DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Studiju kurss

Veselo skaitļu teorija

7.lekcija (datoriķiem)

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Vienādojumu risināšana atlikumu kopās **3**

1.1. Invertējama elementa indekss (diskrētais logaritms) . . 3

1.2. Modulāro Diofanta vienādojumu risināšanas pamati . 8

1.3. Modulāro vienādojumu ekvivalentie pārveidojumi un moduļa maiņa 12

1.4. Lineārs vienādojums ar vienu nezināmo 15

2. 7.mājasdarbs **19**

1. Vienādojumu risināšana atlikumu kopās

1.1. Invertējama elementa indekss (diskrētais logaritms)

Dots, ka $a \in U_m$ un $b \in U_m$. Teiksim, ka s ir b *indekss ar bāzi* a *pēc moduļa* m, ja

$$a^s \equiv b \pmod{\mathrm{m}}.$$

Apzīmēsim ar $\mathsf{ind}_a(b)$ vai $\mathsf{ind}(b)$.

Par indeksu var domāt kā par "logaritmu pie bāzes a", tāpēc to sauc arī par *diskrēto logaritmu*.

Ievērosim, ka

- pagaidām indekss ir noteikts ar precizitāti līdz $\varphi(m)$ daudzkārtnim, tāpēc ka

$$a^{s+k\varphi(m)} \equiv a^s (a^{\varphi(m)})^k \equiv b \pmod{\mathrm{m}};$$

- dabiski ir definēt $\mathsf{ind}_a(1) \equiv 0 \pmod{\varphi(m)}$;

- $\mathrm{ind}_a(a) \equiv 1 \pmod{\varphi(m)}$.

1.1. piemērs.

- $p = 5$, $\mathrm{ind}_3(4) = \mathrm{ind}_2(4) = 2$, $\mathrm{ind}_3(2) = \mathrm{ind}_2(3) = 3$;
- $p = 7$, $\mathrm{ind}_3(2) = \mathrm{ind}_4(2) = \mathrm{ind}_2(4) = \mathrm{ind}_5(4) = 2$, $\mathrm{ind}_3(6) = \mathrm{ind}_5(6) = 3$, $\mathrm{ind}_5(2) = \mathrm{ind}_3(4) = 4$, $\mathrm{ind}_3(5) = \mathrm{ind}_5(3) = 5$;

1.1. teorēma. Ja g ir primitīva sakne pēc moduļa m, tad

1. katram $a \in U_m$ eksistē indekss pie bāzes g;
2. visas iespējamās a indeksa vērtības pieder vienai atlikumu klasei pēc moduļa $\varphi(m)$,

PIERĀDĪJUMS

1. Ja g ir primitīva sakne, tad katrs $a \in U_m$ ir izsakāms formā $a \equiv g^s \pmod{\mathrm{m}}$, tāpēc indekss eksistē.

2. Ja g ir primitīvas sakne, tad visas tās pakāpes ar kāpinātājiem $0, 1, ..., \varphi(m)$ ir dažādas un $g^{\varphi(m)} \equiv 1 \pmod{\mathrm{m}}$. Ja $g^{s_1} \equiv g^{s_2} \pmod{\mathrm{m}}$, tad $g^{s_1 - s_2} \equiv 1 \pmod{\mathrm{m}}$, tāpēc $s_1 - s_2 \equiv 0 \pmod{\varphi(m)}$. ■

1.2. teorēma. Ja g ir primitīva sakne pēc moduļa m, tad

1. ind_g ir bijektīva funkcija $U_m \to \mathbb{Z}/\varphi(m)\mathbb{Z}$;
2. $\mathsf{ind}_g(ab) \equiv \mathsf{ind}_g(a) + \mathsf{ind}_g(b) \pmod{\varphi(m)}$;
3. $\mathsf{ind}_g(a^k) \equiv k \cdot \mathsf{ind}_g(a) \pmod{\varphi(m)}$;
4. $\mathsf{ind}_g(\frac{a}{b}) \equiv \mathsf{ind}_g(a) - \mathsf{ind}_g(b) \pmod{\varphi(m)}$;
5. $\mathsf{ind}_g(a) \equiv \mathsf{ind}_g(h) \cdot \mathsf{ind}_h(a) \pmod{\varphi(m)}$, kur h arī ir primitīva sakne pēc moduļa m;

PIERĀDĪJUMS 1. Ja $\mathsf{ind}_g(a_1) \equiv \mathsf{ind}_g(a_2) \pmod{\varphi(m)}$, tad

$$\mathsf{ind}_g(a_1) = \mathsf{ind}_g(a_1) + \varphi(m) \cdot l$$

un

$$a_1 \equiv a_2(g^{\varphi(m)})^l \pmod{\mathrm{m}}$$

un $a_1 \equiv a_2 \pmod{\mathrm{m}}$, tātad ind_g ir injektīva funkcija. Tā kā g ir primitīva sakne, tad katram k eksistē $a \in U_m$ tāds, ka $a \equiv g^k \pmod{\mathrm{m}}$, tātad ind_g ir sirjektīva funkcija.

2.

$$g^{\mathsf{ind}_g(ab)} \equiv ab \equiv g^{\mathsf{ind}_g(a)} g^{\mathsf{ind}_g(b)} \equiv g^{\mathsf{ind}_g(a)+\mathsf{ind}_g(b)} \pmod{\mathrm{m}},$$

tāpēc $\mathsf{ind}_g(ab) \equiv \mathsf{ind}_g(a) + \mathsf{ind}_g(b) \pmod{\varphi(m)}$.

3.,4. - pierāda līdzīgi kā 2.

5.

$$a \equiv g^{\mathsf{ind}_g(a)} \equiv h^{\mathsf{ind}_h(a)} \equiv (g^{\mathsf{ind}_g(h)})^{\mathsf{ind}_h(a)} \equiv g^{\mathsf{ind}_g(h)\cdot\mathsf{ind}_h(a)} \pmod{\mathrm{m}},$$

■

1.1. piezīme. Diskrētā logaritma atrašana ir grūta problēma no skaitļošanas viedokļa, to izmanto šifrēšanā.

1.2. piezīme. Izmantojot diskrētos logaritmus, var risināt vienādojumus atlikumu kopās, kuros ir iesaistīta tikai reizināšana, piemēram, vienādojumus, kas ir izsakāmi formā

$$x^k \equiv a \pmod{\mathrm{m}}$$

saskaņā ar šādu algoritmu:

1. atrast primitīvu sakni g (mod m),
2. atrast a indeksu pie bāzes g, apzīmēsim to ar α,
3. pieņemt, ka $x \equiv g^y \pmod{\text{m}}$, citiem vārdiem sakot, veikt nezināmo substitūciju $x \to y$,
4. izteikt vienādojuma abas puses kā g pakāpes, iegūt vienādojumu
$$g^{ky} \equiv g^{\alpha} \pmod{\text{m}},$$
5. atrisināt vienādojumu
$$ky \equiv \alpha \pmod{\varphi(m)}$$
attiecībā uz y.

1.2. Modulāro Diofanta vienādojumu risināšanas pamati

1.3. piezīme. Atrisināt Diofanta vienādojumu pēc moduļa m

$$f(x_1, ..., x_n) \equiv 0 \pmod{\text{m}}$$

vai Diofanta vienādojumu sistēmu pēc moduļa m

$$\begin{cases} f_1(x_1, ..., x_n) \equiv 0 \pmod{m_1} \\ f_2(x_1, ..., x_n) \equiv 0 \pmod{m_2} \\ ... \\ f_k(x_1, ..., x_n) \equiv 0 \pmod{m_k} \end{cases}$$

nozīmē to atrisināt *veselos skaitļos* (gredzenā $\mathbb{Z}$). Šādus vienādojumu un vienādojumu sistēmas sauksim par *modulārām Diofanta sistēmām*.

Parasti kā starprezultāts tiek iegūts kāds rezultāts par nezināmo vērtībām reducējot tos pēc noteiktiem moduļiem. Tādējādi risinot

vienādojumu sistēmas atlikumu gredzenos, nezināmie līdz noteiktam brīdim tiek uzskatīti par elementiem atlikumu gredzenos.

1.4. piezīme. Kā zināms, atlikumu klases a (mod m) pārstāvji ir visi veselie x, kuriem izpildās nosacījums

$$x \equiv a \text{ (mod m)}.$$

Visu šādu veselo skaitļu kopu $\mathcal{C}_m(a)$ var interpretēt kā atlikumu klases a inverso attēlu attiecībā uz reducēšanas pēc moduļa m funkciju

$$\pi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}.$$

Tādējādi $\mathcal{C}_m(a) = \pi_m^{-1}(a)$. Pāreju no atlikumu klases uz veselo skaitļu kopu interpretēsim kā redukcijas inverso attēlojumu.

1.3. teorēma. Ja vesels skaitlis a apmierina sistēmu

$$\begin{cases} f_1(x) \equiv 0 \pmod{m_1} \\ f_2(x) \equiv 0 \pmod{m_2} \\ \ldots \\ f_k(x) \equiv 0 \pmod{m_k} \end{cases},$$

tad jebkurš skaitlis a' tāds, ka

$$a \equiv a' \pmod{MKD(m_1, ..., m_k)},$$

arī apmierina šo sistēmu.

PIERĀDĪJUMS Ja $a \equiv a' \pmod{MKD(m_1, ..., m_k)}$, tad katram i izpildās

$$f_i(a) \equiv f_i(a') \pmod{MKD(m_1, ..., m_k)}.$$

Saskaņā ar atlikumu kongruences īpašībām katram m_j izpildās

$$f_i(a) \equiv f_i(a') \equiv 0 \pmod{m_j}.$$

■

1.5. piezīme. Ņemot vērā iepriekšējo teorēmu, var konstatēt, ka modulārās Diofanta sistēmas veselie atrisinājumu veido atlikumu klases pēc moduļa $MKD(m_1, ..., m_k)$.

1.6. piezīme. Pilnīgs analoģisks apgalvojums ir spēkā, ja tiek risināta sistēma ar vairākiem nezināmiem: ja skaitļu virkne $(a_1, ..., a_n)$ apmierina sistēmu

$$\begin{cases} f_1(x_1, ..., x_n) \equiv 0 \pmod{m_1} \\ f_2(x_1, ..., x_n) \equiv 0 \pmod{m_2} \\ ... \\ f_k(x_1, ..., x_n) \equiv 0 \pmod{m_k} \end{cases},$$

tad jebkura virkne $(a'_1, ..., a'_n)$, kur $a_j \equiv a'_j \pmod{MKD(m_1, ..., m_k)}$, arī apmierina šo sistēmu.

1.3. Modulāro vienādojumu ekvivalentie pārveidojumi un moduļa maiņa

1.4. teorēma. Zemāk aprakstītās operācijas saglabā modulāra vienādojuma atrisinājumu kopu:

1. reducēt polinomu koeficientus pēc dotā moduļa;
2. pieskaitīt vienādojuma abām pusēm vienu un to pašu atlikumu klasi;
3. reizināt abas puses ar vienu un to pašu invertējamu atlikumu klasi;
4. reizināt visus locekļus un moduli ar nenulles veselu skaitli k;
5. ja katrs vienādojuma loceklis un modulis dalās ar d, tad var izdalīt visus locekļus un moduli ar d;

PIERĀDĪJUMS

4.-5. $f(x) \equiv 0 \pmod{\mathrm{m}} \implies f(x) = mq$, tātad $kf(x) = (mk)q$. Katru $f(x)$ koeficientu var reizināt ar k.

Ja katrs $f(x)$ koeficients dalās ar d un m dalās ar d un $f(x) \equiv 0 \pmod{\text{m}}$, tad $f(x) = mq$ un $d \cdot f_1(x) = d \cdot m_1 q$, tātad $f_1(x) = m_1 q$. Esam ieguvuši vienādojumu $f_1(x) \equiv 0 \pmod{m_1}$. ■

1.2. piemērs. $x + 2 \equiv 0 \pmod{5} \iff x + 2 - 2 \equiv 0 - 2 \pmod{5}$ un $x \equiv 3 \pmod{5}$.

$4x + 2 \equiv 0 \pmod{5} \iff 4(4x + 2) \equiv 4 \cdot 0 \pmod{5}$ un $x \equiv 2 \pmod{5}$.

$2x \equiv 6 \pmod{8} \iff x \equiv 3 \pmod{4}$.

1.7. piezīme. Ja $(x_1, ..., x_n)$ ir vesels atrisinājums vienādojumam

$$f(x_1, ..., x_n) \equiv 0 \pmod{\mathrm{m}}$$

un $k|m$, tad $(x_1, ..., x_n)$ ir atrisinājums arī vienādojumam

$$f(x_1, ..., x_n) \equiv 0 \pmod{\mathrm{k}}.$$

Bet ne otrādi. Vienādojumam

$$f(x_1, ..., x_n) \equiv 0 \pmod{\mathrm{k}}$$

var būt vairāk atrisinājumu nekā sākotnējam vienādojumam. Šo īpašību izmanto kontrapozitīvajā formā: ja nav atrisinājumu mod k, tad nav atrisinājumu mod m.

