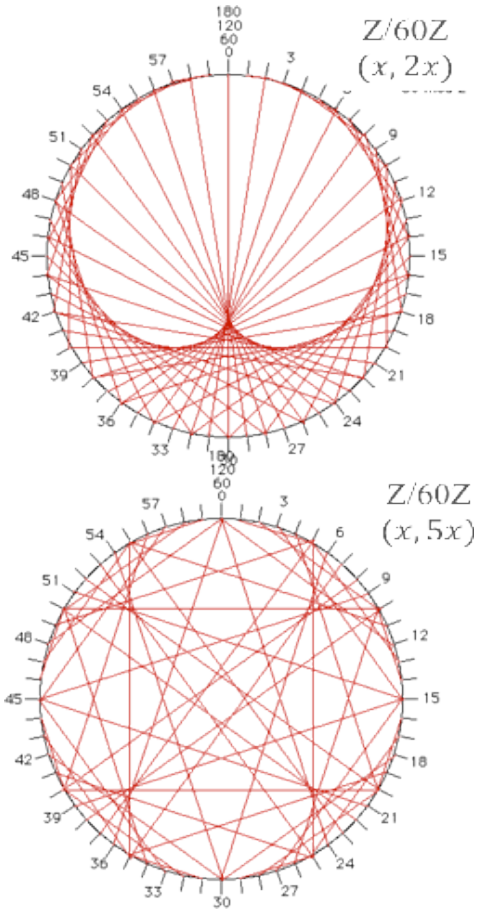
Week 8: Commutative Groups (Textbook Chapter 9)



Prof. Michael Gastpar

Slides by Prof. M. Gastpar and Prof. em. B. Rimoldi

EPFL

Spring Semester 2025

LAST WEEK

- MULTIPLICATIVE INVERSE IN $\mathbb{Z}/m\mathbb{Z}$

a has inverse $\Leftrightarrow$ $\gcd(m,a) = 1$

$\Leftrightarrow$ $ax = b$ has unique solution

FIND INVERSE VIA EXTENDED EUCLID.

Outline

After $\mathbb{Z}/m\mathbb{Z}$ we could proceed in two directions:

- focus on finite groups, which are finite sets with one operation, like $(\mathbb{Z}/m\mathbb{Z}, +)$. We do so now because we need them for cryptography.

- focus on finite fields, which are finite sets with two operations, like $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$, with the extra property that every non-zero element has a multiplicative inverse. We do so later as we need finite fields for channel coding.

We care about commutative groups because:

- they lead to exponentiation and logarithms
- which are the building blocks of various cryptographic algorithms, including DH, RSA, and ElGamal's encryption scheme.

Definition (Commutative group)

A **commutative group** (also called Abelian group) is a set G endowed with a binary operation $\star$ that combines any two elements a and b to form another element denoted $a \star b$. The group operation $\star$ must satisfy the following five axioms:

- (Closure:) For all $a, b \in G$, the result of the operation $a \star b$ is also in G.
- (Associativity:) For all $a, b \in G$, $a \star (b \star c) = (a \star b) \star c$.
- (Identity element:) There exists an element $e \in G$, such that for all $a \in G$, $a \star e = e \star a = a$.
- (Inverse element:) For all $a \in G$, there exists $b \in G$, such that $a \star b = b \star a = e$.
- (Commutativity:) For all $a, b \in G$, $a \star b = b \star a$.

EXERCISE

Which are commutative groups?

1. $(\mathbb{R}, +)$ YES
2. $(\mathbb{R}, \cdot)$ NO. because 0 has no inverse!
3. $(\mathbb{R}\backslash\{0\}, \cdot)$ YES
4. $(\mathbb{C}, +)$ YES
5. $(\mathbb{Z}/m\mathbb{Z}, +)$ YES
6. $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ NO
7. $(\mathbb{Z}/m\mathbb{Z}\backslash\{[0]_m\}, \cdot)$ If m is prime ✓ otherwise NO!
8. $(\mathbb{N}, +)$
9. $(\mathbb{Z}, +)$
10. $(\mathbb{Z}\backslash\{0\}, \cdot)$

Solution

Which are commutative groups?

1. $(\mathbb{R}, +)$: Yes.
2. $(\mathbb{R}, \cdot)$: No, 0 has no inverse.
3. $(\mathbb{R}\backslash\{0\}, \cdot)$: Yes.
4. $(\mathbb{C}, +)$: Yes.
5. $(\mathbb{Z}/m\mathbb{Z}, +)$: Yes.
6. $(\mathbb{Z}/m\mathbb{Z}, \cdot)$: No, $[0]_m$ has no inverse.
7. $(\mathbb{Z}/m\mathbb{Z}\backslash\{[0]_m\}, \cdot)$: Only if m is prime.
8. $(\mathbb{N}, +)$: No.
9. $(\mathbb{Z}, +)$: Yes.
10. $(\mathbb{Z}\backslash\{0\}, \cdot)$: No, only 1 is invertible.

$(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$

To obtain a commutative group with the modulo multiplication, we take only the elements of $\mathbb{Z}/m\mathbb{Z}$ that have a multiplicative inverse. The resulting set is denoted $\mathbb{Z}/m\mathbb{Z}^*$.

Theorem (Textbook Thm 9.1)

For every integer $m > 1$, $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$ is a commutative group.

Proof

Check the axioms: **closure**, associativity, identity element, inverse element, commutativity.

EXAMPLE: $(\mathbb{Z}/10\mathbb{Z}^+, \cdot)$

$$\mathbb{Z}/10\mathbb{Z}^+ = \{1, 3, 7, 9\}$$

$$3 \cdot 9 = 27 = 7 \quad \checkmark$$

$$7 \cdot 9 = 63 = 3 \quad \checkmark$$

$$\mathbb{Z}/15\mathbb{Z}^+ = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

CLOSURE ?

Let $a, b \in \mathbb{Z}/m\mathbb{Z}^+$.

↳ is $ab \in \mathbb{Z}/m\mathbb{Z}^+$?

ANSWER: YES!

PROOF BY CONSTRUCTION:

CONSTRUCT THE INVERSE OF ab.

↳ $b^{-1}a^{-1}$

WORKS BECAUSE $b^{-1}a^{-1}ab = b^{-1}b = 1$

$abb^{-1}a^{-1} = 1$ ✓

Definition (Textbook Def. 8.5)

Euler's $\phi(n)$ function (also called **Euler's totient function**) is the number of positive integers in $\{1, \ldots, n\}$ that are relatively prime to n.

Observations:

- Recall that two integers a and b are relatively prime iff $\gcd(a, b) = 1$.
- Hence 1 is relatively prime with every integer.
- $\phi(m)$ is the cardinality of $\mathbb{Z}/m\mathbb{Z}^*$.
- If p is prime, $\phi(p) = p - 1$.

Example

- $\phi(1) = 1$
- $\phi(2) = 1, \quad \mathbb{Z}/2\mathbb{Z}^* = \{1\}$
- $\phi(3) = 2, \quad \mathbb{Z}/3\mathbb{Z}^* = \{1, 2\}$
- $\phi(4) = 2, \quad \mathbb{Z}/4\mathbb{Z}^* = \{1, 3\}$
- $\phi(5) = 4, \quad \mathbb{Z}/5\mathbb{Z}^* = \{1, 2, 3, 4\}$
- $\phi(6) = 2, \quad \mathbb{Z}/6\mathbb{Z}^* = \{1, 5\}$
- $\phi(7) = 6, \quad \mathbb{Z}/7\mathbb{Z}^* = \{1, 2, 3, 4, 5, 6\}$

EXERCISE

Prove the following:

- If p is prime and k is a positive integer, $\phi(p^k) = p^k - p^{k-1}$.
- If p and q are distinct primes, $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.

p (prime)

$$\boxed{\phi(p^k) = p^k - p^{k-1}}$$

$\{1, 2, 3, \ldots \quad p, p+1, p+2, \ldots 2p, 2p+1, \ldots 3p, \ldots$

$\ldots p^2, p^2+1, \ldots$

$\ldots \quad - \quad - \quad - \quad p^k\}$

p (prime)

$$\boxed{\phi(p^k) = p^k - p^{k-1}}$$

$\{1, 2, 3, \ldots p-1, p, p+1, p+2, \ldots, 2p-1, 2p, \ldots$

$\ldots 3p, 3p+1, \ldots 4p, \ldots$

$\ldots p^{k-1} p\}$

p, q : primes (distinct)

$(p < q)$

$$\phi(pq) = (p-1)(q-1)$$

$\{ 1, 2, 3, \ldots, \quad p, p+1, \ldots 2p, \ldots q, \quad 2q$

$\ldots$

$pq \}$

$$pq - q - p + 1$$

Solution (outline)

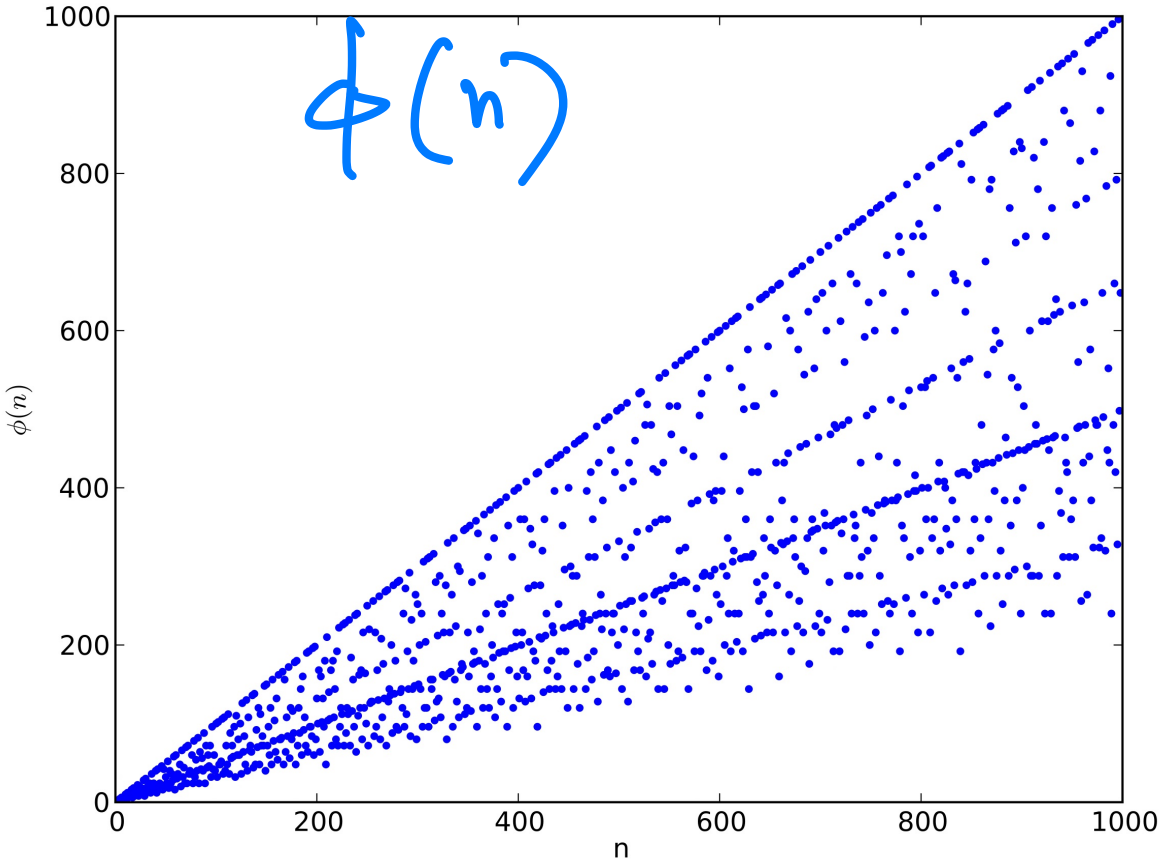
- In $\{1, 2, \ldots, p^k\}$, only the numbers $p, 2p, 3p, \ldots, p^{k-1}p$ are divisible by p.

  Hence $p^k - p^{k-1}$ elements of $\{1, 2, \ldots, p^k\}$ are not divisible by p.

- In $\{1, 2, \ldots, pq\}$, only pq is divisible by both, p and q.

  Hence, there are q elements that are divisible by p, p elements that are divisible by q, and one which is divisible by both.

  $pq - p - q + 1 = (p - 1)(q - 1)$ elements are divisible by neither.


φ(n)
1000
800
600
400
200
0
$\phi(n)$
0
200
400
600
800
1000
n

EXERCISE

Below is the multiplication table of $(\mathbb{Z}/5\mathbb{Z}^*, \cdot)$. Every element of $\mathbb{Z}/5\mathbb{Z}^*$ shows up exactly once in every row. Is it surprising?

$\mathbb{Z}/5\mathbb{Z}^*$	$\times$	1	2	4	3
	1	1	2	4	3
	2	2	4	3	1
	4	4	3	1	2
	3	3	1	2	4

Solution

We have seen that in $\mathbb{Z}/m\mathbb{Z}$, when a^{-1} exists, the map $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

$$x \to ax$$

is a bijection.

Each row of the above table is such a map. (The same is true for each column.) □

Nota Bene:

- In $(\mathbb{Z}/m\mathbb{Z}, +)$, the identity element is $[0]_m$.
- In $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$, the identity element is $[1]_m$.

Recall that if $\mathcal{A}_1$ and $\mathcal{A}_2$ are sets, the cartesian product $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$ is the set

$$\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2 = \{(a_1, a_2) : a_1 \in \mathcal{A}_1, a_2 \in \mathcal{A}_2\}.$$

Similarly, $(G, \star) = (G_1, \star_1) \times (G_2, \star_2)$ is the set $G = G_1 \times G_2$ endowed with the binary operation $\star$ defined by

$$(a_1, a_2) \star (b_1, b_2) = (a_1 \star_1 b_1, a_2 \star_2 b_2).$$

$\mathbb{Z}/2\mathbb{Z}$	$+$	0	1
	0	0	1
	1	1	0

$\mathbb{Z}/3\mathbb{Z}$	$+$	0	1	2
	0	0	1	2
	1	1	2	0
	2	2	0	1

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$= \{(0,0), (0,1), (0,2),$
$(1,0), (1,1), (1,2)\}$

$+$	00	01	02	10	11	12
00	00					
01						
02						
10						12
11						
12						

$\mathbb{Z}/2\mathbb{Z}$	$+$	0	1
	0	0	1
	1	1	0

$\mathbb{Z}/3\mathbb{Z}$	$+$	0	1	2
	0	0	1	2
	1	1	2	0
	2	2	0	1

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$= \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

$+$	00	01	02	10	11	12
00	00					
01						
02						
10						
11						
12						00

Example $((\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/3\mathbb{Z}, +))$

$\mathbb{Z}/2\mathbb{Z}$	$+$	0	1
	0	0	1
	1	1	0

$\mathbb{Z}/3\mathbb{Z}$	$+$	0	1	2
	0	0	1	2
	1	1	2	0
	2	2	0	1

$+$	00	01	02	10	11	12
00	00	01	02	10	11	12
01	01	02	00	11	12	10
02	02	00	01	12	10	11
10	10	11	12	00	01	02
11	11	12	10	01	02	00
12	12	10	11	02	00	01

The Cartesian Product of Commutative Groups is a Commutative Group

Recall the axioms of a commutative group:

- (Closure:) For all $a, b \in G$, the result of the operation $a \star b$ is also in G.
- (Associativity:) For all $a, b \in G$, $a \star (b \star c) = (a \star b) \star c$.
- (Identity element:) There exists an element $e \in G$, such that for all $a \in G$, $a \star e = e \star a = a$.
- (Inverse element:) For all $a \in G$, there exists $b \in G$, such that $a \star b = b \star a = e$.
- (Commutativity:) For all $a, b \in G$, $a \star b = b \star a$.

and check that they apply to elements of the form $(a_1, a_2) \in (G_1, \star_1) \times (G_2, \star_2)$.

$(G_1, \star_1) \times (G_2, \star_2)$ is called the **product group**.

EXERCISE

Consider $(G, \star) = (G_1, \star_1) \times (G_2, \star_2)$, where $(G_1, \star_1) = (\mathbb{Z}/4\mathbb{Z}, +)$ and $(G_2, \star_2) = (\mathbb{Z}/3\mathbb{Z}^*, \cdot)$:

- evaluate $(3, 2) \star (1, 2)$;
- find the identity element; $\longrightarrow (0, 1)$
- find the inverse element of $(3, 2)$.

$(3, 2) * (1, 2) = (0, 1)$

$(\mathbb{Z}/4\mathbb{Z}, +) \times (\mathbb{Z}/3\mathbb{Z}^*, \cdot)$

$a(0,1)$

	01	02	11	12	21	22	31	32
01	01							
02								
11								
12								
21								
22							12	
31								
32								

Solution

In $(\mathbb{Z}/4\mathbb{Z}, +) \times (\mathbb{Z}/3\mathbb{Z}^*, \cdot)$:

- $(3, 2) \star (1, 2) = (0, 1)$;
- $e = (0, 1)$;
- the inverse of $(3, 2)$ is $(1, 2)$.

The operation $\star$ of a product group is called **product operation**.

NB: The product operation can be a component-wise addition, as in

Example $((\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/3\mathbb{Z}, +))$

$\mathbb{Z}/2\mathbb{Z}$	$+$	0	1
	0	0	1
	1	1	0

$\mathbb{Z}/3\mathbb{Z}$	$+$	0	1	2
	0	0	1	2
	1	1	2	0
	2	2	0	1

$+$	00	01	02	10	11	12
00	00	01	02	10	11	12
01	01	02	00	11	12	10
02	02	00	01	12	10	11
10	10	11	12	00	01	02
11	11	12	10	01	02	00
12	12	10	11	02	00	01

Exercise

Which of the following are product groups?

- $(\mathbb{Z}/2\mathbb{Z}, \cdot) \times (\mathbb{Z}/3\mathbb{Z}, \cdot)$.
- $(\mathbb{Z}/2\mathbb{Z}^*, \cdot) \times (\mathbb{Z}/3\mathbb{Z}^*, \cdot)$.

Exercise

Which of the following are product groups?

- $(\mathbb{Z}/2\mathbb{Z}, \cdot) \times (\mathbb{Z}/3\mathbb{Z}, \cdot)$.
- $(\mathbb{Z}/2\mathbb{Z}^*, \cdot) \times (\mathbb{Z}/3\mathbb{Z}^*, \cdot)$.

Solution

- $(\mathbb{Z}/2\mathbb{Z}, \cdot) \times (\mathbb{Z}/3\mathbb{Z}, \cdot)$: Not a commutative group, because $(0, 0)$ has no inverse.
- $(\mathbb{Z}/2\mathbb{Z}^*, \cdot) \times (\mathbb{Z}/3\mathbb{Z}^*, \cdot)$: Indeed a commutative group.

EXERCISE

Let m and n be integers greater than 1.

- Is it true that the subset of $(\mathbb{Z}/m\mathbb{Z}, \cdot) \times (\mathbb{Z}/n\mathbb{Z}, \cdot)$ that consists of elements that have an inverse is a commutative group?
- If yes, is it the same commutative group as $(\mathbb{Z}/m\mathbb{Z}^*, \cdot) \times (\mathbb{Z}/n\mathbb{Z}^*, \cdot)$?

Solution

Yes to both questions.

In fact, $(G_1, \star_1) \times (G_1, \star_1)$ is a group iff both $(G_1, \star_1)$ and $(G_1, \star_1)$ are groups.

The subset of $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ that contains all the elements of $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ that have an inverse is a group, denoted $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$.

Similarly, ... (same argument with n instead of m).

GROUP ISOMORPHISM

G

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

H

$\otimes$	0	1	2
0	x^0	x^1	x^2
1	x^1	x^2	x^0
2	x^2	x^0	x^1

ARE G AND H DIFFERENT?

YES AND NO!

THEY ARE ISOMORPHIC.

GROUP ISOMORPHISM

G

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

H

$\otimes$	2	0	1
2	2	0	1
0	0	1	2
1	1	2	0

ARE G AND H DIFFERENT?

ANSWER: YES AND NO.

↳ THEY ARE ISOMORPHIC

GROUP ISOMORPHISM

G

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

H

$\otimes$	2	0	1
2	2	0	1
0	0	1	2
1	1	2	0

G AND H ARE ISOMORPHIC:

$\varphi(0) = 2$

$\varphi(1) = 0$

$\varphi(2) = 1$

$\varphi^{-1}(0) = 1$

$\varphi^{-1}(1) = 2$

$\varphi^{-1}(2) = 0$

Isomorphism

Some sets endowed with an operation might look different, but they are actually the same once their elements are re-labeled.

Definition

Let $(G, \star)$ and $(H, \otimes)$ be sets, each endowed with a binary operation.

An **isomorphism** from $(G, \star)$ to $(H, \otimes)$ is a bijection $\psi : G \to H$ such that

$$\psi(a \star b) = \psi(a) \otimes \psi(b)$$

holds for all $a, b \in G$.

We say that $(G, \star)$ and $(H, \otimes)$ are **isomorphic** if there exists an isomorphism between them.

Suppose that ψ is an isomorphism from $(G, \star)$ to $(H, \otimes)$. The following properties hold:

- If $(G, \star)$ is a commutative group, so is $(H, \otimes)$.
- If e is the identity element of $(G, \star)$, then $\psi(e)$ is the identity element of $(H, \otimes)$.
- If a, b are inverse of one another in $(G, \star)$, then $\psi(a), \psi(b)$ are inverse of one-another in $(H, \otimes)$.

From a group-theoretic viewpoint, isomorphic groups are the same object.

Proofs: For the first point, we show that if $(G, \star)$ is a commutative group, so is $(H, \otimes)$. To do so, each element of H is written as $\psi(x)$ for some $x \in G$.

- Closure: $\psi(a) \otimes \psi(b) = \psi(a \star b) \in H$;
- Associativity: No matter in which order we perform the operations on the LHS (left-hand side), $\psi(a) \otimes \psi(b) \otimes \psi(c) = \psi(a \star b \star c)$;
- Identity Element: $\psi(e) \otimes \psi(a) = \psi(e \star a) = \psi(a)$, proving that $\psi(e)$ is the identity element in $(H, \otimes)$;
- Inverse Element: $\psi(a) \otimes \psi(a^{-1}) = \psi(a \star a^{-1}) = \psi(e)$, showing that the inverse of $\psi(a)$ is $\psi(a^{-1})$;
- Commutativity: $\psi(a) \otimes \psi(b) = \psi(a \star b) = \psi(b \star a) = \psi(b) \otimes \psi(a)$.

We have also proved the other two points of the previous slide.

Example

$(\mathbb{Z}/2\mathbb{Z}, +)$ and $(\mathbb{Z}/4\mathbb{Z}^*, \cdot)$ are isomorphic.

$\mathbb{Z}/2\mathbb{Z}$	$+$	0	1
	0	0	1
	1	1	0

$\mathbb{Z}/4\mathbb{Z}^*$	$\times$	1	3
	1	1	3
	3	3	1

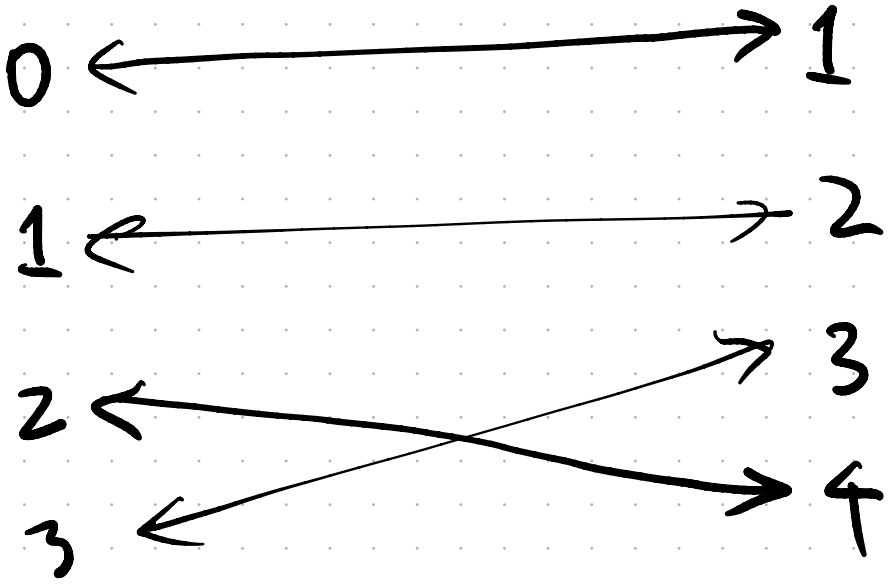
$$\psi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}^*$$
$$0 \to 1$$
$$1 \to 3$$

- Check that $\psi([0]_2)$ is the identity element in $(\mathbb{Z}/4\mathbb{Z}^*, \cdot)$.
- Check that $\psi(-[1]_2)$ is the (multiplicative) inverse of $\psi([1]_2)$ in $(\mathbb{Z}/4\mathbb{Z}^*, \cdot)$.

$\mathbb{Z}/4\mathbb{Z}$	$+$	0	1	2	3
	0	0	1	2	3
	1	1	2	3	0
	2	2	3	0	1
	3	3	0	1	2

ISO-
MORPHIC
?

$\mathbb{Z}/5\mathbb{Z}^*$	$\times$	1	2	3	4
	1	1	2	3	4
	2	2	4	1	3
	3	3	1	4	2
	4	4	3	2	1



EXERCISE

Are $(\mathbb{Z}/4\mathbb{Z}, +)$ and $(\mathbb{Z}/5\mathbb{Z}^*, \cdot)$ isomorphic?

$\mathbb{Z}/4\mathbb{Z}$	$+$	0	1	2	3
	0	0	1	2	3
	1	1	2	3	0
	2	2	3	0	1
	3	3	0	1	2

$\mathbb{Z}/5\mathbb{Z}^*$	$\times$	1	2	3	4
	1	1	2	3	4
	2	2	4	1	3
	3	3	1	4	2
	4	4	3	2	1

- Hint 1: match up identity elements.
- Hint 2: $[2]_4$ is the inverse of itself in $(\mathbb{Z}/4\mathbb{Z}, +)$.

Solution

The following correspondence is not negotiable:

- $0 \to 1$ (identity elements must match);
- $2 \to 4$ (inverses must match).

There are two ways to complete:

- $1 \to 2$ and $3 \to 3$

or

- $1 \to 3$ and $3 \to 2$.

Both form an isomorphism.

$\{(0,0), (0,1), (1,0), (1,1)\}$

Exercise

Say why the following cannot be isomorphic:

- $(\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$ and $(\mathbb{Z}/3\mathbb{Z}, +)$;
- $(\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$ and $(\mathbb{Z}/4\mathbb{Z}, +)$.

$\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$

Solution

- $(\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$ and $(\mathbb{Z}/3\mathbb{Z}, +)$:
  They do not have the same cardinality.

- $(\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$ and $(\mathbb{Z}/4\mathbb{Z}, +)$:
  They do have the same cardinality.
  In $(\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$, the inverse of x is x.
  Not the case for $(\mathbb{Z}/4\mathbb{Z}, +)$.

EXERCISE

Find an isomorphism from $((0, +\infty), \cdot)$ to $(\mathbb{R}, +)$.

Exercise

Find an isomorphism from $((0, +\infty), \cdot)$ to $(\mathbb{R}, +)$.

Solution

An isomorphism from $((0, +\infty), \cdot)$ to $(\mathbb{R}, +)$ is:

$$\begin{aligned} \psi : (0, +\infty) &\to \mathbb{R} \\ x &\mapsto \log(x) \end{aligned}$$

$$\psi : (x \cdot y) \mapsto \log(x) + \log(y).$$

Theorem (textbook Thm 9.4)

Let $(G, \star)$ be a finite commutative group with identity element e.

For every $a \in G$, there exists an integer $k \geq 1$, such that

$$\underbrace{a \star a \star \cdots \star a}_{k \text{ terms}} = e.$$

PROOF: $(G, \star)$, G FINITE

LET $a \in G$:

$a, a^2, a^3, a^4, a^5, a^6, a^7, \ldots$

BECAUSE G IS FINITE, THERE MUST BE $i < j$ SUCH

$$a^i = a^j \underbrace{\qquad}_{j-i}$$

$$= (a \star a \star a \ldots) \star a^i$$

For the proof, we use the notation $a^k := \underbrace{a \star a \star \cdots \star a}_{k \text{ terms}}$.

For instance, in $(\mathbb{Z}, +)$, $a^3 = a + a + a$.

Proof:

- The commutative group is finite, hence the sequence

$$a, a^2, a^3, a^4, \ldots$$

  must contain repetitions.

- Suppose $a^i = a^j$ with $i < j$.
- By multiplying both sides by $(a^{-1})^i$ we obtain $e = a^{j-i}$. □

DEFINITION (TEXTBOOK DEFINITION 9.4)

Let $(G, \star)$ be a finite commutative group with identity element e, and let $a \in G$.

The smallest positive integer k such that

$$\underbrace{a \star a \star \cdots \star a}_{k \text{ terms}} = e$$

is called the **order** of a.

Sometimes it is called the **period** of a. ("Période de a" in French.)

Example

The order of $[a]_{12} \in (\mathbb{Z}/12\mathbb{Z}, +)$ is the smallest k such that

$$\underbrace{[a]_{12} + [a]_{12} + \cdots + [a]_{12}}_{k \text{ terms}} = [0]_{12}.$$

- For $a = 3$, the order is 4.
- For $a = 4$, the order is 3.
- For $a = 5$, the order is 12.

Example

The order of $[a]_8 \in (\mathbb{Z}/8\mathbb{Z}^*, \cdot)$ is the smallest k such that

$$\underbrace{[a]_8 \cdot [a]_8 \cdots [a]_8}_{k \text{ terms}} = [1]_8.$$

Mind that $\mathbb{Z}/8\mathbb{Z}^* = \{[1]_8, [3]_8, [5]_8, [7]_8\}$).

- For $a = 1$, the order is 1.
- For $a = 3$, the order is 2.
- For $a = 5$, the order is 2.
- For $a = 7$, the order is 2.

$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 \quad \mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$

EXERCISE

Find the order of every element in $((\mathbb{Z}/2\mathbb{Z})^2, +)$.

$= (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$

$= (\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$

$\text{order}((0,0)) = 1$

$\text{order}((0,1)) = 2$

$\text{order}((1,0)) = 2$

$\text{order}((1,1)) = 2$

Exercise

Find the order of every element in $((\mathbb{Z}/2\mathbb{Z})^2, +)$.

Solution

In $((\mathbb{Z}/2\mathbb{Z})^2, +)$, the identity is $([0]_2, [0]_2)$.

- $([0]_2, [0]_2)$ has order 1.
- $([0]_2, [1]_2)$ has order 2.
- idem for $([1]_2, [0]_2)$.
- idem for $([1]_2, [1]_2)$.

EXAMPLE

$\mathbb{Z}/10\mathbb{Z}^* = \{1, 3, 7, 9\}$. Find the order of each element in $(\mathbb{Z}/10\mathbb{Z}^*, \cdot)$.

Hint: it is recommended to reduce intermediate results.

order $(1) = 1$

$3^2 = 9$ $\quad 3^3 = 3^2 \cdot 3 = 9 \cdot 3 = 7$

$3^4 = 3^3 \cdot 3 = 7 \cdot 3 = 21 = 1$

Example

$\mathbb{Z}/10\mathbb{Z}^* = \{1, 3, 7, 9\}$. Find the order of each element in $(\mathbb{Z}/10\mathbb{Z}^*, \cdot)$.

Hint: it is recommended to reduce intermediate results.

Solution

x	x^2	x^3	x^4	order
1				1
3	9	7	1	4
7	9	3	1	4
9	1			2

or, for instance,

x	x^2	x^3	x^4	order
1				1
3	-1	-3	1	4
7	-1	3	1	4
9	1			2

- Recall: An isomorphism ψ from $(G, \star)$ to $(H, \otimes)$ maps the identity element of $(G, \star)$ to the identity element of $(H, \otimes)$.
- This implies that the order of $g \in (G, \star)$ is the same as the order of $\psi(g) \in (H, \otimes)$.

Example

- In $(\mathbb{Z}/2\mathbb{Z}^2, +)$, the orders are $1, 2, 2, 2$.
- In $(\mathbb{Z}/10\mathbb{Z}^*, \cdot)$, the orders are $1, 4, 4, 2$.
- Hence the two commutative groups cannot be isomorphic.

The following result is given without proof:

THEOREM

Two finite commutative groups are isomorphic iff they have the same set of orders.

Let e be the identity element of a commutative group $(G, \star)$ and let $a \in G$.

Find the integers k such that $\underbrace{a \star a \star \cdots \star a}_{k \text{ terms}} = e$.

Example (addition)

$(G, \star) = (\mathbb{Z}/12\mathbb{Z}, +)$, $e = [0]_{12}$, $a = [2]_{12}$

k	1	2	3	4	5	6	7	8	9	$\cdots$
$([2]_{12})^k = k[2]_{12}$	2	4	6	8	10	0	2	4	6	$\cdots$

The values of k are the integer multiples of the order of a, which is 6.

Example (multiplication)

$(G, \star) = (\mathbb{Z}/10\mathbb{Z}^*, \cdot)$, $e = [1]_{10}$, $a = [3]_{10}$

k	1	2	3	4	5	6	7	8	9	$\cdots$
$([3]_{10})^k$	3	9	7	1	3	9	7	1	3	$\cdots$

The values of k are the integer multiples of the order of a, which is 4.

It is always like that: For $a \in (G, \star)$, $a^k = e$ when k is an integer multiple of the order of a.

This is not surprising: if q is the order of a and $k = qn$, we can write $a^k = (a^q)^n = e^n = e$. The following theorem states an even stronger result.

THEOREM

Let $(G, \star)$ be a commutative group and $a \in G$.

An integer k satisfies $\underbrace{a \star a \star \cdots \star a}_{k \text{ terms}} = e$ iff the order of a divides k.

Proof

Recall the notation: a^k means $\underbrace{a \star a \star \cdots \star a}_{k \text{ terms}}$.

- Let p be the order of a and write $k = pq + r, \;\; 0 \leq r < p$.
- $e = a^k = a^{pq+r} = (a^p)^q \star a^r = a^r$.
- $r = 0$, because p is the smallest positive integer such that $a^p = e$.
- Hence k is a multiple of p.

YESTERDAY

- GROUP $(G, \star)$
- $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$: $\phi(m)$ ELEMENTS
- PRODUCT GROUP:
  (a, b) WITH: $a \in (G_1, \star_1)$
  $b \in (G_2, \star_2)$
- ISOMORPHISM

- CURIOUS PROPERTY IN FINITE GROUPS:

$$a^k = \underbrace{a * a * a \dots * a}_{k \text{ TERMS}} = e$$

- SMALLEST SUCH k IS CALLED ORDER OF a.

- $a^k = e \iff k$ IS A MULTIPLE OF THE ORDER OF a.

Example

- the order of $[2]_{12} \in (\mathbb{Z}/12\mathbb{Z}, +)$ is 6:

l	1	2	3	4	5	6	7	8	$\cdots$
$l[2]_{12}$	2	4	6	8	10	0	2	4	$\cdots$

- the order of $[3]_{10} \in (\mathbb{Z}/10\mathbb{Z}^*, \cdot)$ is 4:

l	1	2	3	4	5	6	$\cdots$
$([3]_{10})^l$	3	9	7	1	3	9	$\cdots$

$\mathbb{Z}/12\mathbb{Z}$ has cardinality 12 and the cardinality of $\mathbb{Z}/10\mathbb{Z}^* = \{1, 3, 7, 9\}$ is 4.

In both cases, the order divides the cardinality of the commutative group. A coincidence?

Theorem (Lagrange, Textbook Thm 9.3)

Let $(G, \star)$ be a finite commutative group of cardinality n. The order of each of its elements divides n.

Equivalence Relation and Equivalence Classes

To be ready for the elegant proof of Lagrange's theorem, we review the concept and the implication of an **equivalence relation** .

Relationships occur in many contexts in life. In math, they are represented by the structure called a **binary relation**.

Example

To relate people to their car, we can define

- a set A of all people;
- a set B of all cars;
- a set $R \subset A \times B$ that contains (a, b) iff person a owns car b.

The set R is called **a binary relation from A to B**.

The shorthand notations $a \sim b$ and $a\,R\,b$ mean the same as $(a, b) \in R$.

If the sets A and B are the same, then we speak of a **relation on** A.

An equivalence relation is a special case of a relation on a set. It is used to relate objects that are similar in some way, like in $\mathbb{Z}$, we may relate a and b if, for a specified m, $[a]_m = [b]_m$.

Definition

A relation on a set A is called an **equivalence relation** if it is *reflexive, symmetric, and transitive*.

Example

Let A be the set of all EPFL students.

Define $R = \{(a, b) \in A \times A : a \text{ and } b \text{ graduated from the same high school}\}$

R is an equivalence relation. In fact

- $a \sim a$ (reflexive);
- if $a \sim b$ then $b \sim a$ (symmetric);
- if $a \sim b$ and $b \sim c$ then $a \sim c$ (transitive).

Exercise

Let A be a set of people.

Define $R = \{(a, b) \in A \times A : a \text{ trusts } b\}$.,

Is this an equivalence relation?

Exercise

Let A be a set of people.

Define $R = \{(a, b) \in A \times A : a \text{ trusts } b\}$.,

Is this an equivalence relation?

Solution

No, this relation on A is not symmetric.

EXERCISE

Let A be the students of AICC-II.

Define
$R = \{(a, b) \in A \times A : a \text{ and } b \text{ got the same score in AICC-I or AICC-II}\}$.

Is this an equivalence relation?

Exercise

Let A be the students of AICC-II.

Define
$R = \{(a, b) \in A \times A : a \text{ and } b \text{ got the same score in AICC-I or AICC-II}\}$.

Is this an equivalence relation?

Solution

No, this relation on A is not transitive.

Let R be an equivalence relation on A and $a \in A$.

By $[a]$ we denote the **equivalence class of** a:

$$[a] = \{b \in A : b \sim a\}.$$

Any element of an equivalence class can be used to represent the class: if $b \in [a]$ then $[b]$ and $[a]$ are the same class.

Every $a \in A$ is in one and only one equivalence class. In fact, if $a \in [b]$ and $a \in [c]$ then $[b] = [a] = [c]$.

To say it in a different way, an equivalence relation on A partitions A into equivalence classes: they are disjoint subsets of A and their union is A.

Example (continuation)

Let A be the set of all EPFL students.

Define $R = \{(a, b) \in A \times A : a \text{ and } b \text{ graduated from the same high school}\}$.

We can partition A into sets of students that graduated from the same high school. Each student is in exactly one such subset.

$$(\mathbb{Z}/20\mathbb{Z}^*, \cdot) = (\{1,3,7,9,11,13,17,19\}, \cdot)$$

Equivalence relation:

1) Select <u>arbitrary</u> $h \in \mathbb{Z}/20\mathbb{Z}^*$.

$$(\mathbb{Z}/20\mathbb{Z}^*, \cdot) = (\{1,3,7,9,11,13,17,19\}, \cdot)$$

Equivalence relation:

1) Select <u>arbitrary</u> $h \in \mathbb{Z}/20\mathbb{Z}^*$.

2) $a \sim b$ means $ah^i = b$ for some $i \geq 1$.

Is this really an equivalence relation?

1) reflexivity ✓

2) symmetry: $b \sim a$ or $bh^j = a$

3) transitivity: $\left.\begin{array}{l} a \sim b \text{ or } ah^i = b \\ b \sim c \text{ or } bh^k = c \end{array}\right\} \Rightarrow a \sim c$

$(\mathbb{Z}/20\mathbb{Z}^*, \cdot) = (\{1,3,7,9,11,13,17,19\}, \cdot)$

Equivalence relation:

1) Select <u>arbitrary</u> $h \in \mathbb{Z}/20\mathbb{Z}^*$.

2) $a \sim b$ means $ah^i = b$ for some i.

Equivalence relation?

2) <u>symmetry</u) $a \sim b \Rightarrow b \sim a$

$\Updownarrow$ $\Updownarrow$

$ah^i = b$ $bh^j = a$

$ah^{i+k} = bh^k$

FOR 3)

We know

$a \sim b \iff ah^i = b$

$a \sim c \iff ah^k = c$

Question

$b \sim c \iff bh^m = c$?

$\Updownarrow$

$ah^i h^m = ah^k$

$\Updownarrow$

$h^{i+m} = h^k$

$(\mathbb{Z}/20\mathbb{Z}^*, \cdot) = (\{1,3,7,9,11,13,17,19\}, \cdot)$

Select <u>arbitrary</u> $h \in \mathbb{Z}/20\mathbb{Z}^*$.

Ex: $\boxed{h = 7}$

$$[1] = \{ a \in G : a = 1 \cdot h^i \text{ for some } i \}$$

$$= \{7, 9, 3, 1\}$$

$(\mathbb{Z}/20\mathbb{Z}^*, \cdot) = (\{1,3,7,9,11,13,17,19\}, \cdot)$

Select <u>arbitrary</u> $h \in \mathbb{Z}/20\mathbb{Z}^*$.

Ex: $\boxed{h = 7}$

$[1] = \{1, 7, 9, 3\}$

$[3] = \{ \quad " \quad \}$

$[11] = \{11, 17, 19, 13\}$

$= \{a \in G : a = 11 \cdot h^i \text{ for some } i\}$

KEY OBSERVATION

- ALL EQUIVALENCE CLASSES MUST HAVE THE SAME CARDINALITY (I.E, NUMBER OF ELEMENTS)
- AND THIS CARDINALITY IS PRECISELY ORDER(h).

$(\mathbb{Z}/20\mathbb{Z}^*, \cdot) = (\{1,3,7,9,11,13,17,19\}, \cdot)$

Select <u>arbitrary</u> $h \in \mathbb{Z}/20\mathbb{Z}^*$.

Ex: $\boxed{h = 19}$

$$[1] = \{ a \in G : a = 1 \cdot h^i \text{ for all } i \in \mathbb{Z}_+ \}$$

$$= \{19, 1\}$$

$(\mathbb{Z}/20\mathbb{Z}^*, \cdot) = (\{1,3,7,9,11,13,17,19\}, \cdot)$

Select <u>arbitrary</u> $h \in \mathbb{Z}/20\mathbb{Z}^*$.

