Innhold

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).