

1. Exercise. Let

$$M = \begin{pmatrix} 1 & t \\ -3 & 4 \end{pmatrix},$$

where t is an integer. We know that M^{-1} is also a matrix consisting of integer elements. Using the eigenvalue-eigenvector method, determine M^n and M^{-n} in closed form! Since $M^n[0,0] + M^{-n}[0,0]$ is equal to what?

2. Exercise. Shamir's secret sharing in \mathbb{Z}_{29} . The secret shares are:

$$\begin{aligned} s_2 &= 1, \\ s_4 &= 12, \\ s_{20} &= 8, \\ s_{22} &= 28, \\ s_{26} &= 3. \end{aligned}$$

Three secret shares are sufficient to reconstruct the secret. We know that exactly one secret share has been recorded incorrectly. Which one is it, and what is the correct value?

3. Exercise. Using the following modified Pollard ρ method, determine an x such that

$$13^x \equiv 321 \pmod{821}.$$

Where the sequence used is: $x_0 = 1$ and

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

4. Exercise. Using algebraic methods, determine a valid 3-coloring of the graph $G = \text{graphs.StaircaseGraph}(5)$ in which vertices 0, 2, and 7 have the same color!

5. Exercise. For the graph in the previous exercise, use the greedy algorithm to find a valid coloring in which vertices 4 and 7 have the same color!