INTEGERS: VIDEO XI
SOME RESULTS ABOUT PRIMES

Bézout's Identity

Theorem (Bézout's Identity)

Let a, $b \in \mathbb{Z} - \{0\}$. Then there exist $x, y \in \mathbb{Z}$, such that $ax + by = \gcd(a, b)$.

Idea of Proof: Exercise!

Bézout's Identity

Theorem (Bézout's Identity)

Let a, $b \in \mathbb{Z} - \{0\}$. Then there exist $x, y \in \mathbb{Z}$, such that $ax + by = \gcd(a, b)$.

Idea of Proof: Exercise!

- Use the Well-Ordering Principle (WOP)
    - Look at the set $S = \{n \in \mathbb{N} | n = ax + by > 0, x, y \in \mathbb{Z}\} \subseteq \mathbb{N}$

Bézout's Identity

Theorem (Bézout's Identity)

Let a, $b \in \mathbb{Z} - \{0\}$. Then there exist $x, y \in \mathbb{Z}$, such that $ax + by = \gcd(a, b)$.

Idea of Proof: Exercise!

- Use the Well-Ordering Principle (WOP)
  - Look at the set $S = \{n \in \mathbb{N} | n = ax + by > 0, x, y \in \mathbb{Z}\} \subseteq \mathbb{N}$
  - Show that $S \neq \varnothing$.

Bézout's Identity

Theorem (Bézout's Identity)

Let $a,\ b \in \mathbb{Z} - \{0\}$. Then there exist $x, y \in \mathbb{Z}$, such that $ax + by = \gcd(a, b)$.

Idea of Proof: Exercise!

- Use the Well-Ordering Principle (WOP)
    - Look at the set $S = \{n \in \mathbb{N} | n = ax + by > 0, x, y \in \mathbb{Z}\} \subseteq \mathbb{N}$
    - Show that $S \neq \varnothing$.
    - By the WOP, there exists a least element $d = ax_0 + by_0 > 0$, $x_0, y_0 \in \mathbb{Z}$!

Bézout's Identity

Theorem (Bézout's Identity)

Let $a, b \in \mathbb{Z} - \{0\}$. Then there exist $x, y \in \mathbb{Z}$, such that $ax + by = \gcd(a, b)$.

Idea of Proof: Exercise!

- Use the Well-Ordering Principle (WOP)
  - Look at the set $S = \{n \in \mathbb{N} | n = ax + by > 0, x, y \in \mathbb{Z}\} \subseteq \mathbb{N}$
  - Show that $S \neq \varnothing$.
  - By the WOP, there exists a least element $d = ax_0 + by_0 > 0$, $x_0, y_0 \in \mathbb{Z}$!
- Show that $d|a$ (similarly $d|b$) using the Quotient-Remainder Theorem:
  - By QRT $a = dq + r$, $0 \leq r < d$

Bézout's Identity

Theorem (Bézout's Identity)

Let $a, b \in \mathbb{Z} - \{0\}$. Then there exist $x, y \in \mathbb{Z}$, such that $ax + by = \gcd(a, b)$.

Idea of Proof: Exercise!

- Use the Well-Ordering Principle (WOP)
    - Look at the set $S = \{n \in \mathbb{N} | n = ax + by > 0, x, y \in \mathbb{Z}\} \subseteq \mathbb{N}$
    - Show that $S \neq \emptyset$.
    - By the WOP, there exists a least element $d = ax_0 + by_0 > 0$, $x_0, y_0 \in \mathbb{Z}$!
- Show that $d|a$ (similarly $d|b$) using the Quotient-Remainder Theorem:
    - By QRT $a = dq + r$, $0 \leq r < d$
    - Deduce plugging in $d = ax_0 + by_0$, that $r \in S$, if $r > 0$: contradiction to d least element!
      Therefore, we need to have $r = 0$.

