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

Studiju kurss

Veselo skaitļu teorija

8.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Invertējamo atlikuma klašu kopas U_m īpašības

1.1. U_m kā grupa attiecībā uz atlikumu klašu reizināšanas operāciju

U_m (multiplikatīvi invertējamo atlikuma klašu kopa pēc moduļa m) ar atlikumu reizināšanas operāciju ir komutatīva grupa, jo izpildās grupas aksiomas:

- U_m ir slēgta attiecībā uz reizināšanas operāciju: ja $a \in U_n$ un $b \in U_m$, tad $ab \in U_m$, jo
$$(ab)(b^{-1}a^{-1}) \equiv a(bb^{-1})a^{-1} \equiv a \cdot 1 \cdot a^{-1} \equiv aa^{-1} \equiv 1 \pmod{\text{m}};$$
- atlikumu reizināšana ir asociatīva;
- eksistē neitrālais elements attiecībā uz reizināšanu: katram $a \in U_m$ izpildās
$$a \cdot 1 \equiv 1 \cdot a \equiv a \pmod{\text{m}};$$
- katram elementam eksistē multiplikatīvi inversais elements;

- atlikumu reizināšana ir komutatīva - $ab \equiv ba \pmod{m}$.

1.2. Elementa kārta un tās īpašības

Par elementa $a \in U_m$ kārtu sauksim mazāko nenegatīvo veselo skaitli k tādu, ka

$$a^k \equiv 1 \pmod{m}.$$

No Eilera teorēmas seko, ka katram $a \in U_m$ izpildās nosacījums

$$k \leq \varphi(m).$$

Elementa a kārtu apzīmēsim ar $P_m(a)$ vai $P(a)$, ja m ir fiksēts. Elementa 1 kārta ir vienāda ar 1.

1.1. piemērs. Atradīsim kārtas invertējamiem elementiem gredzenos $GF(5)$, $GF(7)$.

1.1. teorēma. $a^k \equiv 1 \pmod{\text{m}} \implies P_m(a)|k.$

PIERĀDĪJUMS Izdalīsim k ar $P_m(a)$:

$$k = qP_m(a) + r,$$

kur $0 \leq r < P_m(a)$. Redzam, ka

$$a^k \equiv a^{qP_m(a)+r} \equiv (a^{P_m(a)})^q a^r \equiv a^r \equiv 1 \pmod{\text{m}}.$$

Ja $r \neq 0$, tad $a^r \not\equiv 1 \pmod{\text{m}}$, jo $r < P_m(a)$ un $P_m(a)$ ir a kārta. Tātad $r = 0$ un $P_m(a)|k$. ■

1.2. teorēma. $P_m(a)|\varphi(m)$.

PIERĀDĪJUMS Apgalvojums seko no Eilera teorēmas un iepriekšējās teorēmas: $a^{\varphi(m)} \equiv 1 \pmod{\text{m}} \implies P_m(a)|\varphi(m)$.■

1.2. piemērs. Elementu kārtas var būt tikai $\varphi(m)$ dalītāji. Apskatīsim $m = 20$, $\varphi(20) = 8$. Invertējamie elementi ir

$$\{1, 3, 7, 9, 11, 13, 17, 19\}.$$

Elementa kārta var būt 1,2,4 vai 8. Invertējamo elementu kvadrāti ir

$$1^2 \equiv 1, 3^2 \equiv 9, 7^2 \equiv 9, 9^2 \equiv 1, 11^2 \equiv 1,$$
$$13^2 \equiv 9, 17^2 \equiv (-3)^2 \equiv 9, 19^2 \equiv 1.$$

Tātad elementiem $9, 11, 19$ kārta ir 2. Visu invertējamo elementu ceturtās pakāpes ir kongruentas ar 1, jo $9^2 \equiv 1$. Tātad tiem elementiem, kuru kārta nav ne 1, ne 2, tā ir vienāda ar 4. Šie elementi ir $3, 7, 13, 17$.

1.3. teorēma. $a^{k_1} \equiv a^{k_2} \pmod{\text{m}} \iff k_1 \equiv k_2 (\text{mod } P_m(a))$.

PIERĀDĪJUMS $a^{k_1} \equiv a^{k_2} \pmod{\text{m}} \implies a^{k_1-k_2} \equiv 1 \pmod{\text{m}}$. No tā seko, ka $P_m(a)|k_1 - k_2$ jeb $k_1 \equiv k_2 \pmod{P_m(a)}$.

$$k_1 \equiv k_2 (\text{mod } P_m(a)) \implies k_1 - k_2 = qP_m(a) \implies$$
$$k_1 = k_2 + qP_m(a).$$

Redzam, ka

$$a^{k_1} \equiv a^{k_2+qP_m(a)} \equiv a^{k_2}(a^{P_m(a)})^q \equiv a^{k_2} \pmod{\text{m}}.$$

■

1.1. piezīme. No teorēmas seko, ka dažādo elementa a pakāpju skaits ir vienāds ar $P_m(a)$.

1.4. teorēma. $P_m(a^k) = P_m(a) \iff LKD(k, P_m(a)) = 1.$

PIERĀDĪJUMS No sākuma atzīmēsim, ka $P_m(a^k) \leq P_n(a)$, jo elementa a^k pakāpju kopa ir a pakāpju kopas apakškopa.

Ja $LKD(k, P_m(a)) = 1$, tad no kongruences

$$(a^k)^t \equiv a^{kt} \equiv 1 \text{ (mod m)}$$

seko, ka $P_m(a)|kt$ un $P_m(a)|t$. Bet mazākā t vērtība ir $P_m(a^k)$, kas nepārsniedz $P_m(a)$. Tātad $P_m(a^k) = P_m(a)$.

Ja $LKD(k, P_m(a)) = d \neq 1$, tad

$$(a^k)^{\frac{P_m(a)}{d}} \equiv (a^{P_m(a)})^{\frac{k}{d}} \equiv 1 \text{ (mod m)}.$$

Seko, ka $P_m(a^k) = \frac{P_m(a)}{d} < P_m(a)$. ■

1.3. piemērs. Ja $p = 7$, tad $P(3) = 6$ un tikai vēl $P(3^5) = 6$.

1.5. teorēma. (palīgteorēma - *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 (savstarpēji nekongruenti) 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.■

1.6. 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
$$x^{P_m(a)} \equiv 1 \pmod{\text{m}}$$

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. ■

1.2. piezīme. Iepriekšējā teorēma ļauj risināt vienādojumus

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

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.

1.3. Klašu skaits ar dotu kārtu

Ja m ir fiksēts, tad apskatīsim visus grupas U_m elementus, kuru kārta ir vienāda ar k. Šādu elementu skaitu apzīmēsim ar $\psi(k)$. Ievērosim, ka ja $k \nmid \varphi(m)$, tad $\psi(k) = 0$.

1.4. piemērs.

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

1.7. teorēma. Katram m izpildās vienādība

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

PIERĀDĪJUMS Katrai invertējamai atlikuma klasei kārta ir $\varphi(m)$ dalītājs. Summas

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

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

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

■

1.8. teorēma. Ja p ir pirmskaitlis, tad

1. katram $k \neq 0$ izpildās nevienādība
$$\psi(k) \leq \varphi(k).$$
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 $x^k \equiv 1$ (mod 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 $\psi(k) = \varphi(k)$. ■

1.9. teorēma. Katram naturālam $m \geq 2$ izpildās vienādība

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

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. ■

1.4. Eilera teorēmas pastiprinājums

Pieņemsim, ka $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$. Definēsim *vispārināto Eilera funkciju* $L(n)$:

$$L(m) = MKD(\varphi(p_1^{\alpha_1}), ..., \varphi(p_k^{\alpha_k})) =$$
$$= MKD(p_1^{\alpha_1 - 1}(p_1 - 1), ..., p_k^{\alpha_k - 1}(p_k - 1)).$$

1.5. piemērs. $\varphi(30) = 8$, $L(30) = 4$.
$\varphi(1365) = 576$, $L(1365) = 12$.

