DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Jauno matemātiķu skola

Studiju kurss

Veselo skaitļu teorija

5.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas kopsavilkums:

- apgūt veselo skaitļu salīdzināmības teorijas pamatus,
- apgūt atlikumu (modulārās) aritmētikas pamatus.

Svarīgākie jēdzieni: Eilera funkcija, atlikuma kārta,

Svarīgākie fakti un metodes: Eilera funkcijas īpašības, Fermā un Eilera teorēmas, atlikuma kārtas īpašības, Vilsona teorēma.

1. Ievads atlikumu multiplikatīvās grupas īpašībās

1.1. Pamatfakti par invertējamiem atlikumiem

x - invertējams atlikums mod m, ja $\exists\, y$:

$$xy \equiv 1 (\mathrm{mod}\ m).$$

Pamatfakti:

- invertējamo atlikumu klašu mod m kopa $\mathcal{U}_m$ ir slēgta attiecībā uz atlikumu reizināšanu:

$$u, u' \in \mathcal{U}_m \implies uu' \in \mathcal{U}_m,$$

- $1 \in \mathcal{U}_m$ - neitrālais elements,
- $u \in \mathcal{U}_m \implies \exists\, u^{-1} \in \mathcal{U}_m$- multiplikatīvi inversais elements,
- $|\mathcal{U}_m| \leq |m| \implies \mathcal{U}_m$ ir galīga kopa.

1.1. teorēma. Atlikumiem mod m ir spēkā šādas īpašības:

1. $\forall\ x \in \mathbb{Z}_m\ \exists$ viens un tikai viens $y \in \mathbb{Z}_m$:
$$x + y \equiv 0(\text{mod m})$$
(*aditīvi inversā elementa eksistence un viennozīmīgums*),
2. $p \in \mathbb{P} \implies$
$$\Big(xy \equiv 0(\text{mod p})\Big) \implies \Big(x \equiv 0(\text{mod p}) \text{ vai } y \equiv 0(\text{mod p})\Big)$$
(*nulles dalītāju neeksistence*),
3. $p \in \mathbb{P} \implies \forall\ x \in \mathbb{Z}_p,\ x \not\equiv 0(\text{mod p})\ \exists$ viens un tikai viens $z \in \mathbb{Z}_p$:
$$xz \equiv 1(\text{mod p}),$$
4. $m \notin \mathbb{P} \implies \exists\ x, y \in \mathbb{Z}_m$:
$$\begin{cases} xy \equiv 0(\text{mod } m) \\ x \not\equiv 0(\text{mod } m) \\ y \not\equiv 0(\text{mod } m) \end{cases}$$
5. x ir invertējams attiecībā uz reizināšanu mod m ($\exists\ y:\ xy \equiv 1(\text{mod m})$) $\iff$ $LKD(x, m) = 1$ (*multiplikatīvi inversā elementa eksistence*).

PIERĀDĪJUMS

1. $\forall\, x \in \mathbb{Z}\ \exists\, y \in \mathbb{Z}:\ x + y = m \implies [x] + [y] = [0]$.

$x + y_1 \equiv x + y_2 \equiv 0(\text{mod m}) \implies y_1 \equiv y_2(\text{mod m})$.

2. $p \in \mathbb{P} \implies \Big(p|xy \implies p|x \text{ vai } p|y\Big)$. Pārtulkojot to atlikumu klašu terminos: $xy \equiv 0(\text{mod p}) \implies \Big(x \equiv 0(\text{mod p}) \text{ vai } y \equiv 0(\text{mod p})\Big)$.

3. $p \in \mathbb{P} \implies \Big(1 \le x \le p-1 \implies LKD(x,p) = 1\Big) \implies$ saskaņā ar LKD lineārās kombinācijas īpašību $\exists\, a, b \in \mathbb{Z}:\ ax + bp = 1 \implies$

$$ax + bp \equiv ax + b \cdot 0 \equiv \boxed{ax \equiv 1}(\text{mod p}).$$

4. $m \notin \mathbb{P} \implies \exists$ vismaz divi skaitļi $a > 1$ un $b > 1:\ ab = m \implies$

$$ab \equiv m \equiv 0(\text{mod m}).$$

5. $LKD(x,m)=1 \Longrightarrow \exists\, a,b\in\mathbb{Z}:\ ax+bm=1 \Longrightarrow$

$$ax+bm\equiv ax+b\cdot 0\equiv ax\equiv 1(\text{mod m}).$$

Ja $\exists\ y:\ xy\equiv 1(\text{mod m}) \Longrightarrow xy-1=mq$ un $xy-mq=1$. Reducējot mod $d=LKD(x,m) \Longrightarrow 0\equiv 1(\text{mod d}) \Longrightarrow d=1$. ■

1.2. Eilera funkcija un tās īpašības

Par naturāla skaitļa n *Eilera funkciju* $\varphi(n)$ sauksim tādu skaitļu x skaitu, kuriem izpildās nosacījumi $0\le x<n$ un $LKD(x,n)=1$:

$$\varphi(n)=\sum_{1\le x<n, LKD(x,n)=1} 1.$$

1.1. piezīme. No iepriekš pierādītas teorēmas seko, ka to atlikuma klašu skaits mod n, kurām eksistē multiplikatīvi inversais elements, ir vienāds ar $\varphi(n)$.

1.2. piezīme. $x \equiv x'(\text{mod n}) \implies \exists\, k \in \mathbb{Z} : x + kn = x' \implies$

$$LKD(x, n) = LKD(x + kn, n) = LKD(x', n),$$

tāpēc jebkurā atlikumu klašu pārstāvju kopā to skaitļu skaits, kas ir savstarpēji pirmskaitļi ar n, ir vienāds ar $\varphi(n)$.

1.2. teorēma.

1. $LKD(n, m) = 1 \implies$

$$\varphi(nm) = \varphi(n)\varphi(m)$$

(Eilera funkcija ir *multiplikatīva*),

2. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
3. $n = p_1^{\alpha_1} ... p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i} \implies$

$$\varphi(n) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

PIERĀDĪJUMS

1. Sakārtosim skaitļus no 0 līdz $nm-1$ matricā, kurā ir m rindas un n kolonnas šādā veidā:

$$\begin{bmatrix} 0 & 1 & \dots & n-1 \\ n & n+1 & \dots & 2n-1 \\ \dots & \dots & \dots & \dots \\ n(m-1) & n(m-1)+1 & \dots & nm-1 \end{bmatrix}$$

Skaitīsim, cik šajā matricā ir skaitļu, kas ir savstarpēji pirmskaitļi ar nm.

Ievērosim šādus faktus:

- katra rinda veido atlikumu klašu pārstāvju kopu pēc moduļa n (jo katrā rindā ir n pēc kārtas ejoši skaitļi),
- katrā kolonnā visi skaitļi ir kongruenti pēc moduļa n,
- katra kolonna veido atlikumu klašu pārstāvju kopu pēc moduļa m (jo katrā kolonnā ir m skaitļi formā $a+nq$, kur $0 \leq q < m$),

pēc algebriskiem pārveidojumiem redzam, ka

$$\begin{aligned} a + nq_1 \equiv a + nq_2 (\text{mod m}) &\iff \\ nq_1 \equiv nq_2 (\text{mod m}) &\iff \\ n^{-1}nq_1 \equiv n^{-1}nq_2 (\text{mod m}) &\iff \\ q_1 \equiv q_2 (\text{mod m}). & \end{aligned}$$

Ievērosim, ka

$$LKD(x, nm) = 1 \iff LKD(x, n) = 1 \text{ un } LKD(x, m) = 1.$$

Tātad ir spēkā šādi fakti:

- skaitļi x, kuriem $LKD(x, nm) = 1$, var atrasties tikai tajās kolonnās, kurās $LKD(x, n) = 1$, tādu kolonnu skaits ir $\varphi(n)$,
- katrā kolonnā, kur $LKD(x, n) = 1$, to skaitļu skaits, kuriem $LKD(x, m) = 1$, ir vienāds ar $\varphi(m)$.

Tādējādi $\varphi(nm) = \varphi(n)\varphi(m)$.

2. $n = p^\alpha \implies \Big(LKD(n,m) \neq 1 \iff p|m\Big) \implies m = p \cdot k$, kur $0 \leq p \cdot k < p^\alpha \implies 0 \leq k < p^{\alpha-1}$, tātad tādu skaitļu m skaits ir $|\{0, p, ..., p^{\alpha-1} - 1\}| = p^{\alpha-1} \implies \varphi(n) = p^\alpha - p^{\alpha-1}$.

3. Pieņemsim, ka $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$. $LKD(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ u.t.t.

Vairākas reizes pielietosim multiplikatīvo īpašību:

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2} ... p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})\varphi(p_2^{\alpha_2} ... p_k^{\alpha_k}) = ...$$

$$(p_1^{\alpha_1} - p_1^{\alpha_1 - 1})\varphi(p_2^{\alpha_2})\varphi(p_3^{\alpha_3} ... p_k^{\alpha_k}) = ... = \prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) =$$

$$\prod_{i=1}^{k} p_i^{\alpha_i}(1 - \frac{1}{p_i}) = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{k}(1 - \frac{1}{p_i}) = n \prod_{i=1}^{k}(1 - \frac{1}{p_i}).\blacksquare$$

1.1. piemērs. $\varphi(2007) = \varphi(3^2 \cdot 223) = (3^2 - 3^1) \cdot 222 = 6 \cdot 222 = 1332$.

$\varphi(2008) = \varphi(2^3 \cdot 251) = (2^3 - 2^2) \cdot 250 = 4 \cdot 250 = 1000$. $\varphi(1000) = 400$, $\varphi(400) = 160$, ... $\varphi(160) = 64$,

1.3. Fermā un Eilera teorēmas

1.2. piemērs. Atradīsim kāpinātājus, ar kuriem invertējamie elementi ir kongruenti ar 1 mod 5 vai 7.

1.3. teorēma. (*Fermā Mazā teorēma*)

$$\begin{cases} p \in \mathbb{P} \\ a \not\equiv 0 (\text{mod } p) \end{cases} \Longrightarrow a^{p-1} \equiv 1 (\text{mod } p).$$

PIERĀDĪJUMS Apskatīsim funkciju

$$f_a : U_p \to U_p,$$

$$f_a(x) = ax.$$

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

Pierādīsim, ka f_a ir bijektīva funkcija:

- injektivitāte - $f_a(x_1) = f_a(x_2) \Longrightarrow ax_1 \equiv ax_2$, reizinot abas puses ar a^{-1}, iegūsim $x_1 \equiv x_2 \Longrightarrow f_a$ ir injektīva;

- sirjektivitāte - $\forall y \in U_p: \quad y \equiv a(a^{-1}y) \equiv f_a(a^{-1}y) \implies f_a$ ir sirjektīva.

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

Apskatīsim reizinājumu $(az_1)(az_2) \cdot ... \cdot (az_{p-1})$ divos veidos:

- no vienas puses, pielietojot reizināšanas komutativitāti:

$$(az_1)(az_2) \cdot ... \cdot (az_{p-1}) = a^{p-1}(z_1 \cdot ... \cdot z_{p-1}),$$

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

$$(az_1)(az_2) \cdot ... \cdot (az_{p-1}) = z_1 \cdot ... \cdot z_{p-1}.$$

Tātad

$$a^{p-1}(z_1 \cdot ... \cdot z_{p-1}) \equiv z_1 \cdot ... \cdot z_{p-1} (\text{mod p}) \implies \boxed{a^{p-1} \equiv 1} (\text{mod p}). \blacksquare$$

1.3. piemērs. $2^2 \equiv 1(\text{mod } 3)$, $2^4 \equiv 1(\text{mod } 5)$, $2^{10} \equiv 1(\text{mod } 11)$, $88^{88} \equiv 1(\text{mod } 89)$.

1.4. teorēma. (*Eilera teorēma*) $LKD(a, m) = 1 \Longrightarrow$

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

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

1.4. piezīme. Fermā teorēmu formulē arī šādos veidos:

$$a^p \equiv a(\text{mod p})$$

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

1.5. piezīme. Fermā un Eilera teorēmu pielietojums - *ātrā kāpināšana*,

ja $a \not\equiv 0(\text{mod p})$, tad :

$$a^b \equiv a^{b(\text{mod } p-1)}(\text{mod p}).$$

1.4. Atlikuma kārta un tās īpašības

Par invertējama atlikuma $a \in \mathcal{U}_m$ kārtu sauksim mazāko nenegatīvo veselo skaitli k tādu, ka

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

No Eilera teorēmas seko, ka katram $a \in \mathcal{U}_m$ izpildās nosacījums

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

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

1.4. piemērs. Atradīsim kārtas invertējamiem elementiem mod 5 un 7.

1.5. teorēma.

1. $a^k \equiv 1 \pmod{m} \implies P_m(a)|k.$
2. $P_m(a)|\varphi(m).$
3. $a^{k_1} \equiv a^{k_2} \pmod{m} \iff k_1 \equiv k_2 (\mathrm{mod}\ P_m(a)).$
4. $P_m(a^k) = P_m(a) \iff LKD(k, P_m(a)) = 1.$

PIERĀDĪJUMS
■

1.5. piemērs. Atlikumu 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 $3, 7, 13, 17$.

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

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

1.5. Vilsona teorēma

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

1.6. teorēma. (*Vilsona teorēma*)

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

PIERĀDĪJUMS
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.

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:

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

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. 5.mājasdarbs

2.1. Obligātie uzdevumi

5.1 Atrisināt vienādojumus naturālos skaitļos:

(a) $\varphi(x) = 8$;
(b) $\varphi(x) = \varphi(2008)$;
(c) $\varphi(x) = \frac{x}{4}$.

5.2 Pierādīt, ka $66^{66} \equiv 1 (\text{mod } 67)$.

5.3 Pierādīt, ka $\forall\, a, b \in \mathbb{Z}$: $ab(a^{60} - b^{60})$ dalās ar $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$.

5.4 Izmantojot Fermā teorēmu pierādiet, ka $\forall\, p \in \mathbb{P}$ un $\forall\, a, b$:

$$(a + b)^p \equiv a^p + b^p \ (\text{mod p}).$$

5.5 $p, q \in \mathbb{P}$, $p \neq q$. Pierādīt, ka

(a) $p^{q-1} + q^{p-1} \equiv 1 (\text{mod } pq)$;
(b) $a^{pq} - a^p - a^q - a \equiv 0 (\text{mod } pq)$, $\forall\, a$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

5.6 $\{x_0, ..., x_{m-1}\} \subseteq \mathbb{Z}$ veido PAK mod m. Kādiem jābūt $a, b \in \mathbb{Z}$, lai $\{ax_0 + b, ..., ax_{m-1} + b\}$ arī veidotu PAK.