Methods Sheet - SM503M

A collection of methods to accompany revisions of Mathematics for Cryptography.

Doryan Denis

2024-2025

Contents

1 Arithmetics

Learning Outcomes.

- Find the prime factorisation of a given integer.
- Find the set of all divisors of a given integer from its prime factorisation.
- Find the gcd of two integers (either using the prime factorisation or the Euclidean algorithm).
- Perform computations in the ring $(\mathbb{Z}/n\mathbb{Z}, \oplus, \otimes)$. In particular, quickly compute powers modulo n.
- For $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, determine whether a is invertible and, if this is the case, find a^{-1} using the extended Euclidean algorithm.
- For $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, solve the linear equation $\overline{a}x = \overline{b}$

1.1 Find the prime factorisation of an integer

Method.

1. Start by dividing the number by the smallest prime number, which is 2.
2. If the number is divisible by 2, divide it by 2 and continue dividing by 2 until you get an odd number.
3. Then, divide the number by the smallest prime number greater than 2, which is 3.
4. Continue dividing by the smallest prime number greater than 2 until you get a prime number.
5. The prime factorisation of the number is the product of all the prime numbers you used to divide the number.

Remark.
We can deduce the number of divisors of a number from its prime factorisation.
If the prime factorisation of a number is $n = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_k^{a_k}$, then the number of divisors of n is $(a_1 + 1) \times (a_2 + 1) \times \ldots \times (a_k + 1)$.

Example. Find the prime factorisation of 792.

Solution.

$$\begin{aligned} 792 &= 2 \times 396 \\ &= 2 \times 2 \times 198 \\ &= 2 \times 2 \times 2 \times 99 \\ &= 2 \times 2 \times 2 \times 3 \times 33 \\ &= 2 \times 2 \times 2 \times 3 \times 3 \times 11 \\ &= 2^3 \times 3^2 \times 11 \end{aligned}$$

We can deduce that the number of divisors of 792 is $(3 + 1) \times (2 + 1) \times (1 + 1) = 24$.

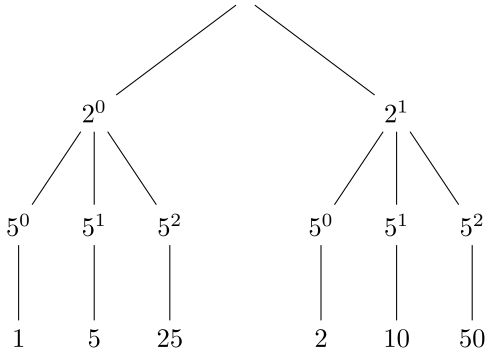
1.2 Find the set of all divisors of a given integer from its prime factorisation

Method.

1. Write the prime factorisation of the number.
2. To find the divisors of the number, consider all the possible combinations of the prime factors. We can use a tree diagram to help us.
3. The divisors of the number are the products of the prime factors in each combination.

Example. Find the set of all divisors of 50.

Solution.
The prime factorisation of 50 is $50 = 2 \times 5^2$.



The divisors of 50 are 1, 2, 5, 10, 25, and 50.

1.3 Find the gcd of two integers

Method. Using the prime factorisation

1. Find the prime factorisation of the two numbers.
2. The gcd of the two numbers is the product of the common prime factors raised to the smallest power.

Example. Find the gcd of 792 and 198.

Solution.
The prime factorisation of 792 is $792 = 2^3 \times 3^2 \times 11$ and the prime factorisation of 198 is $198 = 2 \times 3^2 \times 11$.
The gcd of 792 and 198 is $2 \times 3^2 \times 11 = 198$.

Remark.
This method is not efficient for large numbers. In this case, we can use the Euclidean algorithm.

Method. Using the Euclidean algorithm

1. Divide the larger number by the smaller number and find the remainder.
2. Replace the larger number by the smaller number and the smaller number by the remainder.
3. Repeat the process until the remainder is 0.
4. The gcd of the two numbers is the last non-zero remainder.

Example. Find the gcd of 735 and 133.

Solution.

$$\begin{aligned} 735 &= 5 \times 133 + 70 \\ 133 &= 1 \times 70 + 63 \\ 70 &= 1 \times 63 + 7 \\ 63 &= 9 \times 7 + 0 \end{aligned}$$

The gcd of 735 and 133 is 7.

1.4 Find the Bézout coefficients of two integers

Method.
We can perform the extended Euclid algorithm in two different ways: by going back up the Euclidean algorithm or by using the table method.

1. **Going back up the Euclidean algorithm**:
   - (a) Perform the Euclidean algorithm.
   - (b) Write the last non-zero remainder as a linear combination of the two numbers.
   - (c) Look at the line above and write the remainder as a linear combination of the two numbers into the current formula.
   - (d) Repeat the process until you get u and v as a linear combination of a and b.
2. **Table method**:
   - (a) Make a table with 4 columns: u_k, v_k, r_k, and q_k.
   - (b) In the first 2 lines, write 1 and 0 for u_0 and v_0 and 0 and 1 for u_1 and v_1.
   - (c) Also write a for r_0 and b for r_1, and a cross for q_0 and q_1.
   - (d) Perform the Euclidean algorithm and write the next quotients in the q_k column.
   - (e) Calculate $u_k = u_{k-2} - q_k \times u_{k-1}$ and $v_k = v_{k-2} - q_k \times v_{k-1}$.
   - (f) Deduce the remainder by computing $r_k = r_{k-2} - q_k \times r_{k-1}$.
   - (g) Repeat the process until you get $r_k = 0$.
   - (h) The Bézout coefficients are the second-to-last two numbers in the u_k and v_k columns.

Recap. Contruction of the Table
Here is the general construction of the table for the extended Euclidean algorithm:

u_k	v_k	r_k	q_k
1	0	a	$\times$
0	1	b	$\times$
$u_2 = u_0 - q_2 \times u_1$	$v_2 = v_0 - q_2 \times v_1$	$r_2 = r_0 - q_2 \times r_1$	q_2
$u_3 = u_1 - q_3 \times u_2$	$v_3 = v_1 - q_3 \times v_2$	$r_3 = r_1 - q_3 \times r_2$	q_3
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$u_n = u_{n-2} - q_n \times u_{n-1}$	$v_n = v_{n-2} - q_n \times v_{n-1}$	$r_n = r_{n-2} - q_n \times r_{n-1}$	q_n

Example. Find the Bézout coefficients of 735 and 133.

Solution.
For better understanding, we reminded the Euclid algorithm that we already computed.
Using the table method, we get the following pattern:

$$\begin{aligned} 735 &= 5 \times 133 + 70 \\ 133 &= 1 \times 70 + 63 \\ 70 &= 1 \times 63 + 7 \\ 63 &= 9 \times 7 + 0 \end{aligned}$$

u_k	v_k	r_k	q_k
1	0	735	×
0	1	133	×
1	-5	70	5
-1	6	63	1
2	-11	7	1
-19	105	0	9

Computation for u_2

$$\begin{aligned} u_2 &= u_0 - q_2 \times u_1 \\ &= 1 - 5 \times 0 \\ &= 1 \end{aligned}$$

Computation for r_2

$r_2 = 1 \times 735 - 5 \times 133 = 70$

The Bézout coefficients of 735 and 133 are 2 and -11.

Remark.
We can also find this Bézout couple by going back up the Euclidean algorithm. Let's apply this method to the previous example.
As a reminder, here is the Euclidean algorithm:

$$\begin{aligned} 735 &= 5 \times 133 + 70 \\ 133 &= 1 \times 70 + 63 \\ 70 &= 1 \times 63 + 7 \\ 63 &= 9 \times 7 + 0 \end{aligned}$$

We can write the last non-zero remainder as a linear combination of 735 and 133:

$$\begin{aligned} 7 &= 70 - 1 \times 63 \\ &= 70 - 1 \times (133 - 1 \times 70) \\ &= 2 \times 70 - 1 \times 133 \\ &= 2 \times (735 - 5 \times 133) - 1 \times 133 \\ &= 2 \times 735 - 11 \times 133 \end{aligned}$$

1.5 Compute powers modulo n

Method.
To compute $a^b \mod n$, we can use the following method:

1. First, each time that one is handling a number, remplace it by its remainder modulo n (except for powers!).

2. Then, decompose b as a sum of powers of 2. In this way, we have:

$$b = 2^{k_1} + 2^{k_2} + \ldots + 2^{k_m}$$

3. Lastly, compute $a^p \equiv a^{2k_1} \times a^{2k_2} \times ... \times a^{2k_m} [n]$.

Example. Compute $\overline{27}^{25}$ in $\mathbb{Z}/11\mathbb{Z}$.

Solution.
First, we have $27 \equiv 5[11]$. Then, we can decompose 25 as $25 = 16 + 8 + 1 = 2^4 + 2^3 + 2^0$.
We can then compute:

$$\begin{aligned}
\overline{5}^1 &= \overline{5} \equiv 5[11] \\
\overline{5}^2 &= \overline{5} \times \overline{5} \equiv 5 \times 5 = 25 \equiv 3[11] \\
\overline{5}^4 &= (\overline{5}^2)^2 = \overline{3}^2 = \overline{3} \times \overline{3} \equiv 3 \times 3 = 9 \equiv 9[11] \\
\overline{5}^8 &= (\overline{5}^4)^2 = \overline{9}^2 = \overline{9} \times \overline{9} \equiv 9 \times 9 = 81 \equiv 4[11] \\
\overline{5}^{16} &= (\overline{5}^8)^2 = \overline{4}^2 = \overline{4} \times \overline{4} \equiv 4 \times 4 = 16 \equiv 5[11]
\end{aligned}$$

Therefore, $\overline{27}^{25} = \overline{5} \otimes \overline{4} \otimes \overline{5} = \overline{100} = \overline{1}$ in $\mathbb{Z}/11\mathbb{Z}$.

Remark.
In the case where $a = n - 1$, we can use the following property to simplify the computation:

$$a^b \mod n = -1^b \mod n$$

For instance, to compute $15^{2311} \mod 16$, we can write that it is equivalent to $(-1)^{2311} \mod 16$.
As 2311 is odd, we have $(-1)^{2311} = -1 \mod 16$.

1.6 Methods on invertible elements in $\mathbb{Z}/n\mathbb{Z}$

Method. Find if an element is invertible
An element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is invertible if and only if $\gcd(a, n) = 1$.

If we need to find the invertible elements in $\mathbb{Z}/n\mathbb{Z}$, we can use the following method:

1. Find the prime factorisation of n.
2. For each element a between 1 and $n - 1$, check if $\gcd(a, n) = 1$.
3. The invertible elements are the ones that satisfy this condition.

Example. Find the invertible elements in $\mathbb{Z}/24\mathbb{Z}$.

Solution.
The prime factorisation of 24 is $24 = 2^3 \times 3$.
We now need to find all the numbers not divisible by 2 or 3.
The invertible elements in $\mathbb{Z}/24\mathbb{Z}$ are 1, 5, 7, 11, 13, 17, 19, and 23.

Method. Find the inverse of an element
To find the inverse of an element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, we can use the extended Euclidean algorithm.

1. Find the Bézout coefficients of a and n such as $n \times u + a \times v = 1$.
2. The inverse of a is v.

Example. Find the inverse of $\overline{7}$ in $\mathbb{Z}/24\mathbb{Z}$.

Solution.
We have already found that 7 is invertible in $\mathbb{Z}/24\mathbb{Z}$.
Let's apply the extended Euclidean algorithm to 24 and 7:

u_k	v_k	r_k	q_k
1	0	24	×
0	1	7	×
1	-3	3	3
-2	7	1	2
7	-24	0	3

Initial value: $r_0 = 24$
Initial value: $r_1 = 7$
$r_2 = 1 \times 24 - 3 \times 7 = 3$
$r_3 = -2 \times 24 + 7 \times 7 = 1$
$r_4 = 7 \times 24 - 24 \times 7 = 0$

The inverse of $\overline{7}$ in $\mathbb{Z}/24\mathbb{Z}$ is $\overline{7}^{-1} = \overline{7}$.

1.7 Solve a linear equation in $\mathbb{Z}/n\mathbb{Z}$

Method.
Consider the equation $\overline{a} \otimes \overline{x} = \overline{b}$ where $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^2$ are the coefficients and $\overline{x}$ is the unknown. Then,

1. If $\overline{a}$ is invertible, the equation admits a unique solution, namely $\overline{x} = \overline{a}^{-1}\overline{b}$.
2. If $\overline{a}$ is not invertible and b is not a multiple of $a \wedge n$, the equation admits no solutions.
3. If $\overline{a}$ is not invertible and b is a multiple of $a \wedge n$, the equation admits exactly $a \wedge n$ different solutions.

Example. No. 1
Solve the equation $\overline{7} \otimes \overline{x} = \overline{15}$ in $\mathbb{Z}/24\mathbb{Z}$.

Solution.
We have already found that 7 is invertible in $\mathbb{Z}/24\mathbb{Z}$.
The solution to the equation is $\overline{x} = \overline{7}^{-1} \otimes \overline{15} = \overline{7} \otimes \overline{15} = \overline{105} = \overline{9}$.

Example. No. 2
Solve the equation $\overline{3} \otimes \overline{x} = \overline{15}$ in $\mathbb{Z}/24\mathbb{Z}$.

Solution.
We have already found that 3 is not invertible in $\mathbb{Z}/24\mathbb{Z}$.
As 15 is a multiple of $3 \wedge 24 = 3$, the equation admits exactly 3 different solutions.

$$\begin{aligned} 3x \equiv 15\ [24] &\Leftrightarrow 3x \equiv 3 \times 5\ [3 \times 8] \\ &\Leftrightarrow x \equiv 5\ [8] \end{aligned}$$

So $x = 8k + 5$ where $k \in \mathbb{Z}$ and the values should be between 0 and 23.
Therefore, the solutions are $\overline{5}$, $\overline{13}$, and $\overline{21}$.

Example. No. 3
Solve the equation $\overline{3} \otimes \overline{x} = \overline{17}$ in $\mathbb{Z}/24\mathbb{Z}$.

Solution.
We have already found that 3 is not invertible in $\mathbb{Z}/24\mathbb{Z}$.
As 17 is not a multiple of $3 \wedge 24 = 3$, the equation admits no solutions.

2 Fundamentals of Cryptography

2.1 Preliminar concepts

Definition. Essential Vocabulary
Here are some essential vocabulary terms in cryptography:

- **Plaintext**: The original message that one wants to transmit.
- **Ciphertext**: The encrypted message.
- **Enciphering**: The process of converting plaintext into ciphertext.
- **Deciphering**: The process of converting ciphertext into plaintext.
- **Key**: A piece of information that controls the operation of the encryption and decryption algorithms.
- **Cryptosystem**: A system that implements encryption and decryption.
- **Cryptanalysis**: The study of methods for obtaining the meaning of encrypted information without access to the key.

Definition. Symmetric and Public Key Cryptosystems

Symmetric Cryptosystem:

- The knowledge of the enciphering key implies the knowledge of the deciphering key.
- The same key is used for both encryption and decryption.
- The key must be kept secret: it is shared between the sender and the receiver via private channels.
- It is efficient in terms on computational power.

Public Key Cryptosystem:

- The knowledge of the enciphering key does not imply the knowledge of the deciphering key.
- Two keys are used: a public key for encryption and a private key for decryption.
- The public key can be distributed to anyone. The private key must be kept secret.
- The fundamental realization that made public key cryptography possible is the existence of problems that are easy to solve in one direction but hard to solve in the opposite direction (trapdoor functions).
- It is less efficient in terms of computational power.

2.2 Encipher and decipher a message with Caesar's cipher

Definition. Caesar's Cipher (Generalized)
Caesar's cipher is a substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet.

Given an alphabet of n letters encoded as elements of $\mathbb{Z}/n\mathbb{Z}$, the enciphering transformation is given by:

$$\begin{aligned} Enc_{\overline{a},\overline{b}} : \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ \overline{x} &\mapsto \overline{a} \otimes \overline{x} \oplus \overline{b} \end{aligned}$$

where $(\overline{a}, \overline{b}) \in Inv(\mathbb{Z}/n\mathbb{Z}) \times \mathbb{Z}/n\mathbb{Z}$ is the enciphering key.
The associated deciphering key is $(\overline{a}^{-1}, -\overline{a}^{-1} \otimes \overline{b})$. In other words, the deciphering transformation is

$$\begin{aligned} Dec_{\overline{a}^{-1}, -\overline{a}^{-1}\otimes\overline{b}} : \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ \overline{y} &\mapsto \overline{a}^{-1} \otimes \overline{y} \oplus \overline{a}^{-1} \otimes \overline{-b} \end{aligned}$$

Example.
To communicate between them, Alice and Bob use an alphabet of only eleven letters: a=0, b=1, c=2, d=3, e=4, f=5, g=6, h=7, i=8, j=9, k=10. They decide to use the generalised Caesar's cipher as encryption method. Knowing that the enciphering key is $(\overline{5}, \overline{3})$:

1. Encipher the message "`decide`".
2. Decipher the message "`bggkcdcb`".

Solution.

1. Knowing that the enciphering key is $(\overline{5}, \overline{3})$, and $n = 11$, we have:

$$Enc(\overline{x}) = \overline{5} \otimes \overline{x} \oplus \overline{3}$$

Therefore, we can deduce that the ciphered letters used in the word "`decide`" are:

$$\begin{aligned} \texttt{d} &\mapsto Enc(\overline{3}) = \overline{5} \otimes \overline{3} \oplus \overline{3} = \overline{4} \oplus \overline{3} = \overline{7} = \texttt{h} \\ \texttt{e} &\mapsto Enc(\overline{4}) = \overline{5} \otimes \overline{4} \oplus \overline{3} = \overline{9} \oplus \overline{3} = \overline{1} = \texttt{b} \\ \texttt{c} &\mapsto Enc(\overline{2}) = \overline{5} \otimes \overline{2} \oplus \overline{3} = \overline{10} \oplus \overline{3} = \overline{2} = \texttt{c} \\ \texttt{i} &\mapsto Enc(\overline{8}) = \overline{5} \otimes \overline{8} \oplus \overline{3} = \overline{7} \oplus \overline{3} = \overline{10} = \texttt{k} \end{aligned}$$

Therefore, the enciphered message is "`hbckhb`".

2. To find the deciphering information, we need to compute the inverse of $\overline{5}$ in $\mathbb{Z}/11\mathbb{Z}$.

We have $\overline{5} \otimes \overline{2} = \overline{-1}$ so $\overline{5}^{-1} = \overline{-2} = \overline{9}$. This is the first element of our deciphering key.
Moreover, $\overline{9} \otimes \overline{-3} = \overline{-27} = \overline{-5}$ which is the second element of our deciphering key.

Therefore, the deciphering operation can be written as follows:

$$Dec(\overline{y}) = \overline{9} \otimes \overline{y} \ominus \overline{5}$$

Therefore, we can deduce that the deciphered letters used in the word "`bggkcdcb`" are:

$$\begin{aligned} \texttt{b} &\mapsto Dec(\overline{1}) = \overline{9} \otimes \overline{1} \ominus \overline{5} = \overline{9} \ominus \overline{5} = \overline{4} = \texttt{e} \\ \texttt{g} &\mapsto Dec(\overline{6}) = \overline{9} \otimes \overline{6} \ominus \overline{5} = \overline{10} \ominus \overline{5} = \overline{5} = \texttt{f} \\ \texttt{k} &\mapsto Dec(\overline{10}) = \overline{9} \otimes \overline{10} \ominus \overline{5} = \overline{2} \ominus \overline{5} = \overline{8} = \texttt{i} \\ \texttt{c} &\mapsto Dec(\overline{2}) = \overline{9} \otimes \overline{2} \ominus \overline{5} = \overline{7} \ominus \overline{5} = \overline{2} = \texttt{c} \\ \texttt{d} &\mapsto Dec(\overline{3}) = \overline{9} \otimes \overline{3} \ominus \overline{5} = \overline{5} \ominus \overline{5} = \overline{0} = \texttt{a} \end{aligned}$$

Therefore, the deciphered message is "`efficace`".

2.3 Determine if an affine transformation is a bijection

Method.
Let's consider an affine transformation $f_{A,b}$ defined on $(\mathbb{Z}/n\mathbb{Z})^p$.

1. The transformation is a bijection if and only if the matrix A is invertible.
2. The matrix A is invertible if and only if $\det(A) \wedge n = 1$.
3. The determinant of a 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by $\det(A) = ad - bc$.
4. If the transformation is a bijection, the inverse transformation is given by
$$(f_{A,b})^{-1}y = A^{-1}y - A^{-1}b$$
5. The inverse of a 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by $A^{-1} = \frac{1}{det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Example.
Among the following affine transformations, determine those that are bijective and compute their inverse maps.

1. $f(\begin{pmatrix} \overline{x_1} \\ \overline{x_2} \end{pmatrix}) = \begin{pmatrix} \overline{7} & \overline{3} \\ \overline{-3} & \overline{4} \end{pmatrix} \begin{pmatrix} \overline{x_1} \\ \overline{x_2} \end{pmatrix} + \begin{pmatrix} \overline{2} \\ \overline{1} \end{pmatrix}$ on $(\mathbb{Z}/14\mathbb{Z})^2$
2. $g(\begin{pmatrix} \overline{x_1} \\ \overline{x_2} \end{pmatrix}) = \begin{pmatrix} \overline{8} & \overline{6} \\ \overline{139} & \overline{10} \end{pmatrix} \begin{pmatrix} \overline{x_1} \\ \overline{x_2} \end{pmatrix} + \begin{pmatrix} \overline{111} \\ \overline{27} \end{pmatrix}$ on $(\mathbb{Z}/143\mathbb{Z})^2$

Solution.

1. To know if the affine transformation is a bijection, by proposition, we need to see if $det(A) \wedge n = 1$.
Here, $n = 14$ and $det(A) = \begin{vmatrix} \overline{7} & \overline{3} \\ \overline{-3} & \overline{4} \end{vmatrix} = \overline{7} \otimes \overline{4} \ominus \overline{3} \otimes \overline{-3} = \overline{0} \ominus \overline{5} = \overline{-5} = \overline{9}$.
We have $9 \wedge 14 = 1$ so A is invertible and the transformation is a bijection.

   Now, we need to find the associate inverse map of f. In order to do that, we need to compute the inverse of A.
$$A^{-1} = \frac{1}{det(A)} \otimes \begin{pmatrix} \overline{4} & \overline{-3} \\ \overline{3} & \overline{7} \end{pmatrix} = \overline{9}^{-1} \otimes \begin{pmatrix} \overline{4} & \overline{-3} \\ \overline{3} & \overline{7} \end{pmatrix}$$
We see that $\overline{9} \otimes \overline{3} = \overline{27} = \overline{-1}$ so $\overline{9}^{-1} = \overline{-3} = \overline{11}$. Therefore:
$$A^{-1} = \overline{11} \otimes \begin{pmatrix} \overline{4} & \overline{-3} \\ \overline{3} & \overline{7} \end{pmatrix} = \begin{pmatrix} \overline{2} & \overline{9} \\ \overline{5} & \overline{7} \end{pmatrix}$$
The inverse map of f is then given by:
$$\begin{aligned} f^{-1}(\begin{pmatrix} \overline{y_1} \\ \overline{y_2} \end{pmatrix}) &= A^{-1} \begin{pmatrix} \overline{y_1} \\ \overline{y_2} \end{pmatrix} - A^{-1} \begin{pmatrix} \overline{2} \\ \overline{1} \end{pmatrix} \\ &= \begin{pmatrix} \overline{2} & \overline{9} \\ \overline{5} & \overline{7} \end{pmatrix} \begin{pmatrix} \overline{y_1} \\ \overline{y_2} \end{pmatrix} - \begin{pmatrix} \overline{2} & \overline{9} \\ \overline{5} & \overline{7} \end{pmatrix} \begin{pmatrix} \overline{2} \\ \overline{1} \end{pmatrix} \\ &= \begin{pmatrix} \overline{2} & \overline{9} \\ \overline{5} & \overline{7} \end{pmatrix} \begin{pmatrix} \overline{y_1} \\ \overline{y_2} \end{pmatrix} - \begin{pmatrix} \overline{13} \\ \overline{3} \end{pmatrix} \\ &= \begin{pmatrix} \overline{2} & \overline{9} \\ \overline{5} & \overline{7} \end{pmatrix} \begin{pmatrix} \overline{y_1} \\ \overline{y_2} \end{pmatrix} + \begin{pmatrix} \overline{1} \\ \overline{11} \end{pmatrix} \end{aligned}$$

2. Here, $n = 143$ and $det(A) = \begin{vmatrix} \overline{8} & \overline{6} \\ \overline{139} & \overline{10} \end{vmatrix} = \overline{8} \otimes \overline{10} \ominus \overline{139} \otimes \overline{6} = \overline{80} \ominus \overline{119} = \overline{-39} = \overline{104}$.
We have $104 \wedge 143 = 13 \neq 1$ so A is not invertible. Therefore, the transformation is not a bijection.

2.4 Decipher a message using Vigenère's cipher

Definition. Vigenère's Cipher (Generalized)
Mathematically, going from Caesar's cipher and its generalisation to Vigenère's cipher and its generalisation corresponds to moving from one dimension to p-dimensions.

Given an alphabet with n letters encoded as elements of $\mathbb{Z}/n\mathbb{Z}$ and an integer $p > 1$, the enciphering transformation is given by:

$$\begin{aligned} Enc_{A,b} : (\mathbb{Z}/n\mathbb{Z})^p &\to (\mathbb{Z}/n\mathbb{Z})^p \\ x &\mapsto Ax + b \end{aligned}$$

where $(A, b) \in Inv(\mathcal{M}_p(\mathbb{Z}/n\mathbb{Z})) \times (\mathbb{Z}/n\mathbb{Z})^p$ is the ciphering key.

The associated deciphering key is $(A^{-1}, -A^{-1}b)$. In other words, the deciphering transformation is

$$\begin{aligned} Dec_{A^{-1},-A^{-1}b} : (\mathbb{Z}/n\mathbb{Z})^p &\to (\mathbb{Z}/n\mathbb{Z})^p \\ x &\mapsto A^{-1}x - A^{-1}b \end{aligned}$$

Example.
To communicate between them, Anaïs and Bastien use an alphabet of only ten letters: a=0, b=1, c=2, d=3, e=4, f=5, g=6, h=7, i=8, blank=9.
To encipher their messages, they decide to use the generalised Vigenère cipher on bigrams. Bastien receives from Anaïs the ciphertext "`dfgbidfcgbdi`".
Decipher this message knowing that the enciphering key is $\left(\begin{pmatrix}\overline{8} & \overline{3}\\ \overline{9} & \overline{7}\end{pmatrix}, \begin{pmatrix}\overline{9}\\ \overline{4}\end{pmatrix}\right)$

Solution.
To find the meaning of the ciphertext, we need to find the deciphering key.
We have $n = 10$ (letters in the alphabet) and we now need to compute the inverse of the matrix A.
First, $det(A) = \begin{vmatrix}\overline{8} & \overline{3}\\ \overline{-9} & \overline{7}\end{vmatrix} = \overline{8} \otimes \overline{7} \ominus \overline{9} \otimes \overline{3} = \overline{6} \ominus \overline{7} = \overline{9}$
Therefore, we have: $A^{-1} = \frac{1}{det(A)} \otimes \begin{pmatrix}\overline{7} & \overline{-3}\\ \overline{-9} & \overline{8}\end{pmatrix} = \overline{9}^{-1} \otimes \begin{pmatrix}\overline{7} & \overline{-3}\\ \overline{-9} & \overline{8}\end{pmatrix}$
We notice that $\overline{9} \otimes \overline{9} = \overline{81} = \overline{1}$ so $\overline{9}^{-1} = \overline{9}$ and we have:

$$A^{-1} = \overline{9} \otimes \begin{pmatrix}\overline{7} & \overline{-3}\\ \overline{-9} & \overline{8}\end{pmatrix} = \begin{pmatrix}\overline{3} & \overline{3}\\ \overline{9} & \overline{2}\end{pmatrix}$$

We now need to find the second element of our deciphering key, so we compute the following operation:

$$-A^{-1} \otimes b = \begin{pmatrix}\overline{-3} & \overline{-3}\\ \overline{-9} & \overline{-2}\end{pmatrix} \otimes \begin{pmatrix}\overline{9}\\ \overline{4}\end{pmatrix} = \begin{pmatrix}\overline{1}\\ \overline{1}\end{pmatrix}$$

We can now decipher each digraph of the ciphertext:

$$\texttt{df} \mapsto Dec(\begin{pmatrix}\overline{3}\\ \overline{5}\end{pmatrix}) = \begin{pmatrix}\overline{3} & \overline{3}\\ \overline{9} & \overline{2}\end{pmatrix}\begin{pmatrix}\overline{3}\\ \overline{5}\end{pmatrix} + \begin{pmatrix}\overline{1}\\ \overline{1}\end{pmatrix} = \begin{pmatrix}\overline{5}\\ \overline{8}\end{pmatrix} = \texttt{fi}$$

$$\texttt{gb} \mapsto Dec(\begin{pmatrix}\overline{6}\\ \overline{1}\end{pmatrix}) = \begin{pmatrix}\overline{3} & \overline{3}\\ \overline{9} & \overline{2}\end{pmatrix}\begin{pmatrix}\overline{6}\\ \overline{1}\end{pmatrix} + \begin{pmatrix}\overline{1}\\ \overline{1}\end{pmatrix} = \begin{pmatrix}\overline{2}\\ \overline{7}\end{pmatrix} = \texttt{ch}$$

$$\texttt{id} \mapsto Dec(\begin{pmatrix}\overline{8}\\ \overline{3}\end{pmatrix}) = \begin{pmatrix}\overline{3} & \overline{3}\\ \overline{9} & \overline{2}\end{pmatrix}\begin{pmatrix}\overline{8}\\ \overline{3}\end{pmatrix} + \begin{pmatrix}\overline{1}\\ \overline{1}\end{pmatrix} = \begin{pmatrix}\overline{4}\\ \overline{9}\end{pmatrix} = \texttt{e␣}$$

