Exercise 5.1 (Small Public Exponent RSA Cryptosystem). (4 points)

This exercise will show that, when using the RSA cryptosystem as a public key encryption scheme, small public exponents may be a real danger.

In a public domain the exponent \( e = 3 \) is used as public exponent, thus every user chooses a public modulus \( N \) such that \( \gcd(\varphi(N), 3) = 1 \) and computes his respective secret exponent \( d \) such that \( (3 \cdot d) \mod \varphi(N) = 1 \). Suppose that the users \( A, B, C \) have the following public moduli:

\[
N_1 = 5000746010773, \quad N_2 = 5000692010527, \quad N_3 = 5000296004107.
\]

(i) ALICE sends a message \( m \) to \( A, B, C \) by encrypting: \( m_i = m^3 \mod N_i \). EVEn drops in and captures the following values:

\[
m_1 = 1549725913504, \quad m_2 = 2886199297672, \quad m_3 = 2972130153144.
\]

Show that EVEn can recover the value of \( m \) without factoring \( N_i \) and compute this value with a Computer Algebra System of your choice (Maple, MuPAD, Mathematica, SAGE, etc.). (Hint: Use the Chinese Remainder Theorem.)

(ii) Generalize the method used by EVEn above for a general public exponent \( e \). How many messages should EVEn intercept in order to recover the clear text message?

Exercise 5.2 (Diffie-Hellman key exchange in \( \mathbb{Z}_{20443}^\times \)). (5 points)

ALICE and BOB want to agree on a common key over an insecure channel. To do so, they perform a Diffie-Hellman key exchange in the group \( \mathbb{Z}_{20443}^\times \)

(i) To find a generator for the cyclic group \( \mathbb{Z}_{20443}^\times \), the following fact is used:
**Theorem.** An element \( a \in \mathbb{Z}_p^\times \) is a generator if and only if \( a^{(p-1)/t} \neq 1 \) (mod \( p \)) holds for all prime divisors \( t \) of \( p-1 \).

Use this to show that \( 2 \) is a generator of \( \mathbb{Z}_{20443}^\times \).

(ii) Next, ALICE chooses her private key \( a = 257 \) and BOB chooses his private key \( b = 1280 \). What are the further steps, both sides have to perform, until they are both in possession of the common key, corresponding to their private keys? Do them.

**Exercise 5.3 (Orders).**

Let \( G \) be a (multiplicative) commutative group, \( a \) an element of order \( u \) and \( b \) an element of order \( v \). We want to investigate two questions:

- What is the order of \( a^2, a^3, \ldots \)?
- What are possible orders of \( ab \)?

First, let us look at an example: Take \( G = \mathbb{Z}_{1321}^\times \), \( a = 53 \) and \( b = 17 \). We have \( a^{33} = 1 \) and \( b^{24} = 1 \) in \( G \) and for all respective smaller positive exponents the result is not 1.

(i) Compute the order of \( a^2, a^3, a^9, a^{10}, a^{11} \).

(ii) Compute the order of \( ab, a^2b, a^3b \).

Now, we want to investigate the general case:

(iii) Show: The order of the power \( x^n \) of a group element \( x \in G \) is the order of \( x \) divided by the greatest common divisor of \( n \) and that order.

In short:

\[
\text{ord}(x^n) = \frac{\text{ord}(x)}{\gcd(n, \text{ord}(x))}.
\]

(Hint: Look at the special cases \( \gcd(n, \text{ord}(x)) = 1 \) and \( n|\text{ord}(x) \) and derive the general solution from there.)

(iv) Show: If the orders of two group elements \( x, y \in G \) are coprime, then the order of \( xy \) is actually equal to the the least common multiple of those orders.

In short:

\[
\text{If} \ \gcd(\text{ord}(x), \text{ord}(y)) = 1, \ \text{then} \ \text{ord}(xy) = \ellcm(\text{ord}(x), \text{ord}(y)).
\]