BRněnský KOrespondenční Seminář

XXXII. ročník
2025/2026

Pomocný text ke 4. sérii

TEORIE ČÍSEL

autor: *Tonda*

1 Úvod

Fermat, Lagrange, Gauss a Euler,
koupili si novej bojler.
Doma jim však vybouchl,
všechny pěkně ošplouchl.
Popálil jim půlku třísel,
a tak začli dělat
TEORII ČÍSEL

Teorie čísel se zabývá čísly, to asi dává smysl. Konkrétněji jde většinou o nějaké algebraické vlastnosti celých čísel. V tomto textu si ukážeme pár tvrzení o celých číslech, která možná většina z vás zná, text je tedy určen spíše začátečníkům. Vždy, když v tomto textu čtete slovo číslo, je tím myšleno celé číslo.

2 Dělitelnost

S dělením se každý setkal už na základce. A už tehdy jsme si asi povšimli základního konceptu teorie čísel - dělitelnosti. Někdy to prostě jde vydělit hezky, někdy ne a něco nám zbyde.

Později jsme se dozvěděli o kritériech dělitelnosti, např. „číslo je dělitelné devíti, právě tehdy, když jeho ciferný součet je dělitelný devíti“.

Ukážeme si, že všechna tato kritéria platí mnohem silněji.

Definice: Řekneme, že číslo a je dělitelné číslem b, jestliže existuje číslo c takové, že $c \cdot b = a$. Píšeme $b|a$.

To asi není nic nového, pojďme dál.

Definice: Řekneme, že číslo a je kongruentní s číslem b modulo n (píšeme $a \equiv b \ (mod\ n)$), jestliže $n|(a-b)$.

Intuitivně to znamená, že a a b dávají stejný zbytek po dělení číslem n. Například tedy $3 \equiv 8 \ (mod\ 5)$, $11 \equiv -1 \ (mod\ 3)$,....

Ultra jednoduše se ověří, že relace $\equiv$ je ekvivalence. Třídám ekvivalence říkáme zbytkové třídy.

Příklad 1: Určete všechna celočíselná řešení rovnice $6x + 1 = 3y + 2$.
Stačí se na tuhle rovnici podívat modulo 3, na levé straně dostaneme 1, neboť $3|6x$, na

pravé straně dostáváme 2, neboť $3|3y$. Celkem tedy

$$1 \equiv 2 \ (mod\ 3),$$

což je blbost a rovnice nemá řešení.

Věta 1 (Kritérium dělitelnosti 9)**:** Nechť $CS(n)$ značí ciferný součet čísla n. Potom $CS(n) \equiv n \ (mod\ 9)$.

Důkaz: Zapišme číslo n v desítkovém zápisu jako

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \cdots + a_n \cdot 10^n.$$

Podívejme se na celou rovnici modulo 9. Jelikož číslo 10 dává zbytek 1, $10^m \equiv 1^m = 1$. Proto $n \equiv a_0 + a_1 + a_2 + \cdots + a_n = CS(n) \ (mod\ 9)$.

Tedy kritérium dělitelnosti devíti neříká pouze, že číslo je dělitelné právě když ciferný součet je. Číslo a jeho ciferný součet dávají dokonce stejný zbytek po dělení 9.

Můžete si to stejným způsobem vyzkoušet pro další kritéria, která znáte.

Také jste se ve škole učili, jak hledat největší společný dělitel a nejmenší společný násobek. Jedna možnost je hledání pomocí rozkladu na prvočísla, což je sice super, ale obecně nezvládneme číslo rozložit na prvočísla. Další způsob je takzvaný Eukleidův algoritmus. Eukleidův algoritmus je založen na dělení se zbytkem. Mějme dvě celá čísla $a, b \in \mathbb{Z}$. Cílem je nalézt jejich největší společný dělitel $\gcd(a, b)$ pomocí eukleidovského dělení se zbytkem.