Theorem (Bézout's Identity)

Let a, $b \in \mathbb{Z} - \{0\}$. Then there exist $x, y \in \mathbb{Z}$, such that $ax + by = \gcd(a, b)$.

Idea of Proof: **Exercise!**

- Use the Well-Ordering Principle (WOP)
  - Look at the set $S = \{n \in \mathbb{N} | n = ax + by > 0, x, y \in \mathbb{Z}\} \subseteq \mathbb{N}$
  - Show that $S \neq \emptyset$.
  - By the WOP, there exists a least element $d = ax_0 + by_0 > 0$, $x_0, y_0 \in \mathbb{Z}$!
- Show that $d|a$ (similarly $d|b$) using the Quotient-Remainder Theorem:
  - By QRT $a = dq + r$, $0 \leq r < d$
  - Deduce plugging in $d = ax_0 + by_0$, that $r \in S$, if $r > 0$: contradiction to d least element!
    Therefore, we need to have $r = 0$.
- Show finally that d is the greatest common divisor of a and b.

...and a useful application

Theorem (Bézout's Identity)

Let $a,\ b \in \mathbb{Z} - \{0\}$. Then there exist $x, y \in \mathbb{Z}$, such that $ax + by = \gcd(a, b)$.

Corollary

Let $a, b \in \mathbb{Z}$. If $n|ab$ for some $n \in \mathbb{N}$ and $\gcd(n, a) = 1$, then $n|b$.

proof

Fundamental Theorem of Arithmetic

Corollary

Let $a, b \in \mathbb{Z}$*. If* $n | ab$ *and* $\gcd(n, a) = 1$*, then* $n | b$*.*

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n > 1$ *has a unique prime factorization.*

Fundamental Theorem of Arithmetic

Corollary

Let $a, b \in \mathbb{Z}$. *If* $n | ab$ *and* $\gcd(n, a) = 1$, *then* $n | b$.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n > 1$ *has a unique prime factorization.*

Proof:

- **We already proved with the Well-Ordering Principle** (Video 6):
  All $n \in \mathbb{N}$, $n > 1$ can be factored by a product of primes!

Fundamental Theorem of Arithmetic

Corollary

Let $a, b \in \mathbb{Z}$. *If* $n|ab$ *and* $\gcd(n, a) = 1$, *then* $n|b$.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n > 1$ *has a unique prime factorization.*

Proof:

- **We already proved with the Well-Ordering Principle** (Video 6):
  All $n \in \mathbb{N}$, $n > 1$ can be factored by a product of primes!
- **We just need to prove the uniqueness: Proof by contradiction!**
  - Assume there are two distinct prime factorizations

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l, \; k, l \in \mathbb{N}.$$

Fundamental Theorem of Arithmetic

Corollary

Let $a, b \in \mathbb{Z}$. If $n|ab$ and $\gcd(n, a) = 1$, then $n|b$.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n > 1$ has a unique prime factorization.

Proof:

- **We already proved with the Well-Ordering Principle** (Video 6):
  All $n \in \mathbb{N}$, $n > 1$ can be factored by a product of primes!
- **We just need to prove the uniqueness: Proof by contradiction!**
  - Assume there are two distinct prime factorizations
    $$n = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_l, \ k, l \in \mathbb{N}.$$
  - Remove all common primes:
    $$p_{i_1} p_{i_2} \ldots p_{i_m} = q_{j_1} q_{j_2} \ldots q_{j_m}.$$

Fundamental Theorem of Arithmetic

Corollary

Let $a, b \in \mathbb{Z}$. If $n|ab$ and $\gcd(n, a) = 1$, then $n|b$.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n > 1$ has a unique prime factorization.

Proof:

- **We already proved with the Well-Ordering Principle** (Video 6):
  All $n \in \mathbb{N}$, $n > 1$ can be factored by a product of primes!
- **We just need to prove the uniqueness: Proof by contradiction!**
  - Assume there are two distinct prime factorizations
    $$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l, \ k, l \in \mathbb{N}.$$
  - Remove all common primes:
    $$p_{i_1} p_{i_2} \dots p_{i_m} = q_{j_1} q_{j_2} \dots q_{j_m}.$$
    Now all p_{i_s} are different from all q_{j_t}!

Corollary

Let $a, b \in \mathbb{Z}$. *If* $n|ab$ *and* $\gcd(n, a) = 1$, *then* $n|b$.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n > 1$ *has a unique prime factorization.*

Proof:

- **We already proved with the Well-Ordering Principle** (Video 6):
  All $n \in \mathbb{N}$, $n > 1$ can be factored by a product of primes!
- **We just need to prove the uniqueness: Proof by contradiction!**
  - Assume there are two distinct prime factorizations
    $$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l, \ k, l \in \mathbb{N}.$$
  - Remove all common primes:
    $$p_{i_1} p_{i_2} \dots p_{i_m} = q_{j_1} q_{j_2} \dots q_{j_m}.$$
    Now all p_{i_s} are different from all q_{j_t}!
  - Obviously p_{i_1} divides the left handside, hence $p_{i_1} \big| q_{j_1} q_{j_2} \dots q_{j_m}$.

Fundamental Theorem of Arithmetic

Corollary

Let $a, b \in \mathbb{Z}$. If $n|ab$ and $\gcd(n, a) = 1$, then $n|b$.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n > 1$ has a unique prime factorization.

Proof:

- **We already proved with the Well-Ordering Principle** (Video 6):
  All $n \in \mathbb{N}$, $n > 1$ can be factored by a product of primes!
- **We just need to prove the uniqueness: Proof by contradiction!**
  - Assume there are two distinct prime factorizations
    $$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l, \ k, l \in \mathbb{N}.$$
  - Remove all common primes:
    $$p_{i_1} p_{i_2} \dots p_{i_m} = q_{j_1} q_{j_2} \dots q_{j_m}.$$
    Now all p_{i_s} are different from all q_{j_t}!
  - Obviously p_{i_1} divides the left handside, hence $p_{i_1} \big| q_{j_1} q_{j_2} \dots q_{j_m}$.
  - By above Corollary: $p_{i_1} | q_{j_t}$, for some j_t.
    Contradiction since q_{j_t} prime! $\Rightarrow$ The factorization is unique. $\square$

Fundamental Theorem of Arithmetic

Corollary

Let $a, b \in \mathbb{Z}$. If $n|ab$ and $\gcd(n, a) = 1$, then $n|b$.

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n > 1$ has a unique prime factorization.

Proof:

- **We already proved with the Well-Ordering Principle** (Video 6):
  All $n \in \mathbb{N}$, $n > 1$ can be factored by a product of primes!
- **We just need to prove the uniqueness: Proof by contradiction!**
  - Assume there are two distinct prime factorizations
    $$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l, \; k, l \in \mathbb{N}.$$
  - Remove all common primes:
    $$p_{i_1} p_{i_2} \dots p_{i_m} = q_{j_1} q_{j_2} \dots q_{j_m}.$$
    Now all p_{i_s} are different from all q_{j_t}!
  - Obviously p_{i_1} divides the left handside, hence $p_{i_1} \big| q_{j_1} q_{j_2} \dots q_{j_m}$.
  - By above Corollary: $p_{i_1} | q_{j_t}$, for some j_t.
    Contradiction since q_{j_t} prime! $\Rightarrow$ The factorization is unique. $\square$

Prime power factorization: $a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$**,** $n_1 \dots n_k > 0$, $p_1 < p_2 < \dots < p_k$**.**

Applications of the Fundamental Theorem

Theorem (Fundamental Theorem of Arithmetic)

Every integer $n > 1$ has a unique prime factorization.

Theorem ((Infinitude of primes))

There are infinitely many primes.

