Forelesning 22 — mandag den 3. november

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

$$n_2 x_1 c_1 + n_1 x_2 c_2 \equiv c_1 \pmod{n_1},$$

altså at

$$x = n_2 x_1 c_1 + n_1 x_2 c_2$$

er en løsning til kongruensen

$$x \equiv c_1 \pmod{n_1}.$$

Nå gjør vi følgende observasjoner.

(1) Siden $n_2 \mid n_2 x_1 c_1$, er

$$n_2 x_1 c_1 \equiv 0 \pmod{n_2}.$$

Det følger at

$$n_2 x_1 c_1 + n_1 x_2 c_2 \equiv n_1 x_2 c_2 \pmod{n_2}.$$

(2) Siden

$$n_1 x_2 \equiv 1 \pmod{n_2},$$

er

$$n_1 x_2 c_2 \equiv c_2 \pmod{n_2}.$$

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

$$y \equiv z \pmod{n_1n_2}$$

Dermed er (II) sant.

Anta istedenfor nå at y og z er heltall slik at

$$y \equiv z \pmod{n_1n_2},$$

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 $127+3\cdot221$, 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 $127-8\cdot221$, 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, $2p$, $3p$, …, $\left(\frac{q-1}{2}\right)p$.

(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, $2q$, $3q$, …, $\left(\frac{p-1}{2}\right)q$.

(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

$$u \equiv v \pmod{21}.$$

Dette 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

$$1 \times 2 \times \cdots \times \left(\frac{q-1}{2}\right) \times \left(\frac{q-1}{2}+1\right) \times \left(\frac{q-1}{2}+2\right) \times \cdots \times \left(\frac{q-1}{2}+\frac{q-1}{2}\right)$$
$$\equiv (-1)^{\frac{q-1}{2}} \times \left(\frac{q-1}{2}\right)! \times \left(\frac{q-1}{2}\right)! \pmod{q}.$$

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 5.3.5 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 5.3.6 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 5.3.7 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 5.3.7 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 5.3.6 er $\mathbb{L}_5^3 = -1$. Ut ifra Proposisjon 5.5.3 og Eksempel 5.3.5 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 5.3.7 er $\mathbb{L}_7^3 = -1$. Ut ifra Proposisjon 5.5.3 og Eksempel 5.3.5 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 5.3.7 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 5.3.7 er $\mathbb{L}_5^2 = -1$, altså er det riktignok sant at $\mathbb{L}_5^7 = -1$.

Eksempel 5.9.4. Ut ifra Eksempel 5.3.8 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 5.3.7 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 5.3.7 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 5.3.5 er $\mathbb{L}_3^2 = -1$, altså er det riktignok sant at $\mathbb{L}_3^{-7} = -1$.

Eksempel 5.9.8. Ut ifra Eksempel 5.3.8 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 5.3.6 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 5.3.6, og Eksempel 5.3.7 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 5.3.5, Eksempel 5.3.5, og Eksempel 5.3.5 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 $q_1, q_2, \ldots, q_t$ 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 5.3.6 er dette rikignok sant.

Eksempel 5.9.23. Korollar 5.9.21 fastslår at $\mathbb{L}_7^2 = 1$. Ut ifra Eksempel 5.3.7 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 5.3.8 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.

Oppgaver

O5.1 Oppgaver i eksamens stil

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.