3. vnitrosemestrální práce MB104, 22. 5. 2017
skupina A

Příklad 1. (4b.) V celých číslech vyřešte rovnici

$$x^3 - y^3 = 91$$

(nelze $x^3 - y^3$ nějak rozložit?; nebo jak velký, resp. malý, může být rozdíl třetích mocnin?)

Řešení. „vyřešte rovnici“ je terminus technikus a znamená nalézt všechna řešení a ukázat, že žádná další nejsou.

Rozkladem převést na soustavu rovnic, nebo hrubou silou. $(6,5)$, $(-5,-6)$, $(3,-4)$, $(4,-3)$. Jenom trefená řešení (všechna) 1.5b, aspoň dvě 1b. Záleží na argumentaci, o neexistenci dalších řešení na udělení bodů.

$x^3 - y^3 = (x-y)(x^2+xy+y^2) = 7 \cdot 13$, $x^2+xy+y^2 \geq 0$, $x^2+xy+y^2 \geq (x-y)$, tedy $(x-y) = 1 \& x^2+xy+y^2 = 91$ nebo $(x-y) = 7 \& x^2+xy+y^2 = 13$. Vyjádřením jedné neznámé z lineární rovnice a dosazením do kvadratické dostáváme dvě kvadratické rovnice, každá o jedné neznámé, celkem čtyři dvojice uvedených řešení.

Rozklad 0.5*b*, sestavení rovnic (i více) 2.5b, jejich vyřešení 1b.

Příklad 2. (4b.) V šifře ElGamal Honza zveřejnil klíč $(79, 3, 13)$. Přijal od Martina šifru $(2, 10)$. Jakou zprávu mu Martin zaslal? (víte, že $3^{34} \equiv 13 \pmod{79}$).

Řešení. $(2^{34})^{-1} = 2^{44} = 32 \pmod{79}$. Vědět, co chci počítat $(2^{34})^{-1}$ za 1b. Na výpočet inverze možno použít jak přímého výpočtu 2^{44}, nebo 2^{34} a dopočtu pomocí EA (2b) závěrečný výpočet $32 \cdot 10 \equiv 4 \pmod{79}$, 1b.

Příklad 3. (5b.) V $(20, 10)$ lineárním kódu generovaném polynomem $x^{10}+x^6+x^3+x^2+1$ zakódujte slovo 1010000001. (odpovídá polynomu $1+x^2+x^9$) (Je nutné počítat generující matici kódu?)

Řešení. Správný postup pomocí generující matice 2.5b nebo pomocí dělitelnosti polynomu $x^{10}(x^9+x^2+1)$ 3.5b, správný výpočet 2.5b, resp 1.5b. Numerické chyby ve výpočtu srážky dolů po půl bodu, závažnější 1b.

$$\begin{aligned} x^{19}+x^{12}+x^{10} &\equiv (x^{15}+x^{12}+x^{11}+x^9)+x^{12}+x^{10} \equiv x^{15}+x^{11}+x^9+x^{10} \equiv \\ &\equiv (x^{11}+x^8+x^7+x^5)+x^{11}+x^9+x^{10} \equiv x^8+x^7+x^5+x^9+x^{10} \equiv \\ &\equiv x^8+x^7+x^5+x^9+(x^6+x^3+x^2+1) \pmod{x^{10}+x^6+x^3+x^2+1} \end{aligned}$$

(odčítám vždy takový násobek generujícího polynomu monomem x^k, aby se mě odečetla nejvyšší aktuální mocina; jakmile jsou všechny mocniny menší než x^{10} jsem hotov). Výsledek 1011011111 1010000001.

P.S. Omlouvám se za opravu zadání ((21,10) kód na (20,10) kód). Na uvedeném způsobu řešení se tím ale nic neměnilo. Navíc zadání vyzívalo k nepoužívání generující matice (ale i tam jste mohli záhy zjistit, že to zadání nesedí).

Příklad 4. (7b.) Metodou vytvořující funkce nalezněte jedinou posloupnost a_n vyhovující diferenční rovnici

$$a_{n+2} = 5a_{n+1} + 6a_n + n + 2,\ a_1 = 1\ a_2 = 7$$

.

Řešení. Dopočítání nultého člene 0.5b ($a_0 = 0$) Nalezení rovnice pro $a(x)$ ($= \sum_0^\infty a_n x^n$) 3.5b.

$$a(x) = \frac{x}{(1+x)(1-6x)(1-x)^2}$$

(správné přepsání rekurence 0.5b, vyjádření nehomogenity 2b, zkouška doplnění prvních dvou členů – není třeba doplňovat 1b).

Rozklad na parc. zlomky 2b (správná forma 1b, dopočet 1b). Odečtení výsledku 1b.

$$a_n = \frac{36}{175}6^n - \frac{1}{28}(-1)^n - \frac{7}{100} - \frac{1}{10}(n+1)$$