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

Studiju kurss

Veselo skaitļu teorija

10.lekcija (papildmateriāls)

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

1. Dažu primitīvo saķņu teorijas teorēmu pierādījumi

1.1. Palīgapgalvojumi

1.1. teorēma. (*Lagranža teorēma*) Ja $f(x)$ ir nekonstants polinoms ar pakāpi n un veseliem koeficientiem un p ir pirmskaitlis, tad vienādojumam

$$f(x) \equiv 0 \pmod{\mathrm{p}}$$

ir ne vairāk kā n dažādi atrisinājumi mod p. atrisinājumi.

PIERĀDĪJUMS Izmantosim matemātisko indukciju ar parametru n.

Indukcijas bāze Ja polinoma pakāpe ir 1, tad vienādojums ir

$$a_1 x + a_0 \equiv 0 \pmod{\mathrm{p}}.$$

Tam ir tieši viens atrisinājums

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

Indukcijas bāze ir pierādīta.

Indukcijas solis Pieņemsim, ja teorēmas apgalvojums ir spēkā, ja polinoma pakāpe nepārsniedz $i-1$. Apskatīsim polinomu

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

kura pakāpe ir vienāda ar i. Ja tam nav atrisinājumu, tad indukcijas solis ir pierādīts. Ja tam ir atrisinājums x_0, tad

$$f(x) \equiv f(x) - f(x_0) \equiv \sum_{j=0}^{i} a_j x^j - \sum_{j=0}^{i} a_j x_0^j = \sum_{j=0}^{i} a_j (x^j - x_0^j) \pmod{\text{p}}.$$

Atcerēsimiem vienādību

$$x^j - x_0^j = (x - x_0)(x^{j-1} + x^{j-2}x_0 + ... + x \cdot x_0^{j-2} + x_0^{j-1}).$$

Redzam, ka

$$f(x) \equiv f(x) - f(x_0) \equiv (x - x_0)g(x) \pmod{\text{p}},$$

kur $g(x)$ ir polinoms ar pakāpi, kas nepārsniedz $i-1$. Tādējādi vienādojumam

$$f(x) - f(x_0) \equiv (x - x_0)g(x) \equiv 0 \pmod{\text{p}}$$

atrisinājumu skaits nepārsniedz i - viens atrisinājums x_0 un vēl ne vairāk kā $i-1$ vienādojuma $g(x) \equiv 0 \pmod{\text{p}}$ atrisinājumi.■

1.2. teorēma.

1. Elementa a pakāpes $a^1, ..., a^{P_m(a)}$ ir vienādojuma
$$x^{P_m(a)} \equiv 1 \pmod{\text{m}}$$
dažādi atrisinājumi.
2. Ja m ir pirmskaitlis, tad elementa a pakāpes $a^1, ..., a^{P_m(a)}$ ir vienādojuma
$$x^{P_m(a)} \equiv 1 \pmod{\text{m}}$$
visi atrisinājumi.

PIERĀDĪJUMS 1. Ja $0 \leq l < P_m(a)$, tad $(a^l)^{P_m(a)} \equiv 1 \pmod{\text{m}}$.

Apgalvojums seko no iepriekšējās teorēmas.

2. Saskaņā ar Lagranža teorēmu vienādojumam

$$x^{P_m(a)} \equiv 1 \pmod{\mathrm{m}}$$

ir ne vairāk kā $P_m(a)$ nekongruentu atrisinājumu. Bet atlikumu klases $a = a^1, ..., a^{P_m(a)}$ ir šī vienādojuma $P_m(a)$ atrisinājumi un citu nevar būt. ■

1.1. piezīme. Iepriekšējā teorēma ļauj risināt vienādojumus

$$x^k \equiv 1 \pmod{\mathrm{p}},$$

ja p ir pirmskaitlis. Ja $k \leq p-1$ un $k \nmid p-1$, tad atrisinājumu noteikti nav. Ja $k|p-1$, tad jāatrod vismaz viens elements a tāds, ka $P(a) = k$, tā pakāpes būs atrisinājumi.

1.1. piemērs. Atrisināsim vienādojumu

$$x^2 \equiv 1 (\mathrm{mod}\ 7).$$

Elementam 6 kārta ir vienāda ar 2, tāpēc atrisinājumi ir 6 un 1.

