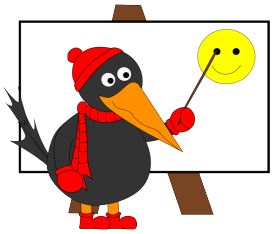
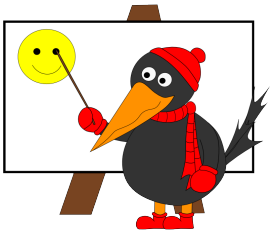


Pomocný text

Teorie čísel



V tomto textu se budeme zabývat řešením rovnic v oboru čísel celých (značíme $\mathbb{Z}$) a přirozených (značíme $\mathbb{N}$). Protože ne všichni matematici mají na nulu stejný názor, vězte, že v BRKOSu $0 \notin \mathbb{N}$.

Téměř všechny úlohy z teorie čísel, s nimiž se setkáte v korespondenčních seminářích a olympiádách, se dají řešit jedním ze dvou triků:

1. Vybereme vhodný modul a zjistíme, jaké zbytky musí dávat čísla a výrazy po dělení tímto modulem.

2. Rozložíme nějaký výraz na součin a využijeme jednoznačnosti rozkladu celých čísel na prvočísla.

Pro vyřešení naší třetí série by vám mohl stačit trik č. 2, ale my vám zkusíme poradit, jak používat oba.

Zbytkové třídy

Zbytková třída vzhledem k nějakému číslu m (tzv. modulu), je množina čísel, které dávají po dělení číslem m stejný zbytek. Když dvě čísla a, b patří do stejné zbytkové třídy, řekneme o nich, že jsou „kongruentní modulo m“, a zapisujeme

$$a \equiv b \pmod{m}.$$

Pokud máme dvě kongruence

$$\begin{aligned} a &\equiv b \pmod{m}, \\ c &\equiv d \pmod{m}, \end{aligned}$$

můžeme je sčítat, násobit a umocňovat:

$$\begin{aligned} a + c &\equiv b + d \pmod{m}, \\ ac &\equiv bd \pmod{m}, \\ a^n &\equiv b^n \pmod{m} \quad pro \ \ \forall n \in \mathbb{N}. \end{aligned}$$

Toto nám značně usnadní zápisy tam, kde se nějak pracuje se zbytky nebo dělitelností. Příkladem využití je například odvození pravidla dělitelnosti devíti:

Víme, že $10 \equiv 1 \pmod 9$, pak také platí $10^n \equiv 1^n \pmod 9$. Protože $1^n = 1$, můžeme psát

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0 \equiv a_n \cdot 1 + a_{n-1} \cdot 1 + \cdots + a_0 \pmod 9.$$

Zajímavějším využitím jsou tzv. kvadratické zbytky. Víme třeba, že pro všechna $a \in \mathbb{Z}$ platí buď $a^2 \equiv 0 \pmod 4$ (pro a sudá), nebo $a^2 \equiv 1 \pmod 4$ (pro a lichá). Když nás pak někdo nechá hledat všechna $c, d \in \mathbb{Z}$, pro která $c^2 + d^2 = 555$, můžeme toto uvážit $\pmod 4$ a hned vidíme, že kongruence $c^2 + d^2 \equiv 3 \pmod 4$ nemá řešení, protože oba sčítance na levé straně jsou 1 nebo 0.

Rozklad na součin

Při řešení rovnic v celých číslech pomůže, když se nám podaří dostat na jedné straně rovnice součin nějakých výrazů a na druhé straně buď číslo, nebo třeba druhou mocninu výrazu. Většinou je potřeba něco přičíst, něčím vynásobit, těžko dávat univerzální návod. Hodí se ale mít na paměti pár vzorců na rozklady jako

$$a^3 - b^3 = (a - b)(a^2 + ab + b^2)$$

nebo méně známý

$$a^4 + 4b^4 = (a^2 - 2ab + 2b^2)(a^2 + 2ab + 2b^2).$$

Jak se dají rozklady využít, ukážeme na následujících dvou příkladech.

