Talteori, Föreläsning 6

Kvadratiska residyer, kvadratisk reciprocitet

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

Föreläsningsanteckningar på kurshemsidan `http://courses.mai.liu.se/GU/TATA54/`

Sammanfattning

Kvadratiska modulära ekvationer
- Kvadratiska ekvationer modulo ett primtal

Kvadratiska residyer

Legendresymbol
- Eulerkriterium
- Gauss lemma

Kvadratisk reciprocitet
- Eulers förmodan/sats
- Bevis av kvadratisk reciprocitet
- Andra bevise av kvadratisk reciprocitet
- Tillämpningar

Kvadratiska modulära ekvationer

- N heltal
- $f(x) = Ax^2 + Bx + C$
- Vill lösa $f(x) \equiv 0 \mod N$
- Restsatsen: om $N = mn$, $\gcd(m, n) = 1$, $f(a) \equiv 0 \mod m$, $f(b) \equiv 0 \mod n$, så finns unikt c ($\mod mn$) med $c \equiv a \mod m$, $c \equiv b \mod n$, och alltså $f(c) \equiv 0 \mod m$, $f(c) \equiv 0 \mod n$, så $f(c) \equiv 0 \mod N$
- Hensel-lyft: antag $f(a) \equiv 0 \mod p$. Då $f'(a) \equiv 2Aa + B \mod p$. Om nollskild, så lyfter a unikt till rot mod p^r.

Kvadratiska ekvationer modulo ett primtal

- p primtal
- $f(x) = Ax^2 + Bx + C$,
- $p \nmid A$
-

$$
\begin{aligned}
Ax^2 + Bx + C &\equiv 0 \mod p \\
x^2 + A^{-1}Bx + A^{-1}C &\equiv 0 \mod p \\
x^2 + Dx + F &\equiv 0 \mod p \\
x^2 + 2Ex + F &\equiv 0 \mod p \\
(x + E)^2 &\equiv E^2 - F \mod p \\
t^2 &\equiv u \mod p
\end{aligned}
$$

Definition

- p primtal
- $p \nmid u$
- u är en kvadratisk residy modulo p om

$$x^2 \equiv u \mod p$$

är lösbar, kvadratisk icke-residy annars

Exempel

$p = 5$, kvadrera:

x	0	1	2	3	4
x^2	0	1	4	4	1

1,4 k.r, 2,3 k.i.r, 0 kvadrat men ej k.r.

Hädanefter så är p ett udda primtal.

Lemma

Antag $\langle g \rangle = \mathbb{Z}_p^*$. Då är $u = g^s$ en k.r. omm s är jämn. Alltså är precis hälften av elementen i $\mathbb{Z}_p^*$ k.r, hälften k.i.r.

Bevis.

Låt $x = g^t$. Då $x^2 = u \in \mathbb{Z}_p^*$ omm $2t \equiv s \mod p-1$. Om s jämn, lösbart, annars ej. □

Vi ser vidare (Laplace) att när u är k.r, så har $x^2 \equiv u \mod p$ två lösningar , $a, -a$.

Definition

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ k.r.} \mod p \\ -1 & a \text{ i.k.r.} \mod p \\ 0 & a \equiv 0 \mod p \end{cases}$$

Vanligen så är $a \not\equiv 0 \mod p$. p fortfarande ett udda primtal!

Lemma

Låt $\langle g \rangle = \mathbb{Z}_p^*$. *Då*

$$\left(\frac{g^s}{p}\right) = (-1)^s$$

Bevis.

g^s k.r. omm s jämnt. □

Teorem

p udda primtal, $a, b \not\equiv 0 \mod p$. *Då*

- $\left(\frac{1}{p}\right) = 1$
- $\left(\frac{a^2}{p}\right) = 1$
- *Om* $a \equiv b \mod p$ *så* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Bevis.

Låt $\langle g \rangle = \mathbb{Z}_p^*$, $a = g^s$, $b = g^t$. Eftersom $\left(\frac{a}{p}\right) = (-1)^s$, $\left(\frac{b}{p}\right) = (-1)^t$, så gäller att

$$\left(\frac{ab}{p}\right) = (-1)^{s+t} = (-1)^s(-1)^t = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

□

Teorem (Eulerkriterium)

p udda primtal, $P = (p-1)/2$, $a \not\equiv 0 \mod p$. Då

$$a^P \equiv \left(\frac{a}{p}\right) \mod p$$

Bevis.

Enligt Fermat, $a^{p-1} \equiv 1 \mod p$, så

$$0 \equiv a^{2P} - 1 \equiv (a^P + 1)(a^P - 1) \mod p$$

varför $a^P \equiv 1 \mod p$ eller $a^P \equiv -1 \mod p$.
Låt g vara en primitiv rot, $a = g^s$, $a^P = g^{sP}$.

1. Om s jämn, så $p-1 | sP$, så $g^{sP} \equiv 1 \mod p$
2. Om s udda, så $p-1 \not| s\frac{p-1}{2}$, så $g^{sP} \not\equiv 1 \mod p$

□

När är -1 k.r.?

Teorem

$$\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) \equiv (-1)^P \mod p \equiv \begin{cases} +1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$$

Bevis.

Eulerkrieriet och $P = (4k+1-1)/2$ eller $P = (4k+3-1)/2$. □

Lemma (Gauss)

- p, P, a *som tidigare*
- $S = \{a, 2a, 3a, \ldots, Pa\}$
- *För* $s \in S$, *finns unikt* $t \in (-p/2, p/2) \cap \mathbb{Z}$ *med* $s \equiv t \mod p$
- v *antal negativa representanter*
- *Då:* $\left(\frac{a}{p}\right) = (-1)^v$.

Exempel

$p = 7, P = 3, a = 3$. $S = \{3, 6, 9\} \equiv \{3, -1, 2\} \subseteq (-7/2, 7/2)$. $v = 1$, $\left(\frac{3}{7}\right) = -1$.

Bevis.

Uppenbarligen så $ia \not\equiv ja \mod p$ för $i \neq j$.
Vidare: $ia \not\equiv -ja \mod p$, ty annars: $0 \equiv ia + ja \equiv (i+j)a \mod p$, så $i + j \equiv 0 \mod p$, omöjligt eftersom $1 \leq i, j \leq (p-1)/2$.
Så $ia \equiv \varepsilon(i)\sigma(i) \mod p$, $\varepsilon(i) \in \{-1, 1\}$, $\sigma : \{1, 2, \ldots, P\} \to \{1, 2, \ldots, P\}$ permutation.

$$\prod_{i=1}^{P} ia \equiv \prod_{i=1}^{P} \varepsilon(i)\sigma(i) \mod p$$

Stryk $P!$, och erhåll

$$a^P \equiv \prod_{i=1}^{P} \varepsilon(i) = (-1)^v \mod p.$$

□

Teorem

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases}$$

Bevis

Gauss lemma: reducera $S = \{2, 4, 6, \ldots, 2P = p - 1\}$ till $(-p/2, p/2)$, hur många negativa representanter? Räkna $S \cap (p/2, p)$.

$$p/2 < 2x < p \quad \Longleftrightarrow \quad p/4 < x < p/2, \qquad x \in \mathbb{Z}$$

Sätt $p = 8k + r$, $r \in \{1, 3, 5, 7\}$.

$$2k + r/4 < x < 4k + r/2, \quad x \in \mathbb{Z}$$

$2k$ och $4k$ jämna heltal, så pariteten av antal heltal x ändras inte om vi istället betraktar

$$r/4 < x < r/2.$$

Bevis.

- $r = 1$:

$$1/4 < x < 1/2, \quad x \in \mathbb{Z}$$

inga lösningar

- $r = 3$:

$$3/4 < x < 3/2, \quad x \in \mathbb{Z}$$

1 lösning, $x = 1$

- $r = 5$:

$$5/4 < x < 5/2, \quad x \in \mathbb{Z}$$

1 lösning, $x = 2$

- $r = 7$:

$$7/4 < x < 7/2, \quad x \in \mathbb{Z}$$

2 lösningar, $x = 2, 3$

So jämnt antal lösningar om $r = 1$ eller $r = 7$. □

Exempel

- $p = 11,\ P = 5$
- $S = \{2, 4, 6, 8, 10\} \equiv \{2, 4, -5, -3, -1\}$
- $v = 3,\ \left(\frac{2}{11}\right) = -1$
- $r = 3,$
- Heltalslösningar till

$$11/2 < x < 11$$
$$\frac{8 * 1 + 3}{2} < 2x < 8 * 1 + 3$$
$$\frac{8 * 1 + 3}{4} < x < \frac{8 * 1 + 3}{2}$$
$$2 + \frac{3}{4} < x < 4 + \frac{3}{2}$$

är $x = 3, 4, 5$

- Heltalslösningar till

$$\frac{3}{4} < x < \frac{3}{2}$$

är $x = 1$.

Teorem

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \mod 12 \\ -1 & p \equiv \pm 3 \mod 12 \end{cases}$$

Teorem

$$\left(\frac{p-3}{p}\right) = \left(\frac{-3}{p}\right) = \begin{cases} +1 & p \equiv 1 \mod 6 \\ -1 & p \equiv -1 \mod 6 \end{cases}$$

Bevis.

Gauss lemma, eller använd kvadratisk reciprocitet så snart vi lärt oss det! □

Teorem (Kvadratisk reciprocitet)

Låt p, q vara två olika udda primtal. Då gäller att

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

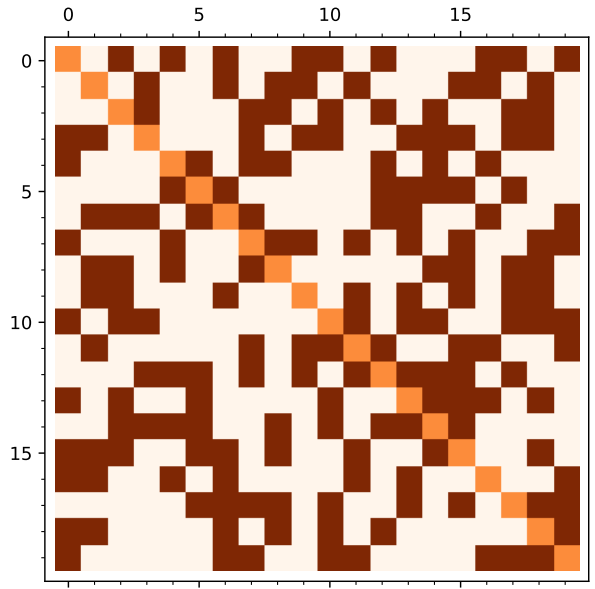
Med andra ord så är

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

om inte

$$p \equiv q \equiv -1 \mod 4$$

Bild av $\left(\frac{p_i}{p_j}\right)$, p_i i:e udda primtalet. Någorlunda symmetriskt!



Teorem (Euler)

- p_1, p_2, p_3 *udda primtal,*
- a *heltal* $p_i \nmid a$
- $p_i = 4ak_i + r_i$, $0 < r_i < 4a$
- $r_2 = r_1$
- $r_3 = 4a - r_1$

Då:

- $\left(\frac{a}{p_2}\right) = \left(\frac{a}{p_1}\right)$
- $\left(\frac{a}{p_3}\right) = \left(\frac{a}{p_1}\right)$

Exempel

- $\left(\frac{5}{23}\right) = \left(\frac{5}{43}\right)$, $4a = 20$, $r = 3$
- $\left(\frac{8}{37}\right) = \left(\frac{8}{59}\right)$, $4a = 32$, $r = 4$, $4a - 5 = 27$

Bevis I

- p udda primtal
- $P = (p-1)/2$
- $S = \{a, 2a, \ldots, Pa\}$
- Reducera till $(-p/2, p/2)$, v antal negativa
- Sätt $b = a/2$ om a jämn eller $b = (a-1)/2$ om a udda
- v är antal heltal S och samtidigt i

$$(\frac{1}{2}p, p) \cup (\frac{3}{2}p, 2p) \cup \cdots \cup ((b - \frac{1}{2})p, bp)$$

- Inga ändpunkter heltal, ingen överlappning, lätt räkning
- Vill ha

$$xa \in (\frac{1}{2}p, p) \cup (\frac{3}{2}p, 2p) \cup \cdots \cup ((b - \frac{1}{2})p, bp)$$

Bevis II

- Ekvivalent: heltal x ligger i

$$\bigcup_{\ell=1}^{P}\left(\frac{2\ell-1}{2a}p, \frac{\ell}{a}p\right)$$

- Byt p mot $4ak+r$, får

$$\bigcup_{\ell=1}^{P}\left((2\ell-1)2k+\frac{2\ell-1}{2a}r, 4\ell k+\frac{\ell}{a}r\right)$$

- Annat k, samma r: så v-na skiljer sig med ett jämnt heltal, samma $\left(\frac{a}{p}\right)$
- Speciellt, kan byta ut mot r, får: räknar antal heltal i

$$\bigcup_{\ell=1}^{P}\left(\frac{2\ell-1}{2a}r, \frac{\ell}{a}r\right)$$

Bevis III

- Andra delen av beviset: samma ide, lite knepigare
- Lämnas därför som övning!

Vi formulerar Eulerförmodan lite enklare:

Teorem (Euler)

Låt p, q vara udda primtal, och a ett heltal så att $p \nmid a$. Om $q \equiv \pm p \mod 4a$ så $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Vi påminner om

Lemma

Om $a \equiv b \mod p$ så $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Det gäller alltid att $\left(\frac{a^2}{p}\right) = 1$. Speciellt så $\left(\frac{4}{p}\right) = 1$.

Teorem (Kvadratisk reciprocitet)

Låt p, q vara två olika udda primtal. Då gäller att

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

Med andra ord så är

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

om inte

$$p \equiv q \equiv -1 \mod 4$$

Bevis då $p \equiv q \mod 4$

Studera först fallet $p \equiv q \mod 4$. Kan anta att $p > q$. Skriv $p - q = 4a$, så $p = 4a + q$.
Har då

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{4}{q}\right)\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right)$$

och

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$$

Eulerförmodan ger att $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$, eftersom $p \equiv q \mod 4$. Vidare så är $(p-1)/2$ jämn omm $(q-1)/2$ jämn.

Bevis då $p \equiv q \mod 4$, fortsättning

Vi ser att

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

Bevis då $p \not\equiv q \mod 4$

Om istället $p \not\equiv q \mod 4$ så gäller att $p \equiv -q \mod 4a$. Skriv $p + q = 4a$. Då gäller

$$\left(\frac{p}{q}\right) = \left(\frac{4a - q}{q}\right) = \left(\frac{a}{q}\right),$$

och

$$\left(\frac{q}{p}\right) = \left(\frac{4a - p}{p}\right) = \left(\frac{a}{p}\right).$$

Eulerförmodan ger, då $p \equiv -q \mod 4a$, att

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Eftersom

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

i detta fall, är vi klara.

Lemma (Eisenstein)

Låt p, q vara udda primtal, $p \neq q$. Då är

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{t=1}^{(p-1)/2} \lfloor \frac{2tq}{p} \rfloor}$$

Bevis.

1. Sätt $u = 2t$, så $u \in \left\{2, 4, 6, \ldots, \frac{p-1}{2}\right\} = J$
2. $r(u)$ minsta positiva rest av qu mod p
3. Eftersom p udda, så $[-\text{odd}]_p = [\text{even}]_p$
4. $(-1)^{r(u)} r(u)$ är
   - **4.1** jämna (enl föregående)
   - **4.2** distinkta, ty om $(-1)^{r(u)} r(u) \equiv (-1)^{r(v)} r(v) \mod p$ så $(-1)^{qu+np}(qu+np) \equiv (-1)^{qv+mp}(qv+mp) \mod p$ så $u \equiv \pm v \mod p$. Men u, v båda jämna, så $u \equiv v \mod p$.
   - **4.3** hela J, ty J har $(p-1)/2$ element.

□

forts.

5. Multiplicera alla, får

$$\prod_{t=1}^{(p-1)/2} (-1)^{r(2t)} 2tq \equiv \prod_{t=1}^{(p-1)/2} 2t \mod p$$

6. Kancellera:

$$\prod_{t=1}^{(p-1)/2} (-1)^{r(2t)} \prod_{t=1}^{(p-1)/2} q \equiv 1 \mod p$$

dvs

$$q^{(p-1)/2} \equiv (-1)^{\left(\sum_{t=1}^{(p-1)/2} r(2t)\right)} \mod p$$

□

Bevis.

7.

$$\frac{qu}{p} = \left\lfloor \frac{qu}{p} \right\rfloor + \frac{r(u)}{p} \qquad \Longrightarrow \qquad qu = p \left\lfloor \frac{qu}{p} \right\rfloor + r(u)$$

8. Så $\left\lfloor \frac{qu}{p} \right\rfloor \equiv r(u) \mod 2$

9. Så

$$q^{(p-1)/2} \equiv (-1)^{\left(\sum_{t=1}^{(p-1)/2} r(2t)\right)} \equiv (-1)^{\left(\sum_{t=1}^{(p-1)/2} \left\lfloor \frac{2tq}{p} \right\rfloor\right)} \mod p$$

10. Men $\left(\frac{q}{p}\right) \equiv q^{(p-1)/2} \mod p$.

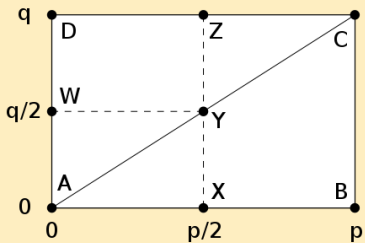
□

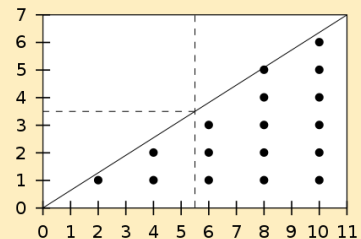
Kvadratisk reciprocitet.

1.

$$\sum_{t=1}^{(p-1)/2} \left\lfloor \frac{2tq}{p} \right\rfloor$$

räknar gitterpunkter med jämn x-koordinat i det inre av triangeln ABC nedan:

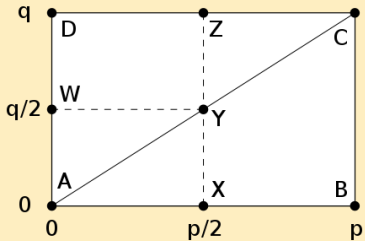


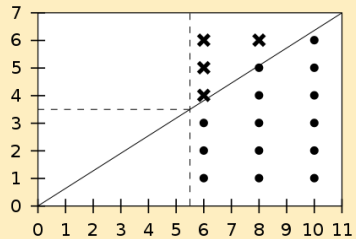


□

Kvadratisk reciprocitet, forts.

2. Varje kolumn (i det inre av rektangeln) har $q - 1$ punkter, jämnt antal
3. Inga punkter på diagonalen!
4. Samma antal punkter mod 2 i BCYX som i CZY

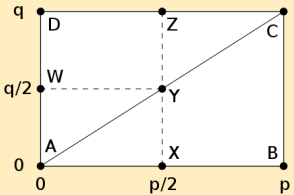


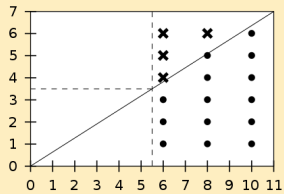


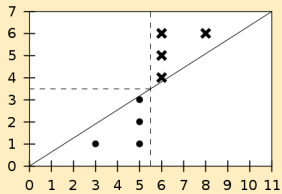
□

Kvadratisk reciprocitet, forts.

5. Spegla bilden i linjen $x = y$, ser att antal punkter med jämn x-koordinat inuti CZY är samma som antalet punkter med udda x-koordinat i AXY







6. Direkt bevis:

$$q - 1 - \left\lfloor \frac{2tq}{p} \right\rfloor = \left\lfloor \frac{(p-2t)q}{p} \right\rfloor$$

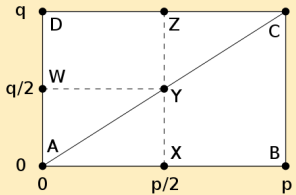
□

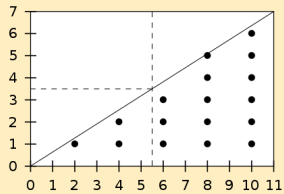
Kvadratisk reciprocitet, forts.

