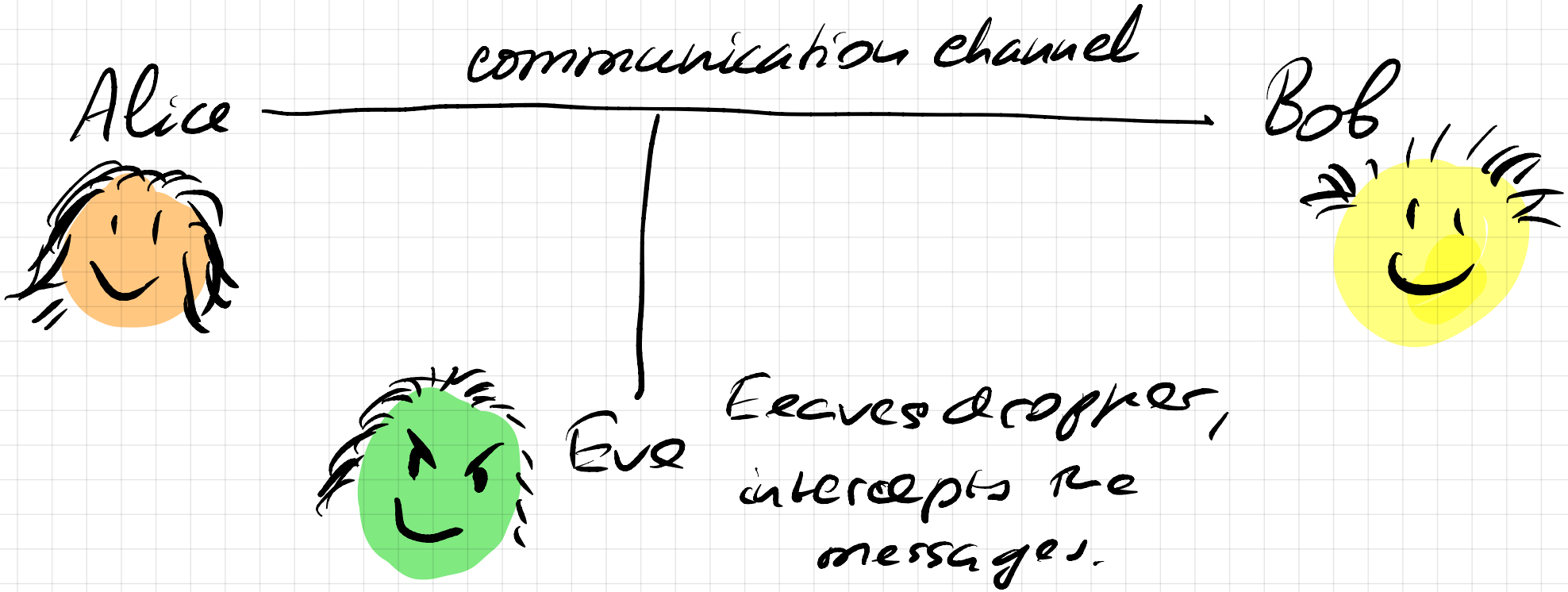
0 Introduction



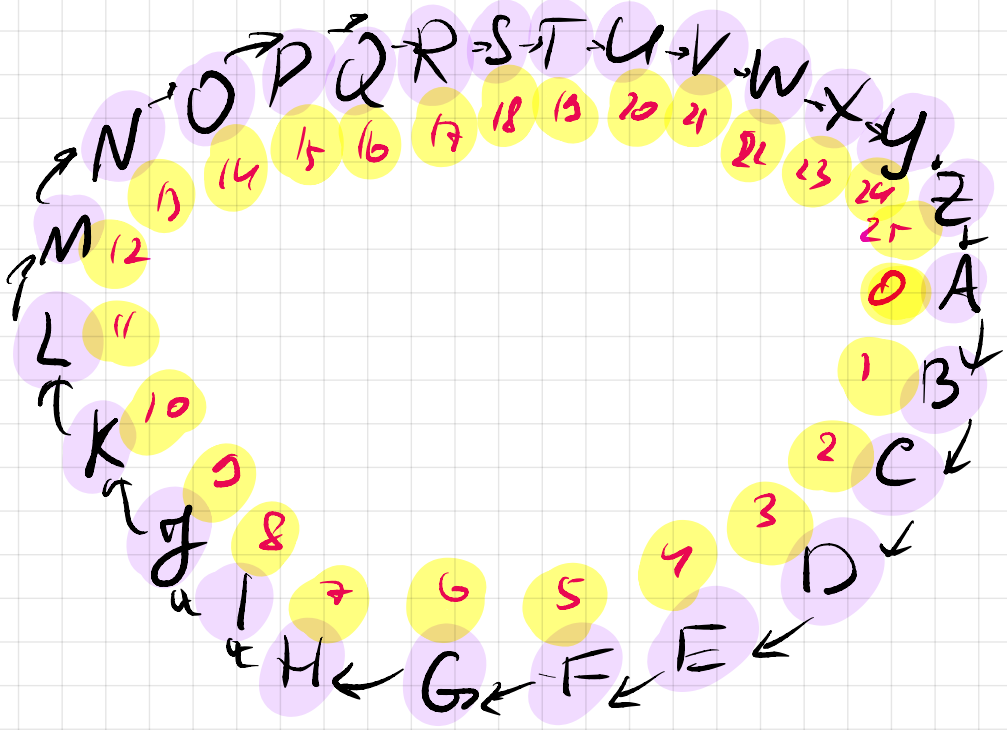
Alice and Bob want to establish secure communication via encryption / decryption

Eve wants to break the cipher.

Example

Caesar's cypher.

Alphabet: $A \hat{=} 0$, $B \hat{=} 1$, $\ldots$, $Z \hat{=} 25$



A key $k \in \{0, \ldots, 25\}$, which Alice and Bob choose and decide to use.

Encryption:

$$e_k(x_1, \ldots, x_n) = (y_1, \ldots, y_n),$$ where

$x_1, \ldots, x_n$: symbols of the plaintext message

$$y_i = (x_i + k) \bmod 26$$

Remainder of the division of $x_i + k$ by 26.

Decryption:

$$d_k(y_1, \ldots, y_n) = (x_1, \ldots, x_n)$$

$y_1, \ldots, y_n$: cypher text

$$x_i = (y_i - k) \bmod 26.$$

Definition A cryptosystem consists of

$\mathcal{K}$, a set keys,

$\mathcal{P}$, a set of plaintexts.

$\mathcal{C}$, a set of ciphertexts

$e_k : \mathcal{P} \longrightarrow \mathcal{C}$ encryption functions, parametrized by keys $k \in \mathcal{K}$.

$d_k : \mathcal{C} \longrightarrow \mathcal{P}$ decryption functions, parametrized by key $k \in \mathcal{K}$

such that $d_K(e_K(x)) = x$

for every $x \in \mathcal{P}$ and every $K \in \mathcal{K}$.

We assume $\mathcal{K}, \mathcal{P}, \mathcal{C}$ to be non-empty finite sets.

Whenever you don't know some of the notation or terminology that I use without explanation, ask me, and I will explain it.

Some basic math to clarify first:

$\mathbb{N} := \{1, 2, 3, \dots\}$ set of natural numbers

$\mathbb{N}_0 := \{0, 1, 2, 3 \dots\}$ set of non-negative integers

$\mathbb{Z} := \{0, 1, -1, 2, -2, 3, -3 \dots\}$ set of integers.

For a set A, by $|A|$ we denote its size
= number of elements = cardinality

Notation $f: X \longrightarrow Y$ means that f is a map (i.e. a function) that goes from X (the domain) to Y (the range). The function f gives exactly one $f(x) \in Y$ for each $x \in X$.

Injective: $x, x' \in X$ and $x \neq x'$, then $f(x) = f(x')$.

