Forelesning 19 —torsdag den 23. oktober

5.3 Eulers kriterium

Merknad 5.3.1. Følgende proposisjon er kjernen til teorien for kvadratiske rester. Kanskje ser beviset ikke så vanskelig ut, men la merke til at det bygger på Proposisjon **??**, det vil si at det finnes en primitiv rot modulo et hvilket som helst primtall. Vi måtte jobbe ganske harde å bevise at dette er sant. Beviset bygger også på Fermats lille teorem.

Proposisjon 5.3.2. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at $p \mid a$. Da er a en kvadratisk rest modulo p hvis og bare hvis

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Bevis. Anta først at a er en kvadratisk rest modulo p. Da er det et heltall x slik at

$$x^2 \equiv a \pmod{p}.$$

Da er

$$a^{\frac{p-1}{2}} \equiv \left(x^2\right)^{\frac{p-1}{2}} = x^{2\left(\frac{p-1}{2}\right)} = x^{p-1} \pmod{p}.$$

Ut ifra Korollar 4.10.8 er

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

Dermed er

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Anta istedenfor at

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Ut ifra Proposisjon **??** finnes det en primitiv rot modulo p. La oss betegne denne primitive roten som x. Ut ifra Proposisjon 4.13.6 finnes det et heltall t slik at $1 \leq t \leq p-1$ og

$$x^t \equiv a \pmod{p}.$$

Da er

$$\left(x^t\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p},$$

altså

$$x^{t\left(\frac{p-1}{2}\right)} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Siden

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

følger det at

$$x^{t\left(\frac{p-1}{2}\right)} \equiv 1 \pmod{p}.$$

Ut ifra Proposisjon 4.12.10 har vi da: $\mathsf{ord}_p(x) \mid t\left(\frac{p-1}{2}\right)$. Siden x er en primitiv rot modulo p, er $\mathsf{ord}_p(x) = p-1$. Da har vi: $p-1 \mid t\left(\frac{p-1}{2}\right)$. Dermed finnes det et heltall k slik at

$$t\left(\frac{p-1}{2}\right) = k \cdot (p-1).$$

Da er

$$t(p-1) = 2k \cdot (p-1).$$

Det følger fra Proposisjon 2.2.25 at $t = 2k$.

Vi har:

$$\left(x^k\right)^2 = x^{2k} = x^t \equiv a \pmod{p},$$

altså

$$\left(x^k\right)^2 \equiv a \pmod{p}.$$

Med andre ord er $y = x^k$ en løsning til kongruensen

$$y^2 \equiv a \pmod{p}.$$

Dermed er a en kvadratisk rot modulo p.

□

Terminologi 5.3.3. Proposisjon 5.3.2 kalles *Eulers kriterium*.

Eksempel 5.3.4. Ut ifra Eksempel 5.2.15 er 5 en kvadratisk rest modulo 11. Proposisjon 5.3.2 fastslår at

$$5^{\frac{11-1}{2}} \equiv 1 \pmod{11},$$

altså at

$$5^5 \equiv 1 \pmod{11}.$$

Vi har:

$$5^5 = \left(5^2\right)^2 \cdot 5 = 25^2 \cdot 5 \equiv 3^2 \cdot 5 = 9 \cdot 5 = 45 \equiv 1 \pmod{11}.$$

Dermed er det riktignok sant at

$$5^5 \equiv 1 \pmod{11}.$$

Eksempel 5.3.5. Ut ifra Eksempel 5.2.13 er 3 ikke en kvadratisk rest modulo 5. Proposisjon 5.3.2 fastslår at det ikke er sant at

$$3^{\frac{5-1}{2}} \equiv 1 \pmod{5},$$

altså at det ikke er sant at

$$3^2 \equiv 1 \pmod{5}.$$

Vi har: $3^2 = 9$ og

$$9 \equiv 4 \pmod{5}.$$

Siden det ikke er sant at

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

er det riktignok ikke sant at

$$3^2 \equiv 1 \pmod{5}.$$

Eksempel 5.3.6. Proposisjon 5.3.2 fastslår at 3 er en kvadratisk rest modulo 31 hvis og bare hvis

$$3^{\frac{31-1}{2}} \equiv 1 \pmod{31},$$

altså hvis og bare hvis

$$3^{15} \equiv 1 \pmod{31}.$$

Vi har:

$$3^3 = 27 \equiv -4 \pmod{31}.$$

Da er

$$\begin{aligned} 3^{15} &= 3^9 \cdot 3^6 \\ &= \left(3^3\right)^3 \cdot \left(3^3\right)^2 \\ &\equiv (-4)^3 \cdot (-4)^2 \\ &= (-64) \cdot 16 \\ &\equiv (-2) \cdot 16 \\ &= -32 \\ &\equiv -1 \pmod{31}, \end{aligned}$$

altså

$$3^{15} \equiv -1 \pmod{31}.$$

Vi konkluderer at 3 ikke er en kvadratisk rest modulo 31.

Eksempel 5.3.7. Proposisjon 5.3.2 fastslår at -5 er en kvadratisk rest modulo 127 hvis og bare hvis

$$(-5)^{\frac{127-1}{2}} \equiv 1 \pmod{127},$$

altså hvis og bare hvis

$$(-5)^{63} \equiv 1 \pmod{127}.$$

Vi har:

$$\begin{aligned}(-5)^{63} &= -\left(5^3\right)^{21} \\ &= -(125)^{21} \\ &\equiv -(-2)^{21} \\ &= -\left((-2)^7\right)^3 \\ &= -(-128)^3 \\ &\equiv -(-1)^3 = -(-1) \\ &= 1 \pmod{127},\end{aligned}$$

altså

$$(-5)^{63} \equiv 1 \pmod{127}.$$

Vi konkluderer at 5 er en kvadratisk rest modulo 127.

Merknad 5.3.8. De siste to eksemplene viser at Proposisjon 5.3.2 er en kraftig verktøy for å bestemme om et heltall er eller ikke er en kvadratisk rest modulo et primtall. Argumentet i Eksempel 5.3.6 er å foretrekke fremfor å vise at det ikke er sant at

$$x^2 \equiv 3 \pmod{31}$$

for hvert av de naturlige tallene 1, 2, ..., 30. Argumentet i Eksempel 5.3.7 er å foretrekke fremfor å gå gjennom alle de naturlige tallene 1, 2, ..., 126 til vi finner ett som er kongruent til 5 når vi opphøyer det i andre potens.

Derimot måtte vi være litt kreative for å regne ut 3^{15} modulo 31 og $(-5)^{63}$ modulo 127 i disse to eksemplene. Det er ikke alltid lett å fullføre slike utregninger.

Imidlertid kan vi gå videre. Vi kommer til å se at vi kan bygge på Proposisjon 5.3.2 for å komme fram til en metode for å bestemme om et heltall er eller ikke er en kvadratisk rest modulo et primtall, uten å regne ut i det hele tatt.

Først kommer vi til å gi et annet eksempel, litt mer teoretisk, på hvordan Proposisjon 5.3.2 kan benyttes i praksis. Vi må gjøre noen forberedelser.

Merknad 5.3.9. Følgende proposisjon er veldig enkel. Likevel er den svært nyttig: vi kommer til å benytte den ofte i dette kapittelet.

Proposisjon 5.3.10. La n være et naturlig tall slik at $n > 2$. La a være 1 eller -1. La b være 1 eller -1. Da er

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

hvis og bare hvis $a = b$.

Bevis. Ett av følgende utsagn er sant:

(A) $a = 1$ og $b = 1$;

(B) $a = 1$ og $b = -1$;

(C) $a = -1$ og $b = 1$;

(D) $a = -1$ og $b = -1$.

Anta først at (B) er sant. Hvis

$$1 \equiv -1 \pmod{n},$$

er

$$2 \equiv 0 \pmod{n}.$$

Da har vi: $n \mid 2$. Ut ifra Proposisjon 2.5.30 er da $n \leq 2$. Imidlertid har vi antatt at $n > 2$. Siden antakelsen at (B) er sant fører til denne motsigelsen, konkluderer vi at (B) ikke er sant.

Anta nå at (C) er sant. Hvis

$$-1 \equiv 1 \pmod{n},$$

er

$$-2 \equiv 0 \pmod{n}.$$

Da har vi: $n \mid -2$. Det følger fra Proposisjon 2.5.12 at vi da har: $n \mid 2$. Ut ifra Proposisjon 2.5.30 er da $n \leq 2$. Imidlertid har vi antatt at $n > 2$. Siden antakelsen at (C) er sant fører til denne motsigelsen, konkluderer vi at (C) ikke er sant.

Således har vi bevist at

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

hvis og bare hvis enten (A) eller (B) sant, altså hvis og bare hvis $a = b$.

□

Lemma 5.3.11. La p være et primtall slik at $p > 2$. Da er følgende sanne:

(1) $x = 1$ og $x = -1$ er løsninger til kongruensen

$$x^2 \equiv 1 \pmod{p};$$

(2) det ikke er sant at

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

(3) enhver annen løsning til kongruensen

$$x^2 \equiv 1 \pmod{p}$$

er kongruent modulo p til enten 1 eller -1;

Bevis. Siden $1^2 = 1$ og $(-1)^2 = 1$, er (1) sant. Ut ifra Proposisjon 5.3.10 er (2) sant. Siden (1) og (2) er sanne, følger det fra Proposisjon 4.14.11 (II) at (3) er sant. □

Korollar 5.3.12. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at $p \mid a$. Da er a ikke er en kvadratisk rest modulo p hvis og bare hvis

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Vi har:

$$\left(a^{\frac{p-1}{2}}\right)^2 = a^{2\cdot\left(\frac{p-1}{2}\right)} = a^{p-1}.$$

Ut ifra Korollar 4.10.8, er

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

Dermed er

$$\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}.$$

Da følger fra Lemma 5.3.11 at enten

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

eller

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

(2) Ut ifra Proposisjon 5.3.2 er a ikke en kvadratisk rest modulo p hvis og bare hvis det ikke er sant at

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Det følger fra (1) og (2) at a ikke er en kvadratisk rest modulo p hvis og bare hvis

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

□

Eksempel 5.3.13. Ut ifra Eksempel 5.2.15 er 6 ikke en kvadratisk rest modulo 11. Da fastslår Korollar 5.3.12 at

$$6^{\frac{11-1}{2}} \equiv -1 \pmod{11},$$

altså

$$6^5 \equiv -1 \pmod{11}.$$

Dette er riktignok sant:

$$6^5 = \left(6^2\right)^2 \cdot 6 = 36^2 \cdot 6 \equiv 3^2 \cdot 6 = 54 \equiv -1 \pmod{11}.$$

Eksempel 5.3.14. Korollar 5.3.12 fastslår at 10 ikke er en kvadratisk rest modulo 23 hvis og bare hvis

$$10^{\frac{23-1}{2}} \equiv -1 \pmod{23},$$

altså hvis og bare hvis

$$10^{11} \equiv -1 \pmod{23}.$$

Vi har:

$$10^4 = \left(10^2\right)^2 = 100^2 \equiv 8^2 = 64 \equiv -5 \pmod{23}.$$

I tillegg har vi:

$$10^3 = 10^2 \cdot 10 \equiv 8 \cdot 10 = 80 \equiv 11 \pmod{23}.$$

Dermed er

$$10^{11} = \left(10^4\right)^2 \cdot 10^3 \equiv (-5)^2 \cdot 11 = 25 \cdot 11 \equiv 2 \cdot 11 = 22 \equiv -1 \pmod{23}.$$

Vi konkluderer at 10 ikke er en kvadratisk rest modulo 23.

