O zbytcích

Lenka Zalabová

Ústav matematiky a biomatematiky, Přírodovědecká fakulta, Jihočeská univerzita v Českých Budějovicích

November 24, 2015

Celá čísla $\mathbb{Z}$

Budeme se bavit počítáním s celými čísly

$$\ldots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \ldots$$

Ta mezi sebou umíme

- sčítat a odčítat $7 + 9 = 16,\ 2 - 4 = -2$
- násobit $3 \cdot 7 = 21,\ (-2) \cdot 6 = -12$
- někdy bezproblémově vydělit $12 : 3 = 4$
- a někdy taky ne $13 : 5 = ?$

Dělení se zbytkem

Theorem

Mějme celá čísla $a > 0$ a $b \geq 0$. Pak existují jednoznačně čísla $q \geq 0$ a $0 \leq r < a$ tak, že

$$b = a \cdot q + r.$$

- q ... *podíl* po dělení čísla b číslem a
- r ... *zbytek* po dělení čísla b číslem a

Example

$$13 = 5 \cdot 2 + 3$$

Dělení beze zbytku

Definition

Řekneme, že celé číslo a *dělí* celé číslo b, jestliže existuje celé číslo q takové, že

$$b = a \cdot q.$$

V takovém případě píšeme $a \mid b$.
V opačném případě říkáme, že a *nedělí* b, a píšeme $a \nmid b$.

Example

Platí:

- $7 \mid 35$, protože $35 = 7 \cdot 5$,
- $8 \nmid 60$, protože $60 = 8 \cdot 7 + 4$.

(De)motivační příklad

Example

Ukažte, že číslo 13 dělí $2010^{2010} + 1$.

- Platí $2010 = 13 \cdot 154 + 8$.
- Pak $2010^{2010} + 1 = (13 \cdot 154 + 8)^{2010} + 1$.
- Představme si roznásobení

$$\underbrace{(13 \cdot 154 + 8) \cdot (13 \cdot 154 + 8) \cdot \ldots \cdot (13 \cdot 154 + 8)}_{2010}.$$

Které části výsledku obsahují nějaký násobek 13 a které ne?

(De)motivační příklad

- Je vidět, že násobek 13 nebude obsahovat pouze člen 8^{2010}. Vlastně máme

$$2010^{2010} + 1 = 13 \cdot (\text{odpad}) + (8^{2010} + 1)$$

  a dál tedy stačí zkoumat číslo $8^{2010} + 1$.
- Platí $8^{2010} = (8^2)^{1005} = 64^{1005}$ a dostaneme

$$8^{2010} + 1 = 64^{1005} + 1 = (13 \cdot 5 - 1)^{1005} + 1.$$

- Opět si představme roznásobení

$$\underbrace{(13 \cdot 5 - 1)(13 \cdot 5 - 1) \cdot \cdots \cdot (13 \cdot 5 - 1)}_{1005}.$$

  Které části výsledku obsahují nějaký násobek 13 a které ne?

(De)motivační příklad

- Je vidět, že násobek 13 nebude obsahovat pouze člen $(-1)^{1005}$. Vlastně máme

$$8^{2010} + 1 = 13 \cdot (\text{odpad}) + ((-1)^{1005} + 1).$$

- Tedy zbytek po dělení čísla $8^{2010} + 1$ číslem 13 je $(-1)^{1005} + 1 = -1 + 1 = 0$.

V podstatě jsme neustále zkoumali zbytky po dělení, aniž bychom se zajímali o podíly při dělení. Podíl při dělení čísla $2010^{2010} + 1$ číslem 13 neznáme.

Kongruence

... pojem kongruence byl vytvořen pro efektivní počítání se zbytky při dělení.

Definition

Buď n přirozené číslo. Dvě celá čísla a, b se nazývají *kongruentní podle modulu n*, píšeme

$$a \equiv b \mod n,$$

jestliže platí následující ekvivalentní podmínky:

1. $n \mid a - b$, neboli: rozdíl čísel $a - b$ je dělitelný číslem n beze zbytku,
2. $a = b + k \cdot n$ pro vhodné $k \in \mathbb{Z}$, neboli: čísla a, b se od sebe liší o nějaký vhodný násobek n,
3. čísla a, b dávají při dělení číslem n stejný zbytek.

Kongruence

Example

Platí

$$25 \equiv 7 \mod 6,$$

protože:

1. $6 \mid 25 - 7 = 18$, neboli: rozdíl $25 - 7 = 18$ je dělitelný číslem 6 beze zbytku,
2. $25 = 7 + 3 \cdot 6$, neboli: čísla 25 a 7 se od sebe liší o trojnásebek čísla 6,
3. Čísla 25 a 7 dávají při dělení číslem 6 stejný zbytek 1. Platí:
   - $25 = 6 \cdot 4 + 1$,
   - $7 = 6 \cdot 1 + 1$.

Kongruence

... zejména platí: Každé celé číslo x je modulo n kongruentní se zbytkem po dělení čísla x číslem n!

Example

Platí:

- $25 \equiv 1 \mod 6$,
- $7 \equiv 1 \mod 6$.

Zatím jsme pomocí kongruencí získali pouze nový způsob, jak zapisovat dělení a zbytky. Výhoda tohoto zápisu je hlavně v tom, že s kongruencemi se dá efektivně ‘počítat’, a tedy efektivně řešit úlohy o dělení a zbytcích.

Jak se počítá s kongruencemi?

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

(1) Jestliže $a \equiv b \mod n$, pak $a + c \equiv b + c \mod n$.

(2) Jestliže $a \equiv b \mod n$, pak $a - c \equiv b - c \mod n$.

(3) Jestliže $a \equiv b \mod n$, pak $a \cdot c \equiv b \cdot c \mod n$.

(4) Jestliže $a \equiv b \mod n$ a zároveň $c \equiv d \mod n$, pak $a + c \equiv b + d \mod n$.

(5) Jestliže $a \equiv b \mod n$ a zároveň $c \equiv d \mod n$, pak $a - c \equiv b - d \mod n$.

(6) Jestliže $a \equiv b \mod n$ a zároveň $c \equiv d \mod n$, pak $a \cdot c \equiv b \cdot d \mod n$.

(7) Jestliže $a \equiv b \mod n$, pak $a^k \equiv b^k \mod n$.

1. příklad

Example

Nalezněte zbytek po dělení čísla 2^{30} číslem 5.

Hledáme číslo $0 \leq x < 5$ splňující $x \equiv 2^{30} \mod 5$.

- Platí $2^2 = 4$ a z definice kongruence $4 \equiv -1 \mod 5$.
- Platí $2^{30} = (2^2)^{15} = 4^{15}$ a vlastnost (7) pak říká

$$4^{15} \equiv (-1)^{15} \mod 5.$$

- Zřejmě $(-1)^{15} = -1$. Dohromady dostaneme

$$2^{30} \equiv -1 \mod 5.$$

- Protože $-1 \equiv 4 \mod 5$, je zbytek po dělení čísla 2^{30} číslem 5 roven 4.

2. příklad

Example

Zjistěte, zda číslo 5 dělí číslo $47^2 + 12^{136}$.

Zjišťujeme, zda platí $47^2 + 12^{136} \equiv 0 \mod 5$.

- Platí $12^{136} = (12^2)^{68} = 144^{68}$.
- Z definice kongruence $144 \equiv -1 \mod 5$.
- Vlastnost (7) pak říká $144^{68} \equiv (-1)^{68} \mod 5$.
- Zřejmě $(-1)^{68} = 1$. Dohromady dostaneme

$$12^{136} \equiv 1 \mod 5.$$

2. příklad

- Platí $47 \equiv 2 \mod 5$.
- Vlastnost (7) pak říká $47^2 \equiv 2^2 \mod 5$ a máme tedy

$$47^2 \equiv 4 \mod 5.$$

- Získané kongruence $12^{136} \equiv 1 \mod 5$ a $47^2 \equiv 4 \mod 5$ sečteme podle (4) a dostaneme

$$12^{136} + 47^2 \equiv 5 \mod 5.$$

- Protože $5 \equiv 0 \mod 5$, je dělení beze zbytku.

3. příklad

Example

Nalezněte zbytek po dělení čísla 72^{11} číslem 17.

- Platí $72 = 4 \cdot 18$ a tedy $72^{11} = 4^{11} \cdot 18^{11}$.
- Z definice kongruence $18 \equiv 1 \mod 17$ a tedy podle (7) platí $18^{11} \equiv 1^{11} \mod 17$.
- Zřejmě $1^{11} = 1$ Podle (3) platí

$$4^{11} \cdot 18^{11} \equiv 4^{11} \mod 17,$$

a tedy stačí hledat zbytek po dělení čísla 4^{11} číslem 17.

3. příklad

- Platí $4^{11} = 4 \cdot 4^{10} = 4 \cdot (4^2)^5 = 4 \cdot 16^5$.
- Z definice kongruence $16 \equiv -1 \mod 17$ a podle (7) máme $16^5 \equiv (-1)^5 \mod 17$.
- Podle (3) dostaneme $4 \cdot 16^5 \equiv 4 \cdot (-1)^5 \mod 17$.
- Zřejmě $4 \cdot (-1)^5 = -4$. Dohromady dostaneme

$$4^{11} \equiv -4 \mod 17.$$

- Protože $-4 \equiv 13 \mod 17$, je zbytek po dělení čísla 72^{11} číslem 17 roven 13.

4. příklad

Example

Najděte zbytek po dělení čísla 4^{48} číslem 97.

- Platí $4^{48} = (4^3)^{16} = 64^{16}$.
- Z definice kongruence $64 \equiv -33 \mod 97$ a tedy podle (7) platí $64^{16} = (-33)^{16} \mod 97$.
- Platí $(-33)^{16} = 33^{16} = (33^2)^8 = (1089)^8$.
- Platí $1089 = 11 \cdot 97 + 22$.
- Z definice kongruence $1089 \equiv 22 \mod 97$ a tedy podle (7) platí

$$1089^8 \equiv 22^8 \mod 97.$$

4. příklad

- Platí $22^8 = (22^2)^4 = 484^4$.
- Platí $484 = 4 \cdot 97 + 96$.
- Z definice kongruence $484 \equiv -1 \mod 97$ a tedy

$$484^4 \equiv (-1)^4 \mod 97.$$

- Zřejmě $(-1)^4 = 1$ a tedy zbytek po dělení je 1.

5. příklad

Example

Ukažte, že číslo 13 dělí číslo $16^{15} + 29^{14} + 42^{13}$.

- Platí $16 \equiv 3 \mod 13$ a podle (7) dostaneme $16^{15} \equiv 3^{15} \mod 13$.
- Stejně dostaneme $29^{14} \equiv 3^{14} \mod 13$ a $42^{13} \equiv 3^{13} \mod 13$.
- Podle (3) dostaneme

$$16^{15} + 29^{14} + 42^{13} \equiv 3^{15} + 3^{14} + 3^{13} \mod 13.$$

- Platí $3^{15} + 3^{14} + 3^{13} = 3^{13} \cdot (9 + 3 + 1) = 3^{13} \cdot 13$.
- Dohromady dostaneme

$$16^{15} + 29^{14} + 42^{13} \equiv 13 \cdot 3^{13} \mod 13$$

a tedy dělení je beze zbytku.

6. příklad

Example

Nalezněte zbytek po dělení čísla $13^{12} + 12^{11} + 11^{10}$ číslem 9.

- Platí $13 \equiv 4 \mod 9$ a podle (7) dostaneme $13^{12} \equiv 4^{12} \mod 9$.
- Stejně dostaneme $12^{11} \equiv 3^{11} \mod 9$ a $11^{10} \equiv 2^{10} \mod 9$.
- Podle (3) dostaneme

$$13^{12} + 12^{11} + 11^{10} \equiv 4^{12} + 3^{11} + 2^{10} \mod 9.$$

6. příklad

- Upravíme výraz $4^{12} + 3^{11} + 2^{10}$.
- Platí $4^{12} = (2^2)^{12} = 2^{24} = (2^3)^8 = 8^8$.
- Platí $3^{11} = 3^2 \cdot 3^9 = 9 \cdot 3^9$.
- Platí $2^{10} = 2 \cdot 2^9 = 2 \cdot (2^3)^3 = 2 \cdot 8^3$.
- Dohromady dostaneme

$$13^{12} + 12^{11} + 11^{10} \equiv 8^8 + 9 \cdot 3^9 + 2 \cdot 8^3 \mod 9.$$

6. příklad

- Platí $8 \equiv -1 \mod 9$ a zároveň $9 \equiv 0 \mod 9$.
- Dostaneme

$$13^{12} + 12^{11} + 11^{10} \equiv (-1)^8 + 2 \cdot (-1)^3 \mod 9.$$

- Dohromady dostaneme $13^{12} + 12^{11} + 11^{10} \equiv 1 - 2 \mod 9$ a tedy

$$13^{12} + 12^{11} + 11^{10} \equiv -1 \mod 9.$$

- Platí $-1 \equiv 8 \mod 9$ a tedy zbytek po dělení je 8.

7. příklad

Example

Určete poslední dvě cifry dekadického zápisu čísla $3^{9876543}$.

Poslední dvě čísla dekadického zápisu ... zbytek po dělení číslem 100. Hledáme x splňující $x \equiv 3^{9876543} \mod 100$.

- Platí $3^{9876543} = (3^3)^{3292181} = 27^{3292181} = 27 \cdot 27^{3292180}$.
- Platí $27^{3292180} = (27^2)^{1646090}$.
- Platí $27^2 = 729 = 7 \cdot 100 + 29$ a tedy $27^2 \equiv 29 \mod 100$.
- Dohromady dostaneme $27^{3292180} \equiv 29^{1646090} \mod 100$ a tedy celkem

$$3^{9876543} \equiv 27 \cdot 27^{3292180} \equiv 27 \cdot 29^{1646090} \mod 100.$$

7. příklad

- Platí $29^{1646090} = (29^2)^{823045} = 841^{823045}$.
- Platí $841 = 8 \cdot 100 + 41$ a tedy $841 \equiv 41 \mod 100$.
- Dohromady dostaneme $29^{1646090} \equiv 41^{823045} \mod 100$ a tedy celkem

$$3^{9876543} \equiv 27 \cdot 29^{1646090} \equiv 27 \cdot 41^{823045} \mod 100.$$

7. příklad

- Platí $41^{823045} = (41^5)^{164609} = (115856201)^{164609}$.
- Platí $115856201 = 1158562 \cdot 100 + 1$ a tedy $115856201 \equiv 1 \mod 100$.
- Dohromady dostaneme $41^{823045} \equiv 1^{164609} \mod 100$ a tedy celkem

$$3^{9876543} \equiv 27 \cdot 41^{823045} \equiv 27 \cdot 1 \mod 100.$$

- Tedy poslední dvě cifry čísla $3^{9876543}$ jsou 27.

Dělitelnost třemi

Ze základky všichni víte...

Theorem

Celé číslo je dělitelné třemi právě tehdy, když jeho ciferný součet je dělitelný třemi.

Example

Je číslo 138309241 dělitelné třemi?

- Platí $1+3+8+3+0+9+2+4+1=28$, a to není dělitelné třemi. Tedy 138309241 není dělitelné třemi.

Proč to funguje?

Každé číslo $a_n a_{n-1} \cdots a_2 a_1 a_0$ lze zapsat ve tvaru

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$$
$$= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 100 + a_1 \cdot 10 + a_0$$

Example

$$489 = 4 \cdot 100 + 8 \cdot 10 + 9$$

Budeme zkoumat zbytek takto zapsaného čísla při dělení třemi.

Proč to funguje?

- Z definice kongruence $10 \equiv 1 \mod 3$.
- Vlastnost (7) pak říká, že pro každé přirozené číslo k platí

$$10^k \equiv 1^k = 1 \mod 3.$$

- Vlastnost (3) pak říká, že pro každou cifru a_k platí

$$a_k \cdot 10^k \equiv a_k \cdot 1 = a_k \mod 3.$$

- Vlastnost (4) pak říká, že pro jejich součet platí

$$\begin{aligned} &a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \mod 3. \end{aligned}$$

- Tedy $a_n a_{n-1} \cdots a_2 a_1 a_0$ dává stejný zbytek při dělení třemi jako $a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0$.

Dělitelnost sedmi

Na základce vám nejspíš neříkali...

Theorem

Celé číslo je dělitelne sedmi právě tehdy, když je sedmi dělitelný součet vypočtený tak, že se cifry odzadu vynásobí postupně periodicky se opakujícími čísly $1, 3, 2, 6, 4, 5$ *a to se sečte.*

Example

Je číslo 138309241 dělitelné sedmi?

- Platí
  $\mathbf{1} \cdot 1 + \mathbf{3} \cdot 4 + \mathbf{2} \cdot 2 + \mathbf{6} \cdot 9 + \mathbf{4} \cdot 0 + \mathbf{5} \cdot 3 + \mathbf{1} \cdot 8 + \mathbf{3} \cdot 3 + \mathbf{2} \cdot 1 = 105.$
  Dále platí $\mathbf{1} \cdot 5 + \mathbf{3} \cdot 0 + \mathbf{2} \cdot 1 = 7$. Tedy 135797531 je dělitelné sedmi.

Proč to funguje?

- Z definice kongruence $10 \equiv 3 \mod 7$.
- Vlastnost (7) pak říká, že pro každé přirozené číslo k platí

$$10^k \equiv 3^k \mod 7.$$

- Vlastnost (3) pak říká, že pro každou cifru a_k platí

$$a_k \cdot 10^k \equiv a_k \cdot 3^k \mod 3.$$

- Vlastnost (4) pak říká, že pro jejich součet platí

$$\begin{aligned} &a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0 \\ \equiv &a_n \cdot 3^n + a_{n-1} \cdot 3^{n-1} + \cdots + a_2 \cdot 3^2 + a_1 \cdot 3^1 + a_0 \cdot 3^0 \mod 3. \end{aligned}$$

Proč to funguje?

Platí:

- $3^0 = 1$ a $3^1 = 3$,
- $3^2 = 9$ a platí $9 \equiv 2 \mod 7$. Dohromady

$$3^2 \equiv 2 \mod 7.$$

- $3^3 = 3 \cdot 3^2$ a podle (3) platí $3 \cdot 3^2 \equiv 3 \cdot 2 \mod 7$. Dohromady

$$3^3 \equiv 6 \mod 7.$$

- $3^4 = 3 \cdot 3^3$ a podle (3) platí $3 \cdot 3^3 \equiv 3 \cdot 6 \mod 7$. Platí $18 \equiv 4 \mod 7$ a dohromady

$$3^4 \equiv 4 \mod 7.$$

Proč to funguje?

- $3^5 = 3 \cdot 3^4$ a podle (3) platí $3 \cdot 3^4 \equiv 3 \cdot 4 \mod 7$. Platí $12 \equiv 5$ a dohromady

$$3^5 \equiv 5 \mod 7.$$

- $3^6 = 3 \cdot 3^5$ a podle (3) platí $3 \cdot 3^5 \equiv 3 \cdot 5 \mod 7$. Platí $15 \equiv 1 \mod 7$ a dohromady

$$3^6 \equiv 1 \mod 7.$$

... a už jedeme dokolečka.

Použitá literatura

- TEORIE ČÍSEL sbírka příkladu, Jiří Růžička, Diplomová práce, Masarykova univerzita, Brno, 2006
- Teorie čísel a úvod do šifrování, Zbyněk Šír, `http://www.talnet.cz/documents/18/54ffba6e-4e85-4475-b14d-4a63c19b4e3c`
- Dělitelnost aneb modulární aritmetika, Mirko Rokyta, `http://physics.ujep.cz/~jmaly/mo/delitelnost11.pdf`
- Obecná algebra pro učitele, Pavel Tlustý, České Budějovice, 2006