

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

Studiju kurss

Veselo skaitļu teorija

6.lekcija (datoriķiem)

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

1. Invertējamo atlikuma klašu kopas U_m īpašības	3
1.1. Fermā un Eilera teorēmas	3
1.2. Elementa kārtā un tās īpašības	9
1.3. Primitīvās saknes (ģeneratori)	19
2. 6.mājasdarbs	26

1. Invertējamo atlikuma klašu kopas U_m īpašības

Multiplikatīvi invertējamo atlikumu klašu kopu pēc moduļa m apzīmēsim ar U_m .

1.1. Fermā un Eilera teorēmas

1.1. piemērs. Atradīsim kāpinātājus, ar kuriem invertējamie elementi ir kongruenti ar 1 gredzenos $GF(5)$, $GF(7)$.

1.1. teorēma. (*Fermā Mazā teorēma*) Ja p ir pirmskaitlis un

$$a \not\equiv 0 \pmod{p},$$

tad

$$a^{p-1} \equiv 1 \pmod{p}$$

PIERĀDĪJUMS Apskatīsim funkciju

$$f_a : U_p \rightarrow U_p,$$

kas tiek definēta šādi:

$$f_a(x) = ax.$$

Apskatīsim piemērus gredzenos $GF(5)$ ($a = 2$) un $GF(7)$ ($a = 2$ vai $a = 3$).

Pierādīsim, ka f_a ir bijektīva funkcija. Ja $f_a(x_1) = f_a(x_2)$, tad $ax_1 \equiv ax_2$ un reizinot abas puses ar a^{-1} , iegūsim $x_1 \equiv x_2$, tātad f_a ir injektīva. Katram $y \in \mathbb{Z}/p\mathbb{Z}$ izpildās $y \equiv a(a^{-1}y)$, tātad f_a ir surjektīva.

Ja f_a ir bijektīva funkcija, tad reizinot ar a kopas U_p dažādos elementus sakārtotus kādā noteiktā kārtībā (z_1, \dots, z_{p-1}), iegūsim tos pašus elementus citā kārtībā. Apskatīsim reizinājumu

$$(az_1)(az_2) \cdot \dots \cdot (az_{p-1}).$$

No vienas puses, pielietojot reizināšanas komutativitāti, tas ir vienāds ar

$$a^{p-1}(z_1 \cdot \dots \cdot z_{p-1}),$$

no otras puses, tas ir vienāds ar elementu z_i reizinājumu kādā citā kārtībā un, pielietojot vēlreiz atlikumu klašu reizināšanas komutativitātes īpašību, redzam, ka tas ir vienāds ar

$$z_1 \cdot \dots \cdot z_{p-1}.$$

Tātad

$$a^{p-1}(z_1 \cdot \dots \cdot z_{p-1}) \equiv z_1 \cdot \dots \cdot z_{p-1} \pmod{p}$$

un

$$a^{p-1} \equiv 1 \pmod{p}.$$



1.2. piemērs. $2^2 \equiv 1 \pmod{3}$, $2^4 \equiv 1 \pmod{5}$, $2^{10} \equiv 1 \pmod{11}$,
 $88^{88} \equiv 1 \pmod{89}$.

1.2. teorēma. (*Eilera teorēma*) Ja $LKD(a, m) = 1$, tad

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

PIERĀDĪJUMS Tā kā $LKD(a, m) = 1$, tad a klase ir multiplikatīvi invertējams elements kopā U_m . Tālāk pierādījums ir līdzīgs Fermā teorēmas pierādījumam, ievērojot, ka $|U_m| = \varphi(m)$. Apskatīsim funkciju

$$f_a : U_m \rightarrow U_m,$$

kas tiek definēta šādi:

$$f_a(x) = ax.$$

Līdzīgi kā Fermā teorēmā pierādām, ka f_a ir bijektīva funkcija.

Ja f_a ir bijektīva funkcija, tad reizinot ar a kopas U_m dažādos elementus sakārtotus kādā noteiktā kārtībā $(z_1, \dots, z_{\varphi(m)})$, iegūsim tos

pašus elementus citā kārtībā. Apskatīsim reizinājumu

$$(az_1)(az_2) \cdot \dots \cdot (az_{\varphi(m)}).$$

Tas ir vienāds gan ar

$$a^{\varphi(m)}(z_1 \cdot \dots \cdot z_{\varphi(m)}),$$

gan ar

$$z_1 \cdot \dots \cdot z_{\varphi(m)}.$$

Tātad saīsinot iegūsim

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$



1.1. piezīme. Ievērosim, ka Fermā teorēma ir Eilera teorēmas speciālgadījums.

1.2. piezīme. Dažreiz Fermā teorēmu formulē arī veidā

$$a^p \equiv a \pmod{p}$$

vai

$$a^{-1} \equiv a^{p-2} \pmod{p}.$$

1.3. piezīme. Fermā un Eilera teorēmu pielietojums - *ātrā kāpināšana*, ja $a \not\equiv 0 \pmod{m}$, tad :

$$a^b \equiv a^{b \pmod{\varphi(m)}} \pmod{p}.$$

1.2. Elementa kārtā 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 kārtā ir vienāda ar 1.

1.3. piemērs. Atradīsim kārtas invertējamiem elementiem gredzenos $GF(5)$, $GF(7)$. Var izmantot MAGMA vai Mathematica.

1.3. teorēma. Ja $a^k \equiv 1 \pmod{m}$, tad $P_m(a)|k$.

PIERĀDĪJUMS Izdalīsim k ar $P_m(a)$: $k = qP_m(a) + r$, kur $0 \leq r < P_m(a)$. Redzam, ka

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

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

1.4. teorēma. $P_m(a)|\varphi(m)$.

PIERĀDĪJUMS Apgalvojums seko no Eilera teorēmas un iepriekšējās teorēmas. Tā kā $a^{\varphi(m)} \equiv 1 \pmod{m}$, tad $P_m(a)|\varphi(m)$. ■

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

1.5. teorēma. $a^{k_1} \equiv a^{k_2} \pmod{m}$ tad un tikai tad, ja

$$k_1 \equiv k_2 \pmod{P_m(a)}.$$

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

Ja $k_1 \equiv k_2 \pmod{P_m(a)}$, tad $k_1 - k_2 = qP_m(a)$ un $k_1 = k_2 + qP_m(a)$. Redzam, ka

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



1.6. teorēma. Dažādo elementa a pakāpju skaits ir vienāds ar $P_m(a)$.

PIERĀDĪJUMS Apgalvojums seko no iepriekšējās teorēmas. ■

1.7. teorēma. $P_m(a^k) = P_m(a)$ tad un tikai tad, ja

$$LKD(k, P_m(a)) = 1.$$

PIERĀDĪJUMS No sākuma atzīmēsim, ka

$$P_m(a^k) \leq P_m(a),$$

jo elementa a^k pakāpju kopa ir a pakāpju kopas apakškopa. Ja

$$LKD(k, P_m(a)) = 1,$$

tad no kongruences

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

seko, ka $P_m(a) | kt$ un $P_m(a) | t$. Tātad $P_m(a^k) = P_m(a)$.

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

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

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

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

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

ir ne vairāk kā n dažādi (savstarpēji nekongruenti) atrisinājumi.

PIERĀDĪJUMS Izmantosim matemātisko indukciju pēc parametra n . Ja polinoma pakāpe ir 1, tad vienādojums ir

$$a_1x + a_0 \equiv 0 \pmod{p}.$$

Tam ir tieši viens atrisinājums $x \equiv a_1^{-1}(-a_0) \pmod{p}$. Indukcijas bāze ir pierādīta.

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

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

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

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

Atcerēsime vienādību

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

Redzam, ka

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

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

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

atrisinājumu skaits nepārsniedz $i - 1$ - viens atrisinājums x_0 un vēl ne vairāk kā $i - 1$ vienādojuma

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

atrisinājumi. ■

1.9. teorēma.

1. Elementa a pakāpes $a^1, \dots, a^{P_m(a)}$ ir vienādojuma

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

dažādi atrisinājumi.

2. Ja m ir pirmskaitlis, tad elementa a pakāpes $a^1, \dots, a^{P_m(a)}$ ir vienādojuma

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

visi atrisinājumi.

PIERĀDĪJUMS 1. Ja $0 \leq l < P_m(a)$, tad $(a^l)^{P_m(a)} \equiv 1 \pmod{m}$.
 Apgalvojums seko no iepriekšējās teorēmas.

2. Saskaņā ar Lagranža teorēmu vienādojumam

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

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

1.4. piezīme. Iepriekšējā teorēma ļauj risināt vienādojumus

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

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.

1.5. 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.

1.3. Primitīvās saknes (ģeneratori)

Elementu $a \in U_m$ sauksim par *primitīvu sakni*, ja

$$P_m(a) = \varphi(m).$$

Citiem vārdiem sakot, neeksistē nekāda cita invertējama klase b un naturāls $l > 1$, $l|\varphi(m)$ tādi, ka

$$b^l \equiv a \pmod{m}$$

(no a nevar izvilkt nekādu sakni $b = \sqrt[l]{a}$). Tas ir tāpēc, ka pretējā gadījumā mēs iegūtu, ka

$$a^{\frac{\varphi(m)}{l}} \equiv b^{l \cdot \frac{\varphi(m)}{l}} \equiv b^{\varphi(m)} \equiv 1 \pmod{m}$$

un a kārta būtu vienāda ar $\frac{\varphi(m)}{l} < \varphi(m)$.

1.5. piemērs. $2 \equiv 3^2 \pmod{7}$, tāpēc var uzskatīt, ka $\sqrt{2} \equiv 3 \pmod{7}$. Neeksistē klase x tāda, ka $x^k \equiv 3 \pmod{7}$, ja $k \geq 2$ un $k|6$.

1.10. teorēma. Ja g ir primitīva sakne pēc moduļa m , tad klases $g, g^2, \dots, g^{\varphi(m)}$ veido reducēto atlikumu klašu pārstāvju kopu.

PIERĀDĪJUMS Tā kā $P_m(g) = \varphi(m)$, tad visas pakāpes

$$g, g^2, \dots, g^{\varphi(m)}$$

ir dažādas pēc moduļa m . Tā kā $LKD(g, m) = 1$, tad katram i izpildās $LKD(g^i, m) = 1$, tāpēc šīs pakāpes ir invertējamu klašu pārstāvji. ■

1.6. piemērs.

- $m = 2, \{1\}$;
- $m = 3, \{2\}$;
- $m = 4, \{3\}$;
- $m = 5, \{2, 3\}$;
- $m = 6, \{5\}$;
- $m = 7, \{3, 5\}$;
- $m = 8, \emptyset$;
- $m = 9, \{2, 5\}$;
- $m = 10, \{3, 7\}$;
- $m = 11, \{2, 6, 7, 8\}$;
- $m = 12, \emptyset$;
- $m = 13, \{2, 6, 7, 11\}$;
- $m = 14, \{3, 5\}$;
- $m = 15, \emptyset$;

- $m = 16, \emptyset$;
- $m = 17, \{3, 5, 6, 7, 10, 11, 12, 14\}$;
- $m = 18, \{5, 11\}$;
- $m = 19, \{2, 3, 10, 13, 14, 15\}$;
- $m = 20, \emptyset$;
- $m = 2007, \emptyset$;
- $m = 2008, \emptyset$.

1.11. teorēma. Ja $m = p$ ir pirmskaitlis, tad primitīvās saknes eksistē.

PIERĀDĪJUMS Pieņemsim, ka lielākā iespējamā elementa kārtā ir $k < p - 1$. Tātad eksistē elements a , kura k dažādās pakāpes apmierina vienādojumu

$$x^k \equiv 1 \pmod{p}.$$

Tā kā $k < p - 1$, tad eksistē elements b , kurš nav izsakāms formā a^s nekādam s . Elementa b kārtai nevar būt kopīgi dalītāji ar a kārtu, jo tad vienādojumam

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

būtu vairāk kā k atrisinājumi, kas ir pretruna ar Lagranža teorēmu. Apskatīsim elementu $c = ab$. Ja $c^l \equiv 1 \pmod{p}$, tad $a^l \equiv b^{-l} \pmod{p}$. Tas ir iespējams tikai tad, ja $MKD(P(a), P(b)) | l$. Tā ir pretruna, jo šādā gadījumā $P(c) > P(a)$. Tātad $P(a) = k = p - 1$. ■

1.6. piezīme. Ja g ir primitīva sakne pēc moduļa p , tad dažām k vērtībām pakāpe g^k , $0 < k < p - 1$, apmierina nosacījumu

$$LKD(k, p - 1) = 1,$$

tāpēc $P_p(g^k) = P_p(g)$. Tātad visas šīs pakāpes veido visu primitīvo sakņu kopu pēc moduļa p .

1.12. teorēma. Grupā U_m eksistē primitīva sakne tad un tikai tad, ja $m \in \{2, 4\}$, $m = p^\alpha$ vai $m = 2p^\alpha$, kur p ir nepāra pirmskaitlis.

2. 6.mājasdarbs

1. Izmantojot Fermā teorēmu, pierādiet, ka

$$666666^{666666} \equiv 1 \pmod{666667}.$$

2. Atrodiet elementu skaitus ar visām kārtām, kas dala $\varphi(m)$, ja
 - (a) $m = 8$;
 - (b) $m = 10$.
3. Izmantojot primitīvās saknes un indeksus, atrisiniet šādus vienādojumus:
 - (a) $x^6 \equiv 4 \pmod{23}$;
 - (b) $x^7 \equiv 9 \pmod{18}$.