Teorie čísel

Lenka Slavíková

Abstrakt. Seznámíme se se základními pojmy a větami z teorie čísel a ukážeme si, jak těchto znalostí využít při řešení konkrétních příkladů.

Teorie čísel je odvětví matematiky, které se zabývá vztahy mezi celými čísly. Seznámíme se s některými základními pojmy a větami a ukážeme si, jak lze těchto znalostí využít při řešení konkrétních příkladů.

V následujícím textu bude $\mathbb{N}$ značit množinu přirozených čísel, tj. $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$, a $\mathbb{Z}$ množinu celých čísel.

Nejprv tedy trocha teorie ...

Dělitelnost, prvočísla a složená čísla

Definice. *Nechť a, b jsou celá čísla. Řekneme, že a* dělí *b (b je* násobkem *a), pokud existuje celé číslo q takové, že $b = aq$. Tuto skutečnost budeme značit $a \mid b$.*

Největším společným dělitelem *čísel a, b budeme rozumět největší přirozené číslo, které současně dělí a i b. Značíme (a, b). Čísla a, b nazveme* nesoudělná, *pokud $(a, b) = 1$. Přirozené číslo nazveme* prvočíslem *pokud má právě dva kladné dělitele.* Složená čísla *jsou přirozená čísla, která mají alespoň tři kladné dělitele.*

Věta. *Existuje nekonečně mnoho prvočísel.*

Věta. *Pro každé přirozené číslo n existuje n po sobě jdoucích složených čísel.*

Věta. (Bezoutova) *Nechť $a, b \in \mathbb{Z}$, $d = (a, b)$. Potom existují celá čísla x, y taková, že $ax + by = d$.*

Kongruence

Definice. *Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Řekneme, že a* je kongruentní s *b* modulo *m, píšeme $a \equiv b \pmod m$, pokud $m \mid (a - b)$.*

Jinak řečeno, čísla a, b jsou kongruentní modulo m, pokud dávají při dělení číslem m stejný zbytek.

Věta. (vlastnosti kongruencí) *Nechť $a, b, c, d \in Z$, $m \in \mathbb{N}$.*

(a) Pokud $a \equiv b \pmod m$, $c \equiv d \pmod m$, pak platí $a + c \equiv b + d \pmod m$, $ac \equiv bd \pmod m$.

(b) Pokud $ac \equiv bc \pmod m$ a $(c, m) = 1$, pak $a \equiv b \pmod m$.

Klíčová slova. teorie čísel, dělitelnost, kongruence

Tedy kongruence mezi sebou můžeme sčítat a násobit. Navíc můžeme dělit čísly nesoudělnými s modulem.

Definice. *Nechť $n \in \mathbb{N}$. Počet všech přirozených čísel, která jsou menší než n a nesoudělná s n, značíme $\varphi(n)$. Funkci, která přirozenému číslu přiřadí číslo $\varphi(n)$, říkáme* Eulerova funkce.

Věta. *Nechť $n > 1$ je přirozené číslo. Je-li $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ rozklad čísla n na součin prvočísel (tj. $p_1, p_2, \ldots, p_k$ jsou po dvou různá prvočísla, $r_1, r_2, \ldots, r_k$ jsou přirozená čísla), pak platí*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Věta. (Eulerova) *Nechť $a \in \mathbb{Z}, m \in \mathbb{N}$ a platí $(a, m) = 1$. Pak $a^{\varphi(m)} \equiv 1$ (mod m).*

Věta. (malá Fermatova) *Nechť a je přirozené číslo, p je prvočíslo a platí $(a, p) = 1$. Pak $a^{p-1} \equiv 1$ (mod p).*

Všimni si, že malou Fermatovu větu dostaneme jako důsledek Eulerovy věty, pokud zvolíme $m = p$.

Věta. (Wilsonova) *Nechť p je prvočíslo. Pak $(p-1)! \equiv -1$ (mod p).*

A teď už konečně nějaké příklady ...

Příklad 1. Nechť $a, b, c, d \in \mathbb{N}$. Dokažte, že pokud $a-c \mid ab+cd$, pak $a-c \mid ad+bc$.

Příklad 2. Nechť $a, b \in \mathbb{N}$. Dokažte, že pokud $3 \mid a^2 + b^2$, pak $3 \mid a$ a $3 \mid b$.

Příklad 3. Dokažte, že neexistuje polynom P s celočíselnými koeficienty takový, že platí $P(2009) = 2010, P(2011) = 2013$.

Příklad 4. Nechť $p > 3$ je prvočíslo. Dokažte, že $6(p-4)! \equiv 1 \pmod{p}$.

Příklad 5. Dokažte, že existuje nekonečně mnoho přirozených čísel n takových, že $\frac{5^{n-2}-1}{n}$ je celé číslo.

Příklad 6. Nechť a, b jsou lichá nesoudělná čísla. Dokažte, že $(2^a+1, 2^b+1) = 3$.

Příklad 7. Nechť $a, b, c, d \in \mathbb{N}$ a platí $ab = cd$. Dokažte, že pak $a^2 + b^2 + c^2 + d^2$ není prvočíslo.

... a úplně na závěr pár diofantických rovnic. Pokud ses ještě s tímto strašidelným pojmem nesetkal, tak věz, že nejde o nic jiného než o rovnice, u nichž nás zajímají jen celočíselná řešení.

Příklad 8. Najděte všechny dvojice prvočísel (p, q) takové, že platí $p^2 - 2q^2 = 1$.

Příklad 9. Dokažte, že dvojice $(x, y) = (0, 0)$ je jediným řešením rovnice $x^2 + y^2 = x^2y^2$ v celých číslech.

Příklad 10. Dokažte, že rovnice $x(x+1)(x+2)(x+3) = y^2$ nemá řešení v přirozených číslech.

Příklad 11. Nechť $m, n \in \mathbb{N}$, $(m, n) = 1$. Dokažte, že rovnice $x^m + y^m = z^n$ má nekonečně mnoho řešení v celých číslech.

Příklad 12. Předpokládejme, že p je liché prvočíslo takové, že $2p + 1$ je rovněž prvočíslo. Dokažte, že rovnice $x^p + 2y^p + 5z^p = 0$ má v celých číslech jediné řešení, a to trojici $(x, y, z) = (0, 0, 0)$.