Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA1301 Tallteori
Høst 2020

Løsningsforslag — Øving 12

9.1.4 Vi bruker Eulers kriterium, og ser at:

$$3^{\frac{23-1}{2}} \equiv 3^{11} \equiv 3^2 \left(3^3\right)^3 \equiv 9 \cdot 27^3 \equiv 9 \cdot 4^3 \equiv 1 \pmod{23}$$
$$3^{\frac{31-1}{2}} \equiv 3^{15} \equiv \left(3^3\right)^5 \equiv (-4)^5 \equiv -1024 \equiv -1 \pmod{31}$$

Så 3 er en kvadratisk rest modulo 23, men ikke modulo 31.

9.2.1a) Vi bruker de ulike egenskapene i teorem 9.2. Siden $9 \equiv -4 \pmod{23}$, får vi at:

$$\begin{aligned}(19/23) = (-4/23) \equiv (-4)^{\frac{23-1}{2}} &\equiv (-1)^{11} \cdot 4^{11} \equiv -4^2 \cdot \left(4^3\right)^3 \equiv -16 \cdot 64^3 \\ &\equiv -16 \cdot (-5)^3 \equiv (-16) \cdot (-125) \equiv 2000 \equiv -1 \pmod{23}\end{aligned}$$

Siden $(19/23)$ må være lik ± 1, betyr dette at $(19/23) = -1$. Følgelig er 19 ikke en kvadratisk rest modulo 23.

9.2.2a) Vi skal finne Legendresymbolet $(a/p) = (8/11)$ ved hjelp av Gauss' lemma. Vi finner først mengden S:

$$S = \{a, 2a, \ldots, \left(\frac{p-1}{2}\right) a\} = \{8, 16, 24, 32, 40\}$$

Resten modulo 40 til hver av disse er hhv. $8, 5, 2, 10$ og 7. Det er 3 av disse som er større enn $11/2 = 5,5$. Altså er $n = 3$ og $(8/11) = (-1)^3 = -1$.

9.2.3 Vi skal vise at for et odde primtall p er det $\frac{p-1}{2} - \phi(p-1)$ kvadratiske ikkerester modulo p som ikke er primitive røtter til p. Fra kapittel 8 vet vi at antallet primitive røtter til p er $\phi(\phi(p)) = \phi(p-1)$. Fra teorem 9.4 vet vi at antallet kvadratiske ikkerøtter modulo p er $\frac{p-1}{2}$. Med andre ord holder det å vise at alle primitive røtter til p er kvadratiske ikkerester modulo p, siden det vil bety at antallet kvadratiske ikkerester som ikke er primitive røtter er lik $\frac{p-1}{2} - \phi(p-1)$.

Det å vise at alle primitive røtter til p er kvadratiske ikkerester modulo p er ekvivalent med å vise at ingen kvadratisk rest modulo p er en primitiv rot til p. Anta nå at a er en kvadratisk rest modulo p. Da gir Eulers kriterium at $a^{\frac{p-1}{2}} \equiv 1 \mod p$. Altså er ordenen til a modulo p mindre enn eller lik $\frac{p-1}{2}$, som er strengt mindre enn $\phi(p) = p-1$. Det betyr at a ikke kan være en primitiv rot, og følgelig at alle primitive røtter til p må være kvadratiske ikkerester modulo p.

Dermed blir antallet kvadratiske ikkerester modulo p som ikke er primitive røtter til p lik antallet kvadratiske ikkerester modulo p, minus antallet primitive røtter til p. Altså $\frac{p-1}{2} - \phi(p-1)$.

9.3.2 Vi bruker teorem 9.10. Fra hintet har vi at $4^n \equiv 4 \pmod{12}$ for alle n. Med litt omskriving får vi at

$$2^{2^n} + 1 \equiv (2^2)^n + 1 \equiv 4^n + 1 \equiv 4 + 1 \equiv 5 \pmod{12}$$
$$2^p - 1 \equiv 2 \cdot 2^{p-1} - 1 \equiv 2 \cdot (2^2)^{\frac{p-1}{2}} - 1 \equiv 2 \cdot 4^{\frac{p-1}{2}} - 1 \equiv 2 \cdot 4 - 1 \equiv -5 \pmod{12}$$

Dermed gir teorem 9.10 at $(3/p) = -1$ for alle primtall som er på en av de gitte formene. Altså er 3 en kvadratiskt ikkerest for alle slike primtall.

9.3.3a) Den kvadratiske kongruensen $x^2 \equiv 219 \pmod{419}$ er løsbar hvis og bare hvis219 er en kvadratisk rest modulo 419 (merk at 419 er et primtall). Vi regner ut Legendre-symbolet $(219/419)$:

$$(219/419) = (3 \cdot 73/419) = (3/419) \cdot (73/419)$$

Vi vil nå bruke teorem 9.10, så vi regner ut $419 \pmod{12}$:

$$419 \equiv 420 - 1 \equiv 35 \cdot 12 - 1 \equiv -1 \pmod{12}$$

Dermed gir teorem 9.10 at $(3/419) = 1$.

Siden 73 og 419 er to ulike odde primtall, gir loven om kvadratisk resiprositet at

$$(73/419) \cdot (419/73) = (-1)^{\frac{72}{2}\frac{418}{2}} = (-1)^{36 \cdot 209} = \left((-1)^2\right)^{18 \cdot 209} = 1.$$

Vi ser at $419 = 54 + 5 \cdot 73$, så

$$(419/73) = (54/73) = (6 \cdot 9/73) = (2/73) \cdot (3/73) \cdot (3^2/73)$$

. Teorem 9.6 gir at $(2/73) = 1$, teorem 9.10 gir at $(3/73) = 1$, og teorem $9.2(e)$ gir at $(3^2/73) = 1$. Altså er $(419/73) = 1$, som fra utregningen over gir at $(73/419) = 1$. Altså er $(219/419) = 1$, som betyr at kongruensen er løsbar.

Eksamen H2011 oppgave 9 Vi skal avgjøre om kongruensen $x^2 + 4x \equiv 30 \pmod{31}$ er løsbar. Vi fullfører kvadratet på venstre side ved å legge til 4 på begge sider av kongruensen:

$$(x + 2)^2 \equiv x^2 + 4x + 4 \equiv 30 + 4 \equiv 3 \pmod{31}$$

Denne kongruensen er løsbar hvis og bare hvis Legendresymbolet $(3/31) = 1$. Fra loven om kvadratisk resiprositet får vi at $(3/31)(31/3) = (-1)^{\frac{3-1}{2}\frac{31-1}{2}} = (-1)^{15} = -1$. Det følger at

$$(3/31) = -(31/3) = -(1/3) = -1$$

hvor vi har brukt at $31 \equiv 1 \pmod{3}$ og at $(1/3) = 1$ (1 er en kvadratisk rest til 3). Siden Legendresymbolet $(3/31) = -1 \neq 1$ konkluderer vi med at kongruensen ikke er løsbar.

Denne oppgaven kunne også vært løst uten å bruke kvadratisk resiprositet, men heller bruke Eulers kriterium. Da finner man at $3^{(31-1)/2} \equiv -1 \pmod{31}$, som gir samme konklusjon.

Eksamen H2018 oppgave 5 For å finne ut om kongruensen har noen løsninger ser vi på Legendresymbolet $(43/19)$. Siden $43 \equiv 5 \pmod{19}$ gir regnereglene at

$$(43/19) \equiv (5/19) \equiv 5^{\frac{19-1}{2}} \equiv 5^9 \equiv 1953125 \equiv 1 \pmod{19}$$

Siden verdien av et Legendresymbol må være lik ± 1, betyr det at $(43/19) = 1$. Derfor er kongruensen $x^2 \equiv 43 \pmod{19}$ løsbar.

For å finne ut om den 'motsatte" kongruensen, dvs. $x^2 \equiv 19 \pmod{43}$, er løsbar, bruker vi loven om kvadratisk resiprositet:

$$(43/19)(19/43) = (-1)^{\frac{43-1}{2}\frac{19-1}{2}} = (-1)^{21 \cdot 9} = -1$$

Siden $(43/19) = 1$, betyr det at $(19/43)$ må være lik -1. Følgelig er kongruensen $x^2 \equiv 19 \pmod{43}$ ikke løsbar.