Úloha 3.1. *Zjistěte, pro která přirozená čísla x, y je výraz $\frac{2}{x} + \frac{2}{y}$ celé číslo.*

Řešení. Hodnotu výrazu označíme k, tedy $\frac{2}{x} + \frac{2}{y} = k$. Vynásobíme rovnici xy a dostáváme

$$\begin{aligned} 2x + 2y &= kxy \\ kxy - 2x - 2y &= 0 \\ k^2xy - 2kx - 2ky &= 0 \\ k^2xy - 2kx - 2ky + 4 &= 4 \\ (kx - 2)(ky - 2) &= 4. \end{aligned}$$

Protože rozklad čísla 4 na prvočísla je jednoznačný, máme $(kx-2) \in \{-1, -2, -4, 1, 2, 4\}$, $kx \in \{1, 0, -2, 3, 4, 6\}$, $x \in \{1, 2, 3, 4, 6\}$. Číslo y ke každému x snadno dopočteme: $(x, y) \in \{(1, 1), (2, 1), (1, 2), (2, 2), (4, 4), (3, 6), (6, 3)\}$.

Úloha 3.2. *Najděte všechny nesoudělné trojice celých čísel a, b, c splňující rovnost*

$$a^2 + b^2 = c^2.$$

Řešení. Kdyby byla obě čísla a, b lichá, dávala by zadaná rovnice $2 \equiv c^2 \pmod 4$, což nelze. Navíc čísla a, b nemohou být současně sudá (kvůli nesoudělnosti), proto je jedno z nich sudé a jedno liché. Řekněme, že liché je a a pro b platí $b = 2t$. Pak ze zadané rovnosti

$$\begin{aligned} 4t^2 &= b^2 = c^2 - a^2 = (c-a)(c+a), \\ t^2 &= \frac{c-a}{2} \cdot \frac{c+a}{2}. \end{aligned}$$

Zlomky $\frac{c+a}{2}$ i $\frac{c-a}{2}$ v rovnosti jsou celá čísla, protože a i c jsou lichá. Kdyby nějaké prvočíslo p dělilo $\frac{c+a}{2}$ i $\frac{c-a}{2}$, dělilo by i jejich součet a jejich rozdíl, tedy c i a, což je ale spor se zadanou nesoudělností. Čísla $\frac{c-a}{2}$ a $\frac{c+a}{2}$ jsou proto nesoudělná.

Nyní přijde jedna z častých aplikací jednoznačnosti rozkladu na součin prvočísel: na levé straně rovnosti je b^2, tedy číslo, které má u všech prvočísel ve svém rozkladu sudý exponent. Stejnou vlastnost musí mít i rozklad pravé strany. Protože ale rozklady závorek $\frac{c-a}{2}$ a $\frac{c+a}{2}$ obsahují každý jiná prvočísla, musí mít každá z těchto závorek u všech prvočísel sudé exponenty a být proto čtvercem. Existují tedy celá čísla u, v taková, že

$$\begin{aligned} \frac{c-a}{2} &= u^2, \\ \frac{c+a}{2} &= v^2. \end{aligned}$$

Z rovnosti $t^2 = \frac{c-a}{2} \cdot \frac{c+a}{2}$ a předchozích vztahů pak plyne

$$\begin{aligned} t &= uv, \\ b &= 2uv, \\ a &= v^2 - u^2, \\ c &= u^2 + v^2. \end{aligned}$$

Za u, v je třeba dosadit nesoudělná čísla, z nichž právě jedno je sudé (aby byla dodržena nesoudělnost a, b a c). Tím pokryjeme všechny trojice odpovídající zadání, v nichž b je sudé. Ostatní trojice pokryjeme tak, že prohodíme vzorce pro a a b.

Nyní se nám podařilo pomocí parametrů u, v popsat všechny trojice vyhovující zadání.