

# Talteori, Föreläsning 6

## Kvadratiske residyer, kvadratisk reciprocitet

Jan Snellman<sup>1</sup>

<sup>1</sup>Matematiska Institutionen  
Linköpings Universitet

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



**TEKNISKA HÖGSKOLAN**  
LINKÖPINGS UNIVERSITET

## **Kvadratiske modulära ekvationer**

Kvadratiske ekvationer modulo ett  
primtal

## **Kvadratiske residyer**

## **Legendresymbol**

Eulerkriterium

Gauss lemma

## **Kvadratisk reciprocitet**

Eulers förmodan/sats

Bevis av kvadratisk reciprocitet

Tillämpningar

- ▶  $N$  heltal
- ▶  $f(x) = Ax^2 + Bx + C$
- ▶ Vill lösa  $f(x) \equiv 0 \pmod{N}$
- ▶ Restsatsen: om  $N = mn$ ,  $\gcd(m, n) = 1$ ,  $f(a) \equiv 0 \pmod{m}$ ,  $f(b) \equiv 0 \pmod{n}$ , så finns unikt  $c \pmod{mn}$  med  $c \equiv a \pmod{m}$ ,  $c \equiv b \pmod{n}$ , och alltså  $f(c) \equiv 0 \pmod{m}$ ,  $f(c) \equiv 0 \pmod{n}$ , så  $f(c) \equiv 0 \pmod{N}$
- ▶ Hensel-lyft: antag  $f(a) \equiv 0 \pmod{p}$ . Då  $f'(a) \not\equiv 0 \pmod{p}$ . Om nollskild, så lyfter  $a$  unikt till rot mod  $p^r$ .

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

$$Ax^2 + Bx + C \equiv 0 \pmod{p}$$

$$x^2 + A^{-1}Bx + A^{-1}C \equiv 0 \pmod{p}$$

$$x^2 + Dx + F \equiv 0 \pmod{p}$$

$$x^2 + 2Ex + F \equiv 0 \pmod{p}$$

$$(x + E)^2 \equiv E^2 - F \pmod{p}$$

$$t^2 \equiv u \pmod{p}$$

## Definition

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

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

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  $2t \equiv s \pmod{p-1}$ . Om  $s$  jämn, lösbart, annars ej. □

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

### Definition

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

Vanligen så är  $a \not\equiv 0 \text{ mod } p$ .  $p$  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,  $a, b \not\equiv 0 \pmod p$ . Då

►  $\left(\frac{1}{p}\right) = 1$

►  $\left(\frac{a^2}{p}\right) = 1$

► Om  $a \equiv b \pmod p$  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,  $P = (p-1)/2$ ,  $a \not\equiv 0 \pmod{p}$ . Då

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

### Bevis.

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

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

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

Låt  $g$  vara en primitiv rot,  $a = g^s$ ,  $a^P = g^{sP}$ .

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



När är  $-1$  k.r.?

### Teorem

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

### Bevis.

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



## Lemma (Gauss)

- ▶  $p, P, a$  som tidigare
- ▶  $S = \{a, 2a, 3a, \dots, Pa\}$
- ▶ För  $s \in S$ , finns unikt  $t \in (-p/2, p/2) \cap \mathbb{Z}$  med  $s \equiv t \pmod{p}$
- ▶  $v$  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  $ia \not\equiv ja \pmod p$  för  $i \neq j$ .

Vidare:  $ia \not\equiv -ja \pmod p$ , ty annars:  $0 \equiv ia + ja \equiv (i+j)a \pmod p$ , så  $i+j \equiv 0 \pmod p$ , omöjligt eftersom  $1 \leq i, j \leq (p-1)/2$ .

Så  $ia \equiv \varepsilon(i)\sigma(i)a \pmod p$ ,  $\varepsilon(i) \in \{-1, 1\}$ ,  $\sigma: \{1, 2, \dots, P\} \rightarrow \{1, 2, \dots, P\}$  permutation.

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

Stryk  $P!$ , och erhåll

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



## Teorem

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

## Bevis

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

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

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

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

### Teorem

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

### 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*

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

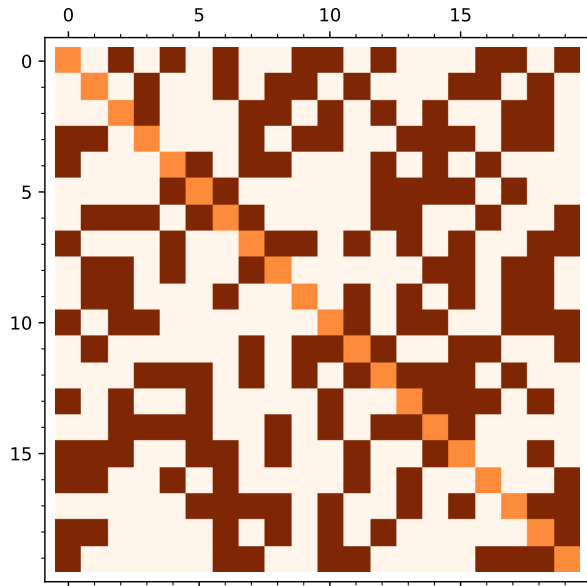
*Med andra ord så är*

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

*om inte*

$$p \equiv q \equiv -1 \pmod{4}$$

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

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

- ▶  $p$  udda primtal
- ▶  $P = (p - 1)/2$
- ▶  $S = \{a, 2a, \dots, Pa\}$
- ▶ 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

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

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

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

- 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

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

- ▶ 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  $q \equiv \pm p \pmod{4a}$  så*  
$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Vi påminner om

### **Lemma**

*Om  $a \equiv b \pmod{p}$  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*

$$p \equiv q \equiv -1 \pmod{4}$$



### Bevis då $p \equiv q \pmod{4}$

Studera först fallet  $p \equiv q \pmod{4}$ . 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

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

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

## Bevis då $p \equiv q \pmod{4}$ , 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 $p \not\equiv q \pmod{4}$

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

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

och

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

Eulerförmödan ger, då  $p \equiv -q \pmod{4a}$ , 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.

## Exempel (Beräkning av Legendresymbol)

$$\begin{aligned}\left(\frac{1234}{17}\right) &= \left(\frac{72 * 17 + 10}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{2}{17}\right) \left(\frac{5}{17}\right) = \\ &1 * \left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1\end{aligned}$$

## Exempel

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

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

Mod  $p$ :

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

så

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

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

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  $p \equiv \pm 1 \pmod{5}$  och  $p \equiv \pm 1, \pm 2, \pm 4, \pm 8 \pmod{17}$ .