IREDUCIBILNÉ POLYNÓMY

Definícia Polynóm f stupňa aspoň 1 sa nazýva ireducibilný, ak je deliteľné **len** konštantami a polynómami asociovanými s f.

Ekvivalentne, f stupňa aspoň 1 je ireducibilný, ak nie je súčinom dvoch polynómov menších stupňov. Polynóm, ktorý nie je ireducibilný a má stupeň aspoň 1 sa nazýva *reducibilný*.

Poznámka. Ireducibilnosť f závisí nielen na f samotnom, ale aj na poli F nad ktorým f posudzujeme. Napríklad $x^2 - 2$ je ireducibilný nad $\mathbb{Q}$, ale nie nad $\mathbb{R}$, kedže $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.
Exiustuje súvislosť medzi ireducibilnosťou a existenciou koreňov.

Lema 1. *Pre každé $f \neq 0$ platí*

- *Ak f má stupeň aspoň 2 a koreň v F, tak je nad F reducibilný.*
- *Ak f má stupeň najviac 3 a nemá koreň v F, tak je nad F ireducibilný.*
- *Ak stupeň f je 2 alebo 3, tak je ireducibilný nad F práve vtedy, keď nemá v F koreň.*

Nasledujúca lema je potrebná k dôkazu vety o rozklade.

Lema 2. *Nech* $h, f_1, \ldots, f_n \in F[x]$.

(i) Ak $h|f_1 f_2$ *a* $(h, f_1) = 1$, *tak* $h|f_2$;

(ii) Ak $h|f_1 f_2 \ldots f_n$ *a* h *je ireducibilný, tak* $h|f_k$ *pre niektoré* k.

Veta 3. *Každý polynóm* f *stupňa aspoň* 1 *sa dá rozložiť na súčin ireducibilných polynómov, a to jednoznačne až na asocionanosť a poradie činiteľov.*

Poznámka Podobne ako pre celé čísla, dôkaz má existenčný charakter a nedáva návod ako rozložiť daný polynóm. Na rozklad existujú rôzne efektívne algoritmy, v závislosti od poľa F.

Znalosť rozkladu na ireducibilné činitele možno využiť pri hľadaní NSD a NSN. Konkrétne, nech polynómy f a g majú rozklady

$$f = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n},$$
$$g = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n},$$

kde $p_1, \ldots, p_n$ sú rôzne ireducibilné polynómy. (Pripúšťame, že niektoré exponenty α_i a β_j môžu byť 0, čo by znamenalo, že príslušný polynóm sa v rozklade nenachádza.) Potom NSD polynómov f, g má rozklad

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

a NSN

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

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

Kontrolný test

Začiatok testu (6 bodov) :

1. Reducibilný polynóm

- ☐ musí mať aspoň 2 ireducibilné delitele
- ☐ môže mať jediného ireducibilného deliteľa

☐ nemusí mať žiadneho ireducibilného deliteľa

2. Polynómy stupňa 1 sú

☐ všetky reducibilné;

☐ všetky ireducibilné;

☐ niektoré reducibilné, niektoré ireducibilné

☐ závisí to od poľa F.

3. Ktoré z nasledujúcich výrokov sú pravdivé?

☐ Každý nenulový polynóm má iba konečne veľa ireducibilných deliteľov

☐ Každý nenulový polynóm nad konečným poľom má iba konečne veľa ireducibilných deliteľov

☐ Každý polynóm f má tie isté ireducibilné delitele ako f^2

☐ Dva rôzne polynómy môžu mať ten istý rozklad

☐ Niektoré polynómy môžu mať dva rôzne rozklady

4. Reducibilný polynóm stupňa 10

☐ musí mať koreň

☐ musí mať ireducibilného deliteľa stupňa menšieho ako 3;

☐ nemusí mať ireducibilného deliteľa stupňa menšieho ako 3, ale musí mať ireducibilného deliteľa stupňa menšieho ako 6;

☐ nemusí mať ireducibilného deliteľa stupňa menšieho ako 6, ale musí mať ireducibilného deliteľa stupňa menšieho ako 10;

☐ nemusí mať ireducibilného deliteľa.

5. Nech p je normovaný ireducibilný polynóm, f ľubovoľný. Potom (f, p) sa rovná

☐ 1

- ☐ f
- ☐ p
- ☐ 1 alebo f
- ☐ 1 alebo p

6. Nech p je ireducibilný polynóm a $[f, g]$ označuje NSN polynómov f, g. Ktoré z nasledujúcich výrokov sú pravdivé?

- ☐ Ak $p|f$ alebo $p|g$, tak $p|(f, g)$.
- ☐ Ak $p|f$ alebo $p|g$, tak $p|[f, g]$.
- ☐ Ak $p|f$ a zároveň $p|g$, tak $p|(f, g)$.
- ☐ Ak $p|f$ a zároveň $p|g$, tak $p|[f, g]$.
- ☐ Ak $p|(f, g)$, tak $p|f$ a zároveň $p|g$.
- ☐ Ak $p|[f, g]$, tak $p|f$ a zároveň $p|g$.

Koniec testu | Správne odpovede

Získané body:

Úspešnosť: