det fra Lemma 5.1.6 at det ikke er sant at

$$2a \equiv 0 \pmod{p}.$$

Dermed følger det fra Lemma 5.1.6 at det ikke er sant at

$$2(2a) \equiv 0 \pmod{p},$$

altså at det ikke er sant at

$$4a \equiv 0 \pmod{p}.$$

□

Lemma 5.1.8. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. Anta at det ikke er sant at $a \equiv 0 \pmod{p}$. Da er x en løsning til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

hvis og bare hvis x er en løsning til kongruensen

$$(4a)\left(ax^2 + bx + c\right) \equiv 0 \pmod{p}.$$

Bevis. Anta først at

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

Ut ifra Korollar 3.2.45 er da

$$(4a)\left(ax^2 + bx + c\right) \equiv 0 \pmod{p}.$$

Anta istedenfor at

$$(4a)\left(ax^2 + bx + c\right) \equiv 0 \pmod{p}.$$

Siden det ikke er sant at

$$a \equiv 0 \pmod{p},$$

følger det fra Lemma 5.1.7 at det ikke er sant at

$$4a \equiv 0 \pmod{p}.$$

Da følger det fra Proposisjon 4.8.28 at

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

□

Proposisjon 5.1.9. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. Anta at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

La y være et heltall slik at

$$y^2 \equiv b^2 - 4ac \pmod{p}.$$

La x være et heltall slik at

$$2ax \equiv y - b \pmod{p}.$$

Da er

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Vi har:

$$\begin{aligned}(2ax + b)^2 - (b^2 - 4ac) &= \left(4a^2x^2 + 4abx + b^2\right) - b^2 + 4ac \\ &= 4a\left(ax^2 + bx + c\right).\end{aligned}$$

Dermed er

$$4a\left(ax^2 + bx + c\right) = (2ax + b)^2 - (b^2 - 4ac).$$

(2) Siden

$$2ax \equiv y - b \pmod{p},$$

er

$$2ax + b \equiv y \pmod{p}.$$

Det følger at

$$(2ax + b)^2 - (b^2 - 4ac) \equiv y^2 - (b^2 - 4ac) \pmod{p}.$$

(3) Siden

$$y^2 \equiv b^2 - 4ac \pmod{p},$$

er

$$y^2 - (b^2 - 4ac) \equiv 0 \pmod{p}.$$

Det følger fra (1) – (3) at

$$4a\left(ax^2 + bx + c\right) \equiv 0 \pmod{p}.$$

Ut ifra Lemma 5.1.8 er da

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

□

Eksempel 5.1.10. La oss se på kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

Vi har:

$$7^2 - 4 \cdot 1 \cdot 10 = 49 - 40 = 9.$$

La oss således se på kongruensen

$$y^2 \equiv 9 \pmod{11}.$$

Vi har: $y = 3$ er en løsning til denne kongruensen.
La oss da se på kongruensen

$$(2 \cdot 1)x \equiv 3 - 7 \pmod{11},$$

altså kongruensen

$$2x \equiv -4 \pmod{11}.$$

Siden

$$-4 \equiv 7 \pmod{11},$$

er et heltall x er en løsning til denne kongruensen hvis og bare hvis det finnes en løsning til kongruensen

$$2x \equiv 7 \pmod{11}.$$

Siden $x = 9$ er en løsning til denne kongruensen, er derfor $x = 9$ en løsning til kongruensen

$$2x \equiv -4 \pmod{11}.$$

Da fastslår Proposisjon 5.1.9 at $x = 9$ er en løsning til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

Siden

$$9^2 + 7 \cdot 9 + 10 = 81 + 63 + 10 = 154$$

og

$$154 \equiv 0 \pmod{11},$$

er dette riktignok sant.

Eksempel 5.1.11. La oss se på kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod{7}.$$

Vi har:

$$6^2 - 4 \cdot 4 \cdot 2 = 36 - 32 = 4.$$

La oss således se på kongruensen

$$y^2 \equiv 4 \pmod{7}.$$

Vi har: $y = 2$ er en løsning til denne kongruensen.

La oss da se på kongruensen

$$(2 \cdot 4)x \equiv 2 - 6 \pmod{7},$$

altså kongruensen

$$8x \equiv -4 \pmod{7}.$$

Siden

$$-4 \equiv 3 \pmod{7}$$

og

$$8 \equiv 1 \pmod{7},$$

er et heltall x er en løsning til denne kongruensen hvis og bare hvis det finnes en løsning til kongruensen

$$x \equiv 3 \pmod{7}.$$

Siden $x = 3$ er en løsning til denne kongruensen, er derfor $x = 3$ en løsning til kongruensen

$$8x \equiv -4 \pmod{7}.$$

Da fastslår Proposisjon 5.1.9 at $x = 3$ er en løsning til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod{7}.$$

Siden

$$4 \cdot (3^2) + 6 \cdot 3 + 2 = 36 + 18 + 2 = 56$$

og

$$56 \equiv 0 \pmod{7},$$

er dette riktignok sant.

Korollar 5.1.12. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. Anta at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

La y være et heltall slik at

$$y^2 \equiv b^2 - 4ac \pmod{p}.$$

La z være et heltall slik at

$$2az \equiv y - b \pmod{p}.$$

La z' være et heltall slik at

$$2az' \equiv -y - b.$$

Da er $x = z$ og $x = z'$ løsninger til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

Dersom det ikke er sant at

$$b^2 - 4ac \equiv 0 \pmod{p},$$

er det ikke sant at

$$z \equiv z' \pmod{p}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Det følger ummidelbart fra Proposisijon 5.1.9 at $x = z$ er en løsning til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

(2) Siden $(-y)^2 = y^2$ og

$$y^2 \equiv b^2 - 4ac \pmod{p},$$

er

$$(-y)^2 \equiv b^2 - 4ac \pmod{p}.$$

(3) Det følger umiddelbart fra (2) og Proposisjon 5.1.9 at $x = z'$ er en løsning til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

Anta at

$$z \equiv z' \pmod{p}.$$

Da er

$$2az \equiv 2az' \pmod{p}.$$

Det følger at

$$y - b \equiv -y - b \pmod{p},$$

altså at

$$2y \equiv 0 \pmod{p}.$$

Siden $p > 2$, er det, ut ifra Proposisjon 2.5.30, ikke sant at $p \mid 2$, altså er det ikke sant at

$$2 \equiv 0 \pmod{p}.$$

Det følger fra Proposisjon 4.8.28 at

$$y \equiv 0 \pmod{p}.$$

Da er

$$y^2 \equiv 0 \pmod{p}.$$

Derfor er

$$b^2 - 4ac \equiv 0 \pmod{p}.$$

Således har vi bevist at, dersom

$$z \equiv z' \pmod{p},$$

er

$$b^2 - 4ac \equiv 0 \pmod{p}.$$

Vi konkluderer at, dersom det ikke er sant at

$$b^2 - 4ac \equiv 0 \pmod{p},$$

er det ikke sant at

$$z \equiv z' \pmod{p}.$$

□

Eksempel 5.1.13. La oss se igjen på kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

I Eksempel 5.1.10 fant vi at $x = 9$ er en løsning til denne kongruensen. Nå skal vi finne en annen løsning.

Ut ifra Eksempel 5.1.10 er $y = 3$ en løsning til kongruensen

$$y^2 \equiv 7^2 - 4 \cdot 1 \cdot 10.$$

Vi fant løsningen $x = 9$ til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}$$

ved å løse kongruensen

$$(2 \cdot 1)x \equiv 3 - 7 \pmod{11}.$$

Korollar 5.1.12 fastlår at vi kan finne en annen løsning til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}$$

ved å løse kongruensen

$$(2 \cdot 1)x \equiv -3 - 7 \pmod{11},$$

altså kongruensen

$$2x \equiv -10 \pmod{11}.$$

Vi har: $x = -5$ er en løsning til denne kongruensen. Derfor er $x = -5$ en løsning til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

Siden

$$-5 \equiv 6 \pmod{11},$$

følger det fra Proposisjon 4.14.2 at $x = 6$ er en løsning til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

Siden

$$6^2 + 7 \cdot 6 + 10 = 88$$

og $11 \mid 88$, er dette riktignok sant.

Således har vi: $x = 9$ og $x = 6$ er løsninger til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

Siden $7^2 - 4 \cdot 1 \cdot 10 = 9$, og det ikke er sant at

$$9 \equiv 0 \pmod{11},$$

fastslår i tillegg Korollar 5.1.12 at disse to løsningene ikke er kongruent til hverandre modulo 11. Ut ifra Proposisjon 3.2.11, er dette riktignok sant.

Eksempel 5.1.14. La oss se igjen på kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod{7}.$$

I Eksempel 5.1.11 fant vi at $x = 3$ er en løsning til denne kongruensen. Nå skal vi finne en annen løsning.

Ut ifra Eksempel 5.1.11 er $y = 2$ en løsning til kongruensen

$$y^2 \equiv 6^2 - 4 \cdot 4 \cdot 2.$$

Vi fant løsningen $x = 3$ til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod{7}$$

ved å løse kongruensen

$$(2 \cdot 4)x \equiv 2 - 6 \pmod{7}.$$

Korollar 5.1.12 fastlår at vi kan finne en annen løsning til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod{7}$$

ved å løse kongruensen

$$(2 \cdot 4)x \equiv -2 - 6 \pmod{7},$$

altså kongruensen

$$8x \equiv -8 \pmod{7}.$$

Vi har: $x = -1$ er en løsning til denne kongruensen. Derfor er $x = -1$ en løsning til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod{7}.$$

Siden

$$-1 \equiv 6 \pmod{7},$$

følger det fra Proposisjon 4.14.2 at $x = 6$ er en løsning til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod{7}.$$

Siden

$$4 \cdot 6^2 + 6 \cdot 6 + 2 = 182$$

og $7 \mid 182$, er dette riktignok sant.

Således har vi: $x = 3$ og $x = 6$ er løsninger til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod{7}.$$

Siden $6^2 - 4 \cdot 4 \cdot 2 = 4$, og det ikke er sant at

$$4 \equiv 0 \pmod{7},$$

fastslår i tillegg Korollar 5.1.12 at disse to løsningene ikke er kongruent til hverandre modulo 7. Ut ifra Proposisjon 3.2.11, er dette riktignok sant.

Terminologi 5.1.15. La a, b, og c være heltall. Heltallet $b^2 - 4ac$ kalles *diskriminanten* til a, b, og c.

Notasjon 5.1.16. La a, b, og c være heltall. Diskriminanten til a, b, og c betegnes ofte som Δ, det greske bokstavet som tilsvarer til bokstavet «d».

Merknad 5.1.17. La p være et primtall slik at $p > 2$. Proposisjon 5.1.9 gir muligheten til å gjøre enklere teorien til kvadratisk kongruenser modulo p. Tidligere i kurset har vi rukket en veldig god forståelse for hvordan løse lineære kongruenser. Dermed forstår vi hvordan kongruensen

$$2ax \equiv y - c \pmod{p}$$

i Proposisjon 5.1.9 kan løses.

For å finne en løsning til en hvilken som helst kvadratisk kongruens, fastslår således Proposisjon 5.1.9 at vi kan fokusere på kongruenser

$$y^2 \equiv \Delta \pmod{p},$$

hvor Δ er et heltall.

Merknad 5.1.18. Sammenlign Proposisjon 5.1.9 med formellen for løsningene til en kvadratisk ligning som du kjenner til fra skolen, nevnt i Merknad 5.1.1. Å si at

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

er det samme som å si at x er en løsning til ligningen

$$2ax = y - b,$$

hvor y er én av de to mulige løsningene til ligningen

$$y^2 = b^2 - 4ac,$$

det vil si enten

$$y = \sqrt{b^2 - 4ac}$$

eller

$$y = -\sqrt{b^2 - 4ac}.$$

Proposisjon 5.1.9 og Korollar 5.1.12 sier at vi kan finne en løsning til en kvadratisk kongruens modulo p på akkurat den samme måten. Den eneste forskjellen er at vi ikke alltid kan ta kvadratroten av et heltall og få et heltall. Med andre ord er det ikke så lett å løse kongruensen

$$y^2 \equiv b^2 - 4ac \pmod{p}$$

som å løse ligningen

$$y^2 = b^2 - 4ac,$$

fordi vi er kun interessert i heltallsløsninger til kongruenser. Dermed må vi studere når i modulær aritmetikk et heltall «har en kvadratrot» som er et heltall. La oss begunne med dette med en gang!

5.2 Kvadratiske rester

Definisjon 5.2.1. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da er a en *kvadratisk rest* modulo p dersom det finnes et heltall x slik at

$$x^2 \equiv a \pmod{p}.$$

Eksempel 5.2.2. Siden $3^2 = 9$ og

$$9 \equiv 2 \pmod{7},$$

er 2 en kvadratisk rest modulo 7.

Eksempel 5.2.3. Siden $4^2 = 16$ og

$$16 \equiv 5 \pmod{11},$$

er 5 en kvadratisk rest modulo 11.

Merknad 5.2.4. Å si at a er en kvadratisk rest modulo p er det samme som å si: «a har en kvadratrot modulo p».

Proposisjon 5.2.5. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da er a en *kvadratisk rest* modulo p hvis og bare hvis det finnes et heltall r slik at $1 \leq r \leq p-1$ og

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

Bevis. Anta først at det finnes et heltall r slik at $1 \leq r \leq p-1$ og

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

Da er a en kvadratisk rest modulo p: la x være r i Definisjon 5.2.1.

Anta istedenfor at a er en kvadratisk rest modulo p. Da finnes det et heltall x slik at

$$x^2 \equiv a \pmod{p}.$$

Ut ifra Proposisjon 3.2.1 finnes det et heltall r slik at $0 \leq r \leq p-1$ og

$$x \equiv r \pmod{p}.$$

Anta først at $r = 0$. Da er

$$x \equiv 0 \pmod{p}.$$

Dermed er

$$x^2 = 0 \pmod{p}.$$

Siden

$$x^2 \equiv a \pmod{p},$$

følger det at

$$a \equiv 0 \pmod{p}.$$

Imidlertid har vi antatt at dette ikke er sant. Siden antakelsen at $r = 0$ fører til denne motsigelsen, deduserer vi at det ikke er sant at $r = 0$. Dermed er $1 \leq r \leq p - 1$.

Siden

$$x \equiv r \pmod{p},$$

er

$$x^2 \equiv r^2 \pmod{p}.$$

Siden

$$x^2 \equiv a \pmod{p},$$

følger det at

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

□

Eksempel 5.2.6. Siden $7^2 = 49$ og

$$49 \equiv 4 \pmod{5},$$

er 4 en kvadratisk rest modulo 5. Proposisjon 5.2.5 fastslår at det da er et heltall r slik at:

(1) $1 \leq r \leq 4$;

(2) $7 \equiv r \pmod{5}$;

(3) $r^2 \equiv 4 \pmod{5}$.

Dette er riktignok sant: vi kan velge r til å være 2.

Eksempel 5.2.7. Siden $17^2 = 289$ og

$$289 \equiv 3 \pmod{11},$$

er 3 en kvadratisk rest modulo 11. Proposisjon 5.2.5 fastslår at det da er et heltall r slik at:

(1) $1 \leq r \leq 10$;

(2) $17 \equiv r \pmod{11}$;

(3) $r^2 \equiv 3 \pmod{11}$.

Dette er riktignok sant: vi kan velge r til å være 6.

Proposisjon 5.2.8. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Ut ifra Proposisjon 3.2.1 finnes det da et heltall r slik at $1 \leq r \leq p-1$ og

$$a \equiv r \pmod{p}.$$

Da er a en kvadratisk rest modulo p hvis og bare hvis r er en kvadratisk rest modulo p.

Bevis. Siden

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

finnes det et heltall x slik at

$$x^2 \equiv a \pmod{p}$$

hvis og bare hvis det finnes et heltall x slik at

$$x^2 \equiv r \pmod{p}.$$

□

Eksempel 5.2.9. Siden $6^2 = 36$ er 36 en kvadratisk rest modulo et hvilket helst primtall p slik at $p > 2$. Siden

$$36 \equiv 1 \pmod{5},$$

fastslår Proposisjon 5.2.8 at 1 er kvadratisk rest modulo 5.
Siden

$$36 \equiv 3 \pmod{11},$$

fastslår Proposisjon 5.2.8 at 3 er kvadratisk rest modulo 11.
Siden

$$36 \equiv 2 \pmod{17},$$

fastslår Proposisjon 5.2.8 at 2 er kvadratisk rest modulo 17.

Eksempel 5.2.10. Siden $8^2 = 64$ er 64 en kvadratisk rest modulo et hvilket helst primtall p slik at $p > 2$. Siden

$$64 \equiv 4 \pmod{5},$$

fastslår Proposisjon 5.2.8 at 4 er kvadratisk rest modulo 5.
Siden

$$64 \equiv 1 \pmod{7},$$

fastslår Proposisjon 5.2.8 at 1 er kvadratisk rest modulo 7.
Siden

$$64 \equiv 9 \pmod{11},$$

fastslår Proposisjon 5.2.8 at 9 er kvadratisk rest modulo 11.

Merknad 5.2.11. La oss avgjøre hvilke heltall er kvadratiske rester modulo noen bestemte primtall. Det følger fra Proposisjon 5.2.5 og Proposisjon 5.2.8 at det er nok å gå gjennom heltallene 1^2, 2^2, ..., $(p-1)^2$ og sjekke hvilke heltall blant 1, 2, ..., $p-1$ de er kongruent til modulo p.

Eksempel 5.2.12. La p være 3. Vi regner som følger.

x	x^2	r slik at $1 \leq r \leq 2$ og $x^2 \equiv r \pmod 3$
1	1	1
2	4	1

Dermed er 1 en kvadratisk rest modulo 3, og enhver annen kvadratisk rest modulo 3 er kongruent til 1 modulo 3.

Eksempel 5.2.13. La p være 5. Vi regner som følger.

x	x^2	r slik at $1 \leq r \leq 4$ og $x^2 \equiv r \pmod 5$
1	1	1
2	4	4
3	9	4
4	16	1

Dermed er 1 og 4 kvadratiske rester modulo 5, og enhver annen kvadratisk rest modulo 5 er kongruent til enten 1 eller 4 modulo 5.

Eksempel 5.2.14. La p være 7. Vi regner som følger.

x	x^2	r slik at $1 \leq r \leq 6$ og $x^2 \equiv r \pmod 7$
1	1	1
2	4	4
3	9	2
4	16	2
5	25	4
6	36	1

Dermed er 1, 2, og 4 kvadratiske rester modulo 7, og enhver annen kvadratisk rest modulo 7 er kongruent til én av disse tre naturlige tallene modulo 7.

Eksempel 5.2.15. La p være 11. Vi regner som følger.

x	x^2	r slik at $1 \leq r \leq 10$ og $x^2 \equiv r \pmod{11}$
1	1	1
2	4	4
3	9	9
4	16	5
5	25	3
6	36	3
7	49	5
8	64	9
9	81	4
10	100	1

Dermed er 1, 3, 4, 5, og 9 kvadratiske rester modulo 11, og enhver annen kvadratisk rest modulo 11 er kongruent til én av disse fem naturlige tallene modulo 11.

Merknad 5.2.16. Følgende proposisjon er motsatt til Proposisjon 5.1.9.

Proposisjon 5.2.17. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. La x være en løsning til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

La $y = 2ax + b$. Da er y en løsning til kongruensen

$$y^2 \equiv b^2 - 4ac \pmod{p}.$$

Bevis. Vi regner som følger.

$$\begin{aligned} y^2 &= (2ax + b)^2 \\ &= 4a^2x^2 + 4abx + b^2 \\ &= b^2 + 4a\left(ax^2 + bx\right) \\ &= b^2 + 4a\left(ax^2 + bx + c - c\right) \\ &= b^2 + 4a\left(ax^2 + bx + c\right) - 4ac. \end{aligned}$$

Siden

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

er

$$b^2 + 4a\left(ax^2 + bx + c\right) - 4ac \equiv b^2 - 4ac \pmod{p}.$$

Dermed er

$$y^2 \equiv b^2 - 4ac \pmod{p}.$$

□

Eksempel 5.2.18. Siden

$$2 \cdot \left(5^2\right) - 5 + 4 = 49$$

og

$$49 \equiv 0 \pmod 7,$$

er $x = 5$ en løsning til kongruensen

$$2x^2 - x + 4 \equiv 0 \pmod 7.$$

Da fastslår Proposisjon 5.2.17 at $y = 2 \cdot 2 \cdot 5 + (-1)$, altså $y = 19$, er en løsning til kongruensen

$$y^2 \equiv (-1)^2 - 4 \cdot 2 \cdot 4 \pmod 7,$$

altså til kongruensen

$$y^2 \equiv -31 \pmod 7.$$

Siden

$$19 \equiv 5 \pmod 7,$$

, er

$$y^2 \equiv 25 \equiv 4 \pmod 7.$$

I tillegg har vi:

$$-31 \equiv 4 \pmod 7.$$

Dermed er det riktignok sant at

$$19^2 \equiv -31 \pmod 7.$$

Eksempel 5.2.19. Siden

$$3 \cdot \left(4^2\right) + 7 \cdot 4 + 1 = 77$$

og

$$77 \equiv 0 \pmod{11},$$

er $x = 3$ en løsning til kongruensen

$$3x^2 + 7x + 1 \equiv 0 \pmod{11}.$$

Da fastslår Proposisjon 5.2.17 at $y = 2 \cdot 3 \cdot 4 + 7$, altså $y = 31$, er en løsning til kongruensen

$$y^2 \equiv 7^2 - 4 \cdot 3 \cdot 1 \pmod{11},$$

altså til kongruensen

$$y^2 \equiv 37 \pmod{11}.$$

Siden

$$31 \equiv -2 \pmod{11},$$

, er

$$y^2 \equiv 4 \pmod{11}.$$

I tillegg har vi:

$$37 \equiv 4 \pmod{11}.$$

Dermed er det riktignok sant at

$$31^2 \equiv 37 \pmod{11}.$$

Lemma 5.2.20. La p være et primtall slik at $p > 2$. La a og b være heltall. Anta at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da har kongruensen

$$2ax \equiv y - b \pmod{p}$$

en løsning for et hvilket som helst heltall y.

Bevis. Siden det ikke er sant at

$$a \equiv 0 \pmod{p},$$

følger det fra Lemma 5.1.6 at det ikke er sant at

$$2a \equiv 0 \pmod{p}.$$

Fra Proposisjon 3.2.13 deduserer vi at det ikke er sant at $p \mid 2a$. Da følger det fra Proposisjon 4.2.28 at kongruensen

$$2ax \equiv y - b \pmod{p}$$

har en løsning når $y - b$ er et hvilket som helst heltall, altså når y er et hvilket som helst heltall. □

Eksempel 5.2.21. Siden det ikke er sant at

$$5 \equiv 0 \pmod{3},$$

fastslår Lemma 5.2.20 at kongruensen

$$10x \equiv y - 6 \pmod{3}$$

har en løsning for et hvilket som helst heltall y. Når for eksempel $y = 2$, er det riktignok sant at $x = 2$ er en løsning til kongruensen

$$10x \equiv -4 \pmod{3}.$$

Når for eksempel $y = 6$, er det riktignok sant at $x = 0$ er en løsning til kongruensen

$$10x \equiv 0 \pmod{3}.$$

Når for eksempel $y = 19$, er $x = 1$ en løsning til kongruensen

$$10x \equiv 13 \pmod{3}.$$

Korollar 5.2.22. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. Anta at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

en løsning om og bare om $b^2 - 4ac$ er en kvadratisk rest modulo p.

Bevis. Anta først at kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

har en løsning. Da følger det fra Proposisjon 5.2.17 at $b^2 - 4ac$ er en kvadratisk rest modulo p.

Anta istedenfor at $b^2 - 4ac$ er en kvadratisk rest modulo p. Vi gjør følgende observasjoner.

(1) Ut ifra Lemma 5.2.20, har kongruensen

$$2ax \equiv y - b \pmod{p}$$

en løsning for et hvilket som helst heltall y.

(2) Siden det ikke er sant at

$$a \equiv 0 \pmod{p},$$

følger det fra Lemma 5.1.6 at det ikke er sant at

$$4a \equiv 0 \pmod{p}.$$

Det følger fra (1), (2), og Proposisjon 5.1.9 at, dersom $b^2 - 4ac$ er en kvadratisk rest modulo p, altså finnes det et heltall y slik at

$$y^2 \equiv b^2 - 4ac \pmod{p},$$

har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

en løsning. □

Terminologi 5.2.23. Med andre ord har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

en løsning hvis og bare hvis $b^2 - 4ac$ «har en kvadratiskrot» som er et heltall modulo p.

Eksempel 5.2.24. La oss se på kongruensen

$$3x^2 + 5x + 4 \equiv 0 \pmod{7}.$$

Vi har:

$$5^2 - 4 \cdot 4 \cdot 3 = 25 - 48 = -23,$$

og

$$-23 \equiv 5 \pmod{7}.$$

Imidlertid vet vi fra Eksempel 5.2.14 at 5 ikke er an kvadratisk rest modulo 7. Da følger det fra Proposisjon 5.2.17 at kongruensen

$$3x^2 + 5x + 4 \equiv 0 \pmod{7}$$

har ingen løsning.

Eksempel 5.2.25. La oss se på kongruensen

$$2x^2 - 3x - 7 \equiv 0 \pmod{11}.$$

Vi har:

$$(-3)^2 - 4 \cdot 2 \cdot (-7) = 9 + 56 = 65,$$

og

$$65 \equiv 10 \pmod{11}.$$

Imidlertid vet vi fra Eksempel 5.2.15 at 10 ikke er an kvadratisk rest modulo 11. Da følger det fra Proposisjon 5.2.17 at kongruensen

$$2x^2 - 3x - 7 \equiv 11 \pmod{7}$$

har ingen løsning.

Merknad 5.2.26. I Merkand 5.1.18 lot vi merke til at finnes noen likheter mellom teorien for kvadratiske ligninger og teorien for kvadratiske kongruenser. Nå skal vi nærmere å disse likhetene.

Lemma 5.2.27. La p være et primtall. La y være et heltall slik at

$$y^2 \equiv 0 \pmod{p}.$$

Da er

$$y \equiv 0 \pmod{p}.$$

Bevis. Siden

$$y^2 \equiv 0 \pmod{p},$$

har vi: $p \mid y^2$. Siden p er et primtall, følger det fra Proposisjon 4.2.12 at $p \mid y$. Dermed er

$$y \equiv 0 \pmod{p}.$$

□

Eksempel 5.2.28. Siden

$$64 \equiv 0 \pmod 2,$$

er $y = 8$ en løsning til kongruensen

$$y^2 \equiv 0 \pmod 2.$$

Lemma 5.2.27 fastslår da at

$$8 \equiv 0 \pmod 2.$$

Dette er riktignok sant.

Eksempel 5.2.29. Siden

$$81 \equiv 0 \pmod 3,$$

er $y = 9$ en løsning til kongruensen

$$y^2 \equiv 0 \pmod 3.$$

Lemma 5.2.27 fastslår da at

$$9 \equiv 0 \pmod 3.$$

Dette er riktignok sant.

Korollar 5.2.30. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. Anta at det ikke er sant at

$$a \equiv 0 \pmod p.$$

Da er følgende sanne.

(A) Dersom $b^2 - 4ac$ ikke er en kvadratisk rest modulo p, har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod p$$

ingen løsning.

(B) Dersom

$$b^2 - 4ac \equiv 0 \pmod p,$$

har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod p$$

en løsning, og alle løsningene til denne kongruesen er kongruent til hverandre modulo p.

(C) Dersom $b^2 - 4ac$ er en kvadratisk rest modulo p, og det ikke er sant at

$$b^2 - 4ac \equiv 0 \pmod p,$$

har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod p$$

to løsninger som ikke er kongruent til hverandre modulo p, og slik at enhver annen løsning til kongruensen er kongruent til én av disse to modulo p.

Bevis. Dersom b^2-4ac ikke er en kvadratisk rest modulo p, følger det fra Korollar 5.2.22 at kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

ikke har en løsning. Dermed er (A) sant.

Anta nå at

$$b^2 - 4ac \equiv 0 \pmod{p}.$$

Da er $y = 0$ en løsning til kongruensen

$$y^2 \equiv b^2 - 4ac \pmod{p},$$

altså b^2-4ac er en kvadratisk rest modulo p. Det følger fra Korollar 5.2.22 at kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

har en løsning.

La z være et heltall slik at

$$az^2 + bz + c \equiv 0 \pmod{p}.$$

La z' være et heltall slik at

$$a(z')^2 + bz' + c \equiv 0 \pmod{p}.$$

Ut ifra antakelesen at

$$b^2 - 4ac \equiv 0 \pmod{p},$$

følger det fra Proposisjon 5.2.17 at

$$(2az + b)^2 \equiv 0 \pmod{p}$$

og

$$(2az' + b)^2 \equiv 0 \pmod{p}.$$

Ut ifra Lemma 5.2.27 er da

$$2az + b \equiv 0 \pmod{p}$$

og

$$2az' + b \equiv 0 \pmod{p}.$$

Med andre ord er både $x = z$ og $x = z'$ løsninger til kongruensen

$$2ax = -b \pmod{p}.$$

Da følger det fra Proposisjon 4.2.28 at

$$z \equiv z' \pmod{p}.$$

Dermed har vi bevist at, dersom

$$b^2 - 4ac \equiv 0 \pmod{p},$$

er følgende sanne:

(1) kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

har en løsning;

(2) alle løsningene til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

er kongruent til hverandre modulo p.

Således er (B) sant.

Anta nå at $b^2 - 4ac$ er en kvadratisk rest modulo p, og at det ikke er sant at

$$b^2 - 4ac \equiv 0 \pmod{p}.$$

Ut ifra Korollar 5.1.12 er da både $x = z$ og $x = z'$ løsninger til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

og det er ikke sant at

$$z \equiv z' \pmod{p}.$$

Det følger fra Proposisjon 4.14.11 at enhver annen løsning til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

er kongruent modulo p til enten z eller z'. Således er (C) sant. □

Eksempel 5.2.31. La oss se på kongruensen

$$3x^2 - 2x + 2 \equiv 0 \pmod{5}.$$

Vi har:

$$(-2)^2 - 4 \cdot 3 \cdot 2 = 4 - 24 = -20$$

og

$$-20 \equiv 0 \pmod{5}.$$

Derfor er $y = 0$ en løsning til kongruensen

$$y^2 \equiv (-2)^2 - 4 \cdot 3 \cdot 2 \pmod{5}.$$

Vi har: $x = 2$ er en løsning til kongruensen

$$6x \equiv 2 \pmod{5},$$

altså til kongruensen

$$(2 \cdot 3)x \equiv 0 - (-2) \pmod{5}.$$

Det følger fra Proposisjon 5.1.9 at $x = 2$ er en løsning til kongruensen

$$3x^2 - 2x + 2 \equiv 0 \pmod{5}.$$

Siden

$$(-2)^2 - 4 \cdot 3 \cdot 2 \equiv 0 \pmod{5},$$

fastslår Korollar 5.2.30 (B) at alle løsningene til kongruensen

$$3x^2 - 2x + 2 \equiv 0 \pmod{5}$$

er kongruent til 2 modulo 5.

Eksempel 5.2.32. La oss se på kongruensen

$$5x^2 + 3x + 3 \equiv 0 \pmod{7}.$$

Vi har:

$$3^2 - 4 \cdot 5 \cdot 3 = 9 - 60 = -51$$

og

$$-51 \equiv 5 \pmod{7}.$$

Ut ifra Eksempel 5.2.14 er 5 ikke en kvadratisk rest modulo 7. Da fastslår Korollar 5.2.30 (A) at kongruensen

$$5x^2 + 3x + 3 \equiv 0 \pmod{7}$$

har ingen løsning.

Eksempel 5.2.33. La oss se på kongruensen

$$6x^2 + 2x + 5 \equiv 0 \pmod{11}.$$

Vi har:

$$2^2 - 4 \cdot 6 \cdot 5 = 4 - 120 = -116$$

og

$$-116 \equiv 5 \pmod{11}.$$

Vi har: $y = 4$ er en løsning til kongruensen

$$y^2 \equiv 5 \pmod{11}.$$

Vi har: $x = 2$ er en løsning til kongruensen

$$12x \equiv 2 \pmod{11},$$

altså til kongruensen

$$(2 \cdot 6)x \equiv 4 - 2 \pmod{11}.$$

I tillegg har vi: $x = 5$ er en løsning til kongruensen

$$12x \equiv -6 \pmod{11},$$

altså til kongruensen

$$(2 \cdot 6)x \equiv -4 - 2 \pmod{11}.$$

Da fastslår Korollar 5.1.12 at $x = 2$ og $x = 5$ er løsninger til kongruensen

$$6x^2 + 2x + 5 \equiv 0 \pmod{11}$$

som ikke er kongruent modulo 11 til hverandre.

Siden det ikke er sant at

$$5 \equiv 0 \mod 11,$$

fastslår Korollar 5.2.30 (C) at enhver annen løsning til kongruensen

$$6x^2 + 2x + 5 \equiv 0 \pmod{11}$$

er kongruent modulo 11 til én av disse to.

Merknad 5.2.34. La oss oppsummere. La p være et primtall slik at $p > 2$. Korollar 5.2.30 fastslår at diskriminanten avgjør hvor mange løsninger en kvadratisk kongruens modulo p har, akkurat som diskriminanten avgjør hvor mange løsninger en kvadratisk ligning her. Det vil si følgende.

(A) Dersom diskriminanten ikke er en kvadratisk rest modulo p, har kongruensen ingen løsning. Med andre ord, dersom diskriminanten ikke har en «kvadratrot» modulo p, har kongruensen ingen løsning.

(B) Dersom diskriminanten er 0, finnes det akkurat én løsning til kongruensen fra synspunktet av aritmetikk modulo p, altså enhver annen løsning er kongruent modulo p til denne løsningen.

(C) Dersom diskriminanten har en kvadratisk rest og ikke er 0, finnes det akkurat to løsninger til kongruensen fra synspunktet av aritmetikk modulo p, altså disse to løsningenen ikke er kongruent til hverandre modulo p, og enhver annen løsning er kongruent modulo p til én av disse to.

I tillegg fastslår Proposisjon 5.1.9 og Korollar 5.1.12 at, i tilfeller (B) og (C), *finnes* løsningene på en tilsvarende måte som løsningene til en kvadratisk ligning finnes når diskriminanten er 0, og når diskriminanten er større enn 0.

5.3 Eulers kriterium

Merknad 5.3.1. Følgende proposisjon er kjernen til teorien for kvadratiske rester. Kanskje ser beviset ikke så vanskelig ut, men la merke til at det bygger på Proposisjon **??**, det vil si at det finnes en primitiv rot modulo et hvilket som helst primtall. Vi måtte jobbe ganske harde å bevise at dette er sant. Beviset bygger også på Fermats lille teorem.

Proposisjon 5.3.2. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at $p \mid a$. Da er a en kvadratisk rest modulo p hvis og bare hvis

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

Bevis. Anta først at a er en kvadratisk rest modulo p. Da er det et heltall x slik at

$$x^2 \equiv a \pmod{p}.$$

Da er

$$a^{\frac{p-1}{2}} \equiv \left(x^2\right)^{\frac{p-1}{2}} = x^{2\left(\frac{p-1}{2}\right)} = x^{p-1} \pmod{p}.$$

Ut ifra Korollar 4.10.8 er

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

Dermed er

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

Anta istedenfor at

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

Ut ifra Proposisjon **??** finnes det en primitiv rot modulo p. La oss betegne denne primitive roten som x. Ut ifra Proposisjon 4.13.6 finnes det et heltall t slik at $1 \leq t \leq p-1$ og

$$x^t \equiv a \pmod{p}.$$

Da er

$$\left(x^t\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p},$$

altså

$$x^{t\left(\frac{p-1}{2}\right)} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Siden

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

følger det at

$$x^{t\left(\frac{p-1}{2}\right)} \equiv 1 \pmod{p}.$$

Ut ifra Proposisjon 4.12.10 har vi da: $\mathsf{ord}_p(x) \mid t\left(\frac{p-1}{2}\right)$. Siden x er en primitiv rot modulo p, er $\mathsf{ord}_p(x) = p-1$. Da har vi: $p-1 \mid t\left(\frac{p-1}{2}\right)$. Dermed finnes det et heltall k slik at

$$t\left(\frac{p-1}{2}\right) = k \cdot (p-1).$$

Da er

$$t(p-1) = 2k \cdot (p-1).$$

Det følger fra Proposisjon 2.2.25 at $t = 2k$.

Vi har:

$$\left(x^k\right)^2 = x^{2k} = x^t \equiv a \pmod{p},$$

altså

$$\left(x^k\right)^2 \equiv a \pmod{p}.$$

Med andre ord er $y = x^k$ en løsning til kongruensen

$$y^2 \equiv a \pmod{p}.$$

Dermed er a en kvadratisk rot modulo p.

□

Terminologi 5.3.3. Proposisjon 5.3.2 kalles *Eulers kriterium*.

Eksempel 5.3.4. Ut ifra Eksempel 5.2.15 er 5 en kvadratisk rest modulo 11. Proposisjon 5.3.2 fastslår at

$$5^{\frac{11-1}{2}} \equiv 1 \pmod{11},$$

altså at

$$5^5 \equiv 1 \pmod{11}.$$

Vi har:

$$5^5 = \left(5^2\right)^2 \cdot 5 = 25^2 \cdot 5 \equiv 3^2 \cdot 5 = 9 \cdot 5 = 45 \equiv 1 \pmod{11}.$$

Dermed er det riktignok sant at

$$5^5 \equiv 1 \pmod{11}.$$

Eksempel 5.3.5. Ut ifra Eksempel 5.2.13 er 3 ikke en kvadratisk rest modulo 5. Proposisjon 5.3.2 fastslår at det ikke er sant at

$$3^{\frac{5-1}{2}} \equiv 1 \pmod{5},$$

altså at det ikke er sant at

$$3^2 \equiv 1 \pmod{5}.$$

Vi har: $3^2 = 9$ og

$$9 \equiv 4 \pmod{5}.$$

Siden det ikke er sant at

$$4 \equiv 1 \pmod{5},$$

er det riktignok ikke sant at

$$3^2 \equiv 1 \pmod{5}.$$

Eksempel 5.3.6. Proposisjon 5.3.2 fastslår at 3 er en kvadratisk rest modulo 31 hvis og bare hvis

$$3^{\frac{31-1}{2}} \equiv 1 \pmod{31},$$

altså hvis og bare hvis

$$3^{15} \equiv 1 \pmod{31}.$$

Vi har:

$$3^3 = 27 \equiv -4 \pmod{31}.$$

Da er

$$\begin{aligned} 3^{15} &= 3^9 \cdot 3^6 \\ &= \left(3^3\right)^3 \cdot \left(3^3\right)^2 \\ &\equiv (-4)^3 \cdot (-4)^2 \\ &= (-64) \cdot 16 \\ &\equiv (-2) \cdot 16 \\ &= -32 \\ &\equiv -1 \pmod{31}, \end{aligned}$$

altså

$$3^{15} \equiv -1 \pmod{31}.$$

Vi konkluderer at 3 ikke er en kvadratisk rest modulo 31.

Eksempel 5.3.7. Proposisjon 5.3.2 fastslår at -5 er en kvadratisk rest modulo 127 hvis og bare hvis

$$(-5)^{\frac{127-1}{2}} \equiv 1 \pmod{127},$$

altså hvis og bare hvis

$$(-5)^{63} \equiv 1 \pmod{127}.$$

Vi har:

$$\begin{aligned} (-5)^{63} &= -\left(5^3\right)^{21} \\ &= -(125)^{21} \\ &\equiv -(-2)^{21} \\ &= -\left((-2)^7\right)^3 \\ &= -(-128)^3 \\ &\equiv -(-1)^3 = -(-1) \\ &= 1 \pmod{127}, \end{aligned}$$

altså

$$(-5)^{63} \equiv 1 \pmod{127}.$$

Vi konkluderer at 5 er en kvadratisk rest modulo 127.

Merknad 5.3.8. De siste to eksemplene viser at Proposisjon 5.3.2 er en kraftig verktøy for å bestemme om et heltall er eller ikke er en kvadratisk rest modulo et primtall. Argumentet i Eksempel 5.3.6 er å foretrekke fremfor å vise at det ikke er sant at

$$x^2 \equiv 3 \pmod{31}$$

for hvert av de naturlige tallene 1, 2, ..., 30. Argumentet i Eksempel 5.3.7 er å foretrekke fremfor å gå gjennom alle de naturlige tallene 1, 2, ..., 126 til vi finner ett som er kongruent til 5 når vi opphøyer det i andre potens.

Derimot måtte vi være litt kreative for å regne ut 3^{15} modulo 31 og $(-5)^{63}$ modulo 127 i disse to eksemplene. Det er ikke alltid lett å fullføre slike utregninger.

Imidlertid kan vi gå videre. Vi kommer til å se at vi kan bygge på Proposisjon 5.3.2 for å komme fram til en metode for å bestemme om et heltall er eller ikke er en kvadratisk rest modulo et primtall, uten å regne ut i det hele tatt.

Først kommer vi til å gi et annet eksempel, litt mer teoretisk, på hvordan Proposisjon 5.3.2 kan benyttes i praksis. Vi må gjøre noen forberedelser.

Merknad 5.3.9. Følgende proposisjon er veldig enkel. Likevel er den svært nyttig: vi kommer til å benytte den ofte i dette kapittelet.

Proposisjon 5.3.10. La n være et naturlig tall slik at $n > 2$. La a være 1 eller -1. La b være 1 eller -1. Da er

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

hvis og bare hvis $a = b$.

Bevis. Ett av følgende utsagn er sant:

(A) $a = 1$ og $b = 1$;

(B) $a = 1$ og $b = -1$;

(C) $a = -1$ og $b = 1$;

(D) $a = -1$ og $b = -1$.

Anta først at (B) er sant. Hvis

$$1 \equiv -1 \pmod{n},$$

er

$$2 \equiv 0 \pmod{n}.$$

Da har vi: $n \mid 2$. Ut ifra Proposisjon 2.5.30 er da $n \leq 2$. Imidlertid har vi antatt at $n > 2$. Siden antakelsen at (B) er sant fører til denne motsigelsen, konkluderer vi at (B) ikke er sant.

Anta nå at (C) er sant. Hvis

$$-1 \equiv 1 \pmod{n},$$

er

$$-2 \equiv 0 \pmod{n}.$$

Da har vi: $n \mid -2$. Det følger fra Proposisjon 2.5.12 at vi da har: $n \mid 2$. Ut ifra Proposisjon 2.5.30 er da $n \leq 2$. Imidlertid har vi antatt at $n > 2$. Siden antakelsen at (C) er sant fører til denne motsigelsen, konkluderer vi at (C) ikke er sant.

Således har vi bevist at

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

hvis og bare hvis enten (A) eller (B) sant, altså hvis og bare hvis $a = b$.

□

Lemma 5.3.11. La p være et primtall slik at $p > 2$. Da er følgende sanne:

(1) $x = 1$ og $x = -1$ er løsninger til kongruensen

$$x^2 \equiv 1 \pmod{p};$$

(2) det ikke er sant at

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

(3) enhver annen løsning til kongruensen

$$x^2 \equiv 1 \pmod{p}$$

er kongruent modulo p til enten 1 eller -1;

Bevis. Siden $1^2 = 1$ og $(-1)^2 = 1$, er (1) sant. Ut ifra Proposisjon 5.3.10 er (2) sant. Siden (1) og (2) er sanne, følger det fra Proposisjon 4.14.11 (II) at (3) er sant. □

Korollar 5.3.12. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at $p \mid a$. Da er a ikke er en kvadratisk rest modulo p hvis og bare hvis

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

Bevis. Vi gjør følgende observasjoner.

(1) Vi har:

$$\left(a^{\frac{p-1}{2}}\right)^2 = a^{2\cdot\left(\frac{p-1}{2}\right)} = a^{p-1}.$$

Ut ifra Korollar 4.10.8, er

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

Dermed er

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}.$$

Da følger fra Lemma 5.3.11 at enten

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

eller

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

(2) Ut ifra Proposisjon 5.3.2 er a ikke en kvadratisk rest modulo p hvis og bare hvis det ikke er sant at

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

Det følger fra (1) og (2) at a ikke er en kvadratisk rest modulo p hvis og bare hvis

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

□

Eksempel 5.3.13. Ut ifra Eksempel 5.2.15 er 6 ikke en kvadratisk rest modulo 11. Da fastslår Korollar 5.3.12 at

$$6^{\frac{11-1}{2}} \equiv -1 \pmod{11},$$

altså

$$6^5 \equiv -1 \pmod{11}.$$

Dette er riktignok sant:

$$6^5 = \left(6^2\right)^2 \cdot 6 = 36^2 \cdot 6 \equiv 3^2 \cdot 6 = 54 \equiv -1 \pmod{11}.$$

Eksempel 5.3.14. Korollar 5.3.12 fastslår at 10 ikke er en kvadratisk rest modulo 23 hvis og bare hvis

$$10^{\frac{23-1}{2}} \equiv -1 \pmod{23},$$

altså hvis og bare hvis

$$10^{11} \equiv -1 \pmod{23}.$$

Vi har:

$$10^4 = \left(10^2\right)^2 = 100^2 \equiv 8^2 = 64 \equiv -5 \pmod{23}.$$

I tillegg har vi:

$$10^3 = 10^2 \cdot 10 \equiv 8 \cdot 10 = 80 \equiv 11 \pmod{23}.$$

Dermed er

$$10^{11} = \left(10^4\right)^2 \cdot 10^3 \equiv (-5)^2 \cdot 11 = 25 \cdot 11 \equiv 2 \cdot 11 = 22 \equiv -1 \pmod{23}.$$

Vi konkluderer at 10 ikke er en kvadratisk rest modulo 23.

Proposisjon 5.3.15. La p være et primtall slik at $p > 2$. Da er -1 en kvadratisk rest modulo p hvis og bare hvis

$$p \equiv 1 \pmod{4}.$$

Bevis. Ut ifra Proposisjon 3.2.1 er ett av følgende utsagn sant.

(A) $p \equiv 0 \pmod{4}$;

(B) $p \equiv 1 \pmod{4}$;

(C) $p \equiv 2 \pmod{4}$;

(D) $p \equiv 3 \pmod 4$.

Anta først at (A) er sant. Da har vi: $4 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Dermed er $p = 4$. Imidlertid er 4 ikke et primtall. Siden antakelsen at (A) er sant fører til denne motsigelsen, konkluderer vi at (A) ikke er sant.

Anta nå at (C) er sant. Siden $2 \mid 2$ og $2 \mid 4$, følger det da fra Proposisjon 3.2.54 at

$$p \equiv 0 \pmod 2.$$

Derfor har vi: $2 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Dermed er $p = 2$. Imidlertid har vi antatt at $p > 2$. Siden antakelsen at (C) er sant fører til denne motsigelsen, konkluderer vi at (C) ikke er sant.

Anta nå at (D) er sant. Hvis

$$p \equiv 3 \pmod 4,$$

har vi: $4 \mid p - 3$. Dermed finnes det et heltall k slik at $p - 3 = 4k$, altså slik at $\frac{p-3}{2} = 2k$. Da er

$$\begin{aligned}
(-1)^{\frac{p-1}{2}} &= (-1)^{\frac{p-3}{2}+1} \\
&= (-1)^{\frac{p-3}{2}} \cdot (-1)^1 \\
&= (-1)^{2k} \cdot (-1) \\
&= \left((-1)^2\right)^k \cdot (-1) \\
&= 1^k \cdot (-1) \\
&= 1 \cdot (-1) \\
&= -1.
\end{aligned}$$

Siden $p > 2$ og $-1 \neq 1$, følger det fra Proposisjon 5.3.10 at det ikke er sant at

$$-1 \equiv 1 \pmod p.$$

Dermed er det ikke sant at

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Det følger fra Proposisjon 5.3.2 at -1 ikke er en kvadratisk rest modulo p.

Anta nå at (B) er sant. Hvis

$$p \equiv 1 \pmod 4,$$

har vi: $4 \mid p - 1$. Dermed finnes det et heltall k slik at $p - 1 = 4k$, altså slik at $\frac{p-1}{2} = 2k$. Da er

$$\begin{aligned}
(-1)^{\frac{p-1}{2}} &= (-1)^{2k} \\
&= \left((-1)^2\right)^k \\
&= 1^k \\
&= 1.
\end{aligned}$$

Det følger fra Proposisjon 5.3.2 at 1 er en kvadratisk rest modulo p.

□

Eksempel 5.3.16. Vi har:

$$7 \equiv 3 \pmod 4.$$

Dermed er det ikke sant at

$$7 \equiv 1 \pmod 4.$$

Da fastslår Proposisjon 5.3.15 at -1 ikke er en kvadratisk rest modulo 7. Dette er riktignok sant: hvis -1 hadde vært en kvadratisk rest, hadde så, ut ifra Proposisjon 5.2.5, 6 vært en kvadratisk rest, og fra Eksempel 5.2.14 vet vi at dette ikke er tilfellet.

Eksempel 5.3.17. Vi har:

$$13 \equiv 1 \pmod 4.$$

Da fastslår Proposisjon 5.3.15 at -1 er en kvadratisk rest modulo 13. Dette er riktignok sant:

$$5^2 = 25 \equiv -1 \pmod{13}.$$

Proposisjon 5.3.18. La n være et naturlig tall. Da finnes det et primtall p slik at $p > n$ og

$$p \equiv 1 \pmod 4.$$

Bevis. La q være produktet av alle primtallene som er mindre enn eller like n, og som er kongruent til 1 modulo 4. Ut ifra Teorem 4.3.3, finnes det et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at

$$(2q)^2 + 1 = p_1 \cdots p_t.$$

Anta at

$$p_1 \equiv 0 \pmod 2.$$

Da er

$$p_1 \cdots p_t \equiv 0 \cdot (p_2 \cdots p_t) \pmod 2,$$

altså

$$(2q)^2 + 1 \equiv 0 \pmod 2.$$

Siden $2 \mid (2q)^2$, er imidlertid

$$(2q)^2 + 1 \equiv 1 \pmod 2.$$

Ut ifra Proposisjon 3.2.11 kan det ikke være sant at både

$$(2q)^2 + 1 \equiv 0 \pmod 2$$

og

$$(2q)^2 + 1 \equiv 1 \pmod 2.$$

Siden antakelsen at

$$p_1 \equiv 0 \pmod 2$$

fører til denne motsigelsen, konkluderer vi at det ikke er sant at

$$p_1 \equiv 0 \pmod 2.$$

Vi konkluderer at $p_1 > 2$.

Siden

$$(2q)^2 + 1 = (p_2 \cdots p_t)\, p_1,$$

har vi: $p_1 \mid (2q)^2 + 1$. Dermed er

$$(2q)^2 \equiv -1 \pmod{p_1},$$

altså -1 er en kvadratisk rest modulo p_1. Siden p_1 er et primtall og $p > 2$, følger det fra Proposisjon 5.3.15 at

$$p_1 \equiv 1 \pmod{4}.$$

Anta at $p_1 \leq n$. Vi gjør følgende observasjoner.

(1) Ut ifra definisjonen til q, følger det da at $p_1 \mid q$. Fra Korollar 2.5.18 har vi da: $p_1 \mid q \cdot (-4q)$, altså $p_1 \mid -(2q)^2$.

(2) Siden vi i tillegg vet at $p_1 \mid (2q)^2 + 1$, følger det fra (1) og Proposisjon 2.5.24 at $p_1 \mid \big((2q)^2 + 1\big) + \big(-(2q)^2\big)$, altså at $p_1 \mid 1$.

Det kan ikke være sant at både $p_1 \mid 1$ og $p_1 > 2$. Siden antakelsen at $p_1 \leq n$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $p_1 \leq n$. Derfor er $p_1 > n$.

□

Merknad 5.3.19. Med andre ord fastslår Proposisjon 5.3.18 at det finnes uendelig mange primtall som er kongruent til 1 modulo 4. Sammenlign med Teorem 4.4.2, Proposisjon 4.4.9, og Oppgave O4.1.3.

Merknad 5.3.20. Det er ikke noe spesielt med p_1 i beviset for Proposisjon 5.3.18. Det samme argumentet viser at $p_i > n$ for alle primtallene p_1, p_2, …, p_t som dukker opp i primtallsfaktorisingen til $(2q)^2 + 1$ i beviset.

Eksempel 5.3.21. La oss gå gjennom beviset for Proposisjon 5.3.18 når $n = 30$. Det finnes fire primtall som er mindre enn eller likt 30 og som er kongruent til 1 modulo 4, nemlig 5, 13, 17, og 29. La q være produktet av disse primtallene, altså

$$q = 5 \cdot 13 \cdot 17 \cdot 29.$$

Da er $(2q)^2 + 1$ likt 4107528101. Beviset for Proposisjon 5.3.18 fastslår at hvert primtall i en primtallsfaktorisering av $(2q)^2 + 1$, altså av 4107528101, er større enn 30. Vi har:

$$4107528101 = 37 \cdot 173 \cdot 641701,$$

og både 37, 173, og 641701 er primtall. Med andre ord, er primtallet p_1 i beviset for Proposisjon 5.3.18 likt 37 i dette tilfellet: det er riktignok sant at $37 > 30$.

Merknad 5.3.22. Kanskje ser beviset for Proposisjon 5.3.18 lettere ut enn beviset for Proposisjon 4.4.9. Imidlertid er dette villedende: beviset for Proposisjon 5.3.18 bygger på Proposisjon 5.3.2, som er et ganske dypt resultat.

5.4 Legendresymbolet

Definisjon 5.4.1. La p være et primtall slik at $p > 2$. La a være et heltall. *Legendresymbolet* til a og p er: 1 dersom a er en kvadratisk rest modulo p; 0 dersom $a \equiv 0 \pmod{p}$; og -1 ellers.

Notasjon 5.4.2. La p være et primtall slik at $p > 2$. La a være et heltall. Vi betegner Legendresymbolet til a og p som $\mathbb{L}_p^a$.

Merknad 5.4.3. La p være et primtall slik at $p > 2$. La a være et heltall. Ved å benytte Notasjon 5.4.2, har vi:

$$\mathbb{L}_p^a = \begin{cases} 1 & \text{dersom } a \text{ er en kvadratisk rest til } p, \\ 0 & \text{dersom } a \equiv 0 \pmod{p}, \\ -1 & \text{ellers.} \end{cases}$$

Merknad 5.4.4. Legendresymbolet til a og p betegnes typisk (a/p), $\left(\frac{a}{p}\right)$, eller $(a \mid p)$. Imidlertid har det ingenting å gjøre med brøk, og ingenting å gjøre med delbarhet med p. For å unngå forvirring, skal vi derfor følge Notasjon 5.4.2.

Eksempel 5.4.5. Fra Eksempel 5.2.12 har vi følgende.

a	$\mathbb{L}_3^a$
0	0
1	1
2	-1

Eksempel 5.4.6. Fra Eksempel 5.2.13 har vi følgende.

a	$\mathbb{L}_5^a$
0	0
1	1
2	-1
3	-1
4	1

Eksempel 5.4.7. Fra Eksempel 5.2.14 har vi følgende.

a	$\mathbb{L}_7^a$
0	0
1	1
2	1
3	-1
4	1
5	-1
6	-1

Eksempel 5.4.8. Fra Eksempel 5.2.15 har vi følgende.

a	$\mathbb{L}_{11}^a$
0	0
1	1
2	-1
3	1
4	1
5	1
6	-1
7	-1
8	-1
9	1
10	-1

5.5 Grunnleggende proposisjoner om Legendresymbolet

Merknad 5.5.1. I denne delen av kapittelet kommer til å bevise en rekke proposisjoner som gir oss muligheten til å regne ut Legendresymboler, og dermed å sjekke om kvadratiske kongruenser har eller ikke har løsninger.

Proposisjon 5.5.2. La p være et primtall slik at $p > 2$. Da er $\mathbb{L}_p^1 = 1$.

Bevis. Siden $x = 1$ er en løsning til kongruensen

$$x^2 \equiv 1 \pmod{p},$$

er 1 e kvadratisk rest modulo p. Dermed er $\mathbb{L}_p^1 = 1$. □

Proposisjon 5.5.3. La p være et primtall slik at $p > 2$. La a og b være heltall slik at

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

Da er $\mathbb{L}_p^a = \mathbb{L}_p^b$.

Bevis. La x være et heltall. Dersom

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

er

$$a \equiv 0 \pmod{p}$$

hvis ogh bare hvis

$$b \equiv 0 \pmod{p}.$$

Derfor er $\mathbb{L}_p^a = 0$ om og bare om $\mathbb{L}_p^b = 0$. Anta at det ikke er sant at $\mathbb{L}_p^a = 0$. Vi har:

$$x^2 \equiv a \pmod{p}$$

om og bare om

$$x^2 \equiv b \pmod{p}.$$

Dermed er a en kvadratisk rest modulo p om og bare om b er en kvadratisk rest modulo p. Således er $\mathbb{L}_p^a = 1$ om og bare om $\mathbb{L}_p^b = 1$, og er $\mathbb{L}_p^a = -1$ om og bare om $\mathbb{L}_p^b = 1$. □

Eksempel 5.5.4. Vi har:

$$10 \equiv 3 \pmod{7}.$$

Ut ifra Eksempel 5.4.7, er $\mathbb{L}_7^3 = -1$. Da fastslår Proposisjon 5.5.3 at $\mathbb{L}_7^{10} = -1$. Dermed er 10 ikke en kvadratisk rest modulo 7.

Eksempel 5.5.5. Vi har:

$$-6 \equiv 5 \pmod{11}.$$

Ut ifra Eksempel 5.4.8, er $\mathbb{L}_{11}^5 = 1$. Da fastslår Proposisjon 5.5.3 at $\mathbb{L}_{11}^{-6} = 1$. Dermed er -6 en kvadratisk rest modulo 11.

Proposisjon 5.5.6. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da er $\mathbb{L}_p^{a^2} = 1$.

Bevis. Siden $x = a$ er en løsning til kongruensen

$$x^2 \equiv a^2 \pmod{p},$$

er a^2 en kvadratisk rest modulo p. Dermed er $\mathbb{L}_p^{a^2} = 1$.

□

Eksempel 5.5.7. Siden $5^2 = 25$, fastslår Proposisjon 5.5.3 at $\mathbb{L}_{17}^{25} = 1$. Siden

$$25 \equiv 8 \pmod{17},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{17}^8 = 1$. Dermed er 8 en kvadratisk rest modulo 17.

Eksempel 5.5.8. Siden $7^2 = 49$, fastslår Proposisjon 5.5.3 at $\mathbb{L}_{31}^{49} = 1$. Siden

$$49 \equiv 18 \pmod{31},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{31}^{18} = 1$. Dermed er 18 en kvadratisk rest modulo 31.

Proposisjon 5.5.9. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da er

$$\mathbb{L}_p^a \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Bevis. Anta først at a er en kvadratisk rest modulo p. Vi gjør følgende observasjoner.

(1) Da er $\mathbb{L}_p^a = 1$.

(2) Ut ifra Proposisjon 5.3.2 er da

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

altså

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

Det følger fra (1) og (2) at

$$\mathbb{L}_p^a \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Anta nå at a ikke er en kvadratisk rest modulo p. Vi gjør følgende observasjoner.

(1) Da er $\mathbb{L}_p^a = -1$.

(2) Ut ifra Korollar 5.3.12 er da

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

altså

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

Det følger fra (1) og (2) at

$$\mathbb{L}_p^a \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

□

Eksempel 5.5.10. Proposisjon 5.5.9 fastslår at

$$\mathbb{L}_7^5 \equiv 5^{\frac{7-1}{2}} \pmod{7},$$

altså at

$$\mathbb{L}_7^5 \equiv 5^3 \pmod{7}.$$

Vi har:

$$5^3 \equiv 5^2 \cdot 5 \equiv 4 \cdot 5 = 20 \equiv -1 \pmod{7}.$$

Ut ifra Eksempel 5.4.6 er det riktignok sant at $\mathbb{L}_7^5 = -1$.

Eksempel 5.5.11. Proposisjon 5.5.9 fastslår at

$$\mathbb{L}_{11}^{14} \equiv 14^{\frac{11-1}{2}} \pmod{11},$$

altså at

$$\mathbb{L}_{11}^{14} \equiv 14^5 \pmod{11}.$$

Vi gjør følgende observasjoner.

(1) Vi har:

$$14^5 \equiv 3^5 = 3^3 \cdot 3^2 = 27 \cdot 9 \equiv 5 \cdot 9 = 45 \equiv 1 \pmod{11}.$$

(2) Ut ifra Proposisjon 5.5.3 er $\mathbb{L}_{11}^{14} = \mathbb{L}_{11}^{3}$. Ut ifra Eksempel 5.4.8 er $\mathbb{L}_{11}^{3} = 1$.

Dermed er det riktignok sant at

$$\mathbb{L}_{11}^{14} \equiv 14^5 \pmod{11}.$$

Merknad 5.5.12. La p være et primtall slik at $p > 2$. La a være et heltall. Legendresymbolet $\mathbb{L}_p^a$ noterer om a er eller ikke er en kvadratisk rest modulo p. Hvorfor valgte vi 1 og -1 for å gjøre dette, og ikke et hvilket som helst annet par heltall?

Svaret er: fordi dette er det eneste valget slik at Proposisjon 5.5.9 er sann! Proposisjon 5.3.2 er dyp og viktig, og Proposisjon 5.5.9 gir oss muligheten til å benytte oss av Proposisjon 5.3.2 når vi manipulerer Legendresymboler. Vi kommer til snart til å se at dette er svært nyttig i praksis. I tillegg er det uunnværlig fra et teoretisk synspunkt for å kunne gi et bevis for Teorem 5.8.30, og for å kunne gi et bevis for følgende to proposisjoner, som vi kommer til å benytte oss hele tida når vi regner ut Legendresymboler.

Proposisjon 5.5.13. La p være et primtall slik at $p > 2$. La a og b være heltall. Da er

$$\mathbb{L}_p^{ab} = \mathbb{L}_p^a \cdot \mathbb{L}_p^b.$$

Bevis. Anta først at

$$a \equiv 0 \pmod{p}.$$

Da er

$$\mathbb{L}_p^{ab} = \mathbb{L}_p^{0 \cdot b} = \mathbb{L}_p^0 = 0.$$

I tillegg er

$$\mathbb{L}_p^a \cdot \mathbb{L}_p^b = \mathbb{L}_p^0 \cdot \mathbb{L}_p^b = 0 \cdot \mathbb{L}_p^b = 0.$$

Dermed er

$$\mathbb{L}_p^{ab} = \mathbb{L}_p^a \cdot \mathbb{L}_p^b.$$

Et lignende argument viser at, dersom

$$b \equiv 0 \pmod{p},$$

er både $\mathbb{L}_p^{ab}$ og $\mathbb{L}_p^a \cdot \mathbb{L}_p^b$ like 0, og derfor er

$$\mathbb{L}_p^{ab} = \mathbb{L}_p^a \cdot \mathbb{L}_p^b.$$

Anta nå at det ikke er sant at

$$a \equiv 0 \pmod{p},$$

og at det ikke er sant at

$$b \equiv 0 \pmod{p}.$$

Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_p^a \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

(2) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_p^b \equiv b^{\frac{p-1}{2}} \pmod{p}.$$

(3) Det følger fra (1) og (2) at

$$\mathbb{L}_p^a \cdot \mathbb{L}_p^b \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \pmod{p}.$$

Siden

$$a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}},$$

er dermed

$$\mathbb{L}_p^a \cdot \mathbb{L}_p^b \equiv (ab)^{\frac{p-1}{2}} \pmod{p},$$

altså

$$(ab)^{\frac{p-1}{2}} \equiv \mathbb{L}_p^a \cdot \mathbb{L}_p^b \pmod{p}.$$

(4) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_p^{ab} \equiv (ab)^{\frac{p-1}{2}} \pmod{p}.$$

Det følger fra (3) og (4) at

$$\mathbb{L}_p^{ab} \equiv \mathbb{L}_p^a \cdot \mathbb{L}_p^b \pmod{p}.$$

Siden $\mathbb{L}_p^a$ er likt 1 eller -1, og $\mathbb{L}_p^a \cdot \mathbb{L}_p^b$ er likt 1 eller -1, følger det fra Proposisjon 5.3.10 at $\mathbb{L}_p^{ab} = \mathbb{L}_p^a \cdot \mathbb{L}_p^b$.

□

Eksempel 5.5.14. Ut ifra Eksempel 5.4.6 er $\mathbb{L}_5^3 = -1$ og $\mathbb{L}_5^4 = 1$. Proposisjon 5.5.13 fastslår at

$$\mathbb{L}_5^{3\dot{4}} = \mathbb{L}_5^3 \cdot \mathbb{L}_5^4 = (-1) \cdot 1 = -1,$$

altså at $\mathbb{L}_5^{12} = -1$. Dette er riktignok sant: ut ifra Proposisjon 5.5.3 er $\mathbb{L}_5^{12} = \mathbb{L}_5^2$, og ut ifra Eksempel 5.4.6 er $\mathbb{L}_5^2 = -1$.

Eksempel 5.5.15. Ut ifra Eksempel 5.4.8 er $\mathbb{L}_{11}^2 = -1$ og $\mathbb{L}_{11}^7 = -1$. Proposisjon 5.5.13 fastslår at

$$\mathbb{L}_{11}^{2\dot{7}} = \mathbb{L}_{11}^2 \cdot \mathbb{L}_{11}^7 = (-1) \cdot (-1) = 1,$$

altså at $\mathbb{L}_{11}^{114} = 1$. Dette er riktignok sant: ut ifra Proposisjon 5.5.3 er $\mathbb{L}_{11}^{14} = \mathbb{L}_{11}^3$, og ut ifra Eksempel 5.4.8 er $\mathbb{L}_{11}^3 = 1$.

Proposisjon 5.5.16. La p være et primtall slik at $p > 2$. Da er

$$\mathbb{L}_p^{-1} = (-1)^{\frac{p-1}{2}}.$$

Bevis. Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_p^{-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Siden $\mathbb{L}_p^{-1}$ er likt enten 1 eller -1, og $(-1)^{\frac{p-1}{2}}$ er likt enten 1 eller -1, følger det fra Proposisjon 5.3.10 at

$$\mathbb{L}_p^{-1} = (-1)^{\frac{p-1}{2}}.$$

□

Eksempel 5.5.17. Proposisjon 5.5.16 fastslår at

$$\mathbb{L}_5^{-1} = (-1)^{\frac{5-1}{2}} = (-1)^2 = 1.$$

Dette er riktignok sant: ut ifra Proposisjon 5.5.3 er $\mathbb{L}_5^{-1} = \mathbb{L}_5^4$, og ut ifra Eksempel 5.4.6 er $\mathbb{L}_5^4 = 1$.

Eksempel 5.5.18. Proposisjon 5.5.16 fastslår at

$$\mathbb{L}_7^{-1} = (-1)^{\frac{7-1}{2}} = (-1)^3 = -1.$$

Dette er riktignok sant: ut ifra Proposisjon 5.5.3 er $\mathbb{L}_7^{-1} = \mathbb{L}_7^6$, og ut ifra Eksempel 5.4.7 er $\mathbb{L}_7^6 = -1$.

5.6 Eksempler på hvordan regne ut Legendresymboler

Merknad 5.6.1. Proposisjonene den foregående delen av kapittelet gir oss en kraftig metode for å regne ut $\mathbb{L}_p^a$ for et hvilket som helst heltall a og et hvilket som helst primtall p slik at $p > 2$.

(1) Finn en primtallsfaktorisering $p_1 \cdots p_t$ til a. Da fastslår Proposisjon 5.5.13 at

$$\mathbb{L}_p^a = \mathbb{L}_p^{p_1} \ldots \mathbb{L}_p^{p_t}.$$

(2) Regn ut hvert av Legendresymbolene $\mathbb{L}_p^{p_1}$, $\mathbb{L}_p^{p_2}$, …, $\mathbb{L}_p^{p_t}$.

I denne delen av kapittelet kommer vi til å se på noen eksempler på hvordan denne metoden gjennomføres. Dette kan ses som en oppvarming før vi ser på kvadratisk gjensidighet, som kommer til å gi oss muligheten til å gjøre metoden ovenfor fullkommen.

Proposisjon 5.6.2. Heltallet 84 er ikke en kvadratisk rest modulo 23.

Bevis. Vi gjør følgende observasjoner.

(1) Siden

$$84 \equiv 15 \pmod{23},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{23}^{84} = \mathbb{L}_{23}^{15}$.

(2) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{23}^{15} = \mathbb{L}_{23}^{3\cdot 5} = \mathbb{L}_{23}^{3} \cdot \mathbb{L}_{23}^{5}.$$

(3) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_{23}^{3} \equiv 3^{\frac{23-1}{2}} \pmod{23},$$

altså

$$\mathbb{L}_{23}^{3} \equiv 3^{11} \pmod{23}.$$

Vi har:

$$3^{11} = \left(3^3\right)^3 \cdot 3^2 = 27^3 \cdot 9 \equiv 4^3 \cdot 9 = 64 \cdot 9 \equiv (-5) \cdot 9 = -45 \equiv 1 \pmod{23}.$$

Dermed er

$$\mathbb{L}_{23}^{3} \equiv 1 \pmod{23}.$$

Det følger fra Proposisjon 5.3.10 at $\mathbb{L}_{23}^{3} = 1$.

(4) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_{23}^{5} \equiv 5^{\frac{23-1}{2}} \pmod{23},$$

altså

$$\mathbb{L}_{23}^{5} \equiv 5^{11} \pmod{23}.$$

Vi har:

$$5^{11} = \left(5^2\right)^5 \cdot 5 = 25^5 \cdot 5 \equiv 2^5 \cdot 5 = 32 \cdot 5 \equiv 9 \cdot 5 = 45 \equiv -1 \pmod{23}.$$

Dermed er

$$\mathbb{L}_{23}^{5} \equiv -1 \pmod{23}.$$

Det følger fra Proposisjon 5.3.10 at $\mathbb{L}_{23}^{5} = -1$.

Det følger fra (1) – (4) at

$$\mathbb{L}_{23}^{84} = \mathbb{L}_{23}^{15} = \mathbb{L}_{23}^{3} \cdot \mathbb{L}_{23}^{5} = 1 \cdot (-1) = -1.$$

Således er 84 ikke en kvadratisk rest modulo 23.

□

Proposisjon 5.6.3. Heltallet 28 er en kvadratisk rest modulo 59.

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{59}^{28} = \mathbb{L}_{59}^{4\cdot 7} = \mathbb{L}_{59}^{4} \cdot \mathbb{L}_{59}^{7}.$$

(2) Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{59}^4 = 1$.

(3) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_{59}^7 \equiv 7^{\frac{59-1}{2}} \pmod{59},$$

altså

$$\mathbb{L}_{59}^7 \equiv 7^{28} \pmod{59}.$$

Vi har:

$$7^2 = 49 \equiv -10 \pmod{59}.$$

Da er

$$7^3 = 7^2 \cdot 7 \equiv (-10) \cdot 7 = -70 \equiv -11 \pmod{7}.$$

Det følger at

$$7^6 = \left(7^3\right)^2 \equiv (-11)^2 = 121 \equiv 3 \pmod{59}.$$

Da er

$$7^{29} = \left(7^6\right)^4 \cdot 7^3 \cdot 7^2 \equiv 3^4 \cdot (-10) \cdot (-11) = 81 \cdot 110 \equiv 22 \cdot (-8) = -176 \equiv 1 \pmod{59}.$$

Dermed er

$$\mathbb{L}_{59}^7 \equiv 1 \pmod{59}.$$

Det følger fra Proposisjon 5.3.10 at $\mathbb{L}_{59}^7 = 1$.

Det følger fra (1) – (3) at

$$\mathbb{L}_{59}^{28} = \mathbb{L}_{59}^4 \cdot \mathbb{L}_{59}^7 = 1 \cdot 1 = 1.$$

Således er 28 en kvadratisk rest modulo 59.

□

Merknad 5.6.4. Proposisjon 5.6.3 fastslår at kongruensen

$$x^2 \equiv 28 \pmod{59}$$

har en løsning. Imidlertid sier proposisjonen ikke hvordan en løsning kan *finnes*. Dette stemmer generelt sett: Legendresymbolet er utrolig nyttig for å bestemme *om* en kvadratisk kongruens har en løsning, men sier ingenting om *hvordan* en eventuell løsning kan finnes.

Faktisk finnes det en algoritme, *Tonelli-Shanks' algoritme*, for å finne løsningene til en kongruens

$$x^2 \equiv a \pmod{p}.$$

I løpet av å gjennomføre denne algoritmen, regner man ut noen Legendresymboler. Det vil si: Legendresymbolet *kan* også benyttes for å *finne* løsninger til kvadratiske kongruenser.

Mens vi har alt vi trenger for å forstå Tonelli-Shanks' algoritme, kommer vi ikke til å se på den i kurset: da hadde vi fått tid til å se på noen av de fine temaene vi kommer til å se på i resten av kurset. Les imidlertid gjerne om Tonelli-Shanks' algoritme: dette er en fin måte å fordype og konsolidere forståelsen din for teorien i dette kapittelet av forelesningsnotatene.

Proposisjon 5.6.5. Kongruensen

$$-25x^2 + 44x - 37 \equiv 0 \pmod{211}$$

har ingen løsning.

Bevis. Vi har:

$$44^2 - 4 \cdot (-25) \cdot (-27) = 1936 - 3700 = -1764.$$

La oss regne ut $\mathbb{L}_{211}^{-1764}$.

(1) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{211}^{-1764} = \mathbb{L}_{211}^{(-1)\cdot 6^2 \cdot 7^2} = \mathbb{L}_{211}^{-1} \cdot \mathbb{L}_{79}^{6^2} \cdot \mathbb{L}_{79}^{7^2}.$$

(2) Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{211}^{6^2} = 1$.

(3) Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{211}^{7^2} = 1$.

(4) Ut ifra Proposisjon 5.5.16 er

$$\mathbb{L}_{211}^{-1} = (-1)^{\frac{211-1}{2}} = (-1)^{105} = -1.$$

Det følger fra (1) – (4) at

$$\mathbb{L}_{211}^{-1764} = \mathbb{L}_{211}^{-1} \cdot \mathbb{L}_{211}^{6^2} \cdot \mathbb{L}_{211}^{7^2} = (-1) \cdot 1 \cdot 1 = -1.$$

Således er -1764 ikke en kvadratisk rest modulo 211. Ut ifra Korollar 5.2.30, konkluderer vi at kongruensen

$$-25x^2 + 44x - 37 \equiv 0 \pmod{211}$$

har ingen løsning.

□

Proposisjon 5.6.6. Kongruensen

$$x^2 - 8x + 57 \equiv 0 \pmod{79}$$

har to løsninger som ikke er kongruent til hverandre modulo 79, og slik at enhver annen løsning er kongruent modulo 79 til én av disse to.

Bevis. Vi har:

$$(-8)^2 - 4 \cdot 1 \cdot 57 = 64 - 228 = -164.$$

La oss regne ut $\mathbb{L}_{79}^{-164}$.

(1) Siden

$$-164 \equiv -6 \pmod{79},$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}_{79}^{-164} = \mathbb{L}_{79}^{-6}.$$

(2) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{79}^{-6} = \mathbb{L}_{79}^{(-1)\cdot 2\cdot 3} = \mathbb{L}_{79}^{-1} \cdot \mathbb{L}_{79}^{2} \cdot \mathbb{L}_{79}^{3}.$$

(3) Ut ifra Proposisjon 5.5.16 er

$$\mathbb{L}_{79}^{-1} = (-1)^{\frac{79-1}{2}} = (-1)^{39} = -1.$$

(4) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_{79}^{2} \equiv 2^{\frac{79-1}{2}} \pmod{79},$$

altså

$$\mathbb{L}_{79}^{2} \equiv 2^{39} \pmod{79}.$$

Vi har:

$$2^6 = 64 \equiv -15 \pmod{79}.$$

Da er

$$2^{12} = \left(2^6\right)^2 \equiv (-15)^2 = 225 \equiv -12 \pmod{79}.$$

Derfor er

$$2^{24} = \left(2^{12}\right)^2 \equiv (-12)^2 = 144 \equiv -14 \pmod{79}.$$

Da er

$$2^{36} = 2^{12} \cdot 2^{24} \equiv (-12) \cdot (-14) = 168 \equiv 10 \pmod{79}.$$

Vi konkluderer at

$$2^{39} = 2^{36} \cdot 2^3 \equiv 10 \cdot 8 = 80 \equiv 1 \pmod{79}.$$

Dermed er

$$\mathbb{L}_{79}^{2} \equiv 1 \pmod{79}.$$

Det følger fra Proposisjon 5.3.10 at $\mathbb{L}_{79}^{2} = 1$.

(5) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_{79}^{3} \equiv 3^{\frac{79-1}{2}} \pmod{79},$$

altså

$$\mathbb{L}_{79}^{3} \equiv 3^{39} \pmod{79}.$$

Vi har:

$$3^4 = 81 \equiv 2 \pmod{79}.$$

Da er

$$3^{36} = \left(3^4\right)^9 \equiv 2^9 \pmod{79}.$$

Ut ifra (4) er

$$2^6 \equiv -15 \pmod{79}.$$

Da er

$$2^9 = 2^6 \cdot 2^3 \equiv -15 \cdot 8 = -120 \equiv 38 \pmod{79}.$$

Dermed er

$$3^{36} \equiv 38 \pmod{79}.$$

Da er

$$3^{37} = 3^{36} \cdot 3 \equiv 38 \cdot 3 = 114 \equiv 35 \pmod{79}.$$

Det følger at

$$3^{38} = 3^{37} \cdot 3 \equiv 35 \cdot 3 = 105 \equiv 26 \pmod{79}.$$

Vi konkluderer at

$$3^{39} = 3^{38} \cdot 3 \equiv 26 \cdot 3 = 78 \equiv -1 \pmod{79}.$$

Dermed er

$$\mathbb{L}_{79}^3 \equiv -1 \pmod{79}.$$

Det følger fra Proposisjon 5.3.10 at $\mathbb{L}_{79}^3 = -1$.

Det følger fra (1) – (5) at

$$\mathbb{L}_{79}^{-164} = \mathbb{L}_{79}^{-6} = \mathbb{L}_{79}^{-1} \cdot \mathbb{L}_{79}^2 \cdot \mathbb{L}_{79}^3 = (-1) \cdot 1 \cdot (-1) = 1.$$

Dermed er -164 en kvadratisk rest modulo 79. Ut ifra Korollar 5.2.30, konkluderer vi at kongruensen

$$x^2 - 8x + 57 \equiv 0 \pmod{79}$$

har to løsninger som ikke er kongruent til hverandre modulo 79, og slik at enhver annen løsning er kongruent modulo 79 til én av disse to.

□

Merknad 5.6.7. For å understreke Merknad 5.6.4, sier Proposisjon 5.6.6 at det *finnes* to løsninger, men ikke hva disse to løsningene er. Tonelli-Shanks' algoritme, som vi ikke kommer til å se på i kurset, kan benyttes for å finne de to løsningene.

5.7 Det kinesiske restteoremet

Merknad 5.7.1. Målet vart nå er Teorem 5.8.30. I løpet av beviset vårt for dette teoremet, kommer vi til å behøve følgende proposisjon, som er interessant og viktig i seg selv.

Proposisjon 5.7.2. La n_1 og n_2 være heltall. Anta at $n_1 \neq 0$, $n_2 \neq 0$, og $\mathsf{sfd}(n_1, n_2) = 1$. La c_1 og c_2 være heltall. La x_1 være et heltall slik at

$$n_2 x_1 \equiv 1 \pmod{n_1}.$$

La x_2 være et heltall slik at

$$n_1 x_2 \equiv 1 \pmod{n_2}.$$

Følgende er sanne.

(I) Da er

$$x = n_2 x_1 c_1 + n_1 x_2 c_2$$

er en løsning både til kongruensen

$$x \equiv c_1 \pmod{n_1}$$

og til kongruensen

$$x \equiv c_2 \pmod{n_2}.$$

(II) La y og z være heltall slik at $x = y$ er en løsning både til kongruensen

$$x \equiv c_1 \pmod{n_1}$$

og til kongruensen

$$x \equiv c_2 \pmod{n_2},$$

og slik at $x = z$ er også en løsning til begge kongruensene. Da er

$$y \equiv z \pmod{n_1 n_2}.$$

(III) La y og z være heltall slik at

$$y \equiv z \pmod{n_1 n_2},$$

og slik at $x = z$ er en løsning både til kongruensen

$$x \equiv c_1 \pmod{n_1}$$

og til kongruensen

$$x \equiv c_2 \pmod{n_2},$$

Da er y en løsning til begge kongruensene.

