NAJVÄČŠÍ SPOLOČNÝ DELITEĽ POLYNÓMOV

Symbolom $D(f)$ označme množinu všetkých deliteľov polynómu f. Ďalej, nech $D(f,g)$ označuje množinu spoločných deliteľov polynómov f, g, t.j. polynómov, ktoré súčasne delia f aj g.

Definícia Polynóm d sa nazýva najväčším spoločným deliteľom (NSD) polynómov f, g ak

(i) $d \in D(f,g)$;

(ii) pre každé $h \in D(f,g)$ platí $h|d$.

Teda spoločné delitele porovnávame reláciou $|$, podobne ako pri NSD celých čísel: najväčší spoločný deliteľ je taký, že je deliteľný všetkými ostatnými spoločnými deliteľmi. Dôsledkom toho je, že najväčší spoločný deliteľ je určený jednoznačne iba až na asociovanosť.

Veta 1. *Pre každé dva polynómy f, g existuje ich NSD. Ten je určený jednoznačne až na asociovanosť a dá sa vyjadriť v tvare $d = fu + gv$ pre nejaké $u, v \in F[x]$.*

Označenie: Normovaný NSD polynómov f a g budeme označovať (f, g).

V prípade, že $(f, g) = 1$ hovoríme, že f a g sú *nesúdeliteľné*.

Na výpočet NSD existuje dobre známa metóda, ktorá sa nazýva *Euklidov algoritmus*. Zakladá sa na nasledujúcom tvrdení.

Lema 2. *Ak $f = gp + z$ $(f, g, p, z \in F[x])$, tak $D(f, g) = D(g, z)$. Následne, NSD polynómov f a g je taký istý, ako NSD polynómov g a z.*

Popis algoritmu: Predpokladajme, že $\mathrm{st}(a) \geq \mathrm{st}(b)$. Podľa Vety o delení so zvyškom nájdeme $p, z \in F[x]$ tak, že $f = bp + z$, kde $z = 0$ alebo $\mathrm{st}(z) < \mathrm{st}(g)$. Ak $z = 0$, tak NSD je g. Ak $z \neq 0$, tak hľadáme NSD polynómov g a z. Výpočet sa nakoniec musí skončiť, lebo stupne zvyškov stále klesajú.

Poznámka: Euklidov algoritmus sa dá využiť aj na vyjadrenie NSD v tvare $d = fu + gv$.

NSD môžeme definovať nielen pre dva polynómy, ale pre ľubovoľný počet. Nech $D(f_1, \ldots, f_n)$ označuje množinu všetkých spoločných deliteľov polynómov f_1,..., f_n.

Definícia Polynóm d sa nazýva najväčším spoločným deliteľom (NSD) polynómov f_1,...,f_n ak

(i) $d \in D(f_1, \ldots, f_n)$;

(ii) pre každé $h \in D(f_1, \ldots, f_n)$ platí $f|d$.

Podobne ako v prípade dvoch polynómov sa dá dokázať, že NSD vždy existuje a je určený jednoznačne až na asociovanosť. Na jeho výpočet môžeme využiť nasledujúce tvrdenie.

Lema 3. *Nech d je NSD polynómov f_1,...,f_n. Nech e je NSD polynómov d a f_{n+1}. Potom e je NSD polynómov f_1,...,f_{n+1}.*

Na základe uvedenej lemy môžeme postupne vypočítať NSD 2 polynómov, 3 polynómov, 4 polynómov, atď.

Definícia Polynóm n sa nazýva najmenším spoločným násobkom (NSN) polynómov f, g ak

(i) $f|n$, $g|n$;

(ii) pre každé h také, že $a|h$, $b|h$ platí $n|h$.

Na výpočet NSN nám slúži nasledujúce tvrdenie.

Veta 4 *Ak* $(f, g) \neq 0$, *tak polynóm*

$$n = \frac{fg}{(f, g)}$$

je NSN polynómov f *a* g.

Kontrolný test

Začiatok testu (7 bodov) :

1. Dva rôzne polynómy nad nekonečným poľom

- ☐ majú vždy 1 NSD
- ☐ majú vždy nekonečne veľa NSD

☐ môžu mať 1 alebo nekonečne veľa NSD

☐ nemusia mať žiaden NSD

2. Dva rôzne polynómy nad n-prvkovým poľom

☐ majú vždy 1 NSD

☐ majú vždy n NSD

☐ môžu mať 1 alebo n NSD

☐ nemusia mať žiaden NSD

3. Ak $f \neq 0$, tak $(0, f)$ (f normovaný) sa rovná

☐ vždy 0

☐ vždy f

☐ niekedy 0, niekedy f

4. Ak $f \neq 1$, (f normovaný), tak $(1, f)$ sa rovná

- ☐ vždy 1
- ☐ vždy f
- ☐ niekedy 1, niekedy f

5. Nech p je NSD polynómov f, g, nech q je NSD polynómov f, g, h. Potom

- ☐ p delí q
- ☐ q delí p
- ☐ p nemusí deliť q ani q nemusí deliť p

6. Nech p je NSD polynómov f, g, nech q je NSN polynómov f, g. Potom

- ☐ p delí q

☐ q delí p

☐ p nemusí deliť q ani q nemusí deliť p

7. Euklidov algoritmus slúži na

☐ rýchle delenie polynómov

☐ výpočet NSD dvoch polynómov

☐ overenie existencie NSD

Koniec testu | Správne odpovede

Získané body:

Úspešnosť: