Oversikt over kvadratiske kongruenser og Legendresymboler

Richard Williamson

3. desember 2014

Oppgave 1

Heltallet 12763 er et primtall. Er 11799 en kvadratisk rest modulo 12763?

Hvordan løse oppgaven?

Oversett først til et utsagn om Legendresymboler. Da blir oppgaven: er $\mathbb{L}_{12763}^{11799} = 1$ eller er $\mathbb{L}_{12763}^{11799} = -1$?

Hva er et Legendresymbol?

Det er ikke noe dypt! Symbolet $\mathbb{L}_{12763}^{11799}$ noterer ganske enkelt om 11799 er en kvadratisk rest modulo 12763 eller ikke.

(1) Dersom 11799 er en kvadratisk rest modulo 12763, er $\mathbb{L}_{12763}^{11799} = 1$.

(2) Dersom 11799 ikke er en kvadratisk rest modulo 12763, er $\mathbb{L}_{12763}^{11799} = -1$.

Poenget med å oversette oppgaven til et utsagn om Legendresymboler er at vi har en kraftig metode for å bestemme om $\mathbb{L}_{12763}^{11799} = 1$ eller $\mathbb{L}_{12763}^{11799} = -1$.

Noe som ikke er så viktig

Det eneste unntaket til at $\mathbb{L}_{12763}^{11799} = 1$ eller $\mathbb{L}_{12763}^{11799} = -1$ er: dersom det hadde vært sant at $12763 \mid 11799$, hadde da $\mathbb{L}_{12763}^{11799}$ vært likt 0. Ut ifra Definisjon 5.2.1, er det imidlertid bare lov å spørre om et 11799 er en kvadratisk rest modulo 12763 dersom det ikke er sant at $12763 \mid 11799$.

Derfor kan du ta det som gitt at det ikke er sant at $12763 \mid 11799$, altså at $\mathbb{L}_{12763}^{11799} = 1$ eller $\mathbb{L}_{12763}^{11799} = -1$.

Hva er en kvadratisk rest for noe?

Å si at 11799 er en kvadratisk rest modulo 12763 er å si at det finnes et heltall y slik at

$$y^2 \equiv 11799 \pmod{12763}.$$

Dette sier at 11799 «har en kvadratrot som er et heltall» i aritmetikk modulo 12763.

Å si at $\mathbb{L}_{12763}^{11799} = 1$ er altså å si at det finnes et heltall y slik at

$$y^2 \equiv 11799 \pmod{12763}.$$

Vi vet ikke hva y er, uten å benytte en algoritme som vi ikke har sett på i kurset, men vi vet at det finnes.

Å si at $\mathbb{L}_{12763}^{11799} = -1$ er å si at det ikke finnes et heltall y slik at

$$y^2 \equiv 11799 \pmod{12763}.$$

Hvordan regne ut et Legendresymbol?

Vi benytter følgende regler, hvor a og b er heltall, r er et naturlig tall, og p og q er primtall slik at $p > 2$, $q > 2$, og $p \neq q$.

(A) $\mathbb{L}_p^{a \cdot b} = \mathbb{L}_p^a \cdot \mathbb{L}_p^b$.

(B) Dersom $a \equiv b \pmod{p}$, er $\mathbb{L}_p^a = \mathbb{L}_p^b$.

(C) $\mathbb{L}_p^1 = 1$.

(D) $\mathbb{L}_p^{r^2} = 1$.

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

(F) $\mathbb{L}_p^2 = 1$ dersom enten $p \equiv 1 \pmod{8}$ eller $p \equiv 7 \pmod{8}$, og $\mathbb{L}_p^2 = -1$ dersom enten $p \equiv 3 \pmod{8}$ eller $p \equiv 5 \pmod{8}$.

(G) $\mathbb{L}_q^p = \mathbb{L}_p^q$ dersom $p \equiv 1 \pmod{4}$ eller $q \equiv 1 \pmod{4}$ eller begge, og $\mathbb{L}_q^p = -\mathbb{L}_p^q$ dersom både $p \equiv 3 \pmod{4}$ og $q \equiv 3 \pmod{4}$.

Hvilke av disse reglene bør jeg huske?

Reglene (F) og (G) blir gitt, men de andre må huskes. Dette blir ikke noe problem: vi må bare øve oss nok! Det er ikke nødvendig å huske (E), fordi vi alltid kan benytte (B) for å erstatte et negativt heltall øverst med et naturlig tall. Imidlertid kan vi noen ganger fullføre en utregning fortere ved å benytte (E).

Hvordan benytter jeg disse reglene i praksis?

Først sjekker vi om 11799 er et primtall: det er ikke, siden $3 \mid 11799$. Da finner vi en primtallsfaktorisering til 11799: vi får $11799 = 3^3 \cdot 19 \cdot 23$.

Hva gjør jeg da?

Benytt (A). Vi får:

$$\mathbb{L}_{12763}^{11799} = \mathbb{L}_{12763}^{3^3 \cdot 19 \cdot 23} = \mathbb{L}_{12763}^{3^3} \cdot \mathbb{L}_{12763}^{19} \cdot \mathbb{L}_{12763}^{23}.$$

Husk: etter å ha funnet en primtallsfaktorisering, benytter vi alltid (A).

Hva gjør vi nå?

Vi regner ut $\mathbb{L}_{12763}^{3^3}$, $\mathbb{L}_{12763}^{19}$, og $\mathbb{L}_{12763}^{23}$ hvert for seg. Husk: etter å ha benyttet (A), regner vi alltid ut alle de nye Legendresymbolene vi har fått hvert for seg.

Hvordan regne ut $\mathbb{L}_{12763}^{3^3}$?

Vi benytter (A):

$$\mathbb{L}_{12763}^{3^3} = \mathbb{L}_{12763}^{3^2 \cdot 3} = \mathbb{L}_{12763}^{3^2} \cdot \mathbb{L}_{12763}^{3}.$$

Nå benytter vi (B): $\mathbb{L}_{12763}^{3^2} = 1$. Dermed er

$$\mathbb{L}_{12763}^{3^3} = 1 \cdot \mathbb{L}_{12763}^{3}.$$

Vi trenger ikke å jobbe med potenser større enn 1

Et lignende triks virker alltid. Hvis vi ønsker å regne ut $\mathbb{L}_{12763}^{3^{57}}$, kan vi benytte (A) og (B) for å få:

$$\mathbb{L}_{12763}^{3^{57}} = \mathbb{L}_{12763}^{3^{56} \cdot 3} = \mathbb{L}_{12763}^{3^{56}} \cdot \mathbb{L}_{12763}^{3} = \mathbb{L}_{12763}^{\left(3^{28}\right)^2} \cdot \mathbb{L}_{12763}^{3} = 1 \cdot \mathbb{L}_{12763}^{3} = \mathbb{L}_{12763}^{3}.$$

Det er ikke noe spesielt med 3 her: akkurat det samme argumentet viser at $\mathbb{L}_{12763}^{a^{57}} = \mathbb{L}_{12763}^{a}$ for et hvilket som helst naturlig tall a. Det er heller ikke noe spesielt med 57 her: $\mathbb{L}_{12763}^{a^k} = \mathbb{L}_{12763}^{a}$ for et hvilket som helst oddetall k.

Hvis vi ønsker å regne ut $\mathbb{L}_{12763}^{3^{58}}$, kan vi benytte (B) for å få:

$$\mathbb{L}_{12763}^{3^{58}} = \mathbb{L}_{12763}^{\left(3^{29}\right)^2} = 1.$$

Igjen er det ikke noe spesielt med 3 her: akkurat det samme argumentet viser at $\mathbb{L}_{12763}^{a^{58}} = 1$ for et hvilket som helst naturlig tall a. Det er heller ikke noe spesielt med 58 her: $\mathbb{L}_{12763}^{a^k} = \mathbb{L}_{12763}^{a}$ for et hvilket som helst partall k.

Hvordan regne ut $\mathbb{L}_{12763}^{3}$?

Vi benytter (G). Vi må sjekke om minst ett av 3 og 12763 er kongruent til 1 modulo 4. Dette er ikke sant: vi har både

$$12763 \equiv 3 \pmod 4$$

og

$$12763 \equiv 3 \pmod 4.$$

Derfor sier (G) at vi har:

$$\mathbb{L}_{12763}^{3} = -\mathbb{L}_{3}^{12763}.$$

Når vi benytter (G), snu vi alltid de to primtallene. Poenget er å bestemme om vi har et minustegn foran den snudde Legendresymbolet eller ikke, og vi gjør dette ved å sjekke om minst ett av 3 og 12763 er kongruent til 1 modulo 4.

Hvorfor hjelper det å snu sånn?

Nå benytter vi (B). Vi har:

$$12763 \equiv 1 \pmod 3.$$

Da sier (B) at $\mathbb{L}_{3}^{12763} = \mathbb{L}_{3}^{1}$.

Nå kan vi benytte (C): vi får

$$\mathbb{L}_{3}^{1} = 1.$$

Husk:

(1) Når vi har et primtall øverst som ikke er 2, benytter vi alltid (G) og deretter (B). Hvis vi da kan benytte (C), (D), (E), eller (F), gjør vi det.

(2) Ellers fortsetter vi. Hvis vi har et primtall, benytter vi igjen (G) og deretter (B).

(3) Hvis vi ikke har et primtall, finner vi en primtallsfaktorisering, og vi regner deretter ut alle de nye Legendresymbolene vi får hvert for seg.

Så langt

Nå har vi regnet ut $\mathbb{L}_{12763}^{3}$. For å oppsummere:

$$\mathbb{L}_{12763}^{3} = -\mathbb{L}_{3}^{12763} = -\mathbb{L}_{3}^{1} = -1.$$

Hvordan regne ut $\mathbb{L}_{12763}^{19}$?

Husk metoden: når vi har et primtall som ikke er 2, benytter vi alltid (G) og deretter (B). Når vi benytter (G), må vi sjekke om minst ett av 19 og 12763 er kongruent til 1 modulo 4. Dette er ikke sant: både

$$19 \equiv 3 \pmod 4$$

og

$$12763 \equiv 3 \pmod 4.$$

Derfor sier (G) at $\mathbb{L}_{12763}^{19} = -\mathbb{L}_{19}^{12763}$.

Nå benytter vi (B). Vi har:

$$12763 \equiv 14 \pmod{19}.$$

Derfor sier (B) at $\mathbb{L}_{19}^{12763} = \mathbb{L}_{19}^{14}$.

Hva gjør jeg når jeg får noe som ikke er et primtall?

Husk: hver gang vi får et nytt Legendresymbol, sjekk først om vi kan benytte (C), (D), (E), eller (F). Hvis ikke, sjekk om heltallet øverst er et primtall. Hvis det er et primtall, benytt (G). Hvis det ikke er primtall, finn en primtallsfaktorisering.

I dette tilfellet har vi 14 øverst, som ikke er et primtall. Da finner vi en primtallsfaktorisering: $14 = 2 \cdot 7$. Husk nå metoden: etter å ha funnet en primtallsfaktorisering, benytt (A), og så regn ut alle de nye Legendresymbolene vi får hvert for seg.

Når vi benytter (A), får vi:

$$\mathbb{L}_{19}^{14} = \mathbb{L}_{19}^{2\cdot 7} = \mathbb{L}_{19}^{2} \cdot \mathbb{L}_{19}^{7}.$$

Da må vi regne ut $\mathbb{L}_{19}^{2}$ og $\mathbb{L}_{19}^{7}$ hvert for seg.

Hvordan regne ut $\mathbb{L}_{19}^{2}$?

Vi benytter (F). Vi har:

$$19 \equiv 3 \pmod 8.$$

Da sier (F) at $\mathbb{L}_{19}^{2} = -1$.

Hvordan regne ut $\mathbb{L}_{19}^{7}$?

Siden vi har et primtall øverst, benytter vi (G) og deretter (B).

Vi må sjekke om minst ett av 7 og 19 er kongruent til 1 modulo 4. Dette er ikke sant: både 7 og 19 er kongruent til 3 modulo 4. Da sier (G) at $\mathbb{L}_{19}^{7} = -\mathbb{L}_{7}^{19}$.

Siden

$$19 \equiv 5 \pmod 7,$$

sier (B) at $\mathbb{L}_{7}^{19} = \mathbb{L}_{7}^{5}$.

Hvordan regne ut $\mathbb{L}_{7}^{5}$?

Siden vi har et primtall øverst, benytter vi (G) og deretter (B).

Vi må sjekke om minst ett av 5 og 7 er kongruent til 1 modulo 4. Dette er sant:

$$5 \equiv 1 \pmod 4.$$

Da sier (G) at $\mathbb{L}_{7}^{5} = \mathbb{L}_{5}^{7}$.

Siden

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

sier (B) at $\mathbb{L}_{5}^{7} = \mathbb{L}_{5}^{2}$.

Hvordan regne ut $\mathbb{L}_{7}^{2}$?

Vi benytter (F). Siden

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

sier (F) at $\mathbb{L}_{5}^{2} = -1$.

Nå kan vi fullføre utregningen av $\mathbb{L}^{19}_{12763}$

Vi har sett at:

$$\begin{aligned}
\mathbb{L}^{19}_{12763} &= -\mathbb{L}^{12763}_{19} \\
&= -\mathbb{L}^{14}_{19} \\
&= -\mathbb{L}^{2}_{19} \cdot \mathbb{L}^{7}_{19} \\
&= -\mathbb{L}^{2}_{19} \cdot \left(-\mathbb{L}^{19}_{7}\right) \\
&= -\mathbb{L}^{2}_{19} \cdot \left(-\mathbb{L}^{5}_{7}\right) \\
&= -\mathbb{L}^{2}_{19} \cdot \left(-\mathbb{L}^{7}_{5}\right) \\
&= -\mathbb{L}^{2}_{19} \cdot \left(-\mathbb{L}^{2}_{5}\right) \\
&= -(-1) \cdot (-(-1)) \\
&= 1 \cdot 1 \\
&= 1.
\end{aligned}$$

Hvordan regne ut $\mathbb{L}^{23}_{12763}$?

Vi har nå sett alt som må forstås for å regne ut et hvilket som helst Legendresymbol. La oss øve oss litt mer.

Husk hva vi gjør når vi har et primtall øverst: vi benytter (G). Vi må sjekke om minst ett av 23 og 12763 er kongruent til 1 modulo 4. Dette er ikke sant: både 23 og 12673 er kongruent til 3 modulo 4. Derfor sier (F) at $\mathbb{L}^{23}_{12763} = -\mathbb{L}^{12763}_{23}$.

Husk nå hva vi gjør etter å ha benyttet (G): vi benytter (B). Siden

$$12763 \equiv 21 \pmod{23},$$

sier (B) at $\mathbb{L}^{12673}_{23} = \mathbb{L}^{21}_{23}$.

21 er ikke et primtall

Husk: hver gang vi får et nytt Legendresymbol, sjekk først om vi kan benytte (C), (D), (E), eller (F). Det kan vi ikke gjøre her. Sjekk så om vi har et primtall. Det har vi ikke her: 21 er ikke et primtall.

