

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

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. Rozkladem převést na soustavu rovnic, nebo hrubou silou. Postup viz sk. A. $(-6, -5)$, $(5, 6)$, $(-4, 3)$, $(-3, 4)$. Jenom trefená řešení (všechna) 1.5b, aspoň dvě 1b. Rozklad 0.5b, sestavení rovnic (i více) 2.5b, jejich vyřešení 1b.

Příklad 2. (4b.) V šifře ElGamal Honza zveřejnil klíč $(79, 3, 13)$ (kde 3 je primitivní kořen modulo 79) Přijal od Martina šifru $(2, 9)$. Jakou zprávu mu Martin zaslal? (víte, že $3^{35} \equiv 39 \pmod{79}$).

Řešení. Viz sk. A

Příklad 3. (5b.) V $(21, 10)$ lineárním kódu generovaném polynomem $x^{10} + x^6 + x^5 + x^2 + 1$ zakódujte slovo 1100000001 (odpovídá polynomu $1 + x + x^9$) (Je nutné počítat generující matici kódu?)

Řešení. Výsledek 1111101000 1100000001. Postup viz sk.A

Příklad 4. (7b.) Metodou vytvořující funkce nalezněte jedinou posloupnost a_n vyhovující diferenční rovnici $a_{n+2} = a_{n+1} + 6a_n + n - 1$, $a_1 = 1$, $a_2 = 6$.

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

$$a(x) = xa(x) + 6x^2a(x) + \frac{4x - 3}{(1 - x)^2} + 4 + 2x$$

$$a(x) = \frac{(4x - 3) + (4 + 2x)(1 - x)^2}{(1 + 2x)(1 - 3x)(1 - x)^2}$$

(správné přepsání rekurence 0.5b, vyjádření nehomogenity 2b, doplnění prvních dvou členů $-4 + 2x$, 1b) Rozklad na parc. zlomky 2b.(tvar 1b, výpočet 1b) Odečtení výsledku 1b.

$$a_n = \frac{11}{20}3^n + \frac{14}{45}(-2)^n - \frac{1}{6}n + \frac{5}{36}$$