Linear Algebra 1

Lecture #0

Mathematical induction. Modular arithmetic. Arithmetic in $\mathbb{Z}_n$

Irena Penev

October 2, 2024

- This lecture covers sections 0.1 and 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:

This lecture has three parts:

1. Mathematical induction;

This lecture has three parts:

1. Mathematical induction;
2. Modular arithmetic;

This lecture has three parts:

1. Mathematical induction;
2. Modular arithmetic;
3. Arithmetic in $\mathbb{Z}_n$ and Fermat's Little Theorem

1. Mathematical induction

1. Mathematical induction

- Mathematical induction is a proof technique that can be used to prove that a certain statement holds for all positive integers n.

1. Mathematical induction

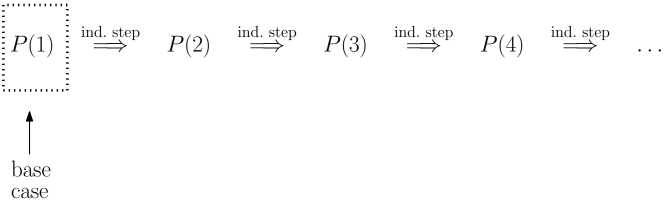
- Mathematical induction is a proof technique that can be used to prove that a certain statement holds for all positive integers n.
- Let $P(n)$ be a statement about the number n.

1. Mathematical induction

- Mathematical induction is a proof technique that can be used to prove that a certain statement holds for all positive integers n.
- Let $P(n)$ be a statement about the number n. In order to prove that $P(n)$ holds for every positive integer n, it suffices to prove the following two statements:

1 Mathematical induction

- Mathematical induction is a proof technique that can be used to prove that a certain statement holds for all positive integers n.
- Let $P(n)$ be a statement about the number n. In order to prove that $P(n)$ holds for every positive integer n, it suffices to prove the following two statements:
  - **Base case:** $P(1)$ is true;
  - **Induction step:** for every positive integer n, if $\underbrace{P(n) \text{ is true}}_{\text{"induction hypothesis"}}$, then $P(n+1)$ is true.



Example 0.1.1

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all positive integers n.

Solution.

Example 0.1.1

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all positive integers n.

Solution. Let $P(n)$ be the statement that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Example 0.1.1

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all positive integers n.

Solution. Let $P(n)$ be the statement that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. Thus:

- $P(1)$ is the statement that $1 = \frac{1 \cdot (1+1)}{2}$;
- $P(2)$ is the statement that $1 + 2 = \frac{2 \cdot (2+1)}{2}$;
- $P(3)$ is the statement that $1 + 2 + 3 = \frac{3 \cdot (3+1)}{2}$;
- etc.

We need to prove that the statement $P(n)$ is true for all positive integers n.

Example 0.1.1

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all positive integers n.

Solution (continued). **Reminder:** $P(n)$ is the statement that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Example 0.1.1

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all positive integers n.

Solution (continued). **Reminder:** $P(n)$ is the statement that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Base case: $n = 1$. Obviously, $1 = \frac{1 \cdot (1+1)}{2}$. Thus, $P(1)$ is true.

Example 0.1.1

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all positive integers n.

Solution (continued). **Reminder:** $P(n)$ is the statement that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Base case: $n = 1$. Obviously, $1 = \frac{1 \cdot (1+1)}{2}$. Thus, $P(1)$ is true.

Induction step: Fix a positive integer n, and assume inductively that $P(n)$ is true. We must show that $P(n+1)$ is true.

Example 0.1.1

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all positive integers n.

Solution (continued). **Reminder:** $P(n)$ is the statement that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Base case: $n = 1$. Obviously, $1 = \frac{1 \cdot (1+1)}{2}$. Thus, $P(1)$ is true.

Induction step: Fix a positive integer n, and assume inductively that $P(n)$ is true. We must show that $P(n+1)$ is true.
The induction hypothesis states that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.
Using this, we must prove that

$1 + 2 + \cdots + n + (n+1) = \frac{(n+1)\big((n+1)+1\big)}{2}$. We compute (next slide):

Example 0.1.1

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all positive integers n.

Solution (continued). **Reminder:** $P(n)$ is the statement that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

$$
\begin{aligned}
1 + 2 + \cdots + n + (n+1) &= (1 + 2 + \cdots + n) + (n+1) \\
&\overset{\text{ind. hyp.}}{=} \frac{n(n+1)}{2} + (n+1) \\
&= (n+1)\left(\frac{n}{2} + 1\right) \\
&= \frac{(n+1)\big((n+1)+1\big)}{2}.
\end{aligned}
$$

Thus, $P(n+1)$ is true. This completes the induction. $\square$

- Sometimes, the base case may be different from $n = 1$.

- Sometimes, the base case may be different from $n = 1$.
- This may happen if we need to prove that a statement $P(n)$ is true for all $n \geq k$, where k is an integer other than 1.
    - Typically, we will have $k = 0$ or $k > 1$. However, in principle, k may even be a negative integer.

- Sometimes, the base case may be different from $n = 1$.
- This may happen if we need to prove that a statement $P(n)$ is true for all $n \geq k$, where k is an integer other than 1.
  - Typically, we will have $k = 0$ or $k > 1$. However, in principle, k may even be a negative integer.
- In this case, the base case will be $n = k$, i.e. we will need to prove the following two statements:
  - **Base case:** $P(k)$ is true;
  - **Induction step:** for every integer $n \geq k$,
    if $\underbrace{P(n) \text{ is true}}_{\text{“induction hypothesis”}}$, then $P(n+1)$ is true.

- Sometimes, the base case may be different from $n = 1$.
- This may happen if we need to prove that a statement $P(n)$ is true for all $n \geq k$, where k is an integer other than 1.
  - Typically, we will have $k = 0$ or $k > 1$. However, in principle, k may even be a negative integer.
- In this case, the base case will be $n = k$, i.e. we will need to prove the following two statements:
  - **Base case:** $P(k)$ is true;
  - **Induction step:** for every integer $n \geq k$, if $\underbrace{P(n) \text{ is true}}_{\text{"induction hypothesis"}}$, then $P(n+1)$ is true.

$$\boxed{P(k)} \overset{\text{ind. step}}{\Longrightarrow} P(k+1) \overset{\text{ind. step}}{\Longrightarrow} P(k+2) \overset{\text{ind. step}}{\Longrightarrow} P(k+3) \overset{\text{ind. step}}{\Longrightarrow} \ldots$$

↑ base case

Example 0.1.2

Prove that $3n < 2^n$ for all integers $n \geq 4$.

Solution.

Example 0.1.2

Prove that $3n < 2^n$ for all integers $n \geq 4$.

Solution. Since we are proving the statement for integers $n \geq 4$, our base case is $n = 4$.

Example 0.1.2

Prove that $3n < 2^n$ for all integers $n \geq 4$.

Solution. Since we are proving the statement for integers $n \geq 4$, our base case is $n = 4$.

Base case: $n = 4$. Clearly, $3 \cdot 4 = 12 < 16 = 2^4$.

Example 0.1.2

Prove that $3n < 2^n$ for all integers $n \geq 4$.

Solution. Since we are proving the statement for integers $n \geq 4$, our base case is $n = 4$.

Base case: $n = 4$. Clearly, $3 \cdot 4 = 12 < 16 = 2^4$.

Induction step: Fix an integer $n \geq 4$, and assume inductively that $3n < 2^n$. We must show that $3(n+1) < 2^{n+1}$.

Example 0.1.2

Prove that $3n < 2^n$ for all integers $n \geq 4$.

Solution. Since we are proving the statement for integers $n \geq 4$, our base case is $n = 4$.

Base case: $n = 4$. Clearly, $3 \cdot 4 = 12 < 16 = 2^4$.

Induction step: Fix an integer $n \geq 4$, and assume inductively that $3n < 2^n$. We must show that $3(n+1) < 2^{n+1}$. We observe the following:

$$\begin{aligned} 3(n+1) &= 3n+3 \\ &< 2^n + 3 && \text{by the induction hypothesis} \\ &< 2^n + 2^2 \\ &< 2^n + 2^n && \text{because } n > 2 \\ &= 2^{n+1} \end{aligned}$$

Thus, the statement is true for $n+1$. This completes the induction. □

- Sometimes, induction can have more than one base case.

- Sometimes, induction can have more than one base case.
- Suppose that k is an integer, and that we wish to prove inductively that $P(n)$ holds for all integers $n \geq k$.

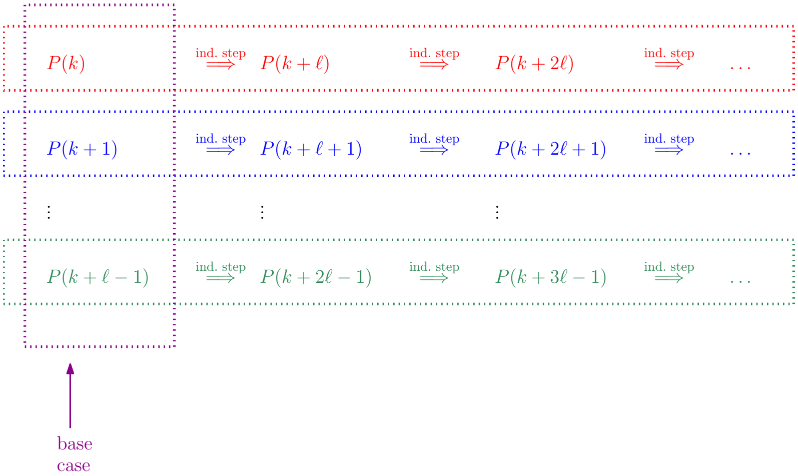
- Sometimes, induction can have more than one base case.
- Suppose that k is an integer, and that we wish to prove inductively that $P(n)$ holds for all integers $n \geq k$.
- Ordinarily, we would expect $n = k$ to be the base case.

- Sometimes, induction can have more than one base case.
- Suppose that k is an integer, and that we wish to prove inductively that $P(n)$ holds for all integers $n \geq k$.
- Ordinarily, we would expect $n = k$ to be the base case.
- However, suppose that we do not know how to prove the implication "$P(n) \Longrightarrow P(n+1)$," but we do know how to prove that "$P(n) \Longrightarrow P(n+\ell)$," where ℓ is some positive integer (other than 1).

- Sometimes, induction can have more than one base case.
- Suppose that k is an integer, and that we wish to prove inductively that $P(n)$ holds for all integers $n \geq k$.
- Ordinarily, we would expect $n = k$ to be the base case.
- However, suppose that we do not know how to prove the implication "$P(n) \implies P(n+1)$," but we do know how to prove that "$P(n) \implies P(n+\ell)$," where ℓ is some positive integer (other than 1).
- In this case, we will have a slightly modified induction step ("$P(n) \implies P(n+\ell)$" instead of "$P(n) \implies P(n+1)$"), and we will have ℓ base cases, namely, $P(k), P(k+1), \ldots, P(k+\ell-1)$.

- Sometimes, induction can have more than one base case.
- Suppose that k is an integer, and that we wish to prove inductively that $P(n)$ holds for all integers $n \geq k$.
- Ordinarily, we would expect $n = k$ to be the base case.
- However, suppose that we do not know how to prove the implication "$P(n) \implies P(n+1)$," but we do know how to prove that "$P(n) \implies P(n+\ell)$," where ℓ is some positive integer (other than 1).
- In this case, we will have a slightly modified induction step ("$P(n) \implies P(n+\ell)$" instead of "$P(n) \implies P(n+1)$"), and we will have ℓ base cases, namely, $P(k), P(k+1), \dots, P(k+\ell-1)$.
- More precisely, we will need to prove the following (next slide):

- **Base case:** $P(k), P(k+1), \ldots, P(k+\ell-1)$ are true;
- **Induction step:** for every integer $n \geq k$, if $\underbrace{P(n) \text{ is true}}_{\text{“induction hypothesis”}}$, then $P(n+\ell)$ is true.



Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution.

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution. We need to show that any integer $n \geq 8$ (our postage in Kč) can be expressed in the form

$$n = 3a + 5b,$$

where a and b are non-negative integers (the number of 3 Kč and 5 Kč stamps, respectively, that we can use to pay our n Kč postage).

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution. We need to show that any integer $n \geq 8$ (our postage in Kč) can be expressed in the form

$$n = 3a + 5b,$$

where a and b are non-negative integers (the number of 3 Kč and 5 Kč stamps, respectively, that we can use to pay our n Kč postage). We will prove this by induction on n.

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution. We need to show that any integer $n \geq 8$ (our postage in Kč) can be expressed in the form

$$n = 3a + 5b,$$

where a and b are non-negative integers (the number of 3 Kč and 5 Kč stamps, respectively, that we can use to pay our n Kč postage). We will prove this by induction on n.

Obviously, if we can pay n Kč using our stamps, then we can also pay $(n + 3)$ Kč: we simply use one 3 Kč stamp more.

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution. We need to show that any integer $n \geq 8$ (our postage in Kč) can be expressed in the form

$$n = 3a + 5b,$$

where a and b are non-negative integers (the number of 3 Kč and 5 Kč stamps, respectively, that we can use to pay our n Kč postage). We will prove this by induction on n.

Obviously, if we can pay n Kč using our stamps, then we can also pay $(n + 3)$ Kč: we simply use one 3 Kč stamp more. In other words, if the statement is true for n, then it is also true for $n + 3$.

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution. We need to show that any integer $n \geq 8$ (our postage in Kč) can be expressed in the form

$$n = 3a + 5b,$$

where a and b are non-negative integers (the number of 3 Kč and 5 Kč stamps, respectively, that we can use to pay our n Kč postage). We will prove this by induction on n.

Obviously, if we can pay n Kč using our stamps, then we can also pay $(n+3)$ Kč: we simply use one 3 Kč stamp more. In other words, if the statement is true for n, then it is also true for $n+3$. This means that we will need three base cases: $n = 8$, $n = 9$, and $n = 10$.

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution. We need to show that any integer $n \geq 8$ (our postage in Kč) can be expressed in the form

$$n = 3a + 5b,$$

where a and b are non-negative integers (the number of 3 Kč and 5 Kč stamps, respectively, that we can use to pay our n Kč postage). We will prove this by induction on n.

Obviously, if we can pay n Kč using our stamps, then we can also pay $(n + 3)$ Kč: we simply use one 3 Kč stamp more. In other words, if the statement is true for n, then it is also true for $n + 3$. This means that we will need three base cases: $n = 8$, $n = 9$, and $n = 10$. Let us give the details.

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution (continued).

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution (continued). **Base case:** We must show that for each $n \in \{8, 9, 10\}$, there exist non-negative integers a and b s.t. $n = 3a + 5b$.

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution (continued). **Base case:** We must show that for each $n \in \{8, 9, 10\}$, there exist non-negative integers a and b s.t. $n = 3a + 5b$. But this is clearly true:

- $8 = 3 \cdot 1 + 5 \cdot 1$;
- $9 = 3 \cdot 3 + 5 \cdot 0$;
- $10 = 3 \cdot 0 + 5 \cdot 2$.

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution (continued). **Base case:** We must show that for each $n \in \{8, 9, 10\}$, there exist non-negative integers a and b s.t. $n = 3a + 5b$. But this is clearly true:

- $8 = 3 \cdot 1 + 5 \cdot 1$;
- $9 = 3 \cdot 3 + 5 \cdot 0$;
- $10 = 3 \cdot 0 + 5 \cdot 2$.

Induction step: Fix an integer $n \geq 8$, and assume inductively that the statement is true for n. WTS it is true for $n + 3$.

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution (continued). **Base case:** We must show that for each $n \in \{8, 9, 10\}$, there exist non-negative integers a and b s.t. $n = 3a + 5b$. But this is clearly true:

- $8 = 3 \cdot 1 + 5 \cdot 1$;
- $9 = 3 \cdot 3 + 5 \cdot 0$;
- $10 = 3 \cdot 0 + 5 \cdot 2$.

Induction step: Fix an integer $n \geq 8$, and assume inductively that the statement is true for n. WTS it is true for $n + 3$. By the induction hypothesis, there exist non-negative integers a and b s.t. $n = 3a + 5b$.

Example 0.1.3

Suppose you have an unlimited number of 3 Kč stamps and 5 Kč stamps (and no other stamps). Show that you can pay any amount of postage greater or equal to 8 Kč (as long as it is in whole Kč).

Solution (continued). **Base case:** We must show that for each $n \in \{8, 9, 10\}$, there exist non-negative integers a and b s.t. $n = 3a + 5b$. But this is clearly true:

- $8 = 3 \cdot 1 + 5 \cdot 1$;
- $9 = 3 \cdot 3 + 5 \cdot 0$;
- $10 = 3 \cdot 0 + 5 \cdot 2$.

Induction step: Fix an integer $n \geq 8$, and assume inductively that the statement is true for n. WTS it is true for $n + 3$. By the induction hypothesis, there exist non-negative integers a and b s.t. $n = 3a + 5b$. But then $n + 3 = 3(a + 1) + 5b$, and so the statement holds for $n + 3$. This completes the induction. □

- Suppose, again, that k is an integer, and that we wish to prove inductively that $P(n)$ holds for all integers $n \geq k$.

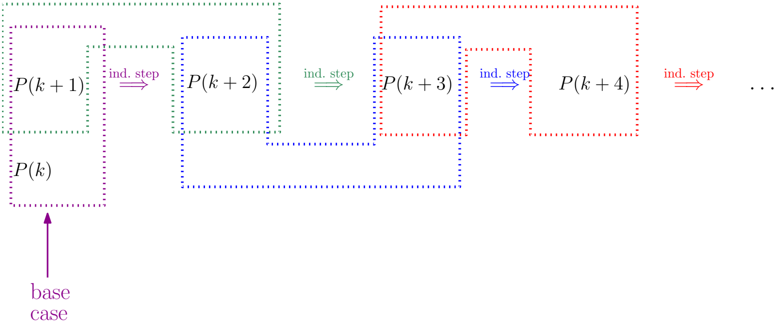
- Suppose, again, that k is an integer, and that we wish to prove inductively that $P(n)$ holds for all integers $n \geq k$.
- However, suppose that we are not able to prove the implication "$P(n) \Longrightarrow P(n+1)$," but that we are able to prove that $P(n), P(n+1), \ldots, P(n+\ell-1)$ together imply $P(n+\ell)$, where ℓ is some positive integer (other than 1).

- Suppose, again, that k is an integer, and that we wish to prove inductively that $P(n)$ holds for all integers $n \geq k$.
- However, suppose that we are not able to prove the implication "$P(n) \implies P(n+1)$," but that we are able to prove that $P(n), P(n+1), \ldots, P(n+\ell-1)$ together imply $P(n+\ell)$, where ℓ is some positive integer (other than 1).
- In this case, we will again have ℓ base cases, namely, $P(k), P(k+1), \ldots, P(k+\ell-1)$.

- Suppose, again, that k is an integer, and that we wish to prove inductively that $P(n)$ holds for all integers $n \geq k$.
- However, suppose that we are not able to prove the implication "$P(n) \Longrightarrow P(n+1)$," but that we are able to prove that $P(n), P(n+1), \ldots, P(n+\ell-1)$ together imply $P(n+\ell)$, where ℓ is some positive integer (other than 1).
- In this case, we will again have ℓ base cases, namely, $P(k), P(k+1), \ldots, P(k+\ell-1)$.
- More precisely, we will need to prove the following:
  - **Base case:** $P(k), P(k+1), \ldots, P(k+\ell-1)$ are true;
  - **Induction step:** for every integer $n \geq k$, if $\underbrace{P(n), P(n+1), \ldots, P(n+\ell-1) \text{ are all true}}_{\text{"induction hypothesis"}}$, then $P(n+\ell)$ is true.

- **Base case:** $P(k), P(k+1), \ldots, P(k+\ell-1)$ are true;
- **Induction step:** for every integer $n \geq k$,
  if $\underbrace{P(n), P(n+1), \ldots, P(n+\ell-1) \text{ are all true}}_{\text{“induction hypothesis”}}$, then $P(n+\ell)$ is true.

Illustration for $\ell = 2$:



Example 0.1.4

The *Fibonacci numbers* are defined as follows:

- $F(1) = F(2) = 1$;
- $F(n+2) = F(n) + F(n+1)$ for all positive intgers n.

Prove that $F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$ for all positive integers n.

Solution.

Example 0.1.4

The *Fibonacci numbers* are defined as follows:

- $F(1) = F(2) = 1$;
- $F(n+2) = F(n) + F(n+1)$ for all positive intgers n.

Prove that $F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$ for all positive integers n.

Solution. The general term is defined in terms of the previous two terms. Thus, instead of one base case, we have two: $n = 1$ and $n = 2$.

Example 0.1.4

The *Fibonacci numbers* are defined as follows:

- $F(1) = F(2) = 1$;
- $F(n+2) = F(n) + F(n+1)$ for all positive intgers n.

Prove that $F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$ for all positive integers n.

Solution. The general term is defined in terms of the previous two terms. Thus, instead of one base case, we have two: $n = 1$ and $n = 2$.

Remark: If the general term were defined in terms of, say, the previous fifteen terms, then we would have fifteen base cases!

Example 0.1.4

The *Fibonacci numbers* are defined as follows:

- $F(1) = F(2) = 1$;
- $F(n+2) = F(n) + F(n+1)$ for all positive intgers n.

Prove that $F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$ for all positive integers n.

Solution (continued). **Base case:** For $n = 1$, we have:

$$\frac{(1+\sqrt{5})^1 - (1-\sqrt{5})^1}{2^1\sqrt{5}} = \frac{2\sqrt{5}}{2\sqrt{5}} = 1 = F(1).$$

For $n = 2$, we have:

$$\frac{(1+\sqrt{5})^2 - (1-\sqrt{5})^2}{2^2\sqrt{5}} = \frac{(1+2\sqrt{5}+5) - (1-2\sqrt{5}+5)}{4\sqrt{5}} = \frac{4\sqrt{5}}{4\sqrt{5}} = 1 = F(2).$$

Thus, the statement is true for $n = 1$ and $n = 2$.

Example 0.1.4

The *Fibonacci numbers* are defined as follows:

- $F(1) = F(2) = 1$;
- $F(n+2) = F(n) + F(n+1)$ for all positive intgers n.

Prove that $F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$ for all positive integers n.

Solution (continued). **Induction step:** Fix a positive integer n, and assume inductively that the statement is true for n and $n+1$. WTS it is true for $n+2$.

Example 0.1.4

The *Fibonacci numbers* are defined as follows:

- $F(1) = F(2) = 1$;
- $F(n+2) = F(n) + F(n+1)$ for all positive intgers n.

Prove that $F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$ for all positive integers n.

Solution (continued). **Induction step:** Fix a positive integer n, and assume inductively that the statement is true for n and $n+1$. WTS it is true for $n+2$.

By the induction hypothesis, we have that

- $F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$;
- $F(n+1) = \frac{(1+\sqrt{5})^{n+1} - (1-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}}$.

Example 0.1.4

The *Fibonacci numbers* are defined as follows:

- $F(1) = F(2) = 1$;
- $F(n+2) = F(n) + F(n+1)$ for all positive intgers n.

Prove that $F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$ for all positive integers n.

Solution (continued). **Induction step:** Fix a positive integer n, and assume inductively that the statement is true for n and $n+1$. WTS it is true for $n+2$.

By the induction hypothesis, we have that

- $F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$;
- $F(n+1) = \frac{(1+\sqrt{5})^{n+1} - (1-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}}$.

WTS $F(n+2) = \frac{(1+\sqrt{5})^{n+2} - (1-\sqrt{5})^{n+2}}{2^{n+2}\sqrt{5}}$.

Example 0.1.4

The *Fibonacci numbers* are defined as follows:

- $F(1) = F(2) = 1$;
- $F(n+2) = F(n) + F(n+1)$ for all positive intgers n.

Prove that $F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$ for all positive integers n.

Solution (continued). **Induction step:** Fix a positive integer n, and assume inductively that the statement is true for n and $n+1$. WTS it is true for $n+2$.

By the induction hypothesis, we have that

- $F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$;
- $F(n+1) = \frac{(1+\sqrt{5})^{n+1} - (1-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}}$.

WTS $F(n+2) = \frac{(1+\sqrt{5})^{n+2} - (1-\sqrt{5})^{n+2}}{2^{n+2}\sqrt{5}}$.
We compute (next slide):

Solution (continued):

$$\begin{aligned}
F(n+2) &\overset{(*)}{=} F(n) + F(n+1) \\
&\overset{(**)}{=} \frac{(1+\sqrt{5})^n-(1-\sqrt{5})^n}{2^n\sqrt{5}} + \frac{(1+\sqrt{5})^{n+1}-(1-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}} \\
&= \frac{4(1+\sqrt{5})^n-4(1-\sqrt{5})^n}{2^{n+2}\sqrt{5}} + \frac{2(1+\sqrt{5})(1+\sqrt{5})^n-2(1-\sqrt{5})(1-\sqrt{5})^n}{2^{n+2}\sqrt{5}} \\
&= \frac{(6+2\sqrt{5})(1+\sqrt{5})^n-(6-2\sqrt{5})(1-\sqrt{5})^n}{2^{n+2}\sqrt{5}} \\
&= \frac{(1+\sqrt{5})^2(1+\sqrt{5})^n-(1-\sqrt{5})^2(1-\sqrt{5})^n}{2^{n+2}\sqrt{5}} \\
&= \frac{(1+\sqrt{5})^{n+2}-(1-\sqrt{5})^{n+2}}{2^{n+2}\sqrt{5}},
\end{aligned}$$

where (*) follows from the definition of Fibonacci numbers, and (**) follows from the induction hypothesis. This completes the induction.

- We now consider a type of induction (sometimes called “strong induction”) that lacks a base case.

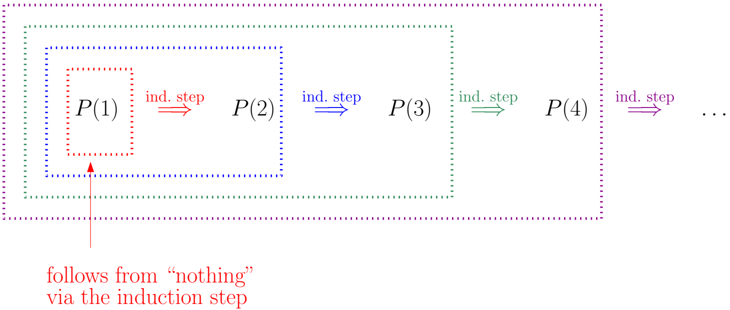
- We now consider a type of induction (sometimes called "strong induction") that lacks a base case.
- Again, let $P(n)$ be a statement about the number n.

- We now consider a type of induction (sometimes called "strong induction") that lacks a base case.
- Again, let $P(n)$ be a statement about the number n.
- In order to prove that $P(n)$ holds for every positive integer n, it suffices to prove the following:
  - **Induction step:** for every positive integer n, if $\underbrace{P(1), \ldots, P(n-1) \text{ are all true}}_{\text{"induction hypothesis"}}$, then $P(n)$ is true.

- We now consider a type of induction (sometimes called "strong induction") that lacks a base case.
- Again, let $P(n)$ be a statement about the number n.
- In order to prove that $P(n)$ holds for every positive integer n, it suffices to prove the following:
  - **Induction step:** for every positive integer n, if $\underbrace{P(1), \ldots, P(n-1) \text{ are all true}}_{\text{"induction hypothesis"}}$, then $P(n)$ is true.
- Here is a slightly different way of writing the same thing:
  - **Induction step:** for every positive integer n, if $\underbrace{P(i) \text{ is true for all positive integers } i < n}_{\text{"induction hypothesis"}}$, then $P(n)$ is true.

- **Induction step:** for every positive integer n, if $\underbrace{P(1), \ldots, P(n-1) \text{ are all true}}_{\text{“induction hypothesis”}}$, then $P(n)$ is true.

- **Induction step:** for every positive integer n, if $\underbrace{P(i) \text{ is true for all positive integers } i < n}_{\text{“induction hypothesis”}}$, then $P(n)$ is true.



- As before, slight variations on the theme are possible.

- As before, slight variations on the theme are possible.
- In particular, for a fixed integer k, we may wish to prove by strong induction that $P(n)$ holds for all integers $n \geq k$.

- As before, slight variations on the theme are possible.
- In particular, for a fixed integer k, we may wish to prove by strong induction that $P(n)$ holds for all integers $n \geq k$.
- In this case, it is enough to prove the following:
    - **Induction step:** for every integer $n \geq k$,
      if $\underbrace{P(k), \ldots, P(n-1) \text{ are all true}}_{\text{"induction hypothesis"}}$, then $P(n)$ is true.

- As before, slight variations on the theme are possible.
- In particular, for a fixed integer k, we may wish to prove by strong induction that $P(n)$ holds for all integers $n \geq k$.
- In this case, it is enough to prove the following:
  - **Induction step:** for every integer $n \geq k$, if $\underbrace{P(k), \ldots, P(n-1) \text{ are all true}}_{\text{"induction hypothesis"}}$, then $P(n)$ is true.
- Another way of writing the same thing is as follows:
  - **Induction step:** for every integer $n \geq k$, if $\underbrace{P(i) \text{ is true for all integers } i \text{ s.t. } k \leq i < n}_{\text{"induction hypothesis"}}$, then $P(n)$ is true.

Example 0.1.5

Prove that every integer $n \geq 2$ can be written as a product of one or more prime numbers.

Solution.

Example 0.1.5

Prove that every integer $n \geq 2$ can be written as a product of one or more prime numbers.

Solution. Fix an integer $n \geq 2$, and assume inductively that each of $2, \ldots, n-1$ can be written as a product of primes. WTS n can be written as a product of primes.

Example 0.1.5

Prove that every integer $n \geq 2$ can be written as a product of one or more prime numbers.

Solution. Fix an integer $n \geq 2$, and assume inductively that each of $2, \ldots, n-1$ can be written as a product of primes. WTS n can be written as a product of primes.

Clearly, n is either prime or composite.

Example 0.1.5

Prove that every integer $n \geq 2$ can be written as a product of one or more prime numbers.

Solution. Fix an integer $n \geq 2$, and assume inductively that each of $2, \ldots, n-1$ can be written as a product of primes. WTS n can be written as a product of primes.

Clearly, n is either prime or composite.

Suppose first that n is prime.

Example 0.1.5

Prove that every integer $n \geq 2$ can be written as a product of one or more prime numbers.

Solution. Fix an integer $n \geq 2$, and assume inductively that each of $2, \ldots, n-1$ can be written as a product of primes. WTS n can be written as a product of primes.

Clearly, n is either prime or composite.

Suppose first that n is prime. Then, obviously, n can be written as a product of primes, namely

$$n = \underbrace{n}_{\text{prime}}.$$

Example 0.1.5

Prove that every integer $n \geq 2$ can be written as a product of one or more prime numbers.

Solution (continued). Suppose now that n is composite.

Example 0.1.5

Prove that every integer $n \geq 2$ can be written as a product of one or more prime numbers.

Solution (continued). Suppose now that n is composite. Then there exist integers n_1, n_2 s.t. $2 \leq n_1, n_2 < n$ and $n = n_1 n_2$.

Example 0.1.5

Prove that every integer $n \geq 2$ can be written as a product of one or more prime numbers.

Solution (continued). Suppose now that n is composite. Then there exist integers n_1, n_2 s.t. $2 \leq n_1, n_2 < n$ and $n = n_1 n_2$.

By the induction hypothesis, n_1 and n_2 can be written as products of primes. Set $n_1 = p_1 \cdot \cdots \cdot p_k$ and $n_2 = q_1 \cdot \cdots \cdot q_\ell$, where $p_1, \ldots, p_k, q_1, \ldots, q_\ell$ are prime numbers.

Example 0.1.5

Prove that every integer $n \geq 2$ can be written as a product of one or more prime numbers.

Solution (continued). Suppose now that n is composite. Then there exist integers n_1, n_2 s.t. $2 \leq n_1, n_2 < n$ and $n = n_1 n_2$.

By the induction hypothesis, n_1 and n_2 can be written as products of primes. Set $n_1 = p_1 \cdot \dots \cdot p_k$ and $n_2 = q_1 \cdot \dots \cdot q_\ell$, where $p_1, \dots, p_k, q_1, \dots, q_\ell$ are prime numbers.

Then $n = n_1 n_2 = p_1 \cdot \dots \cdot p_k \cdot q_1 \cdot \dots \cdot q_\ell$. Thus, n is a product of primes. This completes the induction. $\square$

2. Modular arithmetic

2. 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. $m = kn$.

2. 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. $m = kn$.
- Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we say that a and b are *congruent modulo* n, and we write $a \equiv b \pmod{n}$ or $a \equiv_n b$, provided that $n|(a-b)$, i.e. $a - b = kn$ for some $k \in \mathbb{Z}$.

2. 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. $m = kn$.
- Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we say that a and b are *congruent modulo* n, and we write $a \equiv b \pmod{n}$ or $a \equiv_n b$, provided that $n|(a-b)$, 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 $0, 1, \ldots, n-1$).

2. 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. $m = kn$.
- Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we say that a and b are *congruent modulo* n, and we write $a \equiv b \pmod{n}$ or $a \equiv_n b$, provided that $n|(a-b)$, 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 $0, 1, \ldots, n-1$).
- 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 $a \equiv 0 \pmod{n}$.

2. 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. $m = kn$.
- Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, we say that a and b are *congruent modulo* n, and we write $a \equiv b \pmod{n}$ or $a \equiv_n b$, provided that $n|(a-b)$, 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 $a \equiv 0 \pmod{n}$.

Example 0.2.1

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

- **Reminder:** $a \equiv b \pmod{n}$ means that $n \mid (a - b)$.

- **Reminder:** $a \equiv b \pmod{n}$ means that $n \mid (a - b)$.

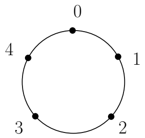
- For fixed $n \in \mathbb{N}$, every integer is congruent modulo n to exactly one of the following n integers: $0, \ldots, n-1$.

- **Reminder:** $a \equiv b \pmod{n}$ means that $n \mid (a - b)$.

- For fixed $n \in \mathbb{N}$, every integer is congruent modulo n to exactly one of the following n integers: $0, \ldots, n-1$.
  - As we shall see, doing arithmetic modulo n essentially boils down to doing arithmetic with only n values (namely $0, \ldots, n-1$), as opposed to infinitely many. This is quite useful for certain applications.

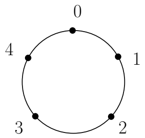
- **Reminder:** $a \equiv b \pmod{n}$ means that $n \mid (a - b)$.

- Congruence modulo n can be visualized in terms of an "n-hour clock" (see the picture below for the case $n = 5$).



- **Reminder:** $a \equiv b \pmod{n}$ means that $n \mid (a - b)$.

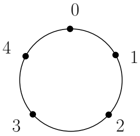
- Congruence modulo n can be visualized in terms of an "n-hour clock" (see the picture below for the case $n = 5$).



- Suppose we are given an integer a, and we wish to determine which of $0, 1, \ldots, n-1$ it is congruent to modulo n.

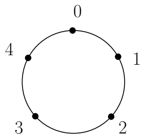
- **Reminder:** $a \equiv b \pmod{n}$ means that $n \mid (a - b)$.

- Congruence modulo n can 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 $0, 1, \ldots, n - 1$ it is congruent to modulo n.
- Obviously, if $a = 0$, then $a \equiv 0 \pmod{n}$.

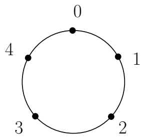
- **Reminder:** $a \equiv b \pmod{n}$ means that $n \mid (a - b)$.
- Congruence modulo n can be visualized in terms of an "n-hour clock" (see the picture below for the case $n = 5$).



- Suppose we are given an integer a, and we wish to determine which of $0, 1, \ldots, n-1$ 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, $14 \equiv 4 \pmod{5}$.

- **Reminder:** $a \equiv b \pmod{n}$ means that $n \mid (a - b)$.

- Congruence modulo n can 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 $0, 1, \ldots, n-1$ 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, $14 \equiv 4 \pmod{5}$.
- On the other hand, if a is negative, then we make $|a| = -a$ many counterclockwise steps.
  - For example, $-7 \equiv 3 \pmod{5}$.

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 0.2.2

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 $a \equiv c \pmod{n}$.

Remark: Proposition 0.2.2 states that congruence modulo n is an "equivalence relation" on $\mathbb{Z}$. (If you are not yet familiar with equivalence relations, you will soon learn about them in Discrete Math.)

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 $a \equiv c \pmod{n}$.

Remark: Proposition 0.2.2 states that congruence modulo n is an "equivalence relation" on $\mathbb{Z}$. (If you are not yet familiar with equivalence relations, you will soon learn about them in Discrete Math.)

Proof.

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 $a \equiv c \pmod{n}$.

Remark: Proposition 0.2.2 states that congruence modulo n is an "equivalence relation" on $\mathbb{Z}$. (If you are not yet familiar with equivalence relations, you will soon learn about them in Discrete Math.)

Proof. (a) and (b) are obvious.

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 $a \equiv c \pmod{n}$.

Remark: Proposition 0.2.2 states that congruence modulo n is an "equivalence relation" on $\mathbb{Z}$. (If you are not yet familiar with equivalence relations, you will soon learn about them in Discrete Math.)

Proof. (a) and (b) are obvious. For (c), assume that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $n \mid (a - b)$ and $n \mid (b - c)$, i.e. there exist $k, \ell \in \mathbb{Z}$ s.t. $a - b = kn$ and $b - c = \ell n$.

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 $a \equiv c \pmod{n}$.

Remark: Proposition 0.2.2 states that congruence modulo n is an "equivalence relation" on $\mathbb{Z}$. (If you are not yet familiar with equivalence relations, you will soon learn about them in Discrete Math.)

Proof. (a) and (b) are obvious. For (c), assume that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $n \mid (a - b)$ and $n \mid (b - c)$, i.e. 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) $a + c \equiv b + d \pmod{n}$;

(b) $a - c \equiv b - d \pmod{n}$;

(c) $ac \equiv bd \pmod{n}$.

Proof.

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) $ac \equiv bd \pmod{n}$.

Proof. Since $a \equiv b \pmod{n}$, we have that $n|(a - b)$, 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. $c - d = \ell n$.

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) $ac \equiv bd \pmod{n}$.

Proof. Since $a \equiv b \pmod{n}$, we have that $n|(a-b)$, 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. $c - d = \ell n$.

To prove (a), we observe that

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

and so $n \mid \big((a+c)-(b+d)\big)$. Thus, $a + c \equiv b + d \pmod{n}$. This proves (a).

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) $ac \equiv bd \pmod{n}$.

Proof. Since $a \equiv b \pmod{n}$, we have that $n|(a-b)$, 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. $c - d = \ell n$.

To prove (a), we observe that

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

and so $n \mid ((a+c)-(b+d))$. Thus, $a + c \equiv b + d \pmod{n}$. This proves (a).

The proof of (b) is similar (details: Lecture Notes).

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) $ac \equiv bd \pmod{n}$.

Proof (continued). **Reminder:** $a - b = kn$ and $c - d = \ell n$.

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) $ac \equiv bd \pmod{n}$.

Proof (continued). **Reminder:** $a - b = kn$ and $c - d = \ell n$.

For (c), we have that

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

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

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 $t \geq 0$.

Proof.

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 $t \geq 0$.

Proof. We proceed by induction on t.

Base case: $t = 0$. By definition, $r^0 = 1$ for all integers r. So, $a^0 = 1 = b^0$, and so $a^0 \equiv b^0 (\text{mod } n)$.

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 $t \geq 0$.

Proof. We proceed by induction on t.

Base case: $t = 0$. By definition, $r^0 = 1$ for all integers r. So, $a^0 = 1 = b^0$, and so $a^0 \equiv b^0 (\text{mod } n)$.

Induction case: Fix a non-negative integer t, and assume inductively that $a^t \equiv b^t \pmod{n}$.

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 $t \geq 0$.

Proof. We proceed by induction on t.

Base case: $t = 0$. By definition, $r^0 = 1$ for all integers r. So, $a^0 = 1 = b^0$, and so $a^0 \equiv b^0 (\text{mod } n)$.

Induction case: Fix a non-negative integer t, and assume inductively that $a^t \equiv b^t \pmod{n}$. Since we also have that $a \equiv b \pmod{n}$, Proposition 0.2.3(c) implies that $a^t a \equiv b^t b \pmod{n}$, i.e. that $a^{t+1} \equiv b^{t+1} \pmod{n}$. This completes the induction. $\square$

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 $a_n, a_{n-1}, \ldots, a_0 \in \{0, 1, \ldots, 9\}$, we define:

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

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

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

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

  Thus, $\overline{a_n a_{n-1} \ldots a_0}$ is the number whose first digit is a_n, whose second digit is a_{n-1}, and so on.
    - It is possible that this first digit is zero.
    - We could eliminate this possibility, but that would result in a messier definition.

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

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

Proposition 0.2.6

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

Proof.

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

Proposition 0.2.6

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

Proof. By definition, an integer is divisible by 9 iff it is congruent to 0 modulo 9. So, the second statement of the proposition follows immediately from the first.

It remains to prove the first statement.

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

Proposition 0.2.6

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

Proof. By definition, an integer is divisible by 9 iff it is congruent to 0 modulo 9. So, the second statement of the proposition follows immediately from the first.

It remains to prove the first statement. Note that $10 \equiv 1 \pmod{9}$.

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

Proposition 0.2.6

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

Proof. By definition, an integer is divisible by 9 iff it is congruent to 0 modulo 9. So, the second statement of the proposition follows immediately from the first.

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.

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

Proposition 0.2.6

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

Proof. By definition, an integer is divisible by 9 iff it is congruent to 0 modulo 9. So, the second statement of the proposition follows immediately from the first.

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 $k \in \{0, \ldots, n\}$, we have that $a_k \cdot 10^k \equiv a_k \pmod 9$.

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

Proposition 0.2.6

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

Proof. By definition, an integer is divisible by 9 iff it is congruent to 0 modulo 9. So, the second statement of the proposition follows immediately from the first.

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,

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

which is what we needed to show. □

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

Proposition 0.2.6

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

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

Proposition 0.2.6

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

Proposition 0.2.7

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

Proof. The proof is completely analogous to that of Proposition 0.2.6: just replace 9 with 3 throughout.

3. Arithmetic in $\mathbb{Z}_n$ and Fermat's Little Theorem

3. Arithmetic in $\mathbb{Z}_n$ and Fermat's Little Theorem

- Given $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, we set

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

note that $[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$.

3. Arithmetic in $\mathbb{Z}_n$ and Fermat's Little Theorem

- Given $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, we set

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

  note that $[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$.
- For example:
  - $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$;
  - $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$;
  - $[0]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\}$;
  - $[1]_3 = \{\dots, -5, -2, 1, 4, 7, \dots\}$;
  - $[2]_3 = \{\dots, -4, -1, 2, 5, 8, \dots\}$.

3. Arithmetic in $\mathbb{Z}_n$ and Fermat's Little Theorem

- Given $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, we set

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

  note that $[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$.
- For example:
  - $[0]_2 = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$;
  - $[1]_2 = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$;
  - $[0]_3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$;
  - $[1]_3 = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$;
  - $[2]_3 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.
- Note also that $a \in [a]_n$, since $a \equiv a \pmod{n}$.

3. Arithmetic in $\mathbb{Z}_n$ and Fermat's Little Theorem

- Given $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, we set

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

  note that $[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$.
- For example:
  - $[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$;
  - $[1]_2 = \{\dots, -3, -1, 1, 3, 5, \dots\}$;
  - $[0]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\}$;
  - $[1]_3 = \{\dots, -5, -2, 1, 4, 7, \dots\}$;
  - $[2]_3 = \{\dots, -4, -1, 2, 5, 8, \dots\}$.
- Note also that $a \in [a]_n$, since $a \equiv a \pmod{n}$.
- We define

$$\mathbb{Z}_n \quad := \quad \{[a]_n \mid a \in \mathbb{Z}\}.$$

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

Proof.

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

Proof. This follows from the fact that, by Proposition 0.2.2, congruence modulo n is an equivalence relation on $\mathbb{Z}$. If you are not familiar with the theory of equivalence relations, here is a detailed proof.

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

Proof (continued). We first prove (a).

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

Proof (continued). We first prove (a). Suppose that $a \equiv b \pmod{n}$. WTS $[a]_n = [b]_n$.

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

Proof (continued). We first prove (a). Suppose that $a \equiv b \pmod{n}$. WTS $[a]_n = [b]_n$. It suffices to show that $[a]_n \subseteq [b]_n$ (the proof of the reverse inclusion is analogous).

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

Proof (continued). We first prove (a). Suppose that $a \equiv b \pmod{n}$. WTS $[a]_n = [b]_n$. 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 $x \equiv b \pmod{n}$.

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

Proof (continued). We first prove (a). Suppose that $a \equiv b \pmod{n}$. WTS $[a]_n = [b]_n$. 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).

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) if $a \not\equiv b \pmod{n}$, then $[a]_n \cap [b]_n = \emptyset$.

Proof (continued). It remains to prove (b).

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) 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 $a \equiv b \pmod{n}$.

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) 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 $x \in [a]_n \cap [b]_n$.

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) 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 $x \equiv b \pmod{n}$.

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

Proposition 0.2.9

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

(a) if $a \equiv b \pmod{n}$, then $[a]_n = [b]_n$;

(b) 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). $\square$

- Note that for $n \in \mathbb{N}$, every integer is congruent to exactly one of $0, \ldots, n-1$ modulo n.

- Note that for $n \in \mathbb{N}$, every integer is congruent to exactly one of $0, \ldots, n-1$ modulo n.
  - By Proposition 0.2.9, it follows that for all $x \in \mathbb{Z}$, the set $[x]_n$ is equal to exactly one of the following: $[0]_n, \ldots, [n-1]_n$.

- Note that for $n \in \mathbb{N}$, every integer is congruent to exactly one of $0, \ldots, n-1$ modulo n.
  - By Proposition 0.2.9, it follows that for all $x \in \mathbb{Z}$, the set $[x]_n$ is equal to exactly one of the following: $[0]_n, \ldots, [n-1]_n$.
- This implies that, in fact:

$$\mathbb{Z}_n \quad = \quad \{[0]_n, \ldots, [n-1]_n\}.$$

- Note that for $n \in \mathbb{N}$, every integer is congruent to exactly one of $0, \ldots, n-1$ modulo n.
    - By Proposition 0.2.9, it follows that for all $x \in \mathbb{Z}$, the set $[x]_n$ is equal to exactly one of the following: $[0]_n, \ldots, [n-1]_n$.
- This implies that, in fact:

$$\mathbb{Z}_n \quad = \quad \{[0]_n, \ldots, [n-1]_n\}.$$

- Moreover, by Proposition 0.2.9, no two of $0, \ldots, n-1$ are congruent to each other modulo n, and consequently, $[0]_n, \ldots, [n-1]_n$ are pairwise disjoint.

- Note that for $n \in \mathbb{N}$, every integer is congruent to exactly one of $0, \ldots, n-1$ modulo n.
  - By Proposition 0.2.9, it follows that for all $x \in \mathbb{Z}$, the set $[x]_n$ is equal to exactly one of the following: $[0]_n, \ldots, [n-1]_n$.
- This implies that, in fact:

$$\mathbb{Z}_n \quad = \quad \{[0]_n, \ldots, [n-1]_n\}.$$

- Moreover, by Proposition 0.2.9, no two of $0, \ldots, n-1$ are congruent to each other modulo n, and consequently, $[0]_n, \ldots, [n-1]_n$ are pairwise disjoint.
- We now deduce that the sets $[0]_n, \ldots, [n-1]_n$ form a "partition" of $\mathbb{Z}$, that is:

- Note that for $n \in \mathbb{N}$, every integer is congruent to exactly one of $0, \ldots, n-1$ modulo n.
  - By Proposition 0.2.9, it follows that for all $x \in \mathbb{Z}$, the set $[x]_n$ is equal to exactly one of the following: $[0]_n, \ldots, [n-1]_n$.
- This implies that, in fact:

$$\mathbb{Z}_n \quad = \quad \{[0]_n, \ldots, [n-1]_n\}.$$

- Moreover, by Proposition 0.2.9, no two of $0, \ldots, n-1$ are congruent to each other modulo n, and consequently, $[0]_n, \ldots, [n-1]_n$ are pairwise disjoint.
- We now deduce that the sets $[0]_n, \ldots, [n-1]_n$ form a "partition" of $\mathbb{Z}$, that is:
  - $\mathbb{Z} = [0]_n \cup \cdots \cup [n-1]_n$, and

- Note that for $n \in \mathbb{N}$, every integer is congruent to exactly one of $0, \ldots, n-1$ modulo n.
  - By Proposition 0.2.9, it follows that for all $x \in \mathbb{Z}$, the set $[x]_n$ is equal to exactly one of the following: $[0]_n, \ldots, [n-1]_n$.
- This implies that, in fact:

$$\mathbb{Z}_n \quad = \quad \{[0]_n, \ldots, [n-1]_n\}.$$

- Moreover, by Proposition 0.2.9, no two of $0, \ldots, n-1$ are congruent to each other modulo n, and consequently, $[0]_n, \ldots, [n-1]_n$ are pairwise disjoint.
- We now deduce that the sets $[0]_n, \ldots, [n-1]_n$ form a "partition" of $\mathbb{Z}$, that is:
  - $\mathbb{Z} = [0]_n \cup \cdots \cup [n-1]_n$, and
  - the sets $[0]_n, \ldots, [n-1]_n$ are pairwise disjoint.

- Note that for $n \in \mathbb{N}$, every integer is congruent to exactly one of $0, \ldots, n-1$ modulo n.
  - By Proposition 0.2.9, it follows that for all $x \in \mathbb{Z}$, the set $[x]_n$ is equal to exactly one of the following: $[0]_n, \ldots, [n-1]_n$.
- This implies that, in fact:

$$\mathbb{Z}_n \quad = \quad \{[0]_n, \ldots, [n-1]_n\}.$$

- Moreover, by Proposition 0.2.9, no two of $0, \ldots, n-1$ are congruent to each other modulo n, and consequently, $[0]_n, \ldots, [n-1]_n$ are pairwise disjoint.
- We now deduce that the sets $[0]_n, \ldots, [n-1]_n$ form a "partition" of $\mathbb{Z}$, that is:
  - $\mathbb{Z} = [0]_n \cup \cdots \cup [n-1]_n$, and
  - the sets $[0]_n, \ldots, [n-1]_n$ 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 $[0]_n, \ldots, [n-1]_n$ are the associated equivalence classes.

