Algorithms in Algebra and Number Theory (May 2025)

Exercise 1. *Determine 2 different Proth-primes for which* $a = 23$ *can be used in the Proth-test to prove primality.*

Exercise 2. *In RSA we have* $(n, e) = (5352499, 3516607)$. *Encrypt the message "The only way to learn mathematics is to do mathematics".*

Exercise 3. *In RSA we know* $(p, q, d) = (12227, 35569, 136215539)$, *and we receive the encrypted message*

$$[158079363, 173377019, 373536605, 97680494, 144518909, 1942499, 413795444, 147133032].$$

Determine the original message.

Exercise 4. *Determine 2 different values of* a *such that* $n = 6409$ *can be factored by using the elliptic curve* $y^2 = x^3 + ax + 1$ *with the point* $P = (0, 1)$.

Exercise 5. *In RSA we know* $(N, e_1, e_2, c_1, c_2) = (8137, 7, 23, 7155, 2626)$. *Apply the common modulus attack to recover the secret message.*

Exercise 6. *Bob, Chris and David have RSA public keys given by* $(N_B, e_B) = (6527, 7), (N_C, e_C) = (11537, 7)$ *and* $(N_D, e_D) = (10123, 7)$, *respectively. Alice sends the same message to both of them, the ciphertexts are as follows* $c_B = 2268, c_C = 3442$ *and* $c_D = 4737$. *Determine the message by means of the low public exponent attack.*

Exercise 7. *Apply Dixon's method with* $B = \{2, 11, 17\}$ *to factor* $n = 1050857$.

Exercise 8. *Apply the continued fraction factorization method with* $B = \{2, 3, 7, 19\}$ *to factor* $n = 55567$.

Exercise 9. *Determine two different* $(x, y) \in \mathbb{N}^2$ *solutions of the equation*

$$x^2 - 67y^2 = 1$$

by using continued fractions.

Exercise 10. *Determine a positive rational solution of the equation*

$$6x^2 + 7y^2 - 13 = 0$$

in which the numerator of x *and the numerator of* y *are prime numbers.*