Proposisjon 5.3.15. La p være et primtall slik at $p > 2$. Da er -1 en kvadratisk rest modulo p hvis og bare hvis

$$p \equiv 1 \pmod{4}.$$

Bevis. Ut ifra Proposisjon 3.2.1 er ett av følgende utsagn sant.

(A) $p \equiv 0 \pmod{4}$;

(B) $p \equiv 1 \pmod{4}$;

(C) $p \equiv 2 \pmod{4}$;

(D) $p \equiv 3 \pmod{4}$.

Anta først at (A) er sant. Da har vi: $4 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Dermed er $p = 4$. Imidlertid er 4 ikke et primtall. Siden antakelsen at (A) er sant fører til denne motsigelsen, konkluderer vi at (A) ikke er sant.

Anta nå at (C) er sant. Siden $2 \mid 2$ og $2 \mid 4$, følger det da fra Proposisjon 3.2.54 at

$$p \equiv 0 \pmod{2}.$$

Derfor har vi: $2 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Dermed er $p = 2$. Imidlertid har vi antatt at $p > 2$. Siden antakelsen at (C) er sant fører til denne motsigelsen, konkluderer vi at (C) ikke er sant.

Anta nå at (D) er sant. Hvis

$$p \equiv 3 \pmod{4},$$

har vi: $4 \mid p-3$. Dermed finnes det et heltall k slik at $p-3=4k$, altså slik at $\frac{p-3}{2}=2k$. Da er

$$\begin{aligned}(-1)^{\frac{p-1}{2}} &= (-1)^{\frac{p-3}{2}+1} \\ &= (-1)^{\frac{p-3}{2}} \cdot (-1)^1 \\ &= (-1)^{2k} \cdot (-1) \\ &= \left((-1)^2\right)^k \cdot (-1) \\ &= 1^k \cdot (-1) \\ &= 1 \cdot (-1) \\ &= -1.\end{aligned}$$

Siden $p > 2$ og $-1 \neq 1$, følger det fra Proposisjon 5.3.10 at det ikke er sant at

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

Dermed er det ikke sant at

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Det følger fra Proposisjon 5.3.2 at -1 ikke er en kvadratisk rest modulo p.

Anta nå at (B) er sant. Hvis

$$p \equiv 1 \pmod{4},$$

har vi: $4 \mid p-1$. Dermed finnes det et heltall k slik at $p-1=4k$, altså slik at $\frac{p-1}{2}=2k$. Da er

$$\begin{aligned}(-1)^{\frac{p-1}{2}} &= (-1)^{2k} \\ &= \left((-1)^2\right)^k \\ &= 1^k \\ &= 1.\end{aligned}$$

Det følger fra Proposisjon 5.3.2 at 1 er en kvadratisk rest modulo p.

□

Eksempel 5.3.16. Vi har:

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

Dermed er det ikke sant at

$$7 \equiv 1 \pmod{4}.$$

Da fastslår Proposisjon 5.3.15 at -1 ikke er en kvadratisk rest modulo 7. Dette er riktignok sant: hvis -1 hadde vært en kvadratisk rest, hadde så, ut ifra Proposisjon 5.2.5, 6 vært en kvadratisk rest, og fra Eksempel 5.2.14 vet vi at dette ikke er tilfellet.

Eksempel 5.3.17. Vi har:

$$13 \equiv 1 \pmod 4.$$

Da fastslår Proposisjon 5.3.15 at -1 er en kvadratisk rest modulo 13. Dette er riktignok sant:

$$5^2 = 25 \equiv -1 \pmod{13}.$$

Proposisjon 5.3.18. La n være et naturlig tall. Da finnes det et primtall p slik at $p > n$ og

$$p \equiv 1 \pmod 4.$$

Bevis. La q være produktet av alle primtallene som er mindre enn eller like n, og som er kongruent til 1 modulo 4. Ut ifra Teorem 4.3.3, finnes det et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at

$$(2q)^2 + 1 = p_1 \cdots p_t.$$

Anta at

$$p_1 \equiv 0 \pmod 2.$$

Da er

$$p_1 \cdots p_t \equiv 0 \cdot (p_2 \cdots p_t) \pmod 2,$$

altså

$$(2q)^2 + 1 \equiv 0 \pmod 2.$$

Siden $2 \mid (2q)^2$, er imidlertid

$$(2q)^2 + 1 \equiv 1 \pmod 2.$$

Ut ifra Proposisjon 3.2.11 kan det ikke være sant at både

$$(2q)^2 + 1 \equiv 0 \pmod 2$$

og

$$(2q)^2 + 1 \equiv 1 \pmod 2.$$

Siden antakelsen at

$$p_1 \equiv 0 \pmod 2$$

fører til denne motsigelsen, konkluderer vi at det ikke er sant at

$$p_1 \equiv 0 \pmod 2.$$

Vi konkluderer at $p_1 > 2$.

Siden

$$(2q)^2 + 1 = (p_2 \cdots p_t)\, p_1,$$

har vi: $p_1 \mid (2q)^2 + 1$. Dermed er

$$(2q)^2 \equiv -1 \pmod{p_1},$$

altså -1 er en kvadratisk rest modulo p_1. Siden p_1 er et primtall og $p > 2$, følger det fra Proposisjon 5.3.15 at

$$p_1 \equiv 1 \pmod 4.$$

Anta at $p_1 \leq n$. Vi gjør følgende observasjoner.

(1) Ut ifra definisjonen til q, følger det da at $p_1 \mid q$. Fra Korollar 2.5.18 har vi da: $p_1 \mid q \cdot (-4q)$, altså $p_1 \mid -(2q)^2$.

(2) Siden vi i tillegg vet at $p_1 \mid (2q)^2 + 1$, følger det fra (1) og Proposisjon 2.5.24 at $p_1 \mid \big((2q)^2 + 1\big) + \big((-(2q)^2\big)$, altså at $p_1 \mid 1$.

Det kan ikke være sant at både $p_1 \mid 1$ og $p_1 > 2$. Siden antakelsen at $p_1 \leq n$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $p_1 \leq n$. Derfor er $p_1 > n$.

□

Merknad 5.3.19. Med andre ord fastslår Proposisjon 5.3.18 at det finnes uendelig mange primtall som er kongruent til 1 modulo 4. Sammenlign med Teorem 4.4.2, Proposisjon 4.4.9, og Oppgave **??**.

Merknad 5.3.20. Det er ikke noe spesielt med p_1 i beviset for Proposisjon 5.3.18. Det samme argumentet viser at $p_i > n$ for alle primtallene p_1, p_2, …, p_t som dukker opp i primtallsfaktorisingen til $(2q)^2 + 1$ i beviset.

Eksempel 5.3.21. La oss gå gjennom beviset for Proposisjon 5.3.18 når $n = 30$. Det finnes fire primtall som er mindre enn eller likt 30 og som er kongruent til 1 modulo 4, nemlig 5, 13, 17, og 29. La q være produktet av disse primtallene, altså

$$q = 5 \cdot 13 \cdot 17 \cdot 29.$$

Da er $(2q)^2 + 1$ likt 4107528101. Beviset for Proposisjon 5.3.18 fastslår at hvert primtall i en primtallsfaktorisering av $(2q)^2 + 1$, altså av 4107528101, er større enn 30. Vi har:

$$4107528101 = 37 \cdot 173 \cdot 641701,$$

og både 37, 173, og 641701 er primtall. Med andre ord, er primtallet p_1 i beviset for Proposisjon 5.3.18 likt 37 i dette tilfellet: det er riktignok sant at $37 > 30$.

Merknad 5.3.22. Kanskje ser beviset for Proposisjon 5.3.18 lettere ut enn beviset for Proposisjon 4.4.9. Imidlertid er dette villedende: beviset for Proposisjon 5.3.18 bygger på Proposisjon 5.3.2, som er et ganske dypt resultat.

5.5 Grunnleggende proposisjoner om Legendresymbolet

Merknad 5.5.1. I denne delen av kapittelet kommer til å bevise en rekke proposisjoner som gir oss muligheten til å regne ut Legendresymboler, og dermed å sjekke om kvadratiske kongruenser har eller ikke har løsninger.

Proposisjon 5.5.2. La p være et primtall slik at $p > 2$. Da er $\mathbb{L}_p^1 = 1$.

Bevis. Siden $x = 1$ er en løsning til kongruensen

$$x^2 \equiv 1 \pmod{p},$$

er 1 e kvadratisk rest modulo p. Dermed er $\mathbb{L}_p^1 = 1$. □

Proposisjon 5.5.3. La p være et primtall slik at $p > 2$. La a og b være heltall slik at

$$a \equiv b \pmod{p}.$$

Da er $\mathbb{L}_p^a = \mathbb{L}_p^b$.

Bevis. La x være et heltall. Dersom

$$a \equiv b \pmod{p},$$

er

$$a \equiv 0 \pmod{p}$$

hvis ogh bare hvis

$$b \equiv 0 \pmod{p}.$$

Derfor er $\mathbb{L}_p^a = 0$ om og bare om $\mathbb{L}_p^b = 0$. Anta at det ikke er sant at $\mathbb{L}_p^a = 0$. Vi har:

$$x^2 \equiv a \pmod{p}$$

om og bare om

$$x^2 \equiv b \pmod{p}.$$

Dermed er a en kvadratisk rest modulo p om og bare om b er en kvadratisk rest modulo p. Således er $\mathbb{L}_p^a = 1$ om og bare om $\mathbb{L}_p^b = 1$, og er $\mathbb{L}_p^a = -1$ om og bare om $\mathbb{L}_p^b = 1$. □

Eksempel 5.5.4. Vi har:

$$10 \equiv 3 \pmod{7}.$$

Ut ifra Eksempel 5.3.7, er $\mathbb{L}_7^3 = -1$. Da fastslår Proposisjon 5.5.3 at $\mathbb{L}_7^{10} = -1$. Dermed er 10 ikke en kvadratisk rest modulo 7.

Eksempel 5.5.5. Vi har:

$$-6 \equiv 5 \pmod{11}.$$

Ut ifra Eksempel 5.3.8, er $\mathbb{L}_{11}^5 = 1$. Da fastslår Proposisjon 5.5.3 at $\mathbb{L}_{11}^{-6} = 1$. Dermed er -6 en kvadratisk rest modulo 11.

Proposisjon 5.5.6. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da er $\mathbb{L}_p^{a^2} = 1$.

Bevis. Siden $x = a$ er en løsning til kongruensen

$$x^2 \equiv a^2 \pmod{p},$$

er a^2 en kvadratisk rest modulo p. Dermed er $\mathbb{L}_p^{a^2} = 1$.

□

Eksempel 5.5.7. Siden $5^2 = 25$, fastslår Proposisjon 5.5.3 at $\mathbb{L}_{17}^{25} = 1$. Siden

$$25 \equiv 8 \pmod{17},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{17}^{8} = 1$. Dermed er 8 en kvadratisk rest modulo 17.

Eksempel 5.5.8. Siden $7^2 = 49$, fastslår Proposisjon 5.5.3 at $\mathbb{L}_{31}^{49} = 1$. Siden

$$49 \equiv 18 \pmod{31},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{31}^{18} = 1$. Dermed er 18 en kvadratisk rest modulo 31.