Bevis. Vi gjør følgende observasjoner.

(1) Siden

$$n_1 \mid n_1 x_2 c_2,$$

er

$$n_1 x_2 c_2 \equiv 0 \pmod{n_1}.$$

Det følger at

$$n_2 x_1 c_1 + n_1 x_2 c_2 \equiv n_2 x_1 c_1 \pmod{n_1}.$$

(2) Siden

$$n_2 x_1 \equiv 1 \pmod{n_1},$$

er

$$n_2 x_1 c_1 \equiv c_1 \pmod{n_1}.$$

Det følger fra (1) og (2) at

$$n_2x_1c_1 + n_1x_2c_2 \equiv c_1 \pmod{n_1},$$

altså at

$$x = n_2x_1c_1 + n_1x_2c_2$$

er en løsning til kongruensen

$$x \equiv c_1 \pmod{n_1}.$$

Nå gjør vi følgende observasjoner.

(1) Siden $n_2 \mid n_2x_1c_1$, er

$$n_2x_1c_1 \equiv 0 \pmod{n_2}.$$

Det følger at

$$n_2x_1c_1 + n_1x_2c_2 \equiv n_1x_2c_2 \pmod{n_2}.$$

(2) Siden

$$n_1x_2 \equiv 1 \pmod{n_2},$$

er

$$n_1x_2c_2 \equiv c_2 \pmod{n_2}.$$

Det følger fra (1) og (2) at

$$n_2x_1c_1 + n_1x_2c_2 \equiv c_2 \pmod{n_2},$$

altså at

$$x = n_2x_1c_1 + n_1x_2c_2$$

er en løsning til kongruensen

$$x \equiv c_2 \pmod{n_2}.$$

Således har vi bevist at (I) er sant.

Anta nå at y og z være et heltall slik at $x = y$ er en løsning både til kongruensen

$$x \equiv c_1 \pmod{n_1}$$

og til kongruensen

$$x \equiv c_2 \pmod{n_2},$$

og slik at $x = z$ er også en løsning til begge kongruensene. Det vil si at følgende er sanne:

(1) $y \equiv c_1 \pmod{n_1}$;

(2) $y \equiv c_2 \pmod{n_2}$;

(3) $z \equiv c_1 \pmod{n_1}$;

(4) $z \equiv c_2 \pmod{n_2}$;

Da følger fra (1) og (3) at

$$y \equiv z \pmod{n_1}.$$

Det følger fra (2) og (4) at

$$y \equiv z \pmod{n_2}.$$

Ut ifra Proposisjon 4.11.3 er da

$$y \equiv z \pmod{n_1 n_2}$$

Dermed er (II) sant.

Anta istedenfor nå at y og z er heltall slik at

$$y \equiv z \pmod{n_1 n_2},$$

og slik at $x = z$ er en løsning både til kongruensen

$$x \equiv c_1 \pmod{n_1}$$

og til kongruensen

$$x \equiv c_2 \pmod{n_2}.$$

Det vil si:

$$z \equiv c_1 \pmod{n_1}$$

og til kongruensen

$$z \equiv c_2 \pmod{n_2}.$$

Siden

$$y \equiv z \pmod{n_1 n_2},$$

følger det fra Proposisjon 3.2.57 at

$$y \equiv z \pmod{n_1}$$

og at

$$y \equiv z \pmod{n_2}.$$

Dermed er

$$y \equiv c_1 \pmod{n_1}$$

og

$$y \equiv c_2 \pmod{n_2}.$$

Dermed er (III) er sant. □

Eksempel 5.7.3. La oss se på kongruensene

$$x \equiv 4 \pmod{9}$$

og

$$x \equiv 6 \pmod{14}.$$

Vi har: $x = 2$ er en løsning til kongruensen

$$14x \equiv 1 \pmod{9}.$$

I tillegg har vi: $x = 11$ en løsning til kongruensen

$$9x \equiv 1 \pmod{14}.$$

Da fastslår Proposisjon 5.7.2 (I) at

$$x = 14 \cdot 2 \cdot 4 + 9 \cdot 11 \cdot 6,$$

altså $x = 706$, er en løsning både til kongruensen

$$x \equiv 4 \pmod{9}$$

og til kongruensen

$$x \equiv 6 \pmod{14}.$$

Dessuten fastslår Proposisjon 5.7.2 (III) at alle heltallene som er kongruent til 706 modulo $9 \cdot 14$, altså modulo 126, er løsninger til begge kongruensene. Vi har:

$$706 \equiv 76 \pmod{126}.$$

Således er $x = 76 + k126$ en løsning til begge kongruensene for alle heltall k. Proposisjon 5.7.2 (II) fastslår at, dersom $x = z$ er en løsning til begge kongruensene, er

$$z \equiv 76 \pmod{126},$$

altså finnes det et heltall k slik at

$$z = 76 + k126.$$

Merknad 5.7.4. Følgende to proposisjoner viser hvordan Proposisjon 5.7.2 kan benyttes for å svare på konkrete spørsmål om delbarhet.

Proposisjon 5.7.5. Et heltall a gir resten 3 når vi deler med 7, og gir resten 5 når vi deler med 11, om og bare om det finnes et heltall k slik at $a = 38 + 77k$.

Bevis. La a være et heltall slik at

$$a \equiv 3 \pmod{7}$$

og

$$a \equiv 5 \pmod{11}.$$

Vi gjør følgende observasjoner.

(1) Vi har: $x = 2$ er en løsning til kongruensen

$$11x \equiv 1 \pmod{7}.$$

(2) Vi har: $x = 8$ er en løsning til kongruensen

$$7x \equiv 1 \pmod{11}.$$

Ut ifra Proposisjon 5.7.2 (I) er da

$$x = 11 \cdot 2 \cdot 3 + 7 \cdot 8 \cdot 5$$

en løsning både til kongruensen

$$x \equiv 3 \pmod{7}$$

og til kongruensen

$$x \equiv 5 \pmod{11},$$

altså $x = 346$ er en løsning til begge kongruensene.

Vi har:

$$38 \equiv 346 \pmod{7 \cdot 11},$$

altså

$$38 \equiv 346 \pmod{77}.$$

Det følger fra Proposisjon 5.7.2 (III) at $x = 38$ er en løsning både til kongruensen

$$x \equiv 3 \pmod{7}$$

og til kongruensen

$$x \equiv 5 \pmod{11}.$$

Ut ifra Proposisjon 5.7.2 (II) er da

$$a \equiv 38 \pmod{77}.$$

Det følger at $77 \mid a - 38$. Dermed finnes det et heltall k slik at $a - 38 = 77k$, altså slik at $a = 38 + 77k$.

For et hvilket som helst heltall k, er

$$38 + 77k \equiv 38 \pmod{77}.$$

Siden 38 er en løsning både til kongruensen

$$x \equiv 3 \pmod{7}$$

og til kongruensen

$$x \equiv 5 \pmod{11},$$

følger det fra Proposisjon 5.7.2 (III) at $x = 38+77k$ er en løsning til begge kongruensene.

Således har vi bevist at et heltall a er en løsning både til kongruensen

$$a \equiv 3 \pmod{7}$$

og til kongruensen

$$a \equiv 5 \pmod{11}$$

om og bare om det finnes et heltall k slik at $a = 38 + 77k$. Dette er det samme som å si at, for et hvilket som helst heltall a, får vi resten 3 når vi deler a med 7, og får vi resten 5 når vi deler a med 11, om og bare om det finnes et heltall k slik at $a = 38 + 77k$.

□

Merknad 5.7.6. For å komme fram til løsningen $x = 2$ til kongruensen

$$11x \equiv 1 \pmod{7},$$

følger vi oppskriften i Merknad 3.4.49. Det vil si: enten går vi gjennom alle mulighetene $x = 1$, $x = 2$, ..., $x = 6$ og sjekker om vi har en løsning, eller benytter vi Euklids algoritme.

Det samme gjelder hvordan finne løsningen $x = 8$ til kongruensen

$$7x \equiv 1 \pmod{11}.$$

Eksempel 5.7.7. Proposisjon 5.7.5 fastslår at vi får resten 3 når vi deler 38 med 7, og får resten 5 når vi deler 38 med 11. Dette er riktignok sant: $38 = 7 \cdot 5 + 3$, og

$$38 = 3 \cdot 11 + 5.$$

Eksempel 5.7.8. Proposisjon 5.7.5 fastslår at vi får resten 3 når vi deler $38 + 77$, altså 115, med 7, og får resten 5 når vi deler 115 med 11. Dette er riktignok sant: $115 = 16 \cdot 7 + 3$, og

$$115 = 10 \cdot 11 + 5.$$

Eksempel 5.7.9. Proposisjon 5.7.5 fastslår at vi får resten 3 når vi deler $38 - 77$, altså -39, med 7, og får resten 5 når vi deler -39 med 11. Dette er riktignok sant: $-39 = (-6) \cdot 7 + 3$, og

$$-39 = (-4) \cdot 11 + 5.$$

Eksempel 5.7.10. Siden det ikke er sant at

$$59 \equiv 38 \pmod{77},$$

fastslår Proposisjon 5.7.5 at enten får vi ikke resten 3 når vi deler 59 med 7, eller får vi ikke resten 5 når vi deler 59 med 11. Dette er riktignok sant: $59 = 5 \cdot 11 + 4$, altså får vi resten 4 når vi deler 59 med 11.

Eksempel 5.7.11. Siden det ikke er sant at

$$27 \equiv 38 \pmod{77},$$

fastslår Proposisjon 5.7.5 at enten får vi ikke resten 3 når vi deler 27 med 7, eller får vi ikke resten 5 når vi deler 27 med 11. Dette er riktignok sant: $27 = 3 \cdot 7 + 6$, altså får vi resten 6 når vi deler 27 med 11.

Eksempel 5.7.12. Siden det ikke er sant at

$$67 \equiv 38 \pmod{77},$$

fastslår Proposisjon 5.7.5 at enten får vi ikke resten 3 når vi deler 27 med 7, eller får vi ikke resten 5 når vi deler 27 med 11. Dette er riktignok sant: $67 = 9 \cdot 7 + 4$, altså får vi resten 4 når vi deler 67 med 7. I tillegg er $67 = 6 \cdot 11 + 1$, altså får vi resten 1 når vi deler 67 med 11.

Proposisjon 5.7.13. Et heltall a gir resten 10 når vi deler med 13, og gir resten 8 når vi deler med 17, om og bare om det finnes et heltall k slik at $a = 127 + 221k$.

Bevis. La a være et heltall slik at

$$a \equiv 10 \pmod{13}$$

og

$$a \equiv 8 \pmod{17}.$$

Vi gjør følgende observasjoner.

(1) Vi har: $x = -3$ er en løsning til kongruensen

$$17x \equiv 1 \pmod{13}.$$

(2) Vi har: $x = 4$ er en løsning til kongruensen

$$13x \equiv 1 \pmod{17}.$$

Ut ifra Proposisjon 5.7.2 (I) er da

$$x = 17 \cdot (-3) \cdot 10 + 13 \cdot 4 \cdot 8$$

en løsning både til kongruensen

$$x \equiv 10 \pmod{13}$$

og til kongruensen

$$x \equiv 8 \pmod{17},$$

altså $x = -94$ er en løsning til begge kongruensene.

Vi har:

$$127 \equiv -94 \pmod{13 \cdot 17},$$

altså

$$127 \equiv -94 \pmod{221}.$$

Det følger fra Proposisjon 5.7.2 (III) at $x = 127$ er en løsning både til kongruensen

$$x \equiv 10 \pmod{13}$$

og til kongruensen

$$x \equiv 8 \pmod{17}.$$

Ut ifra Proposisjon 5.7.2 (II) er da

$$a \equiv 127 \pmod{221}.$$

Det følger at $221 \mid a - 127$. Dermed finnes det et heltall k slik at $a - 127 = 221k$, altså slik at $a = 127 + 221k$.

For et hvilket som helst heltall k, er

$$127 + 221k \equiv 127 \pmod{221}.$$

Siden 127 er en løsning både til kongruensen

$$x \equiv 10 \pmod{13}$$

og til kongruensen

$$x \equiv 8 \pmod{17},$$

følger det fra Proposisjon 5.7.2 (III) at $x = 127 + 221k$ er en løsning til begge kongruensene.

Således har vi bevist at et heltall a er en løsning både til kongruensen

$$a \equiv 10 \pmod{13}$$

og til kongruensen

$$a \equiv 8 \pmod{13}$$

om og bare om det finnes et heltall k slik at $a = 127 + 221k$. Dette er det samme som å si at, for et hvilket som helst heltall a, får vi resten 10 når vi deler a med 13, og får vi resten 8 når vi deler a med 17, om og bare om det finnes et heltall k slik at $x = 127 + 221k$. □

Eksempel 5.7.14. Proposisjon 5.7.13 fastslår at vi får resten 10 når vi deler 127 med 13, og får resten 8 når vi deler 127 med 17. Dette er riktignok sant:

$$127 = 9 \cdot 13 + 10,$$

og

$$127 = 7 \cdot 17 + 8.$$

Eksempel 5.7.15. Proposisjon 5.7.13 fastslår at vi får resten 10 når vi deler $127 + 3 \cdot 221$, altså 790, med 13, og får resten 8 når vi deler 790 med 17. Dette er riktignok sant:

$$790 = 60 \cdot 13 + 10,$$

og

$$790 = 46 \cdot 17 + 8.$$

Eksempel 5.7.16. Proposisjon 5.7.13 fastslår at vi får resten 10 når vi deler $127-8\cdot 221$, altså -1641, med 13, og får resten 8 når vi deler -1641 med 17. Dette er riktignok sant:

$$-1641 = (-127)\cdot 13 + 10,$$

og

$$-1641 = (-97)\cdot 17 + 8.$$

Eksempel 5.7.17. Siden det ikke er sant at

$$101 \equiv 127 \pmod{221},$$

fastslår Proposisjon 5.7.13 at enten får vi ikke resten 10 når vi deler 101 med 13, eller får vi ikke resten 8 når vi deler 101 med 17. Dette er riktignok sant:

$$101 = 5\cdot 17 + 16,$$

altså får vi resten 16 når vi deler 101 med 17.

Eksempel 5.7.18. Siden det ikke er sant at

$$61 \equiv 127 \pmod{221},$$

fastslår Proposisjon 5.7.13 at enten får vi ikke resten 10 når vi deler 61 med 13, eller får vi ikke resten 8 når vi deler 61 med 17. Dette er riktignok sant: $61 = 4\cdot 13 + 9$, altså får vi resten 9 når vi deler 61 med 13.

Eksempel 5.7.19. Siden det ikke er sant at

$$20 \equiv 127 \pmod{221},$$

fastslår Proposisjon 5.7.13 at enten får vi ikke resten 10 når vi deler 20 med 13, eller får vi ikke resten 8 når vi deler 20 med 17. Dette er riktignok sant: $20 = 1\cdot 13 + 7$, altså får vi resten 7 når vi deler 20 med 13. I tillegg er $20 = 1\cdot 17 + 3$, altså får vi resten 3 når vi deler 20 med 17.

Proposisjon 5.7.20. Et heltall a gir resten 2 når vi deler med 5, resten 4 når vi deler med 7, og resten 1 når vi deler med 12, om og bare om det finnes et heltall k slik at $a = 277 + 420k$.

Bevis. La a være et heltall slik at

$$a \equiv 2 \pmod{5}$$

og

$$a \equiv 4 \pmod{7}.$$

Vi gjør følgende observasjoner.

(1) Vi har: $x = 3$ er en løsning til kongruensen

$$7x \equiv 1 \pmod 5.$$

(2) Vi har: $x = 3$ er en løsning til kongruensen

$$5x \equiv 1 \pmod 7.$$

Ut ifra Proposisjon 5.7.2 (I) er da

$$x = 7 \cdot 3 \cdot 2 + 5 \cdot 3 \cdot 4$$

en løsning både til kongruensen

$$x \equiv 2 \pmod 5$$

og til kongruensen

$$x \equiv 4 \pmod 7,$$

altså $x = 102$ er en løsning til begge kongruensene.

Vi har:

$$32 \equiv 102 \pmod{5 \cdot 7},$$

altså

$$32 \equiv 102 \pmod{35}.$$

Det følger fra Proposisjon 5.7.2 (III) at $x = 32$ er en løsning både til kongruensen

$$x \equiv 2 \pmod 5$$

og til kongruensen

$$x \equiv 4 \pmod 7.$$

Ut ifra Proposisjon 5.7.2 (II) er da

$$a \equiv 32 \pmod{35}.$$

Dermed har vi:

$$a \equiv 32 \pmod{35}$$

og

$$a \equiv 1 \pmod{12}.$$

Vi gjør følgende observasjoner.

(1) Vi har: $x = 3$ er en løsning til kongruensen

$$12x \equiv 1 \pmod{35}.$$

(2) Vi har: $x = -1$ er en løsning til kongruensen

$$35x \equiv 1 \pmod{12}.$$

Siden $\mathsf{sfd}(35, 12) = 1$, følger det fra Proposisjon 5.7.2 (I) at

$$x = 12 \cdot 3 \cdot 32 + 35 \cdot (-1) \cdot 1$$

en løsning både til kongruensen

$$x \equiv 32 \pmod{35}$$

og til kongruensen

$$x \equiv 1 \pmod{12},$$

altså $x = 1117$ er en løsning til begge kongruensene.

Vi har:

$$277 \equiv 1117 \pmod{35 \cdot 12},$$

altså

$$277 \equiv 1117 \pmod{420}.$$

Det følger fra Proposisjon 5.7.2 (III) at $x = 277$ er en løsning både til kongruensen

$$x \equiv 32 \pmod{35}$$

og til kongruensen

$$x \equiv 1 \pmod{12}.$$

Ut ifra Proposisjon 5.7.2 (II) er da

$$a \equiv 277 \pmod{420}.$$

Det følger at $420 \mid a - 277$. Dermed finnes det et heltall k slik at $a - 277 = 420k$, altså slik at $a = 277 + 420k$.

For et hvilket som helst heltall k, er

$$277 + 420k \equiv 277 \pmod{420}.$$

Siden $x = 277$ er en løsning både til kongruensen

$$x \equiv 32 \pmod{35}$$

og til kongruensen

$$x \equiv 1 \pmod{12},$$

følger det fra Proposisjon 5.7.2 (III) at $x = 277 + 420k$ er en løsning til begge kongruensene.

Vi har: $277 + 420k = 277 + 35 \cdot (12k)$. Derfor er

$$277 + 420k \equiv 277 \pmod{35}.$$

Siden

$$277 \equiv 32 \pmod{35},$$

deduserer vi at

$$277 + 420k \equiv 32 \pmod{35}.$$

Siden $x = 32$ er en løsning både til kongruensen

$$x \equiv 2 \pmod{5}$$

og til kongruensen

$$x \equiv 4 \pmod{7},$$

følger det fra Proposisjon 5.7.2 (III) at $x = 277 + 420k$ er en løsning til begge kongruensene.

For et hvilket som helst heltall k, er dermed $x = 277 + 420k$ en løsning til alle følgende kongruenser:

(1) $x \equiv 2 \pmod{5}$;

(2) $x \equiv 4 \pmod{7}$;

(3) $x \equiv 1 \pmod{12}$.

Således har vi bevist at et heltall a er en løsning både til (1), (2), og (3) om og bare om det finnes et heltall k slik at $a = 277 + 420k$. Dette er det samme som å si at, for et hvilket som helst heltall a, får vi resten 2 når vi deler a med 5, får vi resten 4 når vi deler a med 7, og får vi resten 1 når vi deler a med 12, om og bare om det finnes et heltall k slik at $a = 277 + 420k$.

□

Eksempel 5.7.21. Proposisjon 5.7.20 fastslår at vi får resten 2 når vi deler 277 med 5, resten 4 når vi deler 277 med 7, og resten 1 når vi deler 277 med 12. Dette er riktignok sant:

(1) $277 = 55 \cdot 5 + 2$;

(2) $277 = 39 \cdot 7 + 4$;

(3) $277 = 23 \cdot 12 + 1$.

Eksempel 5.7.22. Proposisjon 5.7.20 fastslår at vi får resten 2 når vi deler $277 + 8 \cdot 420$, altså 3637, med 5, resten 4 når vi deler 3637 med 7, og resten 1 når vi deler 3637 med 12. Dette er riktignok sant:

(1) $3637 = 727 \cdot 5 + 2$;

(2) $3637 = 519 \cdot 7 + 4$;

(3) $3637 = 303 \cdot 12 + 1$.

Eksempel 5.7.23. Proposisjon 5.7.20 fastslår at vi får resten 2 når vi deler $277 + (-5) \cdot 420$, altså -1823, med 5, resten 4 når vi deler -1823 med 7, og resten 1 når vi deler -1823 med 12. Dette er riktignok sant:

(1) $-1823 = -365 \cdot 5 + 2$;

(2) $-1823 = -260 \cdot 7 + 4$;

(3) $-1823 = -152 \cdot 12 + 1$.

Eksempel 5.7.24. Siden det ikke er sant at

$$67 \equiv 277 \pmod{420},$$

fastslår Proposisjon 5.7.20 at minst ett av følgende utsagn ikke er sant:

(1) vi får resten 2 når vi deler 67 med 5.

(2) vi får resten 4 når vi deler 67 med 7.

(3) vi får resten 1 når vi deler 67 med 12.

Dette er riktignok tilfellet: $67 = 5 \cdot 12 + 7$, altså får vi resten 7 når vi deler 67 med 12.

Eksempel 5.7.25. Siden det ikke er sant at

$$97 \equiv 277 \pmod{420},$$

fastslår Proposisjon 5.7.20 at minst ett av følgende utsagn ikke er sant:

(1) vi får resten 2 når vi deler 97 med 5.

(2) vi får resten 4 når vi deler 97 med 7.

(3) vi får resten 1 når vi deler 97 med 12.

Dette er riktignok tilfellet: $97 = 13 \cdot 7 + 6$, altså får vi resten 6 når vi deler 97 med 7.

Eksempel 5.7.26. Siden det ikke er sant at

$$25 \equiv 277 \pmod{420},$$

fastslår Proposisjon 5.7.20 at minst ett av følgende utsagn ikke er sant:

(1) vi får resten 2 når vi deler 25 med 5.

(2) vi får resten 4 når vi deler 25 med 7.

(3) vi får resten 1 når vi deler 25 med 12.

Dette er riktignok tilfellet: $25 = 5 \cdot 5$, altså får vi resten 0 når vi deler 25 med 5.

Eksempel 5.7.27. Siden det ikke er sant at

$$81 \equiv 277 \pmod{420},$$

fastslår Proposisjon 5.7.20 at minst ett av følgende utsagn ikke er sant:

(1) vi får resten 2 når vi deler 81 med 5.

(2) vi får resten 4 når vi deler 81 med 7.

(3) vi får resten 1 når vi deler 81 med 12.

Dette er riktignok tilfellet: $81 = 16 \cdot 5 + 1$, altså får vi resten 1 når vi deler 81 med 5. I tillegg er $81 = 6 \cdot 12 + 9$, altså får vi resten 9 når vi deler 81 med 12.

Eksempel 5.7.28. Siden det ikke er sant at

$$54 \equiv 277 \pmod{420},$$

fastslår Proposisjon 5.7.20 at minst ett av følgende utsagn ikke er sant:

(1) vi får resten 2 når vi deler 54 med 5.

(2) vi får resten 4 når vi deler 54 med 7.

(3) vi får resten 1 når vi deler 54 med 12.

Dette er riktignok tilfellet: $54 = 10 \cdot 5 + 4$, altså får vi resten 4 når vi deler 54 med 5. I tillegg er $54 = 7 \cdot 7 + 5$, altså får vi resten 5 når vi deler 54 med 7. Dessuten er $54 = 4 \cdot 12 + 6$, altså får vi resten 6 når vi deler 54 med 12.

Merknad 5.7.29. I beviset for Proposisjon 5.7.20 benyttet vi Proposisjon 5.7.2 for å finne en løsning til alle tre følgende kongruenser:

(1) $x \equiv 2 \pmod{5}$;

(2) $x \equiv 4 \pmod{7}$;

(3) $x \equiv 1 \pmod{12}$.

På en lignende måte kan Proposisjon 5.7.2 benyttes for å finne en løsning til et hvilket som helst antall kongruenser. Imidlertid må vi være forsiktig: hver gang vi benytter Proposisjon 5.7.2 må antakelsen at $\mathsf{sfd}(n_1, n_2) = 1$ oppfylles.

Korollar 5.7.30. La n_1 og n_2 være heltall. Anta at $n_1 \neq 0$, $n_2 \neq 0$, og $\mathsf{sfd}(n_1, n_2) = 1$. La a og c være heltall. Da er

$$a \equiv c \pmod{n_1 n_2}$$

om og bare om begge følgende utsagn er sanne:

(1) $a \equiv c \pmod{n_1}$;

(2) $a \equiv c \pmod{n_2}$.

Bevis. Anta først at

$$a \equiv c \pmod{n_1 n_2}.$$

Ut ifra Proposisjon 3.2.57, er da

$$a \equiv c \pmod{n_1}$$

og

$$a \equiv c \pmod{n_2}.$$

Anta istedenfor at

$$a \equiv c \pmod{n_1}$$

og at

$$a \equiv c \pmod{n_2}.$$

Siden det også er tilfellet at

$$c \equiv c \pmod{n_1}$$

og

$$c \equiv c \pmod{n_2},$$

følger det fra Proposisjon 5.7.2 (II) at

$$a \equiv c \pmod{n_1 n_2}.$$

□

Eksempel 5.7.31. Vi har:

$$87 \equiv 3 \pmod{6}$$

og

$$87 \equiv 3 \pmod{7}.$$

Siden $\mathsf{sfd}(6, 7) = 1$, fastslår Korollar 5.7.30 at

$$87 \equiv 3 \pmod{42}.$$

Dette er riktignok sant.

Eksempel 5.7.32. Vi har:

$$62 \equiv 2 \pmod{60}.$$

Siden $60 = 4 \cdot 15$ og $\mathsf{sfd}(4, 15) = 1$, fastslår Korollar 5.7.30 at

$$62 \equiv 2 \pmod{4}$$

og

$$62 \equiv 2 \pmod{15}.$$

Dette er riktignok sant.

Merknad 5.7.33. Følgende korollar kommer til å være nyttig i den neste delen av kapittelet.

Korollar 5.7.34. La p og q være primtall slik at $p \neq q$. La p^{-1} være inversen til p modulo q. La q^{-1} være inversen til q modulo p. La i være et naturlig tall slik at $i \leq p-1$. La j være et naturlig tall slik at $j \leq q-1$. Da er

$$qq^{-1}i + pp^{-1}j \equiv i \pmod{p}$$

og

$$qq^{-1}i + pp^{-1}j \equiv j \pmod{q}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra definisjonen til q^{-1}, er

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

(2) Ut ifra definisjonen til p^{-1}, er

$$pp^{-1} \equiv 1 \pmod{q}.$$

(3) Siden $p \neq q$, og både p og q er primtall, er $\mathsf{sfd}(p, q) = 1$.

Det følger umiddelbart fra Proposisjon 5.7.2 (I) at

$$qq^{-1}i + pp^{-1}j \equiv i \pmod{p}$$

og

$$qq^{-1}i + pp^{-1}j \equiv j \pmod{q}.$$

□

Eksempel 5.7.35. La p være 3, og la q være 5. Siden

$$3 \cdot 2 = 6 \equiv 1 \pmod{5},$$

er $p^{-1} = 2$. Siden

$$5 \cdot 2 = 10 \equiv 1 \pmod{3},$$

er $q^{-1} = 2$. Da er $qq^{-1} = 5 \cdot 2 = 10$ og $pp^{-1} = 3 \cdot 2 = 6$.

Korollar 5.7.34 fastslår for eksempel at

$$10 \cdot 2 + 6 \cdot 3 \equiv 2 \pmod{3},$$

og at

$$10 \cdot 2 + 6 \cdot 3 \equiv 3 \pmod{5}.$$

Siden

$$10 \cdot 2 + 6 \cdot 3 = 38,$$

og siden

$$38 \equiv 2 \pmod 3$$

og

$$38 \equiv 3 \pmod 5,$$

er dette riktignok sant.

Eksempel 5.7.36. La p være 5, og la q være 11. Siden

$$5 \cdot 9 = 45 \equiv 1 \pmod{11},$$

er $p^{-1} = 9$. Siden

$$11 \cdot 1 = 11 \equiv 1 \pmod 5,$$

er $q^{-1} = 1$. Da er $qq^{-1} = 11 \cdot 1 = 11$ og $pp^{-1} = 5 \cdot 9 = 45$.
Korollar 5.7.34 fastslår at for eksempel

$$11 \cdot 3 + 45 \cdot 7 \equiv 3 \pmod 5,$$

og at

$$11 \cdot 3 + 45 \cdot 7 \equiv 7 \pmod 5.$$

Siden

$$11 \cdot 3 + 45 \cdot 7 = 348,$$

og siden

$$348 \equiv 3 \pmod 5$$

og

$$348 \equiv 7 \pmod{11},$$

er dette riktignok sant.

5.8 Kvadratisk gjensidighet

Merknad 5.8.1. Målet i denne delen av kapittelet er å gi et bevis for Teorem 5.8.30. Først må vi gjøre noen forberedelser.

Lemma 5.8.2. La y være et naturlig tall. Da finnes det et naturlig tall s_y og et heltall e_y slik at:

(A) $e_y y \equiv s_y \pmod q$;

(B) $0 < s_y \leq \frac{q-1}{2}$;

(C) enten $e_y = 1$ eller $e_y = -1$.

Bevis. Ut ifra Proposisjon 3.2.1 finnes det et heltall z slik at

$$y \equiv z \pmod{q}$$

og $0 \leq z < q$. Siden det ikke er sant at $q \mid y$, er det ikke sant at $z = 0$. Dermed er $0 < z < q$. Ett av følgende er sant.

(I) $1 \leq z \leq \frac{q-1}{2}$;

(II) $\frac{q-1}{2} < z \leq q - 1$.

Anta først at (I) er sant. La s_y være z, og la e_y være 1. Da er (A) – (C) sanne.

Anta istedenfor at (II) er sant. Da har vi:

$$-(q-1) \leq -z < -\frac{q-1}{2}.$$

Det følger at

$$-(q-1) + q \leq -z + q < -\frac{q-1}{2} + q,$$

altså at

$$1 \leq -z + q < \frac{q-1}{2}.$$

I tillegg er

$$-z + q \equiv -z \pmod{q}.$$

La s_y være $-z + q$, og la e_y være -1. Da er

$$1 \leq s_y \leq \frac{q-1}{2}$$

og

$$e_y y = -y \equiv -z \equiv -z + q = s_y \pmod{q}.$$

Dermed er (A) – (C) sanne.

□

Eksempel 5.8.3. La q være 7, og la y være 12. Da fastslår Lemma 5.8.2 at det finnes et naturlig tall s_y og et heltall e_y slik at:

(A) $e_y 12 \equiv s_y \pmod{7}$;

(B) $0 < s_y \leq 3$;

(C) enten $e_y = 1$ eller $e_y = -1$.

Ved å la s_y være 2 og e_y være -1 er dette riktignok sant:

$$-12 \equiv 2 \pmod{7}.$$

Eksempel 5.8.4. La q være 11, og la y være 15. Da fastslår Lemma 5.8.2 at det finnes et naturlig tall s_y og et heltall e_y slik at:

(A) $e_y 15 \equiv s_y \pmod{11}$;

(B) $0 < s_y \leq 5$;

(C) enten $e_y = 1$ eller $e_y = -1$.

Ved å la s_y være 4 og e_y være 1 er dette riktignok sant:

$$15 \equiv 4 \pmod{11}.$$

Eksempel 5.8.5. La q være 17, og la y være 48. Da fastslår Lemma 5.8.2 at det finnes et naturlig tall s_y og et heltall e_y slik at:

(A) $e_y 48 \equiv s_y \pmod{11}$;

(B) $0 < s_y \leq 8$;

(C) enten $e_y = 1$ eller $e_y = -1$.

Ved å la s_y være 3 og e_y være -1 er dette riktignok sant:

$$-48 \equiv 3 \pmod{17}.$$

Eksempel 5.8.6. La q være 29, og la y være 90. Da fastslår Lemma 5.8.2 at det finnes et naturlig tall s_y og et heltall e_y slik at:

(A) $e_y 90 \equiv s_y \pmod{29}$;

(B) $0 < s_y \leq 14$;

(C) enten $e_y = 1$ eller $e_y = -1$.

Ved å la s_y være 3 og e_y være 1 er dette riktignok sant:

$$90 \equiv 3 \pmod{29}.$$

Lemma 5.8.7. La p og q være primtall slik at $p > 2$, $q > 2$, og $p \neq q$. La v være produktet av alle de naturlige tallene y slik at

$$y \leq \frac{pq-1}{2}$$

og verken $p \mid y$ eller $q \mid y$. Da har v akkurat

$$\frac{pq-q-p+1}{2}$$

ledd.

Bevis. Vi gjør følgende observasjoner.

(1) Det finnes akkurat $\frac{pq-1}{2}$ naturlige tall y slik at $y \leq \frac{pq-1}{2}$.

(2) Det finnes akkurat $\frac{q-1}{2}$ naturlige tall y slik at $y \leq \frac{pq-1}{2}$ og $p \mid y$, nemlig p, $2p$, $3p$, $\ldots$, $\left(\frac{q-1}{2}\right)p$.

(3) Det finnes akkurat $\frac{p-1}{2}$ naturlige tall y slik at $y \leq \frac{pq-1}{2}$ og slik at $q \mid y$, nemlig q, $2q$, $3q$, $\ldots$, $\left(\frac{p-1}{2}\right)q$.

(4) Anta at det finnes naturlige tall i og j slik at

$$ip = jq,$$

hvor $i \leq \frac{q-1}{2}$ og $j \leq \frac{p-1}{2}$. Da har vi: $q \mid ip$. Siden q er et primtall, følger det fra Proposisjon 4.2.12 at enten $q \mid i$ eller $q \mid p$.

(5) Siden q er et primtall og $p \neq q$, er det ikke sant at $q \mid p$.

(6) Siden $i < q$ er det ikke sant at $q \mid i$.

(7) Da har vi motsigelse: på én side er enten $q \mid i$ eller $q \mid p$, mens på en annen side er verken $q \mid i$ eller $q \mid p$. Vi konkluderer at det ikke finnes naturlige tall i og j slik at

$$ip = jq,$$

hvor $i \leq \frac{q-1}{2}$ og $j \leq \frac{p-1}{2}$. Med andre ord finnes det ikke et naturlig tall som tilhører både lista i (2) og lista i (3).

Det følger fra (1), (2), (3), og (7) at v har akkurat

$$\frac{pq-1}{2} - \left(\frac{q-1}{2}\right) - \left(\frac{p-1}{2}\right)$$

ledd, altså akkurat

$$\frac{pq-q-p+1}{2}$$

ledd.

□

Eksempel 5.8.8. La p være 3, og la q være 5. Da er

$$\frac{pq-1}{2} = \frac{15-1}{2} = \frac{14}{2} = 7.$$

Lemma 5.8.7 fastslår at det finnes akkurat

$$\frac{15-5-3+1}{2} = \frac{8}{2} = 4$$

naturlige tall y slik at $y \leq 7$ og verken $p \mid y$ eller $q \mid y$. Dette er riktignok sant: de naturlige tallene som oppfyller disse kravene er 1, 2, 4, og 7.

Eksempel 5.8.9. La p være 3, og la q være 7. Da er

$$\frac{pq-1}{2} = \frac{21-1}{2} = \frac{20}{2} = 10.$$

Lemma 5.8.7 fastslår at det finnes

$$\frac{21-7-3+1}{2} = \frac{12}{2} = 6$$

naturlige tall y slik at $y \leq 10$ og verken $p \mid y$ eller $q \mid y$. Dette er riktignok sant: de naturlige tallene som oppfyller disse kravene er 1, 2, 4, 5, 8, og 10.

Lemma 5.8.10. La p og q være primtall slik at $p > 2$, $q > 2$, og $p \neq q$. La p^{-1} være inversen til p modulo q. La q^{-1} være inversen modulo p. For hvert naturlig tall i slik at $i \leq p-1$, og hvert naturlig tall j slik at

$$j \leq \frac{q-1}{2},$$

la oss betegne

$$qq^{-1}i + pp^{-1}j$$

som $u_{i,j}$.

La u være produktet av alle de naturlige tallene $u_{i,j}$ slik at $i \leq p-1$ og

$$j \leq \frac{q-1}{2}.$$

La v være produktet av alle de naturlige tallene y slik at

$$y \leq \frac{pq-1}{2}$$

og verken $p \mid y$ eller $q \mid y$.

Da er enten

$$u \equiv v \pmod{pq}$$

eller er

$$u \equiv -v \pmod{pq}.$$

Bevis. Anta at følgende har blitt bevist.

(A) For hvert ledd y av v, finnes det et ledd u_{i_y,j_y} av u slik at enten

$$y \equiv u_{i_y,j_y} \pmod{pq}$$

eller

$$y \equiv -u_{i_y,j_y} \pmod{pq}.$$

(B) La y og y' være ulike ledd av v. Dersom

$$u_{i_y,j_y} = u_{i_{y'},j_{y'}},$$

er $y = y'$.

Da gjør vi følgende observasjoner.

(1) La z være produktet av leddene u_{i_y,j_y} av u slik at y er et ledd av v. Det følger det fra (A) at enten

$$v \equiv z \pmod{pq}$$

eller

$$v \equiv -z \pmod{pq}.$$

(2) Ut ifra Lemma 5.8.7 har v akkurat

$$\frac{pq - q - p + 1}{2}$$

ledd. Da følger det fra (B) at enten z eller $-z$ er produktet av

$$\frac{pq - q - p + 1}{2}$$

ulike ledd av u.

(3) Produktet u har samme antall ledd som antall par naturlige tall (i, j) slik at $i \leq p - 1$ og $j \leq \frac{q-1}{2}$, altså akkurat

$$(p-1) \cdot \left(\frac{q-1}{2}\right) = \frac{pq - q - p + 1}{2}$$

ledd.

Det følger fra (2) – (3) at enten z eller $-z$ er kongruent modulo pq til produktet av alle leddene av u, altså til u. Dermed følger det fra (1) at enten

$$v \equiv u \pmod{pq}$$

eller

$$v \equiv -u \pmod{pq}.$$

Således er proposisjonen sann om vi kan bevise at (A) og (B) er sanne. La oss nå gjøre dette. La y være et ledd av v, altså et naturlig tall slik at

$$y \leq \frac{pq - 1}{2}$$

og verken $p \mid y$ eller $q \mid y$. Vi gjør følgende observasjoner.

(1) Ut ifra Lemma 5.8.2 finnes det et heltall j_y og et heltall e_y slik at

$$e_y y \equiv j_y \pmod{p},$$

hvor

$$0 < j_y < \frac{q-1}{2}$$

og enten $e_y = 1$ eller $e_y = -1$.

(2) Ut ifra Proposisjon 3.2.1 finnes det et heltall i_y slik at

$$e_y y \equiv i_y \pmod{p}$$

og $0 \leq i_y < p$. Siden det ikke er sant at $p \mid y$, er det ikke sant at $i_y = 0$, altså er $0 < i_y < p$.

(3) Det følger fra (1) og (2) at $x = e_y y$ er en løsning både til kongruensen

$$x \equiv i_y \pmod{p}$$

og til kongruensen

$$x \equiv j_y \pmod{q}.$$

(4) Ut ifra Korollar 5.7.34 er i tillegg

$$x = qq^{-1}i_y + pp^{-1}j_y,$$

altså $x = u_{i_y,j_y}$, en løsning både til kongruensen

$$x \equiv i_y \pmod{p}$$

og til kongruensen

$$x \equiv j_y \pmod{q}.$$

(5) Det følger fra (3), (4), og Proposisjon 5.7.2 (II) at

$$e_y y \equiv u_{i_y,j_y} \pmod{pq}.$$

Siden $e_y^2 = 1$, er da

$$y \equiv e_y u_{i_y,j_y} \mod pq.$$

Således er (A) sant.

La nå y og y' være ledd av produktet v. Anta at

$$u_{i_y,j_y} = u_{i_{y'},j_{y'}}.$$

Vi gjør følgende observasjoner.

(1) Ut ifra Korollar 5.7.34 er

$$u_{i_y,j_y} \equiv y \pmod{p}$$

og

$$u_{i_{y'},j_{y'}} \equiv y' \pmod{p}.$$

Dermed er

$$y \equiv u_{i_y,j_y} = u_{i_{y'},j_{y'}} \equiv y' \pmod{p}.$$

(2) Ut ifra Korollar 5.7.34 er

$$u_{i_y,j_y} \equiv y \pmod{q}$$

og

$$u_{i_{y'},j_{y'}} \equiv y' \pmod{q}.$$

Dermed er

$$y \equiv u_{i_y,j_y} \equiv u_{i_{y'},j_{y'}} \equiv y' \pmod{q}.$$

(3) Det følger fra (2), (3), og Korollar 5.7.30 at

$$y \equiv y' \pmod{pq}.$$

Siden $0 < y < pq$ og $0 < y' < pq$, følger det fra Proposisjon 3.2.11 at $y = y'$.

Således er (B) sant.

□

Eksempel 5.8.11. La p være 3, og la q være 5. Som i Eksempel 5.7.35 er $qq^{-1} = 10$ og $pp^{-1} = 6$. Vi har:

$$\frac{q-1}{2} = \frac{5-1}{2} = \frac{4}{2} = 2.$$

Vi gjør følgende observasjoner.

(1) Vi har følgende.

i	j	$u_{i,j} \equiv \pmod{15}$	Utregningen
1	1	1	$10 \cdot 1 + 6 \cdot 1 = 16 \equiv 1$
1	2	7	$10 \cdot 1 + 6 \cdot 2 = 22 \equiv 7$
2	1	11	$10 \cdot 2 + 6 \cdot 1 = 26 \equiv 11$
2	2	2	$10 \cdot 2 + 6 \cdot 2 = 32 \equiv 2$

Dermed er

$$u \equiv 1 \cdot 7 \cdot 11 \cdot 2 = 7 \cdot 22 \equiv 7 \cdot 7 = 49 \equiv 4 \pmod{15}.$$

(2) Vi har:

$$\frac{pq-1}{2} = \frac{15-1}{2} = \frac{14}{2} = 7$$

og

$$v = 1 \cdot 2 \cdot 4 \cdot 7 = 56 \equiv -4 \pmod{15}.$$

Lemma 5.8.10 fastslår at enten

$$u \equiv v \pmod{15}$$

eller

$$u \equiv -v \pmod{15}.$$

Dette er riktignok sant:

$$u \equiv -v \pmod{15}.$$

Beviset for Lemma 5.8.10 fastslår at:

(1) v har samme antall ledd som antall naturlige tall $u_{i,j}$;

(2) for hvert ledd y av v, finnes det ett av de naturlige tallene $u_{i,j}$ slik at enten

$$y \equiv u_{i,j} \pmod{15}$$

eller

$$y \equiv u_{i,j} \pmod{15}.$$

Følgende tabell viser at dette riktignok er sant.

Ledd y av u'	Tilsvarende $u_{i,j}$	$y \equiv u_{i,j}$ eller $y \equiv -u_{i,j} \pmod{15}$?
1	$u_{1,1} = 1$	$1 \equiv 1 \pmod{15}$
2	$u_{2,2} = 2$	$2 \equiv 2 \pmod{15}$
4	$u_{2,1} = 11$	$4 \equiv -11 \pmod{15}$
7	$u_{1,2} = 7$	$7 \equiv 7 \pmod{15}$

Eksempel 5.8.12. La p være 3, og la q være 7. Siden

$$3 \cdot 5 = 15 \equiv 1 \pmod{7},$$

er $p^{-1} = 5$. Siden

$$7 \cdot 1 = 7 \equiv 1 \pmod{3},$$

er $q^{-1} = 1$. Da er

$$qq^{-1} = 7 \cdot 1 = 7$$

og

$$pp^{-1} = 3 \cdot 5 = 15.$$

Vi har:

$$\frac{q-1}{2} = \frac{7-1}{2} = \frac{6}{2} = 3.$$

Vi gjør følgende observasjoner.

(1) Vi har følgende.

i	j	$u_{i,j} \pmod{21}$	Utregningen
1	1	1	$7 \cdot 1 + 15 \cdot 1 = 22 \equiv 1$
1	2	16	$7 \cdot 1 + 15 \cdot 2 = 37 \equiv 16$
1	3	10	$7 \cdot 1 + 15 \cdot 3 = 52 \equiv 10$
2	1	8	$7 \cdot 2 + 15 \cdot 1 = 29 \equiv 8$
2	2	2	$7 \cdot 2 + 15 \cdot 2 = 44 \equiv 2$
2	3	17	$7 \cdot 2 + 15 \cdot 3 = 59 \equiv 17$

Dermed er

$$u = u_1 \cdot u_2 \equiv 13 \cdot 20 \equiv (-8) \cdot (-1) = 8 \pmod{21}.$$

(2) Vi har:

$$\frac{pq-1}{2} = \frac{21-1}{2} = \frac{20}{2} = 10$$

og

$$v = 1 \cdot 2 \cdot 4 \cdot 5 \cdot 8 \cdot 10 = 40 \cdot 80 \equiv (-2) \cdot (-4) = 8 \pmod{21}.$$

Lemma 5.8.10 fastslår at enten

$$u \equiv v \pmod{21}$$

eller

$$u \equiv v \pmod{21}.$$

Dete er riktignok sant:

$$u \equiv -v \pmod{21}.$$

Beviset for Lemma 5.8.10 fastslår at:

(1) v har samme antall ledd som antall naturlige tall $u_{i,j}$;

(2) for hvert ledd y av u', finnes det ett av de naturlige tallene $u_{i,j}$ slik at enten

$$y \equiv u_{i,j} \pmod{21}$$

eller

$$y \equiv u_{i,j} \pmod{21}.$$

Følgende tabell viser at dette riktignok er sant.

Ledd y av u'	Tilsvarende $u_{i,j}$	$y \equiv u_{i,j}$ eller $y \equiv -u_{i,j} \pmod{21}$?
1	$u_{1,1} = 1$	$1 \equiv 1$
2	$u_{2,2} = 2$	$2 \equiv 2$
4	$u_{2,3} = 17$	$4 \equiv -17$
5	$u_{1,2} = 16$	$5 \equiv -16$
8	$u_{2,1} = 8$	$4 \equiv 8$
10	$u_{1,3} = 10$	$10 \equiv 10$

Eksempel 5.8.13. La p være 5, og la q være 7. Siden

$$5 \cdot 3 = 15 \equiv 1 \pmod{7},$$

er $p^{-1} = 3$. Siden

$$7 \cdot 3 = 21 \equiv 1 \pmod{5},$$

er $q^{-1} = 3$. Da er

$$qq^{-1} = 7 \cdot 3 = 21$$

og

$$pp^{-1} = 5 \cdot 3 = 15.$$

Vi har:

$$\frac{q-1}{2} = \frac{7-1}{2} = \frac{6}{2} = 3.$$

Vi gjør følgende observasjoner.

(1) Vi har følgende.

i	j	$u_{i,j} \pmod{35}$	Utregningen
1	1	1	$21 \cdot 1 + 15 \cdot 1 = 36 \equiv 1$
1	2	16	$21 \cdot 1 + 15 \cdot 2 = 51 \equiv 16$
1	3	21	$21 \cdot 1 + 15 \cdot 3 = 66 \equiv 31$
2	1	22	$21 \cdot 2 + 15 \cdot 1 = 57 \equiv 22$
2	2	2	$21 \cdot 2 + 15 \cdot 2 = 72 \equiv 2$
2	3	17	$21 \cdot 2 + 15 \cdot 3 = 87 \equiv 17$
3	1	8	$21 \cdot 3 + 15 \cdot 1 = 78 \equiv 8$
3	2	23	$21 \cdot 3 + 15 \cdot 2 = 93 \equiv 23$
3	3	3	$21 \cdot 3 + 15 \cdot 3 = 108 \equiv 3$
4	1	29	$21 \cdot 4 + 15 \cdot 1 = 99 \equiv 29$
4	2	9	$21 \cdot 4 + 15 \cdot 2 = 114 \equiv 9$
4	3	24	$21 \cdot 4 + 15 \cdot 3 = 129 \equiv 24$

Det kan regnes ut at produktet av alle de naturlige tallene $u_{i,j}$ er kongruent til 14 modulo 35, altså er

$$u \equiv 29 \pmod{35}.$$

(2) Vi har:

$$\frac{pq-1}{2} = \frac{35-1}{2} = \frac{34}{2} = 17$$

og

$$v = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 \cdot 8 \cdot 9 \cdot 11 \cdot 12 \cdot 13 \cdot 16 \cdot 17.$$

Det kan regnes ut at

$$v \equiv 6 \pmod{35}.$$

Lemma 5.8.10 fastslår at enten

$$u \equiv v \pmod{35}$$

eller

$$u \equiv v \pmod{35}.$$

Dete er riktignok sant:

$$u \equiv -v \pmod{35}.$$

Beviset for Lemma 5.8.10 fastslår at:

(1) v har samme antall ledd som antall naturlige tall $u_{i,j}$;

(2) for hvert ledd y av u', finnes det ett av de naturlige tallene $u_{i,j}$ slik at enten

$$y \equiv u_{i,j} \pmod{35}$$

eller

$$y \equiv u_{i,j} \pmod{35}.$$

Følgende tabell viser at dette riktignok er sant.

Ledd y av u'	Tilsvarende $u_{i,j}$	$y \equiv u_{i,j}$ eller $y \equiv -u_{i,j} \pmod{35}$?
1	$u_{1,1} = 1$	$1 \equiv 1$
2	$u_{2,2} = 2$	$2 \equiv 2$
3	$u_{3,3} = 3$	$3 \equiv 3$
4	$u_{1,3} = 31$	$4 \equiv -31$
6	$u_{4,1} = 29$	$6 \equiv -29$
8	$u_{3,1} = 8$	$8 \equiv 8$
9	$u_{4,2} = 9$	$9 \equiv 9$
11	$u_{1,3} = 24$	$11 \equiv -24$
12	$u_{3,2} = 23$	$12 \equiv -23$
13	$u_{2,1} = 22$	$13 \equiv -22$
16	$u_{1,2} = 16$	$16 \equiv 16$
17	$u_{2,3} = 17$	$17 \equiv 17$

Merknad 5.8.14. På en måte er Lemma 5.8.10 kjernen til beviset for Teorem 5.8.30. Det gir oss muligheten til å regne ut heltallene u og v hvert for seg, og å konkludere at resultatene er kongruent til hverandre modulo pq.

Vi kommer til å gjennomføre disse to utregningene i Lemma 5.8.22 og Lemma 5.8.25. Vi kommer til å se at Teorem 5.8.30 følger umiddelbart fra at disse to utregningene er kongruent modulo pq.

Med andre ord er Lemma 5.8.10 brua vi trenger mellom Lemma 5.8.22 og Lemma 5.8.25 for å gi et bevis for Teorem 5.8.30.

Merknad 5.8.15. For å unngå forvirring: den venstre siden av kongruensen i følgende lemma er $\left(\frac{q-1}{2}\right)!$ ganger med $\left(\frac{q-1}{2}\right)!$, altså $\left(\frac{q-1}{2}\right)!$ i kvadrat.

Lemma 5.8.16. La q være et primtall slik at $q > 2$. Da er

$$\left(\frac{q-1}{2}\right)!\left(\frac{q-1}{2}\right)! \equiv (-1)^{\frac{q-1}{2}}(q-1)! \pmod{q}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Vi har:

$$\begin{aligned}&(q-1)!\\ &= 1 \times 2 \times \cdots \times (q-1)\\ &= 1 \times 2 \times \cdots \times \left(\frac{q-1}{2}\right) \times \left(\frac{q-1}{2}+1\right) \times \left(\frac{q-1}{2}+2\right) \times \cdots \times \left(\frac{q-1}{2}+\frac{q-1}{2}\right).\end{aligned}$$

(2) Vi har:

$$\left(\frac{q-1}{2}+1\right) - \left(-\left(\frac{q-1}{2}\right)\right) = q,$$

altså

$$\left(\frac{q-1}{2}+1\right) \equiv -\left(\frac{q-1}{2}\right) \pmod{q}.$$

På lignende vis er

$$\left(\frac{q-1}{2}+i\right) \equiv -\left(\frac{q-1}{2}-(i-1)\right) \pmod{q}$$

for hvert naturlig tall i slik at $i \leq \frac{q-1}{2}$. Dermed er

$$\begin{aligned}&\left(\frac{q-1}{2}+1\right) \times \left(\frac{q-1}{2}+2\right) \times \cdots \times \left(\frac{q-1}{2}+\frac{q-1}{2}\right)\\ &\equiv \left(-\left(\frac{q-1}{2}\right)\right) \times \left(-\left(\frac{q-1}{2}-1\right)\right) \times \cdots \times -1 \pmod{q}.\end{aligned}$$

Således er

$$\begin{aligned}&\left(\frac{q-1}{2}+1\right) \times \left(\frac{q-1}{2}+2\right) \times \cdots \times \left(\frac{q-1}{2}+\frac{q-1}{2}\right)\\ &\equiv (-1)^{\frac{q-1}{2}}\left(\left(\frac{q-1}{2}\right) \times \left(\frac{q-1}{2}-1\right) \times \cdots \times 1\right) \pmod{q},\end{aligned}$$

(3) Produktet

$$\left(\frac{q-1}{2}\right) \times \left(\frac{q-1}{2}-1\right) \times \cdots \times 1$$

er produktet

$$1 \times 2 \times \cdots \times \left(\frac{q-1}{2}\right)$$

omvendt. Derfor følger det fra (2) at

$$\begin{aligned}&\left(\frac{q-1}{2}+1\right) \times \left(\frac{q-1}{2}+2\right) \times \cdots \times \left(\frac{q-1}{2}+\frac{q-1}{2}\right)\\ &\equiv (-1)^{\frac{q-1}{2}} \left(1 \times 2 \times \cdots \times \left(\frac{q-1}{2}\right)\right) \pmod{q}.\end{aligned}$$

(4) Ut ifra (3) er

$$\begin{aligned}&1 \times 2 \times \cdots \times \left(\frac{q-1}{2}\right) \times \left(\frac{q-1}{2}+1\right) \times \left(\frac{q-1}{2}+2\right) \times \cdots \times \left(\frac{q-1}{2}+\frac{q-1}{2}\right)\\ &\equiv 1 \times 2 \times \cdots \times \left(\frac{q-1}{2}\right) \times (-1)^{\frac{q-1}{2}} \times \left(1 \times 2 \times \cdots \times \left(\frac{q-1}{2}\right)\right) \pmod{q}.\end{aligned}$$

Dermed er

$$\begin{aligned}&1 \times 2 \times \cdots \times \left(\frac{q-1}{2}\right) \times \left(\frac{q-1}{2}+1\right) \times \left(\frac{q-1}{2}+2\right) \times \cdots \times \left(\frac{q-1}{2}+\frac{q-1}{2}\right)\\ &\equiv (-1)^{\frac{q-1}{2}} \times \left(1 \times 2 \times \cdots \times \left(\frac{q-1}{2}\right)\right)^2 \pmod{q},\end{aligned}$$

altså er

$$\begin{aligned}&1 \times 2 \times \cdots \times \left(\frac{q-1}{2}\right) \times \left(\frac{q-1}{2}+1\right) \times \left(\frac{q-1}{2}+2\right) \times \cdots \times \left(\frac{q-1}{2}+\frac{q-1}{2}\right)\\ &\equiv (-1)^{\frac{q-1}{2}} \times \left(\frac{q-1}{2}\right)! \times \left(\frac{q-1}{2}\right)! \pmod{q}.\end{aligned}$$

Ut ifra (1) og (4) er

$$(q-1)! \equiv (-1)^{\frac{q-1}{2}} \times \left(\frac{q-1}{2}\right)! \times \left(\frac{q-1}{2}\right)! \pmod{q}.$$

Dermed er

$$(-1)^{\frac{q-1}{2}} \times (q-1)! \equiv (-1)^{\frac{q-1}{2}} \times (-1)^{\frac{q-1}{2}} \times \left(\frac{q-1}{2}\right)! \times \left(\frac{q-1}{2}\right)! \pmod{q},$$

altså

$$(-1)^{\frac{q-1}{2}} \times (q-1)! \equiv (-1)^{q-1} \times \left(\frac{q-1}{2}\right)! \times \left(\frac{q-1}{2}\right)! \pmod{q}.$$

Ut ifra Korollar 4.10.8, er

$$(-1)^{q-1} \equiv 1 \pmod{q}.$$

Det følger at

$$(-1)^{\frac{q-1}{2}} \times (q-1)! \equiv \left(\frac{q-1}{2}\right)! \times \left(\frac{q-1}{2}\right)! \pmod{q}.$$

□

Eksempel 5.8.17. Lemma 5.8.16 fastslår at

$$\left(\frac{3-1}{2}\right)!\left(\frac{3-1}{2}\right)! \equiv (-1)^{\frac{3-1}{2}}(3-1)! \pmod{3},$$

altså at

$$1! \cdot 1! \equiv (-1)^1 \cdot 2! \pmod{3}.$$

Vi har:

$$1! \cdot 1! = 1 \cdot 1 = 1$$

og

$$(-1)^1 \cdot 2! = (-1) \cdot 2 = -2.$$

Siden

$$1 \equiv -2 \pmod{3},$$

ser vi at det riktignok er sant at

$$1! \cdot 1! \equiv (-1)^1 \cdot 2! \pmod{3}.$$

Eksempel 5.8.18. Lemma 5.8.16 fastslår at

$$\left(\frac{5-1}{2}\right)!\left(\frac{5-1}{2}\right)! \equiv (-1)^{\frac{5-1}{2}}(5-1)! \pmod{5},$$

altså at

$$2! \cdot 2! \equiv (-1)^2 \cdot 4! \pmod{5}.$$

Vi har:

$$2! \cdot 2! = 2 \cdot 2 = 4$$

og

$$(-1)^2 \cdot 4! = 1 \cdot 24 = 24.$$

Siden

$$4 \equiv 24 \pmod{5},$$

ser vi at det riktignok er sant at

$$2! \cdot 2! \equiv (-1)^2 \cdot 4! \pmod{5}.$$

Korollar 5.8.19. La q være et primtall slik at $q > 2$. Da er

$$\left(\frac{q-1}{2}\right)!\left(\frac{q-1}{2}\right)! \equiv (-1)^{\frac{q-1}{2}} \cdot (-1) \pmod{q}.$$

Bevis. Ut ifra Lemma 5.8.16 er

$$\left(\frac{q-1}{2}\right)!\left(\frac{q-1}{2}\right)! \equiv (-1)^{\frac{q-1}{2}}(q-1)! \pmod{q}.$$

Ut ifra Proposisjon 4.15.8, er

$$(q-1)! \equiv -1 \pmod{q}.$$

Dermed er

$$\left(\frac{q-1}{2}\right)!\left(\frac{q-1}{2}\right)! \equiv (-1)^{\frac{q-1}{2}} \cdot (-1) \pmod{q}.$$

□

Eksempel 5.8.20. Korollar 5.8.19 fastslår at

$$\left(\frac{3-1}{2}\right)!\left(\frac{3-1}{2}\right)! \equiv (-1)^{\frac{3-1}{2}} \cdot (-1) \pmod{3},$$

altså at

$$1! \cdot 1! \equiv (-1)^1 \cdot (-1) \pmod{3}.$$

Siden

$$1! \cdot 1! = 1$$

og

$$(-1)^1 \cdot (-1) = (-1) \cdot (-1) = 1,$$

er dette riktignok sant.

Eksempel 5.8.21. Korollar 5.8.19 fastslår at

$$\left(\frac{5-1}{2}\right)!\left(\frac{5-1}{2}\right)! \equiv (-1)^{\frac{5-1}{2}} \cdot (-1) \pmod{5},$$

altså at

$$2! \cdot 2! \equiv (-1)^2 \cdot (-1) \pmod{5}.$$

Vi har:

$$2! \cdot 2! = 2 \cdot 2 = 4$$

og

$$(-1)^2 \cdot (-1) = 1 \cdot (-1) = -1.$$

Siden

$$4 \equiv -1 \pmod{5},$$

er det riktignok sant at

$$2! \cdot 2! \equiv (-1)^2 \cdot (-1) \pmod{5}.$$

Lemma 5.8.22. La p og q være primtall slik at $p > 2$ og $q > 2$. La p^{-1} være inversen til p modulo q. La q^{-1} være inversen modulo p. For hvert naturlig tall i slik at $i \leq p-1$, og hvert naturlig tall j slik at $j \leq \frac{q-1}{2}$, la oss betegne

$$qq^{-1}i + pp^{-1}j$$

som $u_{i,j}$.

La u være produktet av alle de naturlige tallene $u_{i,j}$ slik at $i \leq p-1$ og $j \leq \frac{q-1}{2}$. Da er:

(A) $u \equiv (-1)^{\frac{q-1}{2}} \pmod{p}$;

(B) $u \equiv (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{(p-1)(q-1)}{4}} \pmod{q}$.

Bevis. Vi gjør følgende observasjoner.

(1) La i være et naturlig tall slik at $i \leq p-1$. La j være et naturlig tall slik at $j \leq \frac{q-1}{2}$. Ut ifra Korollar 5.7.34 er

$$u_{i,j} \equiv j \pmod{q}.$$

(2) La u_i være produktet

$$u_{i,1}u_{i,2}\cdots u_{i,\frac{q-1}{2}}.$$

Det følger fra (1) at

$$u_i \equiv 1 \times 2 \times \cdots \times \frac{q-1}{2} \pmod{q},$$

altså at

$$u_i \equiv \left(\frac{q-1}{2}\right)! \pmod{q}.$$

(3) Vi har:

$$u = u_1 u_2 \cdots u_{p-1}.$$

Det følger fra (2) at

$$u \equiv \underbrace{\left(\frac{q-1}{2}\right)! \times \left(\frac{q-1}{2}\right)! \times \cdots \times \left(\frac{q-1}{2}\right)!}_{p-1 \text{ ganger}} \pmod{q}.$$

Dermed er

$$u \equiv \left(\left(\frac{q-1}{2}\right)!\right)^{p-1} \pmod{q},$$

altså er

$$u \equiv \left(\left(\left(\frac{q-1}{2}\right)!\right)^2\right)^{\frac{p-1}{2}} \pmod{q}.$$

(4) Ut ifra Korollar 5.8.19 er

$$\left(\left(\frac{q-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{q-1}{2}} \cdot (-1) \pmod{q}.$$

(5) Det følger fra (3) og (4) at

$$u \equiv \left((-1)^{\frac{q-1}{2}} \cdot (-1)\right)^{\frac{p-1}{2}} \pmod{q},$$

altså at

$$u \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \cdot (-1)^{\frac{p-1}{2}} \pmod{q}.$$

Således er (B) sant.

Vi gjør nå følgende observasjoner.

(1) La i være et naturlig tall slik at $i \leq p-1$. La j være et naturlig tall slik at $j \leq \frac{q-1}{2}$. Ut ifra Korollar 5.7.34 er

$$u_{i,j} \equiv i \pmod{p}.$$

(2) La u_j være produktet

$$u_{1,j}u_{2,j}\cdots u_{p-1,j}.$$

Det følger fra (1) at

$$u_j \equiv 1 \times 2 \times \cdots \times (p-1) \pmod{p},$$

altså at

$$u_j \equiv (p-1)! \pmod{p}.$$

(3) Ut ifra Proposisjon 4.15.8 er

$$(p-1)! \equiv -1 \pmod{p}.$$

(4) Det følger fra (2) og (3) at

$$u_j \equiv -1 \pmod{p}.$$

(5) Vi har:

$$u = u_1 u_2 \cdots u_{\frac{q-1}{2}}.$$

Det følger fra (4) at

$$u \equiv \underbrace{(-1) \times (-1) \times \cdots \times (-1)}_{\frac{q-1}{2} \text{ ganger}} \pmod{p},$$

altså at

$$u \equiv (-1)^{\frac{q-1}{2}} \pmod{p}.$$

Således er (A) sant.

□

Eksempel 5.8.23. La p være 3, og la q være 5. Ut ifra Eksempel 5.8.11, er

$$u \equiv 4 \pmod{15}.$$

Lemma 5.8.22 fastslår at

$$u \equiv (-1)^{\frac{5-1}{2}} \pmod{3}$$

og at

$$u \equiv (-1)^{\frac{3-1}{2}} \cdot (-1)^{\frac{(3-1)(5-1)}{4}} \pmod{5}.$$

Vi gjør følgende observasjoner.

(1) Vi har:

$$(-1)^{\frac{5-1}{2}} = (-1)^2 = 1.$$

(2) Siden

$$u \equiv 4 \pmod{15},$$

følger det fra Proposisjon 3.2.57 at

$$u \equiv 4 \pmod{3},$$

altså at

$$u \equiv 1 \pmod{3}.$$

Dermed ser vi at det riktignok er sant at

$$u \equiv (-1)^{\frac{5-1}{2}} \pmod{3}.$$

Nå gjør vi følgende observasjoner.

(1) Vi har:

$$\begin{aligned}(-1)^{\frac{3-1}{2}} \cdot (-1)^{\frac{(3-1)(5-1)}{4}} &= (-1)^1 \cdot (-1)^{\frac{2\cdot 4}{4}} \\ &= (-1) \cdot (-1)^2 \\ &= (-1) \cdot 1 \\ &= -1.\end{aligned}$$

(2) Siden

$$u \equiv 4 \pmod{15},$$

følger det fra Proposisjon 3.2.57 at

$$u \equiv 4 \pmod{5},$$

altså at

$$u \equiv -1 \pmod{5}.$$

Dermed ser vi at det riktignok er sant at

$$u \equiv (-1)^{\frac{3-1}{2}} \cdot (-1)^{\frac{(3-1)(5-1)}{4}} \pmod 5.$$

Eksempel 5.8.24. La p være 5, og la q være 7. Ut ifra Eksempel 5.8.13, er

$$u \equiv 29 \pmod{35}.$$

Lemma 5.8.22 fastslår at

$$u \equiv (-1)^{\frac{7-1}{2}} \pmod 5$$

og at

$$u \equiv (-1)^{\frac{5-1}{2}} \cdot (-1)^{\frac{(5-1)(7-1)}{4}} \pmod 7.$$

Vi gjør følgende observasjoner.

(1) Vi har:

$$(-1)^{\frac{7-1}{2}} = (-1)^3 = -1.$$

(2) Siden

$$u \equiv 29 \pmod{35},$$

følger det fra Proposisjon 3.2.57 at

$$u \equiv 29 \pmod 5,$$

altså at

$$u \equiv -1 \pmod 5.$$

Dermed ser vi at det riktignok er sant at

$$u \equiv (-1)^{\frac{7-1}{2}} \pmod 5.$$

Nå gjør vi følgende observasjoner.

(1) Vi har:

$$\begin{aligned}(-1)^{\frac{5-1}{2}} \cdot (-1)^{\frac{(5-1)(7-1)}{4}} &= (-1)^2 \cdot (-1)^{\frac{4\cdot 6}{4}} \\ &= 1 \cdot (-1)^6 \\ &= 1 \cdot 1 \\ &= 1.\end{aligned}$$

(2) Siden

$$u \equiv 29 \pmod{15},$$

følger det fra Proposisjon 3.2.57 at

$$u \equiv 29 \pmod 7,$$

altså at

$$u \equiv 1 \pmod 7.$$

Dermed ser vi at det riktignok er sant at

$$u \equiv (-1)^{\frac{5-1}{2}} \cdot (-1)^{\frac{(5-1)(7-1)}{4}} \pmod 5.$$

Lemma 5.8.25. La p og q være primtall slik at $p > 2$ og $q > 2$. La p og q være primtall slik at $p > 2$ og $q > 2$. La v være produktet av alle de naturlige tallene y slik at

$$y \leq \frac{pq-1}{2}$$

og verken $p \mid y$ eller $q \mid y$. Da er:

(A) $v \equiv (-1)^{\frac{q-1}{2}} \cdot \mathbb{L}_p^q \pmod p$;

(B) $v \equiv (-1)^{\frac{p-1}{2}} \cdot \mathbb{L}_q^p \pmod q$.

Bevis. For hvert heltall j slik at $0 \leq j \leq \frac{q-1}{2} - 1$, la w_j være produktet

$$\big(jp+1\big)\big(jp+2\big)\cdots\big(jp+(p-1)\big).$$

La $w_{\frac{q-1}{2}}$ være produktet

$$\left(\left(\frac{q-1}{2}\right)p+1\right)\left(\left(\frac{q-1}{2}\right)p+2\right)\cdots\left(\left(\frac{q-1}{2}\right)p+\frac{p-1}{2}\right),$$

altså produktet

$$\left(\left(\frac{q-1}{2}\right)p+1\right)\left(\left(\frac{q-1}{2}\right)p+2\right)\cdots\left(\frac{pq-1}{2}\right),$$

La w være produktet

$$w_1 \times w_2 \times \cdots \times w_{\frac{q-1}{2}}.$$

Vi gjør følgende observasjoner.

(1) La j være et heltall slik at

$$0 \leq j \leq \frac{q-1}{2}.$$

For hvert naturlig tall r slik at $r \leq p-1$, er

$$jp + r \equiv r \pmod p.$$

Det følger at

$$(jp+1)(jp+2)\cdots\big(jp+(p-1)\big) \equiv 1 \times 2 \times \cdots \times (p-1) \pmod p,$$

altså at

$$w_j \equiv (p-1)! \pmod p.$$

(2) Ut ifra Proposisjon 4.15.8 er

$$(p-1)! \equiv -1 \pmod{p}.$$

(3) Det følger fra (1) og (2) at, for hvert heltall j slik at $0 \leq i \leq \frac{q-1}{2} - 1$, er

$$w_j \equiv -1 \pmod{p}.$$

(4 Det følger fra (3) at

$$\begin{aligned} & w_0 \times w_1 \times \cdots \times w_{\frac{q-1}{2}-1} \\ & \equiv \underbrace{(-1) \times (-1) \times \cdots \times (-1)}_{\frac{q-1}{2} \text{ ganger}} \pmod{p}, \end{aligned}$$

altså

$$w_0 \times w_1 \times \cdots \times w_{\frac{q-1}{2}-1} \equiv (-1)^{\frac{q-1}{2}} \pmod{p}.$$

(5) Det følger fra (1) at

$$\begin{aligned} & \left(\left(\frac{q-1}{2}\right)p + 1\right) \times \left(\left(\frac{q-1}{2}\right)p + 2\right) \times \cdots \times \left(\left(\frac{q-1}{2}\right)p + \frac{p-1}{2}\right) \\ & \equiv 1 \times 2 \times \cdots \times \frac{p-1}{2} \pmod{p}, \end{aligned}$$

altså at

$$w_{\frac{q-1}{2}} \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

(6) Det følger fra (4) og (5) at

$$\begin{aligned} w &= \left(w_0 \times w_1 \cdots \times w_{\frac{q-1}{2}-1}\right) \times w_{\frac{q-1}{2}} \\ &\equiv (-1)^{\frac{q-1}{2}} \times \left(\frac{p-1}{2}\right)! \pmod{p}. \end{aligned}$$

(7) La t være produktet

$$q \times 2q \times \cdots \times \left(\frac{p-1}{2}\right) q.$$

Vi har:

$$w = vt.$$

(8) Vi har:

$$\begin{aligned} t &= q \times 2q \times \cdots \times \left(\frac{p-1}{2}\right) q \\ &= \left(1 \times 2 \times \cdots \times \left(\frac{p-1}{2}\right)\right) \times \underbrace{q \times q \times \cdots \times q}_{\frac{p-1}{2} \text{ ganger}} \\ &= \left(\frac{p-1}{2}\right)! \times q^{\frac{p-1}{2}}. \end{aligned}$$

(9) Ut ifra Proposisjon 5.3.2 er

$$\mathbb{L}_p^q \equiv q^{\frac{p-1}{2}} \pmod{p}.$$

(10) Det følger fra (8) og (9) at

$$t \equiv \left(\frac{p-1}{2}\right)! \times \mathbb{L}_p^q \pmod{p}.$$

(11) Ut ifra (6), (7) og (10) er

$$(-1)^{\frac{q-1}{2}} \times \left(\frac{p-1}{2}\right)! \equiv v \times \left(\frac{p-1}{2}\right)! \times \mathbb{L}_p^q \pmod{p},$$

altså er

$$(-1)^{\frac{q-1}{2}} \times \left(\frac{p-1}{2}\right)! \equiv v \times \mathbb{L}_p^q \times \left(\frac{p-1}{2}\right)! \pmod{p}.$$

(12) Siden p er et primtall, følger det fra (11) og Proposisjon 4.8.28 at

$$(-1)^{\frac{q-1}{2}} \equiv v \cdot \mathbb{L}_p^q \pmod{p}.$$

Det følger fra (12) at

$$(-1)^{\frac{q-1}{2}} \times \mathbb{L}_p^q \equiv v \times \mathbb{L}_p^q \times \mathbb{L}_p^q \pmod{p}.$$

Ut ifra Proposisjon 5.5.13 og Proposisjon 5.5.6 er

$$\mathbb{L}_p^q \times \mathbb{L}_p^q = \mathbb{L}_p^{q^2} = 1.$$

Vi konkluderer at

$$(-1)^{\frac{q-1}{2}} \times \mathbb{L}_p^q \equiv v \pmod{p},$$

altså at

$$v \equiv (-1)^{\frac{q-1}{2}} \times \mathbb{L}_p^q \pmod{p}.$$

Akkurat det samme argumentet, ved å bytte om p og q, fastslår at

$$v \equiv (-1)^{\frac{p-1}{2}} \times \mathbb{L}_q^p \pmod{q}.$$

□

Merknad 5.8.26. Leddene i produktet w er alle de naturlige tallene som er mindre enn eller like $\frac{pq-1}{2}$, og som ikke er delelig med q. Forskjellen mellom v og w er at de naturlige tallene mindre enn eller like $\frac{pq-1}{2}$ som er delelig med q er ledd av w, men ikke av v. Disse naturlige tallene er: q, $2q$, ..., $\left(\frac{p-1}{2}\right)q$. Siden t er produktet av disse naturlige tallene, får vi riktignok at $w = vt$. Produktene v og uw har nemlig de samme leddene: det er kun rekkefølgen som er ulik.

Merknad 5.8.27. Det er lett å overse at, siden vi teller fra 0 og ikke fra 1, har produktet

$$v_0 \times v_1 \times \cdots \times v_{\frac{q-1}{2}}$$

$\frac{q-1}{2}$ ledd, ikke $\frac{q-1}{2} - 1$ ledd. Det er derfor vi får at

$$w \equiv \underbrace{(-1) \times (-1) \times \cdots \times (-1)}_{\frac{q-1}{2} \text{ ganger}},$$

og ikke at

$$w \equiv \underbrace{(-1) \times (-1) \times \cdots \times (-1)}_{\frac{q-1}{2} - 1 \text{ ganger}}.$$

Eksempel 5.8.28. La p være 3, og la q være 5. Ut ifra Eksempel 5.8.11, er

$$v \equiv -4 \pmod{15}.$$

Lemma 5.8.25 fastslår at

$$v \equiv (-1)^{\frac{5-1}{2}} \cdot \mathbb{L}_3^5 \pmod{3}$$

og at

$$v \equiv (-1)^{\frac{3-1}{2}} \cdot \mathbb{L}_5^3 \pmod{5}.$$

Vi gjør følgende observasjoner.

(1) Siden

$$v \equiv -4 \pmod{15},$$

følger det fra Proposisjon 3.2.57 at

$$v \equiv -4 \pmod{3}.$$

Vi har:

$$-4 \equiv -1 \pmod{3}.$$

Derfor er

$$v \equiv -1 \pmod{3}.$$

(2) Ut ifra Proposisjon 5.5.3 er $\mathbb{L}_3^5 = \mathbb{L}_3^2$. Ut ifra Eksempel 5.4.5 er $\mathbb{L}_3^2 = -1$. Derfor er

$$(-1)^{\frac{5-1}{2}} \cdot \mathbb{L}_3^5 = (-1)^2 \cdot (-1) = 1 \cdot (-1) = -1.$$

Dermed er det riktignok sant at

$$v \equiv (-1)^{\frac{5-1}{2}} \cdot \mathbb{L}_3^5 \pmod 3.$$

Nå gjør vi følgende observasjoner.

(1) Siden

$$v \equiv -4 \pmod{15},$$

følger det fra Proposisjon 3.2.57 at

$$v \equiv -4 \pmod 5.$$

Vi har:

$$-4 \equiv 1 \pmod 5.$$

Derfor er

$$v \equiv 1 \pmod 5.$$

(2) Ut ifra Eksempel 5.4.6 er $\mathbb{L}_5^3 = -1$. Derfor er

$$(-1)^{\frac{3-1}{2}} \cdot \mathbb{L}_5^3 = (-1)^1 \cdot (-1) = (-1) \cdot (-1) = 1.$$

Dermed er det riktignok sant at

$$v \equiv (-1)^{\frac{3-1}{2}} \cdot \mathbb{L}_5^3 \pmod 5.$$

Eksempel 5.8.29. La p være 5, og la q være 7. Ut ifra Eksempel 5.8.13, er

$$v \equiv 6 \pmod{35}.$$

Lemma 5.8.25 fastslår at

$$v \equiv (-1)^{\frac{7-1}{2}} \cdot \mathbb{L}_5^7 \pmod 5$$

og at

$$v \equiv (-1)^{\frac{5-1}{2}} \cdot \mathbb{L}_7^5 \pmod 7.$$

Vi gjør følgende observasjoner.

(1) Siden

$$v \equiv 6 \pmod{35},$$

følger det fra Proposisjon 3.2.57 at

$$v \equiv 6 \pmod 5.$$

Vi har:

$$6 \equiv 1 \pmod 5.$$

Derfor er

$$v \equiv 1 \pmod 5.$$

(2) Ut ifra Proposisjon 5.5.3 er $\mathbb{L}_5^7 = \mathbb{L}_7^2$. Ut ifra Eksempel 5.4.7 er $\mathbb{L}_5^2 = -1$. Derfor er

$$(-1)^{\frac{7-1}{2}} \cdot \mathbb{L}_5^7 = (-1)^3 \cdot (-1) = (-1) \cdot (-1) = 1.$$

Dermed er det riktignok sant at

$$v \equiv (-1)^{\frac{7-1}{2}} \cdot \mathbb{L}_5^7 \pmod 5.$$

Nå gjør vi følgende observasjoner.

(1) Siden

$$v \equiv 6 \pmod{35},$$

følger det fra Proposisjon 3.2.57 at

$$v \equiv 6 \pmod 7.$$

Vi har:

$$6 \equiv -1 \pmod 7.$$

Derfor er

$$v \equiv -1 \pmod 7.$$

(2) Ut ifra Eksempel 5.4.7 er $\mathbb{L}_7^5 = -1$. Derfor er

$$(-1)^{\frac{5-1}{2}} \cdot \mathbb{L}_7^5 = (-1)^2 \cdot (-1) = 1 \cdot (-1) = -1.$$

Dermed er det riktignok sant at

$$v \equiv (-1)^{\frac{5-1}{2}} \cdot \mathbb{L}_7^5 \pmod 7.$$

Teorem 5.8.30. La p og q være primtall slik at $p \neq q$, $p > 2$, og $q > 2$. Da er

$$\mathbb{L}_q^p \cdot \mathbb{L}_p^q = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Bevis. La p^{-1} være inversen til p modulo q. La q^{-1} være inversen modulo p. For hvert naturlig tall i slik at $i \leq p-1$, og hvert naturlig tall j slik at $j \leq \frac{q-1}{2}$, la oss betegne

$$qq^{-1}i + pp^{-1}j$$

som $u_{i,j}$. La u være produktet av alle de naturlige tallene $u_{i,j}$ slik at $i \leq p-1$ og $j \leq \frac{q-1}{2}$.

La v være produktet av alle de naturlige tallene y slik at

$$y \leq \frac{pq-1}{2}$$

og verken $p \mid y$ eller $q \mid y$. Vi gjør følgende observasjoner.

(I) Ut ifra Lemma 5.8.22, er

$$u \equiv (-1)^{\frac{q-1}{2}} \pmod{p}$$

og

$$u \equiv (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{(p-1)(q-1)}{4}} \pmod{q}.$$

(II) Ut ifra Lemma 5.8.25 er

$$v \equiv (-1)^{\frac{q-1}{2}} \cdot \mathbb{L}_p^q \pmod{p}$$

og

$$v \equiv (-1)^{\frac{p-1}{2}} \cdot \mathbb{L}_q^p \pmod{q}.$$

Ut ifra Lemma 5.8.10, er ett av følgende sant:

(A) $u \equiv v \pmod{pq}$;

(B) $u \equiv -v \pmod{pq}$.

Anta først at (A) er sant. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 3.2.57 er da

$$u \equiv v \pmod{p}$$

og

$$u \equiv v \pmod{q}.$$

(2) Det følger fra (I), (II), og (1) at

$$(-1)^{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{2}} \mathbb{L}_p^q \pmod{p}.$$

(3) Det følger fra (2) og Proposisjon 4.8.28 at

$$1 \equiv \mathbb{L}_p^q \pmod{p}.$$

Siden enten $\mathbb{L}_p^q = 1$ eller $\mathbb{L}_p^q = -1$, følger det fra Proposisjon 5.3.10 at

$$1 = \mathbb{L}_p^q.$$

(4) Det følger fra (I), (II), og (1) at

$$(-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{(p-1)(q-1)}{4}} \equiv (-1)^{\frac{p-1}{2}} \cdot \mathbb{L}_q^p \pmod{q}.$$

(5) Det følger fra (4) og Proposisjon 4.8.28 at

$$(-1)^{\frac{(p-1)(q-1)}{4}} \equiv \mathbb{L}_q^p \pmod{q}.$$

(6) Ut ifra (3) er

$$\mathbb{L}_q^p = \mathbb{L}_q^p \cdot 1 = \mathbb{L}_q^p \mathbb{L}_p^q.$$

(7) Det følger fra (5) og (6) at

$$(-1)^{\frac{(p-1)(q-1)}{4}} \equiv \mathbb{L}_q^p \cdot \mathbb{L}_p^q \pmod{q},$$

altså at

$$\mathbb{L}_q^p \cdot \mathbb{L}_p^q \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \pmod{q}.$$

Siden begge sidene av denne kongruensen er enten -1 eller 1, følger det fra Proposisjon 5.3.10 at

$$\mathbb{L}_q^p \cdot \mathbb{L}_p^q = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Anta først at (B) er sant. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 3.2.57 er da

$$u \equiv -v \pmod{p}$$

og

$$u \equiv -v \pmod{q}.$$

(2) Det følger fra (I), (II), og (1) at

$$(-1)^{\frac{q-1}{2}} \equiv (-1) \cdot (-1)^{\frac{q-1}{2}} \mathbb{L}_p^q \pmod{p}.$$

(3) Det følger fra (2) og Proposisjon 4.8.28 at

$$-1 \equiv \mathbb{L}_p^q \pmod{p}$$

Siden enten $\mathbb{L}_p^q = 1$ eller $\mathbb{L}_p^q = -1$, følger det fra Proposisjon 5.3.10 at

$$-1 = \mathbb{L}_p^q.$$

(4) Det følger fra (I), (II), og (1) at

$$(-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{(p-1)(q-1)}{4}} \equiv (-1)(-1)^{\frac{p-1}{2}} \cdot \mathbb{L}_q^p \pmod{q}.$$

(5) Det følger fra (4) og Proposisjon 4.8.28 at

$$(-1)^{\frac{(p-1)(q-1)}{4}} \equiv (-1) \cdot \mathbb{L}_q^p \pmod{q}.$$

(6) Ut ifra (3) er

$$(-1) \cdot \mathbb{L}_q^p = \mathbb{L}_q^p \cdot (-1) = \mathbb{L}_q^p \cdot \mathbb{L}_p^q.$$

(7) Det følger fra (5) og (6) at

$$(-1)^{\frac{(p-1)(q-1)}{4}} \equiv \mathbb{L}_q^p \cdot \mathbb{L}_p^q \pmod{q},$$

altså at

$$\mathbb{L}_q^p \cdot \mathbb{L}_p^q \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \pmod{q}.$$

Siden begge sidene av denne kongruensen er enten -1 eller 1, følger det fra Proposisjon 5.3.10 at

$$\mathbb{L}_q^p \cdot \mathbb{L}_p^q = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

□

Merknad 5.8.31. Teorem 5.8.30 kalles *kvadratisk gjensidighet*.

Merknad 5.8.32. Teorem 5.8.30 er et svært dypt og viktig teorem. Fra et teoretisk synspunkt er det begynnelsen på en lang og fascinerende fortelling som strekker seg helt opp til én av de viktigste delene av dagens forskning i tallteori: *Langlands formodninger*.

Merknad 5.8.33. Det skal visstnok har blitt gitt minst 200 ulike beviser for Teorem 5.8.30! Det første riktige beviset ble gitt av Gauss rundt 1800. Imidlertid er beviset vi ga for Teorem 5.8.30 ganske nytt, og ikke spesielt velkjent: det ble først gitt rundt 1990. Det er sjeldent at vi på dette nivået ser på matematikk som er så ny!

Beviset vi ga for Teorem 5.8.30 er, blant bevisene jeg kjenner til for Teorem 5.8.30, det som bygger best på det vi har sett tidligere i kurset. Både Korollar 4.10.8, Proposisjon 4.15.8, og Proposisjon 5.3.2 dukker opp i løpet av beviset, og disse tre resultatene bygger på alle de andre viktige resultatene vi har sett på i kurset.

Et fint og begrepsmessig bevis for Teorem 5.8.30 kan gis ved å benytte litt *algebraisk tallteori*: teorien for syklomtomiske kropper. Jeg anbefaler kurset ≪Galoisteori≫ for å lære om teorien som fører til dette beviset.

Det finnes geometriske bevis for Teorem 5.8.30, bevis som benytter kompleks analyse, bevis som benytter litt gruppeteori, bevis som se på ikke linære diofantiske ligninger, bevis ved induksjon: alle slags bevis! Jeg liker beviset vi ga for Teorem 5.8.30 best blant de bevisene som er passende for dette kurset, og beviset som benytter teorien for syklotomiske kropper best av alt.

Eksempel 5.8.34. Teorem 5.8.30 fastslår at

$$\mathbb{L}_5^3 \cdot \mathbb{L}_3^5 = (-1)^{\frac{(3-1)(5-1)}{4}},$$

altså at

$$\mathbb{L}_5^3 \cdot \mathbb{L}_3^5 = (-1)^2 = 1.$$

Ut ifra Eksempel 5.4.6 er $\mathbb{L}_5^3 = -1$. Ut ifra Proposisjon 5.5.3 og Eksempel 5.4.5 er $\mathbb{L}_3^5 = \mathbb{L}_3^2 = -1$. Dermed er

$$\mathbb{L}_5^3 \cdot \mathbb{L}_3^5 = (-1) \cdot (-1) = 1,$$

altså er det riktignok sant at

$$\mathbb{L}_5^3 \cdot \mathbb{L}_3^5 = (-1)^{\frac{(3-1)(5-1)}{4}}.$$

Eksempel 5.8.35. Teorem 5.8.30 fastslår at

$$\mathbb{L}_7^3 \cdot \mathbb{L}_3^7 = (-1)^{\frac{(3-1)(7-1)}{4}},$$

altså at

$$\mathbb{L}_7^3 \cdot \mathbb{L}_3^7 = (-1)^3 = -1.$$

Ut ifra Eksempel 5.4.7 er $\mathbb{L}_7^3 = -1$. Ut ifra Proposisjon 5.5.3 og Eksempel 5.4.5 er $\mathbb{L}_3^7 = \mathbb{L}_3^1 = 1$. Dermed er

$$\mathbb{L}_7^3 \cdot \mathbb{L}_3^7 = (-1) \cdot 1 = -1,$$

altså er det riktignok sant at

$$\mathbb{L}_7^3 \cdot \mathbb{L}_3^7 = (-1)^{\frac{(3-1)(7-1)}{4}}.$$

5.9 Korollarer til kvadratisk gjensidighet

Merknad 5.9.1. I praksis benytter vi typisk ikke Teorem 5.8.30 selv, men et par korollarer som vi kommer til å gi et bevis for i denne delen av kapittelet: Korollar 5.9.2 og Korollar 5.9.21.

Korollar 5.9.2. La p og q være primtall slik at $p > 2$, $q > 2$, og $p \neq q$. Dersom

$$p \equiv 1 \pmod 4$$

eller

$$q \equiv 1 \pmod 4,$$

er

$$\mathbb{L}_q^p = \mathbb{L}_p^q.$$

Ellers er

$$\mathbb{L}_q^p = -\mathbb{L}_p^q.$$

Bevis. Siden p er et primtall slik at $p > 2$, fastslår det samme argumentet som i begynnelsen av beviset for Proposisjon 5.3.15 at ett av følgende er sant:

(1) $p \equiv 1 \pmod 4$;

(2) $p \equiv 3 \pmod 4$.

På lignende vis er ett av følgende sant.

(1) $q \equiv 1 \pmod 4$;

(2) $q \equiv 3 \pmod 4$.

Derfor er ett av følgende sant.

(A) $p \equiv 1 \pmod 4$;

(B) $q \equiv 1 \pmod 4$;

(C) $p \equiv 3 \pmod 4$ og $q \equiv 3 \pmod 4$.

Anta først at (A) er sant. Da har vi: $4 \mid p-1$. Dermed finnes det et naturlig tall k slik at $p-1 = 4k$. Da er

$$\begin{aligned}
(-1)^{\frac{(p-1)(q-1)}{4}} &= \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} \\
&= \left((-1)^{\frac{4k}{2}}\right)^{\frac{q-1}{2}} \\
&= \left((-1)^{2k}\right)^{\frac{q-1}{2}} \\
&= \left(\left((-1)^2\right)^k\right)^{\frac{q-1}{2}} \\
&= \left(1^k\right)^{\frac{q-1}{2}} \\
&= 1^{\frac{q-1}{2}} \\
&= 1.
\end{aligned}$$

Da følger det fra Teorem 5.8.30 at

$$\mathbb{L}_q^p \cdot \mathbb{L}_p^q = 1.$$

Dermed er

$$\mathbb{L}_q^p \cdot \mathbb{L}_p^q \cdot \mathbb{L}_p^q = \mathbb{L}_p^q.$$

Ut ifra Proposisjon 5.5.13 og Proposisjon 5.5.13 er

$$\mathbb{L}_p^q \cdot \mathbb{L}_p^q = \mathbb{L}_p^{q^2} = 1.$$

Vi konkluderer at

$$\mathbb{L}_q^p = \mathbb{L}_p^q.$$

Anta nå at (B) er sant. Akurat det samme argumentet, ved å bytte om p og q, som i tilfellet (A) er sant fastslår da at

$$\mathbb{L}_q^p = \mathbb{L}_p^q.$$

Anta nå at (C) er sant. Da har vi: $4 \mid p-3$ og $4 \mid q-3$, altså finnes det et naturlig

tall k slik at $p-3=4k$ og et naturlig tall l slik at $q-3=4l$. Da er

$$\begin{aligned}
(-1)^{\frac{(p-1)(q-1)}{4}} &= \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} \\
&= \left((-1)^{\frac{p-3}{2}+1}\right)^{\frac{q-3}{2}+1} \\
&= \left((-1)^{\frac{4k}{2}+1}\right)^{\frac{4l}{2}+1} \\
&= \left((-1)^{2k+1}\right)^{2l+1} \\
&= \left(\left((-1)^2\right)^k \cdot (-1)\right)^{2l+1} \\
&= \left(1^k \cdot (-1)\right)^{2l+1} \\
&= (1 \cdot (-1))^{2l+1} \\
&= (-1)^{2l+1} \\
&= \left((-1)^2\right)^l \cdot (-1) \\
&= 1^l \cdot (-1) \\
&= 1 \cdot (-1) \\
&= -1.
\end{aligned}$$

Da følger det fra Teorem 5.8.30 at

$$\mathbb{L}_q^p \cdot \mathbb{L}_p^q = -1.$$

Dermed er

$$\mathbb{L}_q^p \cdot \mathbb{L}_p^q \cdot \mathbb{L}_p^q = -\mathbb{L}_p^q.$$

Ut ifra Proposisjon 5.5.13 og Proposisjon 5.5.6 er

$$\mathbb{L}_p^q \cdot \mathbb{L}_p^q = \mathbb{L}_p^{q^2} = 1.$$

Vi konkluderer at

$$\mathbb{L}_q^p = -\mathbb{L}_p^q.$$

□

Eksempel 5.9.3. Ut ifra Eksempel 5.4.7 er $\mathbb{L}_7^5 = -1$. Siden $5 \equiv 1 \pmod 4$, fastslår Korollar 5.9.2 at $\mathbb{L}_5^7 = \mathbb{L}_7^5 = -1$. Siden

$$7 \equiv 2 \pmod 5,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_5^7 = \mathbb{L}_5^2$. Ut ifra Eksempel 5.4.7 er $\mathbb{L}_5^2 = -1$, altså er det riktignok sant at $\mathbb{L}_5^7 = -1$.

Eksempel 5.9.4. Ut ifra Eksempel 5.4.8 er $\mathbb{L}_{11}^3 = 1$. Siden $11 \equiv 3 \pmod 4$, fastslår Korollar 5.9.2 at $\mathbb{L}_3^{11} = -\mathbb{L}_{11}^3 = -1$. Siden

$$11 \equiv 2 \pmod 3,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_3^{11} = \mathbb{L}_3^2$. Ut ifra Eksempel 5.4.7 er $\mathbb{L}_3^2 = -1$, altså er det riktignok sant at $\mathbb{L}_3^{11} = -1$.

Merknad 5.9.5. Hvis verken

$$p \equiv 1 \pmod 4$$

eller

$$q \equiv 1 \pmod 4,$$

er

$$p \equiv 3 \pmod 4$$

og

$$q \equiv 3 \pmod 4.$$

Med andre ord fastslår Korollar 5.9.2 at

$$\mathbb{L}_q^p = \mathbb{L}_p^q$$

dersom

$$p \equiv 1 \pmod 4$$

eller

$$q \equiv 1 \pmod 4,$$

og at

$$\mathbb{L}_q^p = -\mathbb{L}_p^q$$

dersom

$$p \equiv 3 \pmod 4$$

og

$$q \equiv 3 \pmod 4.$$

Korollar 5.9.2 sier ikke:

$$\mathbb{L}_q^p = \mathbb{L}_p^q$$

dersom akkurat ett av utsagn

$$p \equiv 1 \pmod 4$$

og

$$q \equiv 1 \pmod 4$$

er sant. At

$$\mathbb{L}_q^p = \mathbb{L}_p^q$$

når både

$$p \equiv 1 \pmod 4$$

og

$$q \equiv 1 \pmod 4.$$

Korollar 5.9.6. La p og q være primtall slik at $p > 2$, $q > 2$, og $p \neq q$. Anta at

$$p \equiv 3 \pmod 4.$$

Da er $\mathbb{L}_p^q = \mathbb{L}_q^{-p}$.

Bevis. Siden p er et primtall slik at $p > 2$, fastslår det samme argumentet som i begynnelsen av beviset for Proposisjon 5.3.15 at ett av følgende er sant:

(A) $q \equiv 1 \pmod 4$;

(B) $q \equiv 3 \pmod 4$.

Anta først at (A) er sant. Vi gjør følgende observasjoner.

(1) Da følger det fra Korollar 5.9.2 at $\mathbb{L}_p^q = \mathbb{L}_q^p$.

(2) Vi har: $\mathbb{L}_q^p = \mathbb{L}_q^{(-1)\cdot(-p)}$. Ut ifra Proposisjon 5.5.13 er da $\mathbb{L}_q^p = \mathbb{L}_q^{-1} \cdot \mathbb{L}_q^{-p}$.

(3) Ut ifra Proposisjon 5.5.16 er $\mathbb{L}_q^{-1} = (-1)^{\frac{q-1}{2}}$. Siden

$$q \equiv 1 \pmod 4,$$

fastslår det samme argumentet som i beviset for Korollar 5.9.2 at $(-1)^{\frac{q-1}{2}} = 1$. Dermed er $\mathbb{L}_q^{-1} = 1$.

Det følger fra (1) – (3) at $\mathbb{L}_p^q = \mathbb{L}_q^{-p}$.

Anta nå at (B) er sant. Vi gjør følgende observasjoner.

(1) Siden da både

$$p \equiv 3 \pmod 4$$

og

$$q \equiv 3 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_p^q = -\mathbb{L}_q^p$.

(2) Vi har: $\mathbb{L}_q^p = \mathbb{L}_q^{(-1)\cdot(-p)}$. Ut ifra Proposisjon 5.5.13 er da $\mathbb{L}_q^p = \mathbb{L}_q^{-1} \cdot \mathbb{L}_q^{-p}$.

(3) Ut ifra Proposisjon 5.5.16 er $\mathbb{L}_q^{-1} = (-1)^{\frac{q-1}{2}}$. Siden

$$q \equiv 3 \pmod 4,$$

fastslår det samme argumentet som i beviset for Korollar 5.9.2 at $(-1)^{\frac{q-1}{2}} = -1$.

Det følger fra (1) – (3) at $\mathbb{L}_p^q = -\left(-\mathbb{L}_q^{-p}\right)$, altså at $\mathbb{L}_p^q = \mathbb{L}_q^{-p}$.

□

Eksempel 5.9.7. Ut ifra Eksempel 5.4.7 er $\mathbb{L}_7^3 = -1$. Siden

$$7 \equiv 3 \pmod 4,$$

fastslår da Korollar 5.9.6 at $\mathbb{L}_3^{-7} = -1$. Siden

$$-7 \equiv 2 \pmod 3,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_3^{-7} = \mathbb{L}_3^2$. Ut ifra Eksempel 5.4.5 er $\mathbb{L}_3^2 = -1$, altså er det riktignok sant at $\mathbb{L}_3^{-7} = -1$.

Eksempel 5.9.8. Ut ifra Eksempel 5.4.8 er $\mathbb{L}_{11}^5 = 1$. Siden

$$11 \equiv 3 \pmod 4,$$

fastslår da Korollar 5.9.6 at $\mathbb{L}_5^{-11} = 1$. Siden

$$-11 \equiv 4 \pmod 5,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_5^{-11} = \mathbb{L}_5^4$. Ut ifra Eksempel 5.4.6 er $\mathbb{L}_5^4 = -1$, altså er det riktignok sant at $\mathbb{L}_5^{-11} = 1$.

Lemma 5.9.9. La a og b være oddetall. Da er

$$\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod 2.$$

Bevis. Vi gjør følgende observasjoner.

(1) Siden a er et oddetall, er

$$a \equiv 1 \pmod 2,$$

altså har vi: $2 \mid a-1$. Dermed finnes det et naturlig tall k slik at $a - 1 = 2k$.

(2) Siden b er et oddetall, er

$$b \equiv 1 \pmod 2,$$

altså har vi: $2 \mid b-1$. Dermed finnes det et naturlig tall l slik at $b - 1 = 2l$.

(3) Siden

$$a \equiv 1 \pmod 2$$

og

$$b \equiv 1 \pmod 2,$$

er

$$ab \equiv 1 \pmod 2,$$

altså har vi: $2 \mid ab-1$. Dermed finnes det et naturlig tall m slik at $ab - 1 = 2m$.

(4) Det følger fra (1) og (2) at

$$(a-1)(b-1) = 4kl,$$

altså er

$$(a-1)(b-1) \equiv 0 \pmod 4.$$

(5) Vi har:

$$\begin{aligned}(a-1)(b-1) &= ab - a - b + 1 \\ &= (ab-1) - (a-1) - (b-1).\end{aligned}$$

Dermed følger det fra (4) at

$$(ab-1) - (a-1) - (b-1) \equiv 0 \pmod 4.$$

(6) Vi har:

$$\begin{aligned}(ab-1) - (a-1) - (b-1) &= 2m - 2k - 2l \\ &= 2(m-k-l).\end{aligned}$$

Dermed følger det fra (5) at

$$2(m-k-l) \equiv 0 \pmod 4.$$

Siden $2 \mid 4$, følger det fra Proposisjon 3.2.54 at

$$m-k-l \equiv 0 \pmod 2,$$

altså at

$$\frac{ab-1}{2} - \frac{a-1}{2} - \frac{b-1}{2} \equiv 0 \pmod 2.$$

Dermed er

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2.$$

□

Eksempel 5.9.10. Lemma 5.9.9 fastslår at

$$\frac{13-1}{2} + \frac{17-1}{2} \equiv \frac{13 \cdot 17 - 1}{2} \pmod 2,$$

altså at

$$6 + 8 \equiv 110 \pmod 2.$$

Siden både

$$6 + 8 = 14 \equiv 0 \pmod 2$$

og

$$110 \equiv 0 \pmod 2,$$

er dette riktignok sant.

Eksempel 5.9.11. Lemma 5.9.9 fastslår at

$$\frac{19-1}{2}+\frac{5-1}{2}\equiv\frac{19\cdot 5-1}{2} \pmod 2,$$

altså at

$$9+2\equiv 47 \pmod 2.$$

Siden både

$$9+2=11\equiv 1 \pmod 2$$

og

$$47\equiv 1 \pmod 2,$$

er dette riktignok sant.

Lemma 5.9.12. La t være et naturlig tall. For hvert naturlig tall i slik at $i\leq t$, la p_i være et primtall slik at $p_i>2$. Da er

$$\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_t-1}{2}\equiv\frac{p_1\cdots p_t-1}{2} \pmod 2.$$

Bevis. At lemmaet er sant når $t=1$ er tautologisk. Anta at lemmaet har blitt bevist når $t=m$, hvor m er et gitt naturlig tall. Således har det blitt bevist at

$$\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_m-1}{2}\equiv\frac{p_1p_2\cdots p_m-1}{2} \pmod 2.$$

Vi gjør følgende observasjoner.

(1) Da er

$$\begin{aligned}&\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_m-1}{2}+\frac{p_{m+1}-1}{2}\\ &\equiv\frac{p_1p_2\cdots p_m-1}{2}+\frac{p_{m+1}-1}{2} \pmod 2.\end{aligned}$$

(2) Siden $p_i>2$ for hvert naturlig tall i slik at $i\leq m+1$, er p_i et oddetall for hvert naturlig tall i slik at $i\leq m+1$. Dermed er

$$p_i\equiv 1 \pmod 2$$

for hvert naturlig tall i slik at $i\leq m+1$. Det følger at

$$p_1p_2\cdots p_m\equiv 1 \pmod 2.$$

Dermed er

$$p_1p_2\cdots p_m$$

et oddetall. I tillegg er p_{m+1} er et oddetall.

(3) Det følger fra (2) og Lemma 5.9.9 at

$$\frac{p_1 p_2 \cdots p_m - 1}{2} + \frac{p_{m+1} - 1}{2} \equiv \frac{p_1 \cdots p_{m+1} - 1}{2} \pmod 2.$$

(4) Det følger fra (1) og (3) at

$$\frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} + \cdots + \frac{p_m - 1}{2} + \frac{p_{m+1} - 1}{2} \equiv \frac{p_1 \cdots p_{m+1} - 1}{2} \pmod 2.$$

Således er lemmaet sant når $n = m + 1$.

Ved induksjon konkluderer vi at lemmaet er sant for et hvilket som helst naturlig tall t.

□

Eksempel 5.9.13. Lemma 5.9.12 fastslår at

$$\frac{3-1}{2} + \frac{11-1}{2} + \frac{13-1}{2} \equiv \frac{3 \cdot 11 \cdot 13 - 1}{2} \pmod 2,$$

altså at

$$1 + 5 + 6 \equiv \frac{1595 - 1}{2} = \frac{429 - 1}{2} \pmod 2.$$

Siden både

$$1 + 5 + 6 = 12 \equiv 0 \pmod 2$$

og

$$214 \equiv 0 \pmod 2,$$

er dette riktignok sant.

Eksempel 5.9.14. Lemma 5.9.12 fastslår at

$$\frac{5-1}{2} + \frac{11-1}{2} + \frac{29-1}{2} \equiv \frac{5 \cdot 11 \cdot 29 - 1}{2} \pmod 2,$$

altså at

$$2 + 5 + 14 \equiv \frac{1595 - 1}{2} = 797 \pmod 2.$$

Siden både

$$2 + 5 + 14 = 21 \equiv 1 \pmod 2$$

og

$$797 \equiv 1 \pmod 2,$$

er dette riktignok sant.

Lemma 5.9.15. La m og n være naturlige tall slik at

$$s \equiv t \pmod 2.$$

Da er

$$(-1)^s = (-1)^t.$$

Bevis. Anta at $s \leq t$. Siden

$$s \equiv t \pmod 2,$$

finnes det et naturlig tall k slik at $s - t = 2k$, altså at $s = t + 2k$. Da er

$$\begin{aligned}(-1)^s &= (-1)^{t+2k} \\ &= (-1)^t \cdot (-1)^{2k} \\ &= (-1)^t \cdot \left((-1)^2\right)^k \\ &= (-1)^t \cdot 1^k \\ &= (-1)^t \cdot 1 \\ &= (-1)^t.\end{aligned}$$

Akkurat det samme argumentet, ved å bytte om s og t, fastslår at $(-1)^s = (-1)^t$ når $s > t$. □

Eksempel 5.9.16. Siden

$$3 \equiv 7 \pmod 2,$$

fastslår Lemma 5.9.15 at $(-1)^3 = (-1)^7$. Siden både $(-1)^3 = -1$ og $(-1)^7 = -1$, er dette riktignok sant.

Eksempel 5.9.17. Siden

$$4 \equiv 10 \pmod 2,$$

fastslår Lemma 5.9.15 at $(-1)^4 = (-1)^{10}$. Siden både $(-1)^4 = 1$ og $(-1)^{10} = 1$, er dette riktignok sant.

Lemma 5.9.18. La t være et naturlig tall. For hvert naturlig tall i slik at $i \leq t$, la p_i være et primtall. La n være produktet

$$p_1 p_2 \cdots p_t.$$

Da er

$$\mathbb{L}_{p_1}^{-1} \cdot \mathbb{L}_{p_2}^{-1} \cdots \mathbb{L}_{p_t}^{-1} = (-1)^{\frac{n-1}{2}}.$$

Bevis. Ut ifra Proposisjon 5.5.16 er, for hvert naturlig tall i slik at $i \leq t$,

$$\mathbb{L}_{p_i}^{-1} = (-1)^{\frac{p_i - 1}{2}}.$$

Derfor er

$$\begin{aligned}\mathbb{L}_{p_1}^{-1} \cdot \mathbb{L}_{p_2}^{-1} \cdots \mathbb{L}_{p_t}^{-1} &= (-1)^{\frac{p_1-1}{2}} \cdot (-1)^{\frac{p_2-1}{2}} \cdots (-1)^{\frac{p_t-1}{2}} \\ &= (-1)^{\frac{p_1-1}{2} + \frac{p_2-1}{2} + \cdots + \frac{p_t-1}{2}}\end{aligned}$$

Ut ifra Lemma 5.9.12 er

$$\frac{p_1 + p_2 + \cdots + p_t - 1}{2} \equiv \frac{p_1 \cdots p_t - 1}{2} \pmod 2.$$

Da følger det fra Lemma 5.9.15 at

$$(-1)^{\frac{p_1+p_2+\cdots+p_t-1}{2}} = (-1)^{\frac{p_1\cdots p_t-1}{2}}.$$

Dermed er

$$\mathbb{L}_{p_1}^{-1} \cdot \mathbb{L}_{p_2}^{-1} \cdots \mathbb{L}_{p_t}^{-1} = (-1)^{\frac{p_1\cdots p_t-1}{2}},$$

altså er

$$\mathbb{L}_{p_1}^{-1} \cdot \mathbb{L}_{p_2}^{-1} \cdots \mathbb{L}_{p_t}^{-1} = (-1)^{\frac{n-1}{2}}.$$

□

Eksempel 5.9.19. Lemma 5.9.18 fastslår at

$$\mathbb{L}_5^{-1} \cdot \mathbb{L}_7^{-1} = (-1)^{\frac{5\cdot 7-1}{2}},$$

altså at

$$\mathbb{L}_5^{-1} \cdot \mathbb{L}_7^{-1} = (-1)^{17} = -1.$$

Ut ifra Proposisjon 5.5.3, Eksempel 5.4.6, og Eksempel 5.4.7 er

$$\begin{aligned} \mathbb{L}_5^{-1} \cdot \mathbb{L}_7^{-1} &= \mathbb{L}_5^4 \cdot \mathbb{L}_7^6 \\ &= 1 \cdot (-1) \\ &= -1. \end{aligned}$$

Dermed er det riktignok sant at

$$\mathbb{L}_5^{-1} \cdot \mathbb{L}_7^{-1} = (-1)^{\frac{5\cdot 7-1}{2}}.$$

Eksempel 5.9.20. Lemma 5.9.18 fastslår at

$$\mathbb{L}_3^{-1} \cdot \mathbb{L}_7^{-1} \cdot \mathbb{L}_{11}^{-1} = (-1)^{\frac{3\cdot 7\cdot 11-1}{2}},$$

altså at

$$\mathbb{L}_3^{-1} \cdot \mathbb{L}_7^{-1} \cdot \mathbb{L}_{11}^{-1} = (-1)^{115} = -1.$$

Ut ifra Proposisjon 5.5.3, Eksempel 5.4.5, Eksempel 5.4.5, og Eksempel 5.4.5 er

$$\begin{aligned} \mathbb{L}_3^{-1} \cdot \mathbb{L}_7^{-1} \cdot \mathbb{L}_{11}^{-1} &= \mathbb{L}_3^2 \cdot \mathbb{L}_7^6 \cdot \mathbb{L}_{11}^{10} \\ &= (-1) \cdot (-1) \cdot (-1) \\ &= -1. \end{aligned}$$

Dermed er det riktignok sant at

$$\mathbb{L}_3^{-1} \cdot \mathbb{L}_7^{-1} \cdot \mathbb{L}_{11}^{-1} = (-1)^{\frac{3\cdot 7\cdot 11-1}{2}}.$$

Korollar 5.9.21. La p være et primtall slik at $p > 2$. Dersom

$$p \equiv 1 \pmod 8$$

eller

$$p \equiv 7 \pmod 8,$$

er $\mathbb{L}_p^2 = 1$. Ellers er $\mathbb{L}_p^2 = -1$.

Bevis. Siden p er et primtall slik at $p > 2$, fastslår det samme argumentet som i begynnelsen av beviset for Proposisjon 5.3.15 at ett av følgende er sant:

(A) $p \equiv 1 \pmod 4$;

(B) $p \equiv 3 \pmod 4$.

Anta først at (A) er sant. Anta at $2 \mid \frac{p+1}{2}$. Da finnes det et naturlig tall k slik at $\frac{p+1}{2} = 2k$. Derfor er $p + 1 = 4k$, altså er

$$p + 1 \equiv 0 \pmod 4.$$

Dermed er

$$p \equiv -1 \pmod 4,$$

altså er

$$p \equiv 3 \pmod 4.$$

Ut ifra Proposisjon 3.2.11 og antakelsen at (A) er sant, er dette umulig. Vi konkluderer at det ikke er sant at $2 \mid \frac{p+1}{2}$, altså at $\frac{p+1}{2}$ er et oddetall.

Vi gjør følgende observasjoner.

(1) Vi har:

$$2 + 2p = 2(p + 1) = 2 \cdot 2 \cdot \left(\frac{p+1}{2} \right),$$

altså

$$2 + 2p = 4 \left(\frac{p+1}{2} \right).$$

(2) Siden

$$2 \equiv 2 + 2p \pmod p,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_p^2 = \mathbb{L}_p^{2+2p}$. Ut ifra (1) er da $\mathbb{L}_p^2 = \mathbb{L}_p^{4\left(\frac{p+1}{2}\right)}$.

(3) Ut ifra Proposisjon 5.5.13 og Proposisjon 5.5.6 er

$$\mathbb{L}_p^{4\left(\frac{p+1}{2}\right)} = \mathbb{L}_p^4 \cdot \mathbb{L}_p^{\frac{p+1}{2}} = \mathbb{L}_p^{2^2} \cdot \mathbb{L}_p^{\frac{p+1}{2}} = 1 \cdot \mathbb{L}_p^{\frac{p+1}{2}} = \mathbb{L}_p^{\frac{p+1}{2}}.$$

(4) Ut ifra Teorem 4.3.3, finnes det et naturlig tall t og primtall $q_1, q_2, \ldots, q_t$ slik at

$$\frac{p+1}{2} = q_1 \cdots q_t.$$

(5) Ut ifra Proposisjon 5.5.13 er da

$$\mathbb{L}_p^{\frac{p+1}{2}} = \mathbb{L}_p^{q_1 q_2 \cdots q_t} = \mathbb{L}_p^{q_1} \mathbb{L}_p^{q_2} \cdots \mathbb{L}_p^{q_t}.$$

(6) Siden

$$p \equiv 1 \mod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_p^{q_i} = \mathbb{L}_{q_i}^p$ for hvert naturlig tall i slik at $i \leq t$. Dermed er

$$\mathbb{L}_p^{q_1} \mathbb{L}_p^{q_2} \cdots \mathbb{L}_p^{q_t} = \mathbb{L}_{q_1}^p \cdot \mathbb{L}_{q_2}^p \cdots \mathbb{L}_{q_t}^p.$$

(7) Vi har:

$$p = 2\left(\frac{p+1}{2}\right) - 1.$$

For hvert naturlig tall $i \leq t$, er

$$\frac{p+1}{2} = (q_1 \cdots q_{i-1} q_{i+1} \cdots q_t)\, q_i,$$

altså har vi: $q_i \mid \frac{p+1}{2}$. Dermed er

$$\frac{p+1}{2} \equiv 0 \pmod{q_i}.$$

Det følger at

$$2\left(\frac{p+1}{2}\right) - 1 \equiv 2 \cdot 0 - 1 = -1 \pmod{q_i},$$

altså er

$$p \equiv -1 \pmod{q_i}.$$

(8) Det følger fra (7) og Proposisjon 5.5.3 at

$$\mathbb{L}_{q_1}^p \cdot \mathbb{L}_{q_2}^p \cdots \mathbb{L}_{q_t}^p = \mathbb{L}_{q_1}^{-1} \cdot \mathbb{L}_{q_2}^{-1} \cdots \mathbb{L}_{q_t}^{-1}.$$

(9) Ut ifra Lemma 5.9.18 er

$$\mathbb{L}_{q_1}^{-1} \cdot \mathbb{L}_{q_2}^{-1} \cdots \mathbb{L}_{q_t}^{-1} = (-1)^{\frac{q_1 q_2 \cdots q_t - 1}{2}} = (-1)^{\frac{\frac{p+1}{2} - 1}{2}} = (-1)^{\frac{p-1}{4}}.$$

Det følger fra (2), (3), (5), og (7) – (10) at

$$\mathbb{L}_p^2 = (-1)^{\frac{p-1}{4}}.$$

Siden

$$p \equiv 1 \pmod 4,$$

følger det fra Korollar 3.2.63 at ett av følgende er sant.

(I) $p \equiv 1 \pmod 8$;

(II) $p \equiv 5 \pmod 8$.

Dersom (I) er sant, finnes det et naturlig tall k slik at $p - 1 = 8k$. Da er

$$\begin{aligned}(-1)^{\frac{p-1}{4}} &= (-1)^{2k} \\ &= \left((-1)^2\right)^k \\ &= 1^k \\ &= 1.\end{aligned}$$

Dermed er $\mathbb{L}_p^2 = 1$.

Dersom (II) er sant, finnes det et naturlig tall k slik at $p - 5 = 8k$. Da er

$$\begin{aligned}(-1)^{\frac{p-1}{4}} &= (-1)^{\frac{p-5}{4}+1} \\ &= (-1)^{\frac{p-5}{4}} \cdot (-1) \\ &= (-1)^{2k} \cdot (-1) \\ &= \left((-1)^2\right)^k \cdot (-1) \\ &= 1^k \cdot (-1) \\ &= 1 \cdot (-1) \\ &= -1.\end{aligned}$$

Dermed er $\mathbb{L}_p^2 = -1$.

Således er korollaret sant dersom (A) er sant.

Anta nå at (B) er sant. Anta at $2 \mid \frac{p-1}{2}$. Da finnes det et naturlig tall k slik at $\frac{p-1}{2} = 2k$. Da er $p - 1 = 4k$, altså er

$$p - 1 \equiv 0 \pmod 4.$$

Dermed er

$$p \equiv 1 \pmod 4.$$

Ut ifra Proposisjon 3.2.11 og antakelsen at (B) er sant, er dette umulig. Vi konkluderer at det ikke er sant at $2 \mid \frac{p-1}{2}$, altså at $\frac{p-1}{2}$ er et oddetall.

Vi gjør følgende observasjoner.

(1) Vi har: $\mathbb{L}_p^2 = \mathbb{L}_p^{(-1)\cdot(-2)}$. Ut ifra Proposisjon 5.5.13 er $\mathbb{L}_p^{(-1)\cdot(-2)} = \mathbb{L}_p^{-1} \cdot \mathbb{L}_p^{-2}$.

(2) Ut ifra Proposisjon 5.5.16 er $\mathbb{L}_p^{-1} = (-1)^{\frac{p-1}{2}}$. Siden

$$p \equiv 3 \pmod 4,$$

fastslår det samme argumentet som i beviset for Korollar 5.9.2 at $(-1)^{\frac{p-1}{2}} = -1$. Dermed er $\mathbb{L}_p^{-1} = -1$.

(3) Vi har:

$$-2 + 2p = 2(p-1) = 2 \cdot 2 \cdot \left(\frac{p-1}{2}\right),$$

altså

$$-2 + 2p = 4\left(\frac{p-1}{2}\right).$$

(4) Siden

$$-2 \equiv -2 + 2p \equiv p,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_p^{-2} = \mathbb{L}_p^{2+2p}$. Ut ifra (1) er da $\mathbb{L}_p^{-2} = \mathbb{L}_p^{4\left(\frac{p-1}{2}\right)}$.

(5) Ut ifra Proposisjon 5.5.13 og Proposisjon 5.5.6 er

$$\mathbb{L}_p^{4\left(\frac{p-1}{2}\right)} = \mathbb{L}_p^4 \cdot \mathbb{L}_p^{\frac{p-1}{2}} = \mathbb{L}_p^{2^2} \cdot \mathbb{L}_p^{\frac{p-1}{2}} = 1 \cdot \mathbb{L}_p^{\frac{p-1}{2}} = \mathbb{L}_p^{\frac{p-1}{2}}.$$

(6) Ut ifra Teorem 4.3.3, finnes det et naturlig tall t og primtall q_1, q_2, …, q_t slik at

$$\frac{p-1}{2} = q_1 \cdots q_t.$$

(7) Ut ifra Proposisjon 5.5.13 er da

$$\mathbb{L}_p^{\frac{p-1}{2}} = \mathbb{L}_p^{q_1 \cdots q_t} = \mathbb{L}_p^{q_1} \mathbb{L}_p^{q_2} \cdots \mathbb{L}_p^{q_t}.$$

(8) Siden

$$p \equiv 3 \pmod 4,$$

følger det fra Korollar 5.9.6 at $\mathbb{L}_p^{q_i} = \mathbb{L}_{q_i}^{-p}$ for hvert naturlig tall i slik at $i \leq t$. Dermed er

$$\mathbb{L}_p^{q_1} \mathbb{L}_p^{q_2} \cdots \mathbb{L}_p^{q_t} = \mathbb{L}_{q_1}^{-p} \cdot \mathbb{L}_{q_2}^{-p} \cdots \mathbb{L}_{q_t}^{-p}.$$

(9) Vi har:

$$-p = -2\left(\frac{p-1}{2}\right) - 1.$$

For hvert naturlig tall $i \leq t$, er

$$\frac{p-1}{2} = (q_1 \cdots q_{i-1} q_{i+1} \cdots q_t)\, q_i,$$

altså har vi: $q_i \mid \frac{p-1}{2}$. Dermed er

$$\frac{p-1}{2} \equiv 0 \pmod{q_i}.$$

Det følger at

$$-2\left(\frac{p-1}{2}\right) - 1 \equiv (-2) \cdot 0 - 1 = -1 \pmod{q_i},$$

altså er

$$-p \equiv -1 \pmod{q_i}.$$

(10) Det følger fra (8) og Proposisjon 5.5.3 at

$$\mathbb{L}_{q_1}^{-p} \cdot \mathbb{L}_{q_2}^{-p} \cdots \mathbb{L}_{q_t}^{-p} = \mathbb{L}_{q_1}^{-1} \cdot \mathbb{L}_{q_2}^{-1} \cdots \mathbb{L}_{q_t}^{-1}.$$

(11) Ut ifra Lemma 5.9.18 er

$$\mathbb{L}_{q_1}^{-1} \cdot \mathbb{L}_{q_2}^{-1} \cdots \mathbb{L}_{q_t}^{-1} = (-1)^{\frac{q_1 q_2 \cdots q_t - 1}{2}} = (-1)^{\frac{\frac{p-1}{2} - 1}{2}} = (-1)^{\frac{p-3}{4}}.$$

Det følger fra (1) – (5), (7), (8), (10) og (11) at

$$\mathbb{L}_p^2 = \mathbb{L}_p^{-1} \cdot \mathbb{L}_p^{-2} = (-1) \cdot (-1)^{\frac{p-3}{4}}.$$

Siden

$$p \equiv 3 \pmod 4,$$

følger det fra Korollar 3.2.63 at ett av følgende er sant.

