DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Studiju kurss

Veselo skaitļu teorija

6.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Atlikumu gredzena īpašības

1.1. Pamatfakti

1.1. teorēma. Atlikumu gredzenā $\mathbb{Z}/m\mathbb{Z}$ ir spēkā šādas īpašības:

1. katram $x \in \mathbb{Z}/m\mathbb{Z}$ eksistē viens un tikai viens $y \in \mathbb{Z}/m\mathbb{Z}$ tāds, ka
$$x + y \equiv 0(\text{mod m})$$
(*aditīvi inversā elementa eksistence un viennozīmīgums*),
2. ja p ir pirmskaitlis, tad
$$xy \equiv 0(\text{mod p}) \implies x \equiv 0(\text{mod p}) \text{ vai } y \equiv 0(\text{mod p})$$
(*nulles dalītāju neeksistence*),
3. ja p ir pirmskaitlis, tad katram $x \in \mathbb{Z}/m\mathbb{Z}$ tādam , ka
$$x \not\equiv 0(\text{mod p})$$
eksistē viens un tikai viens $z \in \mathbb{Z}/m\mathbb{Z}$, kas apmierina vienādību
$$xz \equiv 1(\text{mod p}),$$

4. ja m nav pirmskaitlis, tad eksistē nenulles elementi x un y tādi, ka
$$xy \equiv 0(\text{mod m}),$$
5. x ir invertējams attiecībā uz reizināšanu pēc moduļa m (eksistē viens un tikai viens y tāds, ka $xy \equiv 1(\text{mod m})$) tad un tikai tad, ja $LKD(x, m) = 1$ (*multiplikatīvi inversā elementa eksistence*).

PIERĀDĪJUMS

1. Katram $x \in \mathbb{Z}$ eksistē viens un tikai viens $y \in \mathbb{Z}$, tāds, ka $x + y = m$, tātad skaitļa x atlikumu klase summā ar y klasi dos 0 klasi. Ja $x + y_1 \equiv x + y_2 \equiv 0(\text{mod m})$, tad $y_1 \equiv y_2(\text{mod m})$.

2. Ja p ir pirmskaitlis, tad no tā, ka $p|xy$ seko, ka $p|x$ vai $p|y$. Pārtulkojot to atlikumu klašu terminos: ja $xy \equiv 0(\text{mod p})$, tad $x \equiv 0(\text{mod p})$ vai $y \equiv 0(\text{mod p})$.

3. Ja p ir pirmskaitlis, tad jebkurš vesels skaitlis x robežās no 1 līdz $p - 1$ un p ir savstarpēji pirmskaitļi - $LKD(x, p) = 1$, tātad

saskaņā ar LKD lineārās kombinācijas īpašību eksistē veseli skaitļi a un b tādi, ka $ax + bp = 1$ un, tādējādi

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

tas nozīmē, ka skaitļa a klase reizinājumā ar x dod klasi 1,

4. Ja m nav pirmskaitlis, tad eksistē vismaz divi skaitļi $a > 1$ un $b > 1$, tādi, ka $ab = m$, no kurienes seko, ka

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

5. Ja $LKD(x, m) = 1$, tad eksistē skaitļi a un b tādi, ka

$$ax + bm = 1$$

un reducējot abas puses pēc moduļa m, iegūsim, ka

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

Ja eksistē divas klases y_1 un y_2 tādas, ka

$$xy_1 \equiv xy_2 \equiv 1(\text{mod m}),$$

tad

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

Reizinot abas puses ar y_1 vai y_2, iegūsim $y_1 - y_2 \equiv 0(\text{mod m})$, tātad $y_1 \equiv y_2(\text{mod m})$. Ja eksistē y tāds, ka $xy \equiv 1(\text{mod m})$, tad $xy - 1 = mq$ un $xy - mq = 1$. Reducējot pēc moduļa $d = LKD(x, m)$, iegūsim $0 \equiv 1(\text{mod d})$, tātad $d = 1$.

■

Par naturāla skaitļa n *Eilera funkciju* $\varphi(n)$ sauksim tādu veselu skaitļu x skaitu, kuriem izpildās nosacījumi

- $0 \leq x < n$,
- $LKD(x, n) = 1$.

1.1. piezīme. No iepriekšējās teorēmas seko, ka to atlikuma klašu skaits pēc moduļa m, kurām eksistē multiplikatīvi inversais elements, ir vienāds ar $\varphi(m)$. Šādas atlikumu klases sauksim par *invertējamām pēc moduļa* m.