Proposisjon 5.5.9. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da er

$$\mathbb{L}_p^a \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Bevis. Anta først at a er en kvadratisk rest modulo p. Vi gjør følgende observasjoner.

(1) Da er $\mathbb{L}_p^a = 1$.

(2) Ut ifra Proposisjon 5.3.2 er da

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

altså

$$1 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Det følger fra (1) og (2) at

$$\mathbb{L}_p^a \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Anta nå at a ikke er en kvadratisk rest modulo p. Vi gjør følgende observasjoner.

(1) Da er $\mathbb{L}_p^a = -1$.

(2) Ut ifra Korollar 5.3.12 er da

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

altså

$$-1 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Det følger fra (1) og (2) at

$$\mathbb{L}_p^a \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

□

Eksempel 5.5.10. Proposisjon 5.5.9 fastslår at

$$\mathbb{L}_7^5 \equiv 5^{\frac{7-1}{2}} \pmod{7},$$

altså at

$$\mathbb{L}_7^5 \equiv 5^3 \pmod{7}.$$

Vi har:

$$5^3 \equiv 5^2 \cdot 5 \equiv 4 \cdot 5 = 20 \equiv -1 \pmod{7}.$$

Ut ifra Eksempel 5.3.6 er det riktignok sant at $\mathbb{L}_7^5 = -1$.

Eksempel 5.5.11. Proposisjon 5.5.9 fastslår at

$$\mathbb{L}_{11}^{14} \equiv 14^{\frac{11-1}{2}} \pmod{11},$$

altså at

$$\mathbb{L}_{11}^{14} \equiv 14^5 \pmod{11}.$$

Vi gjør følgende observasjoner.

(1) Vi har:

$$14^5 \equiv 3^5 = 3^3 \cdot 3^2 = 27 \cdot 9 \equiv 5 \cdot 9 = 45 \equiv 1 \pmod{11}.$$

(2) Ut ifra Proposisjon 5.5.3 er $\mathbb{L}_{11}^{14} = \mathbb{L}_{11}^3$. Ut ifra Eksempel 5.3.8 er $\mathbb{L}_{11}^3 = 1$.

Dermed er det riktignok sant at

$$\mathbb{L}_{11}^{14} \equiv 14^5 \pmod{11}.$$

Merknad 5.5.12. La p være et primtall slik at $p > 2$. La a være et heltall. Legendresymbolet $\mathbb{L}_p^a$ noterer om a er eller ikke er en kvadratisk rest modulo p. Hvorfor valgte vi 1 og -1 for å gjøre dette, og ikke et hvilket som helst annet par heltall?

Svaret er: fordi dette er det eneste valget slik at Proposisjon 5.5.9 er sann! Proposisjon 5.3.2 er dyp og viktig, og Proposisjon 5.5.9 gir oss muligheten til å benytte oss av Proposisjon 5.3.2 når vi manipulerer Legendresymboler. Vi kommer til snart til å se at dette er svært nyttig i praksis. I tillegg er det uunnværlig fra et teoretisk synspunkt for å kunne gi et bevis for Teorem **??**, og for å kunne gi et bevis for følgende to proposisjoner, som vi kommer til å benytte oss hele tida når vi regner ut Legendresymboler.

Proposisjon 5.5.13. La p være et primtall slik at $p > 2$. La a og b være heltall. Da er

$$\mathbb{L}_p^{ab} = \mathbb{L}_p^a \cdot \mathbb{L}_p^b.$$

Bevis. Anta først at

$$a \equiv 0 \pmod{p}.$$

Da er

$$\mathbb{L}_p^{ab} = \mathbb{L}_p^{0 \cdot b} = \mathbb{L}_p^0 = 0.$$

I tillegg er

$$\mathbb{L}_p^a \cdot \mathbb{L}_p^b = \mathbb{L}_p^0 \cdot \mathbb{L}_p^b = 0 \cdot \mathbb{L}_p^b = 0.$$

Dermed er

$$\mathbb{L}_p^{ab} = \mathbb{L}_p^a \cdot \mathbb{L}_p^b.$$

Et lignende argument viser at, dersom

$$b \equiv 0 \pmod{p},$$

er både $\mathbb{L}_p^{ab}$ og $\mathbb{L}_p^a \cdot \mathbb{L}_p^b$ like 0, og derfor er

$$\mathbb{L}_p^{ab} = \mathbb{L}_p^a \cdot \mathbb{L}_p^b.$$

Anta nå at det ikke er sant at

$$a \equiv 0 \pmod{p},$$

og at det ikke er sant at

$$b \equiv 0 \pmod{p}.$$

Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_p^a \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

(2) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_p^b \equiv b^{\frac{p-1}{2}} \pmod{p}.$$

(3) Det følger fra (1) og (2) at

$$\mathbb{L}_p^a \cdot \mathbb{L}_p^b \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \pmod{p}.$$

Siden

$$a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}},$$

er dermed

$$\mathbb{L}_p^a \cdot \mathbb{L}_p^b \equiv (ab)^{\frac{p-1}{2}} \pmod{p},$$

altså

$$(ab)^{\frac{p-1}{2}} \equiv \mathbb{L}_p^a \cdot \mathbb{L}_p^b \pmod{p}.$$

(4) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_p^{ab} \equiv (ab)^{\frac{p-1}{2}} \pmod{p}.$$

Det følger fra (3) og (4) at

$$\mathbb{L}_p^{ab} \equiv \mathbb{L}_p^a \cdot \mathbb{L}_p^b \pmod{p}.$$

Siden $\mathbb{L}_p^a$ er likt 1 eller -1, og $\mathbb{L}_p^a \cdot \mathbb{L}_p^b$ er likt 1 eller -1, følger det fra Proposisjon 5.3.10 at $\mathbb{L}_p^{ab} = \mathbb{L}_p^a \cdot \mathbb{L}_p^b$.

