Kongruence, rozklad na zbytkové třídy.

Věta: Nechť a, b jsou celá čísla taková, že $b \neq 0$. Potom existují celá čísla q, r splňující vztah:

$$a = bq + r,\ 0 \leq r < |b|,$$ přičemž toto vyjádření je jednoznačné.

Poznámka: Je nutno si uvědomit, že zbytek r při dělení je vždy nezáporný, a to i při dělení záporným číslem. Např. a = –26, b = 8, q = –4, r = 6, protože –26 = 8 . (–4) + 6.

Poznámka: Celá čísla a, b jsou nesoudělná, je-li jejich největší společný dělitel roven jedné. V opačném případě se nazývají soudělná. Největší společný dělitel čísel a, b budeme označovat NSD(a, b), nejmenší kladný společný násobek NSN(a, b).

Eulerova funkce $\varphi(n)$ vyjadřuje počet přirozených čísel menších nebo rovných číslu n, nesoudělných s n. Nechť $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, pak platí $\varphi(n) = n \cdot \prod_{i=1}^{k}(1 - \frac{1}{p_i})$. Je-li n prvočíslo, pak $\varphi(n) = n - 1$.

Kongruence: $a, b \in \mathbf{Z}, m \in \mathbf{N}, m \geq 2$. Platí $a \equiv b \Leftrightarrow m \mid (a - b)$. Čteme: Číslo a je kongruentní s číslem b podle modulu m. Dvě čísla kongruentní podle nějakého modulu m dávají při dělení tímto modulem m týž zbytek. Relace kongruence je ekvivalence na množině všech celých čísel (je reflexivní, symetrická a tranzitivní).

Vlastnosti kongruencí:

1) p prvočíslo $\quad a \equiv b \pmod{p^n} \Rightarrow a \equiv b \pmod{p}$

Platí-li kongruence podle modulu, který je mocninou prvočísla, platí i podle modulu rovného tomuto prvočíslu.

2) $a \equiv b \pmod{m_i}$, $i = 1, 2, \ldots, k \Rightarrow a \equiv b \pmod{\mathrm{NSN}(m_1, \ldots, m_k)}$

Platí-li kongruence podle několika modulů, platí i podle modulu rovného nejmenšímu společnému násobku těchto modulů.

3) $a_i \equiv b_i \pmod{m}$, $i = 1, \ldots, k \Rightarrow \sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod{m}$, $\quad \prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{m}$.

Kongruence podle téhož modulu lze sčítat i násobit.

Nechť v dalším platí $a \equiv b \pmod{m}$:

4) $a + x \equiv b + x \pmod{m}$, $\quad a.y \equiv b.y \pmod{m}$

K oběma stranám kongruence lze přičíst stejné celé číslo a obě strany kongruence lze vynásobit týmž celým číslem. **Obecně ale nelze obě strany kongruence dělit týmž celým číslem,** např. $24 \equiv 40 \pmod{8}$, ale po vydělení čtyřmi $6 \not\equiv 10 \pmod{8}$.

5) $m \mid z \Rightarrow a + z \equiv b \pmod{m}$

Celé číslo, které je násobkem modulu, lze přičíst pouze k jedné straně kongruence.

6) $a^n \equiv b^n \pmod{m}$

Obě strany kongruence lze umocnit na libovolný přirozený exponent.

7) $d \mid a \wedge d \mid b \wedge \mathrm{NSD}(d, m) = 1 \Rightarrow \dfrac{a}{d} \equiv \dfrac{b}{d} \pmod{m}$

Obě strany kongruence lze vydělit celým číslem nesoudělným s modulem.

8) $ac \equiv bc \pmod{mc}$

Obě strany kongruence i modul lze vynásobit týmž celým kladným číslem.

9) $e \mid a \wedge e \mid b \wedge e \mid c \Rightarrow \dfrac{a}{e} \equiv \dfrac{b}{e} \pmod{\dfrac{m}{e}}$

Obě strany kongruence i modul lze vydělit týmž celým kladným číslem různým od nuly.

10) $a \equiv b \pmod{m} \wedge d \mid m \Rightarrow a \equiv b \pmod{d}$

Platí-li kongruence podle modulu m, platí i podle modulu rovného libovolnému kladnému děliteli čísla m, většímu než jedna.

Eulerova věta: $m \in \mathrm{N}$, $m > 1$, $a \in \mathbf{Z}$, $\mathrm{D}(a,m) = 1$, pak $a^{\varphi(m)} \equiv 1 \pmod{m}$.
Je-li specielně p prvočíslo, které není dělitelem čísla a, pak platí $a^{p-1} \equiv 1 \pmod{p}$ (tzv. malá Fermatova věta).

Definice.
Nechť m je pevné přirozené číslo. Označme:

$$C_i = \{ x \in \mathbb{Z} \mid x \text{ dává po dělení číslem } m \text{ zbytek } i \}, \quad \text{pro } i = 0, 1, \dots, m-1$$

Pak množina C_i se nazývá **zbytková třída** podle modulu m. Symbolem $\mathbb{Z}_m$ se označí **množina všech zbytkových tříd podle modulu** m, tzn. $\mathbb{Z}_m = \{C_0, C_1, \dots, C_{m-1}\}$.

Poznámka.
Někdy bude technicky výhodnější přeformulovat definici zbytkové třídy C_i do ekvivalentního tvaru:

$$C_i = \{ x \in \mathbb{Z} \mid x \equiv i \pmod{m} \}, \qquad \text{pro } i = 0, 1, \dots, m-1.$$

Ekvivalentnost vyjádření okamžitě plyne z věty , uvědomíme-li si zřejmý fakt, že číslo i, kde $0 \le i \le m-1$, dává po dělení číslem m zbytek i.

Z věty o dělení se zbytkem celých čísel plyne, že zbytkových tříd podle modulu m musí být opravdu právě m (neboť zbytek po dělení každého celého čísla číslem m musí podle této věty nabývat právě jedné z hodnot $0, 1, \dots, m-1$). Dále, každá zbytková třída podle modulu m obsahuje zřejmě nekonečně mnoho celých čísel, lišících se o nějaký celočíselný násobek modulu m. Pokusíme-li se schematicky zapsat jednotlivé zbytkové třídy podle modulu m, dostaneme:

$$\begin{array}{lcl}
C_0 & = & \{ \dots, \; -2m, \; -m, \; 0, \; m, \; 2m, \; \dots \} \\
C_1 & = & \{ \dots, \; -2m+1, \; -m+1, \; 1, \; m+1, \; 2m+1, \; \dots \} \\
C_2 & = & \{ \dots, \; -2m+2, \; -m+2, \; 2, \; m+2, \; 2m+2, \; \dots \} \\
\vdots & & \\
C_{m-1} & = & \{ \dots, \; -m-1, \; -1, \; m-1, \; 2m-1, \; 3m-1, \; \dots \}
\end{array}$$

Věta

Nechť m je pevné přirozené číslo. Pak množina $\mathbb{Z}_m$ všech zbytkových tříd podle modulu m tvoří rozklad na množině $\mathbb{Z}$ všech celých čísel.

Důkaz.
Uvažme množinu zbytkových tříd $\mathbb{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}$.
dokážeme, že $\mathbb{Z}_m$ je rozklad na $\mathbb{Z}$.

1. každá ze zbytkových tříd C_i je zřejmě neprázdnou podmnožinou v $\mathbb{Z}$.
2. nechť $C_i, C_j \in \mathbb{Z}$ a $C_i \cap C_j \neq \emptyset$. Potom existuje číslo $x \in C_i \cap C_j$, což znamená, že x dává po dělení číslem m zbytek i a současně také zbytek j. Ale z věty o dělení celých čísel se zbytkem víme, že zbytek po dělení je určen jednoznačně, tzn. $i = j$, odkud dostáváme, že $C_i = C_j$.
3. zřejmě platí, že sjednocení $C_0 \cup C_1 \cup \cdots \cup C_{m-1} = \mathbb{Z}$.

Užití kongruencí na příkladech

① Dokažte, že mezi 82 libovolně zvolenými přirozenými čísly existují dvě, jejichž rozdíl je dělitelný číslem 81.

Ř: $Z_{81} = \{C_0, \ldots, C_{80}\}$, tzn. existuje 81 zbytkových tříd podle modulu 81. Čísel je ale 82, tj. alespoň dvě musí ležet ve stejné zbytkové třídě. Pak je jejich rozdíl dělitelný 81.

) Dokažte, že každé prvočíslo větší než tři lze zapsat ve tvaru $6k+1$ nebo $6k+5$.

Ř: Platí: $\mathbb{Z}_6 = \{C_0, \ldots, C_5\}$. Prvočíslo $p > 3$ je celé číslo, musí tedy ležet v některé třídě Z_6. Postupně je probereme:

C_0: $p = 6k$ není prvočíslo

C_1: $p = 6k+1$

C_2: $p = 6k+2 = 2(3k+1)$ složené č.

C_3: $p = 6k+3 = 3(2k+1)$ složené

C_4: $p = 6k+4 = 2(3k+2)$ složené

C_5: $p = 6k+5$

Vyloučením C_0, C_2, C_3, C_4 plyne, že $p \in C_1$ nebo $p \in C_5$.

) Nalezněte poslední dvě číslice čísla 3^{1234}.

Ř: Řešíme $3^{1234} \equiv x \pmod{100}$

Všechny kongruence dále platí mod 100.

Užijeme Eulerovu větu. Platí $\varphi(100) = 40$, protože

$100 = 2^2 \cdot 5^2$, tedy $\varphi(100) = 100 \cdot (1-\frac{1}{2}) \cdot (1-\frac{1}{5}) = 40$;

platí $3^{40} \equiv 1 \pmod{100}$; umocníme na exponent 30:

(*) $\quad 3^{1200} \equiv 1 \pmod{100}$.