Surjective: every $y \in Y$ is $y = f(x)$ for some $x \in X$

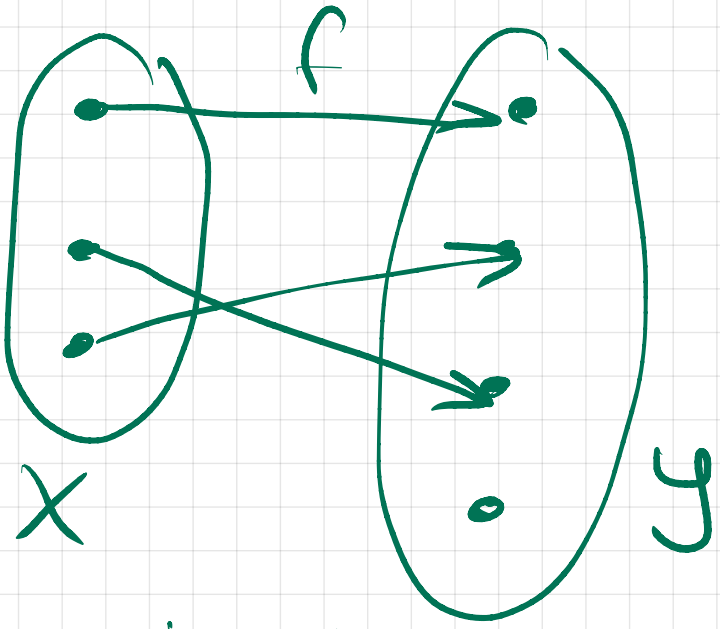
Bijective: injective and surjective.

bijective for $f: X \to Y$

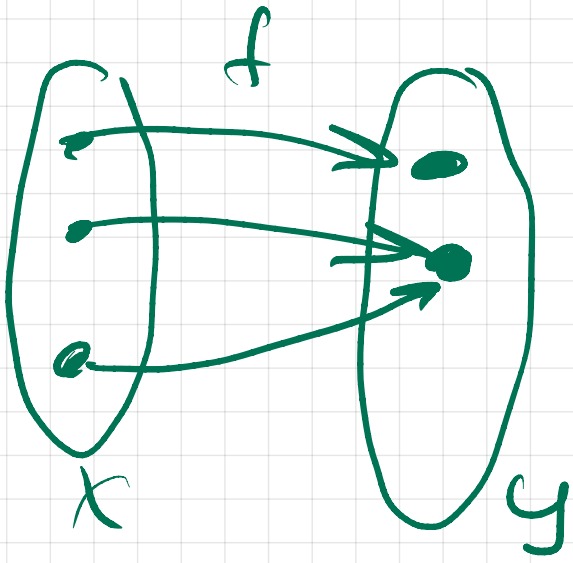
means: different inputs in X go to different outputs and every element in Y is an output for some input.