□

Eksempel 5.5.14. Ut ifra Eksempel 5.3.6 er $\mathbb{L}_5^3 = -1$ og $\mathbb{L}_5^4 = 1$. Proposisjon 5.5.13 fastslår at

$$\mathbb{L}_5^{\dot{34}} = \mathbb{L}_5^3 \cdot \mathbb{L}_5^4 = (-1) \cdot 1 = -1,$$

altså at $\mathbb{L}_5^{12} = -1$. Dette er riktignok sant: ut ifra Proposisjon 5.5.3 er $\mathbb{L}_5^{12} = \mathbb{L}_5^2$, og ut ifra Eksempel 5.3.6 er $\mathbb{L}_5^2 = -1$.

Eksempel 5.5.15. Ut ifra Eksempel 5.3.8 er $\mathbb{L}_{11}^2 = -1$ og $\mathbb{L}_{11}^7 = -1$. Proposisjon 5.5.13 fastslår at

$$\mathbb{L}_{11}^{\dot{27}} = \mathbb{L}_{11}^2 \cdot \mathbb{L}_{11}^7 = (-1) \cdot (-1) = 1,$$

altså at $\mathbb{L}_{11}^{114} = 1$. Dette er riktignok sant: ut ifra Proposisjon 5.5.3 er $\mathbb{L}_{11}^{14} = \mathbb{L}_{11}^3$, og ut ifra Eksempel 5.3.8 er $\mathbb{L}_{11}^3 = 1$.

Proposisjon 5.5.16. La p være et primtall slik at $p > 2$. Da er

$$\mathbb{L}_p^{-1} = (-1)^{\frac{p-1}{2}}.$$

Bevis. Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_p^{-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Siden $\mathbb{L}_p^{-1}$ er likt enten 1 eller -1, og $(-1)^{\frac{p-1}{2}}$ er likt enten 1 eller -1, følger det fra Proposisjon 5.3.10 at

$$\mathbb{L}_p^{-1} = (-1)^{\frac{p-1}{2}}.$$

□

Eksempel 5.5.17. Proposisjon 5.5.16 fastslår at

$$\mathbb{L}_5^{-1} = (-1)^{\frac{5-1}{2}} = (-1)^2 = 1.$$

Dette er riktignok sant: ut ifra Proposisjon 5.5.3 er $\mathbb{L}_5^{-1} = \mathbb{L}_5^4$, og ut ifra Eksempel 5.3.6 er $\mathbb{L}_5^4 = 1$.

Eksempel 5.5.18. Proposisjon 5.5.16 fastslår at

$$\mathbb{L}_7^{-1} = (-1)^{\frac{7-1}{2}} = (-1)^3 = -1.$$

Dette er riktignok sant: ut ifra Proposisjon 5.5.3 er $\mathbb{L}_7^{-1} = \mathbb{L}_7^6$, og ut ifra Eksempel 5.3.7 er $\mathbb{L}_7^6 = -1$.

5.6 Eksempler på hvordan regne ut Legendresymboler

Merknad 5.6.1. Proposisjonene den foregående delen av kapittelet gir oss en kraftig metode for å regne ut $\mathbb{L}_p^a$ for et hvilket som helst heltall a og et hvilket som helst primtall p slik at $p > 2$.

(1) Finn en primtallsfaktorisering $p_1 \cdots p_t$ til a. Da fastslår Proposisjon 5.5.13 at

$$\mathbb{L}_p^a = \mathbb{L}_p^{p_1} \ldots \mathbb{L}_p^{p_t}.$$

(2) Regn ut hvert av Legendresymbolene $\mathbb{L}_p^{p_1}$, $\mathbb{L}_p^{p_2}$, …, $\mathbb{L}_p^{p_t}$.

I denne delen av kapittelet kommer vi til å se på noen eksempler på hvordan denne metoden gjennomføres. Dette kan ses som en oppvarming før vi ser på kvadratisk gjensidighet, som kommer til å gi oss muligheten til å gjøre metoden ovenfor fullkommen.

Proposisjon 5.6.2. Heltallet 84 er ikke en kvadratisk rest modulo 23.

Bevis. Vi gjør følgende observasjoner.

(1) Siden

$$84 \equiv 15 \pmod{23},$$

følger det fra Proposisjon 5.5.3 at $\mathbb{L}_{23}^{84} = \mathbb{L}_{23}^{15}$.

(2) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{23}^{15} = \mathbb{L}_{23}^{3\cdot 5} = \mathbb{L}_{23}^{3} \cdot \mathbb{L}_{23}^{5}.$$

(3) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_{23}^{3} \equiv 3^{\frac{23-1}{2}} \pmod{23},$$

altså

$$\mathbb{L}_{23}^{3} \equiv 3^{11} \pmod{23}.$$

Vi har:

$$3^{11} = \left(3^3\right)^3 \cdot 3^2 = 27^3 \cdot 9 \equiv 4^3 \cdot 9 = 64 \cdot 9 \equiv (-5) \cdot 9 = -45 \equiv 1 \pmod{23}.$$

Dermed er

$$\mathbb{L}_{23}^{3} \equiv 1 \pmod{23}.$$

Det følger fra Proposisjon 5.3.10 at $\mathbb{L}_{23}^{3} = 1$.