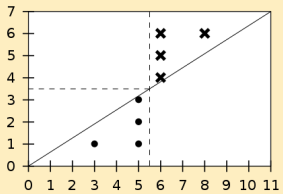
7. Får att

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{t=1}^{(p-1)/2} \left\lfloor \frac{2tq}{p} \right\rfloor} = (-1)^M$$

där M är antalet gitterpunkter i det inre av triangeln AXY.





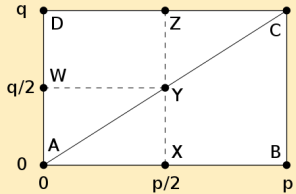


8. Byt plats på p, q, får att $\left(\frac{p}{q}\right) = (-1)^N$ där N är antalet gitterpunkter i det inre av triangeln WYA

□

Kvadratisk reciprocitet, forts.

9. Återigen: inga inre punkter på diagonalen



10. Antalet inre punkter i rektangeln WYXA är $(p-1)(q-1)/4$

11. Så $(p-1)(q-1)/4 = M + N$

12. Så $(-1)^{(p-1)(q-1)/4} = (-1)^{M+N} = (-1)^M(-1)^n$

13. Så $(-1)^{(p-1)(q-1)/4} = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$

□

Exempel (Beräkning av Legendresymbol)

$$\left(\frac{1234}{17}\right) = \left(\frac{72 * 17 + 10}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{5}{17}\right) =$$

$$1 * \left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1$$

Exempel

p udda primtal, n heltal ej delbart med p. Vill lösa Diofantiska ekvationen

$$x^2 - ny^2 = p$$

Om $p|y$ så $p|x$ så $p^2|x^2$, p.s.s. $p^2|y^2$, så $p^2|VL$, så $p^2|HL$, motsägelse. Alltså kan vi anta att att p inte delar y.
Mod p:

$$x^2 \equiv ny^2 \mod p$$

så (eftersom vi kan dela med y)

$$n \equiv \left(\frac{x}{y}\right)^2 \mod p$$

varför måste ha $\left(\frac{n}{p}\right) = 1$.

Exempel (forts)

Om $\left(\frac{n}{p}\right) = 1$ så

$$n \equiv t^2 \mod p$$

något t, och ekvationen

$$\frac{x}{y} \equiv t \mod p$$

har $p-1$ lösningar, sätt y till vad som helst utom noll.
Exempel: $n = 85 = 5 * 17$, så

$$\left(\frac{n}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{p}{5}\right)\left(\frac{p}{17}\right)$$

så ekvation lösbar omm antingen

- $\left(\frac{p}{5}\right) = \left(\frac{p}{17}\right) = 1$, dvs om $p \equiv \pm 1 \mod 5$ och $p \equiv \pm 1, \pm 2, \pm 4, \pm 8 \mod 17$, eller
- $\left(\frac{p}{5}\right) = \left(\frac{p}{17}\right) = -1$.

Exempel (math.stackexchange)

Låt p, q vara primtal, med $q \equiv 3 \mod 5$, $p = 2q + 1$. Är 5 en primitiv rot mod p?

1. q udda, $p > 2$ så udda
2. $p = 2q + 1 \equiv 2 * 3 + 1 \equiv 7 \equiv 2 \mod 5$
3. $q = (p - 1)/2$
4. $5 \equiv 1 \mod 4$, så kvad. res. m.m. ger $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1$
5. Så 5 k.i.r mod p
6. $p = 2q + 1$, $|\mathbb{Z}_p^*| = p - 1 = 2q$
7. Ordningen av element i $\mathbb{Z}_p^*$ är $1, 2, q$, eller $2q$.
8. $o([5]_p$ ej 1,2 (bara $[\pm 1]_p$ har ordning 2
9. $o([5]_p$ ej q, ty i så fall skulle $5^{(p-1)/2} \equiv 1 \mod p$, men $5^{(p-1)/2} \equiv \left(\frac{5}{p}\right) \equiv -1 \mod p$.
10. Så $o([5]_p = 2q = p - 1 = \phi(p)$ d.v.s. 5 är en primitiv rot mod p.