DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Bakalaura studiju programma "Matemātika"

Studiju kurss

Veselo skaitļu teorija

13.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Kvadrātiskās reciprocitātes teorēma

1.1. teorēma. (*Ležandra simbola argumentu simetrijas (kvadrātiskās reciprocitātes) teorēma*) Dots, ka p un q ir nepāra pirmskaitļi.

1. Ja $p \not\equiv 3 \pmod 4$ vai $q \not\equiv 3 \pmod 4$, tad
$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$
2. Ja $p \equiv q \equiv 3 \pmod 4$, tad
$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Ekvivalents formulējums - $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

PIERĀDĪJUMS Izmantosim šādus apzīmējumus: $\mathcal{P} = \{1, 2, ..., \frac{p-1}{2}\}$, $\mathcal{N} = \{-1, -2, ..., -\frac{p-1}{2}\}$, $\mathcal{Q} = \{1, 2, ..., \frac{q-1}{2}\}$.

Saskaņā ar Gausa lemmu, $\left(\frac{q}{p}\right) = (-1)^{\gamma}$, kur $\gamma = |q\mathcal{P} \cap \mathcal{N}|$.

1.solis - γ interpretācija.

γ ir tādu veselu skaitļu $x \in \mathcal{P}$ skaits, kuriem eksistē vesels $n \in \mathcal{N}$ tāds, ka $qx \equiv n \pmod{\text{p}}$.

Tas ir ekvivalents nosacījumam, ka eksistē vesels skaitlis y tāds, ka $qx - py \in \mathcal{N}$ un tātad

$$-\frac{p}{2} < qx - py < 0.$$

Katram x var būt ne vairāk kā viens y, jo pretējā gadījumā eksistē divi dažādi veseli y_1 un y_2 tādi, ka

$$-\frac{p}{2} < qx - py_1 < 0,$$

$$-\frac{p}{2} < qx - py_2 < 0.$$

Bet $|(qx - py_1) - (qx - py_2)| = |p(y_1 - y_2)| \geq p$.

Ja tāds y eksistē, tad pārveidojot nevienādības iegūsim

$$0 < \frac{qx}{p} < y < \frac{qx}{p} + \frac{1}{2}.$$

Tā kā $x \leq \frac{p-1}{2}$, tad

$$y < \frac{q(p-1)}{2p} + \frac{1}{2} < \frac{q+1}{2}.$$

Tātad $y \in \mathcal{Q} = \{1, 2, ..., \frac{q-1}{2}\}$. Esam pierādījuši, ka γ ir to veselu skaitļu pāru (x, y) skaits kopā $\mathcal{P} \times \mathcal{Q}$, kuri apmierina nosacījumu

$$-\frac{p}{2} < qx - py < 0.$$

2.solis - p un q maiņa. Mainot vietām p un q un izmantojot iepriekšējā soļa rezultātu, redzam, ka $\left(\frac{p}{q}\right) = (-1)^{\delta}$, kur δ ir to veselu skaitļu pāru (y, x) skaits kopā $\mathcal{Q} \times \mathcal{P}$, kas apmierina nevienādību

$$-\frac{q}{2} < py - qx < 0.$$

Reizinot visu ar $-$ zīmi un mainot nevienādības iegūsim ekvivalentu nosacījumu

$$0 < qx - py < \frac{q}{2}.$$

3.solis - iepriekšējo soļu rezultātu apvienošana un interpretēšana.

Redzam, ka

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\gamma+\delta},$$

kur $\gamma+\delta$ ir to skaitļu pāru skaits kopā $\mathcal{P}\times\mathcal{Q}$, kas apmierina nosacījumu

$$-\frac{p}{2} < qx - py < 0 \text{ vai } 0 < qx - py < \frac{q}{2}.$$

Tā kā $qx-py \neq 0$, jo $LKD(p,q) = 1$, tad varam abus nosacījumus apvienot vienā:

$$-\frac{p}{2} < qx - py < \frac{q}{2}.$$

Ievērosim arī, ka pietiek zināt $\gamma + \delta \pmod 2$, jo tas ir kāpinātājs skaitlim -1.

4.solis - rezultāta interpretēšana Dekarta koordinātēs.
Apzīmēsim ar T taisnstūri ar virsotnēm

$$(1,1), (1, \frac{q-1}{2}), (\frac{p-1}{2}, 1), (\frac{p-1}{2}, \frac{q-1}{2}).$$

Skaitļu pāriem no kopas $\mathcal{P} \times \mathcal{Q}$ atbilst punkti ar veselām Dekarta koordinātēm, kas pieder T.

Nevienādības

$$-\frac{p}{2} < qx - py < \frac{q}{2}$$

atrisinājumi ir punkti ar veselām Dekarta koordinātēm, kas atrodas joslā J, ko ierobežo taisnes

$$-\frac{p}{2} = qx - py \text{ un } qx - py = \frac{q}{2}.$$

Skaitļu pāriem, kas apmierina šo nevienādību, atbilst punkti ar veselām Dekarta koordinātēm, kas atrodas figūrā $\mathrm{T} \cap \mathrm{J}$. Tādu punktu skaits ir vienāds ar $t - a - b$, kur

- t ir punktu ar veselām koordinātēm skaits taisnstūrī T,
- a ir punktu ar veselām koordinātēm skaits slēgtajā apgabalā virs taisnes $-\frac{p}{2} = qx - py$,
- b ir punktu ar veselām koordinātēm skaits slēgtajā apgabalā zem taisnes $qx - py = \frac{q}{2}$.

5.solis - punktu skaits taisnstūrī T.

Redzam, ka punktu ar veselām koordinātēm skaits t taisnstūrī T ir vienāds ar elementu skaitu kopā $\mathcal{P} \times \mathcal{Q}$, kas ir vienāds ar

$$|\mathcal{P}| \cdot |\mathcal{Q}| = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

6.solis - vienādības $a = b$ **pierādīšana**.

Taisnstūris T ir figūra, kura ir centrāli simetriska ar centru

$$C = (\frac{p+1}{4}, \frac{q+1}{4}).$$

Centrālā simetrija šajā gadījumā ir pārveidojums

$$(x, y) \to (x', y') = (\frac{p+1}{2} - x, \frac{q+1}{2} - y)$$

(trīs vienkāršāku pārveidojumu kompozīcija - paralēli pārnest par vektoru $-\overrightarrow{OC}$, reizināt ar -1, pārnest atpakaļ par vektoru $\overrightarrow{OC}$).

Var pārbaudīt, ka taisnes

$$-\frac{p}{2} = qx - py$$

un

$$qx - py = \frac{q}{2}$$

arī ir centrāli simetriskas attiecībā uz T centru - punkts (x, y) apmierina vienu no vienādojumiem tad un tikai tad, ja punkts (x', y') apmierina otru vienādojumu. Piemēram, ja (x, y) apmierina vienādojumu

$-\frac{p}{2} = qx - py$, tad

$$qx' - py' = q\Big(\frac{p+1}{2} - x\Big) - p\Big(\frac{q+1}{2} - y\Big) =$$
$$(py - qx) + \frac{pq}{2} + \frac{q}{2} - \frac{pq}{2} - \frac{p}{2} =$$
$$\frac{p}{2} + \frac{q}{2} - \frac{p}{2} = \frac{q}{2}.$$

Ņemot vērā centrālo simetriju redzam, ka katram punktam ar veselām koordinātēm taisntūrī T virs taisnes

$$-\frac{p}{2} = qx - py$$

atbilst simetriskais punkts zem taisnes

$$qx - py = \frac{q}{2},$$

tātad šādu punktu skaits ir vienāds un iegūstam, ka

$$a = b.$$

7.solis - lieluma $t-a-b$ paritāte un noslēgums. Tā kā $a = b$, tad

$$t - a - b = t - 2a \equiv t \pmod 2.$$

Redzam, ka $\gamma + \delta \equiv t \pmod 2$, tātad

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

■

2. Kvadrātiskie vienādojumi saliktiem modu

2.1. Pirmskaitļu pakāpju moduļi

2.1. teorēma. $p > 2$ ir pirmskaitlis.

$$a \in Q_{p^\alpha} \iff a \in Q_p.$$

PIERĀDĪJUMS
No iepriekš dotām teorēmām seko šādi fakti:

- Eksistē primitīva sakne g mod p^α.
- Q_{p^α} veido g pāra pakāpes.

