# *Democvičení*

## *MB104 - jaro 2013*

**Příklad 1.** Označme $x_1, x_2, x_3$ kořeny polynomu $x^3 - 6x^2 + 7x - 4 \in \mathbb{R}[x]$. Aniž byste tyto kořeny počítali, určete polynom, který bude mít kořeny $-3x_1,\ -3x_2,\ -3x_3$.

**Příklad 2.** $x^3 + 2x^2 - 5x + 12 \in \mathbb{R}[x]$. Aniž byste tyto kořeny počítali, určete polynom, který bude mít kořeny $-\frac{1}{x_1}\ -\frac{1}{x_2},\ -\frac{1}{x_3}$.

**Příklad 3.** Označme $x_1, x_2, x_3$ kořeny polynomu $2x^3 - 11x^2 + 16x - 6$. Aniž byste tyto kořeny počítali, určete povrch a objem kvádru, který bude mít hrany dlouhé $x_1$, $x_2$, $x_3$.

**Příklad 4.** Zakódujte zprávu 1101 pomocí kódu generovaného polynomem $1 + x + x^2$.

**Příklad 5.** Určete generující matici a matici kontroly parity pro lineární kód $(7, 4)$ generovaný polynomem $x^3 + x^2 + 1$.

**Příklad 6.** Alice si za parametry svého RSA klíče zvolila $p = 23$, $q = 31$, $e = 17$. Dopočítejte její soukromý klíč a zašifrujte (následně i dešifrujte) zprávu $m = 12$. zprávu m = 12.

**Příklad 7.** Alice zvolila za parametry v kryptosystému ElGamal $p = 23$; $g = 5$, za svůj soukromý klíč zvolila $x = 13$ a zveřejnila veřejný klíč $(p; g; gx)$. Ukažte, jak Bob zašifruje zprávu $m = 17$ určenou Alici a jak tuto zprávu následně Alice dešifruje.