Kongruences

Mārtiņš Kokainis

Latvijas Universitāte, NMS

Rīga, 2015

Pamatjēdzieni

Dalāmība

1. definīcija

Saka, ka vesels skaitlis m dalās ar veselu skaitli n ($n \neq 0$) un pieraksta $m \vdots n$, ja eksistē tāds vesels skaitlis k, ka $m = n \cdot k$.

Piemēram,

- $9 \vdots 3$, jo $9 = 3 \cdot 3$.
- $142 \vdots 71$, jo $142 = 71 \cdot 2$.
- $142 \vdots (-71)$, jo $142 = (-71) \cdot (-2)$.
- $(-35) \vdots (-7)$, jo $-35 = (-7) \cdot 5$.

Dalīšana ar atlikumu

2. definīcija

Izdalīt veselu skaitli m ar **naturālu skaitli** n ar atlikumu nozīmē atrast tādus veselus skaitļus q un r, kuriem izpildās vienādība $m = q \cdot n + r$, turklāt $r = 0, 1, 2, \ldots, n-1$.
Ja $r = 0$, tad sakām, ka m dalās ar n bez atlikuma (jeb, ka m dalās ar n).

- 29 dalot ar 5, iegūst dalījumu 5 un atlikumu 4, jo $29 = 5 \cdot 5 + 4$.
- -29 dalot ar 5, iegūst dalījumu -6 un atlikumu 1, jo $-29 = (-6) \cdot 5 + 1$.
- -24 dalot ar 3, iegūst dalījumu -8 un atlikumu 0, jo $-24 = (-8) \cdot 3 + 0$.

Skaitļu sadalījums klasēs

- Veselo skaitļu iedalījums pāra un nepāra skaitļos:
  - $\ldots, -4, -2, 0, 2, 4, \ldots$ – skaitļi, kas dalās ar 2 (pāra skaitļi);
  - $\ldots, -3, -1, 1, 3, 5, \ldots$ – skaitļi, kas nedalās ar 2 (nepāra skaitļi).
- Šī iedalījuma vispārinājums?
  - $\ldots, -3, 0, 3, 6, \ldots$ – skaitļi, kas dalās ar 3;
  - $\ldots, -2, -1, 1, 2, 4, 5, \ldots$ – skaitļi, kas nedalās ar 3.

Skaitļu sadalījums klasēs

- Skaitļu sadalījums atkarībā no tā, kādus atlikumus tie dod, dalot ar 3:
  - $\ldots, -6, -3, 0, 3, \ldots$ – skaitļi, kuri, dalot ar 3, dod atlikumu 0;
  - $\ldots, -5, -2, 1, 4, \ldots$ – skaitļi, kuri, dalot ar 3, dod atlikumu 1;
  - $\ldots, -4, -1, 2, 5, \ldots$ – skaitļi, kuri, dalot ar 3, dod atlikumu 2.

$\cdots$	-3	-2	-1	0	1	2	3	4	5	6	7	$\cdots$

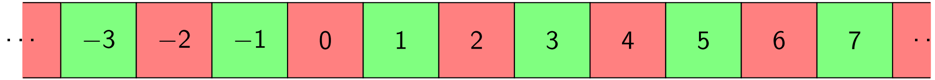
Skaitļu krāsošana

- Skaitļu krāsošana atkarībā no atlikuma, dalot skaitļus ar 2:

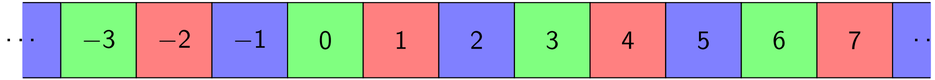
$\cdots$	-3	-2	-1	0	1	2	3	4	5	6	7	$\cdots$

Skaitļu krāsošana

- Skaitļu krāsošana atkarībā no atlikuma, dalot skaitļus ar 2:



- Skaitļu krāsošana atkarībā no atlikuma, dalot skaitļus ar 3:



Kongruences jēdziens

- Kongruences jēdziens – formalizē aplūkoto skaitļu "krāsošanu".

