Algorithms in Algebra and Number Theory
2026

Exercise 1. *Let* $M = \begin{pmatrix} 1 & -1 \\ 6 & -4 \end{pmatrix}$. *Provide functions* $f_1(n), f_2(n), f_3(n), f_4(n)$, *such that*

$$M^n = \begin{pmatrix} f_1(n) & f_2(n) \\ f_3(n) & f_4(n) \end{pmatrix}.$$

Determine three different prime values of n, *for which* $f_1(n)$ *is a prime.*

Exercise 2. *Balance the following chemical equation:*

$$aAl_2(SO_4)_3 + bCa(OH)_2 \longrightarrow cAl(OH)_3 + dCaSO_4.$$

Exercise 3. *By means of the algebraic method determine a 3-coloring of the graph*
`G=graphs.PetersenGraph()`
such that the vertices 0, 7 and 8 are colored in the same way.

Exercise 4. *Let* $f(x) = x^6 + 5x^2 + x + 3$ *be a polynomial over* $\mathbb{F}_p$, *for some prime* p. *Determine the largest two digit prime for which the polynomial is reducible by applying the Berlekamp's algorithm. What is the value of* p*?*

Exercise 5. *Solve the discrete logarithm problem* $23^x \equiv 57 \pmod{557}$ *by means of the modified Pollard's-*ρ *method in which the sequence is defined by* $x_0 = 1$ *and*

$$x_{n+1} = \begin{cases} gx_n & \text{if } x_n \equiv 0 \pmod 3, \\ ghx_n & \text{if } x_n \equiv 1 \pmod 3, \\ x_n^2 & \text{if } x_n \equiv 2 \pmod 3. \end{cases}$$