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

- **Reminder:** For a positive integer n:
  - $[a]_n := \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$ for all $a \in \mathbb{Z}$;
  - $\mathbb{Z}_n := \{[a]_n \mid a \in \mathbb{Z}\} = \{[0]_n, \dots, [n-1]_n\}$.
- **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 0.2.10

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 $[1]_2$.

[a] In 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) $a + c \equiv b + d \pmod{n}$;

(b) $a - c \equiv b - d \pmod{n}$;

(c) $ac \equiv bd \pmod{n}$.

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) $ac \equiv bd \pmod{n}$.

- By Proposition 0.2.3, 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
  - $[a + b]_n = [a' + b']_n$,
  - $[a - b]_n = [a' - b']_n$, and
  - $[ab]_n = [a'b']_n$.

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) $ac \equiv bd \pmod{n}$.

- By Proposition 0.2.3, 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
  - $[a + b]_n = [a' + b']_n$,
  - $[a - b]_n = [a' - b']_n$, and
  - $[ab]_n = [a'b']_n$.
- Thus, we may define addition, subtraction, and multiplication in $\mathbb{Z}_n$ as follows.

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) $ac \equiv bd \pmod{n}$.

- By Proposition 0.2.3, 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
  - $[a + b]_n = [a' + b']_n$,
  - $[a - b]_n = [a' - b']_n$, and
  - $[ab]_n = [a'b']_n$.
- Thus, we may define addition, subtraction, and multiplication in $\mathbb{Z}_n$ as follows.
- 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 0.2.11

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

(a) 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 $ab = ba$;

(b) 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 $(ab)c = a(bc)$;

(c) multiplication is distributive over addition in $\mathbb{Z}_n$, that is, for all $a, b, c \in \mathbb{Z}_n$, we have that $a(b + c) = ab + ac$.

Proof.

Proposition 0.2.11

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

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

Proof. 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 $\mathbb{Z}$.

The proof of the commutativity of addition is in the Lecture Notes. The rest is an exercise. □

- Let us now take a look at the addition and multiplication tables for $\mathbb{Z}_n$, for a few small values of n.

- Let us now take a look at the addition and multiplication tables for $\mathbb{Z}_n$, for a few small values of n.

Example 0.2.12

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 0.2.13

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

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

[a] Remember, in this context, 0 stands for $[0]_3$, 1 stands for $[1]_3$, and 2 stands for $[2]_3$.

Example 0.2.14

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

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

[a] Remember, 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 0.2.15

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

$\cdot$	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

[a] Remember, 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

·	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

$\mathbb{Z}_4$:

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

·	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

·	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, $0 = [0]_n$).

- **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.

- **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.

- **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 $\mathbb{Z}_2$: $-0 = 0, \quad -1 = 1;$
  - in $\mathbb{Z}_3$: $-0 = 0, \quad -1 = 2, \quad -2 = 1;$
  - in $\mathbb{Z}_4$: $-0 = 0, \quad -1 = 3, \quad -2 = 2, \quad -3 = 1;$
  - in $\mathbb{Z}_5$: $-0 = 0, \quad -1 = 4, \quad -2 = 3, \quad -3 = 2, \quad -4 = 1.$

$\mathbb{Z}_2$:

+	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

$\mathbb{Z}_4$:

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

·	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

·	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:** 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.
- As Theorem 0.2.16 and Corollary 0.2.17 (see below) show, this is not an accident!

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

Proof.

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

Proof. WTS no two of $0, a, 2a, \ldots, (n-1)a$ are congruent modulo n. (Note that this implies that $[a]_n, [2a]_n, \ldots, [(n-1)a]_n$ are pairwise distinct.)

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

Proof. WTS no two of $0, a, 2a, \ldots, (n-1)a$ are congruent modulo n. (Note that this implies that $[a]_n, [2a]_n, \ldots, [(n-1)a]_n$ are pairwise distinct.)

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

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

Proof. WTS no two of $0, a, 2a, \ldots, (n-1)a$ are congruent modulo n. (Note that this implies that $[a]_n, [2a]_n, \ldots, [(n-1)a]_n$ are pairwise distinct.)

Suppose otherwise, and fix distinct $i, j \in \{0, \ldots, n-1\}$ s.t. $ia \equiv ja \pmod{n}$. Then $(i-j)a \equiv 0 \pmod{n}$, that is, $n | (i-j)a$.

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

Proof. WTS no two of $0, a, 2a, \ldots, (n-1)a$ are congruent modulo n. (Note that this implies that $[a]_n, [2a]_n, \ldots, [(n-1)a]_n$ are pairwise distinct.)

Suppose otherwise, and fix distinct $i, j \in \{0, \ldots, n-1\}$ 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 $n|(i-j)$.

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

Proof. WTS no two of $0, a, 2a, \ldots, (n-1)a$ are congruent modulo n. (Note that this implies that $[a]_n, [2a]_n, \ldots, [(n-1)a]_n$ are pairwise distinct.)

Suppose otherwise, and fix distinct $i, j \in \{0, \ldots, n-1\}$ 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 $i, j \in \{0, \ldots, n-1\}$ and $i \neq j$, and so $0 < |i-j| < n$.

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

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

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

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

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

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

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a]This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

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

We know that every integer is congruent modulo n to one of the following n integers: $0, 1, 2, \ldots, n-1$. We showed above that no two of the following n integers are congruent to each other modulo n: $0, a, 2a, \ldots, (n-1)a$.

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

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

We know that every integer is congruent modulo n to one of the following n integers: $0, 1, 2, \ldots, n-1$. We showed above that no two of the following n integers are congruent to each other modulo n: $0, a, 2a, \ldots, (n-1)a$. It follows that (exactly) one of $0, a, 2a, \ldots, (n-1)a$ is congruent to 1 modulo n.

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

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

We know that every integer is congruent modulo n to one of the following n integers: $0, 1, 2, \ldots, n-1$. We showed above that no two of the following n integers are congruent to each other modulo n: $0, a, 2a, \ldots, (n-1)a$. It follows that (exactly) one of $0, a, 2a, \ldots, (n-1)a$ is congruent to 1 modulo n.

In other words, for exactly one value of $b \in \{0, 1, 2, \ldots, n-1\}$, we have that $ba \equiv 1 \pmod{n}$.

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

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

We know that every integer is congruent modulo n to one of the following n integers: $0, 1, 2, \ldots, n-1$. We showed above that no two of the following n integers are congruent to each other modulo n: $0, a, 2a, \ldots, (n-1)a$. It follows that (exactly) one of $0, a, 2a, \ldots, (n-1)a$ is congruent to 1 modulo n.

In other words, for exactly one value of $b \in \{0, 1, 2, \ldots, n-1\}$, we have that $ba \equiv 1 \pmod{n}$. For this b, we have that $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$. □

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

Theorem 0.2.16

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime.[a] Then there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$, and therefore, $[a]_n[b]_n = [1]_n$.

---

[a] This means that the greatest common divisor of n and a, denoted by $\gcd(n, a)$, is 1. In other words, the only positive integer that divides both n and a is 1.

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

---

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

Proof.

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

Proof. We first prove (a).

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

Proof. We first prove (a). Since p is a prime number, every integer that is not a multiple of p is relatively prime to p; (a) now follows from Theorem 0.2.17.

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

Proof (continued). Statement (b) immediately follows from (a).

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

Proof (continued). Statement (b) immediately follows from (a). Indeed, fix $a \in \mathbb{Z}_p \setminus \{0\}$.

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

Proof (continued). Statement (b) immediately follows from (a). Indeed, fix $a \in \mathbb{Z}_p \setminus \{0\}$. Then there exists an integer $a' \in \{1, \dots, p-1\}$ s.t. $a = [a']_p$.

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

Proof (continued). Statement (b) immediately follows from (a). Indeed, fix $a \in \mathbb{Z}_p \setminus \{0\}$. Then there exists an integer $a' \in \{1, \dots, p-1\}$ s.t. $a = [a']_p$. By (a), there exists an integer b' s.t. $a'b' \equiv 1 \pmod{p}$.