3. definīcija

Doti veseli skaitļi a un b un naturāls skaitlis $n \geq 2$. Saka, ka skaitļi a un b ir kongruenti pēc moduļa n un pieraksta $a \equiv b \pmod{n}$, ja a un b, dalot tos ar n, dod vienādus atlikumus.

- $3 \equiv 5 \pmod{2}$, jo 5 un 3 abi dod atlikumu 1, dalot ar 2;
- $4 \equiv -2 \pmod{3}$, jo 4 un -2 abi dod atlikumu 1, dalot ar 3;
- $-4 \equiv 87 \pmod{7}$, jo -4 un 87 abi dod atlikumu 3, dalot ar 7.

1. uzdevums

Vai sekojošās kongruences ir pareizas?

- $3 \equiv 7 \pmod{4}$?

1. uzdevums

Vai sekojošās kongruences ir pareizas?

- $3 \equiv 7 \pmod 4$?

  Jā, jo gan 3, gan 7 dod atlikumu 3, dalot ar 4;

1. uzdevums

Vai sekojošās kongruences ir pareizas?

- $3 \equiv 7 \pmod{4}$?
  Jā, jo gan 3, gan 7 dod atlikumu 3, dalot ar 4;
- $3 \equiv 7 \pmod{3}$?

1. uzdevums

Vai sekojošās kongruences ir pareizas?

- $3 \equiv 7 \pmod 4$?

  Jā, jo gan 3, gan 7 dod atlikumu 3, dalot ar 4;

- $3 \equiv 7 \pmod 3$?

  Nē, jo 3 dod atlikumu 0, dalot ar 3, bet 7 dod atlikumu 1, dalot ar 3;

1. uzdevums

Vai sekojošās kongruences ir pareizas?

- $3 \equiv 7 \pmod{4}$?
  Jā, jo gan 3, gan 7 dod atlikumu 3, dalot ar 4;
- $3 \equiv 7 \pmod{3}$?
  Nē, jo 3 dod atlikumu 0, dalot ar 3, bet 7 dod atlikumu 1, dalot ar 3;
- $17 \equiv 73 \pmod{14}$?

1. uzdevums

Vai sekojošās kongruences ir pareizas?

- $3 \equiv 7 \pmod{4}$?
  Jā, jo gan 3, gan 7 dod atlikumu 3, dalot ar 4;
- $3 \equiv 7 \pmod{3}$?
  Nē, jo 3 dod atlikumu 0, dalot ar 3, bet 7 dod atlikumu 1, dalot ar 3;
- $17 \equiv 73 \pmod{14}$?
  Jā, jo gan 17, gan 73 dod atlikumu 3, dalot ar 14;

1. uzdevums

Vai sekojošās kongruences ir pareizas?

- $3 \equiv 7 \pmod 4$?
  Jā, jo gan 3, gan 7 dod atlikumu 3, dalot ar 4;
- $3 \equiv 7 \pmod 3$?
  Nē, jo 3 dod atlikumu 0, dalot ar 3, bet 7 dod atlikumu 1, dalot ar 3;
- $17 \equiv 73 \pmod{14}$?
  Jā, jo gan 17, gan 73 dod atlikumu 3, dalot ar 14;
- $71 \equiv 8 \pmod 9$?

1. uzdevums

Vai sekojošās kongruences ir pareizas?

- $3 \equiv 7 \pmod{4}$?
  Jā, jo gan 3, gan 7 dod atlikumu 3, dalot ar 4;
- $3 \equiv 7 \pmod{3}$?
  Nē, jo 3 dod atlikumu 0, dalot ar 3, bet 7 dod atlikumu 1, dalot ar 3;
- $17 \equiv 73 \pmod{14}$?
  Jā, jo gan 17, gan 73 dod atlikumu 3, dalot ar 14;
- $71 \equiv 8 \pmod{9}$?
  Jā, jo gan 71, gan 8 dod atlikumu 8, dalot ar 9.

Kongruences jēdziens

1. teorēma

$a \equiv b \pmod{n}$ tad un tikai tad, ja starpība $a - b$ dalās ar n.

- $3 \equiv 5 \pmod{2}$, jo $5 - 3 = 2$ dalās ar 2;
- $4 \equiv -2 \pmod{3}$, jo $4 - (-2) = 6 = 3 \cdot 2$ dalās ar 3;
- $-6 \equiv 85 \pmod{7}$, jo $-6 - 85 = -91 = 7 \cdot (-13)$ dalās ar 7;
- $17 \equiv 73 \pmod{14}$, jo $17 - 73 = -56 = 14 \cdot (-4)$ dalās ar 14;
- $71 \equiv 8 \pmod{9}$, jo $71 - 8 = 63 = 9 \cdot 7$ dalās ar 9.

Kongruenču īpašības

- Visiem veseliem skaitļiem a izpildās kongruence $a \equiv a \pmod{n}$ (refleksivitāte);

Kongruenču īpašības

- Visiem veseliem skaitļiem a izpildās kongruence $a \equiv a \pmod{n}$ (refleksivitāte);
- Ja $a \equiv b \pmod{n}$, tad $b \equiv a \pmod{n}$ (simetrija);

Kongruenču īpašības

- Visiem veseliem skaitļiem a izpildās kongruence $a \equiv a \pmod{n}$ (refleksivitāte);
- Ja $a \equiv b \pmod{n}$, tad $b \equiv a \pmod{n}$ (simetrija);
- Ja $a \equiv b \pmod{n}$ un $b \equiv c \pmod{n}$, tad $a \equiv c \pmod{n}$ (transitivitāte).

Kongruenču īpašības

- Visiem veseliem skaitļiem a izpildās kongruence $a \equiv a \pmod{n}$ (refleksivitāte);
- Ja $a \equiv b \pmod{n}$, tad $b \equiv a \pmod{n}$ (simetrija);
- Ja $a \equiv b \pmod{n}$ un $b \equiv c \pmod{n}$, tad $a \equiv c \pmod{n}$ (transitivitāte).

- Ja $a \equiv b \pmod{n}$ un $c \equiv d \pmod{n}$, tad
  1. $a + c \equiv b + d \pmod{n}$;

Kongruenču īpašības

- Visiem veseliem skaitļiem a izpildās kongruence $a \equiv a \pmod{n}$ (refleksivitāte);
- Ja $a \equiv b \pmod{n}$, tad $b \equiv a \pmod{n}$ (simetrija);
- Ja $a \equiv b \pmod{n}$ un $b \equiv c \pmod{n}$, tad $a \equiv c \pmod{n}$ (transitivitāte).

- Ja $a \equiv b \pmod{n}$ un $c \equiv d \pmod{n}$, tad
  1. $a + c \equiv b + d \pmod{n}$;
  2. $a - c \equiv b - d \pmod{n}$;

Kongruenču īpašības

- Visiem veseliem skaitļiem a izpildās kongruence $a \equiv a \pmod{n}$ (refleksivitāte);
- Ja $a \equiv b \pmod{n}$, tad $b \equiv a \pmod{n}$ (simetrija);
- Ja $a \equiv b \pmod{n}$ un $b \equiv c \pmod{n}$, tad $a \equiv c \pmod{n}$ (transitivitāte).

- Ja $a \equiv b \pmod{n}$ un $c \equiv d \pmod{n}$, tad
  1. $a + c \equiv b + d \pmod{n}$;
  2. $a - c \equiv b - d \pmod{n}$;
  3. $a \cdot c \equiv b \cdot d \pmod{n}$;

Kongruenču īpašības

- Visiem veseliem skaitļiem a izpildās kongruence $a \equiv a \pmod{n}$ (refleksivitāte);
- Ja $a \equiv b \pmod{n}$, tad $b \equiv a \pmod{n}$ (simetrija);
- Ja $a \equiv b \pmod{n}$ un $b \equiv c \pmod{n}$, tad $a \equiv c \pmod{n}$ (transitivitāte).

- Ja $a \equiv b \pmod{n}$ un $c \equiv d \pmod{n}$, tad
  1. $a + c \equiv b + d \pmod{n}$;
  2. $a - c \equiv b - d \pmod{n}$;
  3. $a \cdot c \equiv b \cdot d \pmod{n}$;
  4. $a^m \equiv b^m \pmod{n}$, visiem naturāliem skaitļiem m.

1. piemērs

Aprēķināt atlikumu, kāds rodas, skaitli $A = 113^2 + 21^7 - 43 \cdot 15$ dalot ar 11!

1. piemērs

Aprēķināt atlikumu, kāds rodas, skaitli $A = 113^2 + 21^7 - 43 \cdot 15$ dalot ar 11!

Jāaprēķina, ar ko kongruents A pēc moduļa 11:

$$113^2 + 21^7 - 43 \cdot 15 \equiv ? \pmod{11}$$

1. piemērs

Aprēķināt atlikumu, kāds rodas, skaitli $A = 113^2 + 21^7 - 43 \cdot 15$ dalot ar 11!

Jāaprēķina, ar ko kongruents A pēc moduļa 11:

$$113^2 + 21^7 - 43 \cdot 15 \equiv {\color{red}?} \pmod{11}$$

Veiksim aprēķinus pēc moduļa 11, izmantojot kongruenču īpašības:

$$\begin{aligned}
113 &= 110 + 3 = 11 \cdot 10 + 3 \equiv 3 \pmod{11};\\
21 &= 22 - 1 = 11 \cdot 2 - 1 \equiv -1 \pmod{11};\\
43 &= 44 - 1 = 11 \cdot 4 - 1 \equiv -1 \pmod{11};\\
15 &\equiv 11 + 4 \equiv 4 \pmod{11}.
\end{aligned}$$

1. piemērs

Tātad $113^2 + 21^7 - 43 \cdot 15 \equiv 3^2 + (-1)^7 - (-1) \cdot 4 \pmod{11}$.

$$A \equiv 9 - 1 + 4 \equiv 12 \equiv 1 \pmod{11}.$$

Līdz ar to secinām, ka, dalot skaitli A ar 11, atlikums ir 1.

2. uzdevums

Aprēķināt atlikumu, skaitli A dalot ar n!

$$A = 25^3 - 73 \cdot 7 + 220^{220} \cdot 300, \quad n = 12$$

un

$$A = 37^3 - 89 \cdot 192^2 - 181 \cdot 54, \quad n = 7.$$

2. uzdevums

Aplūkojam atbilstošās kongruences:

- $25^3 - 73 \cdot 7 + 220^{220} \cdot 300 \pmod{12}$;
- $37^3 - 89 \cdot 192^2 - 181 \cdot 54 \pmod{7}$.

2. uzdevums

$$
\begin{aligned}
&25^3 - 73 \cdot 7 + 220^{220} \cdot 300 \equiv \\
&\equiv 1^3 - 1 \cdot 7 + 220^{220} \cdot 0 \equiv \\
&\equiv 1 - 7 \equiv -6 \equiv 6 \pmod{12};
\end{aligned}
$$

2. uzdevums

$$
\begin{aligned}
&37^3 - 89 \cdot 192^2 - 181 \cdot 54 \equiv \\
&\equiv 2^3 - 5 \cdot 3^2 - (-1) \cdot 5 \equiv \\
&\equiv 1 - 5 \cdot 2 + 5 \equiv -4 \equiv 3 \pmod{7}.
\end{aligned}
$$

Veselu skaitļu virknes

Virkne a^m

- Piemēros, kuros iesaistītas veselu skaitļu pakāpes ar mainīgu kāpinātāju, var noderēt šāda teorēma:

2. teorēma

Pieņemsim, ka a un n ir veseli skaitļi, $n \geq 2$. Tad virkne $x_m = a^m$, $m = 0, 1, 2, \ldots$ ir periodiska pēc moduļa n.

Piemēram, $a = 2$, $n = 5$:

- $2^0 = 1 \equiv 1 \pmod{5}$
- $2^1 = 2 \equiv 2 \pmod{5}$
- $2^2 = 2 \equiv 4 \pmod{5}$
- $2^3 = 8 \equiv 3 \pmod{5}$
- $2^4 = 16 \equiv 1 \pmod{5}$
- $2^5 = 32 \equiv 2 \pmod{5}$
- $\ldots$

Piemēram, $a = 2$, $n = 5$:

- $2^0 = 1 \equiv 1 \pmod 5$
- $2^1 = 2 \equiv 2 \pmod 5$
- $2^2 = 2 \equiv 4 \pmod 5$
- $2^3 = 8 \equiv 3 \pmod 5$
- $2^4 = 16 \equiv 1 \pmod 5$
- $2^5 = 32 \equiv 2 \pmod 5$
- ...

Apkopojot šo informāciju tabulā:

m	0	1	2	3	4	5	6	7	8	...
$2^m \pmod 5$	1	2	4	3	1	2	4	3	1	...

2. piemērs

Aprēķināt, kādu atlikumu dod skaitlis 12^{23}, dalot to ar 5!

2. piemērs

Aprēķināt, kādu atlikumu dod skaitlis 12^{23}, dalot to ar 5!

- Jāaprēķina $12^{23} \pmod 5$.

2. piemērs

Aprēķināt, kādu atlikumu dod skaitlis 12^{23}, dalot to ar 5!

- Jāaprēķina $12^{23} \pmod 5$.
- Ievēro, ka $12 \equiv 2 \pmod 5$. Tātad $12^{23} \equiv 2^{23} \pmod 5$.

2. piemērs

Aprēķināt, kādu atlikumu dod skaitlis 12^{23}, dalot to ar 5!

- Jāaprēķina $12^{23} \pmod 5$.
- Ievēro, ka $12 \equiv 2 \pmod 5$. Tātad $12^{23} \equiv 2^{23} \pmod 5$.
- Jau noskaidrojām, ka $2^4 \equiv 1 \pmod 5$. Tātad

$$2^{23} = 2^{4\cdot 5+3} = \left(2^4\right)^5 \cdot 2^3 \equiv 1^5 \cdot 8 \equiv 3 \pmod 5.$$

- Secinām ka 12^{23}, dalot ar 5, dod atlikumu 3.

3. piemērs

Aprēķināt, kādu atlikumu dod skaitlis 2^{23}, dalot to ar 24!

3. piemērs

Aprēķināt, kādu atlikumu dod skaitlis 2^{23}, dalot to ar 24!

- Jāaprēķina $2^{23} \pmod{24}$.

3. piemērs

Aprēķināt, kādu atlikumu dod skaitlis 2^{23}, dalot to ar 24!

- Jāaprēķina $2^{23} \pmod{24}$.
- Sastādām tabulu:

m	0	1	2	3	4	5	6	7	8	...
$2^m \pmod{24}$	1	2	4	8	16	8	16	8	16	...

3. piemērs

Aprēķināt, kādu atlikumu dod skaitlis 2^{23}, dalot to ar 24!

- Jāaprēķina $2^{23} \pmod{24}$.
- Sastādām tabulu:

m	0	1	2	3	4	5	6	7	8	...
$2^m \pmod{24}$	1	2	4	8	16	8	16	8	16	...

- Visiem $m \geq 3$ skaitlis 2^m dalās ar 8. Arī 24 dalās ar 8.
- Virknei $2^m \pmod{24}$, $m = 0, 1, 2, \ldots,$ ir priekšperiods!
- Perioda garums ir 2.

3. piemērs

- Aprēķināt, kādu atlikumu dod skaitlis 2^{23}, dalot to ar 24!
- Ievēro, ka

$$2^{23} = 2^{2\cdot 11+1} = \left(2^2\right)^{10} \cdot 2 \equiv 4^{10} \cdot 2 \pmod{24}.$$

3. piemērs

- Aprēķināt, kādu atlikumu dod skaitlis 2^{23}, dalot to ar 24!
- Ievēro, ka

$$2^{23} = 2^{2\cdot 11+1} = \left(2^2\right)^{10} \cdot 2 \equiv 4^{10} \cdot 2 \pmod{24}.$$

- Sastādām tabulu:

m	1	2	3	4	5	6	7	8	...
$4^m \pmod{24}$	4	16	16	16	16	16	16	16	...

- Secinām, ka $4^m \equiv 16 \pmod{24}$ visiem $m \geq 2$.

3. piemērs

- Aprēķināt, kādu atlikumu dod skaitlis 2^{23}, dalot to ar 24!
- Ievēro, ka

$$2^{23} = 2^{2\cdot 11+1} = \left(2^2\right)^{10} \cdot 2 \equiv 4^{10} \cdot 2 \pmod{24}.$$

- Sastādām tabulu:

m	1	2	3	4	5	6	7	8	...
$4^m \pmod{24}$	4	16	16	16	16	16	16	16	...

- Secinām, ka $4^m \equiv 16 \pmod{24}$ visiem $m \geq 2$.
- Tātad

$$2^{23} \equiv 4^{10} \cdot 2 \equiv 16 \cdot 2 \equiv 32 \equiv 8 \pmod{24}.$$

- Iegūstam, ka 2^{23}, dalot ar 24, dod atlikumu 8.

3. uzdevums

Aprēķināt skaitļa 12^{23} pēdējo ciparu!

3. uzdevums

Jāaprēķina, ar ko kongruents $12^{23} \pmod{10}$. Ievēro, ka $12 \equiv 2 \pmod{10}$.

3. uzdevums

Sastāda tabulu:

m	0	1	2	3	4	5	6	7	8	...
$2^m \pmod{10}$	1	2	4	8	6	2	4	8	6	...

Virkne ir periodiska ar priekšperiodu; perioda garums ir 4.

3. uzdevums

Aprēķinām

$$12^{23} \equiv 2^{23} = 2^{4\cdot 5+3} = \left(2^4\right)^5 \cdot 2^3 \equiv 6^5 \cdot 8 \pmod{10}.$$

- Jau noskaidrojām, ka $2^4 \equiv 6 \pmod{10}$. Ievēro, ka $6^2 \equiv 6 \pmod{10}$, tāpēc $6^m \equiv 6 \pmod{10}$ visiem naturāliem m.

3. uzdevums

Aprēķinām

$$12^{23} \equiv 2^{23} = 2^{4\cdot 5+3} = \left(2^4\right)^5 \cdot 2^3 \equiv 6^5 \cdot 8 \pmod{10}.$$

- Jau noskaidrojām, ka $2^4 \equiv 6 \pmod{10}$. Ievēro, ka $6^2 \equiv 6 \pmod{10}$, tāpēc $6^m \equiv 6 \pmod{10}$ visiem naturāliem m.
- Tātad
$$2^{23} \equiv 6^5 \cdot 8 \equiv 6 \cdot 8 \equiv 8 \pmod{10}.$$
- Secinām ka 12^{23} pēdējais cipars ir 8.

Fibonači virkne

- Fibonači skaitļu virkni definē šādi:

$F_1 = 1,\ F_2 = 1,$

$$F_{m+2} = F_m + F_{m+1}, \quad \text{visiem naturāliem skaitļiem } m.$$

- Arī Fibonači skaitļu virkne ir periodiska pēc jebkura moduļa $n \geq 2$.

4. piemērs

Vai F_{2015} dalās ar 3?

4. piemērs

Vai F_{2015} dalās ar 3?

- Aprēķināsim $F_{2015} \pmod 3$.

4. piemērs

Vai F_{2015} dalās ar 3?

- Aprēķināsim $F_{2015} \pmod 3$.
- Apskata pirmos Fibonači virknes locekļus pēc moduļa 3:

m	1	2	3	4	5	6	7	8	9	10	11	...
F_m	1	1	2	3	5	8	13	21	34	55	89	...
$F_m \pmod 3$	1	1	2	0	2	2	1	0	1	1	2	...

4. piemērs

Vai F_{2015} dalās ar 3?

- Aprēķināsim $F_{2015} \pmod 3$.
- Apskata pirmos Fibonači virknes locekļus pēc moduļa 3:

m	1	2	3	4	5	6	7	8	9	10	11	...
F_m	1	1	2	3	5	8	13	21	34	55	89	...
$F_m \pmod 3$	1	1	2	0	2	2	1	0	1	1	2	...

- Pirmie astoņi virknes $F_m \pmod 3$ virknes locekļi veido periodu.

4. piemērs

- Secinām, ka $F_m \equiv F_{m+8k} \pmod{3}$ visiem $k \in \mathbb{N}$.

4. piemērs

- Secinām, ka $F_m \equiv F_{m+8k} \pmod 3$ visiem $k \in \mathbb{N}$.
- Ievēro, ka $2015 = 8 \cdot 251 + 7$. Tātad
$$F_{2015} \equiv F_7 \equiv 1 \pmod 3.$$
- Tātad F_{2015} nedalās ar 3.

Veselu skaitļu pakāpes

Veselu skaitļu pakāpes

- Vai vesela skaitļa kvadrāts var dot atlikumu 2, dalot ar 3?
- Kādus atlikumus, dalot ar 3, dod veselu skaitļu kvadrāti?

$n \pmod 3$	0	1	2
$n^2 \pmod 3$	$0^2 \equiv 0 \pmod 3$	$1^2 \equiv 1 \pmod 3$	$2^2 \equiv 1 \pmod 3$

- Secinām: vesela skaitļa kvadrāts, dalot ar 3, var dot atlikumus 0 vai 1.
- $n^2 \in \{0; 1\} \pmod 3$.

5. piemērs

Dots, ka a, b – naturāli skaitļi un $a^2 + b^2$ dalās ar 3. Pierādīt, ka $a^2 + b^2$ dalās ar 9!

5. piemērs

Dots, ka a, b – naturāli skaitļi un $a^2 + b^2$ dalās ar 3. Pierādīt, ka $a^2 + b^2$ dalās ar 9!

- $a^2 \equiv 0 \pmod 3$ vai $a^2 \equiv 1 \pmod 3$;
- $b^2 \equiv 0 \pmod 3$ vai $b^2 \equiv 1 \pmod 3$;
- Atliksim iespējamās $a^2 + b^2$ vērtības (pēc moduļa 3) tabulā.

5. piemērs

Dots, ka a, b – naturāli skaitļi un $a^2 + b^2$ dalās ar 3. Pierādīt, ka $a^2 + b^2$ dalās ar 9!

- $a^2 \equiv 0 \pmod 3$ vai $a^2 \equiv 1 \pmod 3$;
- $b^2 \equiv 0 \pmod 3$ vai $b^2 \equiv 1 \pmod 3$;
- Atliksim iespējamās $a^2 + b^2$ vērtības (pēc moduļa 3) tabulā.

