PRVOČÍSLA

Definícia. Celé číslo $p > 1$ sa nazýva prvočíslo, ak je deliteľné **len** číslami $1, -1, p$ a $-p$.

Ekvivalentne, $p > 1$ je prvočíslo, ak nie je súčinom dvoch menších kladných čísel. Ak $p > 1$ nie je prvočíslo, tak p sa nazýva *zložené*.

Lema 1. *Nech* $p, a_1, \ldots, a_n \in \mathbb{Z}$.

(i) Ak $p|a_1a_2$ *a* $(p, a_1) = 1$, *tak* $p|a_2$;

(ii) Ak $p|a_1a_2 \ldots a_n$ *a* p *je prvočíslo, tak* $p|a_k$ *pre niektoré* k.

Nasledujúce tvrdenie o rozklade sa tiež nazýva *Hlavná veta aritmetiky.*

Veta 2. *Každé celé číslo* $n > 1$ *sa dá rozložiť na súčin prvočísel, a to jednoznačne až na poradie činiteľov.*

Poznámka. Dôkaz Základnej vety aritmetiky má existenčný charakter

a nedáva návod ako rozložiť dané celé číslo (iný než vyskúšanie všetkých možností). Pre malé čísla to nie je problém. Pre veľké čísla však nie sú známe žiadne efektívne metódy rozkladu (faktorizácie). Na tomto fakte sa zakladajú viaceré šifrovacie algoritmy.

Na rozklad malých čísel používame známe kritériá deliteľnosti a tiež nasledujúce jednoduché tvrdenie.

Lema 3. *Každé zložené n má deliteľa $1 < k \leq \sqrt{n}$*

Veta 4. *Existuje nekonečne veľa prvočísel*

Znalosť prvočíselného rozkladu možno využiť pri hľadaní NSD a NSN. Konkrétne, nech čísla a a b majú rozklady

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n},$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n},$$

kde $p_1, \dots, p_n$ sú rôzne prvočísla. (Pripúšťame, že niektoré exponenty α_i a β_j môžu byť 0, čo by znamenalo, že príslušné prvočíslo sa v rozklade

nenachádza.) Potom NSD čísel a, b má rozklad

$$p_1^{\min\{\alpha_1,\beta_1\}} \dots p_n^{\min\{\alpha_n,\beta_n\}}$$

a NSN

$$p_1^{\max\{\alpha_1,\beta_1\}} \dots p_n^{\max\{\alpha_n,\beta_n\}}.$$

V špeciálnych prípadoch táto metóda môže byť rýchlejšia než Euklidov algoritmus. Vo všeobecnosti je ale nájdenie prvočíselného rozkladu výpočtovo podstatne zložitejšie než výpočet NSD.

Kontrolný test

Začiatok testu (6 bodov) :

1. Zložené číslo

- ☐ musí mať aspoň 2 prvočíselné delitele
- ☐ môže mať jediného prvočíselného deliteľa
- ☐ nemusí mať žiadneho prvočíselného deliteľa

2. Počet celých čísel, ktoré majú presne 2 prvočíselné delitele je

- ☐ 2
- ☐ 4
- ☐ viac ako 4, ale konečný
- ☐ nekonečný

3. Ktoré z nasledujúcich výrokov sú pravdivé?

- ☐ Každé celé číslo má iba konečne veľa prvočíselných deliteľov
- ☐ Každé celé n má tie isté prvočíselné delitele ako n^2
- ☐ Dve rôzne celé čísla môžu mať ten istý rozklad
- ☐ Niektoré celé čísla môžu mať dva rôzne rozklady

4. Zložené číslo $n < 10000$

- ☐ musí byť deliteľné 2 alebo 5
- ☐ musí mať deliteľa, ktorý je menší ako 10
- ☐ nemusí mať deliteľa, ktorý je menší ako 10, ale musí mať deliteľa, ktorý je menší ako 100
- ☐ nemusí mať deliteľa, ktorý je menší ako 100, ale musí mať deliteľa, ktorý je menší ako 1000
- ☐ nemusí mať deliteľa, ktorý je menší ako 1000, ale musí mať deliteľa, ktorý je menší ako 5000

5. Nech p je prvočíslo a $p \neq n > 0$. Poton (n, p) sa rovná

- ☐ 1
- ☐ n
- ☐ p
- ☐ 1 alebo p

☐ 1 alebo n

6. Nech p je prvočíslo a $[x, y]$ označuje NSN čísel x, y. Ktoré z nasledujúcich výrokov sú pravdivé?

☐ Ak $p|x$ alebo $p|y$, tak $p|(x, y)$.

☐ Ak $p|x$ alebo $p|y$, tak $p|[x, y]$.

☐ Ak $p|x$ a zároveň $p|y$, tak $p|(x, y)$.

☐ Ak $p|x$ a zároveň $p|y$, tak $p|[x, y]$.

☐ Ak $p|(x, y)$, tak $p|x$ a zároveň $p|y$.

☐ Ak $p|[x, y]$, tak $p|x$ a zároveň $p|y$.

Koniec testu Správne odpovede

Získané body:

Úspešnosť: