9.3 Kvadratisk resiprositet

Fra tidligere: (1) Ønsker å avgjøre om $x^2 \equiv a \pmod p$ er løsbar, hvor p er odde prim og ptа. Hvis ja så er a en kvadratisk rest av p.

(2) Eulers kriterium:

a kv. rest av $p \iff a^{\frac{p-1}{2}} \equiv 1 \pmod p$

a ikke kv. rest av $p \iff a^{\frac{p-1}{2}} \equiv -1 \pmod p$

(3) Legendresymbolet:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{hvis ja, altså hvis } x^2 \equiv a \pmod p \text{ løsbar} \\ -1 & \text{hvis nei} \end{cases}$$

(4)
* $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$
* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
* $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$, $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Lemma

$$\left(\frac{a}{p}\right) = (-1)^m \quad \text{hvor} \quad m = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] = \left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + \cdots + \left[\frac{\frac{p-1}{2}a}{p}\right]$$

Merk: $[x]$ er heltallsdelen av et reelt tall. F.eks er $[\pi] = 3$ og $[5{,}89] = 5$.

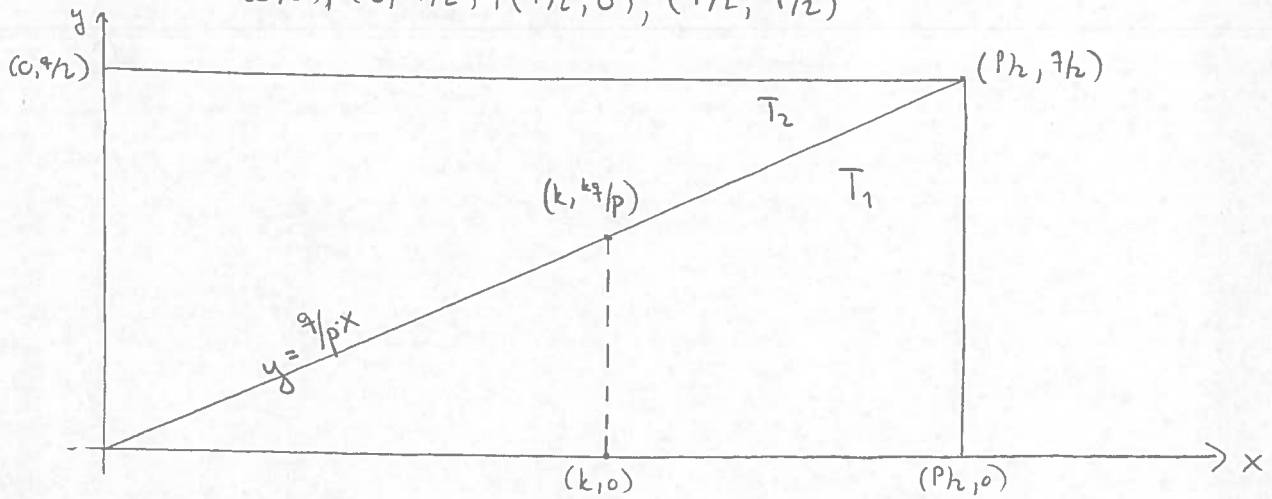
Teorem 9.9 (Kvadratisk resiprositet)

Hvis p og q er ulike odde primtall så er

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

Bevis: Se på den rektangulære boksen i xy-planet med hjørner

$$(0,0),\ (0, q/2),\ (p/2, 0),\ (p/2, q/2)$$



La R betegne området inne i boksen, ikke medregnet sidekantene. Da vil

$$\{(m,n) \mid 1 \le m \le \tfrac{p-1}{2},\ 1 \le n \le \tfrac{q-1}{2}\}$$

være alle heltallspunktene i R, og antall slike punkter er

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

Se på diagonalen D gitt ved $y = {}^{q}/_{p} \cdot x$. Det deler R i to regioner, T_1 og T_2. Ligger det noen heltallspunkter på D? Hvis ja, så finnes to heltall m, n med $n = \frac{qm}{p}$, dvs $pn = qm$. Siden $p \mid qm$ og $p \neq q$ må da $p \mid m$. Umulig hvis $1 \leq m \leq \frac{p-1}{2}$. Så diagonalen D inneh. ingen heltallspunkter.

