

Modular arithmetic. Fermat's Little Theorem.
Arithmetic in $\mathbb{Z}_n$

Irena Penev

September 29, 2026

- This lecture covers sections 0.2 of the Lecture Notes (<https://iuuk.mff.cuni.cz/~ipenev/LALectureNotes.pdf>).

Notation: Throughout this course, we will use the following notation:

- $\mathbb{N}$ is the set of all natural numbers (positive integers);
- $\mathbb{N}_0$ is the set of all non-negative integers;
- $\mathbb{Z}$ is the set of all integers;
- $\mathbb{Q}$ is the set of all rational numbers;
- $\mathbb{R}$ is the set of all real numbers;
- $\mathbb{C}$ is the set of all complex numbers.

This lecture has three parts:

- ① Modular arithmetic
- ② Fermat's Little Theorem
- ③ Arithmetic in $\mathbb{Z}_n$

1 Modular arithmetic

- Given $n \in \mathbb{N}$ and $m \in \mathbb{Z}$, we write $n \mid m$ if m is divisible by n , that is, if there exists some $k \in \mathbb{Z}$ s.t. $m = kn$. Otherwise (i.e. if m is **not** divisible by n), we write $n \nmid m$.

Definition

Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we say that a and b are *congruent modulo n* , and we write

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b,$$

provided that $n \mid (a - b)$, i.e. $a - b = kn$ for some $k \in \mathbb{Z}$; equivalently, we have that $a \equiv b \pmod{n}$ provided that a and b leave the same remainder when divided by n (where the remainder is required to be one of the integers $0, 1, \dots, n - 1$).

- Note that for a positive integer n and an integer a , we have that a is divisible by n (equivalently: a is a multiple of n) iff $a \equiv 0 \pmod{n}$.

Definition

Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we say that a and b are *congruent modulo n* , and we write

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b,$$

provided that $n \mid (a - b)$, i.e. $a - b = kn$ for some $k \in \mathbb{Z}$; equivalently, we have that $a \equiv b \pmod{n}$ provided that a and b leave the same remainder when divided by n (where the remainder is required to be one of the integers $0, 1, \dots, n - 1$).

Example 0.2.1

All the following hold:

- $2 \equiv 17 \pmod{3}$;
- $-13 \equiv 8 \pmod{7}$;
- $-1 \equiv 7 \pmod{4}$;
- $2 \not\equiv 17 \pmod{2}$;
- $-13 \not\equiv 8 \pmod{5}$;
- $-1 \not\equiv 7 \pmod{6}$.

Definition

Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we say that a and b are *congruent modulo n* , and we write

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b,$$

provided that $n \mid (a - b)$, i.e. $a - b = kn$ for some $k \in \mathbb{Z}$; equivalently, we have that $a \equiv b \pmod{n}$ provided that a and b leave the same remainder when divided by n (where the remainder is required to be one of the integers $0, 1, \dots, n - 1$).

- **Remark:** For fixed $n \in \mathbb{N}$, every integer is congruent modulo n to exactly one of the following n integers: $0, \dots, n - 1$.
 - Indeed, for $k \in \{0, \dots, n - 1\}$, the integers congruent to k modulo n are k itself, plus those that can be reached via a certain number steps of length n (to the left or to the right).
 - We represent this on the next slide via color coding.

- For $n = 2$, an integer k can satisfy $k \equiv 0 \pmod{2}$ or $k \equiv 1 \pmod{2}$.

$\dots, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots$

- For $n = 3$, an integer k can satisfy $k \equiv 0 \pmod{3}$, $k \equiv 1 \pmod{3}$, or $k \equiv 2 \pmod{3}$.

$\dots, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots$

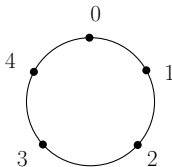
- For $n = 4$, an integer k can satisfy $k \equiv 0 \pmod{4}$, $k \equiv 1 \pmod{4}$, $k \equiv 2 \pmod{4}$, or $k \equiv 3 \pmod{4}$.

$\dots, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots$

- For $n = 5$, an integer k can satisfy $k \equiv 0 \pmod{5}$, $k \equiv 1 \pmod{5}$, $k \equiv 2 \pmod{5}$, $k \equiv 3 \pmod{5}$, or $k \equiv 4 \pmod{5}$.

$\dots, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots$

- **Remark:** Congruence modulo n can also be visualized in terms of an “ n -hour clock” (see the picture below for the case $n = 5$).



- Suppose we are given an integer a , and we wish to determine which of $0, 1, \dots, n-1$ it is congruent to modulo n .
- Obviously, if $a = 0$, then $a \equiv 0 \pmod{n}$.
- If a is positive, then we start at 0 and make a clockwise steps; the number we finish at is the number we need.
 - For example, we have that $14 \equiv 4 \pmod{5}$ because if we start at 0 and then make 14 steps clockwise on the 5-hour clock, we finish at 4.
- On the other hand, if a is negative, then we make $|a| = -a$ many counterclockwise steps.
 - For example, we have that $-7 \equiv 3 \pmod{5}$ because if we start at 0 and then make 7 steps counterclockwise on the 5-hour clock, then we finish at 3.

Definition

Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we say that a and b are *congruent modulo n* , and we write

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b,$$

provided that $n \mid (a - b)$, i.e. $a - b = kn$ for some $k \in \mathbb{Z}$; equivalently, we have that $a \equiv b \pmod{n}$ provided that a and b leave the same remainder when divided by n (where the remainder is required to be one of the integers $0, 1, \dots, n - 1$).

- **Remark:** As we shall see, doing arithmetic modulo n essentially boils down to doing arithmetic with only n values (namely $0, \dots, n - 1$), as opposed to infinitely many. This is quite useful for certain applications.

Proposition 0.2.2

Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Then the following hold:

- Ⓐ $a \equiv a \pmod{n}$;
- Ⓑ if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;
- Ⓒ if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

- **Remark:** Proposition 0.2.2 states that congruence modulo n is an “equivalence relation” on $\mathbb{Z}$. (Equivalence relations are studied in Discrete Mathematics.)

Proposition 0.2.2

Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Then the following hold:

- Ⓐ $a \equiv a \pmod{n}$;
- Ⓑ if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;
- Ⓒ if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proof. For (a), we simply observe that

$$n \mid \underbrace{(a - a)}_{=0},$$

and so $a \equiv a \pmod{n}$.

For (b), we have the following equivalent statements:

$$\begin{aligned} a \equiv b \pmod{n} &\iff n \mid (a - b) && \text{by definition} \\ &\iff n \mid (b - a) \\ &\iff b \equiv a \pmod{n} && \text{by definition.} \end{aligned}$$

Proposition 0.2.2

Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Then the following hold:

- Ⓐ $a \equiv a \pmod{n}$;
- Ⓑ if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;
- Ⓒ if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proof (continued). It remains to prove (c). So, assume that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. By definition, this means that $n \mid (a - b)$ and $n \mid (b - c)$, that is, there exist $k, \ell \in \mathbb{Z}$ s.t. $a - b = kn$ and $b - c = \ell n$. But then

$$a - c = (a - b) + (b - c) = kn + \ell n = (k + \ell)n,$$

i.e. $n \mid (a - c)$. Thus, $a \equiv c \pmod{n}$. $\square$

Proposition 0.2.3

Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$, and assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

- Ⓐ $a + c \equiv b + d \pmod{n}$;
- Ⓑ $a - c \equiv b - d \pmod{n}$;
- Ⓒ $ac \equiv bd \pmod{n}$.

Proof. Parts (a) and (b) are easy (see the Lecture Notes). Let us prove (c).

Since $a \equiv b \pmod{n}$, we have that $n \mid (a - b)$, and so there exists some $k \in \mathbb{Z}$ s.t. $a - b = kn$. Similarly, since $c \equiv d \pmod{n}$, there exists some $\ell \in \mathbb{Z}$ s.t. $c - d = \ell n$.

$$\begin{aligned} ac - bd &= ac - ad + ad - bd \\ &= a(c - d) + (a - b)d \\ &= a\ell n + knd \\ &= (a\ell + dk)n, \end{aligned}$$

and so $n \mid (ac - bd)$. Thus, $ac \equiv bd \pmod{n}$. This proves (c). $\square$

Proposition 0.2.3

Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$, and assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

- Ⓐ $a + c \equiv b + d \pmod{n}$;
- Ⓑ $a - c \equiv b - d \pmod{n}$;
- Ⓒ $ac \equiv bd \pmod{n}$.

- **Warning:** Do not divide!!!

- For example, we have that $4 \equiv 8 \pmod{4}$, but if we divide both sides by 2, we get $2 \not\equiv 4 \pmod{4}$.

Proposition 0.2.3

Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$, and assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

- Ⓐ $a + c \equiv b + d \pmod{n}$;
- Ⓑ $a - c \equiv b - d \pmod{n}$;
- Ⓒ $ac \equiv bd \pmod{n}$.

- Via repeated application of Proposition 0.2.3, we get the following:

Proposition 0.2.4

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Assume that $a \equiv b \pmod{n}$. Then $a^t \equiv b^t \pmod{n}$ for all integers $t \geq 0$.

- **Remark:** The formal proof uses mathematical induction (Lecture Notes).

Proposition 0.2.2

Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Then the following hold:

- (a) $a \equiv a \pmod{n}$;
- (b) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;
- (c) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proposition 0.2.3

Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$, and assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

- (a) $a + c \equiv b + d \pmod{n}$;
- (b) $a - c \equiv b - d \pmod{n}$;
- (c) $ac \equiv bd \pmod{n}$.

Proposition 0.2.4

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Assume that $a \equiv b \pmod{n}$. Then $a^t \equiv b^t \pmod{n}$ for all integers $t \geq 0$.

- **Notation:** For $a_n, a_{n-1}, \dots, a_0 \in \{0, 1, \dots, 9\}$, we define:

$$\overline{a_n a_{n-1} \dots a_0} := \sum_{k=0}^n a_k 10^k.$$

Thus, $\overline{a_n a_{n-1} \dots a_0}$ is the number whose first digit is a_n , whose second digit is a_{n-1} , and so on.

Proposition 0.2.6

Let $a = \overline{a_n a_{n-1} \dots a_0}$. Then $a \equiv a_n + a_{n-1} + \dots + a_0 \pmod{9}$. Therefore, a positive integer is divisible by 9 iff the sum of its digits is divisible by 9.

Proposition 0.2.7

Let $a = \overline{a_n a_{n-1} \dots a_0}$. Then $a \equiv a_n + a_{n-1} + \dots + a_0 \pmod{3}$. Therefore, a positive integer is divisible by 3 iff the sum of its digits is divisible by 3.

- We prove Proposition 0.2.6. The proof of Proposition 0.2.7 is completely analogous (just replace 9 with 3 throughout).

Proposition 0.2.6

Let $a = \overline{a_n a_{n-1} \dots a_0}$. Then $a \equiv a_n + a_{n-1} + \dots + a_0 \pmod{9}$.
Therefore, a positive integer is divisible by 9 iff the sum of its digits is divisible by 9.

Proof. Note that the second statement follows from the first, via the following sequence of equivalent statements:

$9 \mid a$	$\iff$	$a \equiv 0 \pmod{9}$	by definition
	$\iff$	$a_n + a_{n-1} + \dots + a_0 \equiv 0 \pmod{9}$	by the first statement
	$\iff$	$9 \mid (a_n + a_{n-1} + \dots + a_0)$	by definition.

Proposition 0.2.6

Let $a = \overline{a_n a_{n-1} \dots a_0}$. Then $a \equiv a_n + a_{n-1} + \dots + a_0 \pmod{9}$. Therefore, a positive integer is divisible by 9 iff the sum of its digits is divisible by 9.

Proof (continued). It remains to prove the first statement.

Note that $10 \equiv 1 \pmod{9}$.

So, by Proposition 0.2.4, we have that $10^k \equiv 1 \pmod{9}$ for all non-negative integers k .

It follows that for all $k \in \{0, \dots, n\}$, we have that $a_k \cdot 10^k \equiv a_k \pmod{9}$. Consequently,

$$a = \overline{a_n a_{n-1} \dots a_0} = \sum_{k=0}^n a_k 10^k \equiv_9 \sum_{k=0}^n a_k = a_n + a_{n-1} + \dots + a_0.$$

This completes the argument. $\square$

2 Fermat's Little Theorem

- Two integers are said to be *relatively prime* if they have no common divisors strictly greater than 1.
 - In other words, $a, b \in \mathbb{Z}$ are relatively prime iff $\gcd(a, b) = 1$, where $\gcd(a, b)$ denotes the greatest common divisor of a and b .
- Before stating and proving Fermat's Little Theorem, we state and prove a related theorem and its corollary (next slide).
 - We first state the theorem and the corollary; then we prove the corollary (using the theorem); and then we prove the theorem.

Theorem 0.2.9

Let $n \in \mathbb{N}$ ($n \geq 2$) and $a \in \mathbb{Z}$.

- Ⓐ If a and n are relatively prime, then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$.
- Ⓑ If a and n are **not** relatively prime, then for all $b \in \mathbb{Z}$, we have that $ab \not\equiv 1 \pmod{n}$.

- Proof: Next slide!

Corollary 0.2.10

Let $p \in \mathbb{N}$ be a prime number. Then for all $a \in \mathbb{Z}$ s.t. a is **not** a multiple of p , there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$.

Proof (assuming Theorem 0.2.9). Since p is a prime number, every integer that is not a multiple of p is relatively prime to p . So, the result follows immediately from Theorem 0.2.9(a). $\square$

Theorem 0.2.9

Let $n \in \mathbb{N}$ ($n \geq 2$) and $a \in \mathbb{Z}$.

- Ⓐ If a and n are relatively prime, then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$.
- Ⓑ If a and n are **not** relatively prime, then for all $b \in \mathbb{Z}$, we have that $ab \not\equiv 1 \pmod{n}$.

Proof. We first prove (b). So, assume that a and n are **not** relatively prime. Fix an integer $m \geq 2$ s.t. $m \mid n$ and $m \mid a$. Then there exists some $k \in \mathbb{Z}$ s.t. $a = mk$.

But now for any $b \in \mathbb{Z}$, we have that $m \nmid (mkb - 1)$, that is, $m \nmid (ab - 1)$.

Since $m \mid n$, it follows that $n \nmid (ab - 1)$, and consequently, $ab \not\equiv 1 \pmod{n}$. This proves (b).

Theorem 0.2.9

Let $n \in \mathbb{N}$ ($n \geq 2$) and $a \in \mathbb{Z}$.

- Ⓐ If a and n are relatively prime, then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$.
- Ⓑ If a and n are **not** relatively prime, then for all $b \in \mathbb{Z}$, we have that $ab \not\equiv 1 \pmod{n}$.

Proof (continued). It remains to prove (a). So, assume that a and n are relatively prime.

WTS no two of $0, a, 2a, \dots, (n-1)a$ are congruent modulo n .

Suppose otherwise, and fix distinct $i, j \in \{0, \dots, n-1\}$ s.t. $ia \equiv ja \pmod{n}$.

Then $(i-j)a \equiv 0 \pmod{n}$, that is, $n|(i-j)a$. Since n and a are relatively prime, it follows that $n|(i-j)$. But this is impossible because $i, j \in \{0, \dots, n-1\}$ and $i \neq j$, and so $0 < |i-j| < n$. Thus, no two of $0, a, 2a, \dots, (n-1)a$ are congruent modulo n .

Theorem 0.2.9

Let $n \in \mathbb{N}$ ($n \geq 2$) and $a \in \mathbb{Z}$.

- Ⓐ If a and n are relatively prime, then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$.
- Ⓑ If a and n are **not** relatively prime, then for all $b \in \mathbb{Z}$, we have that $ab \not\equiv 1 \pmod{n}$.

Proof (continued). **Reminder:** No two of $0, a, 2a, \dots, (n-1)a$ are congruent modulo n .

We know that every integer is congruent modulo n to one of the following n integers: $0, 1, 2, \dots, n-1$.

Since no two of $0, a, 2a, \dots, (n-1)a$ are congruent modulo n , it follows that (exactly) one of $0, a, 2a, \dots, (n-1)a$ is congruent to 1 modulo n . In other words, for exactly one value of $b \in \{0, 1, 2, \dots, n-1\}$, we have that $ba \equiv 1 \pmod{n}$. For this b , we have that $ab \equiv 1 \pmod{n}$. This proves (a). $\square$

Theorem 0.2.9

Let $n \in \mathbb{N}$ ($n \geq 2$) and $a \in \mathbb{Z}$.

- Ⓐ If a and n are relatively prime, then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$.
- Ⓑ If a and n are **not** relatively prime, then for all $b \in \mathbb{Z}$, we have that $ab \not\equiv 1 \pmod{n}$.

Corollary 0.2.10

Let $p \in \mathbb{N}$ be a prime number. Then for all $a \in \mathbb{Z}$ s.t. a is **not** a multiple of p , there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$.

- **Remark:** Note that Corollary 0.2.10 is an **existence** result: it establishes that for a prime number p and an integer a s.t. $p \nmid a$, there **exists** an integer b s.t. $ab \equiv 1 \pmod{p}$.
 - Fermat's Little Theorem (next slide) strengthens this result by giving a formula for a suitable b .

Corollary 0.2.10

Let $p \in \mathbb{N}$ be a prime number. Then for all $a \in \mathbb{Z}$ s.t. a is **not** a multiple of p , there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$.

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number, and $a \in \mathbb{Z}$ is **not** a multiple of p , then $a^{p-1} \equiv 1 \pmod{p}$.

- Before proving Fermat's Little Theorem, we need a definition.
- For non-negative integers n , we define $n!$ (read “ n factorial”) recursively, as follows:
 - $0! := 1$;
 - $(n+1)! := n! \cdot (n+1)$ for all non-negative integers n .

So, for a positive integer n , we have $n! = 1 \cdot 2 \cdot \dots \cdot n$.

- Now let's prove Fermat's Little Theorem!

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number, and $a \in \mathbb{Z}$ is **not** a multiple of p , then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Fix a prime number $p \in \mathbb{N}$. Let $a \in \mathbb{Z}$, and assume that a is not a multiple of p . As in the proof of Theorem 0.2.9, no two of $0, a, 2a, \dots, (p-1)a$ are congruent modulo p .

- This is exactly the same as in the proof of Theorem 0.2.9, but for the sake of completeness, here is the full proof.
- Suppose that some two of $0, a, \dots, (p-1)a$ are congruent modulo p .
- Fix distinct $i, j \in \{0, 1, \dots, p-1\}$ s.t. $ia \equiv ja \pmod{p}$.
- Then $(i-j)a \equiv 0 \pmod{p}$, that is, $p \mid (i-j)a$. Since p is prime and does not divide a , we see that $p \mid (i-j)$.
- But this is impossible because $i, j \in \{0, \dots, p-1\}$ and $i \neq j$, and so $0 < |i-j| < p$.
- Thus, no two of $0, a, 2a, \dots, (p-1)a$ are congruent modulo p .

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number, and $a \in \mathbb{Z}$ is **not** a multiple of p , then $a^{p-1} \equiv 1 \pmod{p}$.

Proof (continued). **Reminder:** No two of $0, a, 2a, \dots, (p-1)a$ are congruent modulo p .

