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

Studiju kurss

Veselo skaitļu teorija

11.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis:

- apgūt modulāro vienādojumu teorijas pamatus un vienkāršākos speciālgadījumus.

Lekcijas kopsavilkums:

- modulārām vienādojumu sistēmām var noteikt pārveidojumus, kas nemaina to atrisinājumu kopu,
- modulāru lineāru vienādojumu ar vienu nezināmo var atrisināt izmantojot vienkāršākos faktus no modulārās aritmētikas,
- modulārajiem vienādojumiem mod p var pazemināt pakāpi līdz $p-1$,
- modulārajiem vienādojumiem mod p atrisinājumu skaits nepārsniedz vienādojuma pakāpi.

Svarīgākie jēdzieni: modulāra Diofanta sistēma, polinomu redukcija mod m, redukcijas un to inversie attēlojumi, Fermā redukcija.

Svarīgākie fakti un metodes: teorēma par modulāru Diofanta sistēmu atrisinājumiem, relatīvās redukcijas inversā attēlojuma īpašības, modulāro Diofanta sistēmu ekvivalentie pārveidojumi, lineāra vienādojuma ar vienu nezināmo risināšana, Lagranža teorēma, vienādojumu pakāpes samazināšana mod p.

1. Modulāro vienādojumu risināšana - pamatfakti un vienkāršākie speciālgadījumi

1.1. Pamatfakti

1.1.1. Modulārās Diofanta sistēmas

Atrisināt vienādojumu

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

vai vienādojumu sistēmu

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

nozīmē to atrisināt *veselos skaitļos* (gredzenā $\mathbb{Z}$).

Šādus vienādojumus un vienādojumu sistēmas sauc 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 $a \in \mathbb{Z}$ 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 $\forall\ a' \in \mathbb{Z}$ tāds, ka

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

arī apmierina šo sistēmu.

PIERĀDĪJUMS
$a \equiv a' \pmod{MKD(m_1, ..., m_k)} \Longrightarrow \forall\ i$ izpildās

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

$\forall\ j\ m_j | MKD(m_1, ..., m_k) \Longrightarrow f_i(a) \equiv f_i(a') \equiv 0 \pmod{m_j}$. ■

1.1. piezīme. Seko, ka modulārās Diofanta sistēmas veselie atrisinājumi veido atlikumu klases mod $MKD(m_1, ..., m_k)$.

1.2. piezīme. Analoģisks apgalvojums ir spēkā, ja tiek risināta sistēma ar vairākiem nezināmiem: ja virkne $(a_1, ..., a_n) \in \mathbb{Z}^n$ 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.

1.3. piezīme. Ja sākotnēji vienādojumi ir doti ar veseliem koeficientiem, tad reducējot mod m, ir jāreducē arī koeficienti:

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

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

1.1.2. Redukcijas

Kā ir saistītas savā starpā atlikumu klases dažādiem moduļiem?

1.4. piezīme. Atlikumu klases a (mod m) pārstāvji ir visi $x \in \mathbb{Z}$:

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

Visu šādu veselo skaitļu kopa $\mathcal{C}_m(a)$ ir atlikumu klases a inversais attēls attiecībā uz reducēšanas mod m funkciju

$$\pi_m : \mathbb{Z} \to \mathbb{Z}_m.$$

Tādējādi $\mathcal{C}_m(a) = \pi_m^{-1}(a)$.

1.5. piezīme. $k|m \Longrightarrow$

- $a_1 \equiv a_2$ (mod m) $\Longrightarrow$ $a_1 \equiv a_2$ (mod 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 (*relatīvā redukcija no m uz k*)

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

kas ∀ atlikuma klasei $[x]$ mod m piekārto $\pi_k(x)$. Citiem vārdiem sakot,

$$\pi_{m,k}([x]) = \pi_k(x).$$

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 kā

$$\{x, x + k \cdot 1, x + k \cdot 2, ..., x + k \cdot (\frac{m}{k} - 1)\}.$$

2. $|\pi_{m,k}^{-1}(a)| = \frac{m}{k}$.

PIERĀDĪJUMS

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

$$t = q \cdot \frac{m}{k} + r, \text{ kur } 0 \le r < \frac{m}{k}.$$

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

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

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

$$x + kr_1 \equiv x + kr_2 \pmod{m} \Longrightarrow k(r_1 - r_2) = mt',$$

bet $|r_1 - r_2| < \frac{m}{k}$ $\Longrightarrow$ $t' = 0$ un $r_1 = r_2$.

2. Seko no pirmā apgalvojuma. ■

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

1.6. piezīme.

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

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 polinoma koeficients un modulis dalās ar d, tad izdalīt visus koeficientus un moduli ar d.

PIERĀDĪJUMS
1.-3. Acīmredzami.

4.-5. $f(x) \equiv 0 \pmod{m} \Longrightarrow f(x) = mq \Longrightarrow kf(x) = (mk)q$

$\implies (kf)(x) \equiv 0(\text{mod } km)$. Ja x apmierina sākotnējo sistēmu, tad tas apmierina arī jauno un otrādi.

Ja katrs $f(x)$ koeficients un m dalās ar d un $f(x) \equiv 0 \ (\text{mod m})$, tad $f(x) = mq$ un $d \cdot f_1(x) = d \cdot m_1 q \implies f_1(x) = m_1 q$. Esam ieguvuši vienādojumu $f_1(x) \equiv 0 \ (\text{mod } m_1)$. Ja x apmierina sākotnējo sistēmu, tad tas apmierina arī jauno un otrādi. ■

1.2. piemērs. $x + 2 \equiv 0 \ (\text{mod } 5) \iff x + 2 - 2 \equiv 0 - 2 \ (\text{mod } 5)$ un $x \equiv 3 \ (\text{mod } 5)$.

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

$2x \equiv 6 \ (\text{mod } 8) \iff x \equiv 3 \ (\text{mod } 4)$. 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

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

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

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

Bet ne otrādi. Vienādojumam

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

var būt vairāk atrisinājumu nekā sākotnējam vienādojumam. Šo īpašību izmanto kontrapozitīvajā formā: nav atrisinājumu mod k $\Longrightarrow$ 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.

$x^4+1 \equiv 0$ (mod 27) $\Longrightarrow$ $x^4+1 \equiv 0$ (mod 3). Pēdējam vienādojumam nav atrisinājumu, tātad to nav arī sākotnējam vienādojumam.

1.3. Lineārs vienādojums ar vienu nezināmo

1.8. piezīme. Vienādojums

$$ax \equiv b \pmod{m}, \text{ kur } LKD(a, m) = 1,$$

ir viegli atrisināms, jo eksistē $a^{-1} \pmod{m}$:

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

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

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

1.4. teorēma. Apzīmēsim $LKD(a, m)$ ar d.

1. $b \not\equiv 0 \pmod{d} \implies$ vienādojumam

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

neeksistē atrisinājumi,

2. $b \equiv 0 \pmod{d} \implies$ vienādojuma

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

atrisinājumu kopa ir klase $(\frac{a}{d})^{-1}(\frac{b}{d}) \pmod{(\frac{m}{d})}$.

PIERĀDĪJUMS
1. $d = 1 \implies b \equiv 0 \pmod{\mathrm{d}}$.
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 $q \in \mathbb{Z} \implies b \equiv 0 \pmod{d}$.

2. $b \equiv 0 \pmod{\mathrm{d}} \implies b = b_1 d$. Vienādojums

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

ir ekvivalents vienādojumam

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

Izdalot visus koeficientus un moduli ar d, iegūsim ekvivalentu vienādojumu

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

$LKD(a_1, m_1) = 1 \implies$ šim vienādojumam eksistē viena atrisinājumu klase

$$x \equiv a_1^{-1} b_1 \pmod{m_1} = (\frac{a}{d})^{-1}(\frac{b}{d}) \pmod{(\frac{m}{d})}.\blacksquare$$

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.

$6x \equiv 9 \pmod{15} \iff 2x \equiv 3 \pmod 5$, kura atrisinājums ir

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

2. Modulārie vienādojumi ar pirmskaitļa moduļa

2.1. Pamatfakti

2.1. piezīme. $\mathbb{Z}_p$ 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.

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

2.1. piemērs. Atrisināsim sistēmu

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

2.3. piezīme. Atgādinājums par Bezū teorēmu: a ir vienādojuma $f(x) = 0$ atrisinājums $\iff (x-a)|f(x) \iff f(x) = (x-a)g(x)$.

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

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

2.1. teorēma.

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

PIERĀDĪJUMS Atlikumu gredzenā mod p nav nulles dalītāju -

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

Polinomu $f(x)$ sauc par *dalāmu mod p*, ja

$$f(x) \equiv \bar{f}(x) \equiv f_1(x) f_2(x) \pmod{p}, \text{ kur } f_i \text{ - nekonstanti.}$$

Pretējā gadījuma polinomu sauc par *nedalāmu*.

2.2. piemērs. $x^2 + 1 \equiv (x+1)^2 \pmod{2}$.
$x^2 + x + 1 \pmod{2}$ ir nedalāms, bet $x^2 + x + 1 \equiv (x+2)^2 \pmod{3}$.
$x^2 + x + 3 \equiv (x+2)(x+4) \pmod{5}$.

2.2. Lagranža teorēma

Apzīmēsim visu viena argumenta polinomu kopu ar koeficientiem gredzenā R kā $R[X]$. Polinoma $f \in R[X]$ pakāpi apzīmēsim kā $\deg(f)$.

2.2. teorēma. (*Lagranža teorēma*) $f \in \mathbb{Z}[X]$, $\deg(f) = n \geq 1$, $p \in \mathbb{P}$. Tad vienādojumam

$$f(X) \equiv 0 \pmod{p}$$

ir ne vairāk kā n dažādi atrisinājumi mod p.

PIERĀDĪJUMS Matemātiskā indukcija ar parametru n.

Indukcijas bāze $\deg(f) = 1 \implies$ vienādojums ir

$$f(X) = a_1 X + a_0 \equiv 0 \pmod{p}.$$

Tam ir tieši viens atrisinājums

$$X \equiv a_1^{-1}(-a_0) \pmod{p}.$$

Indukcijas solis Pieņemsim, ja apgalvojums ir spēkā, ja $\deg(f) \leq i-1$. Apskatīsim polinomu ar pakāpi i

$$f(X) = a_i X^i + a_{i-1} X^{i-1} + \ldots + a_1 X + a_0 = \sum_{j=0}^{i} a_j X^j.$$

$f(X) \equiv 0 (\text{mod } p)$ nav atrisinājumu $\Longrightarrow$ indukcijas solis ir pierādīts.

Ja $f(X) \equiv 0 (\text{mod } p)$ ir atrisinājums X_0, tad

$$f(X) \equiv f(X) - f(X_0) \equiv \sum_{j=0}^{i} a_j X^j - \sum_{j=0}^{i} a_j X_0^j = \sum_{j=0}^{i} a_j (X^j - X_0^j) \text{ (mod p)}.$$

Izmantosim vienādību

$$X^j - X_0^j = (X - X_0)(X^{j-1} + X^{j-2} X_0 + \ldots + X \cdot X_0^{j-2} + X_0^{j-1}).$$

Redzam, ka

$$f(X) \equiv f(X) - f(X_0) \equiv (X - X_0) g(X) \text{ (mod p)},$$

kur $\deg(g) \leq i - 1$. Tādējādi vienādojumam

$$f(X) - f(X_0) \equiv (X - X_0) g(X) \equiv 0 \text{ (mod p)}$$

atrisinājumu skaits nepārsniedz i - viens atrisinājums X_0 un vēl ne vairāk kā $i - 1$ vienādojuma $g(X) \equiv 0$ (mod p) atrisinājumi.$\blacksquare$

2.3. Pakāpes samazināšana

Vai ir iespējams samazināt polinoma pakāpi nemainot atrisinājumu kopu? Pamatideja: izmantosim Fermā teorēmu - $x^p \equiv x (\mathrm{mod}\ p)$.

Par polinoma $f(X) = \sum_{i=1}^{n} a_i X^i$ *Fermā redukciju mod p* sauksim polinomu $\hat{f}_p$, ko iegūst no f aizvietojot X^p ar X tik ilgi, kamēr iegūst polinomu ar pakāpi ne lielāku kā $p-1$.

2.3. piemērs. $f(X) = X^6 + X^5 + X + 1$, $\hat{f}_3(X) = X^2 + 2X + 1$.

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

2.3. teorēma. Jebkurš algebrisks vienādojums ar vienu nezināmo mod p ir ekvivalents vienādojumam, kura pakāpe nepārsniedz $p-1$.

PIERĀDĪJUMS
Dots vienādojums $f(X) \equiv 0 (\mathrm{mod}\ p)$. Atradīsim $\hat{f}_p(X)$.

$f(X) \equiv 0(\text{mod } p) \iff \hat{f}_p(X) \equiv 0(\text{mod } p)$ saskaņā ar Fermā teorēmu. ■

2.5. piezīme. Algoritms vienādojuma $f(X) \equiv 0$ (mod p) risināšanai:

1. atrast f Fermā redukciju $\hat{f}_p$,
2. mēģināt sadalīt reizinātājos $\hat{f}_p(X)$ (mod p) - izteikt to formā
$$\hat{f}_p(X) \equiv g_1(X)...g_l(X) \text{ (mod p)};$$
3. katram i atrisināt vienādojumu
$$g_i(X) \equiv 0 \text{ (mod p)}$$
un atrast visu atrisinājumu apvienojumu.

2.4. piemērs. Atrisināsim vienādojumu
$$X^7 + 8X^5 - 2X^3 + X - 1 = 0 \text{ (mod 5)}.$$
Reducējot koeficientus mod 5, iegūsim
$$X^7 + 3X^5 + 3X^3 + X + 4 = 0 \text{ (mod 5)}.$$

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.

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

3. 11.mājasdarbs

11.1 Atrast

(a) $\pi_{8,2}^{-1}(1)$,
(b) $\pi_{20,4}^{-1}(3)$,
(c) $\pi_{77,7}^{-1}(2)$.

11.2 Atrisiniet vienādojumus

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

11.3 Atrisiniet vienādojumus:

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

11.4 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)

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

3.1. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

11.5 Izmantojot modulārās vienādojumu sistēmas, atrisināt spēles "All Lights" uzdevumu.