DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Studiju kurss

SKAITĻU TEORIJA

5.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

- apgūt "ķīniešu atlikumu teorēmu" un tās vispārinājumus,
- apgūt veselo skaitļu pozicionālo pierakstu.

Lekcijas kopsavilkums:

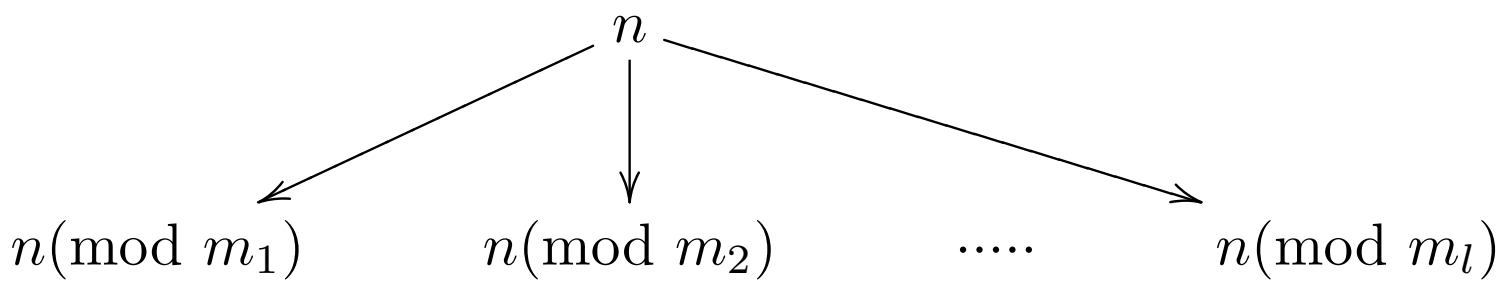
- var meklēt veselus skaitļus, ja ir zināmi to atlikumi pēc vairākiem moduļiem,
- var vispārināt decimālo pierakstu uz patvaļīgu bāzi.

Svarīgākie jēdzieni: pozicionālais pieraksts.

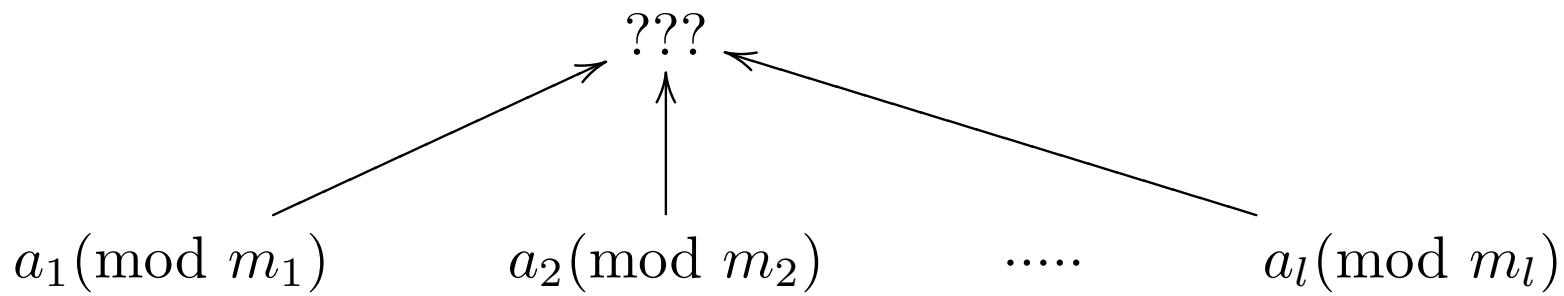
Svarīgākie fakti un metodes: klasiskā ķīniešu atlikumu teorēma (ĶAT), ĶAT ar vairākiem vienādojumiem, pastiprinātās ĶAT, pozicionālo pierakstu pārveidošanas algoritmi.

1. Ķīniešu atlikumu teorēma

Ja $n \in \mathbb{Z}$, tad $\forall\ m_1, ..., m_l$ var atrast $n(\mathrm{mod}\ m_1)$,...,$n(\mathrm{mod}\ m_l)$:



Vai ir iespējams "rekonstruēt" n, ja ir zināmi tā atlikumi mod m_1,..., mod m_l? Vai n ir viennozīmīgi noteikts?