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

Proof (continued). Statement (b) immediately follows from (a). Indeed, fix $a \in \mathbb{Z}_p \setminus \{0\}$. Then there exists an integer $a' \in \{1, \dots, p-1\}$ s.t. $a = [a']_p$. By (a), there exists an integer b' s.t. $a'b' \equiv 1 \pmod{p}$. We now set $b := [b']_p$, and we see that $ab = [a']_p[b']_p = [a'b']_p = [1]_p$.

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

[a]Here, $0 = [0]_p$ and $1 = [1]_p$.

Proof (continued). Statement (b) immediately follows from (a). Indeed, fix $a \in \mathbb{Z}_p \setminus \{0\}$. Then there exists an integer $a' \in \{1, \dots, p-1\}$ s.t. $a = [a']_p$. By (a), there exists an integer b' s.t. $a'b' \equiv 1 \pmod{p}$. We now set $b := [b']_p$, and we see that $ab = [a']_p[b']_p = [a'b']_p = [1]_p$. Moreover, $b \neq 0$, since (in $\mathbb{Z}_p$) we have that $a \cdot 0 = 0 \neq 1 = ab$. This proves (b). $\square$

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

---

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

- Corollary 0.2.17(b) states that, for a prime number p, every number in $\mathbb{Z}_p \setminus \{0\}$ has a multiplicative inverse.

Corollary 0.2.17

Let $p \in \mathbb{N}$ be a prime number. Then:

(a) for all $a \in \mathbb{Z}$ s.t. a is not a multiple of p, there exists some $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{p}$, and consequently, $[a]_p[b]_p = [1]_p$;

(b) for all $a \in \mathbb{Z}_p \setminus \{0\}$, there exists some $b \in \mathbb{Z}_p \setminus \{0\}$ s.t. $ab = 1$.[a]

[a] Here, $0 = [0]_p$ and $1 = [1]_p$.

- Corollary 0.2.17(b) states that, for a prime number p, every number in $\mathbb{Z}_p \setminus \{0\}$ has a multiplicative inverse.
- Fermat's Little Theorem (below) is a strengthening of Corollary 0.2.17 in that it gives an actual formula for this multiplicative inverse.

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 $a^{p-1} \equiv 1 \pmod{p}$.

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 will prove Fermat's Little Theorem in a bit, but first: how does this give a formula for multiplicative inverses?

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 will prove Fermat's Little Theorem in a bit, but first: how does this give a formula for multiplicative inverses?
- 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

$$a^m = \underbrace{a \cdot \cdots \cdot a}_{m},$$

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

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 will prove Fermat's Little Theorem in a bit, but first: how does this give a formula for multiplicative inverses?
- 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

$$a^m = \underbrace{a \cdot \cdots \cdot a}_{m},$$

  where it is understood that the multiplication on the right-hand-side is in $\mathbb{Z}_n$.
- With this set-up, we can restate Fermat's Little Theorem in two ways, as follows.

- Old version (to be proven later):

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 $a^{p-1} \equiv 1 \pmod{p}$.

- Old version (to be proven later):

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 $a^{p-1} \equiv 1 \pmod{p}$.

- Restatements:

- Old version (to be proven later):

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 $a^{p-1} \equiv 1 \pmod{p}$.

- Restatements:

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 $\left([a]_p\right)^{p-1} = [1]_p$.

- Old version (to be proven later):

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 $a^{p-1} \equiv 1 \pmod{p}$.

- Restatements:

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 $\left([a]_p\right)^{p-1} = [1]_p$.

Fermat's Little Theorem

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

Fermat's Little Theorem

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

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 $a \in \mathbb{Z}_p \setminus \{0\}$.

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: $a \cdot a^{p-2} = a^{p-2} \cdot a = 1$.

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 $\mathbb{Z}_p$.

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 $ab = 1$, then by multiplying both sides by a^{p-2}, we obtain

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

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

Fermat's Little Theorem

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

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

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

Fermat's Little Theorem

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

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

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

- Note, 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.

Fermat's Little Theorem

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

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

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

- Note, 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.
- By taking a quick look at the multiplication tables for $\mathbb{Z}_2$, $\mathbb{Z}_3$, and $\mathbb{Z}_5$, we get the following (next slide):

$\mathbb{Z}_2$:

$+$	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

$\mathbb{Z}_5$:

$+$	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

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

- Proof of 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 of 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 $a^{p-1} \equiv 1 \pmod{p}$.

- First, we need some notation.

- Proof of 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 $a^{p-1} \equiv 1 \pmod{p}$.

- First, we need some notation.
- 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.

- Proof of 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 $a^{p-1} \equiv 1 \pmod{p}$.

- First, we need some notation.
- 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 $n! = 1 \cdot 2 \cdot \cdots \cdot n$.

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 $a^{p-1} \equiv 1 \pmod{p}$.

Proof.

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.

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 0.2.16, no two of $0, a, 2a, \ldots, (p-1)a$ are congruent modulo p. For the sake of completeness, here is a full proof.

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 0.2.16, no two of $0, a, 2a, \ldots, (p-1)a$ are congruent modulo p. For the sake of completeness, here is a full proof.

Suppose that some two of $0, a, \ldots, (p-1)a$ 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. 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 0.2.16, no two of $0, a, 2a, \ldots, (p-1)a$ are congruent modulo p. For the sake of completeness, here is a full proof.

Suppose that some two of $0, a, \ldots, (p-1)a$ are congruent modulo p. Fix distinct $i, j \in \{0, 1, \ldots, p-1\}$ s.t. $ia \equiv ja \pmod{p}$.

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. 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 0.2.16, no two of $0, a, 2a, \ldots, (p-1)a$ are congruent modulo p. For the sake of completeness, here is a full proof.

Suppose that some two of $0, a, \ldots, (p-1)a$ are congruent modulo p. Fix distinct $i, j \in \{0, 1, \ldots, p-1\}$ s.t. $ia \equiv ja \pmod{p}$. Then $(i-j)a \equiv 0 \pmod{p}$, that is, $p | (i-j)a$.

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 0.2.16, no two of $0, a, 2a, \ldots, (p-1)a$ are congruent modulo p. For the sake of completeness, here is a full proof.

Suppose that some two of $0, a, \ldots, (p-1)a$ are congruent modulo p. Fix distinct $i, j \in \{0, 1, \ldots, p-1\}$ s.t. $ia \equiv ja \pmod{p}$. Then $(i-j)a \equiv 0 \pmod{p}$, that is, $p|(i-j)a$. Since p is prime and does not divide a, we see that $p|(i-j)$.

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 0.2.16, no two of $0, a, 2a, \ldots, (p-1)a$ are congruent modulo p. For the sake of completeness, here is a full proof.

Suppose that some two of $0, a, \ldots, (p-1)a$ are congruent modulo p. Fix distinct $i, j \in \{0, 1, \ldots, p-1\}$ s.t. $ia \equiv ja \pmod{p}$. Then $(i-j)a \equiv 0 \pmod{p}$, that is, $p|(i-j)a$. Since p is prime and does not divide a, we see that $p|(i-j)$. But this is impossible because $i, j \in \{0, \ldots, p-1\}$ and $i \neq j$, and so $0 < |i-j| < p$.

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. 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 0.2.16, no two of $0, a, 2a, \ldots, (p-1)a$ are congruent modulo p. For the sake of completeness, here is a full proof.

Suppose that some two of $0, a, \ldots, (p-1)a$ are congruent modulo p. Fix distinct $i, j \in \{0, 1, \ldots, p-1\}$ s.t. $ia \equiv ja \pmod{p}$. Then $(i-j)a \equiv 0 \pmod{p}$, that is, $p|(i-j)a$. Since p is prime and does not divide a, we see that $p|(i-j)$. But this is impossible because $i, j \in \{0, \ldots, p-1\}$ and $i \neq j$, and so $0 < |i-j| < p$. Thus, no two of $0, a, 2a, \ldots, (p-1)a$ 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 $0, a, 2a, \ldots, (p-1)a$ 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 $0, a, 2a, \ldots, (p-1)a$ are congruent modulo p.

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

- $a \equiv r_1 \pmod{p}$;
- $2a \equiv r_2 \pmod{p}$;

  $\vdots$
- $(p-1)a \equiv r_{p-1} \pmod{p}$.

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 $0, a, 2a, \ldots, (p-1)a$ are congruent modulo p.

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

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

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

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

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

and so $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$.

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. **Reminder:** $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$.

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. **Reminder:** $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$.

But now

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

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. **Reminder:** $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$.

But now

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

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

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. **Reminder:** $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$.

But now

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

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

Since p is prime, we see that p and $(p-1)!$ are relatively prime.

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. **Reminder:** $(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$.

But now

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

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

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. □