(4) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_{23}^{5} \equiv 5^{\frac{23-1}{2}} \pmod{23},$$

altså

$$\mathbb{L}_{23}^{5} \equiv 5^{11} \pmod{23}.$$

Vi har:

$$5^{11} = \left(5^2\right)^5 \cdot 5 = 25^5 \cdot 5 \equiv 2^5 \cdot 5 = 32 \cdot 5 \equiv 9 \cdot 5 = 45 \equiv -1 \pmod{23}.$$

Dermed er

$$\mathbb{L}_{23}^{5} \equiv -1 \pmod{23}.$$

Det følger fra Proposisjon 5.3.10 at $\mathbb{L}_{23}^{5} = -1$.

Det følger fra (1) – (4) at

$$\mathbb{L}_{23}^{84} = \mathbb{L}_{23}^{15} = \mathbb{L}_{23}^{3} \cdot \mathbb{L}_{23}^{5} = 1 \cdot (-1) = -1.$$

Således er 84 ikke en kvadratisk rest modulo 23.

□

Proposisjon 5.6.3. Heltallet 28 er en kvadratisk rest modulo 59.

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{59}^{28} = \mathbb{L}_{59}^{4 \cdot 7} = \mathbb{L}_{59}^{4} \cdot \mathbb{L}_{59}^{7}.$$

(2) Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{59}^{4} = 1$.

(3) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_{59}^{7} \equiv 7^{\frac{59-1}{2}} \pmod{59},$$

altså

$$\mathbb{L}_{59}^{7} \equiv 7^{28} \pmod{59}.$$

Vi har:

$$7^2 = 49 \equiv -10 \pmod{59}.$$

Da er

$$7^3 = 7^2 \cdot 7 \equiv (-10) \cdot 7 = -70 \equiv -11 \pmod{7}.$$

Det følger at

$$7^6 = \left(7^3\right)^2 \equiv (-11)^2 = 121 \equiv 3 \pmod{59}.$$

Da er

$$7^{29} = \left(7^6\right)^4 \cdot 7^3 \cdot 7^2 \equiv 3^4 \cdot (-10) \cdot (-11) = 81 \cdot 110 \equiv 22 \cdot (-8) = -176 \equiv 1 \pmod{59}.$$

Dermed er

$$\mathbb{L}_{59}^{7} \equiv 1 \pmod{59}.$$

Det følger fra Proposisjon 5.3.10 at $\mathbb{L}_{59}^{7} = 1$.

Det følger fra (1) – (3) at

$$\mathbb{L}_{59}^{28} = \mathbb{L}_{59}^{4} \cdot \mathbb{L}_{59}^{7} = 1 \cdot 1 = 1.$$

Således er 28 en kvadratisk rest modulo 59.

□

Merknad 5.6.4. Proposisjon 5.6.3 fastslår at kongruensen

$$x^2 \equiv 28 \pmod{59}$$

har en løsning. Imidlertid sier proposisjonen ikke hvordan en løsning kan *finnes*. Dette stemmer generelt sett: Legendresymbolet er utrolig nyttig for å bestemme *om* en kvadratisk kongruens har en løsning, men sier ingenting om *hvordan* en eventuell løsning kan finnes.

Faktisk finnes det en algoritme, *Tonelli-Shanks' algoritme*, for å finne løsningene til en kongruens

$$x^2 \equiv a \pmod{p}.$$

I løpet av å gjennomføre denne algoritmen, regner man ut noen Legendresymboler. Det vil si: Legendresymbolet *kan* også benyttes for å *finne* løsninger til kvadratiske kongruenser.

Mens vi har alt vi trenger for å forstå Tonelli-Shanks' algoritme, kommer vi ikke til å se på den i kurset: da hadde vi fått tid til å se på noen av de fine temaene vi kommer til å se på i resten av kurset. Les imidlertid gjerne om Tonelli-Shanks' algoritme: dette er en fin måte å fordype og konsolidere forståelsen din for teorien i dette kapittelet av forelesningsnotatene.

Proposisjon 5.6.5. Kongruensen

$$-25x^2 + 44x - 37 \equiv 0 \pmod{211}$$

har ingen løsning.

Bevis. Vi har:

$$44^2 - 4 \cdot (-25) \cdot (-27) = 1936 - 3700 = -1764.$$

La oss regne ut $\mathbb{L}_{211}^{-1764}$.

(1) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{211}^{-1764} = \mathbb{L}_{211}^{(-1)\cdot 6^2 \cdot 7^2} = \mathbb{L}_{211}^{-1} \cdot \mathbb{L}_{79}^{6^2} \cdot \mathbb{L}_{79}^{7^2}.$$

(2) Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{211}^{6^2} = 1$.

(3) Ut ifra Proposisjon 5.5.6 er $\mathbb{L}_{211}^{7^2} = 1$.

(4) Ut ifra Proposisjon 5.5.16 er

$$\mathbb{L}_{211}^{-1} = (-1)^{\frac{211-1}{2}} = (-1)^{105} = -1.$$

Det følger fra (1) – (4) at

$$\mathbb{L}_{211}^{-1764} = \mathbb{L}_{211}^{-1} \cdot \mathbb{L}_{211}^{6^2} \cdot \mathbb{L}_{211}^{7^2} = (-1) \cdot 1 \cdot 1 = -1.$$

Således er -1764 ikke en kvadratisk rest modulo 211. Ut ifra Korollar 5.2.30, konkluderer vi at kongruensen

$$-25x^2 + 44x - 37 \equiv 0 \pmod{211}$$

har ingen løsning.

□

Proposisjon 5.6.6. Kongruensen

$$x^2 - 8x + 57 \equiv 0 \pmod{79}$$

har to løsninger som ikke er kongruent til hverandre modulo 79, og slik at enhver annen løsning er kongruent modulo 79 til én av disse to.

Bevis. Vi har:

$$(-8)^2 - 4 \cdot 1 \cdot 57 = 64 - 228 = -164.$$

La oss regne ut $\mathbb{L}_{79}^{-164}$.