1.1. Divu vienādojumi

1.1. teorēma. (*Ķīniešu atlikumu teorēma (ĶAT)- klasiskais variants*) $LKD(m_1, m_2) = 1 \implies \forall\, a, b \in \mathbb{Z}\ \exists$ tieši viena klase $c (\mathrm{mod}\ m_1 m_2)$:

$$\begin{cases} x \equiv a\ (\mathrm{mod}\ m_1) \\ x \equiv b\ (\mathrm{mod}\ m_2) \end{cases} \iff x \equiv c\ (\mathrm{mod}\ m_1 m_2)$$

PIERĀDĪJUMS $LKD(m_1, m_2) = 1 \implies a - b = (a - b) \cdot 1$ var tikt izteikts kā m_1 un m_2 lineāra kombinācija: $\exists\, u_1, u_2 \in \mathbb{Z}$:

$$a - b = u_1 m_1 + u_2 m_2.$$

Pārnesot dažus locekļus uz pretējām pusēm definēsim

$$\widetilde{x} = a - u_1 m_1 = b + u_2 m_2.$$

$$\begin{cases} \widetilde{x} \equiv a\ (\mathrm{mod}\ m_1) \\ \widetilde{x} \equiv b\ (\mathrm{mod}\ m_2) \end{cases} \implies \begin{cases} \widetilde{x} + q m_1 m_2 \equiv a\ (\mathrm{mod}\ m_1) \\ \widetilde{x} + q m_1 m_2 \equiv b\ (\mathrm{mod}\ m_2),\ \forall\, q \in \mathbb{Z} \end{cases}$$

$\implies$ visa $\widetilde{x}$ klase mod $m_1 m_2$ arī apmierina sistēmu.

Pieņemsim, ka divi skaitļi $\widetilde{x}_1$ un $\widetilde{x}_2$ apmierina sistēmu, tad

$$\begin{cases} \widetilde{x}_1 - \widetilde{x}_2 = m_1 q_1 \\ \widetilde{x}_1 - \widetilde{x}_2 = m_2 q_2 \end{cases} \Longrightarrow m_1 q_1 = m_2 q_2.$$

$$\begin{cases} m_1 \Big| m_2 q_2 \\ LKD(m_1, m_2) = 1 \end{cases} \Longrightarrow m_1 \Big| q_2 \Longrightarrow \widetilde{x}_1 - \widetilde{x}_2 = m_1 m_2 q'$$

$\Longrightarrow \widetilde{x}_1 - \widetilde{x}_2 \equiv 0 \pmod{m_1 m_2}$. Ir pierādīts, ka atrisinājumi veido vienu klasi mod $m_1 m_2$. ■

1.1. piemērs. Atrisināsim sistēmu

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5. \end{cases}$$

$3 - 2 = 1 = 2 \cdot 3 - 1 \cdot 5 \Longrightarrow x \equiv 3 + 1 \cdot 5 = 2 + 2 \cdot 3 = 8 \pmod{15}$.

1.2. Vairāki vienādojumi

1.2. teorēma. $LKD(m_i, m_j) = 1, \forall\ i, j \implies \forall\ a_1, ..., a_s \in \mathbb{Z}\ \exists$ tieši viena klase $c \pmod{m_1 ... m_s}$:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ ... \\ x \equiv a_s \pmod{m_s} \end{cases} \iff x \equiv c \pmod{m_1 ... m_s}$$

PIERĀDĪJUMS Risināsim doto vienādojumu sistēmu S vairākos soļos, katrā solī risinot sistēmu ar diviem vienādojumiem un pēctecīgi pievienojot jaunu vienādojumu iegūtajam atrisinājumam:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \iff x \equiv c_1 \pmod{m_1 m_2} \implies$$

$$S \iff \begin{cases} x \equiv c_1 \pmod{m_1 m_2} \\ x \equiv a_3 \pmod{m_3} \\ \dots \\ x \equiv a_s \pmod{m_s}. \end{cases}$$

$$\begin{cases} x \equiv c_1 \pmod{m_1 m_2} \\ x \equiv a_3 \pmod{m_3} \end{cases} \iff x \equiv c_2 \pmod{m_1 m_2 m_3} \implies$$

$$S \iff \begin{cases} x \equiv c_2 \pmod{m_1 m_2 m_3} \\ x \equiv a_4 \pmod{m_4} \\ \dots \\ x \equiv a_s \pmod{m_s}. \end{cases} \quad , \dots \blacksquare$$

1.2. piemērs. Atrisināsim sistēmu

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7}. \end{cases}$$

Zinām, ka pirmo divu vienādojumu atrisinājums ir $x \equiv 8 \pmod{15}$, tāpēc sistēma ir ekvivalenta divu vienādojumu sistēmai

$$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 5 \pmod{7}. \end{cases}$$

$$8 - 5 = 3 = 3 \cdot 15 - 6 \cdot 7 \implies x \equiv 8 - 3 \cdot 15 = -37 \equiv 68 \pmod{105}.$$

1.3. Vispārīgo moduļu gadījums

1.3. teorēma. $m = p_1^{\alpha_1} ... p_n^{\alpha_n}$. Vienādojums

$$x \equiv a (\mathrm{mod}\ m)$$

ir ekvivalents sistēmai

$$\begin{cases} x \equiv a (\mathrm{mod}\ p_1^{\alpha_1}) \\ x \equiv a (\mathrm{mod}\ p_2^{\alpha_2}) \\ \ldots \\ x \equiv a (\mathrm{mod}\ p_n^{\alpha_n}) \end{cases}$$

PIERĀDĪJUMS $LKD(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1 \implies$ apgalvojums seko no kongruences īpašības

$$\begin{cases} a \equiv b(\text{mod } m_1) \\ a \equiv b(\text{mod } m_2) \\ \dots \\ a \equiv b(\text{mod } m_n) \end{cases} \iff a \equiv b(\text{mod } MKD(m_1, ..., m_n)),$$

ja definē $m_i = p_i^{\alpha_i}$. ■

1.4. teorēma. Jebkura vienādojumu sistēma

$$\begin{cases} x \equiv a_1(\text{mod } m_1) \\ x \equiv a_2(\text{mod } m_2) \\ \dots \\ x \equiv a_s(\text{mod } m_s) \end{cases}$$

ir ekvivalenta vienādojumu sistēmai

$$\begin{cases} x \equiv b(\text{mod } q_1) \\ x \equiv b_2(\text{mod } q_2) \\ \dots \\ x \equiv b_t(\text{mod } q_t) \end{cases}$$

kur q_i ir pirmskaitļu pakāpes.

PIERĀDĪJUMS Katram vienādojumam $x \equiv a_i(\text{mod } m_i)$ atrodam atbilstošo ekvivalento sistēmu ar pirmskaitļu pakāpju moduļiem. Apvienojam visas iegūtās sistēmas vienā sistēmā, katram pirmskaitlim p apskatām vienādojumu apakšsistēmu, kas atbilst p pakāpju moduļiem. ■

Ķīniešu vienādojumu sistēmu risināšana ar patvaļīgiem moduļiem:

- atrodam dotajai sistēmai ekvivalento sistēmu ar pirmkaitļu pakāpju moduļiem, ja iegūstam pretrunīgu sistēmu, tad konstatējam, ka sistēma ir nesaderīga;
- atrisinam iegūto sistēmu ar pirmskaitļu pakāpju moduļiem pēc iepriekš dotas metodes.

1.3. piemērs. Atrisināsim sistēmu $\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 4 \pmod{20}. \end{cases}$.

$$x \equiv 2 \pmod 6 \iff \begin{cases} x \equiv 2 \pmod 2 \\ x \equiv 2 \pmod 3 \end{cases}$$

$$x \equiv 4 \pmod{20} \iff \begin{cases} x \equiv 4 \pmod 4 \\ x \equiv 4 \pmod 5 \end{cases}$$

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 4 \pmod{20}. \end{cases} \iff \begin{cases} x \equiv 0 \pmod 4 \\ x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \end{cases}$$

Atrisinot ar ĶAT metodi, iegūsim $x \equiv 44 \pmod{60}$.

2. Pozicionālais pieraksts

2.1. Teorija

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

- viena svītriņa (I) - vienīnieks 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, kaut arī izņēmumi. 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. $m \in \mathbb{N}$, $m \geq 2$. $\forall\, n \in \mathbb{N}$ 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 : $\boldsymbol{n = q_1 m + a_0;}$
2. Izdalīsim q_1 ar m : $\boldsymbol{q_1 = q_2 m + a_1,}$
   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 : $\boldsymbol{q_2 = q_3 m + a_2,}$

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 $\dfrac{n - a_0}{m} \bmod m$:

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

$\implies a_1 = b_1$,

3. ... u.t.t. ■

Skaitļa izvirzījumu m pakāpju lineārās kombinācijas veidā sauc par skaitļa *m-āro pozicionālo pierakstu* (vai par *m-adisko pierakstu*),

apzīmē ar $\overline{a_k a_{k-1} ... a_0}_m$ vai kādā vienkāršākā veidā.

m - bāze, a_i -m-adiskais cipars.

2.2. Pārveidošanas algoritmi

2.1. 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 simboliem $0,1,2,3,4,5,6,7,8,9,A = 10,B = 11,C = 12,D = 13,E = 14,F = 15$) - *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: $a_k m^k + a_{k-1} m^{k-1} + \ldots + a_0 \stackrel{?}{=} n$.

2.1. piemērs. Pārveidosim skaitli 2011 5-ārajā pierakstā:

1. $2011 = 402 \cdot 5 + 1 \to a_0 = 1, q_1 = 402$;
2. $402 = 80 \cdot 5 + 2 \to a_1 = 2, q_2 = 80$;

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 $2011 = \overline{31021}_5$;
7. Veicam pārbaudi: $3 \cdot 5^4 + 1 \cdot 5^3 + 0 \cdot 5^2 + 2 \cdot 5^1 + 1 = 1875 + 125 + 10 + 1 = 2011$.

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

1. Dots skaitlis $n = \overline{a_k a_{k-1} \ldots a_0}_m$. Aprēķināt decimālajā pierakstā summu
$$n = a_k m^k + a_{k-1} m^{k-1} + \ldots + a_0.$$

2.2. piemērs. $N = \overline{3621}_7 \Longrightarrow N = 3 \cdot 7^3 + 6 \cdot 7^2 + 6 \cdot 7^1 + 1 = 1338.$

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:

$$\overline{3621}_7 \to 1338 \to \overline{53A}_{16}$$

3. 4.mājasdarbs

3.1. Obligātie uzdevumi

4.1 Atrisināt vienādojumu sistēmas izmantojot ĶAT

(a) $\begin{cases} x \equiv 4 \pmod 7 \\ x \equiv 5 \pmod{11} \end{cases}$

(b) $\begin{cases} x \equiv 10 \pmod{12} \\ x \equiv 16 \pmod{18} \end{cases}$

4.2 Atrisināt vienādojumu sistēmas

(a) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \\ x \equiv 4 \pmod{11} \end{cases}$

(b) $\begin{cases} x \equiv 1 \pmod 8 \\ x \equiv 9 \pmod{20} \\ x \equiv 4 \pmod{15} \end{cases}$

4.3 Studentiem ir trīs dažādi studiju kursi - A,B un C. Semestra pirmajā nedēļā pirmdien notiek nodarbība kursā A, otrdien - kursā B, trešdien - kursā C. Starp divām kursa A nodarbībām ir divas brīvas dienas, starp divām kursa B nodarbībām ir trīs brīvas dienas, starp divām kursa C nodarbībām ir četras brīvas dienas (nodarbības notiek bez brīvdienām). Nodarbības tiek atceltas, ja vienā dienā iekrīt visas trīs nodarbības. Kad pirmo reizi tiks atceltas nodarbības?

4.4 Pierādīt vai atspēkot šādus apgalvojumus:

(a) $\forall\, p \in \mathbb{P},\ p \geq 5\colon\ p \equiv \pm 1 \pmod 6$,
(b) $\forall\, n \geq 1$ vai nu $6n-1$ vai arī $6n+1$ (vai abi) ir pirmskaitlis.

4.5 Skaitli 2013 pārveidot šādos pozicionālajos pierakstos:

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

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

4.6 Atrast tiešu formulu (piemēram, veidā $x = \sum_{i=1}^{s} c_i a_i$) vienādojumu sistēmas

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_s \pmod{m_s} \end{cases}$$

atrisināšanai.

4.7 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 ne vairāk kā

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

simboli.