Jebkuru šādu klašu pārstāvju kopu sauksim par *reducētu atlikumu klašu kopu pēc moduļa* m. Kopas $\mathbb{Z}/m\mathbb{Z}$ multiplikatīvi invertējamo elementu kopu apzīmēsim ar $(\mathbb{Z}/m\mathbb{Z})^\times$ vai U_m.

1.1. piemērs. $\varphi(p) = p - 1$, jo visi skaitļi kopā $\{1, ..., p-1\}$ ir savstarpēji pirmskaitļi ar p un $LKD(0, p) = p$.

$\varphi(4) = |\{1, 3\}| = 2.$
$3^{-1} \equiv 3.$
$\varphi(6) = |\{1, 5\}| = 2.$
$5^{-1} \equiv 5.$
$\varphi(8) = |\{1, 3, 5, 7\}| = 4.$
$3^{-1} \equiv 3.\ 5^{-1} \equiv 5.\ 7^{-1} \equiv 7.$
$\varphi(9) = |\{1, 2, 4, 5, 7, 8\}| = 6.$
$2^{-1} \equiv 5.\ 5^{-1} \equiv 2.\ 4^{-1} \equiv 7.\ 7^{-1} \equiv 4.\ 8^{-1} \equiv 8.$

2. Atlikumu gredzeni un algebriskās struktūras

2.1. Ievads algebriskajās struktūrās

2.1.1. Grupas

Par *grupu* sauc kopu G, kurā ir uzdota viena binära (divu argumentu) operācija

$$G \times G \to G, (x, y) \mapsto xy$$

kas apmierina šādas īpašības:

- operācija ir asociatīva: $(xy)z = x(yz)$ visiem x, y, z,
- eksistē neitrālais elements e: $xe = ex = x$ katram $x \in G$,
- katram elementam eksistē inversais elements: katram $x \in G$ eksistē $y \in G$ tāds, ka $xy = yx = e$.

Grupas operāciju apzīmē ar kādu atdalošo simbolu $(\cdot, *, +)$.

Ja ir dotas divas grupas G_1 un G_2, tad funkciju $f : G_1 \to G_2$ sauc par *grupu homomorfizmu*, ja tā saglabā grupas operāciju (komutē ar grupas operāciju):

$$f(x *_{G_1} y) = f(x) *_{G_2} f(y).$$

Grupas jēdziens ir viens no svarīgākajiem algebrā un vispār matemātikā.

Grupas operācija var būt gan komutatīva, gan arī nekomutatīva. Vispārīgā gadījumā, kad grupa var būt nekomutatīva, lieto *multiplikatīvo pierakstu* - atdalošu simbolu nelieto, inverso elementu apzīmē ar x^{-1}. Ja ir zināms, ka grupa ir komutatīva, tad bieži izmanto *aditīvo pierakstu* - par atdalošo simbolu izmanto + vai līdzīgu simbolu, neitrālo elementu apzīmē ar 0, inverso elementu $-x$.

Grupas apakšstruktūras - grupas apakškopu H sauksim par *apakšgrupu*, ja tā satur neitrālo elementu un ir slēgta attiecībā uz operāciju:

ja $x' \in H$ un $y' \in H$, tad $x'y' \in H$. Apzīmējums: $H \leq G$.

Grupas faktorstruktūras - *faktorgrupas*. Katrai apakšgrupa H definē kreisās un labās *blakusklases* - kopas

$$gH = \{gh | h \in H\}$$

un

$$Hg = \{hg | h \in H\}.$$

Tādējādi tiek definēti divi kopas G sadalījumi un divas ekvivalences attiecības.

Noteiktos apstākļos (piemēram, ja G ir komutatīva grupa) var definēt operāciju blakusklašu kopā G/H līdzīgi tam kā tika definētas operācija atlikumu klasēs -

- izvēlamies no katras klases vienu pārstāvi,
- atrodam operācijas rezultātu,
- definējam klašu operācijas rezultātu kā pārstāvju operācijas rezultāta klasi.

2.1. teorēma. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ar saskaitīšanas operāciju ir grupas.

2.2. teorēma. $m\mathbb{Z}$ ar saskaitīšanas operāciju ir grupa.

2.3. teorēma. Redukcija pēc moduļa m ir grupu homomorfizms $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

2.1.2. Gredzeni

Par *gredzenu* sauc kopu R, kurā ir uzdotas divas bināras operācijas

$$(x, y) \mapsto x + y, (x, y) \mapsto xy,$$

kas apmierina šādas īpašības:

- attiecībā uz operāciju + R ir komutatīva grupa (asociativitātes, neitrālais elements 0, inversais elements, komutativitāte),
- operācija $\cdot$ ir asociatīva,
- ir spēkā kreisā un labā distributīvās īpašības: $a(b + c) = ab + ac, (a + b)c = ac + bc$.