(1) Siden

$$-164 \equiv -6 \pmod{79},$$

følger det fra Proposisjon 5.5.3 at

$$\mathbb{L}_{79}^{-164} = \mathbb{L}_{79}^{-6}.$$

(2) Ut ifra Proposisjon 5.5.13 er

$$\mathbb{L}_{79}^{-6} = \mathbb{L}_{79}^{(-1)\cdot 2\cdot 3} = \mathbb{L}_{79}^{-1} \cdot \mathbb{L}_{79}^{2} \cdot \mathbb{L}_{79}^{3}.$$

(3) Ut ifra Proposisjon 5.5.16 er

$$\mathbb{L}_{79}^{-1} = (-1)^{\frac{79-1}{2}} = (-1)^{39} = -1.$$

(4) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_{79}^{2} \equiv 2^{\frac{79-1}{2}} \pmod{79},$$

altså

$$\mathbb{L}_{79}^{2} \equiv 2^{39} \pmod{79}.$$

Vi har:

$$2^6 = 64 \equiv -15 \pmod{79}.$$

Da er

$$2^{12} = \left(2^6\right)^2 \equiv (-15)^2 = 225 \equiv -12 \pmod{79}.$$

Derfor er

$$2^{24} = \left(2^{12}\right)^2 \equiv (-12)^2 = 144 \equiv -14 \pmod{79}.$$

Da er

$$2^{36} = 2^{12} \cdot 2^{24} \equiv (-12) \cdot (-14) = 168 \equiv 10 \pmod{79}.$$

Vi konkluderer at

$$2^{39} = 2^{36} \cdot 2^3 \equiv 10 \cdot 8 = 80 \equiv 1 \pmod{79}.$$

Dermed er

$$\mathbb{L}_{79}^2 \equiv 1 \pmod{79}.$$

Det følger fra Proposisjon 5.3.10 at $\mathbb{L}_{79}^2 = 1$.

(5) Ut ifra Proposisjon 5.5.9 er

$$\mathbb{L}_{79}^3 \equiv 3^{\frac{79-1}{2}} \pmod{79},$$

altså

$$\mathbb{L}_{79}^3 \equiv 3^{39} \pmod{79}.$$

Vi har:

$$3^4 = 81 \equiv 2 \pmod{79}.$$

Da er

$$3^{36} = \left(3^4\right)^9 \equiv 2^9 \pmod{79}.$$

Ut ifra (4) er

$$2^6 \equiv -15 \pmod{79}.$$

Da er

$$2^9 = 2^6 \cdot 2^3 \equiv -15 \cdot 8 = -120 \equiv 38 \pmod{79}.$$

Dermed er

$$3^{36} \equiv 38 \pmod{79}.$$

Da er

$$3^{37} = 3^{36} \cdot 3 \equiv 38 \cdot 3 = 114 \equiv 35 \pmod{79}.$$

Det følger at

$$3^{38} = 3^{37} \cdot 3 \equiv 35 \cdot 3 = 105 \equiv 26 \pmod{79}.$$

Vi konkluderer at

$$3^{39} = 3^{38} \cdot 3 \equiv 26 \cdot 3 = 78 \equiv -1 \pmod{79}.$$

Dermed er

$$\mathbb{L}_{79}^3 \equiv -1 \pmod{79}.$$

Det følger fra Proposisjon 5.3.10 at $\mathbb{L}_{79}^3 = -1$.

Det følger fra (1) – (5) at

$$\mathbb{L}_{79}^{-164} = \mathbb{L}_{79}^{-6} = \mathbb{L}_{79}^{-1} \cdot \mathbb{L}_{79}^{2} \cdot \mathbb{L}_{79}^{3} = (-1) \cdot 1 \cdot (-1) = 1.$$

Dermed er -164 en kvadratisk rest modulo 79. Ut ifra Korollar 5.2.30, konkluderer vi at kongruensen

$$x^2 - 8x + 57 \equiv 0 \pmod{79}$$

har to løsninger som ikke er kongruent til hverandre modulo 79, og slik at enhver annen løsning er kongruent modulo 79 til én av disse to.

□

Merknad 5.6.7. For å understreke Merknad 5.6.4, sier Proposisjon 5.6.6 at det *finnes* to løsninger, men ikke hva disse to løsningene er. Tonelli-Shanks' algoritme, som vi ikke kommer til å se på i kurset, kan benyttes for å finne de to løsningene.

Oppgaver

O5.1 Oppgaver i eksamens stil

Merknad. Benytt ikke kvadratisk gjensidighet eller proposisjoner som bygger på kvadratisk gjendsidighet i løpet av svarene dine til følgende oppgaver. Benytt imidlertid gjerne Legendresymbolet! Med andre ord, benytt kun teorien vi har sett på opp til slutten av Forelesning 19.

Oppgave O5.1.4. Gjør følgende.

(1) Vis uten å regne ut at
$$2^{26} \equiv -1 \pmod{53}.$$

(2) Vis uten å regne ut at
$$7^{26} \equiv 1 \pmod{53}.$$

(3) Er 173 en kvadratisk rest modulo 53? Benytt Legendresymbolet, (1), og (2) i løpet av svaret ditt.

Oppgave O5.1.5. Er 45 en kvadratisk rest modulo 89? *Tips*: Vis at $5^4 \equiv 2 \pmod{89}$.

Oppgave O5.1.6. Hvor mange løsninger (slik at ingen par av disse er kongruent til hverandre) har følgende kongruenser? Begrunn svaret. Det er ikke nødvendig å *finne* løsninger.

(1) $-4x^2 + 2x - 1 \equiv 0 \pmod{241}$

(2) $7x^2 + 16x + 10 \equiv 0 \pmod{61}$

(3) $9x^2 - 12x + 4 \equiv 0 \pmod{113}$