$b^2 \pmod 3$ \ $a^2 \pmod 3$	0	1
0	$0 + 0 \equiv 0 \pmod 3$	$1 + 0 \equiv 1 \pmod 3$
1	$0 + 1 \equiv 1 \pmod 3$	$1 + 1 \equiv 2 \pmod 3$

$a^2 + b^2$ dalās ar 3 tikai tad, ja a un b katrs dalās ar 3.
Taču tad gan a^2, gan b^2 dalās ar 9; tātad arī to summa dalās ar 9.

5. piemērs

- Faktiski pierādīts: nevar atrast tādus veselus skaitļus a, b, n, ka izpildītos kāda no vienādībām

$$a^2 + b^2 = 9n + 3$$

vai

$$a^2 + b^2 = 9n + 6.$$

4. uzdevums

Pierādīt, ka nevar atrast tādus veselus skaitļus n, x, y, ka

$$7n + 3 = x^3 + y^3 \ !$$

4. uzdevums

- Atrodam, kādus atlikumus var dot vesela skaitļa kubs, dalot ar 7:

$a \pmod 7$	0	1	2	3	4	5	6
$a^3 \pmod 7$							

4. uzdevums

- Atrodam, kādus atlikumus var dot vesela skaitļa kubs, dalot ar 7:

$a \pmod 7$	0	1	2	3	4	5	6
$a^3 \pmod 7$	0	1	1	6	1	6	6

4. uzdevums

- $x^3, y^3 \in \{-1; 0; 1\} \pmod 7$;
- Sastādām tabulu, pa rindiņām apskatot iespējamās x^3 vērtības pēc moduļa 7, pa kolonnām y^3 vērtības pēc moduļa 7, bet tabulas šūnās atliekot $x^3 + y^3 \pmod 7$:

$x^3 \pmod 7$ / $y^3 \pmod 7$	-1	0	1
-1			
0			
1			

- Secinām: $x^3 + y^3 \in \{-2; -1; 0; 1; 2\} \pmod 7$.
- Tātad $7n + 3 \neq x^3 + y^3$.

4. uzdevums

- $x^3, y^3 \in \{-1; 0; 1\} \pmod 7$;
- Sastādām tabulu, pa rindiņām apskatot iespējamās x^3 vērtības pēc moduļa 7, pa kolonnām y^3 vērtības pēc moduļa 7, bet tabulas šūnās atliekot $x^3 + y^3 \pmod 7$:

$y^3 \pmod 7$ \ $x^3 \pmod 7$	-1	0	1
-1	-2	-1	0
0			
1			

- Secinām: $x^3 + y^3 \in \{-2; -1; 0; 1; 2\} \pmod 7$.
- Tātad $7n + 3 \neq x^3 + y^3$.

4. uzdevums

- $x^3, y^3 \in \{-1; 0; 1\} \pmod 7$;
- Sastādām tabulu, pa rindiņām apskatot iespējamās x^3 vērtības pēc moduļa 7, pa kolonnām y^3 vērtības pēc moduļa 7, bet tabulas šūnās atliekot $x^3 + y^3 \pmod 7$:

$x^3 \pmod 7$ / $y^3 \pmod 7$	-1	0	1
-1	-2	-1	0
0	-1	0	1
1			

- Secinām: $x^3 + y^3 \in \{-2; -1; 0; 1; 2\} \pmod 7$.
- Tātad $7n + 3 \neq x^3 + y^3$.

4. uzdevums

- $x^3, y^3 \in \{-1; 0; 1\} \pmod 7$;
- Sastādām tabulu, pa rindiņām apskatot iespējamās x^3 vērtības pēc moduļa 7, pa kolonnām y^3 vērtības pēc moduļa 7, bet tabulas šūnās atliekot $x^3 + y^3 \pmod 7$:

$x^3 \pmod 7$ / $y^3 \pmod 7$	-1	0	1
-1	-2	-1	0
0	-1	0	1
1	0	1	2

- Secinām: $x^3 + y^3 \in \{-2; -1; 0; 1; 2\} \pmod 7$.
- Tātad $7n + 3 \neq x^3 + y^3$.

Paldies par uzmanību!