Proof:

Applications of the Fundamental Theorem

Proposition

Let $a, b \in \mathbb{N}$ *with prime power factorization*

$$a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} q_1^{s_1} \dots q_l^{s_l}, \quad b = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} r_1^{t_1} \dots r_j^{t_j},$$

where

Applications of the Fundamental Theorem

Proposition

Let $a, b \in \mathbb{N}$ with prime power factorization

$$a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} q_1^{s_1} \dots q_l^{s_l}, \quad b = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} r_1^{t_1} \dots r_j^{t_j},$$

where

- ***the primes appearing** (p_i, q_i, r_i) **are all distinct***
- *all exponents are positive*
- *we **don't require the primes be in increasing order** here!*

Applications of the Fundamental Theorem

Proposition

Let $a, b \in \mathbb{N}$ with prime power factorization

$$a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} q_1^{s_1} \dots q_l^{s_l}, \quad b = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} r_1^{t_1} \dots r_j^{t_j},$$

where

- ***the primes appearing** (p_i, q_i, r_i) **are all distinct***
- *all exponents are positive*
- *we **don't require the primes be in increasing order** here!*

Then

$$\begin{aligned} gcd(a,b) &= p_1^{\min(n_1,m_1)} p_2^{\min(n_2,m_2)} \dots p_k^{\min(n_k,m_k)}, \\ lcm(a,b) &= p_1^{\max(n_1,m_1)} p_2^{\max(n_2,m_2)} \dots p_k^{\max(n_k,m_k)} q_1^{s_1} \dots q_i^{s_i} r_1^{t_1} \dots r_j^{t_j}. \end{aligned}$$

Example:

INTEGERS: VIDEO XII
MODULAR ARITHMETIC

Modular arithmetic

Definition

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}, n > 0$. We say that a is congruent to b modulo n if $n|(a-b)$.

Notation: $a \equiv b \mod n$.

Modular arithmetic

Definition

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}, n > 0$. We say that a is congruent to b modulo n if $n|(a-b)$.
Notation: $a \equiv b \mod n$.

Proposition

Let $a, b, c \in \mathbb{Z}$. Then for $n \in \mathbb{N}, n > 0$.

1. $a \equiv a \mod n$, *for all $a \in \mathbb{Z}$.*

Modular arithmetic

Definition

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}, n > 0$. We say that a is congruent to b modulo n if $n | (a - b)$.
Notation: $a \equiv b \mod n$.

Proposition

Let $a, b, c \in \mathbb{Z}$. Then for $n \in \mathbb{N}, n > 0$.

1. $a \equiv a \mod n$, *for all* $a \in \mathbb{Z}$.
2. *If* $a \equiv b \mod n$, *then* $b \equiv a \mod n$.

Modular arithmetic

Definition

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}, n > 0$. We say that a is congruent to b modulo n if $n|(a-b)$.
Notation: $a \equiv b \mod n$.

Proposition

Let $a, b, c \in \mathbb{Z}$. Then for $n \in \mathbb{N}, n > 0$.

1. $a \equiv a \mod n$, *for all* $a \in \mathbb{Z}$.
2. *If* $a \equiv b \mod n$, *then* $b \equiv a \mod n$.
3. *If* $a \equiv b \mod n$ *and* $b \equiv c \mod n$, *then* $a \equiv c \mod n$.

Modular arithmetic

Definition

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}, n > 0$. We say that a is congruent to b modulo n if $n|(a-b)$.
Notation: $a \equiv b \mod n$.

Proposition

Let $a, b, c \in \mathbb{Z}$. Then for $n \in \mathbb{N}, n > 0$.

1. $a \equiv a \mod n$, *for all* $a \in \mathbb{Z}$.
2. *If* $a \equiv b \mod n$, *then* $b \equiv a \mod n$.
3. *If* $a \equiv b \mod n$ *and* $b \equiv c \mod n$, *then* $a \equiv c \mod n$.

★ **This means that $\equiv$ defines an equivalence relation on the set of integers!**

Definition

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}, n > 0$. We say that a is congruent to b modulo n if $n|(a-b)$.