(I) $p \equiv 3 \pmod 8$;

(II) $p \equiv 7 \pmod 8$.

Dersom (I) er sant, finnes det et naturlig tall k slik at $p - 3 = 8k$. Da er

$$\begin{aligned}(-1)^{\frac{p-3}{4}} &= (-1)^{2k} \\ &= \left((-1)^2\right)^k \\ &= 1^k \\ &= 1.\end{aligned}$$

Dermed er $\mathbb{L}_p^2 = (-1) \cdot 1 = -1$.

Dersom (II) er sant, finnes det et naturlig tall k slik at $p - 7 = 8k$. Da er

$$\begin{aligned}(-1)^{\frac{p-3}{4}} &= (-1)^{\frac{p-7}{4}+1} \\ &= (-1)^{\frac{p-7}{4}} \cdot (-1) \\ &= (-1)^{2k} \cdot (-1) \\ &= \left((-1)^2\right)^k \cdot (-1) \\ &= 1^k \cdot (-1) \\ &= 1 \cdot (-1) \\ &= -1.\end{aligned}$$

Dermed er $\mathbb{L}_p^2 = (-1) \cdot (-1) = 1$.

Således er korollaret sant dersom (B) er sant.

□

Eksempel 5.9.22. Korollar 5.9.21 fastslår at $\mathbb{L}_5^2 = -1$. Ut ifra Eksempel 5.4.6 er dette rikignok sant.

Eksempel 5.9.23. Korollar 5.9.21 fastslår at $\mathbb{L}_7^2 = 1$. Ut ifra Eksempel 5.4.7 er dette rikignok sant.

Eksempel 5.9.24. Siden

$$11 \equiv 3 \pmod 8,$$

fastslår Korollar 5.9.21 at $\mathbb{L}_{11}^2 = -1$. Ut ifra Eksempel 5.4.8 er dette rikignok sant.

Eksempel 5.9.25. Siden

$$17 \equiv 1 \pmod 8,$$

fastslår Korollar 5.9.21 at $\mathbb{L}_{17}^2 = 1$. Siden

$$6^2 = 36 \equiv 2 \pmod{17},$$

er det riktignok sant at 2 er en kvadratisk rest modulo 17.

5.10 Eksempler på hvordan regne ut Legendresymboler ved å benytte kvadratisk gjensidighet

Eksempel 5.10.1. La oss se igjen på Proposisjon 5.6.2, hvor vi regnet ut $\mathbb{L}_{23}^{84}$. I beviset for denne proposisjonen, måtte vi være ganske kreativ for å regne ut $\mathbb{L}_{23}^3$ og $\mathbb{L}_{23}^5$. Korollar 5.9.2 og Korollar 5.9.21 gir oss muligheten til å unngå dette helt, som følger.

(1) Siden

$$84 \equiv 15 \pmod{23},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{23}^{84} = \mathbb{L}_{23}^{15}$.

(2) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{23}^{15} = \mathbb{L}_{23}^{3\cdot 5} = \mathbb{L}_{23}^3 \cdot \mathbb{L}_{23}^5.$$

(3) Siden $23 \equiv 3 \pmod 4$ og $3 \equiv 3 \pmod 4$, følger det fra Korollar 5.9.2 at $\mathbb{L}_{23}^3 = -\mathbb{L}_3^{23}$. Siden

$$23 \equiv 2 \pmod 3,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_3^{23} = \mathbb{L}_3^2$. Det følger fra Korollar 5.9.21 at $\mathbb{L}_3^2 = -1$. Dermed er

$$\mathbb{L}_{23}^3 = -\mathbb{L}_3^{23} = -\mathbb{L}_3^2 = -(-1) = 1.$$

(4) Siden

$$5 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at

$$\mathbb{L}_{23}^{5} = \mathbb{L}_{5}^{23}.$$

Siden

$$23 \equiv 3 \pmod 5,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{5}^{23} = \mathbb{L}_{5}^{3}$. Siden

$$5 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at

$$\mathbb{L}_{5}^{3} = \mathbb{L}_{3}^{5}.$$

Siden

$$5 \equiv 2 \pmod 3,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{3}^{5} = \mathbb{L}_{3}^{2}$. Det følger fra Korollar 5.9.21 at $\mathbb{L}_{3}^{2} = -1$. Dermed er

$$\mathbb{L}_{23}^{5} = \mathbb{L}_{5}^{23} = \mathbb{L}_{5}^{3} = \mathbb{L}_{3}^{5} = \mathbb{L}_{3}^{2} = -1.$$

Det følger fra (1) – (4) at

$$\mathbb{L}_{23}^{84} = \mathbb{L}_{23}^{15} = \mathbb{L}_{23}^{3} \cdot \mathbb{L}_{23}^{5} = 1 \cdot (-1) = -1.$$

Således er 84 ikke en kvadratisk rest modulo 23.

Merknad 5.10.2. Metoden nevnt i Merknad 5.6.1 for å regne ut $\mathbb{L}_{p}^{a}$, for et hvilket som helst heltall a og et hvilket som helst primtall p slik at $p > 2$, kan nå gjøres fullkommen.

(1) Finn først et heltall r slik at

$$a \equiv r \pmod p$$

og $r < p$. Da fastslår Proposisjon 5.5.3 at $\mathbb{L}_{p}^{a} = \mathbb{L}_{p}^{r}$.

(2) Dersom $r = 1$, er $\mathbb{L}_{p}^{a} = 1$. Finn ellers en primtallsfaktorisering $p_1 \cdots p_t$ til r. Da fastslår Proposisjon 5.5.13 at

$$\mathbb{L}_{p}^{r} = \mathbb{L}_{p}^{p_1} \ldots \mathbb{L}_{p}^{p_t}.$$

(2) Regn ut hvert av Legendresymbolene $\mathbb{L}_{p}^{p_1}$, $\mathbb{L}_{p}^{p_2}$, …, $\mathbb{L}_{p}^{p_t}$.

(3) For å regne ut $\mathbb{L}_{p}^{p_i}$, hvor $i \leq t$, benytt Korollar 5.9.21 om $p_i = 2$. Benytt ellers Korollar 5.9.2 for å få enten at $\mathbb{L}_{p}^{p_i} = \mathbb{L}_{p_i}^{p}$ eller $\mathbb{L}_{p}^{p_i} = -\mathbb{L}_{p_i}^{p}$.

(4) Gjennomfør Steg (1) – Steg (4) for å regne ut $\mathbb{L}_{p_i}^{p}$.

Merknad 5.10.3. Vær forsiktig: Korollar 5.9.2 kan benyttes kun når vi ønsker å regne ut $\mathbb{L}_p^q$, hvor både p og q er primtall. Hvis vi trenger å regne ut $\mathbb{L}_p^n$, hvor n ikke er et primtall, må vi finne en primtallsfaktorisering til n og benytt da Proposisjon 5.5.13. Dette kan lett glemmes hvis vi har jobbet med en rekke primtall i løpet av et bevis, men et heltall som ikke er et primtall dukker plutselig opp, som kan godt hende!

Eksempel 5.10.4. La oss se igjen på Proposisjon 5.6.3, hvor vi regnet ut $\mathbb{L}_{53}^{28}$.

(1) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{59}^{28} = \mathbb{L}_{59}^{4\cdot 7} = \mathbb{L}_{59}^{4} \cdot \mathbb{L}_{59}^{7}.$$

(2) Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{59}^{4} = 1$.

(3) Siden

$$59 \equiv 3 \pmod 4$$

og

$$7 \equiv 3 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{59}^{7} = -\mathbb{L}_{7}^{59}$. Siden

$$59 \equiv 3 \pmod 7,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{7}^{59} = \mathbb{L}_{7}^{3}$. Siden

$$7 \equiv 3 \pmod 4$$

og

$$3 \equiv 3 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{7}^{3} = -\mathbb{L}_{3}^{7}$. Siden

$$7 \equiv 1 \pmod 3,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{3}^{7} = \mathbb{L}_{7}^{1}$. Ut ifra Proposisjon 5.5.2 er $\mathbb{L}_{7}^{1} = 1$. Dermed er

$$\mathbb{L}_{59}^{7} = -\mathbb{L}_{7}^{59} = -\mathbb{L}_{7}^{3} = -(-\mathbb{L}_{3}^{7}) = -(-\mathbb{L}_{3}^{1}) = -(-1) = 1.$$

Det følger fra (1) – (3) at

$$\mathbb{L}_{59}^{28} = \mathbb{L}_{59}^{4} \cdot \mathbb{L}_{59}^{7} = 1 \cdot 1 = 1.$$

Således er 28 en kvadratisk rest modulo 59.

Merknad 5.10.5. Metoden er svært effektiv til og med om vi jobber med ganske store heltall, som følgende proposisjoner viser.

Proposisjon 5.10.6. Heltallet 2457 er ikke en kvadratisk rest modulo 3491.

Bevis. Vi har: 3491 er et primtall. Vi gjør følgende observasjoner.

(1) En primtallsfaktorisering til 2457 er:

$$3^3 \cdot 7 \cdot 13.$$

Ut ifra Proposisjon 5.5.13 er da

$$\mathbb{L}_{3491}^{2457} = \mathbb{L}_{3491}^{3^2} \cdot \mathbb{L}_{3491}^{3} \cdot \mathbb{L}_{3491}^{7} \cdot \mathbb{L}_{3491}^{13}.$$

(2) Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{3491}^{3^2} = 1$.

(3) Vi har:

$$3491 \equiv 3 \pmod 4$$

og

$$3 \equiv 3 \pmod 4.$$

Da følger det fra Korollar 5.9.2 at $\mathbb{L}_{3491}^{3} = -\mathbb{L}_{3}^{3491}$. Siden

$$3491 \equiv 2 \pmod 3,$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}_{3}^{3491} = \mathbb{L}_{3}^{2}.$$

Siden

$$3 \equiv 3 \pmod 8,$$

følger det fra Korollar 5.9.21 at $\mathbb{L}_{3}^{2} = -1$. Dermed er

$$\mathbb{L}_{3491}^{3} = -\mathbb{L}_{3}^{3491} = -\mathbb{L}_{3}^{2} = -(-1) = 1.$$

(4) Vi har:

$$3491 \equiv 3 \pmod 4$$

og

$$7 \equiv 3 \pmod 4.$$

Da følger det fra Korollar 5.9.2 at $\mathbb{L}_{3491}^{7} = -\mathbb{L}_{7}^{3491}$. Siden

$$3491 \equiv 5 \pmod 7,$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}_{7}^{3491} = \mathbb{L}_{7}^{5}.$$

Siden

$$5 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_7^5 = \mathbb{L}_5^7$. Siden

$$7 \equiv 2 \pmod 5,$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}_5^7 = \mathbb{L}_5^2.$$

Siden

$$5 \equiv 5 \pmod 8,$$

følger det fra Korollar 5.9.21 at $\mathbb{L}_5^2 = -1$. Dermed er

$$\mathbb{L}_{3491}^7 = -\mathbb{L}_7^{3491} = -\mathbb{L}_7^5 = -\mathbb{L}_5^7 = -\mathbb{L}_5^2 = -(-1) = 1.$$

(5) Vi har:

$$3491 \equiv 3 \pmod 4$$

og

$$13 \equiv 1 \pmod 4.$$

Da følger det fra Korollar 5.9.2 at $\mathbb{L}_{3491}^{13} = \mathbb{L}_{13}^{3491}$. Siden

$$3491 \equiv 7 \pmod{13},$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}_{13}^{3491} = \mathbb{L}_{13}^7.$$

Siden

$$13 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{13}^7 = \mathbb{L}_7^{13}$. Siden

$$13 \equiv 6 \pmod 7,$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}_7^{13} = \mathbb{L}_7^6.$$

Legendresymbolet $\mathbb{L}_7^6$ kan regnes ut på flere måter: vi kan for eksempel benytte primtallsfaktoriseringen $2 \cdot 3$ til 6, og regne ut deretter $\mathbb{L}_7^2$ og $\mathbb{L}_7^3$. Fortest er å observere istedenfor at

$$6 \equiv -1 \pmod 7.$$

Ut fra Proposisjon 5.5.3 er da $\mathbb{L}_7^6 = \mathbb{L}_7^{-1}$. Ut ifra Proposisjon 5.5.16 er $\mathbb{L}_7^{-1} = (-1)^{\frac{7-1}{2}} = (-1)^3 = -1$. Dermed er

$$\mathbb{L}_{3491}^{13} = \mathbb{L}_{13}^{3491} = \mathbb{L}_{13}^7 = \mathbb{L}_7^{13} = \mathbb{L}_7^{-1} = -1.$$

Det følger fra (1) – (5) at

$$\mathbb{L}_{3491}^{2457} = \mathbb{L}_{3491}^{3^2} \cdot \mathbb{L}_{3491}^{3} \cdot \mathbb{L}_{3491}^{7} \cdot \mathbb{L}_{3491}^{13} = 1 \cdot 1 \cdot 1 \cdot (-1) = -1.$$

Således er 2457 ikke en kvadratisk rest modulo 3491.

□

Proposisjon 5.10.7. Heltallet -1003 er en kvadratisk rest modulo 1549.

Bevis. Vi har: 1549 er et primtall. Vi gjør følgende observasjoner.

(1) En primtallsfaktorisering til 1003 er:

$$17 \cdot 59.$$

Ut ifra Proposisjon 5.5.13 er da

$$\mathbb{L}_{1549}^{-1003} = \mathbb{L}_{1549}^{(-1)\cdot 17\cdot 59} = \mathbb{L}_{1549}^{-1} \cdot \mathbb{L}_{1549}^{17} \cdot \mathbb{L}_{1549}^{59}.$$

(2) Ut ifra Proposisjon 5.5.16 er $\mathbb{L}_{1549}^{-1} = (-1)^{\frac{1549-1}{2}} = (-1)^{774} = 1$.

(3) Vi har:

$$1549 \equiv 1 \pmod 4.$$

Da følger det fra Korollar 5.9.2 at $\mathbb{L}_{1549}^{17} = \mathbb{L}_{17}^{1549}$. Siden

$$1549 \equiv 2 \pmod{17},$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}_{17}^{1549} = \mathbb{L}_{17}^{2}.$$

Siden

$$17 \equiv 1 \pmod 8,$$

følger det fra Korollar 5.9.21 at $\mathbb{L}_{17}^{2} = 1$. Dermed er

$$\mathbb{L}_{1549}^{17} = \mathbb{L}_{17}^{1549} = \mathbb{L}_{17}^{2} = 1.$$

(4) Siden

$$1549 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{1549}^{59} = \mathbb{L}_{59}^{1549}$. Siden

$$1549 \equiv 15 \pmod{59},$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}_{59}^{1549} = \mathbb{L}_{59}^{15}.$$

Ut ifra Proposisjon 5.5.13 er $\mathbb{L}_{59}^{15} = \mathbb{L}_{59}^{3\cdot 5} = \mathbb{L}_{59}^{3} \cdot \mathbb{L}_{59}^{5}$.

(5) Vi har:

$$3 \equiv 3 \pmod 4$$

og

$$59 \equiv 3 \pmod 4.$$

Da følger det fra Korollar 5.9.2 at $\mathbb{L}_{59}^{3} = -\mathbb{L}_{3}^{59}$. Siden

$$59 \equiv 2 \pmod 3,$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}_{3}^{59} = \mathbb{L}_{3}^{2}.$$

Siden

$$3 \equiv 3 \pmod 8,$$

følger det fra Korollar 5.9.21 at $\mathbb{L}_{3}^{2} = -1$. Dermed er

$$\mathbb{L}_{59}^{3} = -\mathbb{L}_{3}^{59} = -\mathbb{L}_{3}^{2} = -(-1) = 1.$$

(6) Vi har:

$$5 \equiv 1 \pmod 4.$$

Da følger det fra Korollar 5.9.2 at $\mathbb{L}_{59}^{5} = \mathbb{L}_{5}^{59}$. Siden

$$59 \equiv 4 \pmod 5,$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}_{5}^{59} = \mathbb{L}_{5}^{4}.$$

Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{5}^{4} = \mathbb{L}_{5}^{2^2} = 1$. Dermed er

$$\mathbb{L}_{59}^{5} = \mathbb{L}_{5}^{59} = \mathbb{L}_{5}^{4} = 1.$$

Det følger fra (1) – (6) at

$$\mathbb{L}_{1549}^{-1003} = \mathbb{L}_{1549}^{-1} \cdot \mathbb{L}_{1549}^{17} \cdot \mathbb{L}_{1549}^{59} = 1 \cdot 1 \cdot 1 = 1.$$

Således er -1003 en kvadratisk rest modulo 1549.

□

Proposisjon 5.10.8. Kongruensen

$$2x^2 + 87x + 29 \equiv 0 \pmod{63533}$$

har to løsninger som ikke er kongruent til hverandre modulo 63533, og slik at enhver annen løsning er kongruent modulo 63533 til én av disse to.

Bevis. Heltallet 63533 er et primtall. Vi har:

$$87^2 - 4 \cdot 2 \cdot 29 = 7337.$$

La oss regne ut $\mathbb{L}_{63533}^{7337}$.

(1) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{63533}^{7337} = \mathbb{L}_{63533}^{11 \cdot 23 \cdot 29} = \mathbb{L}_{63533}^{11} \cdot \mathbb{L}_{63533}^{23} \cdot \mathbb{L}_{63533}^{29}.$$

(2) Siden

$$63533 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{63533}^{11} = \mathbb{L}_{11}^{63533}$. Siden

$$63533 \equiv 8 \pmod{11},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{11}^{63533} = \mathbb{L}_{11}^{8}$.

(3) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{11}^{8} = \mathbb{L}_{11}^{2^2 \cdot 2} = \mathbb{L}_{11}^{2^2} \cdot \mathbb{L}_{11}^{2}.$$

Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{11}^{2^2} = 1$.

(4) Siden

$$11 \equiv 3 \pmod 8,$$

følger det fra Korollar 5.9.21 at

$$\mathbb{L}_{11}^{2} = -1.$$

(5) Det følger fra (2) – (4) at

$$\mathbb{L}_{63533}^{11} = \mathbb{L}_{11}^{63533} = \mathbb{L}_{11}^{8} = \mathbb{L}_{11}^{2^2} \cdot \mathbb{L}_{11}^{2} = 1 \cdot (-1) = -1.$$

(6) Siden

$$63533 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{63533}^{23} = \mathbb{L}_{23}^{63533}$. Siden

$$63533 \equiv 7 \pmod{23},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{23}^{63533} = \mathbb{L}_{23}^{7}$.

(7) Siden

$$7 \equiv 3 \pmod 4$$

og

$$23 \equiv 4 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{23}^{7} = -\mathbb{L}_{7}^{23}$. Siden

$$23 \equiv 2 \pmod{7},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{7}^{23} = \mathbb{L}_{7}^{2}$. Siden

$$7 \equiv 7 \pmod{8},$$

følger det fra Korollar 5.9.21 at $\mathbb{L}_{7}^{2} = 1$.

(8) Det følger fra (6) – (7) at

$$\mathbb{L}_{63533}^{23} = \mathbb{L}_{23}^{63533} = \mathbb{L}_{23}^{7} = -\mathbb{L}_{7}^{23} = -\mathbb{L}_{7}^{2} = -1.$$

(9) Siden

$$63533 \equiv 1 \pmod{4},$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{63533}^{29} = \mathbb{L}_{29}^{63533}$. Siden

$$63533 \equiv 23 \pmod{29},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{29}^{63533} = \mathbb{L}_{29}^{23}$.

(10) Siden

$$29 \equiv 1 \pmod{4},$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{29}^{23} = \mathbb{L}_{23}^{29}$. Siden

$$29 \equiv 6 \pmod{23},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{23}^{29} = \mathbb{L}_{23}^{6}$.

(11) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{23}^{6} = \mathbb{L}_{23}^{2\cdot 3} = \mathbb{L}_{23}^{2} \cdot \mathbb{L}_{23}^{3}.$$

(12) Siden

$$23 \equiv 7 \pmod{8},$$

følger det fra Korollar 5.9.21 at $\mathbb{L}_{23}^{2} = 1$.

(13) Siden

$$3 \equiv 3 \pmod{4}$$

og

$$23 \equiv 3 \pmod{4},$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{23}^{3} = -\mathbb{L}_{3}^{23}$. Siden

$$23 \equiv 2 \pmod{3},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_3^{23} = \mathbb{L}_3^2$. Siden

$$3 \equiv 3 \pmod 8,$$

følger det fra Korollar 5.9.21 at $\mathbb{L}_3^2 = -1$. Dermed er

$$\mathbb{L}_{23}^3 = -\mathbb{L}_3^{23} = -\mathbb{L}_3^2 = -(-1) = 1.$$

(14) Det følger fra (9) – (12) at

$$\mathbb{L}_{63533}^{29} = \mathbb{L}_{29}^{63533} = \mathbb{L}_{29}^{23} = \mathbb{L}_{23}^{29} = \mathbb{L}_{23}^6 = \mathbb{L}_{23}^2 \cdot \mathbb{L}_{23}^3 = 1 \cdot 1 = 1.$$

Det følger fra (1), (8), og (14) at

$$\mathbb{L}_{63533}^{7337} = \mathbb{L}_{63533}^{11} \cdot \mathbb{L}_{63533}^{23} \cdot \mathbb{L}_{63533}^{29} = (-1) \cdot (-1) \cdot 1 = 1.$$

Således er 7337 en kvadratisk rest modulo 63533. Ut ifra Korollar 5.2.30, konkluderer vi at kongruensen

$$2x^2 + 87x + 29 \equiv 0 \pmod{63533}$$

har to løsninger som ikke er kongruent til hverandre modulo 63533, og slik at enhver annen løsning er kongruent modulo 63533 til én av disse to.

□

Proposisjon 5.10.9. Kongruensen

$$173x^2 - 27x - 5 \equiv 0 \pmod{6427}$$

har ingen løsning.

Bevis. Heltallet 6427 er et primtall. Vi har:

$$(-27)^2 - 4 \cdot 173 \cdot (-5) = 4189.$$

La oss regne ut $\mathbb{L}_{6427}^{4189}$.

(1) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{6427}^{4189} = \mathbb{L}_{6427}^{59 \cdot 71} = \mathbb{L}_{6427}^{59} \cdot \mathbb{L}_{6427}^{71}.$$

(2) Siden

$$59 \equiv 3 \pmod 4$$

og

$$6427 \equiv 3 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{6427}^{59} = -\mathbb{L}_{59}^{6427}$. Siden

$$6427 \equiv 55 \pmod{59},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{59}^{6427} = \mathbb{L}_{59}^{55}$.

(3) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{59}^{55} = \mathbb{L}_{59}^{5\cdot 11} = \mathbb{L}_{59}^{5} \cdot \mathbb{L}_{59}^{11}.$$

(4) Siden

$$5 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at

$$\mathbb{L}_{59}^{5} = \mathbb{L}_{5}^{59}.$$

Siden

$$59 \equiv 4 \pmod 5,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{5}^{59} = \mathbb{L}_{5}^{4}$. Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{5}^{4} = \mathbb{L}_{5}^{2^2} = 1$. Dermed er

$$\mathbb{L}_{59}^{5} = \mathbb{L}_{5}^{59} = \mathbb{L}_{5}^{4} = 1.$$

(5) Siden

$$11 \equiv 3 \pmod 4$$

og

$$59 \equiv 3 \pmod 4,$$

følger det fra Korollar 5.9.2 at

$$\mathbb{L}_{59}^{11} = -\mathbb{L}_{11}^{59}.$$

Siden

$$59 \equiv 4 \pmod{11},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{11}^{59} = \mathbb{L}_{11}^{4}$. Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{11}^{4} = \mathbb{L}_{11}^{2^2} = 1$. Dermed er

$$\mathbb{L}_{59}^{11} = -\mathbb{L}_{11}^{59} = -\mathbb{L}_{11}^{4} = -1.$$

(6) Det følger fra (2), (4),og (5) at

$$\mathbb{L}_{6427}^{59} = -\mathbb{L}_{59}^{6427} = -\mathbb{L}_{59}^{55} = -\mathbb{L}_{59}^{5} \cdot \mathbb{L}_{59}^{11} = -1 \cdot (-1) = 1.$$

(7) Siden

$$71 \equiv 3 \pmod 4$$

og

$$6427 \equiv 3 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{6427}^{71} = -\mathbb{L}_{71}^{6427}$. Siden

$$6427 \equiv 37 \pmod{71},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{71}^{6427} = \mathbb{L}_{71}^{37}$.

(8) Siden

$$37 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{71}^{37} = \mathbb{L}_{37}^{71}$. Siden

$$71 \equiv 34 \pmod{37},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{37}^{71} = \mathbb{L}_{37}^{34}$.

(9) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{37}^{34} = \mathbb{L}_{37}^{2\cdot 17} = \mathbb{L}_{37}^{2} \cdot \mathbb{L}_{37}^{17}.$$

(10) Siden

$$37 \equiv 5 \pmod 8,$$

følger det fra Korollar 5.9.21 at $\mathbb{L}_{37}^{2} = -1$.

(11) Siden

$$37 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{37}^{17} = \mathbb{L}_{17}^{37}$. Siden

$$37 \equiv 3 \pmod{17},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{17}^{37} = \mathbb{L}_{17}^{3}$.

(12) Siden

$$17 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}_{17}^{3} = \mathbb{L}_{3}^{17}$. Siden

$$17 \equiv 2 \pmod 3,$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{3}^{17} = \mathbb{L}_{3}^{2}$. Siden

$$3 \equiv 3 \pmod 8,$$

følger det fra Korollar 5.9.21 at $\mathbb{L}_{3}^{2} = -1$.

(13) Det følger fra (11) – (12) at

$$\mathbb{L}_{37}^{17} = \mathbb{L}_{17}^{37} = \mathbb{L}_{17}^{3} = \mathbb{L}_{3}^{17} = \mathbb{L}_{3}^{2} = -1.$$

(14) Det følger fra (7) – (10) og (12) at

$$\mathbb{L}_{6427}^{71} = -\mathbb{L}_{71}^{6427} = -\mathbb{L}_{71}^{37} = -\mathbb{L}_{37}^{71} = -\mathbb{L}_{37}^{34} = -\mathbb{L}_{37}^{2} \cdot \mathbb{L}_{37}^{17} = -(-1) \cdot (-1) = -1.$$

Det følger fra (6) og (14) at

$$\mathbb{L}_{6427}^{4189} = \mathbb{L}_{6427}^{59} \cdot \mathbb{L}_{6427}^{71} = 1 \cdot (-1) = -1.$$

Således er 4189 ikke en kvadratisk rest modulo 6427. Ut ifra Korollar 5.2.30, konkluderer vi at kongruensen

$$173x^2 - 27x - 5 \equiv 0 \pmod{6427}$$

har ingen løsning modulo 6427. □

5.11 Det finnes uendelig mange primtall som er kongruent til 7 modulo 8

Merknad 5.11.1. Teorem 5.8.30, Korollar 5.9.2, og Korollar 5.9.21 er også svært viktige teoretiske verktøy. Flere proposisjoner som ligner på følgende kan for eksempel bevises.

Proposisjon 5.11.2. La n være et naturlig tall. Det finnes et primtall p slik at $p > n$ og

$$p \equiv 7 \pmod 8.$$

Bevis. La q være produktet av alle de primtallene som er mindre enn eller like n, og som er kongruent til 7 modulo 8. Ut ifra Teorem 4.3.3, finnes det et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at

$$8q^2 - 1 = p_1 \cdots p_t.$$

Vi gjør følgende observasjoner.

(1) Anta at det finnes et naturlig tall i slik at $i \leq t$ og $p_i = 2$. Da er

$$p_1 \cdots p_t = (p_1 \cdots p_{i-1} p_{i+1} \cdots p_t)\, 2,$$

altså har vi:

$$2 \mid p_1 \cdots p_t.$$

Da er

$$p_1 \cdots p_t \equiv 0 \pmod 2.$$

(2) Det følger fra (1) at

$$8q^2 - 1 \equiv 0 \pmod 2.$$

Imidlertid er

$$8q^2 - 1 \equiv -1 \equiv 1 \pmod 2.$$

Ut ifra Proposisjon 3.2.11, kan det ikke være sant at både

$$8q^2 - 1 \equiv 0 \pmod 2$$

og

$$8q^2 - 1 \equiv 1 \pmod 2.$$

Siden antakelsen at $p_i = 2$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $p_i = 2$. Derfor er $p_i > 2$ for alle de naturlige tallene i slik at $i \leq t$.

(3) La i være et naturlig tall slik at $i \leq t$. Vi har

$$(4q)^2 - 2 = 2\left(8q^2 - 1\right) = 2p_1 \cdots p_t = (2p_1 \cdots p_{i-1} p_{i+1} \cdots p_t)\, p_i.$$

Dermed har vi: $p_i \mid (4q)^2 - 2$. Derfor er

$$(4q)^2 - 2 \equiv 0 \pmod{p_i},$$

altså er

$$(4q)^2 \equiv 2 \pmod{p_i}.$$

Dermed er 2 en kvadratisk rest modulo p_i, altså er $\mathbb{L}^2_{p_i} = 1$, for hvert naturlig tall i slik at $i \leq t$.

(4) For hvert naturlig tall i slik at $i \leq t$, følger det fra (3) og Korollar 5.9.21 at enten

$$p_i \equiv 1 \pmod{8}$$

eller

$$p_i \equiv 7 \pmod{8},$$

altså enten

$$p_i \equiv 1 \pmod{8}$$

eller

$$p_i \equiv -1 \pmod{8}.$$

(5) Anta at

$$p_i \equiv 1 \pmod{8}$$

for alle de naturlige tallene i slik at $i \leq t$. Da er

$$p_1 \cdots p_t \equiv 1 \pmod{8},$$

altså er

$$8q^2 - 1 \equiv 1 \pmod{8}.$$

Imidlertid er

$$8q^2 - 1 \equiv -1 \equiv 7 \pmod{8}.$$

Ut ifra Proposisjon 3.2.11, kan det ikke være sant at både

$$8q^2 - 1 \equiv 1 \pmod{8}$$

og

$$8q^2 - 1 \equiv 7 \pmod{8}.$$

Siden antakelsen at

$$p_i \equiv 1 \pmod{8}$$

for alle de naturlige tallene i slik at $i \leq t$ fører til denne motsigelsen, konkluderer vi at det finnes et naturlig tall i slik at $i \leq t$ og

$$p_i \equiv -1 \pmod{8},$$

altså

$$p_i \equiv 7 \pmod{8}.$$

(6) Anta at $p_i \leq n$. Ut ifra definisjonen til q, har vi da: $p_i \mid q$. Ut ifra Korollar 2.5.18 følger det at

$$p_i \mid q \cdot 8q,$$

altså $p_i \mid 8q^2$.

(7) Siden

$$8q^2 - 1 = p_1 \cdots p_t,$$

har vi: $p_i \mid 8q^2 - 1$. Ut ifra Korollar 2.5.18 har vi da: $p_i \mid -\big(8q^2 - 1\big)$.

(8) Det følger fra (6), (7), og Proposisjon 2.5.24 at $p_i \mid 8q^2 - \big(8q^2 - 1\big)$, altså at $p_i \mid 1$.

(9) Det kan ikke være sant at både $p_i \mid 1$ og $p_i > 2$. Siden antakelsen at $p_i \leq n$ fører til denne motsigelsen, konkluderer vi at $p_i > n$.

□

Merknad 5.11.3. Med andre ord fastslår Proposisjon 5.11.2 at det finnes uendelig mange primtall som er kongruent til 7 modulo 8.

Eksempel 5.11.4. La oss gå gjennom beviset for Proposisjon 5.11.2 når $n = 32$. Det finnes tre primtall som er mindre enn eller likt 32 og som er kongruent til 7 modulo 8, nemlig 7, 23, og 31. La q være produktet av disse primtallene, altså

$$q = 7 \cdot 23 \cdot 31.$$

Da er $8q^2 - 1$ likt 199280647. Beviset for Proposisjon 5.11.2 fastslår at ett av primtallene i en primtallsfaktorisering av $8q^2 - 1$, altså av 199280647, er større enn 32. Vi har:

$$199280647 = 17 \cdot 11722391,$$

og både 17 og 11722391 er primtall. Det er riktignok sant at $11722391 > 32$.

Merknad 5.11.5. Vi har nå sett flere eksempler på proposisjoner som ligner på Proposisjon 5.11.2: Teorem 4.4.2, Proposisjon 4.4.9, Oppgave O4.1.3, og Proposisjon 5.3.18.

Utgangspunktet for bevisene for alle disse proposisjonene er beviset for Teorem 4.4.2. Vi har benyttet stadig dypere resultater for å gjennomføre et lignende argument i de andre tilfellene.

Faktisk finnes det uendelig mange primtall som er kongruent til r modulo m for hvilke som helst naturlige tall m og r slik at $\mathsf{sfd}(m, r) = 1$. Dette kalles *Dirichlets teorem*, og er et dypt resultat.

En ny tilnærmingsmetode behøves for å gi et bevis for Dirichlets teorem, det vil si et bevis som virker for alle de mulige tilfellene samtidig. Ett av bevisene benytter teorien for *L-funksjoner* i *analytisk tallteori*. Det finnes både algebraiske og analytiske varianter av L-funksjoner, og teorien for dem er ett av de viktigste temaene innen dagens forskning i tallteori.

5.12 Mersenne-primtall

Merknad 5.12.1. Nå kommer vi til å se på et fint tema hvor kvadratisk gjensidighet kan benyttes.

Terminologi 5.12.2. La n være et naturlig tall. Vi sier at $2^n - 1$ er et *Mersenne-tall*. Dersom $2^n - 1$ er et primtall, sier vi at det er et *Mersenne-primtall*.

Eksempel 5.12.3. Den andre kolonnen i følgende tabell viser de første 15 Mersenne-tallene.

n	$2^n - 1$
1	1
2	3
3	7
4	15
5	31
6	63
7	127
8	255
9	511
10	1023
11	2047
12	4095
13	8191
14	16383
15	32767

Merknad 5.12.4. Når er et Mersenne-tall et primtall? Dette spørsmålet har fascinert matematikkere siden Antikkens Hellas. I denne delen av kapittelet kommer vi til å utforske det litt.

Proposisjon 5.12.5. La n være et naturlig tall slik at $n \geq 2$. La a være et naturlig tall. Anta at $a^n - 1$ er et primtall. Da er $a = 2$, og n er et primtall.

Bevis. La oss først bevise at $a = 2$. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 1.13.6 er

$$(a^n - 1) = (a - 1)\left(a^{n-1} + a^{n-2} + \cdots + a + 1\right).$$

(2) Siden $n \geq 2$, er

$$a^{n-1} + a_{n-2} + \cdots + a + 1 \geq a + 1.$$

Siden a er et naturlig tall, er $a + 1 > 1$. Dermed er

$$a^{n-1} + a_{n-2} + \cdots + a + 1 > 1.$$

(3) Siden $a^n - 1$ er et primtall, er 1 og $a^n - 1$ de eneste divisorene til $a^n - 1$.

(4) Det følger fra (1) – (3) at

$$a^{n-1} + a^{n-2} + \cdots + a + 1 = a^n - 1.$$

(5) Det følger fra (1) og (4) at

$$a^n - 1 = (a - 1)\left(a^n - 1\right).$$

Ut ifra Proposisjon 2.2.25 er da

$$a - 1 = 1,$$

altså $a = 2$.

La oss nå bevise at n er et primtall. Anta at det finnes et naturlig tall m slik at $m \mid n$. Da finnes det et naturlig tall k slik at $n = km$. Vi gjør følgende observasjoner.

(1) Da er

$$\begin{aligned} 2^n - 1 &= 2^{km} - 1 \\ &= (2^m)^k - 1. \end{aligned}$$

(2) Ut ifra Proposisjon 1.13.6 er

$$\left((2^m)^k - 1\right) = (2^m - 1)\left((2^m)^{k-1} + (2^m)^{k-2} + \cdots + 2^m + 1\right).$$

(3) Det følger fra (1) og (2) at

$$2^n - 1 = (2^m - 1)\left((2^m)^{k-1} + (2^m)^{k-2} + \cdots + 2^m + 1\right).$$

(4) Dersom $m > 1$, er $2^m - 1 > 1$.

(5) Siden $2^n - 1$ er et primtall, er 1 og $2^n - 1$ de eneste divisorene til $2^n - 1$.

(6) Det følger fra (3) – (5) at $2^m - 1 = 2^n - 1$, altså at $2^m = 2^n$. Da er $m = n$.

Således har vi bevist at, dersom $m \mid n$ og $m > 1$, er $m = n$. Derfor er n et primtall.

□

Eksempel 5.12.6. De eneste naturlige tallene i den andre kolonnen i tabellen i Eksempel 5.12.3 som er primtall er: 3, 7, 31, 127, og 8191. Vi får disse primtallene når n er 2, 3, 5, 7, og 13. Proposisjon 5.12.5 fastslår at alle disse verdiene av n er primtall. Dette er riktignok sant.

Eksempel 5.12.7. Siden 21 ikke er et primtall, fastslår Proposisjon 5.12.5 at det ikke er sant at $2^{21} - 1$ er et primtall. Dette er riktignok sant: $2^{21} - 1 = 2097151$, og $7 \mid 2097151$.

Merknad 5.12.8. Når p er ett av de første fire primtallene, altså 2, 3, 5, og 7, er $2^p - 1$ et primtall. Er $2^p - 1$ alltid et primtall når p er et primtall? Nei! Når $p = 11$, er

$$2^p - 1 = 2^{11} - 1 = 2047.$$

Siden $2047 = 23 \cdot 89$, er 2047 ikke et primtall.

For hvilke primtall p er $2^p - 1$ et primtall? Resten av denne delen av kapittelet handle om dette spørsmålet.

Proposisjon 5.12.9. La p være et primtall. Anta at $2p + 1$ er et primtall. Da har vi: enten $2p + 1 \mid 2^p - 1$ eller $2p + 1 \mid 2^p + 1$.

Bevis. Siden $2p + 1$ er et primtall, følger det fra Korollar 4.10.8 at

$$2^{(2p+1)-1} \equiv 1 \pmod{2p+1},$$

altså at

$$2^{2p} \equiv 1 \pmod{2p+1}.$$

Derfor er

$$2^{2p} - 1 \equiv 0 \pmod{2p+1}.$$

Siden

$$2^{2p} - 1 = (2^p - 1)(2^p + 1),$$

er da

$$(2^p - 1)(2^p + 1) \equiv 0 \pmod{2p+1}.$$

Siden $2p + 1$ er et primtall, følger det fra Proposisjon 4.2.12 at enten

$$2p + 1 \mid 2^p - 1$$

eller

$$2p + 1 \mid 2^p - 1.$$

□

Eksempel 5.12.10. Siden 3 er et primtall og $2 \cdot 3 + 1 = 7$ er et primtall, fastslår Proposisjon 5.12.9 at enten $7 \mid 2^3 - 1$ eller $7 \mid 2^3 + 1$. Siden $2^3 - 1 = 7$ og $7 \mid 7$, er dette riktignok sant.

Eksempel 5.12.11. Siden 5 er et primtall og $2 \cdot 5 + 1 = 11$ er et primtall, fastslår Proposisjon 5.12.9 at enten $11 \mid 2^5 - 1$ eller $11 \mid 2^5 + 1$. Siden $2^5 + 1 = 33$ og $11 \mid 33$, er dette riktignok sant.

