Algorithms in Algebra and Number Theory
2026

Exercise 1. *Determine all 2-digit Proth-primes for which $a = 9$ can be used in the Proth-test to prove primality.*

Exercise 2. *Apply Dixon's method with $B = \{2, 3, 5, 7\}$ to factor $n = 671773$.*

Exercise 3. *Determine a pair (a, b) such that $n = 447407$ can be factored by using the elliptic curve $y^2 = x^3 + ax + b$ and the point $P = (-1, 2)$.*

Exercise 4. *In RSA we know $(p, q, d) = (2237, 3457, 6623671)$, and we receive the encrypted message*

$$[601610, 1641661, 7441404, 4690271, 2937977, 4695563, 3007762].$$

Determine the original message.

Exercise 5. *A triangular number is an integer of the form $T_n = \frac{n(n+1)}{2}$. Determine 5 different values of n such that the product of three consecutive triangular numbers $T_n T_{n+1} T_{n+2}$ is a perfect square.*