Problem 8.1.

1. Which of the following are commutative groups? For the commutative groups, give the identity element and the inverse of any element.

   (a) $(\mathbb{Z}, \cdot)$

   Solution:

   It is not a commutative group. There is an identity element 1, but not all elements have inverses (in fact only ± 1 have an inverse).

   Relevant slides : 424 - 426

   (b) $(\mathbb{R}^n, +)$, for some fixed positive integer n, where $+$ is the componentwise addition

   Solution:

   It is a commutative group because it is a cartesian product of commutative groups. The identity element is $(0, \ldots, 0)$, and the inverse of $(a_1, \ldots, a_n)$ is $(-a_1, \ldots, -a_n)$.

   Relevant slides : 435 - 437

   (c) $(\mathbb{R}^n, \cdot)$, where $\cdot$ is the scalar product: $(u_1, \ldots, u_n) \cdot (v_1, \ldots, v_n) = \sum_{i=1}^{n} u_i v_i$

   Solution:

   This is not a commutative group. In fact the product of two elements is not an element of $\mathbb{R}^n$, but of $\mathbb{R}$.

   Relevant slides : 424 - 426

   (d) $(\{z \in \mathbb{C} | z^n = 1\}, \cdot)$, for some fixed positive integer n

   Solution:

   It is a commutative group. It is closed: if $x^n = 1$ and $y^n = 1$, then $(xy)^n = 1$. The identity element is 1 and the inverse of z is $1/z$ (which is in the group since $(1/z)^n = 1/z^n = 1/1 = 1$).

   Relevant slides : 424 - 426

   (e) $(e^{i\theta}, \cdot)$, where $\theta \in \mathbb{R}$ and i is the unit complex number such that $i^2 = -1$

   Solution:

   This is a commutative group: the operation is closed under multiplication ($e^{i\theta} e^{i\alpha} = e^{i(\theta+\alpha)}$), the identity element is $e^0 = 1$, and each element $e^{i\theta}$ has a multiplicative inverse which is $e^{-i\theta}$. ($e^{i\theta} e^{-i\theta} = e^0$.)

   Relevant slides : 424 - 426

   (f) $(\{0, 1\}, \wedge)$, where $\wedge$ is the logical "and" operation

Solution:

It is not a commutative group. 1 is the identity element but 0 does not have an inverse since $0 \wedge 1 = 0 \wedge 0 = 0$.

Relevant slides : 424 - 426

(g) $(\mathbb{Z}/5\mathbb{Z}, \cdot)$

Solution:

This is not a commutative group. The identity element is $[1]_5$ but the element $[0]_5$ has no inverse.

Relevant slides : 424 - 426

(h) $(\mathbb{Z}/5\mathbb{Z} \setminus \{[0]_5\}, \cdot)$

Solution:

This is a commutative group. It has the same table as $(\mathbb{Z}/4\mathbb{Z}, +)$ with the correspondence $[1]_5 \mapsto [0]_4$, $[2]_5 \mapsto [1]_4$, $[3]_5 \mapsto [3]_4$, $[4]_5 \mapsto [2]_4$; so it is a commutative group. The identity element is $[1]_5$, the inverse of $[2]_5$ is $[3]_5$ (and vice versa), and $[4]_5$ is its own inverse.

Relevant slides : 424 - 426

(i) $(\mathbb{Z}/5\mathbb{Z} \setminus \{[0]_5\}, +)$

Solution:

This is not a commutative group. The sum $[1]_5 + [4]_5 = [0]_5$ is not contained in the set. Also, there is no identity element.

Relevant slides : 424 - 426

2. Are the following commutative groups isomorphic? If not - prove it. If yes - give the tables and the isomorphism:

   (a) $G_1 = (\mathbb{Z}/5\mathbb{Z}^*, \cdot)$ and $H_1 = (\{z \in \mathbb{C} | z^4 = 1\}, \cdot)$

Solution:

These commutative groups are isomorphic. The first group is $\{[1]_5, [2]_5, [3]_5, [4]_5\}$ with multiplication modulo 5, while the second group is $\{1, -1, i, -i\}$ with complex multiplication. The associated tables are:

G_1	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

H_1	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

The commutative groups are isomorphic via the correspondence

$$[1]_5 \longmapsto 1$$
$$[2]_5 \longmapsto i$$
$$[3]_5 \longmapsto -i$$
$$[4]_5 \longmapsto -1.$$

Exchanging the images of $[2]_5$ and $[3]_5$ is also a valid solution.

Relevant slides : 444 - 446, 461

(b) $G_2 = (\mathbb{Z}/6\mathbb{Z}^*, \cdot)$ and $H_2 = (\mathbb{Z}/3\mathbb{Z}^*, \cdot)$

Solution:

The two commutative groups are isomorphic. G_2 is $\{[1]_6, [5]_6\}$ with multiplication modulo 6, while H_2 is $\{[1]_3, [2]_3\}$ with multiplication modulo 3. The corresponding tables are:

G_2	$[1]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[5]_6$
$[5]_6$	$[5]_6$	$[1]_6$

H_2	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[2]_3$	$[1]_3$

It is immediate to see that the map sending $[1]_6 \mapsto [1]_3$ and $[5]_6 \mapsto [2]_3$ is an isomorphism.

Relevant slides : 444 - 446, 461

(c) $G_3 = (\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$ and $H_3 = (\mathbb{Z}/4\mathbb{Z}, +)$
(Hint: Check the orders of the elements.)

Solution:

The two commutative groups are not isomorphic. Two isomorphic commutative groups must have the same set of orders.
The elements of the first commutative group are, $00, 01, 10, 11$, the identity element is 00. Note that, $00 = 01^2 = 10^2 = 11^2$. Therefore the orders of the elements of this commutative group is $\{1, 2, 2, 2\}$
The elements of the second commutative group are, $0, 1, 2, 3$, the identity element is 0. Note that $0 = 1^4 = 2^2 = 3^4$. Therefore the orders of the elements of this commutative group is $\{1, 2, 4, 4\}$.

Relevant slides : 444 - 446, 461

(d) $G_4 = (\mathbb{Z}/15\mathbb{Z}^*, \cdot)$ and $H_4 = (\mathbb{Z}/7\mathbb{Z}, +)$

Solution:

The two commutative groups are not isomorphic. G_4 is $\{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}, \}$ with multiplication modulo 15, while H_4 is $\{[0]_7, [1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$ with sum modulo 7. The first group has 8 elements, while the second has 7, so they cannot be isomorphic.

Relevant slides : 444 - 446, 451 - 452

Problem 8.2.

1. Compute the order of each element in the commutative group $(\mathbb{Z}/18\mathbb{Z}^*, \cdot)$.

Solution:

The elements of $\mathbb{Z}/18\mathbb{Z}^*$ are all the numbers between 0 and 17 which are coprime with 18. There are 6 such numbers, which are: $1, 5, 7, 11, 13, 17$. The period of any element should divide the cardinality of the group, so it can be $1, 2, 3$ or 6. We construct the table of powers:

x	x^2	x^3	x^6
1			
5	7	17	1
7	13	1	
11	13	17	1
13	7	1	
17	1		

Hence:

1 has order 1,

17 has order 2,

7 and 13 have order 3,

5 and 11 have order 6.

Relevant slides : 427 - 429, 455

2. Can you find an integer k such that $(\mathbb{Z}/18\mathbb{Z}^*, \cdot)$ and $(\mathbb{Z}/k\mathbb{Z}, +)$ are isomorphic? If yes, give an example of such isomorphism.

Solution:

In order to have such an isomorphism, the cardinality of the two groups should be the same, so we must have $k = 6$. Next, we check if we can make an element-to-element correspondence between the two groups such that their periods match. This is possible, and an example of such correspondence is shown in the table below:

$(\mathbb{Z}/18\mathbb{Z}^*, \cdot)$	$(\mathbb{Z}/6\mathbb{Z}, +)$	Element order
1	0	1
5	1	6
7	2	3
11	5	6
13	4	3
17	3	2

Hence, according to the theorem seen in class, the two groups are isomorphic, and the isomorphism is given by the correspondence table above.

Relevant slides : 444 - 446, 461

Problem 8.3.

1. Show that (x, y) is invertible in $(\mathbb{Z}/17\mathbb{Z}, \cdot) \times (\mathbb{Z}/121\mathbb{Z}, \cdot)$ if and only if x is invertible in $(\mathbb{Z}/17\mathbb{Z}, \cdot)$ and y is invertible in $(\mathbb{Z}/121\mathbb{Z}, \cdot)$.

   Solution:

   Let $(x, y) \in (\mathbb{Z}/17\mathbb{Z}, \cdot) \times (\mathbb{Z}/121\mathbb{Z}, \cdot)$ be an invertible element. Then there exists (a, b) such that $(a, b)(x, y) = (1, 1)$. But $(a, b)(x, y) = (ax, by)$. Therefore, we have $ax = [1]_{17}$ and $by = [1]_{121}$ which implies that x is invertible in $(\mathbb{Z}/17\mathbb{Z}, \cdot)$ and y is invertible in $(\mathbb{Z}/121\mathbb{Z}, \cdot)$.
   Conversely, if x is invertible in $(\mathbb{Z}/17\mathbb{Z}, \cdot)$ and y is invertible in $(\mathbb{Z}/121\mathbb{Z}, \cdot)$, with a and b being their corresponding inverses, then (a, b) is the inverse of (x, y) in $(\mathbb{Z}/17\mathbb{Z}, \cdot) \times (\mathbb{Z}/121\mathbb{Z}, \cdot)$.

   Relevant slides : 437 - 439

2. How many invertible elements are in $(\mathbb{Z}/17\mathbb{Z}, \cdot) \times (\mathbb{Z}/121\mathbb{Z}, \cdot)$?

   Solution:

   Let M be the answer. According to the previous question, there are as many invertible elements in $(\mathbb{Z}/17\mathbb{Z}, \cdot) \times (\mathbb{Z}/121\mathbb{Z}, \cdot)$ as the pairs (x, y) where x is an invertible element in $(\mathbb{Z}/17\mathbb{Z}, \cdot)$ and y is an invertible element in $(\mathbb{Z}/121\mathbb{Z}, \cdot)$. Therefore,

   $$M = \phi(17) \times \phi(121) = 16 \cdot 110 = 1760,$$

   where we have used the fact that $\phi(121) = \phi(11^2) = 11^2 - 11$ (as seen in class, for p prime and a positive integer k, $\phi(p^k) = p^k - p^{k-1}$.)

   Relevant slides : 428 - 431, 435 - 437

3. Solve the following equation where the unknown is $n \in \mathbb{N}$:

   $$2^n \equiv 1 \mod 13$$

   Solution:

   The equation is equivalent to

   $$([2]_{13})^n = [1]_{13}$$

   The order of $[2]_{13}$ in $\mathbb{Z}/13\mathbb{Z}^*$ divides $\phi(13) = 12$. It can therefore be equal to 1, 2, 3, 4, 6 or 12. As $[2]_{13} \neq [1]_{13}$, $([2]_{13})^2 = [4]_{13} \neq [1]_{13}$, $([2]_{13})^3 = [8]_{13} \neq [1]_{13}$, $([2]_{13})^4 = [16]_{13} = [3]_{13} \neq [1]_{13}$, $([2]_{13})^6 = [64]_{13} = [12]_{13} \neq [1]_{13}$, the order of $[2]_{13}$ is 12.
   But $[2]_{13}^n = 1$ if and only if n is an integer multiple of the order. Therefore, the solutions of the equation are $\{0, 12, 24, \dots\}$, that is, the positive multiples of 12.

   Relevant slides : 455 - 457, 464

4. Solve the equation $x^{19} = x$ for $x \in (\mathbb{Z}/19\mathbb{Z}, \cdot)$.

Solution:

Since 19 is a prime number, according to Fermat's theorem, all the elements $x \in (\mathbb{Z}/19\mathbb{Z}, \cdot)$ satisfy the equation.

Relevant slide : 480

Problem 8.4.

Consider the El Gamal cryptosystem.

1. Select $p = 47$. Verify that $g = 5$ is indeed a generator of $(\mathbb{Z}/47\mathbb{Z}^*, \cdot)$.

   Solution:

   We know that the order of every element must divide the total number of elements in $(\mathbb{Z}/47\mathbb{Z}^*, \cdot)$. There are exactly 46 elements in this group. Moreover, $46 = 2 \cdot 23$. By Lagrange's theorem, this implies that elements can only have order 2, 23, or 46. We can numerically verify that $5^{23} \bmod 47 = 46$ (you can also do it by hand via smart successive squaring), thus $5^{46} \equiv (5^{23})^2 \equiv (46)^2 \bmod 47 \equiv (46)^2 \equiv (-1)^2 \equiv 1 \pmod{47}$ and therefore order$(5) = 46$, meaning that $g = 5$ is a generator.

   Relevant slide : 485

2. Alice wants to send the plaintext $t = 13$ using $g = 5$ to Bob. Alice receives from Bob $g^x \bmod 47 = 31$ (with x being Bob's secret). Alice's secret number is $y = 2$. What two integers will Alice send to Bob to share the plaintext t?

   Solution:

   Alice computes $g^y \bmod 47 = 5^2 \bmod 47 = 25$ and $g^{xy} \cdot t \bmod 47 = (g^x)^y \cdot t \bmod 47 = 31^2 \cdot 13 \bmod 47 = 21 \cdot 13 \bmod 47 = 38$. That is, Alice sends to Bob $(g^y, g^{xy} \cdot t) \bmod 47 = (25, 38)$.

   Relevant slides : 308 - 309

3. You now learn Bob's secret, $x = 3$ (indeed $g^3 \bmod 47 = 31$). Show how Bob can get back the plaintext from the two integers Alice sent him.

Solution:

To get back the plaintext:

Step 1: Compute the shared secret

$$g^{xy} = (g^y)^x = 25^3 \bmod 47 = 21$$

Step 2: Find the multiplicative inverse of $g^{xy} = 21$

One approach is to use the extended Euclidean algorithm.
Alternatively, observe that:

$$5^6 \equiv 21 \bmod 47$$

Then the inverse of 21 modulo 47 is:

$$21^{-1} \equiv (5^6)^{-1} \equiv 5^{-6} \equiv 5^{46-6} \equiv 5^{40} \equiv 9 \pmod{47}$$

Step 3: Recover the plaintext

$$t = g^{-xy} \cdot (g^{xy} \cdot t) \bmod 47 = 9 \cdot 38 \bmod 47 = 13$$

Relevant slides : 308 - 309

4. Select $p = 61$. Is $g = 9$ a good choice? Eve observes the communication between Alice and Bob:
   — Bob sends $g^x = 58$ to Alice.
   — Alice replies with $(g^y, g^{xy} \cdot t) = (34, 28)$.

   Can Eve recover the message t shared between Alice and Bob? *(Hint: Determine the order of g modulo 61.*

Solution:

Step 1: Determine the order of $g = 9$ in $\mathbb{Z}/61\mathbb{Z}$.
Compute successive powers:

$$9^1 \equiv 9 \bmod 61,$$
$$9^2 \equiv 81 \equiv 20 \bmod 61,$$
$$9^3 \equiv 9 \cdot 20 = 180 \equiv 58 \bmod 61,$$
$$9^4 \equiv 9 \cdot 58 = 522 \equiv 34 \bmod 61,$$
$$9^5 \equiv 9 \cdot 34 = 306 \equiv 1 \bmod 61.$$

So, the order of $g = 9$ is 5.
Step 2: Recover the secret exponents x and y.
Eve sees:

$$g^x = 58 \Rightarrow x \equiv 3 \pmod 5 \quad (\text{since } 9^3 \equiv 58 \bmod 61),$$

$$g^y = 34 \Rightarrow y \equiv 4 \pmod 5 \quad (\text{since } 9^4 \equiv 34 \bmod 61).$$

Step 3: Compute the shared key $g^{xy} = 9^{12}$. Since $9^5 \equiv 1$, we reduce exponent modulo 5:

$$9^{12} \equiv 9^{12 \bmod 5} \equiv 9^2 \equiv 20 \bmod 61.$$

Step 4: Recover t.
Eve sees $g^{xy} \cdot t = 28$, and now knows $g^{xy} = 20$. She computes:

$$t \equiv 28 \cdot 20^{-1} \bmod 61.$$

Compute the inverse of 20 modulo 61. Use the extended Euclidean algorithm:

$$20^{-1} \equiv (9^2)^{-1} \equiv 9^{-2} \equiv 9^{(-2 \bmod 5)} \equiv 9^3 \equiv 58 \pmod{61}$$

Finally:

$$t = 28 \cdot 58 \bmod 61 = 1634 \bmod 61 = 38.$$

Conclusion: Because $g = 9$ has a small order (5), Eve was able to recover both exponents x and y, the shared key g^{xy}, and ultimately the message t by bruteforce. This demonstrates that a generator of large order is required for strong security.

Problem 8.5.

1. Let $(G, \star)$ be a finite commutative group. Consider the following encryption method. The message that Alice wants to send to Bob is an element $t \in G$. The key is a uniformly distributed random element $k \in G$, selected independently of the message t. Alice sends the ciphertext $c = k \star t$ to Bob. Does it provide perfect secrecy?

Solution:

Suppose you are given *both* the plaintext t *and* the ciphertext c. Then, because we are in a group where every element must have an inverse (and the inverse must be unique), there is *exactly* one key k that maps the given plaintext t to the given ciphertext c as $c = k \star t$. Obviously, that key can then be written as $k = c \star t^{-1}$, where t^{-1} is the inverse (with respect to the group operation $\star$) of the element t. Now, if we consider the conditional probability that the ciphertext assumes the particular value c, given that the plaintext has assumed the particular value t, then by the above argument, this probability is precisely the same as the probability that the key is $k = c \star t^{-1}$. Moreover, the key is selected independently of everything else and uniformly distributed over all its possible values. In math, this argument is expressed as:

$$p_{C|T}(c|t) = p_{K|T}(c \star t^{-1}|t) = p_K(c \star t^{-1}) = \frac{1}{|G|}.$$

Said differently, the ciphertext C is uniformly distributed over each element of G, regardless of the plaintext. (An intuitive way to see this is to think of the key k being *shifted* by the plaintext t; since the key is uniformly distributed over the group, and the shift maps each element of a group uniquely to another element, the result of the shift is still uniformly distributed.) Hence C and T are independent. Therefore the method provides perfect secrecy.
Note that the scheme above generalises the one-time pad to an arbitrary group. (And the proof of perfect secrecy follows the same lines as in the proof for one-time pad).

Relevant slides : 286 - 287

2. Let $m > 1$ be an integer, consider a message $t \in \{0, 1, \ldots, m-1\}$ and a uniformly distributed key $k \in \{0, 1, \ldots, m-1\}$. Which of the following encryption methods provide perfect secrecy?

   (a) $c = t + k$

   Solution:

   It does not provide perfect secrecy. For instance, if $c = 0$, then we know that the plaintext was $t = 0$ and the key $k = 0$.

   (b) $c = t + k \bmod m$

   Solution:

   We are within the group $(\mathbb{Z}/m\mathbb{Z}, +)$ so according to the result in question 8.5.1, the method does provide perfect secrecy.

3. Let $m > 1$ be an integer, consider a message $t \in \{1, \ldots, m-1\}$ and a uniformly distributed key $k \in \{1, \ldots, m-1\}$. Which of the following encryption methods provide perfect secrecy?

   (a) $c = t \cdot k$

Solution:

It does not provide perfect secrecy. For instance, if $c = 1$, then we know that the plaintext was $t = 1$ and the key $k = 1$.

(b) $c = t \cdot k \bmod m$

Solution:

It provides perfect secrecy if and only if m is a prime number. Indeed, if m is prime, we are within the group $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$ and again, according to the result in question 8.5.1, the method does provide perfect secrecy. If m is not prime, then it is not an encryption: the message cannot be recovered from the ciphertext when the key k is not invertible in $\mathbb{Z}/m\mathbb{Z}^*$. For instance, with $m = 6$ and $k = 3$, the messages $t = 1$ and $t = 5$ both give the ciphertext $c = 3$.