Algebra och talteori

MMGL31

Föreläsning 11

VT 2010

Samuel Bengmark

Repetition

- Ordning, $e_p(a)$
  - Delar alltid $\phi(p)=p-1$
  - Det finns $\phi(d)$ stycken av ordning d, om $d|p-1$.
- Primitiv rot, generator
  - Finns $\phi(p)=p-1$ stycken.
  - Svårt att veta vilka.
- Index (diskret logaritm) räknas mod p-1
  - $I(ab)\equiv_{p-1} I(a)+I(b)$
  - $I(x^k) \equiv_{p-1} k\, I(x)$
- Lösa ekvationer

Idag

Dagens nya begrepp

- Kvadratiska rester, QR och NR
- Legendre symbolen
- Euler kriterium

Dagens följder

- I vilka $\mathbb{Z}_p$ har $x^2+1\equiv_p 0$ lösning?
- Finns oändligt många primtal $\equiv_4 1$

Kvadrater i $\mathbb{Z}$

Följande tal är de första kvadraterna i $\mathbb{Z}$:

1,4,9,16,25,36,49,…

Vi känner igen dessa. Lite svårare är det att direkt se att 576 är en kvadrat, med det är 24^2.

Även för låga nummer är det inte uppenbart vilka som är kvadrater i tex $\mathbb{Z}_{11}$.

Kvadratisk rest, QR

Definition

Ett tal a är en kvadratisk rest (kvadrat) i $\mathbb{Z}_p$ om det finns ett $b\in\mathbb{Z}_p$ så att $b^2 \equiv_p a$.
Vi skriver kort att a är QR (Quadratic residue).

Tal som ej är kvadratisk rest kallar vi icke-kvadratisk rest, eller NR (non-quadratic residue).

Exempel

Titta på alla kvadrater i $\mathbb{Z}_{11}$.

a	1	2	3	4	5	6	7	8	9	10
a^2	1	4	9	5	3	3	5	9	4	1

Endast talen 1,3,4,5,9 är QR $\mathbb{Z}_{11}$.

Talen 2,6,7,8,10 är NR.

Några observationer

- Verkar vara lika många QR som NR.
- Verkar vara symmetrisk i tabellerna.

Det sista är klart eftersom $a^2 \equiv_p (p-a)^2$.

a	1	2	3	4	5	6	7	8	9	10
a^2	1	4	9	5	3	3	5	9	4	1

dvs talen $1^2, \ldots, ((p-1)/2)^2$ ger alla QR.

QR = # NR = (p-1)/2

Sats

Om p är ett udda primtal då finns det precis (p-1)/2 kvadratiska rester i $\mathbb{Z}_p$.

Bevis

Vi såg att talen $1^2, \ldots, ((p-1)/2)^2$ genererar alla QR.

Vill nu visa att alla dessa är olika.

Tag a, b s.a. $1 \leq a \leq b \leq (p-1)/2$ och antag att $a^2 \equiv_p b^2$.

Då gäller att $p|b^2-a^2$ dvs $p|(b-a)(b+a)$

Ser att $0 \leq b-a \leq (p-3)/2$ och $2 \leq b+a \leq p-1$.

Därför gäller att $p \nmid (b+a)$. Då p primt måste $p|b-a$ och därmed b-a=0, dvs a=b.

QR och primitiv rot

Om g är en primitiv rot i $\mathbb{Z}_p$ så gäller att g^{2k} är QR eftersom

$$g^{2k} = (g^k)^2$$

Dessa blir (p-1)/2 till antalet och därmed finns det inte plats för något g^{udda} att vara QR

Sats

Om g är en primitiv rot i $\mathbb{Z}_p$ så är g^s QR omm s är jämn.

