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

Studiju kurss

Veselo skaitļu teorija

10.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Vienādojumu risināšana atlikumu gredzenos - pamatfakti un vienkāršākie speciālgadījumi

1.1. Pamatfakti

1.1.1. Modulārās Diofanta sistēmas

Atrisināt Diofanta vienādojumu mod m

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

vai Diofanta vienādojumu sistēmu pēc mod 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 vienādojumus 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.

1.1. 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

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

■

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

1.2. 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

$$a_i \equiv a'_i \pmod{MKD(m_1, ..., m_k)}, \forall j$$

arī apmierina šo sistēmu.

1.1.2. Redukcijas

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

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

Visu šādu veselo skaitļu kopu $\mathcal{C}_m(a)$ var interpretēt kā atlikumu klases a inverso attēlu attiecībā uz reducēšanas mod 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 modulāro Diofanta sistēmu risināšanas beigās interpretēsim kā redukcijas inverso attēlojumu.

1.4. piezīme. Atzīmēsim vēl vienu lietderīgu funkciju. Ja $k|m$, tad

- $a_1 \equiv a_2 \pmod{\text{m}} \implies a_1 \equiv a_2 \pmod{\text{k}}$;
- katra ekvivalences klase mod k ir vairāku mod m ekvivalences klašu apvienojums, piemērs - $\bar{0}$ klase mod 2 (pāra skaitļi) ir klašu $\bar{0}$ un $\bar{2}$ mod 4 apvienojums.

Tādējādi ir definēta funkcija

$$\pi_{m,k} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z},$$

kas katrai atlikuma klasei x mod m, kuru pārstāv vesels skaitlis $\tilde{x}$ piekārto $\pi_k(\tilde{x})$. Citiem vārdiem sakot,

$$\pi_{m,k}(x) = \pi_k(\tilde{x}),$$

kur $\tilde{x} \in \pi_m^{-1}(x)$. Šādu funkciju sauksim par *relatīvo redukciju no* m *uz* k. Tāpat kā redukcijas funkcijai, arī relatīvajai redukcijai var interpretēt inverso attēlojumu.

1.2. teorēma.

1. Klases $\pi_{m,k}^{-1}(x)$ dažādo pārstāvju kopa var tikt ņemta vienāda ar
$$\{x, x + k \cdot 1, x + k \cdot 2, ..., x + k \cdot (\frac{m}{k} - 1)\}.$$
2. $|\pi_{m,k}^{-1}(a)| = \frac{m}{k}$.

PIERĀDĪJUMS

1. x klase mod k ir skaitļi formā $x + kt$. Izdalīsim t ar $\frac{m}{k}$:
$$t = q \cdot \frac{m}{k} + r,$$

kur $0 \leq r < \frac{m}{k}$. Redzam, ka

$$x + kt = x + k(q \cdot \frac{m}{k} + r) = x + qm + kr = (x + kr) + qm.$$

Redzam, ka katrs klases $\pi^{-1}_{m,k}(x)$ pārstāvis ir izsakāms vēlamajā formā.

Pierādīsim, ka visas klases formā $x + kr$ ir dažādas. Ja

$$x + kr_1 \equiv x + kr_2 \pmod{\mathrm{m}},$$

tad $k(r_1 - r_2) = mt'$, bet $|r_1 - r_2| < \frac{m}{k}$, tātad $t' = 0$ un $r_1 = r_2$.

2. Seko no pirmā apgalvojuma. ■

1.1. piemērs. $\pi_{4,2}(\bar{0}) = \bar{0}$, $\pi_{4,2}(\bar{1}) = \bar{1}$, $\pi_{4,2}(\bar{2}) = \bar{0}$, $\pi_{4,2}(\bar{3}) = \bar{1}$. $\pi^{-1}_{6,2}(\bar{0}) = \{\bar{0}, \bar{2}, \bar{4}\}$, $\pi^{-1}_{6,2}(\bar{1}) = \{\bar{1}, \bar{3}, \bar{5}\}$.

1.5. piezīme. Relatīvā redukcija ir grupu un pat gredzenu homomorfizms (saglabā abas operācijas).

Relatīvās redukcijas inverso attēlojumu izmanto, ja atrisinājums tiek tiek atrast mod k, bet mūs interesē atrisinājumu mod m, kur $k|m$.

1.6. piezīme. Ja sākotnēji vienādojumi ir doti ar veseliem koeficientiem, tad reducējot vienādojumu mod m, ērti ir reducēt arī koeficientus, piemēram:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0 \equiv$$
$$\overline{a}_n x^n + \overline{a}_{n-1} x^{n-1} + ... + \overline{a}_0 \equiv 0 \pmod{\text{m}}.$$

Šādu operāciju polinomu kopā sauksim par *polinoma redukciju mod* m un apzīmēsim ar $\overline{f}(x)$.

1.2. Modulāro vienādojumu ekvivalentie pārveidojumi un moduļa maiņa

1.3. 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 koeficientus un moduli ar nenulles veselu skaitli k;
5. ja katrs vienādojuma loceklis un modulis dalās ar d, tad var izdalīt visus koeficientus un moduli ar d;

PIERĀDĪJUMS
1.-3. Acīmredzami.

4.-5. $f(x) \equiv 0 \pmod{\text{m}} \implies f(x) = mq$, tātad $kf(x) = (mk)q$. Seko, ka

$$(kf)(x) \equiv 0 (\text{mod } km).$$

Ja x apmierina sākotnējo sistēmu, tad tas apmierina arī jauno un otrādi.

Ja katrs $f(x)$ koeficients 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 $f_1(x) \equiv 0 \pmod{m_1}$. Ja x apmierina sākotnējo sistēmu, tad tas apmierina arī jauno un otrādi. ■

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 $(x_1, ..., x_n)$ ir vesels atrisinājums vienādojumam

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

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

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

Bet ne otrādi. Vienādojumam

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

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.

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

1.3. 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

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

1.4. teorēma.

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

PIERĀDĪJUMS
1. $d = 1 \implies b \equiv 0 \pmod{\text{d}}$.
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. $b \equiv 0 \pmod{d} \implies b = b_1 d$. Vienādojums

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

ir ekvivalents vienādojumam

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

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

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

■

1.9. piezīme. Ja ir nepieciešamība rakstīt atrisinājumu kopu sākotnējā

moduļa m terminos, tad

$$x = \pi^{-1}_{m,\frac{m}{d}}((\frac{a}{d})^{-1}(\frac{b}{d})) =$$
$$\{a_1^{-1}b_1, a_1^{-1}b_1 + m_1, ..., a_1^{-1}b_1 + m_1(d-1)\}.$$

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

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

1.4. Vienādojumi atlikumu gredzenos pēc pirmskaitļa moduļa

1.10. 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 reālo skaitļo gadījumam. Piemēram, lineārām sistēmām var izmantot Gausa metodi, ir spēkā Bezū teorēma.

1.11. piezīme. Atgādinājums par Bezū teorēmu: a ir vienādojuma $f(x) = 0$ atrisinājums tad un tikai tad, ja $(x - a)|f(x)$ jeb

$$f(x) = (x - a)g(x).$$

Ar ko $\mathbb{Z}/p\mathbb{Z}$ atšķiras no $\mathbb{Q}$,$\mathbb{R}$ vai $\mathbb{C}$:

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

1.5. teorēma.

$f_1(x)f_2(x) \equiv 0 \pmod{\text{p}} \implies f_1(x) \equiv 0 \pmod{\text{p}} \vee f_2(x) \equiv 0 \pmod{\text{p}}.$

PIERĀDĪJUMS Tas seko no agrāk pierādīta fakta, ka atlikumu gredzenā pēc pirmskaitļa moduļa nav nulles dalītāju -

$$ab \equiv 0 \pmod{\text{p}} \implies a \equiv 0 \vee b \equiv 0.$$

■

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

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

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

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

$$\hat{f}_p(x) = \sum_{i=0}^{n} a_i x^{i \bmod p-1}.$$

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

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

1.12. piezīme. Fermā redukciju var interpretēt arī polinomu dalīšanas terminos.

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

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

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

Redzam, ka

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

$a_0 \equiv 0 \pmod{\text{p}} \implies f(x) \equiv x^r g(x)$, kur polinoma $g(x)$ brīvais loceklis nav kongruents ar nulli. $f(x)$ atrisinājumu kopa ir 0 un vienādojuma $\hat{g}_p(x) \equiv 0 (\text{mod } p)$ atrisinājumu kopas apvienojums, tāpēc vienādojums $f(x) \equiv 0 \pmod{\text{p}}$ ir ekvivalents vienādojumam

$$x\hat{g}(x) \equiv 0 \pmod{\text{p}},$$

kura pakāpe nepārsniedz $p-1$. ■

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

1. izmantojot Fermā redukciju veikt polinoma $f(x)$ pārveidošanu par ekvivalentu polinomu
$$\tilde{f}(x) = x^s \cdot g(x),$$
kur $s \in \{0, 1\}$ $g(0) \not\equiv 0 \pmod{\text{p}}$ un $g(x)$ pakāpe nepārsniedz $p - 2$;
2. mēģināt sadalīt reizinātājos $g(x) \pmod{\text{p}}$ - izteikt to formā
$$g(x) \equiv g_1(x)...g_l(x) \pmod{\text{p}};$$
3. katram i atrisināt vienādojumu
$$g_i(x) \equiv 0 \pmod{\text{p}}$$
un atrast visu atrisinājumu apvienojumu.

1.8. piemērs. Atrisināsim vienādojumu

$$x^7 + 8x^5 - 2x^3 + x - 1 = 0 \pmod 5.$$

Reducējot koeficientus mod 5, iegūsim

$$x^7 + 3x^5 + 3x^3 + x + 4 = 0 \pmod 5.$$

Pielietojot Fermā redukciju, iegūsim ekvivalento vienājumu

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

Redzam, ka vienādojumam nav atrisinājumu.

1.14. 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.

1.15. piezīme. Ar Gausa metodes palīdzību atrisiniet spēli *All Lights*.

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

2. 10.mājasdarbs

10.1 Atrisiniet vienādojumus

(a) $15x \equiv 40 \pmod{35}$;
(b) $44x \equiv 77 \pmod{33}$;
(c) $540x \equiv 200 \pmod{1465}$.

10.2 Atrisiniet vienādojumus:

(a) $8x^2 + 2008 \equiv 0 \pmod{3}$;
(b) $x^{2009} - 2008x^{2007} + 208x + 1 \equiv 0 \pmod{7}$;

10.3 Izmantojot Gausa metodi atrisiniet lineāru vienādojumu sistēmas

(a)

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

(b)

$$\begin{cases} x_1 - x_2 + x_3 \equiv 4 \pmod{5} \\ x_2 - x_3 + x_1 \equiv 3 \pmod{5} \\ x_3 - x_1 + x_2 \equiv 3 \pmod{5} \end{cases}.$$