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

Studiju kurss

SKAITĻU TEORIJA

9.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

1. Modulāro vienādojumu risināšana - pamatfakti un vienkāršākie speciālgadījumi **5**
1.1. Pamatfakti 5
1.1.1. Modulāro sistēmu risināšana 5
1.1.2. Atlikumu klases kā atrisinājumu kopas 6
1.1.3. Modulāro vienādojumu ekvivalentie pārveidojumi un moduļa maiņa 8
1.1.4. Modulāro sistēmu ekvivalentā sašķelšana 10
1.2. Lineārs vienādojums ar vienu nezināmo 12

2. Modulārie vienādojumi ar pirmskaitļa moduli **14**
2.1. Pamatfakti 14
2.1.1. Atlikumu lauks 14
2.1.2. Lineāru sistēmu risināšana 15
2.2. Vienādojumi ar vienu nezināmo - pakāpes samazināšana 16
2.2.1. Polinomu dalīšana 16
2.2.2. Polinoma Fermā atlikums 20

3. 9.mājasdarbs **22**

3.1. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi 23

Lekcijas mērķis:

- apgūt modulāro vienādojumu teorijas pamatus un vienkāršākos speciālgadījumus.

Lekcijas kopsavilkums:

- modulāro vienādojumu atrisinājumu kopas ir atlikumu klašu apvienojumi,
- modulārām vienādojumu sistēmām var noteikt pārveidojumus, kas nemaina to atrisinājumu kopu,
- modulāru lineāru vienādojumu ar vienu nezināmo var atrisināt izmantojot vienkāršākos modulārās aritmētikas faktus,
- modulārajiem vienādojumiem mod p var pazemināt pakāpi līdz $p-1$,
- modulārajiem vienādojumiem mod p atrisinājumu skaits nepārsniedz vienādojuma pakāpi.

Svarīgākie jēdzieni: modulāra vienādojumu sistēma, polinomu redukcija mod m, Fermā redukcija.

Svarīgākie fakti un metodes: teorēmas par modulāru vienādojumu sistēmu atrisinājumiem, modulāro vienādojumu sistēmu ekvivalentie pārveidojumi, modulāro sistēmu ekvivalentā sašķelšana, lineāra vienādojuma ar vienu nezināmo risināšana, Lagranža teorēma, polinomu dalīšana ar atlikumu, vienādojumu pakāpes samazināšana mod p.

1. Modulāro vienādojumu risināšana - pamatfakti un vienkāršākie speciālgadījumi

1.1. Pamatfakti

1.1.1. Modulāro sistēmu risināšana

Atrisināt *modulāro vienādojumu*

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

vai *modulāro vienādojumu sistēmu*

$$\begin{cases} f_1(x_1, ..., x_n) \equiv 0 \ (\text{mod } m_1) \\ ... \\ f_l(x_1, ..., x_n) \equiv 0 \ (\text{mod } m_l) \end{cases}$$

parasti nozīmē to atrisināt *veselos skaitļos* (gredzenā $\mathbb{Z}$) - atrast $\forall$ virknes $(x_1, ..., x_n) \in \mathbb{Z}^n$, kas apmierina $\forall$ vienādojumu.

Parasti kā starprezultāti tiek iegūti rezultāti par nezināmo vērtībām reducējot tos pēc noteiktiem moduļiem.

Tādējādi risināšanas procesā nezināmie tiek uzskatīti par elementiem atlikumu gredzenos.

1.1.2. Atlikumu klases kā atrisinājumu kopas

1.1. teorēma.

$$\begin{cases} f_1(x) \equiv 0 \pmod{m_1} \\ ... \\ f_l(x) \equiv 0 \pmod{m_l} \end{cases}$$

atrisinājumu kopa ir (pilnu) klašu mod $M = MKD(m_1, ..., m_l)$ apvienojums.

PIERĀDĪJUMS Pieņemsim, ka $a \in \mathbb{Z}$ apmierina sistēmu.

$a \equiv a' \pmod{M} \implies \forall\, i\colon\ f_i(a) \equiv f_i(a') \pmod{M}$.

$\forall\, j\ m_j \mid M \implies f_i(a) \equiv f_i(a') \equiv 0 \pmod{m_j} \implies a'$ arī apmierina sistēmu $\implies$ visa a klase mod M apmierina sistēmu. ■

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

$$\begin{cases} f_1(x_1, ..., x_n) \equiv 0 \pmod{m_1}, \\ ..., \\ f_l(x_1, ..., x_n) \equiv 0 \pmod{m_l}, \end{cases}$$

tad $\forall$ virkne $(a'_1, ..., a'_n) \in \mathbb{Z}^n$, kur $a_i \equiv a'_i \pmod{M}, \forall\, i$, arī apmierina šo sistēmu, $M = MKD(m_1, ..., m_l)$.

1.1.3. Modulāro vienādojumu ekvivalentie pārveidojumi un moduļa maiņa

1.2. 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;
3. reizināt abas puses ar vienu un to pašu invertējamu atlikumu;
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. $f(x) \equiv 0 \pmod{\mathrm{m}} \iff f(x) = mq \iff kf(x) = (mk)q$ $\iff (kf)(x) \equiv 0 (\mathrm{mod}\ km)$.

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

1.1. 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 $x \equiv 2 \pmod 5$.

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

1.3. teorēma.

$$\begin{cases} f(x_1, ..., x_n) \equiv 0 \pmod{\text{m}} \\ k \mid m \end{cases} \implies f(x_1, ..., x_n) \equiv 0 \pmod{\text{k}}.$$

Bet ne otrādi.

PIERĀDĪJUMS Implikācija seko no kongruences pamatīpašībām.

Kontrpiemērs: $x \equiv 1(\text{mod } 2)$ atrisinājums ir $x = 3$, kas nav atrisinājums vienādojumam $x \equiv 1(\text{mod } 4)$. ■

1.2. piezīme. $\Big($nav atrisinājumu mod k un $k|m$ $\Big) \implies \Big($ nav atrisinājumu mod $m\Big)$.

1.2. piemērs. $x^4 + 1 \equiv 0 \ (\text{mod } 27) \implies x^4 + 1 \equiv 0 \ (\text{mod } 3)$. Pēdējam vienādojumam nav atrisinājumu $\implies$ to nav arī sākotnējam vienādojumam.

1.1.4. Modulāro sistēmu ekvivalentā sašķelšana

Viens vienādojums

1.4. teorēma. $m = p_1^{\alpha_1} ... p_k^{\alpha_k}$. Tad

$$f(x_1, ..., x_n) \equiv 0(\text{mod } m) \iff \begin{cases} f(x_1, ..., x_n) \equiv 0 \ (\text{mod } p_1^{\alpha_1}), \\ ..., \\ f(x_1, ..., x_n) \equiv 0 \ (\text{mod } p_k^{\alpha_k}). \end{cases}$$

PIERĀDĪJUMS Bija pierādīts agrāk.■

Sistēma

Ja ir dota modulāra sistēma ar vairākiem moduļiem, tad

1. $\forall$ vienādojumam tiek piekārtota ekvivalenta sašķeltā sistēma pēc pirmskaitļu pakāpju moduļiem,
2. visi vienādojumu tiek apvienoti vienā lielā sistēmā.

1.3. piezīme. Seko, ka ir svarīgi prast risināt vienādojumus mod p^{α}.

1.2. Lineārs vienādojums ar vienu nezināmo

Invertējams koeficients pie x

Vienādojums

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

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

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

Neinvertējams koeficients pie x

1.5. teorēma. $LKD(a,m) = d > 1$.

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

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

atrisinājumu kopa ir klase $\left(\frac{a}{d}\right)^{-1}\left(\frac{b}{d}\right)\ \left(\mathrm{mod}\ \left(\frac{m}{d}\right)\right)$.

PIERĀDĪJUMS

1. $\begin{cases} a \equiv 0(\mathrm{mod}\ d) \\ ax \equiv b(\mathrm{mod}\ m) \end{cases} \Longrightarrow ax \equiv b(\mathrm{mod}\ d) \Longrightarrow b \equiv 0(\mathrm{mod}\ d).$

2. Pieņemsim, ka $\begin{cases} a = a_1 d \\ m = m_1 d \end{cases}$, kur $LKD(a_1, m_1) = 1$.

$b \equiv 0\ (\mathrm{mod\ d}) \Longrightarrow b = b_1 d.$

$ax \equiv b\ (\mathrm{mod}\ m) \iff (a_1 d)x \equiv b_1 d\ (\mathrm{mod}\ m_1 d) \iff$ izdalot visus koeficientus un moduli ar d:

$$a_1 x \equiv b_1\ (\mathrm{mod}\ m_1).$$

$LKD(a_1, m_1) = 1 \Longrightarrow \exists$ viena atrisinājumu klase mod m_1

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

1.3. piemērs. Vienādojumam $4x \equiv 5 \pmod 8$ nav atrisinājumu.

$6x \equiv 9 \pmod{15} \iff 2x \equiv 3 \pmod 5$, $x \equiv 2^{-1}3 \equiv 4 \pmod 5 = \{4, 9, 14\} \pmod{15}$.

2. Modulārie vienādojumi ar pirmskaitļa moduli

2.1. Pamatfakti

2.1.1. Atlikumu lauks

Atlikumu gredzens mod p - $\mathbb{F}_p$ 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 skaitļu gadījumam.

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

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

2.1. teorēma.

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

PIERĀDĪJUMS Atlikumu gredzenā mod p nav nulles dalītāju - $ab \equiv 0(\text{mod } p) \implies a \equiv 0 \vee b \equiv 0$.■

2.1.2. Lineāru sistēmu risināšana

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

2.1. piemērs. Atrisināsim sistēmu

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

2.2. Vienādojumi ar vienu nezināmo - pakāpes samazināšana

Vai ir iespējams samazināt polinoma pakāpi nemainot atrisinājumu kopu? Pamatideja: izmantosim Fermā teorēmu -

$$x^p \equiv x (\mathrm{mod}\ p).$$

2.2.1. Polinomu dalīšana

Polinomu redukcijas solis

Kā samazināt polinoma pakāpi veicot kādu vienkāršu operāciju $f \longrightarrow f - dg$?

Apzīmēsim polinoma f locekli ar augstāko pakāpi ar $\mathcal{H}(f)$.

$f, g \in k[X]$, $\deg(f) \geq \deg(g)$. Definēsim operāciju polinomu kopā - *f redukciju ar g:*

$$(f, g) \mapsto \mathcal{R}_g(f) = f - \left(\frac{\mathcal{H}(f)}{\mathcal{H}(g)}\right) \cdot g.$$

2.2. piemērs. $\mathcal{R}_{X+1}(X^2+1) = (X^2+1) - X(X+1) = -X + 1.$

2.2. teorēma. $\deg\Big(\mathcal{R}_g(f)\Big) < \deg(f).$

PIERĀDĪJUMS

$$\begin{cases} \mathcal{H}(f) = a_n X^n \\ \mathcal{H}(g) = b_m X^m, n \geq m \end{cases} \Longrightarrow \frac{\mathcal{H}(f)}{\mathcal{H}(g)} = \frac{a_n}{b_m} \cdot X^{n-m}.$$

$$\mathcal{H}(\mathcal{R}_g(f)) = \mathcal{H}\Big(f - \frac{\mathcal{H}(f)}{\mathcal{H}(g)}g\Big) = \mathcal{H}\Big(f - \frac{a_nX^n}{b_mX^m}g\Big) =$$

$$\mathcal{H}\Big(f - \frac{a_n}{b_m}X^{n-m}(b_mX^m + ...)\Big) = \mathcal{H}(\underbrace{a_nX^n + ...}_{=f} - a_nX^n - ...).$$

Redzam, ka locekļi ar X^n saīsinās, tāpēc apgalvojums ir spēkā. ■

2.1. piezīme. Redzam, ka operācija $f \longrightarrow \mathcal{R}_g(f)$ samazina pakāpi.

Veicot pēc kārtas vairākas šādas operācijas iegūsim polinomu $r = f - dg$, kura pakāpe ir mazāka nekā $\deg(g)$. Tātad, ir iespējams atrast tādus polinomus d un r, ka

$$f = dg + r, \text{ kur } \deg(r) < \deg(g).$$

Teorēma

2.3. teorēma. (*viena argumenta polinomu dalīšana ar atlikumu*) k - lauks, $f, g \in k[X]$. Tad $\exists$ tieši viens polinomu pāris $d, r \in R[X]$:

1. $f = dg + r$,
2. $\deg(r) < \deg(g)$.

PIERĀDĪJUMS Veiksim pēctecīgi redukcijas $\mathcal{R}_g$ sākot ar f, tik ilgi, kamēr redukcija ir definēta. Iegūsim polinomu virkni

$$f \to \mathcal{R}_g(f) \to \mathcal{R}_g^2(f) \to \ldots \to \mathcal{R}_g^l(f), \text{ kur } \deg \mathcal{R}_g^l(f) < \deg g.$$

Tad $r = \mathcal{R}_g^l(f)$. ■

2.3. piemērs. $f = X^5 + X^2 + 1$, $g = X^2 + X + 1$ virs $\mathbb{R}$.

$$\mathcal{R}_g(f) = f - \left(\frac{\mathcal{H}(f)}{\mathcal{H}(g)}\right) \cdot g = f - X^3 \cdot g = -X^4 - X^3 + X^2 + 1;$$
$$\mathcal{R}_g^2(f) = \mathcal{R}_g(f_1) = f_1 - (-X^2) \cdot g = 2X^2 + 1;$$
$$\mathcal{R}_g^3(f) = \mathcal{R}_g(f_2) = f_2 - 2 \cdot g = -2X - 1.$$

$\mathcal{R}_g^4(f)$ nav definēts, jo $\deg\left(\mathcal{R}_g^3(f)\right) < \deg(g)$.

Rezultātā iegūsim, ka f var izteikt summas veidā, kurā viens locekļis ir g daudzkārtnis, bet otra locekļa pakāpe ir mazāka nekā $\deg(g)$:

$$f = (X^3 - X^2 + 2)g + (-2X - 1).$$

Vēlams izmantot dalīšanu "ar stūrīti".

2.2.2. Polinoma Fermā atlikums

Par polinoma $f(X) = \sum_{i=1}^{n} a_i X^i$ *Fermā atlikumu mod* p sauksim polinomu atlikumu $\widehat{f}_p$, ko iegūst dalot f ar $X^p - X$ mod p:

$$f(X) = d(X) \cdot (X^p - X) + \widehat{f}_p(X), \text{ kur } \deg(\widehat{f}_p) \leq p - 1.$$

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

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

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

$$f(X) \equiv d(X) \underbrace{(X^p - X)}_{\equiv 0} + \widehat{f}_p(X) \equiv 0 (\text{mod } p) \iff$$

$\widehat{f}_p(X) \equiv 0 (\text{mod } p)$. ■

2.5. piemērs. Atrisināsim vienādojumu

$$X^7 + 8X^5 - 2X^3 + X - 1 = 0 \ (\text{mod } 5).$$

Pielietojot Fermā atlikumu, iegūsim ekvivalento vienājumu
$X^3+3X+3X^3+X+4 \equiv 4X^3+4X+4 \equiv 0 \ (\text{mod } 5)$. - atrisinājumu nav.

3. 9.mājasdarbs

9.1 Atrast ekvivalentās sašķeltās sistēmas.

(a) $X^3 - X + 1 \equiv 0 (\text{mod } 10)$

(b) $\begin{cases} X^2 + 3X + 1 \equiv (\text{mod } 20) \\ X^4 + X^2 + 1 \equiv (\text{mod } 30) \end{cases}$

9.2 Atrisināt vienādojumus

(a) $15x \equiv 35 \ (\text{mod } 45)$;

(b) $44x \equiv 77 \ (\text{mod } 33)$;

(c) $540x \equiv 200 \ (\text{mod } 1465)$.

9.3 Izmantojot Gausa metodi atrisināt lineāru vienādojumu sistēmas

(a) $\begin{cases} x_1 + 2x_2 + x_3 \equiv 1 \ (\text{mod } 3) \\ x_2 + 2x_3 + x_4 \equiv 2 \ (\text{mod } 3) \end{cases}$,

(b) $\begin{cases} x_1 - x_2 + x_3 \equiv 4 \ (\text{mod } 5) \\ x_2 - x_3 + x_1 \equiv 3 \ (\text{mod } 5) \\ x_3 - x_1 + x_2 \equiv 3 \ (\text{mod } 5) \end{cases}$.

9.4 Izdalīt polinomus f ar g (atrast dalījumu un atlikumu).

(a) $f = X^4 + X + 1$, $g = X + 1$, virs $\mathbb{Q}$;
(b) $f = X^3 - \sqrt{2}X^2 - 1$, $g = X^2 + X - \sqrt{2}$, virs $\mathbb{R}$.

9.5 Atrisināt vienādojumus:

(a) $8x^2 + 2010 \equiv 0 \pmod 3$;
(b) $x^{10} - 2011x^9 + 2012x + 2013 \equiv 0 \pmod 7$.

3.1. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

9.6 Dots $f(X) = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ - polinoms ar veseliem koeficientiem, $n > 0$. Pierādīt, ka eksistē $m \in \mathbb{Z}$ tāds, ka vienādojumam $f(x) \equiv 0 (\mathrm{mod}\ m)$ ir atrisinājumi. Izstrādāt metodi mazākā šāda m atrašanai.

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