

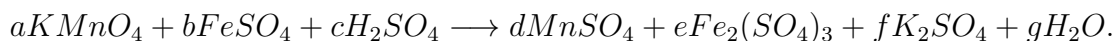
Algorithms in Algebra and Number Theory
2026

Exercise 1. Let $M = \begin{pmatrix} 1 & -3 \\ 5 & 3 \end{pmatrix}$. 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 values of n , for which $f_1(n)$ is a square.

Exercise 2. Balance the following chemical equation:



Exercise 3. Given the shares in Shamir's secret sharing over \mathbb{F}_{29} :

$$\begin{aligned} s_1 &= 9, \\ s_2 &= 2, \\ s_3 &= 2, \\ s_4 &= 19, \\ s_5 &= 1. \end{aligned}$$

Reconstruct the secret by using the shares s_1, s_2, s_3, s_4, s_5 . Compute the value of s_6 .

Exercise 4. Let $f(x) = x^6 + 5x^2 + x + 3$ be a polynomial over \mathbb{F}_p , for some prime p . Determine the smallest 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 $7^x \equiv 300 \pmod{431}$ by means of the modified Pollard's- ρ method in which the sequence is defined by $x_0 = 1$ and

$$x_{n+1} = \begin{cases} gx_n & \text{if } x_n \equiv 0 \pmod{4}, \\ hx_n & \text{if } x_n \equiv 1 \pmod{4}, \\ x_n^2 & \text{if } x_n \equiv 2 \pmod{4}, \\ ghx_n & \text{if } x_n \equiv 3 \pmod{4}. \end{cases}$$