Since every integer is congruent to exactly one of $0, 1, \dots, p-1$ modulo p , it follows that there exists some rearrangement (i.e. permutation) $r_1, \dots, r_{p-1}$ of the sequence $1, \dots, p-1$ s.t.

- $a \equiv r_1 \pmod{p}$;
- $2a \equiv r_2 \pmod{p}$;
- $\vdots$
- $(p-1)a \equiv r_{p-1} \pmod{p}$.

It now follows that

$$\underbrace{a \cdot 2a \cdot \dots \cdot (p-1)a}_{=(p-1)!a^{p-1}} \equiv \underbrace{r_1 r_2 \dots r_{p-1}}_{=(p-1)!} \pmod{p}$$

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number, and $a \in \mathbb{Z}$ is **not** a multiple of p , then $a^{p-1} \equiv 1 \pmod{p}$.

Proof (continued). **Reminder:**

$$\underbrace{a \cdot 2a \cdots (p-1)a}_{=(p-1)!a^{p-1}} \equiv \underbrace{r_1 r_2 \cdots r_{p-1}}_{=(p-1)!} \pmod{p}$$

So, $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$. But now

$$(a^{p-1} - 1)(p-1)! \equiv 0 \pmod{p},$$

that is, $p \mid ((a^{p-1} - 1)(p-1)!)$.

Since p is prime, we see that p and $(p-1)!$ are relatively prime. It follows that $p \mid (a^{p-1} - 1)$, and consequently, $a^{p-1} \equiv 1 \pmod{p}$, which is what we needed to show. $\square$

3 Arithmetic in $\mathbb{Z}_n$

Definition

Given $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, we define the *congruence class* of a modulo n to be the set

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

- Note that:
 - $[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$;
 - $a \in [a]_n$, since $a \equiv a \pmod{n}$.

- **Reminder:** $[a]_n := \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$.

Example 0.2.11

Recall that for $n = 2$, integers k are of two types:

- those that satisfy $k \equiv 0 \pmod{2}$;
- those that satisfy $k \equiv 1 \pmod{2}$.

The two types are represented below (via color coding).

$\dots, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots$

Thus, we have the following:

- $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$;
- $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$.

But note that we also have the following:

- $\dots = [-4]_2 = [-2]_2 = [0]_2 = [2]_2 = [4]_2 = \dots$;
- $\dots = [-3]_2 = [-1]_2 = [1]_2 = [3]_2 = [5]_2 = \dots$

Example 0.2.12

Recall that for $n = 3$, integers k are of three types:

- those that satisfy $k \equiv 0 \pmod{3}$;
- those that satisfy $k \equiv 1 \pmod{3}$;
- and those that satisfy $k \equiv 2 \pmod{3}$.

The three types are represented below (via color coding).

$\dots, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots$

Thus, we have the following:

- $[0]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\}$;
- $[1]_3 = \{\dots, -5, -2, 1, 4, 7, \dots\}$;
- $[2]_3 = \{\dots, -4, -1, 2, 5, 8, \dots\}$.

But note that we also have the following:

- $\dots = [-6]_3 = [-3]_3 = [0]_3 = [3]_3 = [6]_3 = \dots$;
- $\dots = [-5]_3 = [-2]_3 = [1]_3 = [4]_3 = [7]_3 = \dots$;
- $\dots = [-4]_3 = [-1]_3 = [2]_3 = [5]_3 = [8]_3 = \dots$

Proposition 0.2.2

Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Then the following hold:

- Ⓐ $a \equiv a \pmod{n}$;
- Ⓑ if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;
- Ⓒ if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

- **Reminder:** $[a]_n := \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$.

Proposition 0.2.13

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then:

- Ⓐ if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;
- Ⓑ if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

- **Remark:** Proposition 0.2.13 in fact follows from the fact that, by Proposition 0.2.2, congruence modulo n is an equivalence relation on $\mathbb{Z}$.
 - However, a detailed proof that does not rely on the theory of equivalence classes is given on the next slide.

Proposition 0.2.2

Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Then the following hold:

- Ⓐ $a \equiv a \pmod{n}$;
- Ⓑ if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;
- Ⓒ if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proposition 0.2.13

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then:

- Ⓐ if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;
- Ⓑ if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

Proof. We first prove (a). Suppose that $a \equiv b \pmod{n}$. It suffices to show that $[a]_n \subseteq [b]_n$ (the proof of the reverse inclusion is analogous). Fix $x \in [a]_n$. Then $x \equiv a \pmod{n}$. Since $a \equiv b \pmod{n}$, Proposition 0.2.2 guarantees that $x \equiv b \pmod{n}$. Consequently, $x \in [b]_n$, and we deduce that $[a]_n \subseteq [b]_n$. This proves (a).