Skaitlis g ir arī primitīva sakne mod p un tādējādi kopu Q_p veido g pāra pakāpes mod p.

$$a \in Q_{p^\alpha} \iff a \equiv g^{2n} (\mathrm{mod}\ p^\alpha) \implies$$
$$a \equiv g^{2n} (\mathrm{mod}\ p) \iff a \in Q_p.$$

Pierādīsim, ka $a \in Q_p \implies a \in Q_{p^\alpha}$ izmantojot vienkāršotu matemātisko indukciju - pierādīsim, ka

$$\forall \beta \geq 1, a \in Q_{p^\beta} \implies a \in Q_{p^{\beta+1}}.$$

Ja $a \in Q_{p^\beta}$, tad vienādojumam

$$x^2 \equiv a (\mathrm{mod}\ p^\beta)$$

eksistē atrisinājums $x = x_1 + p^\beta x_2$, kur $x_1 \not\equiv 0 (\mathrm{mod}\ p)$.

Ievietosim to vienādojumā

$$x^2 \equiv a (\mathrm{mod}\ p^{\beta+1}).$$

Iegūsim, ka

$$(x_1+p^\beta x_2)^2 \equiv a(\text{mod } p^{\beta+1}) \iff \underbrace{(x_1^2-a)}_{\equiv 0(\text{mod } p^\beta)} +2p^\beta x_1x_2 \equiv 0(\text{mod } p^{\beta+1})$$

$$\iff \frac{(x_1^2-a)}{p^\beta} + 2x_1x_2 \equiv 0(\text{mod } p).$$

Redzam, ka pēdējam vienādojumam ir atrisinājums attiecībā uz x_2:

$$x_2 \equiv -\frac{(x_1^2-a)}{2x_1p^\beta}(\text{mod } p).$$

■

2.1. piemērs. $Q_7 = \{1, 2, 4\}$.

$Q_{49} = \{1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, 32, 36, 37, 39, 43, 44, 4$

Redzam, ka

$$Q_{49} = \{\underline{1}, 8, 15, 22, 29, 36, 43\} \cup$$
$$\{\underline{2}, 9, 16, 23, 30, 37, 44\} \cup$$
$$\{\underline{4}, 11, 18, 25, 32, 39, 46\} =$$
$$\pi_{49,7}^{-1}(1) \cup \pi_{49,7}^{-1}(2) \cup \pi_{49,7}^{-1}(4).$$

2.2. teorēma.

1. $a \in Q_2 \iff a \equiv 1 (\mathrm{mod}\ 2)$.
2. $a \in Q_4 \iff a \equiv 1 (\mathrm{mod}\ 4)$.
3. $\alpha \geq 3 \implies a \in Q_{2^\alpha} \iff a \equiv 1 (\mathrm{mod}\ 8)$.

PIERĀDĪJUMS

1., 2. Tieša pārbaude.

3. Detalizēts pierādījums netiks dots. Viens ceļš - no sākuma pierādīt, ka U_{2^α} ģenerējošā kopa ir $\{5, -5\}$.

■

2.2. piemērs. $Q_{32} = \pi_{32,8}^{-1}(1) = \{1, 9, 17, 25\}$.

2.2. Patvaļīgi moduļi

2.3. teorēma. Dots, ka $m = m_1 m_2 ... m_l$, kur $LKD(m_i, m_j) = 1$. Tad

$$a \in Q_m \iff a \in Q_{m_i}, \forall i.$$

PIERĀDĪJUMS

$a \in Q_m \implies \exists x \in \mathbb{Z} : x^2 \equiv a (\text{mod } m) \implies x^2 \equiv a (\text{mod } m_i), \forall i.$ Tas seko no tā, ka $m_i | m$. Papildus tam $a \in U_m \implies a \in U_{m_i}$.

$a \in Q_{m_i}, \forall i \implies \forall i \exists x_i : x_i^2 \equiv a (\text{mod } m_i)$.

Saskaņā ar ķīniešu atlikumu teorēmu sistēmai

$$\begin{cases} x \equiv x_1 (\mathrm{mod}\ m_1) \\ \dots \\ x \equiv x_l (\mathrm{mod}\ m_l) \end{cases}$$

eksistē atrisinājumu klase x mod m.

Seko, ka x apmierina sistēmu

$$\begin{cases} x^2 \equiv a (\mathrm{mod}\ m_1) \\ \dots \\ x^2 \equiv a (\mathrm{mod}\ m_l) \end{cases},$$

kas ir ekvivalenta vienādojumam

$$x^2 \equiv a (\mathrm{mod}\ m).$$

Tas seko no iepriekš pierādītas teorēmas (11.lekcija). ■

2.1. piezīme. Speciālgadījumā iegūsim šādu apgalvojumu: ja

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_l^{\alpha_l},$$

tad

$$a \in Q_m \iff a \in Q_{p_i^{\alpha_i}}, \forall i.$$

2.4. teorēma. Dots, ka $m = p_1^{\alpha_l} p_2^{\alpha_2} ... p_l^{\alpha_l}$.

$$a \in Q_m \iff$$

1. $a \in Q_{p_i}, \forall i, p_i > 2.$
2. $$ord_2(m) \leq 2 \implies a \equiv 1(\text{mod } 4) \wedge$$
$$ord_2(m) > 2 \implies a \equiv 1(\text{mod } 8).$$

2.3. piemērs. Atradīsim Q_{72}. $72 = 2^3 3^2$. Seko, ka

$$a \in Q_{72} \iff a \equiv 1(\text{mod } 3) \wedge a \equiv 1(\text{mod } 8).$$

Sistēmas

$$\begin{cases} a \equiv 1(\text{mod } 3) \\ a \equiv 1(\text{mod } 8) \end{cases}$$

atrisinājums ir $a \equiv 1 (\mathrm{mod}\ 24)$. Seko, ka

$$Q_{72} = \pi^{-1}_{72,24}(1) = \{1, 25, 49\}.$$

3. Augstāku pakāpju atlikumi

3.1. teorēma. p - pirmskaitlis, $n \geq 2$, $d = LKD(n, p-1)$, $a \not\equiv 0(\text{mod } p)$, g ir primitīva sakne mod p.

1. a ir n-tās pakāpes atlikums $\iff \mathsf{ind}_g(a) \equiv 0(\text{mod } d)$.
2. $\mathsf{ind}_g(a) \equiv 0(\text{mod } d) \iff a^{\frac{p-1}{d}} \equiv 1(\text{mod } p)$.
3. Ja a ir n-tās pakāpes atlikums, tad vienādojumam
$$x^n \equiv a(\text{mod } p)$$
ir d dažādi atrisinājumi mod p;
4. Eksistē $\frac{p-1}{d}$ dažādi n-tās pakāpes atlikumi mod p.

PIERĀDĪJUMS

1. a ir n-tās pakāpes atlikums $\iff \exists y \in \mathbb{Z}$ tāds, ka
$$\begin{cases} x \equiv g^y(\text{mod } p) \\ x^n \equiv g^{ny} \equiv g^{\mathsf{ind}_g(a)}(\text{mod } p) \end{cases}$$
$$\iff ny \equiv \mathsf{ind}_g(a)(\text{mod } p-1).$$

Lineārajai kongruencei ir atrisinājums tad un tikai tad, ja

$$\mathsf{ind}_g(a) \equiv 0 (\mathrm{mod}\ d)$$

2. $\mathsf{ind}_g(a) \equiv 0 (\mathrm{mod}\ d) \implies \exists x : x^n \equiv a (\mathrm{mod}\ p) \implies$

$$a^{\frac{p-1}{d}} \equiv x^{n\frac{p-1}{d}} \equiv (x^{p-1})^{\frac{n}{d}} \equiv 1 (\mathrm{mod}\ p).$$

Apzīmēsim $\mathsf{ind}_g(a)$ ar t. Tad

$$a^{\frac{p-1}{d}} \equiv g^{t\frac{p-1}{d}} \equiv 1 (\mathrm{mod}\ p) \implies t\frac{p-1}{d} \equiv 0 (\mathrm{mod}\ p-1).$$

$LKD(\frac{p-1}{d}, p-1) = 1$, tāpēc var dalīt abas puses ar $\frac{p-1}{d}$. Seko, ka

$$t \equiv 0 (\mathrm{mod}\ p-1) \implies t \equiv 0 (\mathrm{mod}\ d).$$

3. Ja

$$\mathsf{ind}_g(a) \equiv 0(\text{mod } d),$$

tad lineārajai kongruencei

$$ny \equiv \mathsf{ind}_g(a)(\text{mod } p-1)$$

ir d dažādi atrisinājumi mod p - tas seko no lineārā vienādojuma atrisinājumu īpašībām (jāizmanto inversā relatīvā redukcija no $\frac{p-1}{d}$ uz $p-1$.

4. a ir n-tās pakāpes atlikums $\iff$ $\mathsf{ind}_g(a) \equiv 0(\text{mod } d)$. Lielums ind_g pieņem visas vērtības mod $p-1$ un vienādojumam

$$z \equiv 0(\text{mod } d)$$

ir $\frac{p-1}{d}$ atrisinājumi formā

$$0, 0+d, 0+2d, ..., 0+\frac{p-1}{d}-1.$$

Tādējādi eksistē tieši $\frac{p-1}{d}$ n-tās pakāpes atlikumi.

$$g^0, g^d, ..., g^{d\cdot(\frac{p-1}{d}-1)}.$$

■

3.1. piemērs. $p = 11$.

$n = 2$. $Q_{2,11} = \{1, 3, 4, 5, 9\}$. $|Q_{2,11}| = 5 = \frac{11-1}{LKD(2,10)} = 5$.

$n = 3$. $Q_{3,11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. $|Q_{3,11}| = 10 = \frac{11-1}{LKD(3,10)} = 10$.

$n = 4$. $Q_{4,11} = \{1, 3, 4, 5, 9\}$. $|Q_{4,11}| = 5 = \frac{11-1}{LKD(4,10)} = 5$.

$n = 5$. $Q_{5,11} = \{1, 10\}$. $|Q_{5,11}| = 5 = \frac{11-1}{LKD(5,10)} = 2$.

$n = 6$. $Q_{6,11} = \{1, 3, 4, 5, 9\}$. $|Q_{6,11}| = 5 = \frac{11-1}{LKD(6,10)} = 5$.

4. 13.mājasdarbs

13.1 Atrisiniet vienādojumus

(a) $x^2 \equiv 11 (\mathrm{mod}\ 625)$;
(b) $x^2 \equiv 9 (\mathrm{mod}\ 32)$;
(c) $x^2 \equiv 3 (\mathrm{mod}\ 7^5)$.

13.2 Atrisiniet vienādojumus

(a) $x^2 \equiv 40 (\mathrm{mod}\ 72)$;
(b) $x^2 \equiv 120 (\mathrm{mod}\ 210)$.
(c) $x^2 \equiv 18 (\mathrm{mod}\ 441)$.

13.3 Atrodiet

(a) Q_{144},
(b) Q_{168},
(c) Q_{264}.

13.4 Atrodiet

(a) $Q_{3,13}$,
(b) $Q_{4,13}$,
(c) $Q_{6,19}$.