DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Studiju kurss

Veselo skaitļu teorija

4.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi 26

Lekcijas mērķis:

- apgūt modulārās aritmētikas pamatus,
- apgūt svarīgākos modulārās aritmētikas pielietojumus.

Lekcijas kopsavilkums:

- atlikumu klašu kopās var definēt operācijas un pētīt to īpašības, kas seko no veselo skaitļu īpašībām,
- atlikumu operācijas var tikt izmantotas dažādos veidos.

Svarīgākie jēdzieni: atlikumu klase mod m, pilna un kanoniska atlikumu klašu pārstāvju kopa, redukcija mod m, operācijas ar atlikumu klasēm, multiplikatīvi invertējama atlikumu klase, Eilera funkcija φ, pozicionālais pieraksts, dalāmības pazīmes.

Svarīgākie fakti un metodes: atlikumu klašu operāciju īpašības, aritmētisko operāciju pārbaude, pozicionālo pierakstu pārveidošanas algoritmi.

1. Atlikumu klašu gredzens

1.1. Salīdzināmības mod m ekvivalences klases

Salīdzināmības attiecībai atbilstošā veselo skaitļu kopas sadalījuma apakškopas vai klases sauc par *atlikumu klasēm mod m*. Katrā atlikumu klasē ir visi veselie skaitļi, kas dalījumā ar m dod vienu un to pašu atlikumu.

1.1. piemērs. $m = 2$, $\mathbb{Z} = C_0 \bigcup C_1$, kur
C_0 ir 0 klase - pāra skaitļi, $2k$,
C_1 ir 1 klase - nepāra skaitļi, $2k + 1$.

$m = 3$, $\mathbb{Z} = C_0 \bigcup C_1 \bigcup C_2$, kur
C_0 ir 0 klase - skaitļi formā $3k$,
C_1 ir 1 klase - skaitļi formā $3k + 1$,
C_2 ir 2 klase - skaitļi formā $3k + 2$.

1.1. teorēma. Atlikumu klašu skaits mod m ir vienāds ar $|m|$.

PIERĀDĪJUMS Atlikums dalot ar m var būt vesels skaitlis robežās no 0 līdz $|m|-1$, tātad klašu skaits ir $|m|$.■

Jebkuru kopas $\mathbb{Z}$ apakškopu, kas satur tieši vienu elementu no katras atlikumu klases, sauksim par *pilnu atlikumu klašu pārstāvju kopu (PAK)*.

Par *kanonisko klašu pārstāvju kopu sauksim kopu*

$$\{0, 1, ..., |m|-1\}.$$

Ja m ir nepāra skaitlis, tad var izmantot arī atlikumu klašu pārstāvju kopu, kas ir simetriska attiecībā uz 0:

$$\{-\frac{|m|-1}{2}, ... -1, 0, 1, ..., \frac{|m|-1}{2}\}, \text{ja m ir nepāra skaitlis.}$$

Skaitļa r atlikuma klasi mod m, bieži apzīmē kā $m\mathbb{Z}+r$.

Atlikumu klašu sadalījums (faktorkopa) mod m, kuru apzīmē kā $\mathbb{Z}/m\mathbb{Z}$ vai $\mathbb{Z}_m$ definē sirjektīvu funkciju - dabisko projekciju

$$\pi_m : \mathbb{Z} \to \mathbb{Z}_m,$$

kas katram skaitlim piekārto to atlikumu klasi, kurai tas pieder.

Skaitlim n atlikumu klasi $\pi_m(n) = \overline{n} = [n]$ sauksim par n *redukciju mod* m. Strādājot ar atlikumu klasēm parasti ekonomijas nolūkā $[n]$ raksta kā n.

1.2. Operācijas ar atlikumu klasēm

Fiksēsim skaitli m. Par divu atlikumu klašu mod m C un D summu $C + D$, sauksim klasi $\pi_m(a + b)$, kur $a \in C$ un $b \in D$.

