Mazā matemātikas universitāte

Kas tu esi, kongruence? MMU-1

AUGUSTĪNE CELMIŅA, JEKATERINA SOKOLOVA, ROLANDS BRĒŽA

Definīcija

Skaitlis a **dalās** ar skaitli b $(a, b \in \mathbb{Z}, b \neq 0)$ jeb b **dala** a, ja eksistē tāds vesels skaitlis q, ka $a = b \cdot q$.

$$a \vdots b$$

Dalāmības īpašības

- $0 \vdots a$, $a \vdots \pm 1$;
- $a \vdots a$ (refleksivitāte);
- $a \vdots b$ un $b \vdots c \Rightarrow a \vdots c$ (transitivitāte);
- $a \vdots c \Rightarrow ab \vdots c$;
- $a \vdots c$ *un* $b \vdots c \Rightarrow ax+by \vdots c$ (jebkuriem veseliem skaitļiem x un y);
- $a \vdots b$ *un* $b \vdots a \Rightarrow a = \pm b$;
- $a \vdots b$ un $c \vdots d \Rightarrow ac \vdots bd$;
- $ac \vdots bc \Rightarrow a \vdots b$;
- $a \vdots b$ un $a, b > 0 \Rightarrow b \leq a$.

Piemērs

Dots, ka $3a \vdots n$ *un* $(12a + 5b) \vdots n$. *Pierādiet, ka* $10b \vdots n$.

Ja $(12a + 5b) \vdots n$ un $12a = 4 \cdot 3a \vdots n$, tad arī $5b \vdots n$.

Ja $5b \vdots n$, tad arī $10b \vdots n$.

Teorēma

Ja a - vesels, bet m - naturāls skaitlis,
skaitli a vienā vienīgā veidā var uzrakstīt formā

$$\boldsymbol{a = m \cdot q + r},$$

$0 \leq r < m$, kur q - ir vesels, r - naturāls skaitlis.

$$a : m = q\ \frac{r}{m} \Leftrightarrow a : m = q + \frac{r}{m} \Leftrightarrow a = q \cdot m + r$$

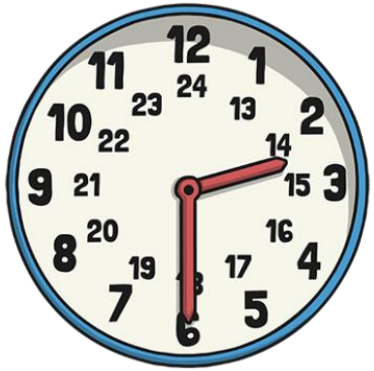
Definīcija

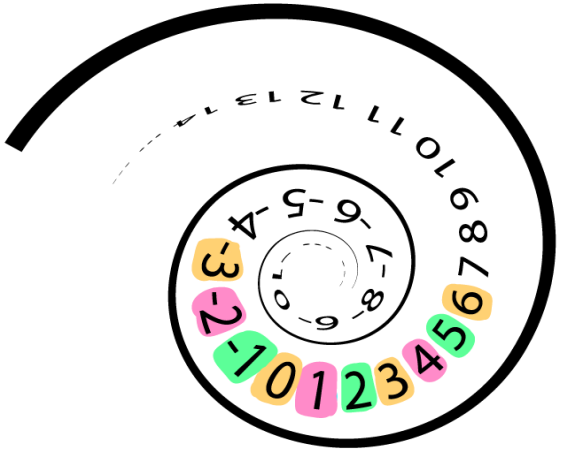
Doti veseli skaitļi a un b un naturāls skaitlis $m \geq 2$. Skaitļi a un b ir **kongruenti** pēc moduļa m ja a un b, dalot tos ar n, dod vienādu atlikumu.

Pieraksta: $a \equiv b \ (mod\ m)$.

Ņemiet vērā pēc teorēmas par dalīšanu ar atlikumu, r ir mazākais nenegatīvais skaitlis, ar ko a ir kongruents pēc moduļa n.

-1	0	1	2	3	4	5	6





(mod 3)

Kur izmanto kongruences

- Kalendārs
- RSA algoritms
- Kredītkaršu numuru leģitimitātes pārbaude
- Pirmskaitļu pārbaudes testi

Teorēma

$$a, b, c, d \in \mathbb{Z}, n \in \mathbb{N}$$

$a \equiv b \ (mod\ n)$ tad un tikai tad, ja $(a - b)$ dalās ar n.

Īpašības

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$
- $a \equiv b \pmod{m}$ un $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

Īpašības

- $a \equiv b \ (mod\ m)\ un\ c \equiv d \ (mod\ m) \Rightarrow a+c \equiv b+d \ (mod\ m)$

$$7 \equiv 4(mod\ 3)\ un\ 8 \equiv 5(mod\ 3) \Rightarrow 15 \equiv 9(mod\ 3)$$

- $a \equiv b \ (mod\ m)\ un\ c \equiv d \ (mod\ m) \Rightarrow a \cdot c \equiv b \cdot d \ (mod\ m)$

$$7 \equiv 4(mod\ 3)\ un\ 8 \equiv 5(mod\ 3) \Rightarrow 56 \equiv 20(mod\ 3)$$

- $a \equiv b \ (mod\ m)\ un\ k \in \mathbb{Z} \Rightarrow a^k \equiv b^k \ (\mathrm{mod}\ m)$

$$3 \equiv 7(mod\ \ 4) \Rightarrow 3^2 \equiv 7^2(mod\ 4)$$

- $a \cdot d \equiv b \cdot d \ (mod\ m)\ un\ LKD(d, m)=1 \Rightarrow a \equiv b \ (mod\ m)$

Kongruentu skaitļu reizinājuma īpašības pierādījums

$$\boldsymbol{a \equiv b (mod\ m)\ un\ c \equiv d\ (mod\ m)\ \Rightarrow\ a \cdot c \equiv b \cdot d\ (mod\ m)}$$

Pēc definīcijas $\boldsymbol{a = q \cdot m + r,\ b = p \cdot m + r,\ c = t \cdot m + z,\ d = l \cdot m + z}$

Izmantojot iepriekš pierādīto teorēmu iegūst, ka skaitļi ir kongruenti tad un tikai tad, ja starpība dalās ar m. Pārbaudīsim:

$$(q \cdot m + r)(t \cdot m + z) - (p \cdot m + r)(\ l \cdot m + z) \equiv 0\ (mod\ m)$$

$$(qm \cdot tm + qm \cdot z + tm \cdot r + rz) - (pm \cdot lm + pm \cdot z + lm \cdot r + rz) \equiv 0\ (mod\ m)$$

$$qm \cdot tm + qm \cdot z + tm \cdot r - pm \cdot lm - pm \cdot z - lm \cdot r \equiv 0\ (mod\ m)$$

$$m(q \cdot tm + q \cdot z + t \cdot r - p \cdot lm - p \cdot z - l \cdot r) \equiv 0\ (mod\ m)$$

Un ir iegūta patiesa izteiksme, no kā seko, ka, ja šo reizinājumu starpība dalās ar m tad arī reizinājumi ir kongruenti pēc mod m. ■

Teorēma

Virkne x_n pēc moduļa m ir periodiska, kur x_n ir a^n atlikums pēc moduļa m.

Piemērs: $2^n \ mod \ 5$:

$\boldsymbol{n}$	*0*	*1*	*2*	*3*	*4*	*5*	*6*
$\boldsymbol{2^n}$	*1*	*2*	*4*	*8*	*16*	*32*	*64*
$\boldsymbol{x_n}$	*1*	*2*	*4*	*3*	*1*	*2*	*4*

Fermā mazā teorēma

Ja p ir pirmskaitlis un eksistē kāds vesels skaitlis a, kur $LKD(a,p) = 1$,

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

Piemēri par kongruenču īpašībām

- Kuri no dotajiem skaitļiem ir kongruenti savā starpā pēc moduļa 10?

$$7,\ 13,\ 117,\ -33,\ 35,\ -38,\ 8.$$

$$771 \cdot 772 + 773 \cdot 774 \, (mod\ 7)$$

$$771 = 770 + 1 \equiv 1 (mod\ 7)$$

$$772 = 770 + 2 \equiv 2 (mod\ 7)$$

$$773 = 770 + 3 \equiv 3 (mod\ 7)$$

$$774 = 770 + 4 \equiv 4 (mod\ 7)$$

$$1 \cdot 2 + 3 \cdot 4 = 14 \equiv 0 (mod\ 7)$$

Vai $8^6 \equiv 1(mod\ 9)$

$$8 \equiv -1(mod\ 9)$$

$$\Rightarrow 8^6 \equiv (-1)^6 = 1(mod\ 9)$$

Atrast $13 \cdot 14^2 \cdot 15^3 \ (mod\ 11)$

$$13 \equiv 2(mod\ 11), 14 \equiv 3(mod\ 11), 15 \equiv 4(mod\ 11)$$

$$\Rightarrow 2 \cdot 3^2 \cdot 4^3 \equiv 2 \cdot 9 \cdot 16 \cdot 4 \equiv 18 \cdot 4 \cdot 5 \equiv 7 \cdot 4 \cdot 5 \equiv 7 \cdot 9$$

$$\equiv 7 \cdot (-2) \equiv -14 \equiv -3 \equiv 8(mod\ 11)$$

Virknes 2^n periods pēc moduļa 10

- Atrast virknes 2^n periodu pēc moduļa 10

n	0	1	2	3	4	5	6	7	8
2^n	1	2	4	8	16	32	64	128	256
$mod\ 10$	1	2	4	8	6	2	4	8	6

- Atrast $2^{23}\ (mod\ 10)$

$23 \equiv 3(mod\ 4) \Rightarrow$ 23 atrodas perioda trešajā posmā, tādēļ dod atlikumu 8

Komentārs par pierakstu

$$1234 = 4 + 3 \cdot 10 + 2 \cdot 100 + 1 \cdot 1000$$

$$N = a_0 + 10 \cdot a_1 + 10^2 a_2 + \cdots + 10^n a_n$$

Dalāmības pazīmes

- mod 3, 9

$$N = a_0 + 10 \cdot a_1 + 10^2 a_2 + \cdots + 10^n a_n$$

Tā kā $10 \equiv 1\ (mod\ 3, 9)$, tad $10^2 \equiv 1^2 = 1\ (mod\ 3, 9)$ utt. Tad

$$N = a_0 + 10 \cdot a_1 + 10^2 a_2 + \cdots + 10^n a_n \equiv a_0 + a_1 + a_2 + \cdots + a_n$$

Piem. $123456 \equiv 1 + 2 + 3 + 4 + 5 + 6 = 21 \equiv 2 + 1 = 3\ (mod\ 9)$

Dalāmības pazīmes

- mod 2, 5, 10

$$N = \overline{a_n \dots a_1 a_0} = a_0 + 10 \cdot \overline{a_n \dots a_1} \equiv a_0 \ (mod\ 2, 5, 10)$$

- mod 20, 25, 50, 100

$$N = \overline{a_1 a_0} + 100 \cdot \overline{a_n \dots a_2} \equiv \overline{a_1 a_0} (mod\ 4, 20, 25, 50, 100)$$

Tāpat var turpināt ar 3 cipariem, iegūstot dalāmības pazīmi uz jebkuru skaitļa 1000 dalītāju (8, 40, 125, …).

Dalāmības pazīmes

Skaitlis dalās ar 2^n ja tā pēdējo n ciparu veidotais skaitlis dalās ar 2^n.

Skaitlis dalās ar 5^n, ja tā pēdējo n ciparu veidotais skaitlis dalās ar 5^n .

Skaitlis dalās ar 10^n, ja tā pēdējo n ciparu veidotais skaitlis dalās ar 10^n.

Dalāmības pazīmes

- mod 11

$$10 \equiv -1 \ (mod\ 11)$$

$$N = a_0 + 10 \cdot a_1 + 10^2 a_2 + 10^3 a_3 + \cdots \equiv a_0 - a_1 + a_2 - a_3 + \cdots$$

Piem. $123456 \equiv 6 - 5 + 4 - 3 + 2 - 1 = 3 \ (mod\ 11)$

Dalāmības pazīmes

- mod 7, 11, 13

$$N = \overline{a_2 a_1 a_0} + 1000 \cdot \overline{a_5 a_4 a_3} + \cdots$$

Tā kā $1001 = 7 \cdot 11 \cdot 13$, tad $1000 \equiv -1 \ (mod\ 7, 11, 13)$

$$N = \overline{a_2 a_1 a_0} + 1000 \cdot \overline{a_5 a_4 a_3} + \cdots \equiv \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \cdots$$

Paldies par uzmanību!

DODAMIES UZ STACIJĀM!