První zkoušková práce, 27. 5. 2016 skupina A

Příklad 1. (5b.) V šifře ElGammal Honza zveřejnil klíč $(53, 3, 12)$, kde 3 je primitivním kořenem modulo 53, $12 \equiv 3^x$, kde x je Honzův tajný klíč. Přijal od Martina šifru $(2, 17)$. Umíte šifru prolomit a říct jakou zprávu mu Martin zaslal? (víte, že $3^{21} \equiv 41 \equiv -12 \pmod{53}$). (malá nápověda: kolik že je $3^{26} \mod 53$?

Řešení. 35.

Příklad 2. (5b.) Určete všechny třetí odmocniny z 57 modulo 143.

Řešení. 7, 73, 128.

Příklad 3. (6b.) Metodou vytvořujících funkcí nalezněte posloupnost (x_n) splňující pro $n \geq 1$:

$$x_{n+2} = x_{n+1} + 2x_n + 2, \quad x_1 = 3,\ x_2 = 1.$$

Řešení. $a_n = -1 + 2^n - 2(-1)^n$.

Příklad 4. (4b.) Kolika způsoby lze vybrat 100 kuliček tří barev (červená, modrá, zelená), přičemž počet červených je větší než počet modrých? Jako výsledek uveďte přirozené číslo.

Řešení. $\frac{1}{2}(\binom{102}{2} - \binom{51}{1}) = 2550$.