1.3. piemērs. Vienādojumam $x \equiv 1$ ir viena atrisinājumu klase mod 4 un viena atrisinājumu klase mod 2, kas satur iepriekšējo klasi kā apakškopu.

Ja $x^4 + 1 \equiv 0 \pmod{27}$, tad $x^4 + 1 \equiv 0 \pmod{3}$. Pēdējam vienādojumam nav atrisinājumu, tātad to nav arī sākotnējam vienādojumam.

1.4. Lineārs vienādojums ar vienu nezināmo

1.8. piezīme. Vienādojums

$$ax \equiv b \pmod{m},$$

kur $LKD(a, m) = 1$, ir viegli atrisināms, jo eksistē $a^{-1} \pmod{m}$:

$$a^{-1}(ax) \equiv x \equiv a^{-1}b \pmod{m}.$$

Atrisinājumu var uzrakstīt arī izmantojot Eilera teorēmu:

$$x \equiv a^{\varphi(m)-1}b \pmod{m}.$$

1.4. piemērs. Vienādojuma $3x \equiv 2 \pmod{5}$ atrisinājums ir

$$x \equiv 3^3 2 \equiv 4 \pmod{5}.$$

1.5. teorēma.

1. Vienādojumam
$$ax \equiv b \pmod{m}$$
neeksistē atrisinājumi, ja $b \not\equiv 0 \pmod{d}$, kur $d = LKD(a, m)$.
2. Ja $b \equiv 0 \pmod{d}$, tad vienādojuma
$$ax \equiv b \pmod{m}$$
atrisinājumu kopa ir klase $(\frac{a}{d})^{-1}(\frac{b}{d}) \pmod{(\frac{m}{d})}$.

PIERĀDĪJUMS

1. Ja $d = 1$, tad vienmēr $b \equiv 0 \pmod{d}$. Pieņemsim, ka $d > 1$, $a = a_1 d$, $m = m_1 d$, kur $LKD(a_1, m_1) = 1$. Vienādojums $ax \equiv b \pmod{m}$ ir ekvivalents vienādojumam
$$(a_1 d)x = b + (m_1 d)q$$
ar kādu $q \in \mathbb{Z}$. Redzam, ka $b \equiv 0 \pmod{d}$.
2. Ja $b \equiv 0 \pmod{d}$, tad $b = b_1 d$. Vienādojums
$$ax \equiv b \pmod{m}$$

ir ekvivalents ar vienādojumu

$$(a_1 d)x \equiv b_1 d \pmod{m_1 d}.$$

Izdalot visus locekļus un moduli ar d, iegūsim ekvivalentu vienādojumu

$$a_1 x \equiv b_1 \pmod{m_1}.$$

Tā kā $LKD(a_1, m_1) = 1$, tad šim vienādojumam eksistē viena atrisinājumu klase

$$x \equiv a_1^{-1} b_1 \pmod{m_1}$$

vai

$$x \equiv (\frac{a}{d})^{-1} (\frac{b}{d}) \pmod{(\frac{m}{d})}.$$

■

1.5. piemērs. Vienādojumam

$$4x \equiv 5 \pmod{8}$$

nav atrisinājumu.

Vienādojums

$$6x \equiv 9 \pmod{15}$$

ir ekvivalents vienādojumam

$$2x \equiv 3 \pmod 5,$$

kura atrisinājums ir

$$x \equiv 2^{-1}3 \equiv 4 \pmod 5 = \{4, 9, 14\} \pmod{15}.$$

2. 7.mājasdarbs

7.1 Par pirmskaitļa p *indeksu matricu* sauc tabulu, kurā rindas tiek indeksētas ar visiem nenulles atlikumiem a_i pēc moduļa p, kolonnas tiek indeksētas ar primitīvajām saknēm g_j pēc moduļa p un katrā rūtiņā, kas atbilst pārim (a, g), tiek ierakstīts $\mathsf{ind}_g(a) \pmod{\varphi(p)}$. Sastādīt indeksu matricu pirmskaitlim 7.

7.2 Atrisiniet vienādojumus

(a) $15x \equiv 40 \pmod{35}$;
(b) $44x \equiv 77 \pmod{33}$;
(c) $1215x \equiv 560 \pmod{2755}$.