$$\texttt{fc} \mapsto Dec(\begin{pmatrix}\overline{5}\\ \overline{2}\end{pmatrix}) = \begin{pmatrix}\overline{3} & \overline{3}\\ \overline{9} & \overline{2}\end{pmatrix}\begin{pmatrix}\overline{5}\\ \overline{2}\end{pmatrix} + \begin{pmatrix}\overline{1}\\ \overline{1}\end{pmatrix} = \begin{pmatrix}\overline{2}\\ \overline{0}\end{pmatrix} = \texttt{ca}$$

$$\texttt{gb} \mapsto Dec(\begin{pmatrix}\overline{6}\\ \overline{1}\end{pmatrix}) = \begin{pmatrix}\overline{3} & \overline{3}\\ \overline{9} & \overline{2}\end{pmatrix}\begin{pmatrix}\overline{6}\\ \overline{1}\end{pmatrix} + \begin{pmatrix}\overline{1}\\ \overline{1}\end{pmatrix} = \begin{pmatrix}\overline{2}\\ \overline{7}\end{pmatrix} = \texttt{ch}$$

$$\texttt{di} \mapsto Dec(\begin{pmatrix}\overline{3}\\ \overline{8}\end{pmatrix}) = \begin{pmatrix}\overline{3} & \overline{3}\\ \overline{9} & \overline{2}\end{pmatrix}\begin{pmatrix}\overline{3}\\ \overline{8}\end{pmatrix} + \begin{pmatrix}\overline{1}\\ \overline{1}\end{pmatrix} = \begin{pmatrix}\overline{4}\\ \overline{4}\end{pmatrix} = \texttt{ee}$$

The deciphered message is "`fiche cachee`".

3 RSA Cryptosystem

3.1 Compute Euler's totient function

Method.
Euler's totient function $\varphi(n)$ is defined as the number of positive integers less than n that are coprime to n.

To compute $\varphi(n)$, we can use the following properties:

1. If p is a prime number and $\alpha \in \mathbb{N}^*$, then $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.
2. If a and b are relatively prime, then $\varphi(ab) = \varphi(a)\varphi(b)$.

Example.
Compute $\varphi(51)$ and $\varphi(200)$.

Solution.
• We have 51 (not a prime number) that we can decompose as 3×17 where 3 and 17 are relatively prime.

$$\varphi(51) = \varphi(3)\varphi(17) = (2 \times 3^0) \times (16 \times 17^0) = 2 \times 16 = 32$$

• We have 200 (not a prime number) that we can decompose as $2^3 \times 5^2$ where 2 and 5 are relatively prime.

$$\varphi(200) = \varphi(2^3)\varphi(5^2) = (1 \times 2^2) \times (4 \times 5^1) = 80$$

3.2 Solve equations of the shape $x^e \equiv a\ [n]$

Remark.
Warning! The following method only works if n is a product of **distinct** prime numbers.

Method.
To solve the equation $x^e \equiv a\ [n]$, we can use the following method:

1. Compute $\varphi(n)$.
2. Find the inverse of e modulo $\varphi(n)$ using the extended Euclidean algorithm.
3. The solutions are given by $x \equiv a^d\ [n]$ where d is the inverse of e modulo $\varphi(n)$.

Example.
Solve the equation $x^9 = \overline{11}$ in $\mathbb{Z}/102\mathbb{Z}$

Solution.
We have $n = 102 = 2 \times 3 \times 17$ where 2, 3, and 17 are distinct prime numbers so the method applies.
We can compute $\varphi(102) = \varphi(2)\varphi(3)\varphi(17) = 1 \times 2 \times 16 = 32$.
We now look for integer solutions to $9u + 32v = 1$, which is possible since $9 \wedge 32 = 1$, using the extended Euclidean algorithm:

u_k	v_k	r_k	q_k
0	1	32	×
1	0	9	×
-3	1	5	3
4	-1	4	1
-7	2	1	1

Initial value: $r_0 = 32$
Initial value: $r_1 = 9$
$r_2 = -3 \times 9 + 1 \times 32 = 5$
$r_3 = 4 \times 9 - 1 \times 32 = 4$
$r_4 = -7 \times 9 + 2 \times 32 = 1$

So we see that $9 \times (-7) \equiv 1\ [32] \Leftrightarrow 9 \times 25 \equiv 1\ [32]$.
Therefore, $x^9 = \overline{11} \Leftrightarrow x \equiv \overline{11}^{25}$. We use the repeated squares to compute this operation.

k	1	2	4	8	16
$\overline{11}^k$	$\overline{11}$	$\overline{19}$	$\overline{55}$	$\overline{67}$	$\overline{1}$

So $\overline{11}^{25} = \overline{11}^{1+8+16} = \overline{11} \otimes \overline{67} \otimes \overline{1} = \overline{23}$.
Therefore, the solutions to the equation are $\overline{23}$ in $\mathbb{Z}/102\mathbb{Z}$.

3.3 Apply the RSA cryptosystem

Definition.
The RSA cryptosystem is based on the following steps:

1. Agent A starts by randomly choosing two prime numbers p_A and q_A and computes their product $n_A = p_A q_A$.
2. A chooses randomly yet another number e_A such that $e_A \wedge \varphi(n_A) = 1$.
3. The ciphering transformation, used by all other agents, to send messages to A, is defined by:
$$\begin{aligned} Enc_{n_A,e_A} : \mathbb{Z}/n_A\mathbb{Z} &\to \mathbb{Z}/n_A\mathbb{Z} \\ \overline{x} &\mapsto \overline{x}^{e_A} \end{aligned}$$
The public key, known to all, that contains all the information needed to send ciphered messages to A, is therefore the couple $(n_A, e_A) \in \mathbb{N} \times Inv(\mathbb{Z}/\varphi(n_A)\mathbb{Z})$.
4. The deciphering transformation, used by A alone to decipher the messages she receives, is:
$$\begin{aligned} Dec_{d_A} : \mathbb{Z}/n_A\mathbb{Z} &\to \mathbb{Z}/n_A\mathbb{Z} \\ \overline{y} &\mapsto \overline{y}^{d_A} \end{aligned}$$
The private key, known only to A, that contains all the information needed to decipher the messages received by A, is therefore $d_A \in Inv(\mathbb{Z}/\varphi(n_A)\mathbb{Z})$.
5. The link between the public and private key is given by $e_A d_A \equiv 1\ [\varphi(n_A)]$.

Remark. Checking the data
To check if the data is correct, we need to verify these conditions:

1. n_A is the product of two distinct prime numbers.
2. e_A is such that $e_A \wedge \varphi(n_A) = 1$.
3. $e_A d_A \equiv 1\ [\varphi(n_A)]$.

Example.
Alice and Bob use the RSA cryptosystem to exchange messages securely. The informations known by Alice are the following:

	Alice	**Bob**
Public key	$n_A = 55$	$n_B = 143$
	$e_A = 3$	$e_B = 7$
Private key	$d_A = 27$	$d_B = ??$

1. Check Alice's data.
2. Alice wants to send the plaintext $x = 12$ to Bob. Determine the ciphertext that she must send to Bob.
3. Alice receives the ciphertext $y = 50$. Decipher it.
4. In this simple example, Bob's private key is not so secret... Find it.

Solution.

1. We have $n_A = 55 = 5 \times 11$ which is a product of two distinct prime numbers.
Also $\varphi(55) = \varphi(5)\varphi(11) = 4 \times 10 = 40$ and $e_A = 3$ is such that $3 \wedge 40 = 1$.
Finally, we have $e_A d_A = 3 \times 27 = 81 \equiv 1\ [40]$.
So Alice's data is correct.

2. To send the plaintext $x = 12$ to Bob, Alice uses Bob's public key. She computes:

$$y \equiv x^{e_B}[n_B] \equiv 12^7[143] = \overline{12}$$

Therefore, Alice must send the ciphertext $y = 12$ to Bob.

3. To decipher the message $y = 50$, Alice uses her own private key. She computes:

$$x \equiv y^{d_A}[n_A] \equiv 50^{27}[55]$$

We use the repeated squares to compute this operation.

k	1	2	4	8	16
$\overline{50}^k$	$\overline{50}$	$\overline{25}$	$\overline{20}$	$\overline{15}$	$\overline{5}$

So $\overline{50}^{27} = \overline{50}^{1+2+8+16} = \overline{50} \otimes \overline{25} \otimes \overline{15} \otimes \overline{5} = \overline{30}$.
Therefore, the plaintext message is $x = 30$.

4. We know that the link between the public and private key is given by $e_B d_B \equiv 1\ [\varphi(n_B)]$.
First, we compute $\varphi(143) = \varphi(11)\varphi(13) = 10 \times 12 = 120$.
We now look for integer solutions to $7 \times d_B \equiv 1\ [120]$, which is possible since $7 \wedge 120 = 1$. We use the extended Euclidean algorithm:

$$120 = 7 \times 17 + 1 \Rightarrow 1 = 120 - 7 \times 17$$

Finally, $\overline{-17} = \overline{103}$ so $d_B = 103$ is Bob's private key.

3.4 Apply the RSA authentication procedure

Definition.
Let (n_A, e_A) and (n_B, e_B) be the public keys of A and B, and d_A, d_B their private keys. Moreover, let s_A be A's plain signature. For A to prove its identity to B, they perform the following operations:

- If $n_A \leq n_B$:
  - A computes $y_{AB} \equiv (s_A^{d_A}\ [n_A])^{e_B}\ [n_B]$ to send the signature to B.
  - B checks that $s_A \equiv ((y_{AB})^{d_B}\ [n_B])^{e_A}\ [n_A]$ to verify A's identity.
- If $n_A \geq n_B$:
  - A computes $y_{AB} \equiv (s_A^{e_B}\ [n_B])^{d_A}\ [n_A]$ to send the signature to B.
  - B checks that $s_A \equiv ((y_{AB})^{e_A}\ [n_A])^{d_B}\ [n_B]$ to verify A's identity.

If the equality holds, A has proven its identity to B.

Remark. Mnemonic trick
To easily remember the correct formula to use, you can do the following.

For **encryption** :

1. Look at who is sending his identity, using his private key, and who is the recipient, using the recipient's public key.
2. Always 'keep side by side' the key and its associated modulo (data from the same person in the same operation).
3. Always start by 'processing' the data with the **smallest modulo**.

For **decryption**, the approach is similar, although you use your own private key and the public key of the person sending you the message. In addition, we start with the data with the **largest modulo**.

Example.
Altaïr and Bharani use the RSA cryptosystem. You are given the data below:

	Altaïr	**Bharani**
Public key	$n_A = 209$	$n_B = 221$
	$e_A = 13$	$e_B = 25$
Private key	$d_A = ??$	$d_B = ??$
Signature	$s_A = 10$	$s_B = 21$

1. Find Altaïr's and Bharani's private keys.
2. Find the message that Altaïr must send to Bharani to prove her his identity.
3. Altaïr receives a message, supposedly from Bharani, with the following ciphered signature: $y_{BA} = 98$. Is this message really coming from Bharani?

Solution.
1. Let's first find Altaïr's private key. We have $\varphi(209) = \varphi(11)\varphi(19) = 10 \times 18 = 180$.
We now look for integer solutions to $13 \times d_A \equiv 1\ [180]$, which is possible since $13 \wedge 180 = 1$, using the extended Euclidean algorithm:

u_k	v_k	r_k	q_k
1	0	180	×
0	1	13	×
1	-13	11	13
-1	14	2	1
6	-83	1	5

Initial value: $r_0 = 180$
Initial value: $r_1 = 13$
$r_2 = 1 \times 180 - 13 \times 13 = 11$
$r_3 = -1 \times 180 + 14 \times 13 = 2$
$r_4 = 6 \times 180 - 83 \times 13 = 1$

So we have $13 \times (-81) \equiv 1\ [180] \Leftrightarrow 13 \times 97 \equiv 1\ [180]$.
Therefore, Altaïr's private key is $d_A = 97$.

Now, let's find Bharani's private key. We have $\varphi(221) = \varphi(13)\varphi(17) = 12 \times 16 = 192$.
We now look for integer solutions to $25 \times d_B \equiv 1\ [192]$, which is possible since $25 \wedge 192 = 1$, using the extended Euclidean algorithm:

u_k	v_k	r_k	q_k
1	0	192	×
0	1	25	×
1	-7	17	7
-1	8	8	1
3	-23	1	2

Initial value: $r_0 = 192$
Initial value: $r_1 = 25$
$r_2 = 1 \times 192 - 25 \times 7 = 17$
$r_3 = -1 \times 192 + 8 \times 25 = 8$
$r_4 = 3 \times 192 - 23 \times 25 = 1$

So we have $25 \times (-23) \equiv 1\ [192] \Leftrightarrow 25 \times 169 \equiv 1\ [192]$.
Therefore, Bharani's private key is $d_B = 169$.

2. To prove his identity to Bharani, Altaïr will send a message using his signature. As $n_A \leq n_B$, Altaïr computes:

$$y_{AB} \equiv (s_A^{d_A}\ [n_A])^{e_B}\ [n_B] \equiv (10^{97}\ [209])^{25}\ [221]$$

We first compute what's inside the parenthesis using the repeated squares.

k	1	2	4	8	16	32	64
$\overline{10}^k$	$\overline{10}$	$\overline{100}$	$\overline{177}$	$\overline{188}$	$\overline{23}$	$\overline{111}$	$\overline{199}$

So $\overline{10}^{97} = \overline{10}^{1+32+64} = \overline{10} \otimes \overline{111} \otimes \overline{199} = \overline{186}$.
We now need to compute $186^{25}\ [221]$ also using the repeated squares.

k	1	2	4	8	16
$\overline{186}^k$	$\overline{186}$	$\overline{120}$	$\overline{35}$	$\overline{120}$	$\overline{35}$

So $\overline{186}^{25} = \overline{186}^{1+8+16} = \overline{186} \otimes \overline{120} \otimes \overline{35} = \overline{186}$.
Therefore, Altaïr must send the message $y_{AB} = 186$ to Bharani.

3. To check if the message $y_{BA} = 98$ is really coming from Bharani, as $n_A \leq n_B$, Altaïr computes:

$$s_B \equiv ((y_{BA})^{e_B}\ [n_B])^{d_A}\ [n_A] \equiv (98^{25}\ [221])^{97}\ [209]$$

We first compute what's inside the parenthesis using the repeated squares.

k	1	2	4	8	16
$\overline{98}^k$	$\overline{98}$	$\overline{101}$	$\overline{35}$	$\overline{120}$	$\overline{35}$

So $\overline{98}^{25} = \overline{98}^{1+8+16} = \overline{98} \otimes \overline{120} \otimes \overline{35} = \overline{98}$.
We now need to compute $98^{97}\ [209]$ also using the repeated squares.

k	1	2	4	8	16	32	64
$\overline{98}^k$	$\overline{98}$	$\overline{199}$	$\overline{100}$	$\overline{177}$	$\overline{188}$	$\overline{23}$	$\overline{111}$

So $\overline{98}^{97} = \overline{21}^{1+32+64} = \overline{98} \otimes \overline{23} \otimes \overline{111} = \overline{21}$.
As this is the same as Bharani's signature, the message is indeed coming from Bharani.

4 Diffie-Hellman-Elgamal

4.1 Prove that a set is a group

Method.
To prove that a set G equipped with a binary operation Δ is a group, we need to verify the following axioms:

1. **Closure:** For all $a, b \in G$, $a\Delta b \in G$.
2. **Associativity:** For all $a, b, c \in G$, $(a\Delta b)\Delta c = a\Delta(b\Delta c)$.
3. **Identity element:** There exists an element $e \in G$ such that for all $a \in G$, $a\Delta e = e\Delta a = a$.
4. **Inverse element:** For all $a \in G$, there exists an element $a^{-1} \in G$ such that $a\Delta a^{-1} = a^{-1}\Delta a = e$.

Remark.
As the definition suggests, if one of those axioms isn't verified then the set is not a group. So, for every proof, we must verify the axioms from the easiest to the hardest. Here is the order in which we should verify them:

1. **Closure:** This one is generally straightforward to verify.
2. **Identity element:** This is also generally easy to check and help us verify the next axiom.
3. **Inverse element:** We need the knowledge of the identity element to verify this axiom.
4. **Associativity:** This can be a long computation, so to not waste time we should verify it last.

Example. No. 1
Find if the following subset of $\mathbb{Z}/17\mathbb{Z}$ form a group under the multiplication $\otimes$:

$$E = \{\overline{1}, \overline{4}, \overline{13}, \overline{16}\}$$

Solution.
Step 1: Closure
To verify closure, we must check that the product of any two elements of E_2 remains in E_2.

- Multiplying by $\overline{1}$ (the potential identity) is straightforward:

  $$\overline{1} \cdot \overline{1} = \overline{1}, \quad \overline{1} \cdot \overline{4} = \overline{4}, \quad \overline{1} \cdot \overline{13} = \overline{13}, \quad \overline{1} \cdot \overline{16} = \overline{16}.$$

  All results are in E_2.
- Now consider $\overline{4}$:

  $$\overline{4} \cdot \overline{4} = \overline{16}, \quad \overline{4} \cdot \overline{13} = \overline{52} = \overline{1}, \quad \overline{4} \cdot \overline{16} = \overline{64} = \overline{13}.$$

  All products involving $\overline{4}$ stay in E_2.
- Next, $\overline{13}$:

  $$\overline{13} \cdot \overline{13} = \overline{169} = \overline{16}, \quad \overline{13} \cdot \overline{16} = \overline{208} = \overline{4}.$$

  Again, all remain in E_2.
- Finally, $\overline{16}$:

  $$\overline{16} \cdot \overline{16} = \overline{256} = \overline{1}.$$

From all these checks, every product of two elements in E_2 lies in E_2. Thus, E_2 is closed under multiplication mod 17.

Step 2: Existence of Identity
For a set to be a group under an operation, it must contain an identity element. In $\mathbb{Z}/17\mathbb{Z}$, the multiplicative identity is $\overline{1}$.

Since $\overline{1} \in E_2$, the identity element is present in E_2.

Step 3: Existence of Inverses
Each element must have a multiplicative inverse in E_2:

- $\overline{1}$ is its own inverse since $\overline{1} \cdot \overline{1} = \overline{1}$.
- From our closure checks:
$$\overline{4} \cdot \overline{13} = \overline{1} \implies \overline{4}^{-1} = \overline{13} \text{ and } \overline{13}^{-1} = \overline{4}.$$
- Also, $\overline{16} \cdot \overline{16} = \overline{1}$ implies $\overline{16}^{-1} = \overline{16}$.

Thus, each element has an inverse within E_2.

Step 4: Associativity
Associativity of multiplication modulo 17 is inherited from the associativity of integer multiplication. Since all elements of E_2 are in $\mathbb{Z}/17\mathbb{Z}$, and the operation is the standard multiplication modulo 17, associativity is guaranteed.

Conclusion
All four group axioms are satisfied. Therefore, $E_2 = \{\overline{1}, \overline{4}, \overline{13}, \overline{16}\}$ is indeed a group under multiplication modulo 17.

Example. No. 2
Consider the set $\mathbb{N}$ equipped with the operation $\odot$ defined by

$$\forall a, b \in \mathbb{N}, a \odot b = a^b$$

Find if $(\mathbb{N}, \odot)$ is a group.

Solution.
Let's check the identity element first. We need to find an element $e \in \mathbb{N}$ such that the operation should satify the following conditions:

- $\forall a \in \mathbb{N}, a^e = a$
- $\forall a \in \mathbb{N}, e^a = a$

The first equation is satisfied only if $e = 1$. However, the second equation is not satisfied for $a = 2$ since $1^2 = 1 \neq 2$. Therefore, the identity axiom is not verified and $(\mathbb{N}, \odot)$ is not a group.

4.2 Find if a group of the shape $(Inv(\mathbb{Z}/n\mathbb{Z}), \otimes)$ is cyclic

We will begin this section by some definitions and properties that will be useful to understand the following examples.

Definition. Order of an element
The order of an element a in a group (G, Δ) is the smallest positive integer n such that $a^n = e$ where e is the identity element of the group.

Definition. Cyclic group
A group (G, Δ) is said to be cyclic if there exists an element $g \in G$ such that every element of G can be written as a power of g. In this case g is called a generator of G.

Proposition.
One can prove that all cyclic groups are finite. Therefore, the following is an equivalent definition of a group generator: if (G, Δ) is a finite group with n elements, then g is a generator of G if and only if $\text{Ord}(g) = n$.

Proposition.
The set $Inv(\mathbb{Z}/n\mathbb{Z})$ of invertible classes of $\mathbb{Z}/n\mathbb{Z}$, equipped with the multiplication $\otimes$, is a finite commutative group with $\varphi(n)$ elements.
According to Euler's theorem, the order of an element of $Inv(\mathbb{Z}/n\mathbb{Z})$ must be a divisor of $\varphi(n)$.

We should also note that if n is prime, then $Inv(\mathbb{Z}/n\mathbb{Z})$ is a cyclic group.

Method.
To solve this type of problems, we need to solve this in five steps:

1. Find the number of elements in the group: this is given by $\varphi(n)$.
2. List these elements, find their inverses.
3. For $\varphi(n) > 2$, if every element is equal to its inverse, then the group is not cyclic (orders are 1 or 2) and we don't compute the next steps.
4. Else, find the order of each element: you can use Euler's theorem to facilitate this step.
5. If at least one element has an order equal to $\varphi(n)$, then the group is cyclic.

Example. No. 1
Find if the group $(Inv(\mathbb{Z}/11\mathbb{Z}), \otimes)$ is cyclic.

Solution.
The group $Inv(\mathbb{Z}/11\mathbb{Z})$ has $\varphi(11) = 10$ elements. These elements are $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}\}$. We can compute their inverses:

$$\begin{array}{ccccc}
\overline{1}^{-1} = \overline{1} & \overline{2}^{-1} = \overline{6} & \overline{3}^{-1} = \overline{4} & \overline{4}^{-1} = \overline{3} & \overline{5}^{-1} = \overline{9} \\
\overline{6}^{-1} = \overline{2} & \overline{7}^{-1} = \overline{8} & \overline{8}^{-1} = \overline{7} & \overline{9}^{-1} = \overline{5} & \overline{10}^{-1} = \overline{10}
\end{array}$$

Let us look at the orders of the elements. According to Euler's theorem, the order of an element must be a divisor of $\varphi(11) = 10$. So the possible orders are 1, 2, 5, and 10. We can compute the orders of the elements:

- Ord$(\overline{1}) = 1$ (trivial)
- $\overline{2}^2 = \overline{4}, \overline{2}^5 = \overline{10}, \overline{2}^{10} = \overline{1} \Rightarrow$ Ord$(\overline{2}) = 10$, also we have Ord$(a) =$ Ord(a^{-1}) so Ord$(\overline{6}) = 10$
- $\overline{3}^2 = \overline{9}, \overline{3}^5 = \overline{1} \Rightarrow$ Ord$(\overline{3}) = 5$, also Ord$(\overline{4}) = 5$
- $\overline{5}^2 = \overline{3}, \overline{5}^5 = \overline{1} \Rightarrow$ Ord$(\overline{5}) = 5$, also Ord$(\overline{9}) = 5$
- $\overline{7}^2 = \overline{5}, \overline{7}^5 = \overline{10}, \overline{7}^{10} = \overline{1} \Rightarrow$ Ord$(\overline{7}) = 10$, also Ord$(\overline{8}) = 10$
- $\overline{10}^2 = \overline{1} \Rightarrow$ Ord$(\overline{10}) = 2$

The generators of the group are the elements with an order equal to $\varphi(11) = 10$. They are $\overline{2}, \overline{6}, \overline{7}, \overline{8}$. Therefore, because there is at least one generator, the group $(Inv(\mathbb{Z}/11\mathbb{Z}), \otimes)$ is cyclic.

Remark.
We should note that it was not necessary to compute the orders of all the elements in the previous example. We could have stopped as soon as we found a generator to prove that the group is cyclic.

Example. No. 2
Find if the group $(Inv(\mathbb{Z}/12\mathbb{Z}), \otimes)$ is cyclic.

Solution.
The group $Inv(\mathbb{Z}/12\mathbb{Z})$ has $\varphi(12) = 4$ elements. These elements are $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. We can compute their inverses:

$$\overline{1}^{-1} = \overline{1} \qquad \overline{5}^{-1} = \overline{5} \qquad \overline{7}^{-1} = \overline{7} \qquad \overline{11}^{-1} = \overline{11}$$

As every element is equal to its inverse, this shows that all elements of Inv$(\mathbb{Z}/12\mathbb{Z}, \otimes)$ are of order either 1 or 2. Therefore, the group is not cyclic.

4.3 Apply the Elgamal cryptosystem

Definition.
The Elgamal cryptosystem is based on the following steps:

1. We start by choosing a cyclic group (G, Δ) with a generator g: this constitutes the public domain (known to all).

2. The agent A starts by choosing randomly an integer d_A between 2 and $n-1$, which is kept secret, and publishes the element $e_A = g^{d_A}$ (known to all).

3. To send a message to A, agent B chooses randomly a second integer k between 2 and $n-1$, which is kept secret, computes the element $r = g^k$, uses the enciphering transformation:

$$\begin{aligned} \text{Enc}_{e_A,k} : Inv(\mathbb{Z}/n\mathbb{Z}) &\to Inv(\mathbb{Z}/n\mathbb{Z}) \\ x &\mapsto y = x\Delta(e_A)^k \end{aligned}$$

   and sends to A the ciphertext (r, y).

   The public key, known to all, that contains all the information needed to send ciphered messages to A, is therefore the element $e_A \in Inv(\mathbb{Z}/n\mathbb{Z})$.

4. If the received ciphertext is $(r, y) \in Inv(\mathbb{Z}/n\mathbb{Z}) \times Inv(\mathbb{Z}/n\mathbb{Z})$, agent A uses the deciphering transformation:

$$\begin{aligned} \text{Dec}_{d_A} : Inv(\mathbb{Z}/n\mathbb{Z}) &\to Inv(\mathbb{Z}/n\mathbb{Z}) \\ y &\mapsto y\Delta(r^{d_A})^{-1} \end{aligned}$$

   The private key, known only to A, that contains all the information needed to decipher the messages received by A, is the number $2 \leq d_A \leq n-1$.

5. The link between the public and private key is

$$e_A = g^{d_A} \iff d_A = \log_g(e_A).$$

Remark. Checking the data
To check the data of the Elgamal cryptosystem, we need to verify the following:

1. The public domain is a group $(Inv(\mathbb{Z}/n\mathbb{Z}), \otimes)$.

2. The generator g is indeed a generator of the group.

3. The link between the public and private key is correct.

Example.
Alexandre and Bernard use the Elgamal cryptosystem to exchange messages. The table below shows the data known to Alexandre:

	Alexandre	**Bernard**
Public domain	$(\mathbb{F}_{23}^*, \overline{7})$	
Public key	$e_A = \overline{13}$	$e_B = \overline{15}$
Private key	$d_A = 10$	$d_B = ??$

1. Check all the data.
2. Alexandre wishes to send the plaintext $x = \overline{12}$ to Bernard. Find the ciphertext that Alexandre must send (suppose he chooses $k = 7$).
3. Alexandre receives from Bernard the ciphertext $(r, y) = (\overline{20}, \overline{11})$. Find the plaintext.
4. In this simple example, the private key is not so secret... Find it.

Solution.
1. The public domain tells us that the cyclic group in use is $(\mathbb{F}_{23}^*, \overline{7})$ and that the chosen generator is $g = \overline{7}$. Let's verify if this is indeed a valid one.
Since $\mathbb{F}_{23}^*$ contains $\varphi(23) = 22$ elements, Euler's theorem tells us that the order of the generator must be 22. Knowing that the order of $\overline{7}$ should be a divisor of 22, it should be either 1, 2, 11, or 22. We can compute the orders of $\overline{7}$:

$$\overline{7}^2 = \overline{3}, \quad \overline{7}^{11} = \overline{22}, \quad \overline{7}^{22} = \overline{1}$$

Therefore, the order of $\overline{7}$ is indeed 22 and it is a generator of the group.

To check the link between the public and private key, we need to verify that $e_A = g^{d_A}$. We have $g = \overline{7}$, $d_A = 10$ and $e_A = \overline{13}$. We can compute g^{d_A} and notice that $\overline{7}^{10} = \overline{13}$. Therefore, the data is correct.

2. To send the plaintext $x = \overline{12}$ to Bernard, Alexandre chooses $k = 7$ and computes these two elements to get his ciphertext:

$$r = g^k = \overline{7}^7 = \overline{5} \quad \text{and} \quad y = x \otimes e_B^k = \overline{12} \otimes \overline{15}^7 = \overline{12} \otimes \overline{11} = \overline{17}$$

So Alexandre must send the ciphertext $(\overline{5}, \overline{17})$ to Bernard.

3. To decipher the message received from Bernard, Alexandre must compute $y \otimes (r^{d_A})^{-1} = \overline{11} \otimes (\overline{20}^{10})^{-1}$. Let's first compute r^{d_A} using the repeated squares:

k	1	2	4	8
$\overline{20}^k$	$\overline{20}$	$\overline{9}$	$\overline{12}$	$\overline{6}$

So $\overline{20}^{10} = \overline{20}^{2+8} = \overline{9} \otimes \overline{6} = \overline{8}$. We now need to find the inverse of $\overline{8}$ using the extended Euclidean algorithm:

u_k	v_k	r_k	q_k
1	0	23	×
0	1	8	×
1	-2	7	2
-1	3	1	1
8	-23	0	7

Initial value: $r_0 = 23$
Initial value: $r_1 = 8$
$r_2 = 23 - 8 \times 2 = 7$
$r_3 = -23 + 8 \times 3 = 1$
$r_4 = 23 \times 8 - 8 \times 23 = 0$

So $\overline{8}^{-1} = \overline{3}$. We can now compute the plaintext:

$$x = \overline{11} \otimes \overline{8}^{-1} = \overline{11} \otimes \overline{3} = \overline{10}$$

4. The link between the public and private key is $e_B = g^{d_B}$. We have $g = \overline{7}$ and $e_B = \overline{15}$. We can solve the equation $\overline{7}^{d_B} = \overline{15}$ to find d_B. Let us compute this number case by case to find d_B:

d_B	1	2	3	4	5	6	7	8	9
$\overline{7}^{d_B}$	$\overline{7}$	$\overline{3}$	$\overline{21}$	$\overline{9}$	$\overline{17}$	$\overline{4}$	$\overline{5}$	$\overline{12}$	$\overline{15}$

As we have $\overline{7}^9 = \overline{15}$, we find that $d_B = 9$.