3. vnitrosemestrální (1.zkoušková) práce MB104, 20. 5. 2015

Příklad 1. (4b.) Váš veřejný klíč pro šifru RSA je $(221, 43)$. Obdrželi jste zprávu 3. Dešifrujte ji.

Řešení. $\varphi(221) = 192$ (1b.), $43^{-1} \equiv 67 \pmod{192}$ (1b.), $2^{67} \equiv 76 \pmod{221}$

Příklad 2. (5b.) Určete nejmenší a největší primitivní kořen modulo 59 (tj. nejmenší a největší číslo z intervalu $[1, 58]$, které je primitivním kořenem).

Řešení. 2 (2b., tj. $2^2 \not\equiv 1 \pmod{59}, 2^{29} \equiv -1 \pmod{59}$), 56.

Příklad 3. (5b.) Kolika způsoby lze vybrat sto kusů ovoce ze tří druhů (mandarinek, pomerančů a citronů) tak, aby součet počtu mandarinek a pomerančů byl dělitelný třemi?

Řešení. Šlo řešit mnoha způsoby. Užitím rozvoje vhodných řad: koeficient u x^{100} ve výrazu

$$\begin{aligned} V(x) &= x(1 + x^3 + x^6 + \cdots)(1 + x + x^2 + \cdots)^2 = x\frac{1}{1-x^3}\frac{1}{(1-x)^2} = \\ &= x\left(\sum_{n=0}^{\infty} x^{3n}\right)\left(\sum_{n=0}^{\infty}\binom{n+1}{1}x^n\right). \end{aligned}$$

Potom

$$[x^{100}]V(x) = 1 + 4 + 7 + \cdots + 100 = 1717.$$

Sčítance v řadě udávají též postupně možnosti rozdělení pomerančů a mandarinek, je-li citrónů postupně 100, 97, 94, ...

Jiná úvaha vede k počítání možností podle toho, jaký zbytek po dělení třemi dávají počty mandarinek a pomerančů. Máme tři možnosti: $3k$ a $3l$, $3k + 1$ a $3l + 2$, $3k + 2$ a $3l + 1$. Opět buď pomocí vytvořujících funkcí nebo přímou kombinatorickou úvahou dojdeme k výsledku

$$\binom{35}{2} + 2\binom{34}{2} = 1717.$$

Příklad 4. (6b.) **Metodou vytvořující funkce** určete jedinou posloupnost vyhovující rekurentnímu vztahu

$$a_n = 2a_{n-1} + 3a_{n-2} + n^2,\ n \geq 2 \quad a_0 = 0,\ a_1 = 1.$$

(odvození vytvořující funkce posloupnosti n^2 1b, zapsání rovnice pro vytvořující funkci 1b, vyjádření vytvořující funkce jakožto součet (neznámých) parciálních zlomků 1b, výpočet zlomků 1b, vyjádření a_n 2b; za vyřešení příkladu bez nelineárního členu 3b)

Řešení. $\frac{1}{8}3^{n+2} - \frac{1}{2}n^2 - n - \frac{9}{8}$.