Hvor mange heltallspkter ligger i T_1? For $1 \leq k \leq \frac{p-1}{2}$, se på linjestykket fra $(k,0)$ opp til D, dvs til pktet $(k, {}^{kq}/_{p})$. På dette linjestykket er

$$(k,1), (k,2), \ldots, (k, [{}^{kq}/_{p}])$$

heltallspktene som ligger i T_1 (husk at $(k,0)$ ikke ligger i T_1). Det er $[{}^{kq}/_{p}]$ slike punkter, så antallet totalt i T_1 er

$$m_1 = \sum_{k=1}^{\frac{p-1}{2}} [{}^{kq}/_{p}]$$

Situasjonen for T_2 er symmetrisk: antall heltallspkter er her

$$m_2 = \sum_{k=1}^{\frac{q-1}{2}} [{}^{kp}/_{q}]$$

Siden det er $\frac{p-1}{2} \cdot \frac{q-1}{2}$ heltallspkter i R får vi

$$\tfrac{p-1}{2} \cdot \tfrac{q-1}{2} = m_1 + m_2$$

Fra lemmaet har vi at $({}^{q}/_{p}) = (-1)^{m_1}$ og $({}^{p}/_{q}) = (-1)^{m_2}$, så

$$({}^{q}/_{p})({}^{p}/_{q}) = (-1)^{m_1+m_2} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$ □

Merk: Teoremet sier altså at løsbarheten av $x^2 \equiv p \pmod{q}$ er sterkt knyttet til løsbarheten av $x^2 \equiv q \pmod{p}$.

Eksempler: (1) Hva er $(5/11)$? Se på $(11/5)$ først. Siden $11 \equiv 1 \pmod 5$ er $(11/5) = (1/5) = 1$. Her nå

$$(5/11)(11/5) = (-1)^{\frac{5-1}{2} \cdot \frac{11-1}{2}} = 1$$

og siden $(11/5) = 1$ må da $(5/11) = 1$. Altså er 5 en kv. rest av 11, dvs $x^2 \equiv 5 \pmod{11}$ er løsbar ($x_1 = 4$ og $x_2 = 11 - 4 = 7$ er løsningene).

(2) Eksamen H2012, oppg 7.

Er $x^2 \equiv 311 \pmod{19}$ løsbar? Bruk dette til å avgjøre om $x^2 \equiv 19 \pmod{311}$ er løsbar.

Siden $311 \equiv 7 \pmod{19}$ er $x^2 \equiv 311 \pmod{19}$ ekv. med $x^2 \equiv 7 \pmod{19}$. Denne er løsbar $\Leftrightarrow 7^{\frac{19-1}{2}} \equiv 1 \pmod{19}$, dvs $7^9 \equiv 1 \pmod{19}$. Har $7^2 \equiv 49 \equiv 11 \pmod{19}$, så $7^3 \equiv 7 \cdot 11 \equiv 77 \equiv 1 \pmod{19}$, som gir $7^9 \equiv (7^3)^3 \equiv 1 \pmod{19}$. Derfor er $x^2 \equiv 7 \pmod{19}$ løsbar (med løsninger $x_1 = 8$ og $x_2 = 19 - 8 = 11$). Så $x^2 \equiv 311 \pmod{19}$ er løsbar.

Har nå at $(311/19) = 1$. Siden 311 og 19 er primtall (og odde) vil

$$(311/19)(19/311) = (-1)^{\frac{311-1}{2} \cdot \frac{19-1}{2}} = (-1)^{155 \cdot 9} = -1$$

og da må $(19/311) = -1$ fordi $(311/19) = 1$. Så $x^2 \equiv 19 \pmod{311}$ er ikke løsbar.