Ja ir doti divi gredzeni R_1 un R_2, tad funkciju $f : R_1 \to R_2$ sauc par *gredzenu homomorfizmu*, ja tā saglabā gredzena operācijas (komutē ar gredzena operācijām):

$$f(x *_{R_1} y) = f(x) *_{R_2} f(y), f(x +_{R_1} y) = f(x) +_{R_2} f(y).$$

Gredzenu sauc par komutatīvu, ja operācija $\cdot$ ir komutatīva. Gredzenu sauc par gredzenu ar vienīnieku, ja eksistē netrālais elements 1 attiecībā uz reizināšanas operāciju: $x \cdot 1 = 1 \cdot x = x$. Gedzena elementu sauksim par invertējamu, ja tam eksistē labais un kreisais inversais elements attiecībā uz reizināšanu. Gredzenu sauc par *lauku*, ja visi nenulles elementi ir invertējami.

Gredzena apakšstruktūras - *ideāli* un *apakšgredzeni*. Kopu I sauc par ideālu, ja tas

- ir apakšgrupa attiecībā uz $+$,
- ir invariants attiecībā uz reizināšanu ar gredzena elementiem - ja $r \in R$ un $i \in I$, tad $ri \in I$.

Ideāla piemērs - kopa $m\mathbb{Z}$ gredzenā $\mathbb{Z}$.

Kopu S sauc par apakšgredzenu, ja tas ir slēgts atiecībā uz abām gredzena operācijām.

Gredzena faktorstruktūra - *faktorgredzens*. Ja ir dots ideāls I, tad faktorgredzenu R/I konstruē līdzīgi atlikumu klašu gredzenam.

2.4. teorēma. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ar saskaitīšanas un reizināšanas operācijām ir komutatīvi gredzeni ar vieninieku. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ir lauki.

2.5. teorēma. Redukcija pēc moduļa m ir gredzenu homomorfizms $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

2.2. Pārskats par atlikumu gredzenu algebriskajām īpašībām

2.6. teorēma. (Kopsavilkums par $\mathbb{Z}/m\mathbb{Z}$ aditīvo struktūru) Kopa $\mathbb{Z}/m\mathbb{Z}$ ar atlikumu saskaitīšanas operāciju $+$ apmierina šādas īpašības:

- tā ir slēgta attiecībā uz saskaitīšanu,
- saskaitīšana ir asociatīva,
- saskaitīšana ir komutatīva,
- eksistē neitrālais elements 0,
- katram elementam eksistē inversais elements attiecībā uz saskaitīšanu.

2.1. piezīme. Ievērosim, ka šīs īpašības ir identiskas veselo skaitļu īpašībām attiecībā uz saskaitīšanu.

2.2. piezīme. $\mathbb{Z}/m\mathbb{Z}$ ar operāciju $+$ ir komutatīva grupa.

2.3. piezīme. $\mathbb{Z}/m\mathbb{Z}$ ir $\mathbb{Z}$ faktorgrupa attiecībā uz apakšgrupu $\mathbb{Z}$.

2.7. teorēma. (Kopsavilkums par $\mathbb{Z}/m\mathbb{Z}$ multiplikatīvo struktūru) Kopa $\mathbb{Z}/m\mathbb{Z}$ ar atlikumu reizināšanas operāciju $\cdot$ apmierina šādas īpašības:

- tā ir slēgta attiecībā uz reizināšanu,
- reizināšana ir asociatīva,
- reizināšana ir komutatīva,
- eksistē neitrālais elements 1,
- ir spēkā distributīvā īpašība,
- dažos gadījumos elementam eksistē inversais elements attiecībā uz reizināšanu,
- multiplikatīvi invertējamo elementu kopa ir slēgta attiecībā uz reizināšanu.

2.4. piezīme. Ievērosim, ka šīs īpašības ir līdzīgas veselo skaitļu īpašībām attiecībā uz reizināšanu. Atšķirība ir tur, ka eksistē vairāk invertējamu elementu.

2.5. piezīme. $\mathbb{Z}/m\mathbb{Z}$ ir komutatīvs gredzens ar vieninieku.

2.6. piezīme. $\mathbb{Z}/m\mathbb{Z}$ ir lauks tad un tikai tad, ja m ir pirmskaitlis (lauku $\mathbb{Z}/p\mathbb{Z}$ parasti apzīmē kā $\mathbb{F}_p^*$ vai $GF(p)$).