Multiplikationregeln

Sats

1. QR · QR = QR
2. QR · NR = NR
3. NR · NR = QR

Bevis skiss

Låt g vara en primitiv rot i $\mathbb{Z}_p$. Då ser vi att

1. $g^{jämn} \cdot g^{jämn} = g^{jämn + jämn} = g^{jämn}$
2. $g^{jämn} \cdot g^{udda} = g^{jämn + udda} = g^{udda}$
3. $g^{udda} \cdot g^{udda} = g^{udda + udda} = g^{jämn}$

Legendresymbolen

Definition

Legendre symbolen

$$\left(\frac{a}{p}\right)$$

är en funktion av a och p som definierad enligt följande

$$\left(\frac{a}{p}\right) = \begin{cases} +1 \text{ om a QR i } Z_p \\ -1 \text{ om a NR i } Z_p \end{cases}$$

Multiplikationsregeln i ny dräkt

Om p är ett udda primtal så gäller att

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Att räkna ut Legandresymbolen

Definitionen av Legendresymbolen ger ingen ny hjälp till att räkna ut funktionen på något bra sätt. Man kan ju alltid prova att lösa ekvation $x^2 \equiv_p a$.

Men det finns ett bättre sätt …

Eulers kriterium

Sats

Om p är ett uddaprimtal så gäller att

$$\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}$$

Bevis

- Om a QR så är $a=g^{2k}$, dvs $a^{(p-1)/2}=g^{k(p-1)}=(g^{p-1})^k=1$.
- Om a NR så är $a=g^{2k+1}$, dvs $a^{(p-1)/2}=g^{k(p-1)}\, g^{(p-1)/2}= g^{(p-1)/2}$. Nu är $g^{(p-1)/2} = \pm 1$ enligt FLS men $g^{(p-1)/2} \neq 1$ eftersom det är en primitiv rot. Slutsats $a^{(p-1)/2}=-1$ om a NR.

Exempel

Reciprositetssatsen, del 1

Sats

Om p är ett udda primtal gäller att

-1 är QR i $\mathbb{Z}_p$ omm $p \equiv_4 1$.

Bevis

$$\left(\frac{-1}{p}\right) \equiv_p (-1)^{\frac{p-1}{2}} = \begin{cases} (-1)^{\frac{4k+1-1}{2}} = (-1)^{2k} = 1 \text{ om } p \equiv_4 1 \\ (-1)^{\frac{4k+3-1}{2}} = (-1)^{2k+1} = -1 \text{ om } p \equiv_4 3 \end{cases}$$

Det finns ∞ antal primtal $\equiv_4 1$

Bevisidé: Varje ändlig lista av primtal innehåller inte alla primtal som finns.

Tag en ändlig listan $\{p_1, \ldots, p_n\}$ av primtal $\equiv_4 1$.

Bilda talet $A=(2p_1 \cdot \ldots \cdot p_n)^2+1$.

Då är $A=q_1^{\alpha 1} \cdot \ldots \cdot q_k^{\alpha k}$ enligt Aritm. f. sats, dvs

$q_1^{\alpha 1} \cdot \ldots \cdot q_k^{\alpha k} = (2p_1 \cdot \ldots \cdot p_n)^2+1$

A och alla q_i är udda.

Betrakta likheten mod q_1. Vi får då

$0 \equiv_{q_1} (2p_1 \cdot \ldots \cdot p_n)^2+1$ dvs $(2p_1 \cdot \ldots \cdot p_n)^2 \equiv_{q_1} -1$.

Alltså är -1 QR i $\mathbb{Z}_{q_1}$, dvs $q_1 \equiv_4 1$

Reciprositetssatsen, del 2

Sats

Om p är ett udda primtal gäller att

2 är QR i $\mathbb{Z}_p$ omm $p \equiv_8 \pm 1$.

Bevis

Lämnas till den intresserade.

Generella reciproccitetssatsen

Om a och b är udda tal så gäller att

$$\left(\frac{-1}{b}\right)=\begin{cases}1 \text{ om } b\equiv_4 1\\ -1 \text{ om } b\equiv_4 3\end{cases}$$

$$\left(\frac{2}{b}\right)=\begin{cases}1 \text{ om } b\equiv_8 \pm 1\\ -1 \text{ om } b\equiv_8 \pm 3\end{cases}$$

$$\left(\frac{a}{b}\right)=\begin{cases}\left(\frac{b}{a}\right) \text{ om } b\equiv_4 1 \text{ eller } a\equiv_4 1\\ -\left(\frac{b}{a}\right) \text{ om } a\equiv_4 b\equiv_4 3\end{cases}$$

Exempel