DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Studiju kurss

Veselo skaitļu teorija

8.lekcija (datoriķiem)

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Vienādojumu risināšana atlikumu kopās

1.1. Vienādojumi atlikumu gredzenos pēc pirmskaitļa moduļa

1.1. 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.

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

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

Atšķirības:

- laukā $\mathbb{Z}/p\mathbb{Z}$ ir galīgs skaits elementu - var atrast visus atrisinājumus ar izsmeļošo pārlasi;

- ne vienmēr eksistē saknes - lietderīgi izmantot primitīvās saknes un indeksus.

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

1.1. 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)*.

1.1. 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

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

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

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

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

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

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

Redzam, ka

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

Ja $a_0 \equiv 0$ (mod 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 $f(x) \equiv 0$ (mod p) ir ekvivalents ar vienādojumu $x\hat{g}(x) \equiv 0$ (mod p), kura pakāpe nepārsniedz $p-1$. ■

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

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

3. katram i atrisināt vienādojumu

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

   un atrast visu atrisinājumu apvienojumu.

1.3. 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 teorēmu, iegūsim ekvivalento vienādojumu

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

Šim vienādojumam nav atrisinājumu.

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

1.4. 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.

1.6. piezīme. Spēle *All Lights*.

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

1.2. Vienādojumi atlikumu gredzenos pēc pirmskaitļa pakāpes moduļa

1.8. piezīme. Modulāros vienādojumus pēc pirmskaitļa pakāpes p^α moduļa risināsim izmantojot šādu faktu: ja $a \equiv b \pmod{\mathrm{m}}$ un $m'|m$, tad $a \equiv b \pmod{m'}$. Konkrētāk, risināsim modulāros vienādojumus sākot no mazām p pakāpēm: no sākuma pēc moduļa p, pēc tam pēc p^2 u.t.t.

1.9. piezīme. No iepriekšējās piezīmes seko algoritms vienādojuma $f(x) \equiv 0 \pmod{p^\alpha}$ risināšanai:

1. Atrisināsim vienādojumu
$$f(x) \equiv 0 \pmod{\mathrm{p}},$$
iegūsim atrisinājumu kopu S_1.
2. Katram $s \in S_1$ ievietosim $x = s + px'$ vienādojumā
$$f(x) \equiv 0 \pmod{p^2},$$
atrisināsim iegūto vienādojumu attiecībā uz x', iegūsim atrisinājumu kopu S_2;

3. ...

1.5. piemērs. Atrisināsim vienādojumu $3x^2 + x - 1 \equiv 0 \pmod{27}$.

1. Jebkurš atrisinājums x apmierina vienādojumu

$$3x^2 + x - 1 \equiv 0 \pmod{3},$$

šim vienādojumam ir viens atrisinājums $x \equiv 1 \pmod{3}$.

2. Ievietosim iegūto atrisinājumu $x = 1 + 3x'$ vienādojumā

$$3x^2 + x - 1 \equiv 0 \pmod{9}.$$

Iegūsim vienādojumu $3x' + 3 \equiv 0 \pmod{9}$. Izdalīsim visu ar 3, iegūsim vienādojumu $x' + 1 \equiv 0 \pmod{3}$, kura atrisinājums ir $x' \equiv 2 \pmod{3}$. Tātad $x \equiv 1 + 3 \cdot 2 = 7 \pmod{9}$.

3. Ievietosim iegūto atrisinājumu $x = 7 + 9x''$ vienādojumā

$$3x^2 + x - 1 \equiv 0 \pmod{27}.$$

Iegūsim vienādojumu $9x'' + 18 \equiv 0 \pmod{27}$. Izdalīsim visu ar 9, iegūsim vienādojumu $x'' + 2 \equiv 0 \pmod{3}$, kura atrisinājums ir $x'' \equiv 1 \pmod{3}$.

Atbilde ir $x \equiv 7 + 9 \cdot 1 = 16 \pmod{27}$.

2. 8.mājasdarbs

7.3 Atrisiniet vienādojumu $8x^2 + 2008 \equiv 0 \pmod 3$.

7.4 Izmantojot Gausa metodi atrisiniet lineāru vienādojumu sistēmu

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