2.7. piezīme. $\mathbb{Z}/m\mathbb{Z}$ ir $\mathbb{Z}$ faktorgredzens attiecībā uz ideālu $m\mathbb{Z}$.

2.8. piezīme. $\mathbb{Z}/m\mathbb{Z}$ multiplikatīvi invertējamie elementi veido komutatīvu grupu attiecībā uz reizināšanas operāciju.

3. Eilera funkcija un tās īpašības

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

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

3.1. piezīme. No iepriekš pierādītas teorēmas seko, ka to atlikuma klašu skaits pēc moduļa m, kurām eksistē multiplikatīvi inversais elements, ir vienāds ar $\varphi(m)$.

3.2. piezīme. Ja $m \equiv m'(\text{mod n})$, tad

$$LKD(m, n) = LKD(m + nq, n) = LKD(m', n),$$

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

3.1. teorēma. Eilera funkcijai piemīt šādas īpašības:

1. Eilera funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ nav ne injektīva, ne sirjektīva,
2. ja $LKD(n, m) = 1$, tad
$$\varphi(nm) = \varphi(n)\varphi(m)$$
(Eilera funkcija ir *multiplikatīva*),
3. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$,
4. ja $n = p_1^{\alpha_1} ... p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$, tad
$$\varphi(n) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}),$$

PIERĀDĪJUMS

1. Eilera funkcija nav injektīva, jo $\varphi^{-1}(2) = \{3, 4, 6\}$. Eilera funkcija nav sirjektīva, jo $\varphi^{-1}(3) = \emptyset$.

2. Pieņemsim, ka n un m ir savstarpēji pirmskaitļi. 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 $\varphi(nm) = \varphi(n)\varphi(m)$.

3. Ja $n = p^\alpha$, tad $LKD(n, m) \neq 1$ tad un tikai tad, ja $p|m$, tātad $m = p \cdot k$, kur $0 \leq p \cdot k < p^\alpha$. Redzam, ka $0 \leq k < p^{\alpha-1}$, tātad tādu skaitļu m skaits ir $|\{0, p, ..., p^{\alpha-1} - 1\}| = p^{\alpha-1}$. Esam ieguvuši, ka $\varphi(n) = p^\alpha - p^{\alpha-1}$.

4. Rezultāts seko no iepriekšējiem teorēmas apgalvojumiem un algebriskiem pārveidojumiem. Sadalīsim n pirmskaitļu pakāpju reizinājumā

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}.$$

Ievērosim, ka dažādu pirmskaitļu pakāpes ir savstarpēji pirmskaitļi.

Vairākas reizes pielietosim multiplikatīvo īpašību:

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

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

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

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

■

3.1. piemērs. $\varphi(2007) = \varphi(3^2 \cdot 223) = (3^2 - 3^1) \cdot 222 = 6 \cdot 222 = 1332$.
$\varphi(2008) = \varphi(2^3 \cdot 251) = (2^3 - 2^2) \cdot 250 = 4 \cdot 250 = 1000$. $\varphi(1000) = 400$, $\varphi(400) = 160$, ... $\varphi(160) = 64$,

3.3. piezīme. Ja $n = p_1 p_2$ (divu pirmskaitļu reizinājums), tad

$$\varphi(n) = (p_1 - 1)(p_2 - 1).$$

Redzam, ka $\varphi(n)$ var viegli aprēķināt, ja p_1 un p_2 ir zināmi. Šo faktu izmanto kriptogrāfijā.

4. 6.mājasdarbs

6.1 Katram atlikumu gredzenam pēc moduļiem 3, 5, 7, 11, 13 atrodiet visas klases, kuru pakāpes veido dotā gredzena nenulles elementus (visus a tādus, ka katrs $x \not\equiv 0(\text{mod p})$ ir izsakāms formā $a^k(\text{mod p})$).

6.2 Gredzena elementu a sauksim par *idempotentu*, ja $a^2 = a$. Gredzena elementu a sauksim par *nilponentu*, ja $a^k = 0$ kādam $k \in \mathbb{N}$. Atrast visus idempotentos un nilpotentos elementus gredzenā $\mathbb{Z}/12\mathbb{Z}$.

6.3 Atrodiet šādus skaitļus:

a) $\varphi(6036)$,
b) visus naturālos skaitļus x, kuriem $\varphi(x) = \varphi(6036)$.

6.4 Pierādiet, ka visiem naturāliem n un k izpildās

$$\varphi(n^k) = n^{k-1}\varphi(n).$$

(*Norādījums: sadaliet n pirmskaitļu pakāpju reizinājumā*)