Injective
Bijective
Surjective

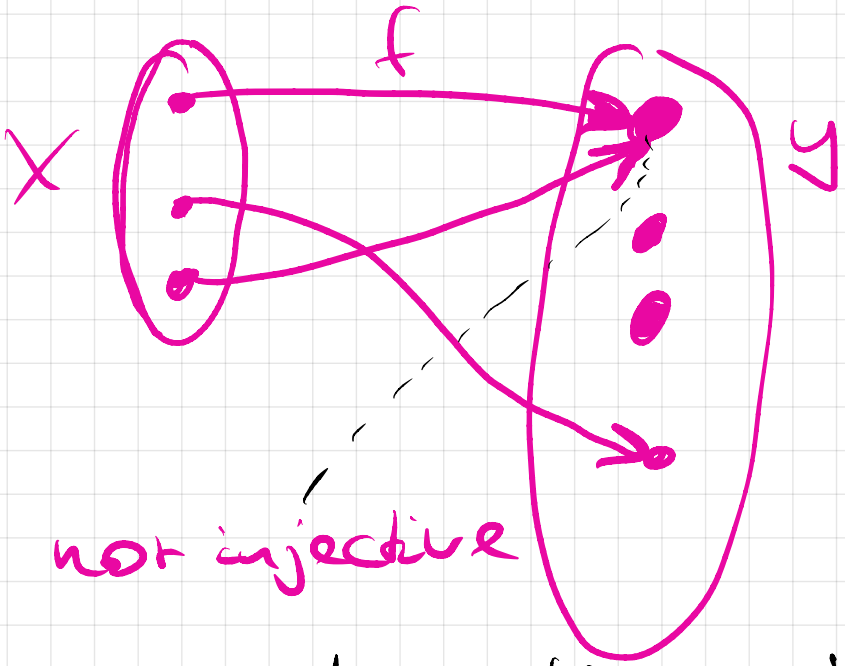
explained with pictures



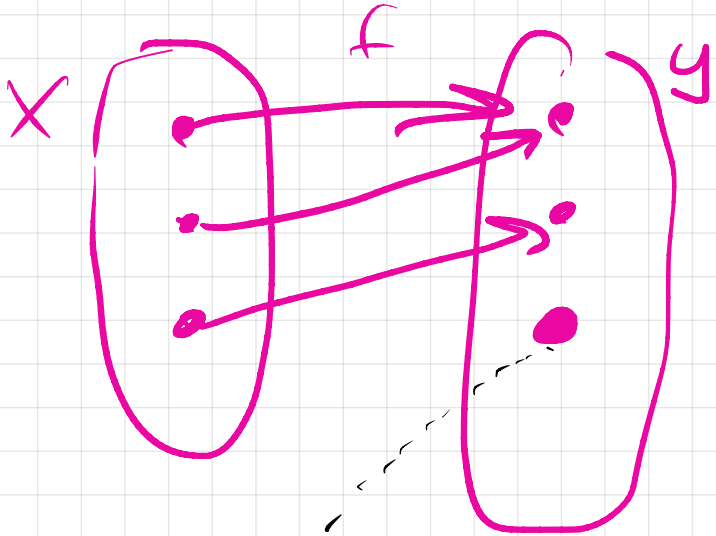
injective



surjective



not injective



not surjective

bijective = injective and surjective

1 Public-key Cryptography

Basic idea of public key cryptography

Public key

Accessible to everyone.

It can only close the mailbox, but not open.

Alice has another key, accessible only to herself, the private one

. This one can only open the box.

P.1 Modular arithmetic

We introduce the integer ring modulo n as follows.

For $x, y \in \mathbb{Z}$ and $n \in \mathbb{N}$ we say that

x and y are congruent modulo $n \in \mathbb{N}$

if $x - y$ is divisible by n, in other words,

they have the same remainder after division by n.

The way of writing:

$$x \equiv y \pmod{n}.$$

The residue class of x modulo n,

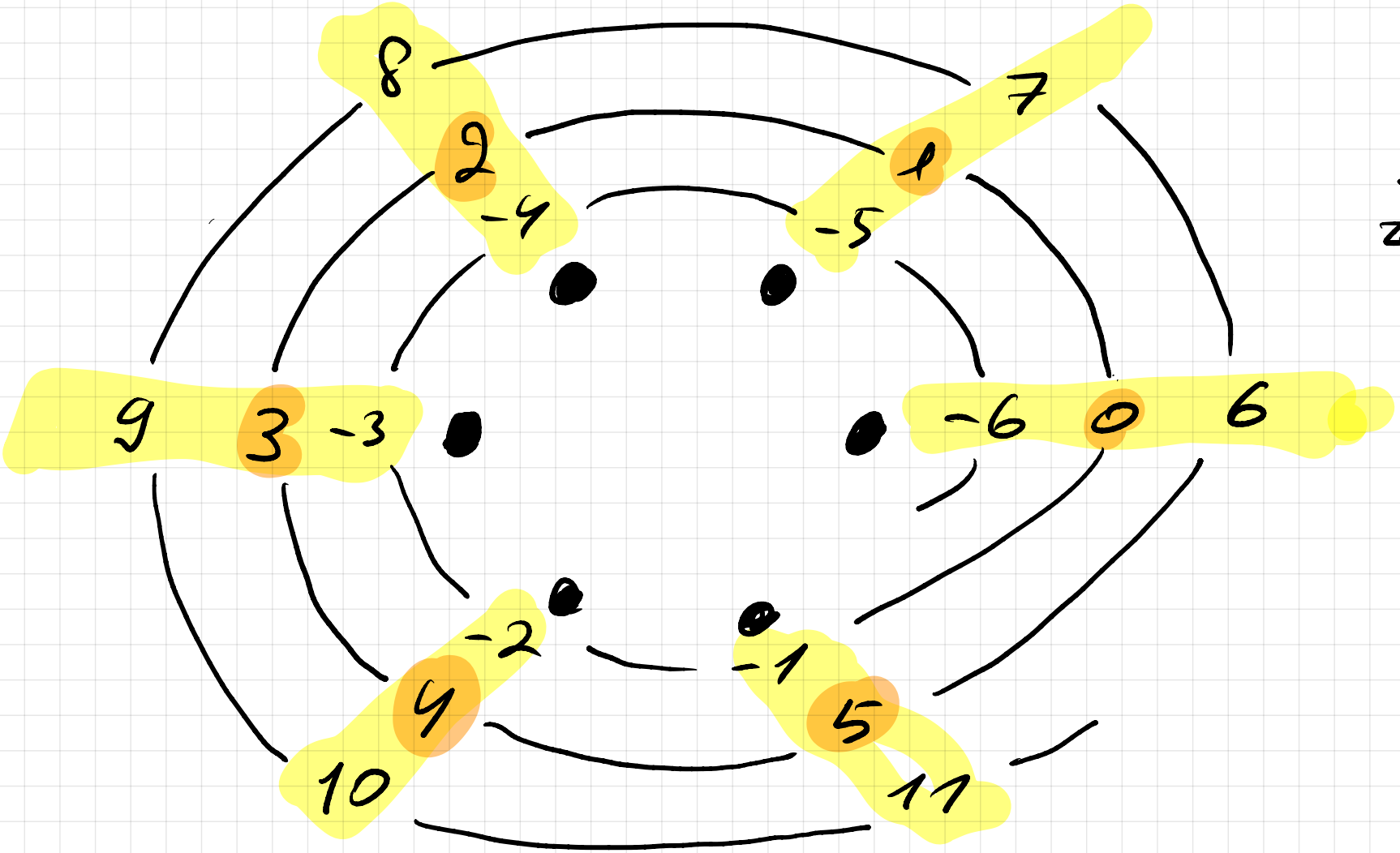
also known as coset modulo n,

is defined by

$$[x]_n := \{ y \in \mathbb{Z} : x \equiv y \pmod{n} \}$$

Sometimes, one omits the subscript n, if it's clear from the context.

Wrap integers onto a cylinder...



$\mathbb{Z}_6$

By $\mathbb{Z}_n$ we denote the set of all cosets modulo n,

$$\mathbb{Z}_n := \{ [x]_n : x \in \mathbb{Z} \}$$

$$= \{ [0]_n, [1]_n, \ldots, [n-1]_n \}$$

Other notation used for this: $\mathbb{Z}/n$, $\mathbb{Z}/n\mathbb{Z}$.

We can do algebra on $\mathbb{Z}_n$ by introducing $+$ and $\cdot$ as follows:

$$[x]_n + [y]_n := [x+y]_n \quad \left\{ \text{for } x, y \in \mathbb{Z} \right.$$
$$[x]_n \cdot [y]_n := [x \cdot y]_n$$

This makes $\mathbb{Z}_n$ to a so called commutative unitary ring, when $n \geq 2$.
That's a structure $(\mathbb{Z}_n, +, \cdot)$ endowed with two operations, obeying certain rules.

Structure $\approx$ set of objects plus interface

algebraic structure $\approx$ set of objects plus algebraic interface ($+$, $\cdot$ etc.).

Def. A unitary commutative ring is a structure $(R, +, \cdot)$ with operations

$$+ : R \times R \longrightarrow R$$

$$\cdot : R \times R \longrightarrow R$$

and two special constants $0 = 0_R$ and $1 = 1_R$ such that $0 \neq 1$ and the following rules are true:

		NAMES OF LAWS
$a + 0 = a$	$a \cdot 1 = a$	neutral elem.
$a + b = b + a$	$a \cdot b = b \cdot a$	commutative
$(a + b) + c = a + (b + c)$	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	associative

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{distributive}$$

for all $a, b, c \in R$.

and for every $a \in R$ there exists some $b \in R$ such that $a + b = 0$.

Remark. For $a \in R$ the b satisfying $a + b = 0$ turns out to be unique. It is denoted by $b = -a$, and is called the negative of a or the additive inverse of a. Once we clarified this, we can define the substraction for $x, y \in R$ by $x - y := x + (-y)$.

So, in ways we can do $+$, $\cdot$ and $-$

But, in general, we cannot do division unconditionally. This means:

sometimes, the equation $a \cdot x = b$ with $a, b \in R$ has a unique solution x and then we can define the quotient $x = \frac{b}{a}$, but not always, in general.

Remark. unitary means: it has 1

commutative means: multiplication is commutative.

There are more structures in algebra: both simpler and more involved. We focus on unitary commutative rings, because we'll make a direct use of them.

Fact $(\mathbb{Z}_n, +, \cdot)$, when $n \geq 2$, is a unitary commutative ring.

