

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

Studiju kurss

Veselo skaitļu teorija

7.lekcija (datoriķiem)

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

1. Vienādojumu risināšana atlikumu kopās	3
1.1. Invertējama elementa indekss (diskrētais logaritms) . .	3
1.2. Modulāro Diofanta vienādojumu risināšanas pamati .	10
1.3. Modulāro vienādojumu ekvivalentie pārveidojumi un moduļa maiņa	14
1.4. Lineārs vienādojums ar vienu nezināmo	18
1.5. Vienādojumi atlikumu gredzenos pēc pirmskaitļa moduļa	22
2. 7.mājasdarbs	29

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

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

Apzīmēsim ar $\text{ind}_a(b)$ vai $\text{ind}(b)$. 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 $\varphi(m)$ daudzkārtņim, tāpēc ka

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

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

1.1. piemērs.

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

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 $a \equiv g^s \pmod{m}$, tāpēc indekss eksistē.

2. Ja g ir primitīvas sakne, tad visas tās pakāpes ar kāpinātājiem $0, 1, \dots, \varphi(m)$ ir dažādas un $g^{\varphi(m)} \equiv 1 \pmod{m}$. Ja $g^{s_1} \equiv g^{s_2} \pmod{m}$, tad $g^{s_1 - s_2} \equiv 1 \pmod{m}$, 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;
2. $\text{ind}_g(ab) \equiv \text{ind}_g(a) + \text{ind}_g(b) \pmod{\varphi(m)}$;
3. $\text{ind}_g(a^k) \equiv k \cdot \text{ind}_g(a) \pmod{\varphi(m)}$;
4. $\text{ind}_g\left(\frac{a}{b}\right) \equiv \text{ind}_g(a) - \text{ind}_g(b) \pmod{\varphi(m)}$;
5. $\text{ind}_g(a) \equiv \text{ind}_g(h) \cdot \text{ind}_h(a) \pmod{\varphi(m)}$, kur h arī ir primitīva sakne pēc moduļa m ;

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

$$\text{ind}_g(a_1) = \text{ind}_g(a_2) + \varphi(m) \cdot l$$

un

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

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

2.

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

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

3.,4. - pierāda līdzīgi kā 2.

5.

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



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

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

saskaņā ar šādu algoritmu:

1. atrast primitīvu sakni $g \pmod{m}$,
2. atrast a indeksu pie bāzes g , apzīmēsim to ar α ,
3. pieņemt, ka $x \equiv g^y \pmod{m}$, citiem vārdiem sakot, veikt nezināmo substitūciju $x \rightarrow y$,
4. izteikt vienādojuma abas puses kā g pakāpes, iegūt vienādojumu

$$g^{ky} \equiv g^{\alpha} \pmod{m},$$

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

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

vai Diofanta vienādojumu sistēmu pēc moduļa m

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

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 $a \pmod{m}$ pārstāvji ir visi veseli x , kuriem izpildās nosacījums

$$x \equiv a \pmod{m}.$$

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

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

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

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

tad jebkurš skaitlis a' tāds, ka

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

arī apmierina šo sistēmu.

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

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

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 veseli atrisinājumu veido atlikumu klases pēc moduļa $MKD(m_1, \dots, m_k)$. Šī iemesla dēļ dažreiz modulāras sistēmas atrisinājumu definē kā atlikumu klasi pēc šī moduļa.

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

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

tad jebkura virkne (a'_1, \dots, a'_n) , kur $a_j \equiv a'_j \pmod{MKD(m_1, \dots, m_k)}$, 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. Ja $f(x) \equiv 0 \pmod{m}$, tad $f(x) = mq$, 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 $f(x) \equiv 0 \pmod{m}$, tad

$f(x) = mq$ un $d \cdot f_1(x) = d \cdot m_1q$, tātad $f_1(x) = m_1q$. Esam ieguvuši vienādojumu $f_1(x) \equiv 0 \pmod{m_1}$. ■

1.2. piemērs. $x + 2 \equiv 0 \pmod{5}$ tad un tikai tad, ja $x + 2 - 2 \equiv 0 - 2 \pmod{5}$ un $x \equiv 3 \pmod{5}$.

$4x + 2 \equiv 0 \pmod{5}$ tad un tikai tad, ja $4(4x + 2) \equiv 4 \cdot 0 \pmod{5}$ un $x \equiv 2 \pmod{5}$.

$2x \equiv 6 \pmod{8}$ tad un tikai tad, ja $x \equiv 3 \pmod{4}$. Ja gribam izteikt atrisinājumu kā klases mod 8, tad $x \in \pi_{8,4}^{-1}(3) = \{3, 7\}$.

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

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

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

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

Bet ne otrādi. Vienādojumam

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

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

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

Vienādojuma $3x \equiv 2 \pmod{15}$ atrisinājums ir

$$x \equiv 3^7 2 \equiv 11 \pmod{15}.$$

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

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

atsisinājumu 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 $d > 1$, $a = a_1d$, $m = m_1d$, kur $LKD(a_1, m_1) = 1$. Vienādojums $ax \equiv b \pmod{m}$ ir ekvivalents vienādojumam

$$(a_1d)x = b + (m_1d)q$$

ar kādu $q \in \mathbb{Z}$. Redzam, ka $b \equiv 0 \pmod{d}$.

2. Ja $b \equiv 0 \pmod{d}$, tad $b = b_1d$. Vienādojums

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

ir ekvivalents ar vienādojumu

$$(a_1d)x \equiv b_1d \pmod{m_1d}.$$

Izdalot visus locekļus un moduli ar d , iegūsim ekvivalentu vienādojumu

$$a_1x \equiv b_1 \pmod{m_1}.$$

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

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



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

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

1.5. Vienādojumi atlikumu gredzenos pēc pirm-skaitļa moduļa

1.9. piezīme. $\mathbb{Z}/p\mathbb{Z}$ ir lauks (visi nenulles elementi ir invertējami). Lauki ir arī, piemēram, \mathbb{Q} , \mathbb{R} , \mathbb{C} . Risināt vienādojumus un vienādojumu sistēmas var līdzīgi kā reālos skaitļos. Piemēram, lineārām sistēmām var izmantot Gausa metodi, ir spēkā Bezū teorēma.

Atšķirības:

- laukā $\mathbb{Z}/p\mathbb{Z}$ ir galīgs skaits elementu - var atrast visus atrisinājumus ar izsmēlošo pārlasi;
- ne vienmēr eksistē saknes - lietderīgi izmantot primitīvās saknes un indeksus.

1.10. piezīme. Ja koeficients pie lielākās nezināmā pakāpes nav kongruents ar 0, tad ar to var izdalīt.

1.6. teorēma. Ja p ir pirmskaitlis un

$$f_1(x)f_2(x) \equiv 0 \pmod{p},$$

tad vai nu $f_1(x) \equiv 0 \pmod{p}$, vai arī $f_2(x) \equiv 0 \pmod{p}$.

PIERĀDĪJUMS Tas seko no agrāk pierādīta fakta, ka atlikumu gredzenā pēc pirmskaitļa moduļa nav nulles dalītāju - ja $ab \equiv 0 \pmod{p}$, tad vai nu $a \equiv 0$, vai arī $b \equiv 0$. ■

Polinomu $f(x)$ sauksim par *sadalāmu pēc moduļa p (reducible)*, ja

$$\bar{f}(x) \equiv f_1(x)f_2(x) \pmod{p},$$

kur $f_i(x)$ ir nekonstanti polinomi. Pretējā gadījuma polinomu sauksim par *nesadalāmu (irreducible)*.

1.6. piemērs. $x^2 + 1 \equiv (x + 1)^2 \pmod{2}$. $x^2 + x + 1 \pmod{2}$ ir nesadalāms, bet $x^2 + x + 1 \equiv (x + 2)^2 \pmod{3}$.

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

Par polinoma $f(x) = \sum_{i=1}^n a_i x^i$ Fermā redukciju ar moduli p sauksim polinomu

$$\hat{f}_p(x) = \sum_{i=1}^n a_i x^{i \bmod p-1}.$$

1.7. piemērs. Ja $f(x) = x^6 + x^5 + x + 1$, tad

$$\hat{f}_3(x) = x^0 + x^1 + x + 1 \equiv 2x + 2.$$

1.7. teorēma. Jebkurš algebrisks vienādojums ar vienu nezināmo pēc moduļa p ir ekvivalents vienādojumam, kura pakāpe nepārsniedz $p - 1$.