Proof of proposition: Let $a, b, c \in \mathbb{Z}$. Then for $n \in \mathbb{N}, n > 0$.

1. Reflexivity: $a \equiv a \mod n$, for all $a \in \mathbb{Z}$.
2. Symmetry: $a \equiv b \mod n$, then $b \equiv a \mod n$.
3. Transitivity: If $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$.

And we can define **congruence classes:**

$$[a]_n := \{b \in \mathbb{Z} | b \equiv a \mod n\}.$$

First results

Proposition

Let $a, b \in \mathbb{Z}$, n a positive integer. Then $a \equiv b \mod n$ if and only if there exists $k \in \mathbb{Z}$ such that $a = b + kn$.

Proof:

Consequently:
$[a]_n := \{a + kn | k \in \mathbb{Z}\} = \{\dots a - 2n,\ a - n,\ a,\ a + n,\ a + 2n, \dots\}$

Proposition

Let $a, b \in \mathbb{Z}$ and n a positive integer. Then $a \equiv b \mod n$ if and only if a and b have the same remainder after division by n.

Proof:

- Keep in mind! $[a]_n := \{a + kn | k \in \mathbb{Z}\} = \{\ldots a - 2n,\ a - n,\ a,\ a + n,\ a + 2n, \ldots\}$.

Proposition

There are exactly n congruences classes modulo n: $[0]_n, [1]_n, ..., [n-1]_n$.

Intuition:

- **n=1**: $[a]_1 := \{a + k | k \in \mathbb{Z}\} = \{\ldots a - 2,\ a - 1,\ a,\ a + 1,\ a + 2, \ldots\} = \mathbb{N}$!

Congruence Classes

- Keep in mind! $[a]_n := \{a + kn | k \in \mathbb{Z}\} = \{\dots a - 2n,\ a - n,\ a,\ a + n,\ a + 2n, \dots\}$.

Proposition

There are exactly n congruences classes modulo n: $[0]_n, [1]_n, \dots, [n-1]_n$.

Intuition:

- **n=1**: $[a]_1 := \{a + k | k \in \mathbb{Z}\} = \{\dots a - 2,\ a - 1,\ a,\ a + 1,\ a + 2, \dots\} = \mathbb{N}$!
  All numbers are congruent modulo 1: $[0]_1 = [1]_1 = [2]_1 = \dots$

$\Rightarrow$ only **one congruence classe mod 1**.

Congruence Classes

- Keep in mind! $[a]_n := \{a + kn | k \in \mathbb{Z}\} = \{\dots a - 2n,\ a - n,\ a,\ a + n,\ a + 2n, \dots\}$.

Proposition

There are exactly n congruences classes modulo n: $[0]_n, [1]_n, ..., [n-1]_n$.

Intuition:

- **n=1**: $[a]_1 := \{a + k | k \in \mathbb{Z}\} = \{\dots a - 2,\ a - 1,\ a,\ a + 1,\ a + 2, \dots\} = \mathbb{N}$!
  All numbers are congruent modulo 1: $[0]_1 = [1]_1 = [2]_1 = \dots$

  $\Rightarrow$ only **one congruence classe mod 1**.

- **n=2**: $[a]_2 := \{a + 2k | k \in \mathbb{Z}\} = \{\dots a - 4,\ a - 2,\ a,\ a + 2,\ a + 4, \dots\}$

Congruence Classes

- Keep in mind! $[a]_n := \{a + kn | k \in \mathbb{Z}\} = \{\dots a - 2n,\ a - n,\ a,\ a + n,\ a + 2n, \dots\}$.

Proposition

There are exactly n congruences classes modulo n: $[0]_n, [1]_n, \dots, [n-1]_n$.

Intuition:

- **n=1**: $[a]_1 := \{a + k | k \in \mathbb{Z}\} = \{\dots a - 2,\ a - 1,\ a,\ a + 1,\ a + 2, \dots\} = \mathbb{N}$!
  All numbers are congruent modulo 1: $[0]_1 = [1]_1 = [2]_1 = \dots$

  $\Rightarrow$ only **one congruence classe mod 1**.

- **n=2**: $[a]_2 := \{a + 2k | k \in \mathbb{Z}\} = \{\dots a - 4,\ a - 2,\ a,\ a + 2,\ a + 4, \dots\}$
  Numbers of the same class have same parity: $[0]_2 = [2]_2 = [4]_2 = \dots$ and $[1]_2 = [3]_2 = [5]_2 = \dots$.

  $\Rightarrow$ **two congruence classes mod 2**.

Congruence Classes

- Keep in mind! $[a]_n := \{a + kn | k \in \mathbb{Z}\} = \{\dots a - 2n,\ a - n,\ a,\ a + n,\ a + 2n, \dots\}$.

Proposition

There are exactly n congruences classes modulo n: $[0]_n, [1]_n, \dots, [n-1]_n$.

Intuition:

- **n=1**: $[a]_1 := \{a + k | k \in \mathbb{Z}\} = \{\dots a - 2,\ a - 1,\ a,\ a + 1,\ a + 2, \dots\} = \mathbb{N}$!
  All numbers are congruent modulo 1: $[0]_1 = [1]_1 = [2]_1 = \dots$

  $\Rightarrow$ only **one congruence classe mod 1**.

- **n=2**: $[a]_2 := \{a + 2k | k \in \mathbb{Z}\} = \{\dots a - 4,\ a - 2,\ a,\ a + 2,\ a + 4, \dots\}$
  Numbers of the same class have same parity: $[0]_2 = [2]_2 = [4]_2 = \dots$ and $[1]_2 = [3]_2 = [5]_2 = \dots$.

  $\Rightarrow$ **two congruence classes mod 2**.

Proposition

There are exactly n congruences classes modulo n: $[0]_n, [1]_n, \ldots, [n-1]_n$.

Proof of Proposition:

- Show that $[0]_n, [1]_n, \ldots, [n-1]_n$ are all different!

- Show that $[0]_n, [1]_n, \ldots, [n-1]_n$ are the only possible classes!

Definition

A **complete system of residues modulo** n is a set of integers such that every integer is congruent modulo n to exactly one integer in the set.

Example:

The set of congruence classes modulo n: $\mathbb{Z}_n$

Definition

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

We want to define operations on our new set of equivalence classes!

Let's just do it the simplest possible way!

The set of congruence classes modulo n: $\mathbb{Z}_n$

Definition

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

We want to define operations on our new set of equivalence classes!

Let's just do it the simplest possible way!

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [a+b]_n$$

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [ab]_n.$$

The set of congruence classes modulo n: $\mathbb{Z}_n$

Definition

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

We want to define operations on our new set of equivalence classes!
Let's just do it the simplest possible way!

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [a+b]_n$$
$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [ab]_n.$$

Are we done so easily?

The set of congruence classes modulo n: $\mathbb{Z}_n$

Definition

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

We want to define operations on our new set of equivalence classes!

Let's just do it the simplest possible way!

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [a+b]_n$$

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [ab]_n.$$

Are we done so easily? NO!!!! WE NEED TO CHECK that the operations are independent of the representatives of the class!

The set of congruence classes modulo n: $\mathbb{Z}_n$

Definition

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

We want to define operations on our new set of equivalence classes!

Let's just do it the simplest possible way!

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [a+b]_n$$
$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [ab]_n.$$

Are we done so easily? NO!!!! WE NEED TO CHECK that the operations are independent of the representatives of the class!

Lemma

Suppose that $a, a', b, b' \in \mathbb{Z}$, such that $[a]_n = [a']_n$ and $[b]_n = [b']_n$. Then

1) $[a+b]_n = [a'+b']_n$ *2)* $[ab]_n = [a'b']_n$.

Proof (of 1)):