Zkoušková práce, 6. 6. 2017

Příklad 1. (3b.) Pomocí Eukleidova algoritmu určete největšího společného dělitele čísel 143 a 53 a příslušné Bezoutovy koeficienty.

Příklad 2. (7b.) Určete zbytek čísla $18^{15^{14^{13}}}$ po dělení číslem 135.

Řešení. 108.

Příklad 3. (6b.) Vyřešte soustavu kongruencí:

$$\begin{aligned} 40x &\equiv 130 \pmod{50} \\ 8x &\equiv 7 \pmod{13} \\ 3x &\equiv 9 \pmod{17} \end{aligned}$$

Řešení. $1105k - 303$

Příklad 4. (7b.) V šifře RSA jste zveřejnili veřejný klíč $(55, 17)$. Obdrželi jste zprávu 3. Dešifrujte.

Řešení. $17^{-1} \equiv 33 \pmod{40}$, $3^{33} \equiv 38 \pmod{55}$.

Příklad 5. (7b.) Určete generující matici G a kontrolní matici H lineárního $(10, 3)$ kódu generovaného polynomem $x^7 + x^6 + x^2 + 1$. V tomto kódování jste obdrželi kódové slovo 0011000101. Určete tříbitovou odeslanou zprávu za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb.

Řešení. Syndrom 0100100, vedoucí reprezentant 0100100000, slovo 0111100101, tedy tříbitová zpráva 101.

Příklad 6. (10b.) Pomocí metody vytvořujících funkcí vyřešte rekurentní vztah ($n \geq 2$)

$$x_n = 5x_{n-1} - 6x_{n-2} + 2n, \quad x_0 = 0,\ x_1 = 0.$$

Řešení. $\frac{5}{2}3^n - 6 \cdot 2^n + n + \frac{7}{2}$.