Nyní $3^2 \equiv 9 \pmod{100}$, $3^4 \equiv 81 \pmod{100}$, $3^8 \equiv 81^2 \equiv 61$ (mod 1

pak $3^{32} \equiv 61^4 \equiv 41 \pmod{100}$;

nyní kongruence $3^2 \equiv 9 \pmod{100}$ a $3^{32} \equiv 41 \pmod{100}$

vynásobíme: (**) $\quad 3^{34} \equiv 369 \pmod{100}$,

tedy $3^{34} \equiv 69 \pmod{100}$;

kongruence (*), (**) vynásobíme: $3^{1234} \equiv 69 \pmod{100}$

tedy číslo 3^{1234} končí na 69.

---

④ Dokažte, že $13 \mid (2^{60} + 7^{30})$

Ř: Eulerova věta: $2^{12} \equiv 1 \pmod{13}$ $\Big|^5$ $\qquad \varphi(13) = 12$

(*) $\quad 2^{60} \equiv 1 \pmod{13}$

Eulerova věta: $7^{12} \equiv 1 \pmod{13}$ $\Big|^2$

$\boxed{7^{24} \equiv 1 \pmod{13}}$;

dále $7^3 \equiv 5 \pmod{13}$, $7^6 \equiv 25 \pmod{13}$, tj. $\boxed{7^6 \equiv -1}$ (mod

kongruence v rámečcích vynásobíme: $7^{30} \equiv -1 \pmod{13}$ (

Obě kongruence (*), (**) sečteme: $2^{60} + 7^{30} \equiv 0 \pmod{13}$

tedy $13 \mid (2^{60} + 7^{30})$.

---

⑤ Dokažte, že platí: $\forall n \in \mathbb{N}: \; 7 \mid (37^{n+2} + 16^{n+1} + 23^n)$

Ř: $37 \equiv 2 \pmod 7$	$16 \equiv 2 \pmod 7$	$23 \equiv 2 \pmod 7$
$37^{n+2} \equiv 2^{n+2} \pmod 7$	$16^{n+1} \equiv 2^{n+1} \pmod 7$	$23^n \equiv 2^n \pmod 7$

…ongruence ve spodním řádku sečteme:

$$37^{n+2} + 16^{n+1} + 23^{n} \equiv 2^{n+2} + 2^{n+1} + 2^{n} \pmod{7},$$

ale $2^{n+2} + 2^{n+1} + 2^{n} = 7 \cdot 2^{n}$, tedy $2^{n+2} + 2^{n+1} + 2^{n} \equiv 0 \pmod{7}$

Relace kongruence je tranzitivní, tedy také

$$37^{n+2} + 16^{n+1} + 23^{n} \equiv 0 \pmod{7}.$$

) Dokažte, že některý násobek čísla 21 končí na 241.

Ř:

$$\begin{aligned} 21n &\equiv 241 \pmod{1000} && \mid +2000 \text{ na pravou stranu} \\ 21n &\equiv 2241 \pmod{1000} && \mid :3 \\ 7n &\equiv 747 \pmod{1000} && \mid +5000 \text{ na pravou stranu} \\ 7n &\equiv 5747 \pmod{1000} && \mid :7 \\ n &\equiv 821 \pmod{1000} \end{aligned}$$

Tedy $n = 1000k + 821$.

Zk:

$$\begin{array}{r} 4821 \\ \cdot\, 21 \\ \hline 4821 \\ 9642 \\ \hline 101241 \end{array} \qquad \begin{array}{r} 29821 \\ \cdot\, 21 \\ \hline 29821 \\ 59642 \\ \hline 626241 \end{array} \qquad \text{atd.}$$

(1)

$$2^{64} \equiv x \pmod{10}$$

$$2^{8} \equiv 6 \pmod{10} \quad \Big|^{8}$$

$$2^{64} \equiv 6^{8} \pmod{10}$$

$$6^{2} \equiv 6 \pmod{10} \quad \Big|^{4}$$

$$6^{8} \equiv 6^{4} \pmod{10}$$

$$6^{4} = 36 \cdot 36 = 1296$$

$$6^{4} \equiv 6 \pmod{10}$$

$$\begin{array}{r} 36 \\ 36 \\ \hline 216 \\ 108 \\ \hline 1296 \end{array}$$

$$6^{4} \equiv 6, \quad 6^{8} \equiv 6, \quad 2^{64} \equiv 6^{8} \Rightarrow 2^{64} \equiv 6$$

$$\underline{2^{64} \equiv 6 \pmod{10}}$$

$$3^{64} \equiv x \pmod{10}$$

$$3^{2} \equiv -1 \pmod{10}$$

$$3^{4} \equiv 1 \pmod{10} \,\big)^{16}$$

$$\underline{3^{64} \equiv 1 \pmod{10}}$$

%