2.zkoušková práce MB104, 3. 6. 2015

Příklad 1. (5b.) Váš veřejný klíč pro šifru ElGamal je $(59, 2, 43)$. Obdrželi jste zprávu $(5, 10)$. Dešifrujte ji. (Pro zjištění soukromého klíče si všimněte, že $43 \equiv -16 \pmod 5$)9 a že 16 je mocnina dvojky)

Řešení. Soukromý klíč je $33(= 29 + 4)$, potom $Z \equiv 5^{25} \cdot 10 \equiv 34 \pmod{59}$. $(5^{25} = (5^{33})^{-1} = 27)$

Příklad 2. (5b.) Vyřešte soustavu konguruencí

$$\begin{aligned} 27x &\equiv 15 \pmod{30} \\ 11x &\equiv 9 \pmod{7} \\ 40x &\equiv 45 \pmod{55} \end{aligned}$$

Řešení. $770u + 305$.

Příklad 3. (4b.) Určete počet binárních slov délky 8, jejichž Hammingova vzdálenost od kteréhokoliv ze slov 11110000, 00001111 nepřevyšuje 5.

Řešení. $\binom{8}{4} + 2\binom{8}{3}$.

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

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

Řešení. $a_n = 2^n + 2(\frac{-1}{2})^n$.