1.10. teorēma. Ja $LKD(a, m) = 1$, tad

$$a^{L(m)} \equiv 1 (\text{mod } m).$$

PIERĀDĪJUMS Pieņemsim, ka $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$.

$LKD(a,m) = 1 \implies LKD(a,p_i^{\alpha_i}) = 1, \forall i$, tāpēc pielietojot Eilera teorēmu modulim $p_i^{\alpha_i}$, iegūsim kongruences

$$a^{\varphi(p_i^{\alpha_i})} = a^{p_i^{\alpha_i-1}(p_i-1)} \equiv 1(\text{mod } p_i^{\alpha_i}), \forall i.$$

Definēsim $\gamma_i = \frac{L(m)}{\varphi(p_i^{\alpha_i})} \in \mathbb{N}, \forall i.$

Redzam, ka

$$a^{\varphi(p_i^{\alpha_i})\gamma_i} \equiv a^{L(m)} \equiv 1(\text{mod } p_i^{\alpha_i}), \forall i.$$

Tā kā visi $p_i^{\alpha_i}$ ir savstarpēji pirmskaitļi, tad no kongruences īpašībām seko, ka

$$a^{L(m)} \equiv 1(\text{mod } MKD(p_1^{\alpha_1}...p_k^{\alpha_k}))$$

un

$$a^{L(m)} \equiv 1(\text{mod } m).$$

■

1.5. Vilsona teorēma

1.6. piemērs. Atradīsim visu invertējamo atlikumu klašu reizinājumu mod p, kur p ir pirmskaitlis.

1.11. teorēma. (*Vilsona teorēma*)

$$(p-1)! \equiv -1 (\text{mod } p) \iff p - \text{pirmskaitlis}.$$

PIERĀDĪJUMS Ja p ir pirmskaitlis, tad nenulles atlikumi veido grupu attiecībā uz reizināšanu.

Ievērosim, ka

$$a^{-1} \equiv a (\text{mod } p) \iff a \in \{1, -1\}.$$

Tas ir tāpēc, ka ekvivalenta vienādība ir

$$a^2 - 1 \equiv 0((\text{mod })\text{p}),$$

kurai ir ne vairāk kā divi atrisinājumi saskaņā ar Lagranža teorēmu.

Visu atlikumu kopu mod p bez 1 un -1 var sadalīt pāros formā $\{u, u^{-1}\}$. Ievērosim, ka $uu^{-1} \equiv 1(\text{mod } p)$.

Reizinājumā $W = 1 \cdot 2 \cdot ... \cdot (p-1)$ pārkārtosim locekļus:

$$W \equiv 1 \cdot (-1) \cdot 2 \cdot 2^{-1} \cdot ... \cdot t \cdot t^{-1} \equiv -1(\text{mod } p).$$

Pieņemsim, ka $W+1 \equiv (\text{mod } p)$ un p nav pirmskaitlis. Tad eksistē tā dalītājs $d : 1 < d < p$. Tad $W \equiv 0(\text{mod } d)$ un $W + 1 \equiv 0(\text{mod } d)$. Seko, ka $1 \equiv 0(\text{mod } d)$, tātad $d = 1$. ■

2. 8.mājasdarbs

2.1. Obligātie uzdevumi

8.1 Atrodiet elementu skaitus ar visām kārtām, kas dala $\varphi(m)$, ja

(a) $m = 8$;
(b) $m = 10$;
(c) $m = 11$.

8.2 Atrisiniet vienādojumus

(a) $x^3 \equiv 1 (\mathrm{mod}\ 7)$;
(b) $x^3 \equiv 1 (\mathrm{mod}\ 11)$;
(c) $x^6 \equiv 1 (\mathrm{mod}\ 13)$.

8.3 Atrodiet

(a) $L(2008)$;
(b) $L(286195)$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

8.4 Pierādiet, ka ja p ir pirmskaitlis, tad

(a) $1^2 \cdot 3^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$;

(b) $2^2 \cdot 4^2 \cdot \ldots \cdot (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.