Eksempel 5.12.12. Siden 11 er et primtall og $2 \cdot 11 + 1 = 23$ er et primtall, fastslår Proposisjon 5.12.9 at enten $23 \mid 2^{11} - 1$ eller $23 \mid 2^{11} + 1$. Siden $2^{11} - 1 = 2047$ og $23 \mid 2047$, er dette riktignok sant.

Merknad 5.12.13. Vi holder på med å svare på spørsmålet: for hvilke primtall p er $2^p - 1$ et primtall? Proposisjon 5.12.9 henleder oss deretter til spørsmålet: for hvilke primtall p, slik at $2p + 1$ er et primtall, er det tilfellet at $2p + 1 \mid 2^p - 1$? Ved hjelp av Korollar 5.9.21, svarer følgende proposisjon på dette.

Proposisjon 5.12.14. La p være et primtall. Anta at $2p + 1$ er et primtall. Dersom

$$2p + 1 \equiv 1 \pmod 8$$

eller

$$2p + 1 \equiv 7 \pmod 8,$$

har vi: $2p + 1 \mid 2^p - 1$. Ellers har vi: $2p + 1 \mid 2^p + 1$.

Bevis. Anta først at enten

$$2p + 1 \equiv 1 \pmod 8$$

eller

$$2p + 1 \equiv 7 \pmod 8.$$

Siden $2p+1$ er et primtall, følger det fra Korollar 5.9.21 at $\mathbb{L}^2_{2p+1} = 1$. Ut ifra Proposisjon 5.3.2 er da

$$2^{\frac{(2p+1)-1}{2}} \equiv 1 \pmod{2p + 1},$$

altså

$$2^p \equiv 1 \pmod{2p + 1}.$$

Det følger at

$$2^p - 1 \equiv 0 \pmod{2p + 1},$$

altså at

$$2p + 1 \mid 2^p - 1.$$

Anta istedenfor at verken

$$2p + 1 \equiv 1 \pmod 8$$

eller

$$2p + 1 \equiv 7 \pmod 8.$$

Da følger det fra Korollar 5.9.21 at $\mathbb{L}^2_{2p+1} = -1$. Ut ifra Korollar 5.3.12 er da

$$2^{\frac{(2p+1)-1}{2}} \equiv -1 \pmod{2p + 1},$$

altså

$$2^p \equiv -1 \pmod{2p + 1}.$$

Det følger at

$$2^p + 1 \equiv 0 \pmod{2p + 1},$$

altså at

$$2p + 1 \mid 2^p + 1.$$

□

Eksempel 5.12.15. Vi har: 3 er et primtall og $2 \cdot 3 + 1 = 7$ er et primtall. Siden

$$7 \equiv 7 \pmod{8},$$

fastslår Proposisjon 5.12.14 at $7 \mid 2^3 - 1$. Siden $2^3 - 1 = 7$ og $7 \mid 7$, er dette riktignok sant.

Eksempel 5.12.16. Vi har: 5 er et primtall og $2 \cdot 5 + 1 = 11$ er et primtall. Siden

$$11 \equiv 3 \pmod{8},$$

fastslår Proposisjon 5.12.14 at $11 \mid 2^5 + 1$. Siden $2^5 + 1 = 33$ og $11 \mid 33$, er dette riktignok sant.

Eksempel 5.12.17. Vi har: 11 er et primtall og $2 \cdot 11 + 1 = 23$ er et primtall. Siden

$$23 \equiv 7 \pmod{8},$$

fastslår Proposisjon 5.12.14 at $23 \mid 2^{11} - 1$. Siden $2^{11} - 1 = 2047$ og $23 \mid 2047$, er dette riktignok sant.

Korollar 5.12.18. La p være et primtall. Anta at $2p + 1$ er et primtall. Dersom

$$p \equiv 3 \pmod{4},$$

har vi: $2p + 1 \mid 2^p - 1$.

Bevis. Dersom

$$p \equiv 3 \pmod{4},$$

følger det fra Korollar 3.2.63 at ett av følgende er sant:

(A) $p \equiv 3 \pmod{8}$;

(B) $p \equiv 7 \pmod{8}$.

Anta først at (A) er sant. Da er

$$2p + 1 \equiv 7 \pmod{8}.$$

Det følger fra Proposisjon 5.12.14 at

$$2p + 1 \mid 2^p - 1.$$

Anta istedenfor at (B) er sant. Da er

$$2p + 1 \equiv 15 \equiv 7 \pmod{8}.$$

Igjen følger det fra Proposisjon 5.12.14 at

$$2p + 1 \mid 2^p - 1.$$

□

Eksempel 5.12.19. Vi har: 3 er et primtall og $2 \cdot 3 + 1 = 7$ er et primtall. Siden

$$3 \equiv 3 \pmod{4},$$

fastslår Korollar 5.12.18 at $7 \mid 2^3 - 1$. Siden $2^3 - 1 = 7$ og $7 \mid 7$, er dette riktignok sant.

Eksempel 5.12.20. Vi har: 11 er et primtall og $2 \cdot 11 + 1 = 23$ er et primtall. Siden

$$11 \equiv 3 \pmod{4},$$

fastslår Korollar 5.12.18 at $23 \mid 2^{11} - 1$. Siden $2^{11} - 1 = 2047$ og $23 \mid 2047$, er dette riktignok sant.

Proposisjon 5.12.21. La p være et primtall slik at $p > 2$. La q være et primtall slik at $q \mid 2^p - 1$. Da finnes det et naturlig tall m slik at $q = 2mp + 1$.

Bevis. Vi gjør følgende observasjoner.

(1) La t være ordenen til 2 modulo q. Siden $q \mid 2^p - 1$, er

$$2^p \equiv 1 \pmod{q}.$$

Ut ifra Proposisjon 4.12.10, har vi da: $t \mid p$.

(2) Siden p er et primtall, er 1 og p de eneste divisorene til p. Derfor følger det fra (1) at enten $t = 1$ eller $t = p$.

(3) Anta at $t = 1$. Da er

$$2^1 \equiv 1 \pmod{q},$$

altså $q \mid 2^1 - 1$. Dermed har vi: $q \mid 1$. Siden q er et primtall, er $q > 1$. Siden antakelsen at $t = 1$ fører til motsigelsen at både $q \mid 1$ og $q > 1$, konkluderer vi at det ikke er sant at $t = 1$. Derfor er $t = p$.

(4) Ut ifra Korollar 4.10.8 er

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

Da følger det fra Proposisjon 4.12.10 at $t \mid q - 1$.

(5) Det følger fra (3) og (4) at $p \mid q - 1$. Dermed finnes det et naturlig tall k slik at $q - 1 = kp$, altså slik at $q = kp + 1$.

(6) Anta at

$$k \equiv 1 \pmod{2}.$$

Siden p er et primtall og $p > 2$, er

$$p \equiv 1 \pmod{2}.$$

Da er

$$q \equiv 1 \cdot 1 + 1 = 1 + 1 = 2 \equiv 0 \pmod{2}.$$

Det følger at $2 \mid q$. Siden $q \mid 2^p - 1$, følger det at $2 \mid 2^p - 1$. Da er

$$2^p - 1 \equiv 0 \pmod{2}.$$

Imidlertid er

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

Ut ifra Proposisjon 3.2.11, kan det ikke være sant at både

$$2^p - 1 \equiv 0 \pmod{2}$$

og at

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

Siden antakelsen at

$$k \equiv 1 \pmod{2}$$

fører til denne motsigelsen, konkluderer vi at det ikke er sant at

$$k \equiv 1 \pmod{2}.$$

Ut ifra Proposisjon 3.2.1, er da

$$k \equiv 0 \pmod{2},$$

altså har vi: $2 \mid k$. Dermed finnes det et naturlig tall m slik at $k = 2m$.

(7) Det følger fra (5) og (6) at $q = 2mp + 1$.

□

Eksempel 5.12.22. Vi har: $2^{11} - 1 = 2047$, og $89 \mid 2047$. Siden 89 er et primtall, fastslår Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $89 = (2m) \cdot 11 + 1$. Dette er riktignok sant: $89 = (2 \cdot 4) \cdot 11 + 1$.

I tillegg har vi: $23 \mid 2047$. Siden 23 er et primtall, fastslår Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $23 = (2m) \cdot 11 + 1$. Dette er riktignok sant: $23 = (2 \cdot 1) \cdot 11 + 1$.

Eksempel 5.12.23. Vi har: $2^{29} - 1 = 536870911$, og en primtallsfaktorisering til 536870911 er

$$233 \cdot 1103 \cdot 2089.$$

Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $233 = (2m) \cdot 29 + 1$. Dette er riktignok sant: $89 = (2 \cdot 4) \cdot 29 + 1$.

I tillegg fastslår Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $1103 = (2m) \cdot 29 + 1$. Dette er riktignok sant: $1103 = (2 \cdot 19) \cdot 29 + 1$.

I tillegg fastslår Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $2089 = (2m) \cdot 29 + 1$. Dette er riktignok sant: $2089 = (2 \cdot 36) \cdot 29 + 1$.

Proposisjon 5.12.24. La p være et primtall slik at $p > 2$. La q være et primtall slik at $q \mid 2^p - 1$. Da er enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 5.12.21, finnes det et naturlig tall m slik at $q = 2mp + 1$.

(2) Ut ifra Proposisjon 5.3.2, er

$$\mathbb{L}_q^2 \equiv 2^{\frac{q-1}{2}} \pmod q.$$

(3) Det følger fra (1) at

$$2^{\frac{q-1}{2}} = 2^{\frac{(2mp+1)-1}{2}} = 2^{mp} = (2^p)^m.$$

Dermed følger det fra (2) at

$$\mathbb{L}_q^2 \equiv (2^p)^m.$$

(4) Siden $q \mid 2^p - 1$, er

$$2^p - 1 \equiv 0 \pmod q,$$

altså er

$$2^p \equiv 1 \pmod q.$$

(5) Det følger fra (3) og (4) at

$$\mathbb{L}_q^2 \equiv 1^m = 1 \pmod p.$$

Ut ifra Proposisjon 5.5.3 er da $\mathbb{L}_q^2 = 1$.

(6) Det følger fra (5) og Korollar 5.9.21 at enten

$$q \equiv 1 \pmod 8,$$

eller

$$q \equiv 7 \pmod 8.$$

□

Eksempel 5.12.25. Vi har: $2^{11} - 1 = 2047$, og $89 \mid 2047$. Siden 89 er et primtall, fastslår Proposisjon 5.12.24 at enten

$$89 \equiv 1 \pmod 8$$

eller

$$89 \equiv 7 \pmod 8.$$

Det er riktignok sant at

$$89 \equiv 1 \pmod 8.$$

I tillegg har vi: $23 \mid 2047$. Siden 23 er et primtall, fastslår Proposisjon 5.12.24 at enten

$$23 \equiv 1 \pmod 8$$

eller

$$23 \equiv 7 \pmod 8.$$

Det er riktignok sant at

$$23 \equiv 7 \pmod 8.$$

Eksempel 5.12.26. Vi har: $2^{29} - 1 = 536870911$, og en primtallsfaktorisering til 536870911 er

$$233 \cdot 1103 \cdot 2089.$$

Proposisjon 5.12.24 fastslår at enten

$$233 \equiv 1 \pmod 8$$

eller

$$233 \equiv 7 \pmod 8.$$

Det er riktignok sant at

$$233 \equiv 1 \pmod 8.$$

I tillegg fastslår Proposisjon 5.12.24 at enten

$$1103 \equiv 1 \pmod 8$$

eller

$$1103 \equiv 7 \pmod 8.$$

Det er riktignok sant at

$$1103 \equiv 7 \pmod 8.$$

I tillegg fastslår Proposisjon 5.12.24 at enten

$$2089 \equiv 1 \pmod 8$$

eller

$$2089 \equiv 7 \pmod 8.$$

Det er riktignok sant at

$$2089 \equiv 1 \pmod 8.$$

Lemma 5.12.27. La n være et naturlig tall. La m være et naturlig tall slik at $m^2 \leq n$ og $(m+1)^2 > n$. Dersom det finnes et naturlig tall a slik at $a \mid n$, finnes det et naturlig tall b slik at $b \mid n$ og $b \leq m$.

Bevis. Ett av følgende er sant:

(A) $a \leq m$;

(B) $a > m$.

Anta først at (A) er sant. Ved å la b være a, er da lemmaet sant.

Anta istedenfor at (B) er sant. Siden $a \mid n$, finnes det et naturlig tall b slik at $n = ba$. Dersom $b > m$, er

$$n = ba > m \cdot m = m^2.$$

Imidlertid har vi antatt at

$$m^2 \leq n.$$

Siden antakelsen at $b > m$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $b > m$. Derfor er $b \leq m$.

□

Eksempel 5.12.28. La n være 54, og la m være 7. Da er $m^2 = 49 < 54$ og $(m+1)^2 = 8^2 = 64 > 54$. Vi har: $9 \mid 54$. Da fastslår Lemma 5.12.27 at det finnes et naturlig tall b slik at $b \leq 7$ og $b \mid 54$. Dette er riktignok sant: $6 \leq 7$, og $6 \mid 54$.

Eksempel 5.12.29. La n være 86, og la m være 9. Da er $m^2 = 81 < 86$ og $(m+1)^2 = 10^2 = 100 > 86$. Vi har: $43 \mid 86$. Da fastslår Lemma 5.12.27 at det finnes et naturlig tall b slik at $b \leq 9$ og $b \mid 86$. Dette er riktignok sant: $2 \leq 9$, og $2 \mid 86$.

Merknad 5.12.30. For et hvilket som helst naturlig tall n, finnes det faktisk et naturlig tall m slik at $m^2 \leq n$ og $(m+1)^2 > n$, nemlig det størstest naturlige tallet som er mindre enn eller likt $\sqrt{n}$. Når $n = 23$, er for eksempel $\sqrt{23} \approx 4.80$. Derfor er $m = 4$. Det er riktignok sant at $4^2 = 16 \leq 23$ og at $5^2 = 25 > 23$.

Imidlertid er dette resultatet ikke viktig for oss. Derfor kommer vi ikke til å gi et bevis for det.

Korollar 5.12.31. La p være et primtall slik at $p > 2$. La m være et naturlig tall slik at $m^2 \leq 2^p - 1$ og $(m+1)^2 > 2^p - 1$. Dersom $2^p - 1$ ikke er et primtall, finnes det et primtall q slik at $q \mid 2^p - 1$, $q \leq m$, og enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8.$$

Bevis. Vi gjør følgende observasjoner.

(1) Dersom $2^p - 1$ ikke er et primtall, finnes det et naturlig tall a slik at $a \mid 2^p - 1$ og $n > 1$. Ut ifra Lemma 5.12.27, finnes det da et naturlig tall b slik at $b \mid 2^p - 1$ og $b \leq m$.

(2) Ut ifra Korollar 4.3.19, finnes det et primtall q slik at $q \mid b$. Ut ifra Proposisjon 2.5.30 er $q \leq b$, altså $q \leq m$.

(3) Det følger fra (1), (2), og Proposisjon 2.5.27 at $q \mid 2^p - 1$.

(4) Det følger fra Proposisjon 5.12.24 at enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8.$$

□

Eksempel 5.12.32. La oss bevise at $2^7 - 1$ er et primtall. Vi har: $2^7 - 1 = 127$ og $11^2 = 121 < 127$ og $12^2 = 144 > 127$. Anta at $2^7 - 1$ ikke er et primtall. Da følger det fra Korollar 5.12.31 at det finnes et primtall q slik at $q \mid 127$, $q \leq 11$, og enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8.$$

Det eneste primtallet som oppfyller disse kravene er 7. Det er ikke sant at $7 \mid 127$. Vi konkluderer at $2^7 - 1$ er et primtall.

Eksempel 5.12.33. La oss bevise at $2^{13} - 1$ er et primtall. Vi har: $2^{13} - 1 = 8191$ og $90^2 = 8100 < 8191$ og $91^2 = 8281 > 8191$. Anta at $2^{13} - 1$ ikke er et primtall. Vi gjør følgende observasjoner.

(1) Det følger fra Korollar 5.12.31 at det finnes et primtall q slik at $q \mid 8191$, $q \leq 90$, og enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8.$$

(2) Det følger fra Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $q = (2m) \cdot 13 + 1$, altså $q = 26m + 1$.

Det eneste naturlige tallene q slik at $q \leq 90$ som oppfyller (2) er: 27, 53, og 79. Det eneste av disse tre naturlige tallene som er kongruent enten til 1 eller til 7 modulo 8 er 79. Det er ikke sant at $79 \mid 8191$. Vi konkluderer at $2^{13} - 1$ er et primtall.

Eksempel 5.12.34. La oss bevise at $2^{17} - 1$ er et primtall. Vi har: $2^{17} - 1 = 131071$ og $362^2 = 131044 < 131071$ og $363^2 = 131769 > 131071$. Anta at $2^{17} - 1$ ikke er et primtall. Vi gjør følgende observasjoner.

(1) Det følger fra Korollar 5.12.31 at det finnes et primtall q slik at $q \mid 131071$, $q \leq 362$, og enten

$$q \equiv 1 \pmod 8$$

eller

$$q \equiv 7 \pmod 8.$$

(2) Det følger fra Proposisjon 5.12.21 at det finnes et naturlig tall m slik at $q = (2m) \cdot 17 + 1$, altså $q = 34m + 1$.

De eneste naturlige tallene q slik at $q \leq 362$ som oppfyller (2) er:

$$35, 69, 103, 137, 171, 205, 239, 273, 307, 341.$$

De eneste av disse naturlige tallene som er kongruente enten til 1 eller til 7 modulo 8 er: 103, 137, 239, og 273. Ingen av disse fire naturlige tallene deler 131071. Vi konkluderer at $2^{17} - 1$ er et primtall.

Istedenfor å ha sjekket om ett av de fire naturlige tallene 103, 137, 239, og 273 deler 131071, kunne vi ha først observert at 273 ikke er et primtall, og dermed ikke oppfyller (1). Da hadde vært nok å sjekke om ett av de tre naturlige tallene 103, 137, og 239 deler 131071.

Merknad 5.12.35. I Eksempel 5.12.3 fant vi de første fem Mersenne-primtallene: 3, 7, 31, 127, og 8191. Faktisk er det kun 48 kjente Mersenne-primtall! Det 48-ende ble oppdaget i 2013: det er $2^{57885161} - 1$, og har 17425170 sifre. Dette er det største kjente primtallet.

Når datamaskiner leter etter større og større primtall, er Mersenne-primtall hovedsakelig fokuset. Grunnen for dette er at vi kan benytte kvadratisk gjensidighet og andre teoretiske verktøy for å komme fram til resultater som ligner på Proposisjon 5.12.21 og Korollar 5.12.31. Disse resultatene gir oss en bedre forståelse for de naturlige tallene som kan dele et Mersenne-tall enn de naturlige tallene som kan dele et hvilket som helst naturlig tall.

O5 Oppgaver – Kvadratisk gjensidighet

O5.1 Oppgaver i eksamens stil

Oppgave O5.1.1. Gjør følgende.

(1) Vis at 12 er en kvadratisk rest modulo 13.

(2) Benytt (1) for å finne en løsning til kongruensen

$$3x^2 + 7x - 11 \equiv 0 \pmod{13}.$$

Oppgave O5.1.2. Har kongruensen

$$4x^2 + 2x + 1 \equiv 0 \pmod{5}$$

en løsning?

Oppgave O5.1.3. Skriv ned Legendresymbolene $\mathbb{L}_{11}^a$ for alle de heltallene a slik at $0 \leq a \leq 10$. *Tips*: Benytt svaret ditt på Oppgave O4.1.10.

Merknad. Benytt ikke kvadratisk gjensidighet eller proposisjoner som bygger på kvadratisk gjendsidighet i løpet av svarene dine til følgende oppgaver. Benytt imidlertid gjerne Legendresymbolet! Med andre ord, benytt kun teorien vi har sett på opp til slutten av Forelesning 19.

Oppgave O5.1.4. Gjør følgende.

(1) Vis uten å regne ut at
$$2^{26} \equiv -1 \pmod{53}.$$

(2) Vis uten å regne ut at
$$7^{26} \equiv 1 \pmod{53}.$$

(3) Er 173 en kvadratisk rest modulo 53? Benytt Legendresymbolet, (1), og (2) i løpet av svaret ditt.

Oppgave O5.1.5. Er 45 en kvadratisk rest modulo 89? *Tips*: Vis at $5^4 \equiv 2 \pmod{89}$.

Oppgave O5.1.6. Hvor mange løsninger (slik at ingen par av disse er kongruent til hverandre) har følgende kongruenser? Begrunn svaret. Det er ikke nødvendig å *finne* løsninger.

(1) $-4x^2 + 2x - 1 \equiv 0 \pmod{241}$

(2) $7x^2 + 16x + 10 \equiv 0 \pmod{61}$

(3) $9x^2 - 12x + 4 \equiv 0 \pmod{113}$

Oppgave O5.1.7. Finn alle heltallene x slik at

$$x \equiv 3 \pmod{19}$$

og

$$x \equiv 14 \pmod{48}.$$

Oppgave O5.1.8. Finn alle heltallene a slik at vi får resten 5 når vi deler a med 6, resten 2 når vi deler a med 11, resten 2 når vi deler a med 91, og resten 5 når vi deler a med 323.

Merknad. Benytt kvadratisk gjensidighet i løpet av svarene dine på Oppgave 9 og Oppgave 10.

Oppgave O5.1.9. Heltallet 17827 er et primtall. Er 16678 en kvadratisk rest modulo 17827?

Oppgave O5.1.10. Hvor mange løsninger (slik at ingen par av disse er kongruent til hverandre) har kongruensen

$$81x^2 - 44x - 2 \equiv 0 \pmod{3461}?$$

Oppgave O5.1.11. Hvilke av følgende Mersenne-tall er primtall? Begrunn svaret.

(1) $2^{18} - 1$.

(2) $2^{19} - 1$.

(3) $2^{41} - 1$.

Oppgave O5.1.12 (Valgfritt, men anbefalt)**.** Løs Oppgave 2-4 i Øving 9 ved å benytte kvadratisk gjensidighet.

Oppgave O5.1.13 (Valgfritt, men anbefalt)**.** Gjør følgende.

(1) La p være et primtall slik at $p > 2$. Bevis at $\mathbb{L}_p^{-2} = 1$ dersom enten

$$p \equiv 1 \pmod{8}$$

eller

$$p \equiv 3 \pmod{8},$$

og at $\mathbb{L}_p^{-2} = -1$ ellers.

(2) La n være et naturlig tall. Bevis at det finnes et primtall p slik at $p > n$ og

$$p \equiv 3 \pmod{8}.$$

Med andre ord, bevis at det finnes uendelig mange primtall som er kongruent til 3 modulo 8. *Tips*: La q være produktet av alle de primtallene mindre enn eller like n som er kongruent til 3 modulo 8, og benytt en primtallsfaktorisering til $q^2 + 2$. Benytt også (1).

6 Kryptografi

6.1 Totienten

Merknad 6.1.1. La p være et primtall. Fermats lille teorem, altså Korollar 4.10.8, fastslår at, dersom det ikke er sant at

$$x \equiv 0 \pmod{p},$$

er

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

Vi har sett at dette resultatet er svært nyttig.

Hva om vi erstatter p med et hvilket som helst naturlig tall? Er et lignende utsagn sant? Det er visselig ikke nødvendigvis sant at

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

når n ikke er et primtall. For eksempel er

$$27 \equiv 3 \pmod{4},$$

altså

$$3^{4-1} \equiv 3 \pmod{4},$$

og det er ikke sant at

$$3 \equiv 1 \pmod{4}.$$

Likevel kan Fermats lille teorem generalises, ved å ertsatte potensen $p-1$ med noe som kalles totienten til n. Nå kommer vi til å se på dette resultatet, som kalles Eulers teorem, og etterpå til å utforske hvordan det benyttes i kryptografi.

Definisjon 6.1.2. La n være et naturlig tall. Da er *totienten* til n antall naturlige tall x slik at $x \leq n$ og $\mathsf{sfd}(x, n) = 1$.

Notasjon 6.1.3. La n være et naturlig tall. Vi betegner totienten til n som $\phi(n)$.

Eksempel 6.1.4. Det eneste naturlige tallet x slik at $x \leq 1$ er 1. Det er sant at $\mathsf{sfd}(1, 1) = 1$. Dermed er $\phi(1) = 1$.

Eksempel 6.1.5. De eneste naturlige tallene x slik at $x \leq 2$ er 1 og 2. Det er sant at $\mathsf{sfd}(1, 2) = 1$, men $\mathsf{sfd}(2, 2) = 2$. Dermed er 1 det eneste naturlige tallet x slik at $x \leq 2$ og $\mathsf{sfd}(x, 2) = 1$. Således er $\phi(2) = 1$.

Eksempel 6.1.6. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(3)$.

x	$\mathsf{sfd}(x, 3)$	Bidrar til $\phi(3)$?
1	1	✓
2	1	✓
3	3	✗

Dermed finnes det to naturlige tall x slik at $x \leq 3$ og $\mathsf{sfd}(x, 3) = 1$. Således er $\phi(3) = 2$.

Eksempel 6.1.7. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(4)$.

x	$\mathsf{sfd}(x, 4)$	Bidrar til $\phi(4)$?
1	1	✓
2	2	✗
3	1	✓
4	4	✗

Dermed finnes det to naturlige tall x slik at $x \leq 4$ og $\mathsf{sfd}(x, 4) = 1$. Således er $\phi(4) = 2$.

Eksempel 6.1.8. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(5)$.

x	$\mathsf{sfd}(x, 5)$	Bidrar til $\phi(5)$?
1	1	✓
2	1	✓
3	1	✓
4	1	✓
5	5	✗

Dermed finnes det fire naturlige tall x slik at $x \leq 5$ og $\mathsf{sfd}(x, 5) = 1$. Således er $\phi(5) = 4$.

Eksempel 6.1.9. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(6)$.

x	$\mathsf{sfd}(x, 6)$	Bidrar til $\phi(6)$?
1	1	✓
2	2	✗
3	3	✗
4	2	✗
5	1	✓
6	6	✗

Dermed finnes det to naturlige tall x slik at $x \leq 6$ og $\mathsf{sfd}(x, 6) = 1$. Således er $\phi(6) = 2$.

Eksempel 6.1.10. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(10)$.

x	$\mathsf{sfd}(x, 10)$	Bidrar til $\phi(10)$?
1	1	✓
2	2	✗
3	1	✓
4	2	✗
5	5	✗
6	2	✗
7	1	✓
8	2	✗
9	1	✓
10	10	✗

Dermed finnes det fire naturlige tall x slik at $x \leq 10$ og $\mathsf{sfd}(x, 10) = 1$. Således er $\phi(10) = 4$.

Eksempel 6.1.11. Tabellen nedenfor viser informasjonen som behøves for å regne ut $\phi(12)$.

x	$\mathsf{sfd}(x, 12)$	Bidrar til $\phi(12)$?
1	1	✓
2	2	✗
3	3	✗
4	4	✗
5	1	✓
6	3	✗
7	1	✓
8	4	✗
9	3	✗
10	2	✗
11	1	✓
12	12	✗

Dermed finnes det fire naturlige tall x slik at $x \leq 12$ og $\mathsf{sfd}(x, 12) = 1$. Således er $\phi(12) = 4$.

Proposisjon 6.1.12. La n være et naturlig tall. Da er $\phi(n) = n - 1$ om og bare om n er et primtall.

Bevis. Anta først at n er et primtall. Vi gjør følgende observasjoner.

(1) Ut ifra Korollar 4.2.5, er da $\mathsf{sfd}(x, n) = 1$ for et hvilket som helst naturlig tall x slik at $x \leq n - 1$.

(2) Vi har: $\mathsf{sfd}(n, n) = n$. Siden n er et primtall, er $n > 1$. Dermed er $\mathsf{sfd}(n, n) \neq 1$.

Vi konkluderer at $\phi(n) = n - 1$.

Anta istedenfor at $\phi(n) = n - 1$. Vi gjør følgende observasjoner.

(1) Vi har: $\mathsf{sfd}(n, n) = n$. Siden $\phi(1) = 1$, er det ikke sant at $n = 1$. Derfor er $n \geq 2$. Dermed er $\mathsf{sfd}(n, n) \neq 1$.

(2) Det følger fra (1) at $\phi(n)$ antall naturlige tall x slik at $x \leq n - 1$ og $\mathsf{sfd}(x, n) = 1$. Siden $\phi(n) = n - 1$, følger det at $\mathsf{sfd}(x, n) = 1$ for alle de naturlige tallene x slik at $x \leq n - 1$.

(3) La x være et naturlig tall slik at $x \mid n$. Da er $\mathsf{sfd}(x, n) = x$.

Det følger fra (2) og (3) at, dersom x er et naturlig tall slik at $x \mid n$ og $x \neq n$, er $x = 1$. Derfor er n et primtall.

□

Eksempel 6.1.13. Proposisjon 6.1.12 fastslår at $\phi(3) = 2$. Ut ifra Eksempel 6.1.6 er dette riktignok sant.

Eksempel 6.1.14. Ut ifra Eksempel 6.1.8 er $\phi(5) = 4$. Da fastslår Proposisjon 6.1.12 at 5 er et primtall. Dette er riktignok sant.

Lemma 6.1.15. La p være et primtall. La n være et naturlig tall. La y være et naturlig tall slik at $y \mid p^n$ og $y > 1$. Da har vi: $p \mid y$.

Bevis. Ut ifra Korollar 4.3.19 finnes det et primtall q slik at $q \mid y$. Ut ifra Proposisjon **??** har vi da: $q \mid p^n$. Det følger fra Korollar 4.2.23 at $q = p$. Siden $q \mid y$, konkluderer vi at $p \mid y$. □

Eksempel 6.1.16. Vi har: $9 \mid 27$, altså $9 \mid 3^3$. Siden 3 er et primtall, fastlår Lemma 6.1.15 at $3 \mid 9$. Dette er rikignok sant.

Eksempel 6.1.17. Vi har: $16 \mid 64$, altså $16 \mid 2^6$. Siden 2 er et primtall, fastlår Lemma 6.1.15 at $2 \mid 16$. Dette er riktignok sant.

Proposisjon 6.1.18. La p være et primtall. La n være et naturlig tall. Da er $\phi(p^n) = p^n - p^{n-1}$.

Bevis. La x være et naturlig tall slik at $x \leq p^n$ og $\mathsf{sfd}(x, p^n) \neq 1$. Vi gjør følgende observasjoner.

(1) Da finnes det et naturlig tall y slik at $y \mid x$ og $y \mid p^n$, og slik at $y > 1$. Siden $y \mid p^n$, følger det fra Lemma 6.1.15 at $p \mid y$. Dermed er $y = kp$, hvor k er et naturlig tall.

(2) Siden $y \mid x$, finnes det et naturlig tall l slik at $x = ly$. Dermed er $x = l(kp)$, altså $x = (kl)p$. La oss betegne det naturlige tallet kl som m.

(3) Siden $x \leq p^n$, altså $mp \leq p^n$, er $m \leq p^{n-1}$.

La nå m være et hvilket som helst naturlig tall slik at $m \leq p^{n-1}$. Da har vi: $p \mid mp$ og $p \mid p^{n-1}$. Derfor er $\mathsf{sfd}(mp, p^n) \geq p$, altså $\mathsf{sfd}(mp, p^n) > 1$.
Således har vi bevist:

(A) dersom $x \leq p^n$ og $\mathsf{sfd}(x, p^n) \neq 1$, finnes det et naturlig tall m slik at $m \leq p^{n-1}$ og $x = mp$;

(B) dersom m er et naturlig tall slik at $m \leq p^{n-1}$, er $\mathsf{sfd}(mp, p^n) \neq 1$.

Det følger at de naturlige tallene x slik at $x \leq p^n$ og $\mathsf{sfd}(x, p^n) \neq 1$ er akkurat de naturlige tallene p, $2p$, $3p$, $\ldots$, $\left(p^{n-1}\right) p$. Denne lista består av akkurat p^{n-1} ulike naturlige tall. Siden antall naturlige tall x slik at $x \leq p^n$ er p^n, konkluderer vi at antall naturlige tall slik at $x \leq p^n$ og $\mathsf{sfd}(x, p^n) = 1$ er $p^n - p^{n-1}$, altså at $\phi\left(p^n\right) = p^n - p^{n-1}$.

□

Eksempel 6.1.19. Proposisjon 6.1.18 fastslår at $\phi(2^2) = 2^2 - 2^1$, altså at $\phi(4) = 2$. Ut ifra Eksempel 6.1.7 er dette riktignok sant.

Eksempel 6.1.20. Proposisjon 6.1.18 fastslår at $\phi(3^2) = 3^2 - 3^1$, altså at $\phi(9) = 6$. Følgende tabell viser at dette riktignok er sant.

x	$\mathsf{sfd}(x, 9)$	Bidrar til $\phi(9)$?
1	1	✓
2	1	✓
3	3	✗
4	1	✓
5	1	✓
6	3	✗
7	1	✓
8	1	✓
9	9	✗

Som fastslått av beviset for Proposisjon 6.1.18, er det de naturlige tallene 3, 6, og 9, altså 3, $2 \cdot 3$, og $3 \cdot 3$, som ikke bidrar til $\phi(9)$.

Eksempel 6.1.21. Proposisjon 6.1.18 fastslår at $\phi(2^3) = 2^3 - 2^2$, altså at $\phi(8) = 4$. Følgende tabell viser at dette riktignok er sant.

x	$\mathsf{sfd}(x, 8)$	Bidrar til $\phi(8)$?
1	1	✓
2	2	✗
3	1	✓
4	4	✗
5	1	✓
6	2	✗
7	1	✓
8	8	✗

Som fastslått av beviset for Proposisjon 6.1.18, er det de naturlige tallene 2, 4, 6, og 8, altså 2, $2 \cdot 2$, $3 \cdot 2$, og $4 \cdot 2$, som ikke bidrar til $\phi(8)$.

6.2 Eulers teorem

Merknad 6.2.1. Vi kommer til å bygge på følgende proposisjon, som er viktig i seg selv, for å gi et bevis for Eulers teorem.

Proposisjon 6.2.2. La m og n være naturlige tall slik at $\mathsf{sfd}(m, n) = 1$. Da er $\phi(mn) = \phi(m) \cdot \phi(n)$.

Bevis. Ut ifra Eksempel 6.1.4 er $\phi(1) = 1$. Det følger umiddelbart at utsagnet er sant når $m = 1$ eller når $n = 1$.

Anta at $m > 1$ og at $n > 1$. Ut ifra definisjonen til $\phi(m)$, finnes det $\phi(m)$ naturlige tall x slik at $\mathsf{sfd}(x, m) = 1$. La oss betegne disse naturlige tallene som x_1, x_2, …, $x_{\phi(m)}$.

Ut ifra definisjonen til $\phi(n)$, finnes det $\phi(n)$ naturlige tall y slik at $\mathsf{sfd}(y, n) = 1$. La oss betegne disse naturlige tallene som y_1, y_2, …, $y_{\phi(n)}$.

Ut ifra Proposisjon 3.2.1 finnes det, for hvert naturlig tall i slik at $i \leq \phi(m)$ og hvert naturlig tall j slik at $j \leq \phi(n)$, et naturlig tall $r_{i,j}$ slik at

$$nx_i + my_j \equiv r_{i,j} \pmod{mn}$$

og $0 \leq r_{i,j} < mn$.

Anta at følgende utsagn har blitt bevist.

(A) For hvert naturlig tall i slik at $i \leq \phi(m)$, og hvert naturlig tall j slik at $j \leq \phi(n)$, er $\mathsf{sfd}(r_{i,j}, mn) = 1$.

(B) La nå i og i' være naturlige tall slik at $i \leq \phi(m)$ og $i' \leq \phi(m)$. La j og j' være naturlige tall slik at $j \leq \phi(n)$ og $j' \leq \phi(n)$. Da er $r_{i,j} = r_{i',j'}$ om og bare om $x_i = x_{i'}$ og $y_j = y_{j'}$.

(C) Dersom z er et naturlig tall slik at $z < mn$ og $\mathsf{sfd}(z, mn) = 1$, finnes det et naturlig tall i og et naturlig tall j slik at $z = r_{i,j}$.

Det følger fra (A) og (C) at $\phi(mn)$ er antall ulike naturlige tall blant de naturlige tallene $r_{i,j}$, hvor i er et naturlig tall slik at $i \leq \phi(m)$, og j er et naturlig tall slik at $j \leq \phi(n)$. Siden alle de naturlige tallene $x_1, x_2, \ldots, x_{\phi(m)}$ er ulike, og siden alle de naturlige tallene $y_1, y_2, \ldots, y_{\phi(n)}$ er ulike, følger det fra (B) at alle de naturlige tallene $r_{i,j}$ er ulike, hvor $i \leq \phi(m)$ og $j \leq \phi(n)$, altså at det er akkurat $\phi(m) \cdot \phi(n)$ av dem. Vi konkluderer at

$$\phi(mn) = \phi(m) \cdot \phi(n).$$

La oss nå bevise at (A) – (C) er sanne. La i være et naturlig tall slik at $i \leq \phi(m)$. La j være et naturlig tall slik at $j \leq \phi(n)$. La z være et naturlig tall slik at $z \mid r_{i,j}$ og $z \mid mn$. Vi gjør følgende observasjoner.

(1) Siden

$$nx_i + my_j \equiv r_{i,j} \pmod{mn},$$

følger det da fra Proposisjon **??** og antakelsen $z \mid r_{i,j}$ at

$$nx_i + my_j \equiv 0 \pmod{z},$$

altså at

$$z \mid nx_i + my_j.$$

(2) Dersom $z > 1$, følger det fra Korollar 4.3.19 at det finnes et primtall p slik at $p \mid z$. Da følger det fra (1) og Proposisjon 2.5.27 at $p \mid nx_i + my_j$.

(3) Siden $p \mid z$ og $z \mid mn$, følger det fra Proposisjon 2.5.27 at $p \mid mn$. Siden p er et primtall, følger det da fra Proposisjon 4.2.12 at enten $p \mid m$ eller $p \mid n$.

(4) Anta først at $p \mid m$. Siden $\mathsf{sfd}(m, n) = 1$, er det da ikke sant at $p \mid n$.

(5) Siden $p \mid m$, følger det fra Korollar 2.5.18 at $p \mid -my_j$.

(6) Det følger fra (3), (5), og Proposisjon 2.5.24 at

$$p \mid (nx_i + my_j) - my_j,$$

altså at $p \mid nx_i$.

(7) Siden det ikke er sant, ut ifra (4), at $p \mid n$, følger det fra (6) og Proposisjon 4.2.12 at $p \mid x_i$. Siden vi har antatt at $p \mid m$, er da $\mathsf{sfd}(x_i, m) \geq p$.

(8) Ut ifra definisjonen til x_i, er imidlertid $\mathsf{sfd}(x_i, m) = 1$. Siden antakelsen at $p \mid m$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $p \mid m$.

(9) Anta istedenfor at $p \mid n$. Et lignende argument som i (4) – (7) fastslår at det da finnes et primtall q slik at $\mathsf{sfd}(y_j, n) \geq q$. Ut ifra definisjonen til y_j, er imidlertid $\mathsf{sfd}(y_j, n) = 1$. Siden antakelsen at $p \mid n$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $p \mid n$.

(10) Dermed har vi en motsigelse: (2) fastslår at enten $p \mid m$ eller $p \mid n$, mens (8) og (9) fastslår at verken $p \mid m$ eller $p \mid n$. Siden antakelsen at $z > 1$ fører til denne motsigelsen, konkluderer vi at $z = 1$.

Således har vi bevist at, dersom $z \mid r_{i,j}$ og $z \mid mn$, er $z = 1$. Vi konkluderer at $\mathsf{sfd}(r_{i,j}, mn) = 1$, altså at (A) er sant.

La nå i og i' være naturlige tall slik at $i \leq \phi(m)$ og $i' \leq \phi(m)$. La j og j' være naturlige tall slik at $j \leq \phi(n)$ og $j' \leq \phi(n')$. Anta at $r_{i,j} = r_{i',j'}$. Da er

$$ns_i + my_j \equiv nx_{i'} + my_{j'} \pmod{mn}.$$

Vi gjør følgende observasjoner.

