Využití dělitelnosti v praxi

Pavel Paták

Úvod

Dělitelnost a modulární aritmetika jsou téma, která pro svou jednoduchost našla řadu uplatnění, výborně se například hodí při řešení diofantovských rovnic či šifrování dat na internetu.

Definice a základní vlastnosti dělitelnosti

Definice. *Pokud a beze zbytku dělí b (tedy $\exists k \in Z$, že $k = \frac{b}{a}$), píšeme $a|b$ (číslo a je* dělitelem *čísla b, a je* násobkem *b).*

Definice. *Pokud polynom P dělí polynom R beze zbytku (tedy existuje polynom Q takový, že $R = PQ$), užíváme stejné označení tj. $P|R$.*

Pro celá čísla zjevně platí:

(i) $a|b \Rightarrow (-a)|b$
(ii) $a|b \Rightarrow |a| \leq |b|$
(iii) $a|b \wedge b|a \Rightarrow |a| = |b|$
(iv) $a|b \wedge a|c \Rightarrow a|(rb \pm sc)$
(v) $a|b \wedge c|d \Rightarrow ac|bd$

Definice.

(1) Největším společným dělitelem *čísel a, b rozumíme největší přirozené číslo k, které současně dělí a i b. Označení* $\mathrm{D}(a,b)$, $\mathrm{qcd}(a,b)$, $\mathrm{nsd}(a,b)$.
(2) Nejmenším společným násobkem *rozumíme nejmenší takové přirozené číslo k, které je současně násobkem a i b. Označení* $\mathrm{n}(a,b)$, $\mathrm{lcm}(a,b)$, $\mathrm{nsn}(a,b)$
(3) *Čísla a, b jsou* nesoudělná, *pokud* $\mathrm{D}(a,b) = 1$

Euklidův algoritmus pro zjištění největšího společného dělitele

Tento algoritmus je založen na faktu, že pokud je t dělitelem a i b, pak t dělí i $a - rb$. Tedy čísla a, b můžeme snižovat, aniž bychom změnili největšího společného dělitele. Po konečném počtu kroků skončíme ve stavu $\mathrm{D}(a,0) = a$.

Věta. (Bézout) *Čísla a, b jsou nesoudělná, právě když $\forall k \in Z$ je rovnice $ra + sb = k$ řešitelná v celých číslech.*

Tvrzení. Rovnice $ra + sb = t$ má celočíselné řešení právě tehdy, když $\mathrm{D}(a, b)$ dělí t.

Věta. (Jednoznačný rozklad) *Každé přirozené číslo lze (až na pořadí) jednoznačně rozložit na součin prvočísel.*

Kongruence

Definice. *Nejjednodušším příkladem kongruence je tzv.* parita – *rozdělení čísel na lichá a sudá. Je zcela přirozené tento pojem zevšeobecnit: Pokud mají čísla a, b stejný zbytek po dělení m, říkáme, že a je* kongruentní s b modulo m. *Píšeme $a \equiv b (mod\ m)$.*

Pro praktické počítání nám tedy stačí zvolit vhodného zástupce (obvykle menšího než m). Kongruence našly velké uplatnění především proto, že je lze sčítat a násobit zcela normálně jako obyčejná čísla.

Příklad 1. Určete:

(i) paritu čísla $N = 22 \cdot 31 + 11 \cdot 17 + 13 \cdot 19$
(ii) poslední číslici N
(iii) zbytek po dělení čísla N sedmi.

Příklad 2. Určete poslední číslici $3^{815} + 2^{701}$.

Tvrzení. $\binom{a}{b} \equiv 0 \pmod{p}$ pro p prvočíslo.

Věta. (Malá Fermatova věta) $a^p \equiv a \pmod{p}$ *pro p prvočíslo.*

Tvrzení. $m \equiv 1 \pmod{p-1} \Rightarrow a^m \equiv a \pmod{p}$, pro p prvočíslo.

Poznámka. Uvědomme si, že s pomocí kongruencí lze velice jednoduše stanovit tzv. kritéria dělitelnosti: V soustavě o základu z stačí jen vypočítat $a_0 + a_1 z + + a_2 z^2 + \cdots + a_n z^n \pmod{k}$. (Tímto postupem navíc zjistíme, jaký zbytek po dělení dané číslo má.)

Například dělitelnost jedenácti v desítkové soustavě zjistíme takto: $a_0 + a_1 \cdot 10 + + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n \equiv a_0 + a_1 \cdot (-1) + a_2 \cdot (-1)^2 + \cdots + a_n \cdot (-1)^n \pmod{11}$. Ke zjištění dělitelnosti jedenácti tedy stačí zjistit rozdíl součtu číslic na lichém a sudém místě.

Příklad 3. Určete kritérium dělitelnosti třinácti v desítkové soustavě.

Příklad 4. V osmičkové soustavě má 17! desítkový zápis $1206773ab63300cd0$. Určete číslice a,b,c,d.

Definice. Eulerova funkce $\varphi(n)$ = *počet přirozených čísel menších než n s n nesoudělných.*

Příklad 5. Najděte vzorec pro výpočet $\varphi(n)$.

Asymetrické šifry

Symetrické šifry využívají k zakódování i dekódování stejný klíč, to je však například pro potřeby internetu poněkud nepraktické. Pokud můžeme bezpečně doručit klíč, proč tímto způsobem nepředat celou zprávu?

Zajímavější jsou šifry asymetrické, využívající veřejného klíče, pomocí něhož se zpráva kóduje, a klíče soukromého, který se používá pro dešifrování. Oba klíče musí být matematicky provázány, avšak mělo by být prakticky nemožné z klíče veřejného vypočítat klíč soukromý. V praxi se používá některých těžko obratitelných matematických operací, např. násobení velice dlouhých prvočísel, diskrétních logaritmů a podobně.

Nejznámější asymetrická šifra RSA využívá prvního z uvedených principů.

Algoritmus m je nezakódovaná zpráva, c zpráva zakódovaná.

(1) Zvolíme dvě obrovská prvočísla p a q.
(2) Spočteme $n = pq$.
(3) Vypočteme $\varphi(n) = (p-1)(q-1)$.
(4) Zvolíme e nesoudělné s $\varphi(n)$ (obvykle se užívá 65537).
(5) Najdeme d, aby $ed \equiv 1 \pmod{\varphi(n)}$.
(6) Veřejný klíč je (e, n), soukromý (d, n).
(7) Odesílatel zprávu zakóduje $c = m^e \pmod{n}$.
(8) Zprávu dekódujeme $m = c^d \pmod{n}$.

Příklady

Příklad 6. Vyzkoušejte uvedený postup na směšně malých hodnotách: $p = 3, q = 5, e = 3, m = 3$.

Příklad 7. Buď n přirozené číslo, dokažte, že rovnice $x^2 - y^2 = a^3$ má vždy celočíselné řešení.

Příklad 8. Najděte všechna přirozená čísla, která nejdou vyjádřit jako $\frac{a}{b} + \frac{a+1}{b+1}$.

Příklad 9. Jaké je největší přirozené číslo N s tou vlastností, že $n^5 - 5n^3 - 4n$ je dělitelné N pro každé n?

Příklad 10. Dokažte, nebo vyvraťte: $2^{70} + 3^{70}$ je dělitelné 13.