Forelesning 20 — mandag den 27. oktober

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 $\mathbb{L}^3_{3491} = -\mathbb{L}^{3491}_3$. Siden

$$3491 \equiv 2 \pmod 3,$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}^{3491}_3 = \mathbb{L}^2_3.$$

Siden

$$3 \equiv 3 \pmod 8,$$

følger det fra Korollar 5.9.21 at $\mathbb{L}^2_3 = -1$. Dermed er

$$\mathbb{L}^3_{3491} = -\mathbb{L}^{3491}_3 = -\mathbb{L}^2_3 = -(-1) = 1.$$

(4) Vi har:

$$3491 \equiv 3 \pmod 4$$

og

$$7 \equiv 3 \pmod 4.$$

Da følger det fra Korollar 5.9.2 at $\mathbb{L}^7_{3491} = -\mathbb{L}^{3491}_7$. Siden

$$3491 \equiv 5 \pmod 7,$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}^{3491}_7 = \mathbb{L}^5_7.$$

Siden

$$5 \equiv 1 \pmod 4,$$

følger det fra Korollar 5.9.2 at $\mathbb{L}^5_7 = \mathbb{L}^7_5$. Siden

$$7 \equiv 2 \pmod 5,$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}^7_5 = \mathbb{L}^2_5.$$

Siden

$$5 \equiv 5 \pmod 8,$$

følger det fra Korollar 5.9.21 at $\mathbb{L}^2_5 = -1$. Dermed er

$$\mathbb{L}^7_{3491} = -\mathbb{L}^{3491}_7 = -\mathbb{L}^5_7 = -\mathbb{L}^7_5 = -\mathbb{L}^2_5 = -(-1) = 1.$$

(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 $\mathbb{L}_{p_i}^2 = 1$, 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 **??**, 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.

Oppgaver

O5.1 Oppgaver i eksamens stil

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 O5.1.12 (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).