ukázková závěrečná písemka z 2020/21

1. Řešte soustavu kongruencí

$$\begin{aligned} 2x^2 &\equiv 6 \pmod{23} \\ 19x &\equiv 9 \pmod{31} \end{aligned}$$

(Nápověda: Prvočíslo 23 je tvaru jako v Rabinově kryptosystému.) **(10 bodů)**

2. a) Ukažte, že 29 je primitivní kořen modulo 89.

b) Demonstrujte protokol výměny klíču Diffie-Hellman s tímto modulem a primitivním kořenem a se zvolenými exponenty 19 a 45.

(10 bodů)

3. Dokažte, že neexistuje přirozené číslo m takové, že $\varphi(m) = 434 = 2 \cdot 7 \cdot 31$. **(10 bodů)**

4. Kolika způsoby mohlo skončit výsledné pořadí týmů volejbalové extraligy s 12 týmy, jestliže se všechny 3 pražské týmy umístily ve spodní polovině tabulky a zároveň za oběma brněnskými celky? (Nápověda: Rozdělte úlohu podle toho, kolik brněnských týmů skončilo v horní/spodní části tabulky.) **(8 bodů)**

5. Určete počet (ne nutně kódových) slov v $(14, 9)$-kódu, které mají od slova (00000|000000000) Hammingovou vzdálenost menší nebo rovnu 3. Určete maximální počet kódových slov, které se mohou mezi slovy z první části vyskytovat v případě lineárního kódu s maticí

$$G = \begin{pmatrix} P \\ \mathbb{I}_k \end{pmatrix}$$

(tak jako na přednáškách; $\mathbb{I}_k$ značí jednotkovou matici). **(8 bodů)**

6. Najděte vytvořující funkci posloupnosti zadané rekurentně vztahy

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

a udejte vzoreček pro n-tý člen posloupnosti. (Pokud budete počítat celou dobu s neznámými koeficienty, budete nakonec potřebovat také a_2, a_3.) **(14 bodů)**