1.2. piezīme. Ja m nav pirmskaitlis, tad vienādojumam

$$x^{P_m(a)} \equiv 1 \pmod{m}$$

var būt arī citi atrisinājumi:

- $m = 8$, $a = 3$, $P_8(3) = 2$, vienādojumam $x^2 \equiv 1 \pmod 8$ atrisinājumi ir arī 5 un 7, šajā gadījumā visiem atrisinājumiem kārtas ir vienādas;
- $m = 15$, $a = 2$, $P_{15}(2) = 4$, vienādojumam $x^4 \equiv 1 \pmod{15}$ atrisinājumi ir arī 11 un 14, kuriem kārtas ir vienādas ar 2 ;

1.2. Klašu skaits ar dotu kārtu

m ir fiksēts, apskatīsim visus $\mathcal{U}_m$ elementus, kuru kārta ir vienāda ar k. Šādu elementu skaitu apzīmēsim ar $\psi(k)$. Ja $k \nmid \varphi(m)$, tad $\psi(k) = 0$.

1.2. piemērs.

- $m = 3$, $\varphi(m) = 2$, $\psi(1) = \psi(2) = 1$;

- $m = 4$, $\varphi(m) = 2$, $\psi(1) = \psi(2) = 1$;
- $m = 5$, $\varphi(m) = 4$, $\psi(1) = \psi(2) = 1$, $\psi(4) = 2$;
- $m = 6$, $\varphi(m) = 2$, $\psi(1) = \psi(2) = 1$;
- $m = 7$, $\varphi(m) = 6$, $\psi(1) = \psi(2) = 1$, $\psi(3) = \psi(6) = 2$;
- $m = 8$, $\varphi(m) = 4$, $\psi(1) = 1$, $\psi(2) = 3$;
- $m = 9$, $\varphi(m) = 6$, $\psi(1) = \psi(2) = 1$, $\psi(3) = \psi(6) = 2$;
- $m = 10$, $\varphi(m) = 4$, $\psi(1) = \psi(2) = 1$, $\psi(4) = 2$;
- $m = 11$, $\varphi(m) = 10$, $\psi(1) = \psi(2) = 1$, $\psi(5) = \psi(10) = 4$;

1.3. teorēma. Katram m izpildās vienādība

$$\sum_{k|\varphi(m)} \psi(k) = \varphi(m).$$

PIERĀDĪJUMS $\forall\, a \in \mathcal{U}_m : P(a)|\varphi(m)$. Summā

$$\sum_{a \in U_m} 1 = \varphi(m)$$

locekļus varam apvienot grupās, kas atbilst $\varphi(m)$ dalītājiem - katram $\varphi(m)$ dalītājam k atbildīs $\psi(k)$ vieninieku, tādējādi

$$\sum_{a\in U_m} 1 = \underbrace{1+\ldots+1}_{\psi(k_1)\text{ locekļi}} + \underbrace{1+\ldots+1}_{\psi(k_2)\text{ locekļi}} + \ldots + \underbrace{1+\ldots+1}_{\psi(k_l)\text{ locekļi}} = \sum_{k|\varphi(m)} \psi(k) = \varphi(m)$$

■

1.4. teorēma. Ja p ir pirmskaitlis, tad

1. katram $k \neq 0$ izpildās nevienādība

$$\psi(k) \leq \varphi(k) \text{ (precīzāk, } \psi(k) \in \{0, \varphi(k)\}).$$

2. katram k, kuram izpildās nosacījums $k|p-1$, izpildās vienādība

$$\psi(k) = \varphi(k).$$

PIERĀDĪJUMS

1. Ja $\psi(k) = 0$, tad nevienādība ir pierādīta.

Ja eksistē vismaz viena klase a tāda, ka $P(a) = k$, tad

a) saskaņā ar iepriekš pierādītu teorēmu pakāpes $a^1, ..., a^k$ ir visi vienādojuma $x^k \equiv 1 \pmod{p}$ atrisinājumi;

b) saskaņā ar (citu) iepriekš pierādītu teorēmu $P(a^s) = P(a) = k$ tad un tikai tad, ja $LKD(s, k) = 1$, tādu kāpinātāju skaits ir vienāds ar $\varphi(k)$.

No punkta a) seko, ka katra klase b, kurai $P(b) = k$, pieder kopai $\{a^1, ..., a^k\}$, jo tā apmierina vienādojumu $x^k \equiv 1 \pmod{p}$. Tātad šādu klašu skaits ir vienāds ar $\varphi(k)$.

2. Izmantosim šādu palīgrezultātu (Eilera funkcijas īpašību), kas tiks pierādīts atsevišķi zemāk. Katram naturālam m izpildās vienādība

$$\sum_{k|m} \varphi(k) = m.$$

Ja $m = p - 1$, tad iegūsim vienādību

$$\sum_{k|p-1} \varphi(k) = p - 1.$$

Tādējādi mums ir divas līdzīgas vienādības:

$$\sum_{k|p-1} \varphi(k) = p - 1$$

un

$$\sum_{k|p-1} \psi(k) = p - 1.$$

(otrā ir no iepriekš pierādītas teorēmas). Ievērosim, ka summēšanas indeksu kopas ir vienādas. Atņemot no pirmās vienādības otro, iegūsim

$$\sum_{k|p-1} (\varphi(k) - \psi(k)) = 0.$$

Bet saskaņā ar šīs teorēmas pirmo punktu $\varphi(k) - \psi(k) \geq 0$, tāpēc visi locekļi ir vienādi ar 0 un katram $k|p-1$ izpildās vienādība $\psi(k) = \varphi(k)$.
■

1.5. teorēma. $\forall\, m \in \mathbb{N}, m \geq 2$ izpildās

$$\sum_{k|m} \varphi(k) = m.$$

PIERĀDĪJUMS Apskatīsim kopu $\{\frac{1}{m}, \frac{2}{m}, ..., \frac{m}{m}\}$. Šajā kopā ir m elementi. Katram no šiem skaitļiem var izdalīt skaitītāju un saucēju ar kopīgo reizinātāju, tādējādi katrs no tiem ir izsakāmas formā $\frac{l}{k}$, kur $k|m$ un $LKD(l,k) = 1$. Ja k ir fiksēts, tad skaitļu skaits, kuriem saucējs ir vienāds ar k, ir $\varphi(k)$. Tāpēc summa kreisajā pusē ir vienāda ar m. ■

1.3. Primitīvo sakņu eksistence

1.6. teorēma. Dots, ka p ir nepāra pirmskaitlis. $g \in \mathcal{G}_p \implies g \in \mathcal{G}_{p^2}$ vai $g + p \in \mathcal{G}_{p^2}$.

PIERĀDĪJUMS Pieņemsim, ka g ir primitīva sakne mod p.

$LKD(g,p) = 1 \implies LKD(g,p^2) = 1$, tāpēc $g \in U_{p^2}$.

Apzīmēsim $P_{p^2}(g)$ ar k. Ir zināms, ka $k|\varphi(p^2) = p(p-1)$.

$g^k \equiv 1(\text{mod } p^2) \implies g^k \equiv 1(\text{mod } p) \implies p-1|k$.

$k|p(p-1)$ un $p-1|k \implies k = p(p-1)$ vai $k = p-1$.

$\underline{k = p(p-1)}$ Ja $k = p(p-1)$, tad g ir primitīva sakne mod p^2, jo $P_{p^2}(g) = k = \varphi(p^2) = p(p-1)$.

$\underline{k = p-1}$ Definēsim $h = g + p$.

Tā kā $h \equiv g(\text{mod } p)$, tad ar tiem pašiem spriedumiem iegūstam, ka $P_{p^2}(h) \in \{p-1, p(p-1)\}$.

Pierādīsim, ka $P_{p^2}(h) \neq p-1$, tas nozīmēs, ka h ir primitīva sakne mod p^2.

Redzam, ka

$$h^{p-1} = (g+p)^{p-1} =$$

$$g^{p-1} + (p-1)g^{p-2}p + \frac{(p-1)(p-2)}{2}g^{p-3}p^2 + ... + p^{p-1} =$$

$$\underbrace{g^{p-1}}_{\equiv 1 (\mathrm{mod}\ p^2)} \quad -g^{p-2}p + p^2(...) \equiv$$

$$1 - g^{p-2}p (\mathrm{mod}\ p^2).$$

$$g \in U_{p^2} \implies g^{p-2}p \not\equiv 0 (\mathrm{mod}\ p^2) \implies h^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2). \blacksquare$$