(1) Det følger at

$$n(x_i - x_{i'}) + m(y_j - y_{j'}) \equiv 0 \pmod{mn}.$$

Derfor har vi:

$$mn \mid n(x_i - x_{i'}) + m(y_j - y_{j'}).$$

(2) Dermed finnes det et heltall k slik at

$$n(x_i - x_{i'}) + m(y_j - y_{j'}) = k(mn),$$

altså slik at

$$n(x_i - x_{i'}) = \big(y_{j'} - y_j + kn\big)m.$$

Således har vi: $m \mid n(x_i - x_{i'})$.

(3) Ut ifra Proposisjon 2.8.22 har vi da: enten $m \mid n$ eller $m \mid x_i - x_{i'}$.

(4) Dersom $m \mid n$, følger det fra Proposisjon 2.6.21 at $\mathsf{sfd}(m, n) = m$. Imidlertid har vi antatt at $\mathsf{sfd}(m, n) = 1$. Siden $m > 1$, har vi da en motsigelse. Siden antakelsen at $m \mid n$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $m \mid n$.

(5) Dersom $m \mid x_i - x_{i'}$, er

$$x_i \equiv x_{i'} \pmod{m}.$$

Siden $x_i < m$ og $x_{i'} < m$, følger det fra Proposisjon 3.2.11 at $x_i = x_{i'}$.

(6) Et lignende argument som i (1) – (5) fastslår at $n \mid m(y_{j'} - y_j)$, og deretter at $y_{j'} = y_j$.

Således har vi bevist at, dersom $r_{i,j} = r_{i',j'}$, er $x_i = x_{i'}$ og $y_j = y_{j'}$. Dermed er (B) sant.

La nå z være et naturlig tall slik at $z < mn$ og $\mathsf{sfd}(z, mn) = 1$. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 2.8.30 er da $\mathsf{sfd}(m, z) = 1$.

(2) Ut ifra Proposisjon 2.2.6, finnes et naturlig tall k og et naturlig tall r slik at $0 \leq r < m - 1$ og

$$z = km + r.$$

(3) Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(m, r) = \mathsf{sfd}(z, m)$.

(4) Det følger fra (1) og (3) at $\mathsf{sfd}(m, r) = 1$. Ut ifra definisjonen til de naturlige tallene x_1, x_2, ..., $x_{\phi(m)}$, finnes det derfor et naturlig tall i slik at $i \leq \phi(m)$ og $r = x_i$. Dermed er

$$km + r \equiv 0 + x_i \pmod{m},$$

altså er

$$z \equiv x_i \pmod{m}.$$

(5) Ut ifra Proposisjon 2.8.30 er $\mathsf{sfd}(n, z) = 1$. Et lignende argument som i (2) – (4) fastslår da at det finnes et naturlig tall j slik at $j \leq \phi(n)$ og

$$z \equiv y_j \pmod{n}.$$

(6) Ut ifra (4) og (5) er $x = z$ en løsning både til kongruensen

$$x \equiv x_i \pmod{m}$$

og til kongruensen

$$x \equiv y_j \pmod{n}.$$

Siden $\mathsf{sfd}(m, n) = 1$, følger det fra Proposisjon 5.7.2 (I) at $x = nx_i + my_j$ også er en løsning til begge kongruensene.

(7) Det følger fra (6) og Proposisjon 5.7.2 (II) at

$$z \equiv nx_i + my_j \pmod{mn},$$

altså at

$$z \equiv r_{i,j} \pmod{mn}.$$

Siden $z < mn$ og $r_{i,j} < mn$, følger det fra Proposisjon 3.2.11 at $z = r_{i,j}$.

Således har vi bevist at, dersom $z < mn$ og $\mathsf{sfd}(z, mn) = 1$, finnes det et naturlig tall i og et naturlig tall j slik at $z = r_{i,j}$, hvor $i \leq \phi(m)$ og $j \leq \phi(n)$. Dermed er (C) sant. □

Eksempel 6.2.3. Ut ifra Eksempel 6.1.6 er $\phi(3) = 2$. Ut ifra Eksempel 6.1.7 er $\phi(4) = 2$. Da fastslår Proposisjon 6.2.2 at $\phi(3 \cdot 4) = \phi(3) \cdot \phi(4)$, altså at $\phi(12) = 2 \cdot 2 = 4$. Ut ifra Eksempel 6.1.11 er dette riktignok sant.

Ut ifra Eksempel 6.1.6 er 1 og 2 de to naturlige tallene x slik at $x \leq 3$ og $\mathsf{sfd}(x, 3) = 1$. Ut ifra Eksempel 6.1.7 er 1 og 3 de to naturlige tallene x slik at $x \leq 4$ og $\mathsf{sfd}(x, 4) = 1$. Da fastslår beviset for Proposisjon 6.2.2 at de naturlige tallene x slik at $x \leq 12$ og $\mathsf{sfd}(x, 12) = 1$ er kongruent modulo 12 til $4 \cdot 1 + 3 \cdot 1$, $4 \cdot 1 + 3 \cdot 3$, $4 \cdot 2 + 3 \cdot 1$, og $4 \cdot 2 + 3 \cdot 3$, altså til 7, 13, 11, og 17. De naturlige tallene x slik at $x \leq 12$ som er kongruent modulo 12 til disse er: 7, 1, 11, og 5. Ut ifra Eksempel 6.1.11 er det riktignok disse fire naturlige tallene som bidrar til $\phi(12)$.

Eksempel 6.2.4. Ut ifra Eksempel 6.1.8 er $\phi(5) = 4$. Ut ifra Eksempel **??** er $\phi(6) = 2$. Da fastslår Proposisjon 6.2.2 at $\phi(5 \cdot 6) = \phi(5) \cdot \phi(6)$, altså at $\phi(30) = 4 \cdot 2 = 8$.

Ut ifra Eksempel 6.1.8 er 1, 2, 3, og 4 de fire naturlige tallene x slik at $x \leq 5$ og $\mathsf{sfd}(x, 5) = 1$. Ut ifra Eksempel **??** er 1 og 5 de to naturlige tallene x slik at $x \leq 6$ og $\mathsf{sfd}(x, 6) = 1$. Da fastslår beviset for Proposisjon 6.2.2 at de naturlige tallene x slik at $x \leq 30$ og $\mathsf{sfd}(x, 30) = 1$ er kongruent modulo 30 til $6 \cdot 1 + 5 \cdot 1$, $6 \cdot 1 + 5 \cdot 5$, $6 \cdot 2 + 5 \cdot 1$, $6 \cdot 2 + 5 \cdot 5$, $6 \cdot 3 + 5 \cdot 1$, $6 \cdot 3 + 5 \cdot 5$, $6 \cdot 4 + 5 \cdot 1$, og $6 \cdot 4 + 5 \cdot 5$, altså til 11, 31, 17, 37, 23, 43, 29, og 49. De naturlige tallene x slik at $x \leq 30$ som er kongruent modulo 30 til disse er: 11, 1, 17, 7, 23, 13, 29, og 19.

Merknad 6.2.5. Proposisjon 6.2.2 er ikke nødvendigvis sant om vi ikke antar at $\mathsf{sfd}(m, n) = 1$. Ut ifra Eksempel 6.1.5 er $\phi(2) = 1$. Derfor er $\phi(2) \cdot \phi(2) = 1 \cdot 1 = 1$. Ut ifra Eksempel 6.1.7 er imidlertid $\phi(2 \cdot 2) = \phi(4) = 2$.

For et annet eksempel, er, ut ifra Eksempel 6.1.7, $\phi(4) = 2$. Ut ifra Eksempel 6.1.7, er $\phi(6) = 2$. Imidlertid viser følgende tabell at $\phi(24) = 8$.

x	$\mathsf{sfd}(x, 24)$	Bidrar til $\phi(24)$?
1	1	✓
2	2	✗
3	3	✗
4	4	✗
5	1	✓
6	6	✗
7	1	✓
8	8	✗
9	1	✓
10	2	✗
11	1	✓
12	12	✗
13	1	✓
14	2	✗
15	3	✗
16	8	✗
17	1	✓
18	6	✗
19	1	✓
20	4	✗
21	3	✗
22	2	✗
23	1	✓
24	24	✗

Merknad 6.2.6. At Proposisjon 6.2.2 er sann gir oss muligheten til å benytte oss av en kraftig og begrepsmessig tilnærmingsmetode for å bevise en proposisjon om totienten til et hvilket som helst naturlig tall n:

(1) Observer at, ut ifra Korollar 4.3.16, finnes det en primtallsfaktorisering

$$n = p_1^{k^1} p_2^{k_2} \cdots p_t^{k_t}$$

til n slik at $p_i \neq p_j$ dersom $i \neq j$.

(2) Siden $p_i \neq p_j$ dersom $i \neq j$, følger det fra Korollar 4.2.9 at $\mathsf{sfd}(p_i^{k_i}, p_j^{k_j}) = 1$ dersom $i \neq j$. Observer at, ut ifra Proposisjon 6.2.2, er da

$$\phi(n) = \phi\left(p_1^{k_1}\right) \phi\left(p_2^{k_2}\right) \cdots \phi\left(p_t^{k_t}\right).$$

(3) Bevis at proposisjonen er sann når $n = q$, hvor q er et primtall.

(4) Benytt (2) og (3) for å gi et bevis for proposisjonen når n er et hvilket som helst naturlig tall.

Vi kommer nå til å benytte oss av denne tilnærmingsmetoden for å gi et bevis for Eulers teorem.

Proposisjon 6.2.7. La p være et primtall. La n være et naturlig tall. La x være et heltall slik at det ikke er sant at

$$x \equiv 0 \pmod{p}.$$

Da er

$$x^{\phi(p^n)} \equiv 1 \pmod{p^n}.$$

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. I dette tilfellet er utsagnet at

$$x^{\phi(p)} \equiv 1 \pmod{p}.$$

Ut ifra Proposisjon 6.1.12 er $\phi(p) = p - 1$. Derfor er utsagnet at

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

Ut ifra Korollar 4.10.8 er dette sant.

Anta nå at proposisjonen har blitt bevist når $n = m$, hvor m et et gitt naturlig tall. Således har det blitt bevist at

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

Vi gjør følgende observasjoner.

(1) Da har vi: $p^m \mid x^{\phi(p^m)} - 1$. Dermed finnes det et naturlig tall k slik at

$$x^{\phi(p^m)} - 1 = kp^m,$$

altså slik at

$$x^{\phi(p^m)} = 1 + kp^m.$$

(2) Ut ifra Proposisjon 6.1.18 er

$$\phi\left(p^{m+1}\right) = p^{m+1} - p^m = p\left(p^m - p^{m-1}\right).$$

Det følger også fra Proposisjon 6.1.18 at

$$\phi\left(p^m\right) = p^m - p^{m-1}.$$

Dermed er

$$\phi\left(p^{m+1}\right) = p\phi\left(p^m\right).$$

(3) Det følger fra (1) og (2) at

$$\begin{aligned} x^{\phi\left(p^{m+1}\right)} &= x^{p\phi(p^m)} \\ &= \left(x^{\phi(p^m)}\right)^p \\ &= (1 + kp^m)^p \end{aligned}$$

(4) Ut ifra Proposisjon 1.9.30 er

$$\begin{aligned} (1 + kp^m)^p &= \sum_{i=0}^{p} \binom{p}{i} 1^{p-i} \left(kp^m\right)^i \\ &= 1 + \binom{p}{1} \cdot \left(kp^m\right)^1 + \cdots + \binom{p}{p-1} \left(kp^m\right)^{p-1} + \left(kp^m\right)^p. \end{aligned}$$

(5) For hvert naturlig tall i slik at $i \geq 2$, er

$$im \geq 2m \geq m + 1.$$

Derfor er

$$im - (m + 1) \geq 0.$$

Siden

$$p^{im} = p^{im-(m+1)} p^{m+1},$$

har vi da: $p^{m+1} \mid p^{im}$. Det følger fra Korollar 2.5.18 at $p^{m+1} \mid kp^{im}$, altså at $p^{m+1} \mid (kp)^i$. Således er

$$(kp)^i \equiv 0 \pmod{p^{m+1}}.$$

(6) Siden $\binom{p}{1} = p$, er

$$\binom{p}{1} kp^m = kpm + 1.$$

Siden $p^{m+1} \mid kp^{m+1}$, har vi da:

$$p^{m+1} \mid \binom{p}{1} kp^m.$$

Derfor er

$$\binom{p}{1} kp^m \equiv 0 \pmod{p^{m+1}}.$$

(7) Ut ifra (5) og (6) er

$$\begin{aligned} &1 + \binom{p}{1} \cdot (kp^m)^1 + \cdots + \binom{p}{p-1} (kp^m)^{p-1} + (kp^m)^p \\ &\equiv 1 + 0 + \cdots + 0 + 0 \pmod{p^{m+1}}, \end{aligned}$$

altså

$$1 + \binom{p}{1} \cdot (kp^m)^1 + \cdots + \binom{p}{p-1} (kp^m)^{p-1} + (kp^m)^p \equiv 1 \pmod{p^{m+1}}.$$

Det følger fra (3), (4), og (7) at

$$x^{\phi\left(p^{m+1}\right)} \equiv 1 \pmod{p^{m+1}}.$$

Således er proposisjonen sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann når n er et hvilket som helst naturlig tall.

□

Eksempel 6.2.8. Ut ifra Eksempel 6.1.21 er $\phi(8) = 4$, altså $\phi\left(2^3\right) = 4$. Da fastslår Proposisjon 6.2.7 at

$$x^4 \equiv 1 \pmod{8}$$

for et hvilket som helst heltall x slik at det ikke er sant at

$$x \equiv 0 \pmod{2}.$$

For eksempel:

$$5^4 \equiv 1 \pmod{8}.$$

Riktignok har vi:

$$5^4 = \left(5^2\right)^2 = 25^2 \equiv 1^2 = 1 \pmod{8}.$$

Eksempel 6.2.9. Ut ifra Eksempel 6.1.20 er $\phi(9) = 6$, altså $\phi\left(3^2\right) = 6$. Da fastslår Proposisjon 6.2.7 at

$$x^6 \equiv 1 \pmod{9}$$

for et hvilket som helst heltall x slik at det ikke er sant at

$$x \equiv 0 \pmod{3}.$$

For eksempel:

$$4^6 \equiv 1 \pmod{9}.$$

Riktignok har vi:

$$4^6 = \left(4^3\right)^2 = 64^2 \equiv 1^2 = 1 \pmod{9}.$$

Proposisjon 6.2.10. La n være et naturlig tall. La x være et heltall slik at $\mathsf{sfd}(x, n) = 1$. Da er

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Korollar 4.3.16, finnes det et naturlig tall t og primtall p_1, p_2, ..., p_t slik at

$$n = p_1^{k^1} p_2^{k_2} \cdots p_t^{k_t},$$

og $p_i \neq p_j$ dersom $i \neq j$.

(2) Siden $p_i \neq p_j$ dersom $i \neq j$, følger det fra Korollar 4.2.9 at $\mathsf{sfd}(p_i^{k_i}, p_j^{k_j}) = 1$ dersom $i \neq j$. Ved å benytte Korollar **??** gjentatte ganger, følger det at

$$\mathsf{sfd}(p_1^{k_1} \cdots p_{i-1}^{k_{t-1}}, p_i^{k_i}) = 1$$

for et hvilket som helst naturlig tall i slik at $2 \leq i \leq t$.

(3) Ut ifra Proposisjon 6.2.2, er da

$$\phi(n) = \phi\left(p_1^{k_1}\right) \phi\left(p_2^{k_2}\right) \cdots \phi\left(p_t^{k_t}\right).$$

(4) La i være et naturlig tall slik at $i \leq t$. La m_i være

$$\phi\left(p_1^{k_1}\right) \cdots \phi\left(p_{i-1}^{k_{i-1}}\right) \phi\left(p_{i+1}^{k_{i+1}}\right) \cdots \phi\left(p_t^{k_t}\right).$$

Ut ifra (3), er $\phi(n) = m_i \phi\left(p_i^{k_i}\right)$.

(5) Dermed er

$$x^{\phi(n)} = x^{m_i \phi\left(p_i^{k_i}\right)} = \left(x^{\phi\left(p_i^{k_i}\right)}\right)^{m_i}.$$

(6) Siden $\mathsf{sfd}(x, n) = 1$, og siden $p_i \mid n$, er det ikke sant at $p_i \mid x$. Ut ifra Proposisjon 6.2.7 er da, for hvert naturlig tall i slik at $i \leq t$,

$$x^{\phi\left(p_i^{k_i}\right)} \equiv 1 \pmod{p_i^{k_i}}.$$

(7) Det følger fra (5) og (6) at

$$x^{\phi(n)} \equiv 1^{m_i} = 1 \pmod{p_i^{k_i}}.$$

Således har vi bevist at, for hvert naturlig tall i slik at $i \leq t$, er

$$x^{\phi(n)} \equiv 1 \pmod{p_i^{k_i}}.$$

Siden

$$\mathsf{sfd}(p_1^{k_1} \cdots p_{i-1}^{k_{t-1}}, p_i^{k_i}) = 1$$

for et hvilket som helst naturlig tall i slik at $2 \leq i \leq t$, følger det fra Korollar 5.7.30 at

$$x^{\phi(n)} \equiv 1 \pmod{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}},$$

altså at

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$

□

Terminologi 6.2.11. Proposisjon 6.2.10 kalles *Eulers teorem.*

Eksempel 6.2.12. Ut ifra Eksempel 6.1.21 er $\phi(8) = 4$. Da fastslår Proposisjon 6.2.10 at, for et hvilket som helst heltall x slik at $\mathsf{sfd}(x, 8) = 1$, er

$$x^4 \equiv 1 \pmod{8}.$$

For eksempel:

$$3^4 \equiv 1 \pmod{8}.$$

Riktignok har vi:

$$3^4 = \left(3^2\right)^2 \equiv 1^2 = 1 \pmod{8}.$$

Eksempel 6.2.13. Ut ifra Merknad 6.2.5 er $\phi(24) = 8$. Da fastslår Proposisjon 6.2.10 at, for et hvilket som helst heltall x slik at $\mathsf{sfd}(x, 24) = 1$, er

$$x^8 \equiv 1 \pmod{24}.$$

For eksempel:

$$7^8 \equiv 1 \pmod{24}.$$

Riktignok har vi:

$$7^8 = \left(7^2\right)^4 \equiv 1^4 = 1 \pmod{24}.$$

Merknad 6.2.14. Følgende korollar er kjernen til RSA-algoritmen, som vi kommer til å se på i den neste delen av kapittelet.

Korollar 6.2.15. La n være et naturlig tall. La a være et heltall slik at $\mathsf{sfd}(a, \phi(n)) = 1$. Ut ifra Korollar 3.4.39, finnes det da et heltall b slik at

$$ab \equiv 1 \pmod{\phi(n)}.$$

La x være et heltall slik at $\mathsf{sfd}(x, n) = 1$. Da er

$$(x^a)^b \equiv x \pmod{n}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Siden
$$ab \equiv 1 \pmod{\phi(n)},$$
har vi: $\phi(n) \mid ab - 1$. Dermed finnes det et naturlig tall k slik at $ab - 1 = k\phi(n)$, altså slik at $ab = 1 + k\phi(n)$.

(2) Da er
$$\begin{aligned}(x^a)^b &= x^{ab} \\ &= x^{1+k\phi(n)} \\ &= x^1 \cdot x^{k\phi(n)} \\ &= x \cdot \left(x^{\phi(n)}\right)^k.\end{aligned}$$

(3) Ut ifra Proposisjon 6.2.10 er
$$x^{\phi(n)} \equiv 1 \pmod{n}.$$
Dermed er
$$x \cdot \left(x^{\phi(n)}\right)^k \equiv x \cdot 1^k = x \pmod{n}.$$

(4) Det følger fra (2) og (3) at
$$(x^a)^b \equiv x \pmod{n}.$$

□

Eksempel 6.2.16. Vi har:

(1) $\phi(11) = 10$;

(2) $\mathsf{sfd}(3, 10) = 1$;

(3) $3 \cdot 7 = 21 \equiv 1 \pmod{10}$.

Da fastslår Korollar 6.2.15 at, for et hvilket som helst heltall x slik at $\mathsf{sfd}(x, 11) = 1$, er
$$\left(x^3\right)^7 \equiv x \pmod{11}.$$
For eksempel:
$$\left(6^3\right)^7 \equiv 6 \pmod{11},$$
altså
$$6^{21} \equiv 6 \pmod{11}.$$
Én måte å vise at dette riktignok er sant er å følge beviset for 6.2.15: ut ifra Korollar **??** er
$$6^{10} \equiv 1 \pmod{11},$$
og deretter er
$$6^{21} = \left(6^{10}\right)^2 \cdot 6 \equiv 1^2 \cdot 6 = 6 \pmod{11}.$$

Eksempel 6.2.17. Vi har:

(1) $\phi(34) = \phi(17) \cdot \phi(2) = 16 \cdot 1 = 16$;

(2) $\mathsf{sfd}(5, 16) = 1$;

(3) $5 \cdot 13 = 65 \equiv 1 \pmod{16}$.

Da fastslår Korollar 6.2.15 at, for et hvilket som helst heltall x slik at $\mathsf{sfd}(x, 34) = 1$, er

$$\left(x^5\right)^{13} \equiv x \pmod{34}.$$

For eksempel:

$$\left(9^5\right)^{13} \equiv 9 \pmod{34},$$

altså

$$9^{65} \equiv 9 \pmod{34}.$$

Én måte å vise at dette riktignok er sant er å følge beviset for 6.2.15: ut ifra Proposisjon 6.2.10 er

$$9^{16} \equiv 1 \pmod{34},$$

og deretter er

$$9^{65} = \left(9^{16}\right)^4 \cdot 9 \equiv 1^4 \cdot 9 = 9 \pmod{34}.$$

6.3 Et eksempel på et bevis hvor Eulers teorem benyttes

Merknad 6.3.1. Proposisjon 6.2.10 kan benyttes på en lignende måte som Korollar 4.10.8 ble benyttet i bevisene for Proposisjon 4.11.1 og Proposisjon 4.11.10. La oss se på et eksempel.

Proposisjon 6.3.2. Det naturlige tallet $3^{37639} - 2187$ er delelig med 87808.

Bevis. Vi gjør følgende observasjoner.

(1) En primtallsfaktorisering til 87808 er

$$2^8 \cdot 7^3.$$

(2) Det følger fra (1) og Proposisjon 6.2.2 at $\phi(87808) = \phi\left(2^8\right) \cdot \phi\left(7^3\right)$.

(3) Ut ifra Proposisjon 6.1.18 er

$$\phi\left(2^8\right) = 2^8 - 2^7 = 128.$$

(4) Ut ifra Proposisjon 6.1.18 er

$$\phi\left(7^3\right) = 7^3 - 7^2 = 294.$$

(5) Det følger fra (2) – (4) at

$$\phi(87808) = 128 \cdot 294 = 37632.$$

(6) Ut ifra Proposisjon 6.2.10 er

$$3^{\phi(87808)} \equiv 1 \pmod{87808}.$$

(7) Det følger fra (5) og (6) at

$$3^{37632} \equiv 1 \pmod{87808}.$$

(8) Det følger fra (7) at

$$3^{37639} - 2187 = 3^{37632} \cdot 3^7 - 2187 \equiv 1 \cdot 3^7 - 2187 = 3^7 - 2187 = 0 \pmod{87808},$$

altså

$$3^{37639} - 2187 \equiv 0 \pmod{87808}.$$

Da har vi:

$$87808 \mid 3^{37639} - 2187.$$

□

6.4 RSA-algoritmen

Merknad 6.4.1. Én av de meste berømte anveldesene av tallteori er i kryptografi. Alle former for sikre elektroniske overføringer er avhengige av tallteoriske algoritmer som ligner på algoritmen vi kommer til å se på i dette kapittelet: RSA-algoritmen. Noen av algoritmene som brukes i dag benytter mer avansert tallteori: teorien for elliptiske kurver for eksempel, og andre deler av *aritmetiske geometri*, en del av dagens forskning i tallteori. Likevel er de fleste algoritmene overraskende enkle. RSA-algoritmen brukes fortsatt veldig mye.

Merknad 6.4.2. Kryptografi handler om hvordan meldinger kan krypteres. For å benytte tallteori for å gjøre dette, må vi oversette meldinger til og fra heltall. En mulighten vises i Tabell 6.1.

Symbolet i den første raden er et mellomrom. Et hvilket som helst heltall kan velges for å oversette et gitt symbol. Det eneste som er viktig er at ulike symboler tilsvarer til ulike heltall. Ved behøv kan flere symboler tas med.

Terminologi 6.4.3. La p og q være primtall slik at $p \neq q$. La n være et heltall slik at

$$1 < n < (p-1)(q-1)$$

og

$$\mathsf{sfd}(n, (p-1)(q-1)) = 1.$$

I forbinelse med RSA-algoritmen, sier vi at paret (pq, n) er en *offentlig nøkkel*. Vi sier at paret (p, q) er en *privat nøkkel*.

Symbol	Tilsvarende heltall
	0
A	1
B	2
C	3
D	4
E	5
F	6
G	7
H	8
I	9
J	10
K	11
L	12
M	13
N	14
O	15
P	16
Q	17
R	18
S	19
T	20
U	21
V	22
W	23
X	24
Y	25
Z	26
Æ	27
Ø	28
Å	29
0	30
1	31
2	32
3	33
4	34
5	35
6	36
7	37
8	38
9	39
.	40
,	41
!	42
:	43
−	44
?	45

Tabell 6.1: Hvordan oversette meldinger fra symboler til heltall

Merknad 6.4.4. Det er avgjørende at det er produktet pq og ikke primtallene p og q hvert for seg som er en del av den offentlige nøkkelen. Grunnen for at RSA-algoritmen er sikker er at vi ikke kjenner til en effektiv algoritme for å finne primtallsfaktoriseringen til et naturlig tall, altså for å finne p og q gitt pq.

Merknad 6.4.5. I forbinelse med RSA-algoritmen, velger alle personene som ønsker å få meldinger kryptert av denne algoritmen en offentlig nøkkel. Den øffentlig nøkkelen til en person kan sjekkes opp, som med en telefonkatalog.

Sikkerheten av en melding som har blitt kryptert ved å benytte RSA-algoritmen er imidlertid avhengig av at den private nøkkelen til en person ikke kan sjekkes opp. Det er kun personen selv, og eventuelt andre personer han eller hun stoler på, som bør vite hans eller huns private nøkkel.

Notasjon 6.4.6. La p og q være primtall slik at $p \neq q$. La n være et heltall slik at

$$1 < n < (p-1)(q-1)$$

og

$$\mathsf{sfd}(n, (p-1)(q-1)) = 1.$$

Ut ifra Korollar 3.4.39, finnes det da et heltall m slik at

$$nm \equiv 1 \pmod{(p-1)(q-1)}.$$

Ut ifra Proposisjon 3.2.1, finnes det et naturlig tall m' slik at

$$m \equiv m' \pmod{(p-1)(q-1)}$$

og $m' \leq (p-1)(q-1)$. Til tross for at $(p-1)(q-1)$ ikke er et primtall, betegner vi m' som n^{-1} i denne delen av kapittelet.

Definisjon 6.4.7. Anta at person A ønsker å sende en meldig til person B. Anta at person B har valgt en offentlig nøkkel, og at person A vet denne nøkkelen. Å kryptere denne meldingen ved å benytte *RSA-algoritmen*, er å gjøre følgende.

(1) Oversett hvert symbol i meldingen til et heltall, ved å benytte for eksempel tabellen i Merknad 6.4.2.

(2) La g_1, g_2, …, g_t være disse heltallene. For hvert naturlig tall i slik at $i \leq t$, finn heltallet r_i slik at

$$g_i^n \equiv r_i \pmod{pq}$$

og $0 \leq r_i < pq$.

Å dekryptere en melding $(r_1, \ldots, r_t)$ som har blitt kryptert ved å benytte RSA-algoritmen, er å gjøre følgende.

(1) Ut ifra Proposisjon 3.2.1, finnes det, for hvert naturlig tall i slik at $i \leq t$, et heltall s_i slik at

$$r_i^{n^{-1}} \equiv s_i \pmod{pq}.$$

Finn disse heltallene s_1, …, s_t.

(2) Oversett heltallene $s_1, \ldots, s_t$ til symboler ved å benytte for eksempel tabellen i Merknad 6.4.2.

Merknad 6.4.8. Vi har:

$$(r_i)^{n^{-1}} \equiv (g_i^n)^{n^{-1}} \pmod{pq}.$$

Ut ifra Proposisjon 6.2.2 og Proposisjon 6.1.12 er

$$\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1).$$

Ut ifra Korollar 6.2.15, er da

$$(g_i^n)^{n^{-1}} \equiv g_i \pmod{n}.$$

Dermed er

$$(r_i)^{n^{-1}} \equiv g_i \pmod{pq}.$$

Siden både $s_i < pq$ og $g_i < pq$, følger det fra Proposisjon 3.2.11 at $s_i = g_i$. Det vil si: ved å kryptere heltallet g_i til heltallet r_i, og ved å da dekryptere r_i, får vi tilbake g_i. Dermed er det Korollar 6.2.15 som fastlår at RSA-algoritmen virker: når vi dekryptere en melding som har blitt kryptert, får vi tilbake den opprinnelige meldingen. Siden det er Eulers teorem som fører til Korollar 6.2.15, er det Eulers teorem som ligger egentlig bak RSA-algoritmen.

Merknad 6.4.9. La merke til at, for å dedusere at $s_i = g_i$, er det nødvendig at $g_i < pq$ og at $s_i < pq$. Det er derfor vi sørge for dette i Steg (2) når vi kryptere, og i Steg (1) når vi dekryptere.

Det er ikke faktisk nødvendig at $0 \leq r_i < pq$. Algoritmen virker ved å sende et hvilket som helst heltall som er kongruent til g_i^n til person B. For å sørge for at meldingen er sikker, bør vi imidlertid ikke sende g_i^n selv til Person B: da kan koden knekkes ved å ta den vanlige n-te roten til hvert heltall i den krypterte meldingen. Så lenge vi velge r_i til å være noe annet, for eksempel til å være et heltall som er mindre enn pq, unngår vi dette problemet, fordi det ikke finnes en effektiv algoritme for å finne «n-te røtter» i modulær aritmetikk.

Merknad 6.4.10. Det er ikke noe spesielt med å bruke to primtall p og q i RSA-algoritmen. Et hvilket som helst naturlig tall kan benyttes istedenfor. Da erstatter vi $(p-1)(q-1)$ med $\phi(n)$.

Derimot gjør dette ikke mye fra synspunktet av kryptografi. Hvis det hadde vært en effektiv algoritme for å faktorisere pq, hadde det nesten sikkert vært en effektiv algoritme for å finne en primtallsfaktorisering til et hvilket som helst naturlig tall.

Når RSA-algoritmen implementeres i praksis, kan det dessuten være nyttig å benytte et produkt av to primtall istedenfor et hvilket som helst naturlig tall.

Eksempel 6.4.11. Anta at person A ønsker å sende meldingen «Elsker deg!» til person B, og å kryptere meldingen ved å benytte RSA-algoritmen. La oss anta at person B har $(17, 3)$ som privat nøkkel, og $(51, 7)$ som offentlig nøkkel. Vi har:

$$(17-1)\cdot(3-1) = 16\cdot 2 = 32,$$

Siden $7 < 16$ og $\mathsf{sfd}(7, 32) = 1$, er denne nøkkelen gyldig.

Siden

$$7\cdot -9 = -63 \equiv 1 \pmod{32},$$

og siden $-9 \equiv 23 \pmod{32}$, er $7^{-1} = 23$.

Først oversetter person A meldingen «Elsker deg!» til heltall, ved å benytte Tabell 6.1. Tabell 6.2 viser oversettelsen. Dermed blir meldingen: 5 12 19 11 5 18 0 4 5 7 42.

Symbol	Tilsvarende heltall
E	5
L	12
S	19
K	11
E	5
R	18
	0
D	4
E	5
G	7
!	42

Tabell 6.2: Oversettelsen av meldingen

Da finner person A et heltall r_i slik at

$$g_i^7 \equiv r_i \pmod{51}$$

for hvert par sifre g_i i den oversatte meldingen. Tabell 6.3 viser resultatene. Utregningene gjennomføres på den vanlige måten. For eksempel:

$$\begin{aligned} 6^7 &= \left(6^3\right)^2 \cdot 6 \\ &= 216^2 \cdot 6 \\ &\equiv 12^2 \cdot 6 \\ &= 144 \cdot 6 \\ &\equiv (-9)\cdot 6 \\ &= -54 \\ &\equiv 48 \pmod{51} \end{aligned}$$

g_i	r_i
6	44
12	24
19	43
11	20
5	44
18	18
0	0
4	13
5	44
7	46
42	15

Tabell 6.3: Hvordan kryptere meldingen

og

$$\begin{aligned} 42^7 &\equiv (-9)^7 \\ &= \left((-9)^3\right)^2 \cdot (-9) \\ &= (-729)^2 \cdot (-9) \\ &\equiv (-15)^2 \cdot (-9) \\ &= 225 \cdot (-9) \\ &\equiv 21 \cdot (-9) \\ &= -189 \\ &\equiv 15 \pmod{51}. \end{aligned}$$

Dermed blir den krypterte meldingen: 48 24 43 20 44 18 00 13 44 46 15.

Når person B mottar denne krypterte meldingen, dekrypterer han eller hun den. For å gjøre dette, finner han eller hun, for hvert par sifre r_i i den krypterte meldingen, et heltall s_i slik at

$$r_i^{23} \equiv s_i \pmod{51}.$$

Ut ifra Merknad 6.4.8, kommer han eller hun til å få g_i. Det vil si: han eller hun kommer til å få tilbake meldingen: 6 12 19 11 5 18 0 4 5 7 42.

Da oversetter han eller hun heltallene til symboler ved å benytte Tabell 6.1. Han eller hun får meldingen: «Elsker deg!».

Eksempel 6.4.12. Anta at person B har fått meldingen

45 9 44 44 41 0 48 4 45 70

fra person A. Anta at den offentlige nøkkelen til person B er $(77, 17)$, og at den private nøkkelen til person B er $(11, 7)$. Vi har: $(11-1)\cdot(7-1) = 10 \cdot 6 = 60$. Siden $17 < 60$ og $\mathsf{sfd}(17, 60) = 1$, er denne nøkkelen gyldig.

Ved for eksempel å benytte Euklids algoritmen, får vi at

$$17 \cdot (-7) \equiv 1 \pmod{60}.$$

Siden

$$-7 \equiv 53 \pmod{60},$$

er $17^{-1} = 53$.

For å dekryptere meldingen, finner person B, for hvert par sifre r_i i den krypterte meldingen, et heltall s_i slik at

$$r_i^{53} \equiv s_i \pmod{77}.$$

Tabell 6.4 viser resultatene. Dermed blir meldingen: 12 25 11 11 6 18 0 20 9 12 42.

r_i	s_i
45	12
9	25
44	11
44	11
41	6
0	0
48	20
4	9
45	12
70	42

Tabell 6.4: Hvordan dekryptere meldingen

Nå oversetter person B denne meldingen til symboler, ved å benytte Tabell 6.1. Tabell 6.5 viser oversettelsen. Person B får altså meldingen: «Lykke til!».

Merknad 6.4.13. La (m, n) være en offentlig nøkkel. Dersom vi kan finne de to primtallene p og q slik at $m = pq$, kan vi regne ut n^{-1}. Da kan vi knekke koden til meldinger som blir kryptert ved å benytte denne offentlige nøkkelen.

Som nevnt i Merknad 6.4.4, finnes det imidlertid ikke en effektiv algoritme for å finne p og q. Så lenge vi velger p og q til å være store nok, kommer til og med den kraftigste datamaskinen som finnes i dag ikke til å ha en sjanse til å finne p og q, med mindre den blir utrolig heldig!

I dag er p og q mer enn store nok om de har rundt 250 sifre.

Eksempel 6.4.14. Anta at person B har fått meldingen

$$2 \ 20 \ 9 \ 0 \ 25 \ 21 \ 13 \ 35$$

fra person A. Anta at den offentlige nøkkelen til person B er $(55, 13)$.

Heltall	Tilsvarende symbol
12	L
25	Y
11	K
11	K
6	E
0	
20	T
9	I
12	L
42	!

Tabell 6.5: Oversettelsen av meldingen

Anta at person C ønsker å knekke koden til meldingen. Da må han eller hun finne primtall p og q slik at $55 = pq$. Han eller hun kommer fram til: $p = 5$ og $q = 11$. Nå regner han eller hun ut 13^{-1}. Vi har:

$$(5-1)\cdot(11-1) = 4\cdot 10 = 40.$$

Siden

$$13\cdot 3 = 39 \equiv -1 \pmod{40},$$

er $x = -3$ en løsning til kongruensen

$$13x \equiv 1 \pmod{40}.$$

Siden

$$-3 \equiv 37 \pmod{40},$$

er da $n^{-1} = 37$. Alternativt kan Euklids algoritme benyttes for å komme fram til dette.

For å dekryptere meldingen, finner person C, for hvert par sifre r_i i den krypterte meldingen, et heltall s_i slik at

$$r_i^{37} \equiv s_i \pmod{55}.$$

Tabell 6.6 viser resultatene. Dermed blir meldingen: 07 15 4 0 20 21 18 40.

Nå oversetter person C denne meldingen til symboler, ved å benytte Tabell 6.1. Tabell 6.7 viser oversettelsen. Person C finner altså at meldingen er: «God tur.».

Merknad 6.4.15. Når RSA-algoritmen benyttes i praksis, må oversettelsen fra symboler til heltall gjøres på en mer sikker måte enn å benytte en tabell som Tabell 6.1. Ett problem er at hadde det vært mulig å for eksempel gjette at en kryptert gruppe sifre som dukker opp ofte er et mellomrom, eller en vokal. Hvis man ser på nok meldinger, hadde det vært mulig å på denne måten gjette hvilke grupper krypterte heltall tilsvarer til hvilke symboler, og dermed dekryptere meldinger til person B.

r_i	s_i
2	7
20	15
9	4
0	0
25	20
21	21
13	18
35	40

Tabell 6.6: Hvordan dekryptere meldingen

Heltall	Tilsvarende symbol
7	G
15	O
04	D
0	
20	T
21	U
18	R
40	.

Tabell 6.7: Oversettelsen av meldingen

Et beslektet problem er at en person som ønsker å knekke koden til meldinger til person B kan for eksempel sende, for hvert symbol, en melding til person B som består av oversettelsen av dette enkelte symbolet: en melding som består kun av oversettelsen av «a», og så en melding som består kun av oversettelsen av «b», osv. Da får han eller hun de gruppene krypterte heltall som tilsvarer til hvert symbol, og dermed kan han eller hun dekryptere en hvilken som helst melding til person B.

Disse to måter å dekryptere meldinger må alltid tas i betraktning i kryptografi. Det finnes måter å oversette meldinger fra symboler til heltall som er like sikre som RSA-algoritmen selv.

O6 Oppgaver – Kryptografi

O6.1 Oppgaver i eksamens stil

Oppgave O6.1.1. Hvor mange naturlige tall x slik at $x \leq 2925$ og $\mathsf{sfd}(x, 2925) = 1$ finnes det?

Oppgave O6.1.2. Vis uten å regne ut at $4721 \cdot \left(11^{2163}\right) + 5324$ er delelig med 4725.

Oppgave O6.1.3. Person A ønsker å sende meldigen ≪Vi sees i morgen!≫ til person B ved å benytte RSA-algoritmen. Den offentlige nøkkelen til person B er $(85, 19)$. Krypter meldingen. Det er ikke nødvendig å begrunne utregningene dine: bruk gjerne kalkulatoren!

Oppgave O6.1.4. Person A har sendt meldigen

$$49\ \ 41\ \ 18\ \ 00\ \ 55\ \ 47\ \ 20\ \ 32\ \ 18\ \ 01\ \ 30$$

til person B ved å benytte RSA-algoritmen. Den offentlige nøkkelen til person B er $(57, 23)$. Den private nøkkelen til person B er $(19, 3)$. Dekrypter meldingen. Det er ikke nødvendig å begrunne utregningene dine: bruk gjerne kalkulatoren!

Oppgave O6.1.5. Person A har sendt meldigen

$$31\ \ 51\ \ 71\ \ 39\ \ 00\ \ 34\ \ 03\ \ 00\ \ 34\ \ 71\ \ 65\ \ 54$$

til person B ved å benytte RSA-algoritmen. Den offentlige nøkkelen til person B er $(87, 25)$. Knekk koden. Det er ikke nødvendig å begrunne utregningene dine: bruk gjerne kalkulatoren!