Par divu atlikumu klašu C un D reizinājumu CD, sauksim klasi $\pi_m(ab)$, kur $a \in C$ un $b \in D$.

1.2. piemērs. $[2] + [3] = [5] = [0] (\text{mod } 5)$,
$[2] \cdot [3] = [6] = [1] (\text{mod } 5)$.

1.3. Atlikumu klašu operāciju īpašības

1.2. teorēma. (*atlikumu operāciju pamatīpašības*)

1. Atlikuma klašu operācijas ir definētas korekti - nav atkarīgas no pārstāvju izvēles.
2. $\pi(a+b) = \pi(a) + \pi(b)$.
3. $\pi(ab) = \pi(a)\pi(b)$.
4. $C + C' = C' + C$.
5. $CC' = C'C$.
6. $(C + C') + C'' = C + (C' + C'')$.
7. $(CC')C'' = C(C'C'')$.
8. $C(C' + C'') = CC' + CC''$.
9. $[0] + C = C + [0] = C$.
10. $[1] \cdot C = C$.

PIERĀDĪJUMS

1. Pieņemsim, ka $a \equiv a' (\mathrm{mod}\ m)$, $b \equiv b' (\mathrm{mod}\ m)$ - a un a' pārstāv vienu klasi, b un b' pārstāv vienu klasi.

$$\begin{cases} a \equiv a' (\mathrm{mod}\ m) \\ b \equiv b' (\mathrm{mod}\ m) \end{cases} \Longrightarrow a + b \equiv a' + b' (\mathrm{mod}\ m).$$

2., 3. Seko no klašu operāciju definīcijām.

4.-10. Seko no aritmētisko operāciju īpašībām. ■

Atlikumu kopu mod m ar tajā uzdotām saskaitīšanas un reizināšanas operācijām sauksim par *atlikumu gredzenu mod* m $(\mathbb{Z}_m, +, \cdot)$. Atlikumu klašu vienādību apzīmēsim ar pierakstu $\equiv \ (\mathrm{mod}\ m)$.

1.1. piezīme. Par atlikumu klašu kopu var domāt kā par veselo skaitļu kopu, kas ir "uztīta" uz riņķa līnijas. Atbilstoši var interpretēt operācijas ar atlikumu klasēm.

1.3. teorēma. Atlikumu gredzenā $\mathbb{Z}_m$ 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. $m \notin \mathbb{P} \Longrightarrow \exists$ vismaz divi skaitļi $a > 1$ un $b > 1 : \ ab = m \Longrightarrow$

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

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 $d = LKD(x, m) \Longrightarrow 0 \equiv 1(\text{mod d}) \Longrightarrow d = 1$. ■

Par $n \in \mathbb{N}$ *Eilera funkciju* $\varphi(n)$ sauksim tādu $x \in \mathbb{Z}$ skaitu, kuriem izpildās nosacījumi

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

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

Jebkuru šādu klašu pārstāvju kopu sauksim par *reducētu atlikumu klašu kopu mod m*. Kopas $\mathbb{Z}_m$ multiplikatīvi invertējamo elementu kopu apzīmēsim ar $(\mathbb{Z}_m)^\times$ vai $\mathcal{U}_m$.

1.3. 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. Modulārās aritmētikas pielietojumi

2.1. Aritmētisko operāciju pārbaude

Aritmētisko operāciju rezultātu pareizības pārbaudē var izmantot vienu no modulārās aritmētikas īpašībām:

$$a = b \implies a \equiv b \pmod{m} \forall m.$$

Pretējais apgalvojums:

$$\exists m : a \not\equiv b \pmod{m} \implies a \neq b.$$

Pārbaudes algoritms:

1. Atrodam operācijas rezultātu $c = a \star b$,
2. Atrodam $c' = a \star b \pmod{m}$ un $c'' = c \pmod{m}$),
3. Ja $c' \neq c''$, tad konstatējam kļūdu.

2.2. Pozicionālais pieraksts

2.2.1. Teorija

Senajos laikos cilvēki izmantoja primitīvu skaitļu pierakstu, kas pēc būtības ir līdzīgs svītriņu vilkšanai (*nepozicionālās sistēmas*), piemēram:

- viena svītriņa (I) - vieninieks vai viens objekts,
- pārsvītrota svītriņa (X) - desmitnieks vai desmit objekti,
- īpaši simboli (hieroglifiskajās sistēmās), kas apzīmē 100 u.t.t.
- burti (alfabētiskās sistēmas senajā Grieķijā un Izraēlā)

Šādā pierakstā simbola vietai nav lielas nozīmes. Parasti simboli tika sakārtoti noteiktā kārtībā, piemēram, lielākā svara simboli atradās pieraksta sākumā.

Problēmas - ar šādu pierakstu grūti veikt aritmētiskās operācijas.

Būtiskas izmaiņas notika tad, kad cilvēki sāka pierakstīt skaitļus tā, lai simbola atrašanās vietai būtu lielāka nozīme - *pozicionālajās sistēmās*. Tāds pieraksts tika ieviests Indijā ap 500 AD. Viduslaikos tas tika pārņemts Eiropā un tiek izmantots līdz pat mūsu dienām.

2.1. teorēma. $m \in \mathbb{N}$. $\forall\, n \in \mathbb{N}$ ir viennozīmīgi izsakāms formā

$$n = \sum_{i=0}^{k} a_i m^i, \text{ kur } a_k \neq 0, \ \forall\, i : 0 \leq a_i < m.$$

PIERĀDĪJUMS Aprakstīsim algoritmu, ar kura palīdzību var atrast skaitļus a_i:

1. Izdalīsim n ar m:
$$n = q_1 m + a_0;$$
2. Izdalīsim q_1 ar m:
$$q_1 = q_2 m + a_1,$$
ievērosim, ka

$$n = q_1 m + a_0 = (q_2 m + a_1)m + a_0 = q_2 m^2 + a_1 m + a_0;$$

3. Izdalīsim q_2 ar m:

$$q_2 = q_3 m + a_2,$$

ievērosim, ka

$$n = q_2 m^2 + a_1 m + a_0 =$$
$$(q_3 m + a_2)m^2 + a_1 m + a_0 =$$
$$q_3 m^3 + a_2 m^2 + a_1 m + a_0;$$

... ...

Algoritms tiek uzskatīts par pabeigtu, kad kārtējais dalījums ir vienāds ar 0 - pēdējais nenulles atlikums ir a_k.

Ievērosim, ka algoritma izpilde vienmēr apstājas, jo dalījumu virkne $q_1, q_2, ...$ ir stingri dilstoša.

Algoritma izpildes rezultātā iegūsim skaitļu virkni $(a_0, a_1, ..., a_k)$, kas apmierina vienādību

$$n = a_k m^k + a_{k-1} m^{k-1} + ... + a_2 m^2 + a_1 m + a_0,$$

tātad skaitļu virkne, kas ir deklarēta teorēmas apgalvojumā, eksistē.

Pierādīsim šādas skaitļu virknes $(a_0, a_1, ..., a_k)$ vienīgumu. Pieņemsim, ka eksistē divi izvirzījumi

$$n = a_k m^k + a_{k-1} m^{k-1} + ... + a_2 m^2 + a_1 m + a_0 = \\ b_k m^k + b_{k-1} m^{k-1} + ... + b_2 m^2 + b_1 m + b_0$$

un sāksim salīdzināt skaitļus a_i un b_i sākot no $i = 0$:

1. $n \equiv a_0 \equiv b_0 \pmod{\text{m}} \implies a_0 = b_0$.
2. Reducēsim $\frac{n-a_0}{m}$ pēc moduļa m:

$$\frac{n - a_0}{m} = a_k m^{k-1} + ... + a_2 m + a_1 \equiv a_1 \equiv \\ b_k m^{k-1} + ... + b_2 m + b_1 \equiv b_1 \pmod{\text{m}},$$

tāpēc

$$a_1 = b_1,$$

3. Reducēsim $\frac{n-a_0-a_1m}{m^2}$ pēc moduļa m:

$$\frac{n-a_0-a_1m}{m^2} = a_km^{k-2} + ... + a_3m + a_2 \equiv a_2 \equiv$$
$$b_km^{k-2} + ... + b_3m + b_2 \equiv b_2 \pmod{\text{m}},$$

tāpēc

$$a_2 = b_2$$

■

2.1. piezīme. Skaitļa izvirzījumu m pakāpju lineārās kombinācijas veidā sauksim par skaitļa *m-āro pozicionālo pierakstu* (vai par *m-adisko pierakstu*) un apzīmēsim ar $\overline{a_ka_{k-1}...a_0}_m$ vai kādā vienkāršākā veidā, ja nav riska pārprast pierakstu. Pēc noklusēšanas pieņemsim $\overline{a_ka_{k-1}...a_0} = \overline{a_ka_{k-1}...a_0}_{10}$. Skaitli m sauksim par pieraksta *bāzi*.

2.2.2. Pārveidošanas algoritmi

2.2. piezīme. Mūsdienās cilvēki gandrīz vienmēr strādā ar decimālo pierakstu ($m = 10$), arī ciparu skaits ir saskaņots ar šo m vērtību.

Plašāk pielietotie pieraksti datorzinātnēs un datortehnoloģijās -

- $m = 2$ - *binārais* pieraksts, simbolus $0, 1$ sauc par *bitiem*,
- $m = 8$ - *oktālais* pieraksts,
- $m = 16$ (ar cipariem $0,1,2,3,4,5,6,7,8,9, A = 10, B = 11, C = 12, D = 13, E = 14, F = 15$) - *heksadecimālais* pieraksts.

Algoritms skaitļa n pārveidošanai no decimālās sistēmas uz m-āro sistēmu:

1. izdalīt n ar m: $n \to (q_1, a_0)$, kur $n = q_1 m + a_0$, ja $q_1 \neq 0$, tad iet tālāk;
2. izdalīt q_1 ar m: $(q_1, a_0) \to (q_2, a_1)$, kur $q_1 = q_2 m + a_1$, ja $q_2 \neq 0$, tad iet tālāk;
3. izdalīt q_2 ar m: $(q_2, a_1) \to (q_3, a_2)$, kur $q_2 = q_3 m + a_2$, ja $q_3 \neq 0$, tad iet tālāk;

... izdalīt ...

k+1. Uzrakstīt simbolus pareizā kārtībā - $\overline{a_k a_{k-1} \ldots a_0}_m$;

k+2. Veikt pārbaudi: $a_k m^k + a_{k-1} m^{k-1} + ... + a_0 \stackrel{?}{=} n$.

2.1. piemērs. Pārveidosim skaitli 2007 5-ārajā pierakstā:

1. $2007 = 401 \cdot 5 + 2 \rightarrow a_0 = 2, q_1 = 401$;
2. $401 = 80 \cdot 5 + 1 \rightarrow a_1 = 1, q_2 = 80$;
3. $80 = 16 \cdot 5 + 0 \rightarrow a_2 = 0, q_3 = 16$;
4. $16 = 3 \cdot 5 + 1 \rightarrow a_3 = 1, q_4 = 3$;
5. $3 = 0 \cdot 5 + 3 \rightarrow a_4 = 3, q_5 = 0$;
6. Pierakstām rezultātu $2007 = \overline{31012}_5$;
7. Veicam pārbaudi: $3 \cdot 5^4 + 1 \cdot 5^3 + 0 \cdot 5^2 + 1 \cdot 5^1 + 2 = 1875 + 125 + 5 + 2 = 2007$.

Algoritms skaitļa n pārveidošanai no m-ārās sistēmas uz decimālo sistēmu:

1. Ja ir dots skaitlis $n = \overline{a_k a_{k-1} ... a_0}_m$, aprēķināt decimālajā pierakstā summu
$$n = a_k m^k + a_{k-1} m^{k-1} + ... + a_0.$$

2.2. piemērs. Ja skaitlis 7-ārajā pierakstā ir $\overline{3621}_7$, tad decimālajā pierakstā tas ir $3 \cdot 7^3 + 6 \cdot 7^2 + 6 \cdot 7^1 + 1 = 1338$.

Algoritms skaitļa n pārveidošanai no m_1-ārās sistēmas uz m_2-āro sistēmu:

1. Pārveidot skaitli n no m_1-ārā pieraksta uz decimālo pierakstu,
2. Pārveidot skaitli n no decimālā pieraksta uz m_2-āro pierakstu.

2.3. piemērs. Pārveidosim skaitli $\overline{3621}_7$ uz heksadecimālo pierakstu:
$$\overline{3621}_7 \to 1338 \to \overline{53A}_{16}$$

2.3. piezīme. Pozicionālās sistēmas plusi:

- simbolu ekonomija,
- ērti veikt aritmētiskās operācijas - algoritmi visiem ir zināmi, tos var vispārināt no $m = 10$ uz jebkuru m vērtību.

2.3. Dalāmības pazīmes

Dalāmības ar m pazīme - īpašība, kas piemīt m daudzkārtņu cipariem (parasti 10-ārajā pierakstā).

Šajā sadaļā pieņemam, ka

$$n = \overline{a_k a_{k-1} ... a_0} = a_k \cdot 10^k + ... + a_1 \cdot 10 + a_0.$$

2.3.1. Pamatideja

$n \in \mathbb{N}$. Lai atrastu dalāmības pazīmi ar m, ir lietderīgi izteikt n decimālajā pierakstā un apskatīt $n (\text{mod } m)$:

$$n = \overline{a_k a_{k-1} ... a_0} = a_k \cdot 10^k + ... + a_1 \cdot 10 + a_0 (\text{mod } m).$$

2.3.2. Dalāmība ar 3

Tā kā $10^l \equiv 1 \pmod 3$, tad

$$n \equiv a_k \cdot 1 + a_{k-1} \cdot 1 + ... + a_0 \equiv a_k + a_{k-1} + ... + a_0 \pmod 3.$$

Dalāmības pazīme ar 3:

$$3|n \iff 3|a_k + a_{k-1} + ... + a_0$$

(ja n ciparu summa dalās ar 3).

2.3.3. Dalāmība ar 11

Tā kā $10 \equiv -1 \pmod{11}$, tad

$$10^{2j} \equiv (-1)^{2j} \equiv 1 \pmod{11}$$

un

$$10^{2j+1} \equiv (-1)^{2j+1} \equiv -1 \pmod{11}.$$

Redzam, ka

$$n \equiv a_k(-1)^k + ... + a_2 - a_1 + a_0 \pmod{11}.$$

Dalāmības pazīme ar 11:

$$11|n \iff 11|a_0 - a_1 + a_2 + ... + a_k(-1)^k$$

(ja n ciparu alternējoša summa dalās ar 11).

3. 4.mājasdarbs

3.1. Obligātie uzdevumi

4.1 Atrodiet saskaitīšanas un reizināšanas tabulas atlikumu klasēm mod 7 un 8. Uzrādiet visus elementus, kuriem eksistē multiplikatīvi inversie elementi.

4.2 Katram atlikumu gredzenam mod $3, 5, 7, 11, 13$ 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 $a^k (\text{mod p})$).

4.3 Skaitli 2008 pārveidojiet šādos pozicionālajos pierakstos:

a) binārajā,
b) oktālajā,
c) heksadecimālajā,
d) ternārajā.

4.4 Atrodiet dalāmības pazīmi ar

(a) 18;
(b) 7.

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

4.5 Pierādīt, ka

(a) maksimālais naturālais skaitlis, ko var ierakstīt m-ārajā sistēmā ar k simboliem ir vienāds ar $m^{k+1} - 1$,

(b) lai skaitli n ierakstītu m-ārajā sistēmā, ir nepieciešami

$$k_n = [\log_m n] + 1$$

simboli.