SKAITĻU TEORIJA SENIORIEM

30.01.2021.

Kongruences

Situācija: jūs rēķināt uzdevumu un jums ir jāsastāda kongruenču tabula izteiksmei a^n pēc moduļa 5.

a (mod 5)	a^2 (mod 5)	a^3 (mod 5)	a^4 (mod 5)	a^5 (mod 5)
0	$0 \cdot 0 = \mathbf{0}$	$0 \cdot 0 = \mathbf{0}$	$0 \cdot 0 = \mathbf{0}$	$0 \cdot 0 = \mathbf{0}$
1	$1 \cdot 1 = \mathbf{1}$	$1 \cdot 1 = \mathbf{1}$	$1 \cdot 1 = \mathbf{1}$	$1 \cdot 1 = \mathbf{1}$
2	$2 \cdot 2 = \mathbf{4}$	$4 \cdot 2 = 8 = \mathbf{3}$	$3 \cdot 2 = 6 = \mathbf{1}$	$1 \cdot 2 = \mathbf{2}$
3	$3 \cdot 3 = 9 = \mathbf{4}$	$4 \cdot 3 = 12 = \mathbf{2}$	$2 \cdot 3 = 6 = \mathbf{1}$	$1 \cdot 3 = \mathbf{3}$
4	$4 \cdot 4 = 16 = \mathbf{1}$	$1 \cdot 4 = \mathbf{4}$	$4 \cdot 4 = 16 = \mathbf{1}$	$1 \cdot 4 = \mathbf{4}$

a (mod 5)	a^2 (mod 5)	a^3 (mod 5)	a^4 (mod 5)	a^5 (mod 5)
0	$0^2 = \mathbf{0}$	$0^3 = \mathbf{0}$	$0^4 = \mathbf{0}$	$0^5 = \mathbf{0}$
1	$1^2 = \mathbf{1}$	$1^3 = \mathbf{1}$	$1^4 = \mathbf{1}$	$1^5 = \mathbf{1}$
2	$2^2 = \mathbf{4}$	$2^3 = 8 = \mathbf{3}$	$2^4 = 16 = \mathbf{1}$	$2^5 = 32 = \mathbf{2}$
3	$3^2 = 9 = \mathbf{4}$	$3^3 = 27 = \mathbf{2}$	$3^4 = 81 = \mathbf{1}$	$3^5 = 243 = \mathbf{3}$
4	$4^2 = 16 = \mathbf{1}$	$4^3 = 64 = \mathbf{4}$	$4^4 = 256 = \mathbf{1}$	$4^5 = 1024 = \mathbf{4}$

Kongruences

Situācija: jūs rēķināt uzdevumu un jums ir jāsastāda kongruenču tabula izteiksmei a^n pēc moduļa 5.

a (mod 5)	a^2 (mod 5)	a^3 (mod 5)	a^4 (mod 5)	a^5 (mod 5)
0	0·0 = **0**	0·0 = **0**	0·0 = **0**	0·0 = **0**
1	1·1 = **1**	1·1 = **1**	1·1 = **1**	1·1 = **1**
2	2·2 = **4**	4·2 = 8 = **3**	3·2 = 6 = **1**	1·2 = **2**
3	3·3 = 9 = **4**	4·3 = 12 = **2**	2·3 = 6 = **1**	1·3 = **3**
4	4·4 = 16 = **1**	1·4 = **4**	4·4 = 16 = **1**	1·4 = **4**

a (mod 5)	a^2 (mod 5)	a^3 (mod 5)	a^4 (mod 5)	a^5 (mod 5)
0	0·0 = **0**	0·0 = **0**	0·0 = **0**	0·0 = **0**
1	1·1 = **1**	1·1 = **1**	1·1 = **1**	1·1 = **1**
2	2·2 = **4** = **-1**	-1·2 = **-2** = **3**	-2·2 = -4 = **1**	1·2 = **2**
3 = -2	-2·(-2) = **4** = **-1**	-1·(-2) = **2**	2·(-2) = -4 = **1**	1·(-2) = **-2** = **3**
4 = -1	-1·(-1) = **1**	1·(-1) = **-1** = **4**	-1·(-1) = **1**	1·(-1) = **-1** = **4**

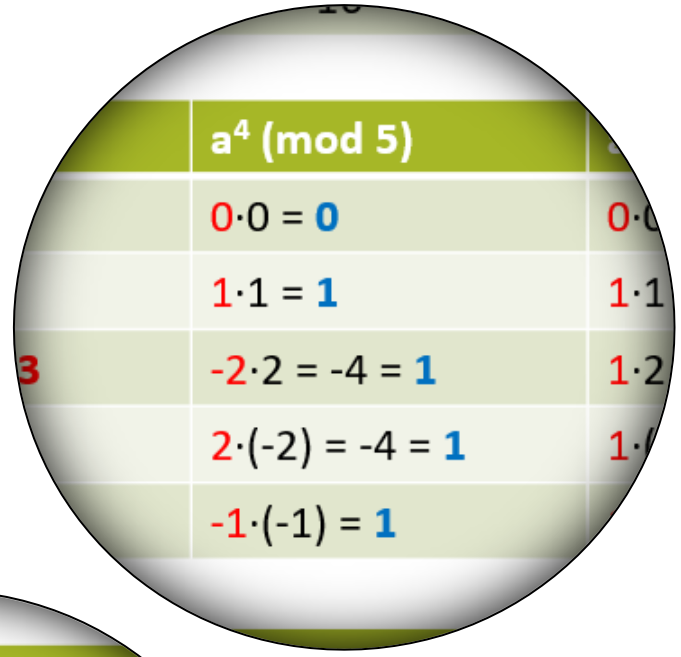
Fermā mazā teorēma

Ja **p** ir pirmskaitlis, un **a** ir vesels skaitlis, tad:

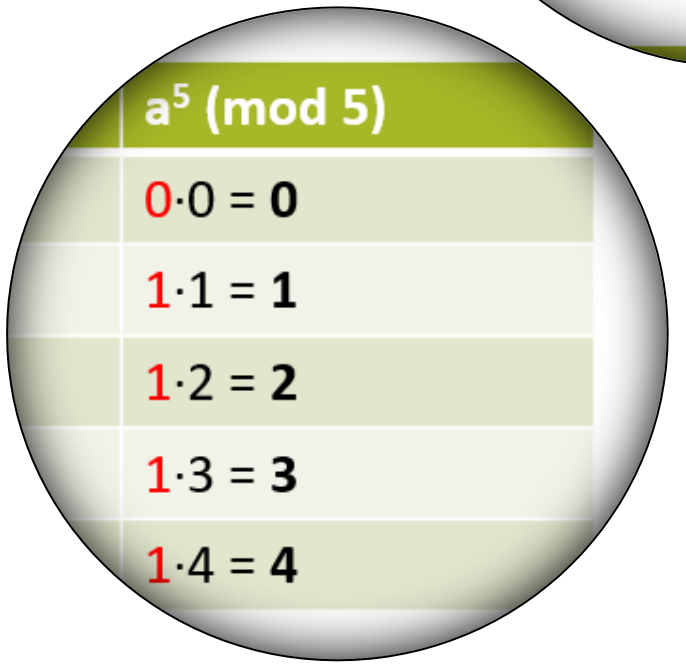
- $a^{p-1} \equiv 1 \pmod{p}$ jeb $a^{p-1} - 1 \equiv 0 \pmod{p}$, ja **a** nedalās ar **p**
- $a^{p-1} \equiv 0 \pmod{p}$, ja **a** dalās ar **p**

Ja **p** ir pirmskaitlis, un **a** ir vesels skaitlis, tad:

- $a^{p} \equiv a \pmod{p}$



	$a^4 \pmod 5$	
	0·0 = **0**	0·
	1·1 = **1**	1·1
3	-2·2 = -4 = **1**	1·2
	2·(-2) = -4 = **1**	1·
	-1·(-1) = **1**	



$a^5 \pmod 5$
0·0 = **0**
1·1 = **1**
1·2 = **2**
1·3 = **3**
1·4 = **4**

Treniņš nr. 1

- $6^{6} \pmod 5$
- $79^{79} + 80^{80} + 81^{81} \pmod 8$
- $17^{4} \pmod{19}$
- $2019^{18} \pmod{19}$
- $2019^{303} \pmod{101}$
- $33^{33} \pmod 5$
- $600^{600} \pmod{42}$

Kvadrātiskie un ne-kvadrātiskie atlikumi

Dots naturāls skaitlis **n** un vesels skaitlis **r**.

Vai eksistē tāds naturāla skaitļa **a** kvadrāts, kurš dos atlikumu **r**, pēc moduļa **n**:

$a^2 \equiv r \pmod{n}$?

- Eksistē → **r** ir kvadrātiskais atlikums (mod n)
- Neeksistē → **r** ir ne-kvadrātiskais atlikums (mod n)

a (mod 8)	a^2 (mod 8)
0	$0^2 = \mathbf{0}$
1	$1^2 = \mathbf{1}$
2	$2^2 = \mathbf{4}$
3	$3^2 = 9 = \mathbf{1}$
4	$4^2 = 16 = \mathbf{0}$
5 = -3	$(-3)^2 = 9 = \mathbf{1}$
6 = -2	$(-2)^2 = \mathbf{4}$
7 = -1	$(-1)^2 = \mathbf{1}$

0, 1, 4 – kvadrātiskie atlikumi (mod 8)

2, 3, 5, 6, 7 – ne-kvadrātiskie atlikumi (mod 8)

Treniņš nr. 2

- 1, (mod 5)
- 7, (mod 5)
- -2 (mod 5)
- 12, (mod 7)
- -1, (mod 7)
- 441, (mod 2021)
- 102, (mod 103)

Kvadrātiskie un ne-kvadrātiskie atlikumi

Izrādās, ka ar kvadrātiskajiem atlikumiem ir īpaši ērti strādāt, ja skatās kongruenci pēc pirmskaitļa moduļa.

Ja ir dots skaitlis **a** un nepāra pirmskaitlis **p**, mēs varam būtiski ietaupīt laiku un atmiņu, mēģinot noskaidrot, vai **a** ir kvadrātisks atlikums pēc moduļa **p**. Pietiek aprēķināt kongruenci:

$$a^{\frac{p-1}{2}} \equiv ? \pmod{p}$$

Izradās, ka šī kongruence var pieņemt tikai trīs vērtības intervālā no 0 līdz **p**. Kādas, jūsuprāt?

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 0 \text{ vai } 1 \pmod{p} \Rightarrow a \text{ ir kvadrātiskais atlikums } \pmod{p} \\ -1 \pmod{p} \Rightarrow a \text{ ir ne-kvadrātiskais atlikums } \pmod{p} \end{cases}$$

Eilera kritērijs

	$a^2 \pmod 5$	
	$0 \cdot 0 = 0$	$0 \cdot 0$
	$1 \cdot 1 = 1$	$1 \cdot 1$
	$2 \cdot 2 = 4$	$4 \cdot 2$
	$3 \cdot 3 = 9 = 4$	$4 \cdot 3$
	$4 \cdot 4 = 16 = 1$	1

0

1

$p-1$

Pieraksta šādi:

0

1

-1

Kvadrātiskie un ne-kvadrātiskie atlikumi

Labi, atmetam gadījumu, kad **a** dalās ar **p**:

$$a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$$

Ja **a** nedalās ar **p**, tad sanāk, ka kongruence ir vai nu 1, vai nu -1.

Kāpēc tā sanāk? Kāpēc nevar būt citi skaitļi?

Padoms: izmantojiet Fermā mazo teorēmu.

$$\left(a^{\frac{p-1}{2}}+1\right)\left(a^{\frac{p-1}{2}}-1\right)=a^{p-1}-1\equiv 0\left(\mathrm{mod}\ p\right),\ \text{ja } a \text{ nedalās ar } p$$

Kvadrātiskie un ne-kvadrātiskie atlikumi

Vēl viens jocīgs fakts par kvadrātiskiem atlikumiem, ja **p** ir nepāra pirmskaitlis: kvadrātisko atlikumu ir par vienu vairāk nekā ne-kvadrātisko. Ja neskaitīt 0, tad atlikumi sadalās precīzi uz pusēm!

Kā to var pierādīt?

1. $x^2 \equiv (p-x)^2 \pmod p$,

tāpēc var apskatīt tikai atlikumus intervāla $\left[0; \frac{p-1}{2}\right]$

2. ja $x \neq y$ un $x, y \in \left[0; \frac{p-1}{2}\right]$, tad pieņemsim, ka

$x^2 \equiv y^2 \pmod p \Rightarrow$

$\Rightarrow x^2 - y^2 \equiv 0 \pmod p \Rightarrow$

$\Rightarrow (x-y)(x+y) \equiv 0 \pmod p$, pretruna, jo

$x - y \not\equiv 0 \pmod p$ un $x + y \not\equiv 0 \pmod p$

a (mod 7)	a^2 (mod 7)
0	$0^2 = \mathbf{0}$
1	$1^2 = \mathbf{1}$
2	$2^2 = \mathbf{4}$
3	$3^2 = 9 = \mathbf{2}$
4 = -3	$(-3)^2 = 9 = \mathbf{2}$
5 = -2	$(-2)^2 = \mathbf{4}$
6 = -1	$(-1)^2 = \mathbf{4}$

3. tātad inervālā $\left[0; \frac{p-1}{2}\right]$ nekādu divu dažādu atlikumu kvadrāti nav vienādi (mod p),

sanāk kopā tieši $\frac{p-1}{2}$ dažādi nenulles atlikumu kvadrāti (mod p) – jeb kvadrātiskie atlikumi

Kvadrātiskie un ne-kvadrātiskie atlikumi

Pierādīsim Eilera kritēriju.

Ja **a** ir kvadrātiskais atlikums pēc moduļa **p** (nepāra pirmskaitlis), tad eksistē tāds vesels **b**, kuram izpildās

$$b^2 \equiv a \pmod{p} \Rightarrow a^{\frac{p-1}{2}} \equiv b^{2\left(\frac{p-1}{2}\right)} \equiv b^{p-1} \pmod{p}$$

Pēc mazās Fermā teorēmas sanāk, ka, ja **a** ir kvadrātisks atlikums (mod **p**), kongruences vērtība ir vienāda ar 0 vai 1, kas atbilst Eilera kritērijam. Kopā sanāk, ka kvadrātiskie atlikumi dod ir $\frac{p-1}{2}$ vieninieku un vienu nulli.

Jeb vienādojumam $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ ir $\frac{p-1}{2}$ sakņu, tad citi vieninieki parādīties nevar – tie ir izsmelti, un ne-kvadrātiskajiem atlikumiem Eilera kritērijs radīs -1.

Ležandra simbols

Ležandra simbols ir funkcija no vesela skaitļa **a** un nepāra pirmskaitļa **p**, kura var pieņemt vērtības 0, 1 un –1 atbilstoši kongruencei:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

lai nejaukt ar parastām daļām, var izmantot indeksus

$$\left(\frac{a}{p}\right)_{Legendre} \equiv a^{\frac{p-1}{2}} \pmod{p}$$

$$\left(\frac{a}{p}\right)_{L} \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Ležandra simbols

Ležandra simbols ir funkcija no vesela skaitļa **a** un nepāra pirmskaitļa **p**, kura var pieņemt vērtības 0, 1 un –1 atbilstoši kongruencei:

$$\left(\frac{a}{p}\right)_L \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Ležandra simbolam ir burvīgas īpašības:

- $\left(\frac{a}{p}\right)_L = \left(\frac{b}{p}\right)_L$, ja $a \equiv b \pmod{p}$
- $\left(\frac{a}{p}\right)_L \cdot \left(\frac{b}{p}\right)_L = \left(\frac{ab}{p}\right)_L$, ja $\gcd(a,b) = 1$
- $\left(\frac{a}{p}\right)_L = \left(\frac{p_1}{p}\right)_L^{\alpha_1} \cdot \left(\frac{p_2}{p}\right)_L^{\alpha_2} \cdot \ldots \cdot \left(\frac{p_{k-1}}{p}\right)_L^{\alpha_{k-1}} \cdot \left(\frac{p_k}{p}\right)_L^{\alpha_k}$, ja $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_{k-1}^{\alpha_{k-1}} \cdot p_k^{\alpha_k}$

Ležandra simbols

Ležandra simbols ir funkcija no vesela skaitļa **a** un nepāra pirmskaitļa **p**, kura var pieņemt vērtības 0, 1 un –1 atbilstoši kongruencei:

$$\left(\frac{a}{p}\right)_L \equiv a^{\frac{p-1}{2}} \pmod{p}$$

- $102, \pmod{103}$

Ležandra simbolam ir arī citas burvīgas īpašības:

- $\left(\frac{-1}{p}\right)_L = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, \text{ ja } p \equiv 1 (\mathrm{mod}\, 4) \\ -1, \text{ ja } p \equiv 3 (\mathrm{mod}\, 4) \end{cases}$
- $\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, \text{ ja } p \equiv 1 \text{ vai } 7 (\mathrm{mod}\, 8) \\ -1, \text{ ja } p \equiv 3 \text{ vai } 5 (\mathrm{mod}\, 8) \end{cases}$
- $\left(\frac{q}{p}\right)_L = \left(\frac{p}{q}\right)_L \cdot (-1)^{\frac{(p-1)(q-1)}{4}}$, ja p un q ir nepāra pirmskaitļi
- $\left(\frac{a}{p}\right)_L = \left(\frac{a}{q}\right)_L$, ja p un q ir nepāra pirmskaitļi, un $p \equiv q \pmod{4a}$

DAŽĀDI UZDEVUMI

par kvadrātu summu

Uzdevums nr. 1

Vai katram naturālam a skaitli $3a^4 + 1$ var izteikt kā trīs veselu skaitļu kvadrātu summu?

- **Jā**
- **Nē**

Uzdevums nr. 2

Pierādiet, ka skaitļus veidā $4^a \cdot (8m + 7)$ nevar izteikt kā trīs veselu skaitļu kvadrātu summu ($a \geq 0$, $m \geq 0$).

Ja naturāls skaitlis nav izsakāms veidā $4^a \cdot (8m + 7)$, tad to var izteikt kā triju veselu skaitļu kvadrātu summu.

Jebkuru naturālu skaitli var izteikt kā četru veselu skaitļu kvadrātu summu.

FAKTI:

- Visi naturāli skaitļi, izņemot tieši tos, kas ir izsakāmi veidā $4^a \cdot (8m + 7)$, var kā trīs veselu skaitļu kvadrātu summu ($a \geq 0$, $m \geq 0$).
- Jebkuru naturālu skaitli var izteikt kā četru veselu skaitļu kvadrātu summu.
- Jebkuru pirmskaitli, kas izsakāms veidā $4m + 1$, var izteikt kā divu naturālu skaitļu kvadrātu summu. (Eilera-Fermā t.s. Ziemassvētku teorēma.

Pitagora trijnieki

$$a^2 + b^2 = c^2$$

- $a = 2xy \cdot z$
- $b = |x^2 - y^2| \cdot z$
- $c = (x^2 + y^2) \cdot z$

Pitagora četrinieki

$a^2 + b^2 + c^2 = d^2$

- $a = 2x \cdot w$
- $b = 2y \cdot w$
- $c = \left(\frac{x^2 + y^2}{z} - z \right) \cdot w$
- $d = \left(\frac{x^2 + y^2}{z} + z \right) \cdot w$

Paldies par uzmanību!