Remark $0_{\mathbb{Z}_n} = [0]_n$

$1_{\mathbb{Z}_n} = [1]_n$

Def. For a unitary commutative ring $(R, +, \cdot)$ an element $a \in R$ is called a unit if a is invertible with respect to multiplication, which means that there exists some $b \in R$ with

$$a \cdot b = 1.$$

(if it exists, it turns out to be unique (which needs to be shown) and is denoted by $b = a^{-1}$.

Remark One can always invert 1 and -1.
One can never invert 0
because $0 \cdot x = 0$ for every $x \in \mathbb{R}$
(which one can show).

$1^{-1} = 1$, because $1 \cdot 1 = 1$

$(-1)^{-1} = -1$, because $(-1) \cdot (-1) = 1$

What can we invert in $\mathbb{Z}_n$?

Example Let's make a table for $\cdot$ in $\mathbb{Z}_5$

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	(1)	2	3	4
2	0	2	4	(1)	3
3	0	3	(1)	4	2
4	0	4	3	2	(1)

$[1]^{-1} = [1]$

$[2]^{-1} = [3]$

$[3]^{-1} = [2]$

$[4]^{-1} = [4] = -[1]$

We omit $[\dots]$ for brevity.

↳ In $\mathbb{Z}_5$ you can divide by every non-zero element, which means that $\mathbb{Z}_5$ is a so-called **field**

$[4] + [1] = [4+1] = [5] = [0]$

$\Rightarrow [4] = -[1]$.

← field remark.

If you want to solve the equation

$a x = b$ with $a, b \in \mathbb{Z}_5$ and $a \neq 0$,

you can always do this:

$$a x = b$$

$$\Updownarrow$$

$$\bar{a}^{1} \cdot a \cdot x = \bar{a}^{1} \cdot b$$

$$\Updownarrow$$

$$x = a^{-1} \cdot b$$

To phrase it yet another way, we can see that the function $f: \mathbb{Z}_5 \to \mathbb{Z}_5$ which is linear, i.e. $f(x) = a \cdot x$ and non-zero, i.e. $a \neq 0$, is bijective.

$f(x) = 2x$ $\quad f: \mathbb{Z}_5 \to \mathbb{Z}_5$

x	0	1	2	3	4
$2x$	0	2	4	1	3

$1 \mapsto 4$ in some randomly looking order.

Example. $(\mathbb{Z}_6, +, \cdot)$

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The only two invertible elements are

$[1] = 1_{\mathbb{Z}_6}$ and $[5] = -[1] = -1_{\mathbb{Z}_6}$

In this ring you can have

$[2] \cdot [3] = [0] = 0_{\mathbb{Z}_6}$

Non-zero $\times$ Non-zero = Zero.

Weird!

Example. $\mathbb{Z}_{35}$ $\quad 35 = 5 \cdot 7$

$$[5] \cdot [7] = [0].$$

(If $[5]^{-1}$ existed, we'd have

$$[5]^{-1} \cdot [5] \cdot [7] = [5]^{-1} \cdot [0]$$

This would give $[7] = [0]$, which is not true. So, $[5]^{-1}$ does not exist. Such kind of argument is called a proof by contradiction.

Def For $(R, +, \cdot)$ (unitary commutative ring).

We denote by $R^\times$ the set of all units in R (i.e. the set of all invertible elements).

If $R^\times = R \setminus \{0\}$ (that is, if all non-zero elements are invertible), then R is called a field.

Alternative notation for $R^\times$ is R^*.

Examples.

$\mathbb{Z}_5$ is a field

$\mathbb{Z}_6, \mathbb{Z}_{35}$ are not fields

$\mathbb{Q}$ (rationals) form a field.

$\mathbb{R}$ (real numbers) form a field.

Remark. We can interpret Caesar's ciphers in the $\mathbb{Z}_n$ terminology. Caesar's ciphers uses $f(x) = x + b$ as $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ to reshuffle the 26-letter alphabet. This function is clearly invertible:

$$y = x + b \iff x = y - b.$$

Limit on the # of participants?

Summary:

- We learned what a cryptosystem is
- We learned about $\mathbb{Z}_n$ and saw examples in which $\mathbb{Z}_n$ was a field and some other examples where it was not a field.
- Calculations in $\mathbb{Z}_n$ will help us establish cryptosystems