PIERĀDĪJUMS Pieņemsim, ka $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$.
Ja $a_0 \not\equiv 0 \pmod{p}$, tad $x \not\equiv 0 \pmod{p}$ un

$$x^i \equiv x^{i \bmod p-1} \pmod{p}.$$

Redzam, ka

$$f(x) \equiv \hat{f}(x) \pmod{p}.$$

Ja $a_0 \equiv 0 \pmod{p}$, tad

$$f(x) \equiv x^r g(x),$$

kur polinoma $g(x)$ brīvais loceklis nav kongruents ar nulli. $f(x)$ atrisinājumu kopa ir 0 un $\hat{g}(x) \equiv 0$ atrisinājumu kopas apvienojums, tāpēc vienādojums $f(x) \equiv 0 \pmod{p}$ ir ekvivalents ar vienādojumu $x\hat{g}(x) \equiv 0 \pmod{p}$, kura pakāpe nepārsniedz $p - 1$. ■

1.11. piezīme. Algoritms vienādojuma $f(x) \equiv 0 \pmod{p}$ risināšanai:

1. veikt polinoma $f(x)$ pārveidošanu par ekvivalentu polinomu

$$\tilde{f}(x) = x^s \cdot g(x),$$

kur $s \in \{0, 1\}$ $g(0) \not\equiv 0 \pmod{p}$ un $g(x)$ pakāpe nepārsniedz $p - 2$;

2. mēģināt sadalīt reizinātājos $g(x) \pmod{p}$ - izteikt to formā

$$g(x) \equiv g_1(x) \dots g_l(x) \pmod{p};$$

3. katram i atrisināt vienādojumu

$$g_i(x) \equiv 0 \pmod{p}$$

un atrast visu atrisinājumu apvienojumu.

1.8. piemērs. Atrisināsim vienādojumu

$$x^7 + 8x^5 - 2x^3 + x - 1 \equiv 0 \pmod{5}.$$

Reducējot koeficientus mod 5, iegūsim

$$x^7 + 3x^5 + 3x^3 + x + 4 \equiv 0 \pmod{5}.$$

Pielietojot Fermā teorēmu, iegūsim ekvivalento vienādjumu

$$x^3 + 3x + 3x^3 + x + 4 \equiv 4x^3 + 4x + 4 \equiv x^3 + x + 1 \equiv 0 \pmod{5}.$$

Sadalīsim kreiso pusi reizinātājos:

$$x^3 + x + 1 \equiv (x + 1)(x^2 + 4x + 2) \equiv 0 \pmod{5}.$$

Redzam, ka saskaņā ar Bezū teorēmu ir viena sakne $x \equiv 4 \pmod{5}$.
Veselos skaitļos atrisinājumu kopa ar $\{5t + 4 | t \in \mathbb{Z}\}$.

1.12. piezīme. Algoritms lineāras modulāru vienādojumu sistēmas atrisināšanai ar fiksētu moduli p - pielietot Gausa metodi.

1.9. piemērs. Atrisināsim sistēmu

$$\begin{cases} x_1 - x_2 - x_3 \equiv 1 \pmod{3} \\ 2x_1 + x_2 - 2x_3 \equiv 2 \pmod{3} \\ 2x_1 - 2x_2 - x_3 \equiv 2 \pmod{3} \end{cases},$$

Šo pašu sistēmu var atrisināt pēc cita moduļa, piemēram, 2 un iegūt citu rezultātu.

1.13. piezīme. Spēle *All Lights*.

1.14. piezīme. Nelineāras vienādojumu sistēmas pēc fiksēta pirmskaitļa moduļa risināt ir grūti, tāpat kā reālos skaitļos. Ja nekas cits neatliek, var izmantot izsmeļošo pārlasi.

2. 7.mājasdarbs

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 $\text{ind}_g(a) \pmod{\varphi(p)}$. Sastādīt indeksu matricu pirmskaitlim 7.
2. Atrisiniet vienādojumu $15x \equiv 40 \pmod{35}$.
3. Atrisiniet vienādojumu $8x^2 + 2008 \equiv 0 \pmod{3}$.
4. Izmantojot Gausa metodi atrisiniet lineāru vienādojumu sistēmu

$$\begin{cases} x_1 + 2x_2 + x_3 \equiv 1 \pmod{3} \\ x_2 + 2x_3 + x_4 \equiv 2 \pmod{3} \end{cases},$$