Příklad 2: Najdi největší společný dělitel čísel $gcd(252, 105)$ Postupujeme iterací algoritmu $r_{i-1} = q_i \cdot r_i + r_{i+1}$, kde $r_0 = a$ a $r_1 = b$:

$$\begin{aligned} 252 &= 2 \cdot 105 + 42 && \text{dělení se zbytkem: } r_2 = 42 \\ 105 &= 2 \cdot 42 + 21 && \text{dělení se zbytkem: } r_3 = 21 \\ 42 &= 2 \cdot 21 + 0 && \text{dělení se zbytkem: } r_4 = 0 \end{aligned}$$

Závěr: Protože $r_4 = 0$, největším společným dělitelem je poslední nenulový zbytek $r_3 = 21$.

$$\gcd(252, 105) = 21$$

Bezoutova rovnost (Zpětný chod)

Pomocí Eukleidova algoritmu jsme navíc schopni vyjádřit největší společný dělitel dvou čísel jako lineární kombinaci těchto čísel. Tedy najít čísla k a l taková, že $k \cdot a + l \cdot b = gcd(a, b)$.

$$\begin{aligned} 21 &= 105 - 2 \cdot 42 \\ 21 &= 105 - 2 \cdot (252 - 2 \cdot 105) \\ 21 &= 5 \cdot 105 - 2 \cdot 252 \end{aligned}$$

Prvky 5 a -2 jsou hledané Bezoutovy koeficienty.

Přesuňme se k dalším cool věcem, které uvedu bez důkazu.

Věta 2 (Malá Fermatova věta)**:** Nechť p je prvočíslo a a libovolné číslo. Potom $a^p \equiv a \ (mod\ p)$

Důsledek: Nechť p je prvočíslo a a je nesoudělné s p. Potom $a^{p-1} \equiv 1 \ (mod\ p)$.

Příklad 3: Určete, jaký zbytek dává číslo 4^{957} po dělení 5.
Zřejmě je prvočíslo 5 nesoudělné s číslem 4. Proto podle důsledku Malé Fermatovy věty platí:

$$4^4 \equiv 1 \ (mod\ 5).$$

Umocněním celé rovnice na 239 dostaneme

$$4^{956} \equiv 1 \ (mod\ 5).$$

No, a víme, že

$$4^{957} \equiv 4^{956} \cdot 4 \equiv 1 \cdot 4 \equiv 4.$$

Pokračujme na zobecnění této věty:

Definice: Eulerova funkce z přirozeného čísla n (psáno $\varphi(n)$) udává počet přirozených čísel menších nebo rovných n, která jsou s n nesoudělná.

Příklad 4: Spočtěme $\varphi(6)$. S šestkou je nesoudělná pouze jednička a pětka, proto $\varphi(6) = 2$.

Takovýhle postup by byl asi docela neefektivní pro velká čísla. Ukažme si tedy vzorec, jak efektivně vypočítat Eulerovu funkci z čísla, které zvládneme rozložit na součin prvočísel.

Věta 3: Pro nesoudělná čísla a, b platí, že $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Věta 4: Pro číslo tvaru p^n, kde p je prvočíslo platí, že $\varphi(p^n) = (p-1)p^{n-1}$.

V praxi tedy rozložíme číslo na prvočísla a určujeme Eulerovu funkci podle vzorce.

Příklad 5: Vypočítej $\varphi(135)$.
$135 = 3^3 \cdot 5$, tedy podle vzorců:

$$\varphi(135) = \varphi(3^3) \cdot \varphi(5) = 2 \cdot 3^2 \cdot 4 = 72.$$

Věta 5 (Eulerova věta)**:** Nechť a je nesoudělné s číslem n. Potom

$$a^{\varphi(n)} \equiv 1 \ (mod\ n).$$

BRKOS Team

Příklad 6: Určete poslední cifru čísla 7^{115}.
Poslední cifra je vlastně zbytek po dělení 10, zajímá nás tedy 7^{115} $(mod\ 10)$. $\varphi(10) = 4$. Proto podle Eulerovy věty $7^4 \equiv 1$. Umocněním na 28 dostáváme $7^{112} \equiv 1$. Zároveň ale

$$7^{115} \equiv 7^{112} \cdot 7^3 \equiv 7^3 = 343 \equiv 3.$$