

# 1 Exercises

**Exercise 1.** How would you test if an integer  $n$  is prime, using the brute-force approach?

**Solution.** We need to check if  $n$  is co-prime to all integers in the range  $[2, \sqrt{n}]$ . If it is the case, then  $n$  is prime.

**Exercise 2.** Apply Fermat primality test to verify the primality of 351, 511, and 717.

**Solution.** For 351, take  $a = 2$  and we have  $2^{350} \bmod 351 = 121 \neq 1$ , hence, 2 is a Fermat witness, and 351 is composite.

For 511, take  $a = 2$  and we have  $2^{510} \bmod 511 = 64 \neq 1$ , hence 2 is a Fermat witness, and 511 is composite.

For 717, take  $a = 2$  and we have  $2^{716} \bmod 717 = 4 \neq 1$ , hence 2 is a Fermat witness, and 717 is composite.

**Exercise 3.** Solve for  $x$ :  $x^2 \bmod 63 = 1$ , where 63 is the product of two primes 7 and 9.

**Solution.** We need to find the square roots of 1 is  $\mathbb{Z}_{63}$ . By the Chinese Remainder Theorem,  $\mathbb{Z}/63\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ , and isomorphism  $\varphi : \mathbb{Z}/63\mathbb{Z} \rightarrow \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$  is given by  $\varphi(n \bmod 63) \mapsto (x \bmod 7, x \bmod 9) = (x_7, x_9)$ . To find the square roots of unity, we need to find elements  $(x_7, x_9)$  that would satisfy  $(x_7^2 \bmod 7, x_9^2 \bmod 9) = (1, 1)$ . For this, we solve a system of equations

$$\begin{cases} x_7^2 \bmod 7 = 1, & \text{and hence } x_7=1 \text{ or } x_7 = 6, \\ x_9^2 \bmod 9 = 1, & \text{and hence } x_9=1 \text{ or } x_9 = 8. \end{cases}$$
 The possible values for  $(x_7, x_9)$  form 4

combinations:  $(1, 1), (1, 8), (6, 1), (6, 8)$ . Now we need to map these elements back into  $\mathbb{Z}/63\mathbb{Z}$ .

The inverse isomorphism  $\psi : \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \rightarrow \mathbb{Z}/63\mathbb{Z}$  is given by the solution to the CRT

$$\begin{cases} x \equiv x_p \pmod{p} \\ x \equiv x_q \pmod{q} \end{cases}$$
 given by  $\psi : (x_p, x_q) \mapsto \beta q x_p + \alpha p x_q \bmod n$ , where  $\alpha$  and  $\beta$  are the Bézout coefficients of  $\gcd(x_p, x_q) = \alpha p + \beta q$ . The Bézout identity is  $\gcd(7, 9) = 4 \cdot 7 + (-3) \cdot 9 = 1$ .

Hence,  $\alpha = 4$  and  $\beta = -3$ .

Solving  $\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 1 \pmod{9} \end{cases}$  has a trivial solution  $x = 1 \in \mathbb{Z}/63\mathbb{Z}$ .

Solving  $\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 8 \pmod{9} \end{cases}$  gives the solution  $x = 8 \in \mathbb{Z}/63\mathbb{Z}$ .

Solving  $\begin{cases} x \equiv 6 \pmod{7} \\ x \equiv 1 \pmod{9} \end{cases}$  gives the solution  $x = -3 \cdot 9 \cdot 6 + 4 \cdot 7 \cdot 1 = -134 \equiv 55 \in \mathbb{Z}/63\mathbb{Z}$ .

Solving  $\begin{cases} x \equiv 6 \pmod{7} \\ x \equiv 8 \pmod{9} \end{cases}$  gives the solution  $x = -3 \cdot 9 \cdot 6 + 4 \cdot 7 \cdot 8 = 62 \in \mathbb{Z}/63\mathbb{Z}$ .

To conclude, there are four 2-nd roots of unity in  $\mathbb{Z}/63\mathbb{Z}$ , they are: 1, 8, 55, 62.

**Exercise 4.** Adversary Carol has intercepted two RSA cryptograms,  $y_1 = 537$  sent by Alice to Bob, and  $y_2 = 285$  sent by Alice to Eve. The public key of Bob is  $(e_1 = 18, n_1 = 943)$ , and the public key of Eve is  $(e_2 = 19, n_2 = 943)$ . What is the message  $m$  sent by Alice to Bob and Eve?

**Solution.** Carol knows that Bob and Eve receive the same message  $m$ . Hence,

$$\begin{aligned}537 &= m^{18} \pmod{943} , \\285 &= m^{19} \pmod{943} .\end{aligned}$$

Since the public exponents of Bob and Eve are co-prime, meaning that  $\gcd(18, 19) = 1$ , the Bézout identity applies.

$$\gcd(18, 19) = 1 \cdot 19 + (-1) \cdot 18 = 1 .$$

Carol needs to combine  $y_1$  and  $y_2$  in such a way that would exploit the Bézout identity to get  $m$ . Observe that given  $\alpha \cdot e_1 + \beta \cdot e_2 = 1$  implies that

$$y_1^\alpha \cdot y_2^\beta = (m^{e_1})^\alpha \cdot (m^{e_2})^\beta = m^{\alpha \cdot e_1} \cdot m^{\beta \cdot e_2} = m^{\alpha \cdot e_1 + \beta \cdot e_2} = m^1 = m .$$

Given that  $\alpha = -1$ , and hence  $y_1^\alpha = 537^{-1} \equiv 72 \pmod{943}$  and  $\beta = 1$ , Carol needs to compute

$$m = 72 \cdot 285 \pmod{943} = 717 .$$

**Exercise 5.** Suppose that adversary Carol has intercepted three cryptograms  $y_1, y_2, y_3$  sent to three different users whose public keys are  $(e = 3, n_1), (e = 3, n_2), (e = 3, n_3)$ . Notice that all public keys use the same public exponent, and different moduli. What does Carol needs to do to reconstruct the message  $m$ ?

**Solution.** Carol knows that

$$\begin{aligned}y_1 &= m^3 \pmod{n_1} \\y_2 &= m^3 \pmod{n_2} \\y_3 &= m^3 \pmod{n_3}\end{aligned}$$

and she knows that  $m < n_1, m < n_2, m < n_3$ . Hence,  $m^3 < n_1 \cdot n_2 \cdot n_3$ , and therefore  $m^3$  is the solution to the CRT

$$\begin{cases} x \pmod{n_1} = y_1 \\ x \pmod{n_2} = y_2 \\ x \pmod{n_3} = y_3 \end{cases}$$

CRT guarantees the existence of the solution, and that the solution is unique. Since  $m^3$  solves the CRT, it must be this unique solution. All that Carol needs to do now is to calculate

$$m = \sqrt[3]{m^3}$$

to reconstruct the message  $m$ .

If the public exponent is relatively small, say,  $n$ , then the adversary needs to intercept  $n$  cryptograms in order to be able to decipher it.