Ex: $\boxed{h = 19}$

$[1] = \{1, 19\}$

$[3] = \{3, 17\}$

$[7] = \{7, 13\}$

$[9] = \{9, 11\}$

The following example is a special case of the construction used in the proof of Lagrange's Theorem.

Example

Let $(G, \star)$ be the group $\left(\mathbb{Z}/20\mathbb{Z}^*, \times\right) = \left(\{1, 3, 7, 9, 11, 13, 17, 19\}, \times\right)$.

Pick an arbitrary group element, e.g., $h = 7$.

Let $H = \{7, 9, 3, 1\}$ be the set that consists of all the powers of h.

We use H to define an equivalence relation on $G = \{1, 3, 7, 9, 11, 13, 17, 19\}$:

$$a \sim b \text{ if } ah^i = b \text{ for some } h^i \in H.$$

(This is an equivalence relation. We prove it later.) Let us construct the equivalence classes:

- $[1] = H = \{7, 9, 3, 1\}$;
- $[11] = \{17, 19, 13, 11\}$.

$G = [1] \cup [11]$. It is not a coincidence that all equivalence classes have the same cardinality. The cardinality of G must be a multiple of the cardinality of H.

Proof of Lagrange's Theorem:

- Let $(G, \star)$ be a finite commutative group of cardinality n.
- Let p be the order of $h \in G$.
- Let $H = \{h, h^2, h^3, \ldots, h^p = e\}$. (Note that $(H, \star)$ is itself a group, and is called a subgroup of G of cardinality p.)
- Define a relation on G:

$$a \sim b \quad \Leftrightarrow \quad \exists h^i \in H \text{ such that } a \star h^i = b.$$

- It is reflexive (H contains the identity element), symmetric (H contains the inverse of each of its elements), and transitive (the product of elements of H is in H) — hence $\sim$ is an equivalence relation.
- An equivalence relation splits G into equivalence classes.
- H is one such equivalence class.

- It suffices to show that each equivalence class has the same cardinality p. Then p must divide n.
- We show that there is a one-to-one map between H and each equivalence class.
- The equivalence class of b is $[b] = \{b \star h, b \star h^2, \ldots, b \star h^p\}$.
- Clearly the cardinality of $[b]$ is at most p.
- It is p because the map $f : H \to [b]$ that sends h^i to $b \star h^i$ is one-to-one.
- Proof by contradiction: $b \star h^i = b \star h^k$ implies $h^i = h^k$ (b has an inverse). But for $1 \leq i, k \leq p$, $h^i = h^k$ holds if and only if $i = k$.
- Hence all equivalence classes have the same cardinality p, which must divide n.

Example (Something Old)

- The cardinality of $(\mathbb{Z}/m\mathbb{Z}, +)$, is m.
- For each element $[a]_m \in \mathbb{Z}/m\mathbb{Z}$, $m[a]_m = [0]_m$.
- Hence the period of each element of $(\mathbb{Z}/m\mathbb{Z}, +)$ divides m.

In $(\mathbb{Z}/m\mathbb{Z}, +)$, Lagrange's Theorem says nothing new to us.

In $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$, Lagrange's Theorem is non-trivial.

Using the fact that the cardinality of $\mathbb{Z}/m\mathbb{Z}^*$ is Euler's $\phi(m)$, we obtain:

Corollary (Euler's Theorem, textbook corollary 9.4)

Let $m \geq 2$ be an integer. For all $a \in (\mathbb{Z}/m\mathbb{Z}^*, \cdot)$

$$a^{\phi(m)} = [1]_m.$$

Equivalently, for all integers a that are relatively prime with m,

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

The above theorem underlies the cryptographic method studied in the next chapter.

PROOF:

1) FROM THM ON p. 464, WE KNOW

$$a^k = [1]_m$$

IF AND ONLY IF k IS A MULTIPLE OF ORDER(a).

2) FROM LAGRANGE, WE KNOW THAT $\phi(m)$ IS A MULTIPLE OF ORDER(a).

Corollary (Fermat's Theorem, textbook corollary 9.5)

Let p be prime. For all $a \in (\mathbb{Z}/p\mathbb{Z}, \cdot)$

$$a^p = a.$$

Equivalently, for all integers a ,

$$a^p \equiv a \pmod{p}.$$

Proof: It follows from Euler's Theorem, and $\phi(p) = p - 1$, that

$$a^{(p-1)} = [1]_p$$

holds for all $a \in (\mathbb{Z}/p\mathbb{Z}, \cdot)$, except for $a = [0]_p$.

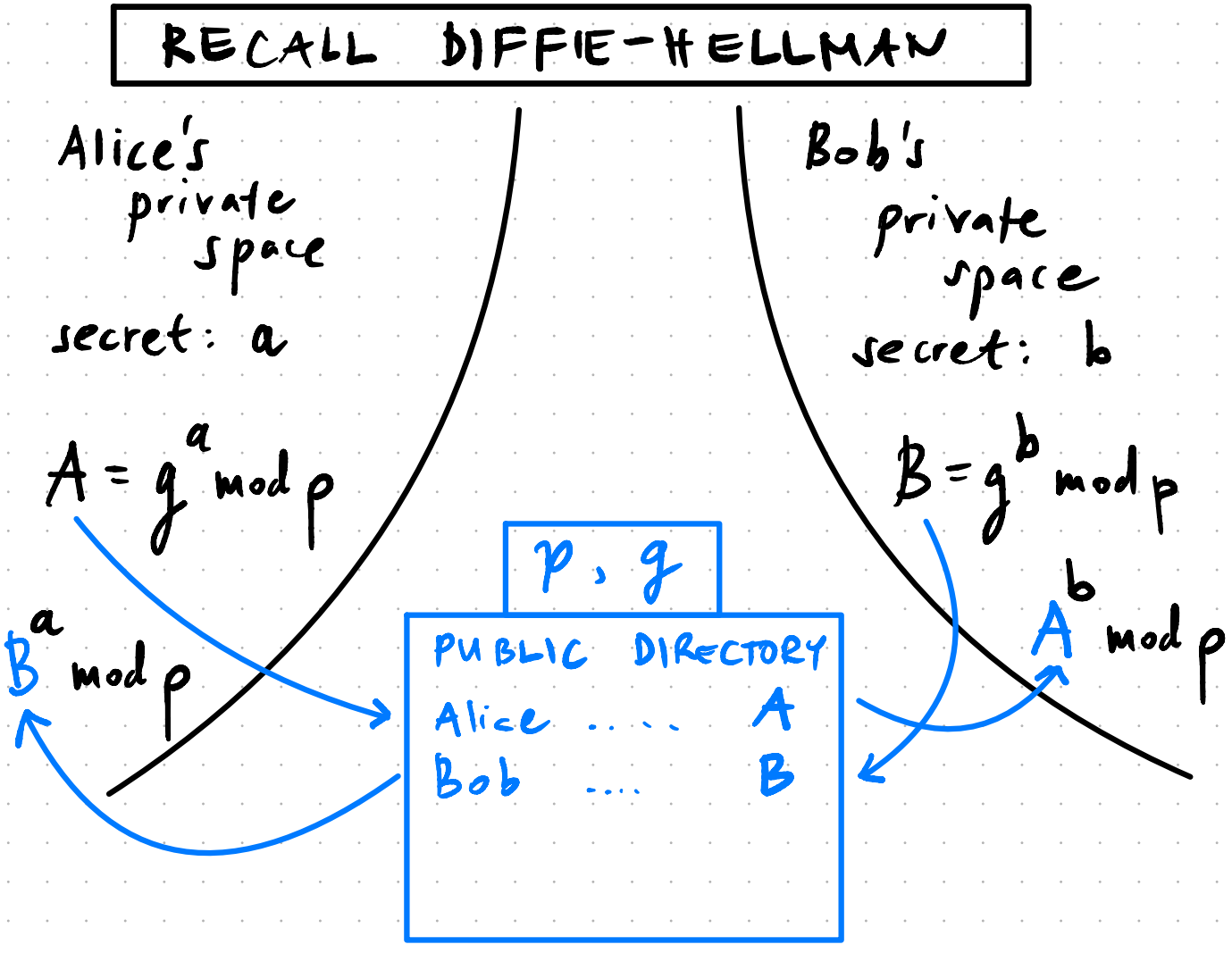
By multiplying both sides by a we obtain

$$a^p = a,$$

which holds also for $a = [0]_p$. □

Example

- $2^3 \equiv 2 \pmod 3$
- $4^3 \equiv 4 \pmod 3$
- $5^3 \equiv 5 \pmod 3$
- etc.


RECALL DIFFIE-HELLMAN
Alice's private space
secret: a
$A = g^a \bmod p$
Bob's private space
secret: b
$B = g^b \bmod p$
p, g
PUBLIC DIRECTORY
Alice .... A
Bob .... B
$B^a \bmod p$
$A^b \bmod p$

Recall the Diffie-Hellman Setup

- Fix a large prime number p. Hereafter all the numbers are in $\{0, 1, \ldots, p-1\}$ and arithmetic is modulo p (more on it later).
- Pick a generator g. A generator has the property that g^i generates all elements in $\{1, 2, \ldots, p-1\}$ when $i = 0, 1, \ldots, p-2$.
- *Note:* Towards the end of this chapter, after introducing all of the algebra necessary, we will see that a generator always exists since we are in what is called a *cyclic group.*

Example

$p = 5$. The numbers are $\{0, 1, 2, 3, 4\}$.

$g = 2$ is a generator. Indeed:

i	g^i
0	1
1	2
2	4
3	3

We are now in a position to deliver on this.

Specifically: Exponentiation can be defined on any finite group, but its inverse, the logarithm, is well-defined only for cyclic groups.

Next, we define cyclic groups and study their properties.

Given a finite commutative group $(G, \star)$, we can take any of its elements, say $g \in G$, and compute g^2, g^3, ..., until for some n (the order of g), $g^n = e$, where e is the identity in G.

The result is the group $H = \{e, g, g^2, \ldots, g^{n-1}\}$.

H is the cycle of a single element, g. Any finite group of cardinality n, that consists of the cycle of a group element g is called a **cyclic group of order n**, and g is called a **generator**. A generator is not necessarily unique.

Note: even if $(G, \star)$ is infinite and non-commutative, $(H, \star)$ is finite (by construction) and commutative. Indeed, $g^i \star g^k = g^{i+k} = g^k \star g^i$.

Example (cyclic group)

$(\mathbb{C}, \cdot)$ is an infinite group that contains $j = \sqrt{-1}$.

$$\left(H = \left\{j, j^2, j^3, j^4 = 1\right\}, \cdot\right)$$

is a cyclic group, and j as well as $-j$ are generators.

Example (cyclic group)

$\left(\mathbb{Z}/m\mathbb{Z}, +\right)$ is a cyclic group of order m and $g = 1$ is one of its generators.

$g=1,\ g^2=2,\ g^3=3,\ldots g^m=m=0$

Example (cyclic group)

$\left(\mathbb{Z}/5\mathbb{Z}^*, \times\right)$ is a finite commutative group. Its elements are $\{1, 2, 3, 4\}$. The group can be generated by the powers of 2. Hence the group is a cyclic group of order $n = 4$ and $g = 2$ is one of its generators.

$g = 2$: $g^2 = 4$, $g^3 = 3$

$g^4 = 1$, $g^5 = 2$

All cyclic groups that have the same order are isomorphic.

Proof: Let $(G, \star)$ and $(H, *)$ be cyclic groups of order n generated by g and h, respectively.

The map

$$\begin{array}{rccc} \psi: & G & \to H & \\ & g^i & \mapsto & h^i. \end{array}$$

is an isomorphism: In fact

- it is a bijection and
- for $a = g^i$ and $b = g^j$ we have

$$\psi(a \star b) = \psi(g^i \star g^j) = \psi(g^{i+j}) = h^{i+j} = h^i * h^j = \psi(a) * \psi(b).$$

□

Let $(G, \star)$ be a cyclic group of order n generated by g.

Let $b = g^i$ be one of its elements, $1 \leq i \leq n$.

The order of b is the smallest k such that $b^k = g^{ik}$ equals e.

ik is the smallest multiple of n and i, i.e.,

$$k = \frac{\text{lcm}(i, n)}{i} = \frac{n}{\gcd(i, n)}.$$

EXAMPLE

$\left(\mathbb{Z}/5\mathbb{Z}^*, \times\right)$ is a cyclic group of order $n = 4$, and $g = 2$ is a generator.

Let $i = 2$ and consider the group element $b = g^i = 4$. The order of b is

$$\frac{n}{\gcd(i, n)} = \frac{4}{\gcd(2, 4)} = 2.$$

(Let us verify: $b^2 = \left(2^2\right)^2 = 1$, as it should.)

g^i is another generator iff it has order n, i.e. iff $\gcd(i, n) = 1$.

The number of such i in $\{1, \ldots, n\}$ is Euler's $\phi(n)$.

EXAMPLE

The elements of $\left(\mathbb{Z}/5\mathbb{Z}^*, \times\right)$ are $\{1, 2, 3, 4\}$, and $g_1 = 2$ is a generator.

Hence $\left(\mathbb{Z}/5\mathbb{Z}^*, \times\right)$ is a cyclic group of order 4.

There are $\phi(4) = 2$ generators, one for each i such that $\gcd(i, 4) = 1$. Those i are $i = 1$ and $i = 3$. The other generator is $g_2 = g_1^3 = 3$.

Recall that we have proved the following: a cyclic group of order n has $\phi(n)$ generators.

However, not all groups are cyclic.

Example (A non-cyclic group)

The elements of the group $\left(\mathbb{Z}/24\mathbb{Z}^*, \times\right)$ are $\{1, 5, 7, 11, 13, 17, 19, 23\}$.

The cardinality of this group is $n = 8$. However, it would be a mistake to conclude that the group has $\phi(8) = 4$ generators.

All we can say is that if it has a generator (in this case the group is a cyclic group of order 8), then it has 4 generators.

But in fact, this group has no generator: except for 1, all the elements have order 2.

For any element h of a finite commutative group $(G, \star)$, the discrete exponentiation h^i is well-defined for any integer i. (Note that i is an integer, not an element of $(G, \star)$.)

The discrete logarithm to the base $b \in G$ of $h \in G$ is the integer i such that $b^i = h$. This is well-defined (for every $h \in G$) iff $(G, \star)$ is a **cyclic group, and b is one of its generators**.

Let $(G, \star)$ be a cyclic group of order n generated by b. The discrete exponentiation to the base b is the map

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & G \\ & [i]_n & \mapsto & b^i. \end{array}$$

We prove that it is well-defined and that it is an isomorphism from $(\mathbb{Z}/n\mathbb{Z}, +)$ to $(G, \star)$.

Proofs:

We show that the map is well-defined: suppose that $[i]_n = [j]_n$, then $j = i + nk$ for some integer k, and

$$f([j]_n) = g^{i+nk} = g^i \star g^{nk} = g^i = f([i]_n).$$

Next we show tha the map is one-to-one: If $f([i]_n) = f([j]_n)$, then:

- $g^i = g^j$;
- $g^{i-j} = e$;
- $i - j \in \{0, n, 2n, \dots\}$;
- $[i]_n = [j]_n$.

By the pigeonhole principle, the map is also onto, hence it is a bijection.

Finally we prove that $f : \mathbb{Z}/n\mathbb{Z} \to G$ is an isomorphism:

$$f([i]_n + [j]_n) = g^{i+j} = g^i \star g^j = f([i]_n) \star f([j]_n).$$

□

The inverse map

$$\begin{array}{rccc} f^{-1}: & G & \to & \mathbb{Z}/n\mathbb{Z} \\ & a = b^i & \mapsto & [i]_n, \end{array}$$

is called the **discrete logarithm to the base** b. Naturally, we write

$$[i]_n = \log_b a.$$

Note that the usual rules for exp and log apply: Specifically, for any group generator b of order n, we have:

- $(a^i)^j = a^{ij}$;
- $a^i a^j = a^{i+j}$;
- $\log_b(c \star d) = \log_b c + \log_b d$;
  Mind that on the RHS we have elements of $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$;
- $\log_b a^k = [k]_n \log_b a$.

For an element of a group of order n, discrete exponentiation requires at most $2\log_2 n$ operations. Let us count them:

- to compute a^k, $1 < k < n$, we write k in binary form using $L = \log_2 n$ bits:

$$k = \sum_{i=0}^{L-1} b_i 2^i, \text{ with } b_i \in \{0, 1\};$$

- now

$$\begin{aligned} a^k = a^{\sum_{i=0}^{L-1} b_i 2^i} &= \prod_{i=0}^{L-1} a^{b_i 2^i} \\ &= \prod_{i=0}^{L-1} \left(a^{2^i}\right)^{b_i} \\ &= \prod_{i=0}^{L-1} a_i^{b_i}, \end{aligned}$$

where $a_i = a^{2^i}$ is computed as follows:

$$\begin{aligned} a_0 &= a \\ a_1 &= a_0^2 \\ a_2 &= a_0^4 = a_1^2 \\ a_3 &= a_0^8 = a_2^2 \\ &\vdots \\ a_{L-1} &= a_0^{2^{L-1}} = a_{L-2}^2. \end{aligned}$$

- It takes $L-1$ operations to compute $a_1, \ldots, a_{L-1}$ It takes at most $L-1$ operations to compute $\prod_{i=0}^{L-1} a_i^{b_i}$. (No computation required to perform $a_i^{b_i}$.)
- The total number of operations is at most $2(L-1) < 2\log_2 n$. □

FINDING THE INVERSE

Recall that in ElGamal's scheme, to invert the function we compute the inverse of g^{yx}. To compute the multiplicative inverse of a number $[b]_m \in (\mathbb{Z}/m\mathbb{Z}^*, \cdot)$, we can proceed two ways:

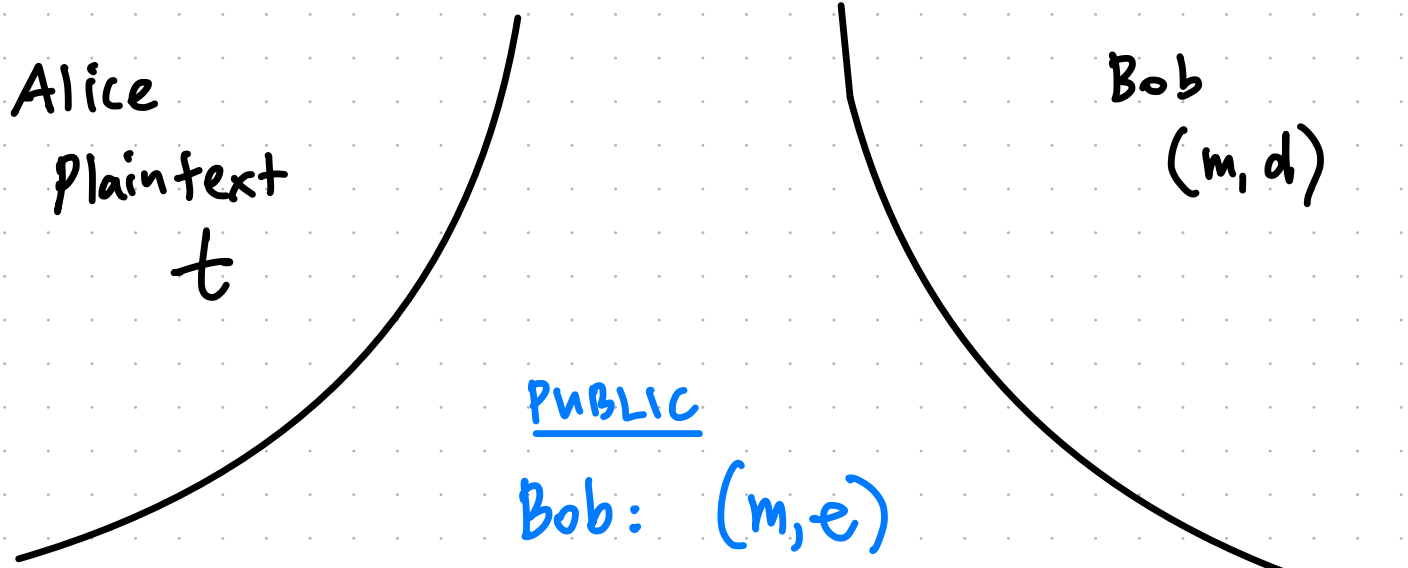
1. we use Bézout to write $1 = \gcd(b, m) = bu + mv$, hence $[u]_m$ is the inverse;

2. we use the fact that $[b]_m^{\phi(m)} = 1$, hence $[b]_m^{\phi(m)-1}$ is the inverse.

Often Bézout is more efficient, but if m is prime, we know that $\phi(m) = m - 1$. Exponentiation can be done efficiently.

If we are in a cyclic group of order n, then we know that $b^n = 1$. Hence the inverse of b is b^{n-1}.

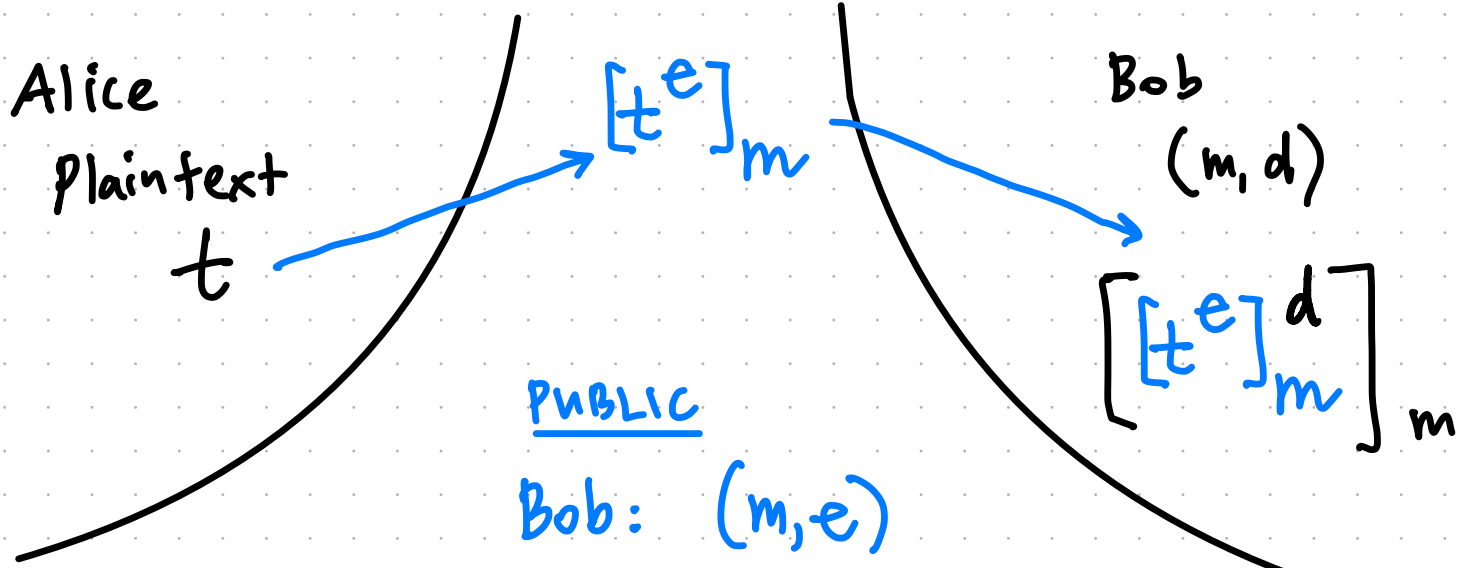
SNEAK PEAK OF RSA



all operations are in

$(\mathbb{Z}/m\mathbb{Z}, \cdot)$

SNEAK PEAK OF RSA



PUBLIC

Bob: (m, e)

all operations are in

$(\mathbb{Z}/m\mathbb{Z}, \cdot)$

$$\left[\left[t^{e}\right]_{m}^{d}\right]_{m} = \left[t^{ed}\right]_{m}$$

Let us select $m = p$, a prime.

Consider $(\mathbb{Z}/p\mathbb{Z}^*, \cdot)$.

cardinality $\phi(p) = p - 1$.

Let us select $m = p$, a prime.

Consider $(\mathbb{Z}/p\mathbb{Z}^*, \cdot)$.

cardinality $\phi(p) = p - 1$.

We have seen that

$$\left[t^{k\phi(p)}\right]_p = [1]_p$$

holds for all $t \in \mathbb{Z}/p\mathbb{Z}^*$.

Let us select $m = p$, a prime.

Consider $(\mathbb{Z}/p\mathbb{Z}^*, \cdot)$.

cardinality $\phi(p) = p - 1$.

We have seen that

$$[t^{k\phi(p)}]_p = [1]_p$$

holds for all $t \in \mathbb{Z}/p\mathbb{Z}^*$.

Hence

$$[t^{k\phi(p)+1}]_p = [t]_p$$

Let us select $m = p$, a prime.

Moreover, for $t = [0]$, we also have

$$[t^{k\phi(p)+1}]_p = [t]_p.$$

no star!

Hence, for all $t \in \mathbb{Z}/p\mathbb{Z}$:

$$[t^{k\phi(p)+1}]_p = [t]_p$$

Let us select $m = p$, a prime.

We want

$$[t^{ed}]_p = [t]_p.$$

Hence, select e, d such that

$$ed = k\,\phi(p) + 1$$

$$ed + \tilde{k}\,\phi(p) = 1$$

Let us select $m = p$, a prime.

We want

$$[t^{ed}]_p = [t]_p.$$

Hence, select e, d such that

$$ed = k\phi(p) + 1$$

By Bézout, if e and $\phi(p)$ are coprime, then d and k exist to satisfy this!