Proposition 0.2.2

Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Then the following hold:

- Ⓐ $a \equiv a \pmod{n}$;
- Ⓑ if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;
- Ⓒ if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proposition 0.2.13

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then:

- Ⓐ if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;
- Ⓑ if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

Proof (continued). It remains to prove (b). We prove the contrapositive: if $[a]_n \cap [b]_n \neq \emptyset$, then $a \equiv b \pmod{n}$. So, assume that $[a]_n \cap [b]_n \neq \emptyset$, and fix some $x \in [a]_n \cap [b]_n$. Since $x \in [a]_n$, we have that $x \equiv a \pmod{n}$, and since $x \in [b]_n$, we have that $x \equiv b \pmod{n}$. But now by Proposition 0.2.2, we have that $a \equiv b \pmod{n}$. This proves (b). $\square$

- **Reminder:** $[a]_n := \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$.

Proposition 0.2.13

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then:

- Ⓐ if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;
- Ⓑ if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

- **Remark:** Note that Proposition 0.2.13(a) can in fact be strengthened as follows: for all $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we have that:

$$[a]_n = [b]_n \iff a \equiv b \pmod{n}$$

Indeed, “ $\Leftarrow$ ” follows immediately from

Proposition 0.2.13(a). For the other direction, note that if $[a]_n = [b]_n$, then we have that $a \in [a]_n = [b]_n$, and so by the definition of $[b]_n$, we have that $a \equiv b \pmod{n}$.

Proposition 0.2.13

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then:

- Ⓐ if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;
- Ⓑ if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

- Recall that for $n \in \mathbb{N}$, every integer is congruent to exactly one of $0, \dots, n-1$ modulo n ; by Proposition 0.2.13, it follows that for all $x \in \mathbb{Z}$, the set $[x]_n$ is equal to exactly one of the following: $[0]_n, \dots, [n-1]_n$.
- So, we may define

$$\mathbb{Z}_n := \{[a]_n \mid a \in \mathbb{Z}\} = \{[0]_n, \dots, [n-1]_n\}.$$

Proposition 0.2.13

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Then:

- Ⓐ if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;
- Ⓑ if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

- **Reminder:** For $n \in \mathbb{N}$: $\mathbb{Z}_n = \{[0]_n, \dots, [n-1]_n\}$.
- By Proposition 0.2.13, no two of $0, \dots, n-1$ are congruent to each other modulo n , and consequently, $[0]_n, \dots, [n-1]_n$ are pairwise disjoint.
- We now deduce that the (non-empty) sets $[0]_n, \dots, [n-1]_n$ form a “partition” of $\mathbb{Z}$, that is:
 - $\mathbb{Z} = [0]_n \cup \dots \cup [n-1]_n$, and
 - the sets $[0]_n, \dots, [n-1]_n$ are pairwise disjoint.
- If you are familiar with “equivalence relations,” then note that congruence modulo n is an equivalence relation on $\mathbb{Z}$ (by Proposition 0.2.2), and the sets $[0]_n, \dots, [n-1]_n$ are the associated equivalence classes.

- **Reminder:** $[a]_n := \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$.
- **Reminder:** $\mathbb{Z}_n := \{[a]_n \mid a \in \mathbb{Z}\} = \{[0]_n, \dots, [n-1]_n\}$.
- **Notation:** When working in $\mathbb{Z}_n$, we often write simply $0, \dots, n-1$ instead of $[0]_n, \dots, [n-1]_n$, respectively. We may do this **only** if we have previously made it clear that our numbers (which are technically sets of integers) are in $\mathbb{Z}_n$.

Example 0.2.14

For $n = 2$, $[0]_2 = \{2t \mid t \in \mathbb{Z}\}$ and $[1]_2 = \{1 + 2t \mid t \in \mathbb{Z}\}$,^a and we have that $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$. Typically, we write simply $\mathbb{Z}_2 = \{0, 1\}$, but technically, 0 stands for the set $[0]_2$, and 1 stands for $[1]_2$.

^aIn other words, $[0]_2$ is the set of all even numbers, and $[1]_2$ is the set of all odd numbers.

Proposition 0.2.3

Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$, and assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

- Ⓐ $a + c \equiv b + d \pmod{n}$;
- Ⓑ $a - c \equiv b - d \pmod{n}$;
- Ⓒ $ac \equiv bd \pmod{n}$.

- By Proposition 0.2.3, for all $n \in \mathbb{N}$ and $a, a', b, b' \in \mathbb{Z}$, if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then
 - $a + b \equiv a' + b' \pmod{n}$,
 - $a - b \equiv a' - b' \pmod{n}$,
 - $ab \equiv a'b' \pmod{n}$;
- equivalently, if $[a]_n = [a']_n$ and $[b]_n = [b']_n$, then
 - $[a + b]_n = [a' + b']_n$,
 - $[a - b]_n = [a' - b']_n$,
 - $[ab]_n = [a'b']_n$.

- **Reminder:** For all $n \in \mathbb{N}$ and $a, a', b, b' \in \mathbb{Z}$, if $[a]_n = [a']_n$ and $[b]_n = [b']_n$, then
 - $[a + b]_n = [a' + b']_n$,
 - $[a - b]_n = [a' - b']_n$,
 - $[ab]_n = [a'b']_n$.
- Thus, we may define addition, subtraction, and multiplication in $\mathbb{Z}_n$ as follows:

Definition

For $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we define:

- $[a]_n + [b]_n = [a + b]_n$;
- $[a]_n - [b]_n = [a - b]_n$;
- $[a]_n [b]_n = [ab]_n$.

Proposition 0.2.15

Let $n \in \mathbb{N}$. Then all the following hold:

- Ⓐ addition and multiplication are commutative in $\mathbb{Z}_n$, that is, for all $a, b \in \mathbb{Z}_n$, we have that $a + b = b + a$ and $ab = ba$;
- Ⓑ addition and multiplication are associative in $\mathbb{Z}_n$, that is, for all $a, b, c \in \mathbb{Z}_n$, we have that $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$;
- Ⓒ multiplication is distributive over addition in $\mathbb{Z}_n$, that is, for all $a, b, c \in \mathbb{Z}_n$, we have that $a(b + c) = ab + ac$.

- This essentially follows from the definition of $\mathbb{Z}_n$, from the fact that addition and multiplication are commutative and associative in $\mathbb{Z}$, and from the fact that multiplication is distributive over addition in $\mathbb{Z}$.
 - Commutativity of addition in $\mathbb{Z}_n$: Lecture Notes.
 - The rest: easy exercise.
- Next: Addition and multiplication tables for $\mathbb{Z}_n$, for a few small values of n .

Example 0.2.16

Below are the addition and multiplication tables for $\mathbb{Z}_2$.

+	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\cdot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

If we omit square brackets and subscripts (as we usually do), we obtain the addition and multiplication tables for $\mathbb{Z}_2$ shown below.

+	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Example 0.2.17

Below are the addition and multiplication tables for $\mathbb{Z}_3$.^a

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

^aRemember, in this context, 0 stands for $[0]_3$, 1 stands for $[1]_3$, and 2 stands for $[2]_3$.

Example 0.2.18

Below are the addition and multiplication tables for $\mathbb{Z}_4$.^a

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

^aRemember, in this context, 0 stands for $[0]_4$, 1 stands for $[1]_4$, 2 stands for $[2]_4$, and 3 stands for $[3]_4$.

Example 0.2.19

Below are the addition and multiplication tables for $\mathbb{Z}_5$.^a

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	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

^aRemember, in this context, 0 stands for $[0]_5$, 1 stands for $[1]_5$, 2 stands for $[2]_5$, 3 stands for $[3]_5$, and 4 stands for $[4]_5$.

$$\mathbb{Z}_2 :$$

+	0	1
0	0	1
1	1	0

$$\cdot$$

	0	1
0	0	0
1	0	1

$$\mathbb{Z}_3 :$$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$$\cdot$$

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$\mathbb{Z}_4 :$$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$$\cdot$$

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$$\mathbb{Z}_5 :$$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$$\cdot$$

	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

- Remark/Notation:** Note that for all positive integers n , each number a in $\mathbb{Z}_n$ has a unique “additive inverse,” denoted by $-a$, i.e. the number (element of $\mathbb{Z}_n$) that we need to add to a in order to obtain 0 (here, $0 = [0]_n$).
 - When using square brackets and subscripts, we do, of course, get $-[a]_n = [-a]_n = [n - a]_n$ for all positive integers n and all integers a .
 - However, we will usually work in $\mathbb{Z}_n$ **without** such brackets.
 - For small values of n , we get the following:
 - in $\mathbb{Z}_2$: $-0 = 0$, $-1 = 1$;
 - in $\mathbb{Z}_3$: $-0 = 0$, $-1 = 2$, $-2 = 1$;
 - in $\mathbb{Z}_4$: $-0 = 0$, $-1 = 3$, $-2 = 2$, $-3 = 1$;
 - in $\mathbb{Z}_5$: $-0 = 0$, $-1 = 4$, $-2 = 3$, $-3 = 2$, $-4 = 1$.
- Remark:** Note that for $n = 2, 3, 5$, every non-zero member of $\mathbb{Z}_n$ has a “multiplicative inverse,” i.e. a number that we can multiply it by to get 1. However, for $n = 4$, this is not the case.
 - This is not an accident, and in fact, it follows from Theorem 0.2.9 and Corollary 0.2.10, which can be “translated” into the language of $\mathbb{Z}_n$ as follows (the next couple of slides).

Theorem 0.2.9

Let $n \in \mathbb{N}$ ($n \geq 2$) and $a \in \mathbb{Z}$.

- Ⓐ If a and n are relatively prime, then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$.
- Ⓑ If a and n are **not** relatively prime, then for all $b \in \mathbb{Z}$, we have that $ab \not\equiv 1 \pmod{n}$.

Corollary 0.2.10

Let $p \in \mathbb{N}$ be a prime number. Then for all $a \in \mathbb{Z}$ s.t. a is **not** a multiple of p , there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$.

- **Reminder:** For all $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we have that

$$[a]_n = [b]_n \iff a \equiv b \pmod{n}$$

- Theorem 0.2.9 and Corollary 0.2.10 can be translated into the language of $\mathbb{Z}_n$ as follows:

Theorem 0.2.20

Let $n \in \mathbb{N}$ ($n \geq 2$) and $a \in \mathbb{Z}$.

- Ⓐ If a and n are relatively prime, then there exists some $b \in \mathbb{Z}$ s.t. $[a]_n[b]_n = [1]_n$.
- Ⓑ If a and n are **not** relatively prime, then for all $b \in \mathbb{Z}$, we have that $[a]_n[b]_n \neq [1]_n$.

Corollary 0.2.21

Let $p \in \mathbb{N}$ be a prime number. Then for all $a \in \mathbb{Z}$ s.t. a is **not** a multiple of p , there exists some $b \in \mathbb{Z}$ s.t. $[a]_p[b]_p = [1]_p$.

Corollary 0.2.21

Let $p \in \mathbb{N}$ be a prime number. Then for all $a \in \mathbb{Z}$ s.t. a is **not** a multiple of p , there exists some $b \in \mathbb{Z}$ s.t. $[a]_p[b]_p = [1]_p$.

- In fact, Corollary 0.2.21 could further be rephrased as follows:

Corollary 0.2.22

Let p be a prime number. Then for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p$ s.t. $ab = 1$.

- **Notation:** In the statement of Corollary 0.2.22, 0 and 1 stand for $[0]_p$, and $[1]_p$, respectively.

Proof. This follows immediately from Corollary 0.2.21, since for all $a \in \mathbb{Z}$, we have that $[a]_p = [0]_p$ iff $p \mid a$. $\square$

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number, and $a \in \mathbb{Z}$ is **not** a multiple of p , then $a^{p-1} \equiv 1 \pmod{p}$.

- Our final goal for this subsection is to restate Fermat's Little Theorem in terms of numbers in $\mathbb{Z}_p$, where p is a prime number. First, we need a definition.

Definition

For a positive integer n and for $a \in \mathbb{Z}_n$, we define powers of a recursively, as follows:

- $a^0 = 1$ (where $1 := [1]_n$);
- $a^{m+1} = a^m a$ for all non-negative integers m .

So, for a positive integer m , we have the familiar formula

$$a^m = \underbrace{a \cdots a}_m,$$

where it is understood that the multiplication on the right-hand-side is in $\mathbb{Z}_n$.

- **Reminder:** For all $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we have that

$$[a]_n = [b]_n \iff a \equiv b \pmod{n}$$

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number, and $a \in \mathbb{Z}$ is **not** a multiple of p , then $a^{p-1} \equiv 1 \pmod{p}$.

- We can now restate Fermat's Little Theorem in two ways, as follows. (Note that in the second restatement of Fermat's Little Theorem, 0 and 1 stand for $[0]_p$ and $[1]_p$, respectively.)

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number, and $a \in \mathbb{Z}$ is **not** a multiple of p , then $([a]_p)^{p-1} = [1]_p$.

Fermat's Little Theorem

If $p \in \mathbb{N}$ is a prime number and $a \in \mathbb{Z}_p \setminus \{0\}$, then $a^{p-1} = 1$.

- Suppose that p is a **prime** number and that $a \in \mathbb{Z}_p \setminus \{0\}$.
 - By Fermat's Little Theorem, a^{p-2} is a “multiplicative inverse” of a , i.e. if we multiply a by a^{p-2} (on either side), we obtain 1.
 - That is: $a \cdot a^{p-2} = a^{p-2} \cdot a = 1$.
 - Moreover, it is easy to see that a^{p-2} is the **only** multiplicative inverse of a in $\mathbb{Z}_p$.
 - Indeed, if $b \in \mathbb{Z}_p$ satisfies $ab = 1$ (which is equivalent to $ba = 1$, by Proposition 0.2.15), then by multiplying both sides by a^{p-2} , we obtain

$$\underbrace{a^{p-2} \cdot a}_{=a^{p-1}=1} b = a^{p-2} \cdot 1,$$

and consequently, $b = a^{p-2}$.

- So, we can say that a^{p-2} is **the** multiplicative inverse of a (denoted by a^{-1}), and we write

$$\underbrace{a^{-1}}_{\text{multiplicative inverse of } a} = a^{p-2}$$

- However, that for small values of the prime number p , it is easier to read off the multiplicative inverses of non-zero numbers in $\mathbb{Z}_p$ from the multiplication table for $\mathbb{Z}_p$ than it is to compute the $(p-2)$ -th powers of those numbers.

$$\mathbb{Z}_2 :$$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$$\mathbb{Z}_3 :$$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$\mathbb{Z}_5 :$$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	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

- in $\mathbb{Z}_2$: $1^{-1} = 1$;
- in $\mathbb{Z}_3$: $1^{-1} = 1$, $2^{-1} = 2$;
- in $\mathbb{Z}_5$: $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$.