Da finner vi en primtallsfaktorisering til 21 og benytter (A). Vi får:

$$\mathbb{L}^{21}_{23} = \mathbb{L}^{3}_{23} \cdot \mathbb{L}^{7}_{23}.$$

Nå regner vi ut $\mathbb{L}^{3}_{23}$ og $\mathbb{L}^{7}_{23}$ hvert for seg.

Hvordan regne ut $\mathbb{L}^{3}_{23}$?

Siden vi har et primtall øverst, benytter vi (G). Både 3 og 23 er kongruent til 3 modulo 4. Da sier (G) at $\mathbb{L}^{3}_{23} = -\mathbb{L}^{23}_{3}$.

Som alltid etter å ha benyttet (G), benytter vi da (B). Siden

$$23 \equiv 2 \pmod 3,$$

sier (B) at $\mathbb{L}_3^{23} = \mathbb{L}_3^2$.

Siden

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

sier (F) at $\mathbb{L}_3^2 = -1$. Dermed har vi:

$$\mathbb{L}_{23}^3 = -\mathbb{L}_3^{23} = -\mathbb{L}_3^2 = -(-1) = 1.$$

Hvordan regne ut $\mathbb{L}_{23}^7$?

Siden vi har et primtall øverst, benytter vi (G). Både 7 og 23 er kongruent til 3 modulo 4. Da sier (G) at $\mathbb{L}_{23}^7 = -\mathbb{L}_7^{23}$.

Som alltid etter å ha benyttet (G), benytter vi da (B). Siden

$$23 \equiv 2 \pmod 7,$$

sier (B) at $\mathbb{L}_7^{23} = \mathbb{L}_7^2$.

Siden

$$7 \equiv 7 \pmod 8,$$

sier (F) at $\mathbb{L}_7^2 = 1$. Dermed har vi:

$$\mathbb{L}_{23}^7 = -\mathbb{L}_7^{23} = -\mathbb{L}_7^2 = -1.$$

Nå kan vi fullføre utregningen av $\mathbb{L}_{12763}^{23}$

Vi har sett:

$$\begin{aligned}
\mathbb{L}_{12763}^{23} &= -\mathbb{L}_{23}^{12763} \\
&= -\mathbb{L}_{23}^{21} \\
&= -\mathbb{L}_{23}^{3} \cdot \mathbb{L}_{23}^{7} \\
&= -1 \cdot (-1) \\
&= 1.
\end{aligned}$$

Nå knytter vi alt sammen

Vi har sett:

$$\begin{aligned}
\mathbb{L}_{12763}^{11799} &= \mathbb{L}_{12763}^{3^3} \cdot \mathbb{L}_{12763}^{19} \cdot \mathbb{L}_{12763}^{23} \\
&= \mathbb{L}_{12673}^{3^2} \cdot \mathbb{L}_{12763}^{3} \cdot \mathbb{L}_{12763}^{19} \cdot \mathbb{L}_{12763}^{23} \\
&= 1 \cdot (-1) \cdot 1 \cdot 1 \\
&= -1.
\end{aligned}$$

Konklusjon

Siden $\mathbb{L}_{12763}^{11799} = -1$, konkluderer vi at 11799 ikke er en kvadratisk rest modulo 12763.

Oppsummering

For å regne ut Legendresymboler, gjør vi følgende.

(1) Hvis vi ikke har et primtall øverst, finn en primtallsfaktorisering til det, og benytt da (A). Regn ut de nye Legendresymbolene vi får hvert for seg.

(2) Hvis vi har et primtall øverst, benytt (G) og deretter (B).

(3) Hver gang vi får et nytt Legendresymbol, sjekk om vi kan benytte (C), (D), (E), (F). Hvis vi kan: gjør det! Gjennomfør ellers (1) eller (2).

Øv deg, øv deg, og øv deg igjen på å regne ut Legendresymboler, og du blir snart fortrolig med metoden!