Algorithms in Algebra and Number Theory (19 May 2025)

Exercise 1. *Determine the largest 3-digit Proth-prime for which $a = 7$ can be used in the Proth-test to prove primality.*

Exercise 2. *Apply Dixon's method with $B = \{2, 11, 17\}$ to factor $n = 1050857$.*

Exercise 3. *Determine a value of $a > 0$ such that $n = 343507$ can be factored by using the elliptic curve $y^2 = x^3 + ax - a$.*

Exercise 4. *In RSA we know $(p, q, d) = (101, 1013, 60173)$, and we receive the encrypted message*

$$[26474, 12942, 59277, 26983].$$

Determine the original message.

Exercise 5. *Determine two different $(x, y) \in \mathbb{N}^2$ solutions of the equation*

$$x^2 - 11y^2 = 1$$

by using continued fractions such that $x + y$ is a prime.