

Definition.

Definition. A **partition** of a set X is a collection of

Definition. A **partition** of a set X is a collection of
non-empty

Definition. A **partition** of a set X is a collection of **non-empty pairwise disjoint** subsets of X

Definition. A **partition** of a set X is a collection of **non-empty pairwise disjoint** subsets of X which **cover** the whole X .

Definition. A **partition** of a set X is a collection of **non-empty pairwise disjoint** subsets of X which **cover** the whole X .

In other words,

Definition. A **partition** of a set X is a collection of **non-empty pairwise disjoint** subsets of X which **cover** the whole X .

In other words,

A **partition** of X is a subset $\Sigma \subset \mathcal{P}(X)$ such that

Definition. A **partition** of a set X is a collection of **non-empty pairwise disjoint** subsets of X which **cover** the whole X .

In other words,

A **partition** of X is a subset $\Sigma \subset \mathcal{P}(X)$ such that

$$\forall A \in \Sigma \quad A \neq \emptyset,$$

Definition. A **partition** of a set X is a collection of **non-empty pairwise disjoint** subsets of X which **cover** the whole X .

In other words,

A **partition** of X is a subset $\Sigma \subset \mathcal{P}(X)$ such that

$$\forall A \in \Sigma \quad A \neq \emptyset,$$

$$\forall A, B \in \Sigma \quad A \neq B \implies A \cap B = \emptyset,$$

Definition. A **partition** of a set X is a collection of **non-empty pairwise disjoint** subsets of X which **cover** the whole X .

In other words,

A **partition** of X is a subset $\Sigma \subset \mathcal{P}(X)$ such that

$$\forall A \in \Sigma \quad A \neq \emptyset,$$

$$\forall A, B \in \Sigma \quad A \neq B \implies A \cap B = \emptyset,$$

$$X = \bigcup_{A \in \Sigma} A.$$

Definition. A **partition** of a set X is a collection of **non-empty pairwise disjoint** subsets of X which **cover** the whole X .

In other words,

A **partition** of X is a subset $\Sigma \subset \mathcal{P}(X)$ such that

$$\forall A \in \Sigma \quad A \neq \emptyset,$$

$$\forall A, B \in \Sigma \quad A \neq B \implies A \cap B = \emptyset,$$

$$X = \bigcup_{A \in \Sigma} A.$$

Yet another reformulation:

Definition. A **partition** of a set X is a collection of **non-empty pairwise disjoint** subsets of X which **cover** the whole X .

In other words,

A **partition** of X is a subset $\Sigma \subset \mathcal{P}(X)$ such that

$$\forall A \in \Sigma \quad A \neq \emptyset,$$

$$\forall A, B \in \Sigma \quad A \neq B \implies A \cap B = \emptyset,$$

$$X = \bigcup_{A \in \Sigma} A.$$

Yet another reformulation:

A **partition** of a set X is a **presentation** of X
as a union of **non-empty pairwise disjoint** sets.

Definition. A **partition** of a set X is a collection of **non-empty pairwise disjoint** subsets of X which **cover** the whole X .

In other words,

A **partition** of X is a subset $\Sigma \subset \mathcal{P}(X)$ such that

$$\forall A \in \Sigma \quad A \neq \emptyset,$$

$$\forall A, B \in \Sigma \quad A \neq B \implies A \cap B = \emptyset,$$

$$X = \bigcup_{A \in \Sigma} A.$$

Yet another reformulation:

A **partition** of a set X is a **presentation** of X
as a union of **non-empty pairwise disjoint** sets.

These disjoint sets are called **elements** of the partition.

Definition. A **partition** of a set X is a collection of **non-empty pairwise disjoint** subsets of X which **cover** the whole X .

In other words,

A **partition** of X is a subset $\Sigma \subset \mathcal{P}(X)$ such that

$$\forall A \in \Sigma \quad A \neq \emptyset,$$

$$\forall A, B \in \Sigma \quad A \neq B \implies A \cap B = \emptyset,$$

$$X = \bigcup_{A \in \Sigma} A.$$

Yet another reformulation:

A **partition** of a set X is a **presentation** of X
as a union of **non-empty pairwise disjoint** sets.

These disjoint sets are called **elements** of the partition.

Each element of X belongs to exactly **one** element of the partition.

Description of a partition by a binary relation

Let X be a set.

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
which elements of X belong to the **same** element of the partition.

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

or in words:

$x \sim_\Sigma y$ iff x and y belong to the same element of the partition Σ .

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
 which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

or in words:

$x \sim_\Sigma y$ iff x and y belong to the same element of the partition Σ .

For any partition Σ of X , the relation \sim_Σ has the following three properties.

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
 which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

or in words:

$x \sim_\Sigma y$ iff x and y belong to the same element of the partition Σ .

For any partition Σ of X , the relation \sim_Σ has the following three properties.

Reflexivity. $\forall a \in X \quad a \sim_\Sigma a$.

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
 which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

or in words:

$x \sim_\Sigma y$ iff x and y belong to the same element of the partition Σ .

For any partition Σ of X , the relation \sim_Σ has the following three properties.

Reflexivity. $\forall a \in X \quad a \sim_\Sigma a$.

Indeed, each $a \in X$ belongs to some element of Σ . Therefore $a \sim_\Sigma a$. □

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
 which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

or in words:

$x \sim_\Sigma y$ iff x and y belong to the same element of the partition Σ .

For any partition Σ of X , the relation \sim_Σ has the following three properties.

Reflexivity. $\forall a \in X \quad a \sim_\Sigma a.$

Indeed, each $a \in X$ belongs to some element of Σ . Therefore $a \sim_\Sigma a.$ □

Symmetry. $\forall a, b \in X \quad a \sim_\Sigma b \implies b \sim_\Sigma a.$

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
 which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

or in words:

$x \sim_\Sigma y$ iff x and y belong to the same element of the partition Σ .

For any partition Σ of X , the relation \sim_Σ has the following three properties.

Reflexivity. $\forall a \in X \quad a \sim_\Sigma a.$

Indeed, each $a \in X$ belongs to some element of Σ . Therefore $a \sim_\Sigma a.$ □

Symmetry. $\forall a, b \in X \quad a \sim_\Sigma b \implies b \sim_\Sigma a.$ Obvious. □

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
 which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

or in words:

$x \sim_\Sigma y$ iff x and y belong to the same element of the partition Σ .

For any partition Σ of X , the relation \sim_Σ has the following three properties.

Reflexivity. $\forall a \in X \quad a \sim_\Sigma a.$

Indeed, each $a \in X$ belongs to some element of Σ . Therefore $a \sim_\Sigma a.$ □

Symmetry. $\forall a, b \in X \quad a \sim_\Sigma b \implies b \sim_\Sigma a.$ Obvious. □

Transitivity. $\forall a, b, c \in X \quad a \sim_\Sigma b \wedge b \sim_\Sigma c \implies a \sim_\Sigma c.$

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
 which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

or in words:

$x \sim_\Sigma y$ iff x and y belong to the same element of the partition Σ .

For any partition Σ of X , the relation \sim_Σ has the following three properties.

Reflexivity. $\forall a \in X \quad a \sim_\Sigma a.$

Indeed, each $a \in X$ belongs to some element of Σ . Therefore $a \sim_\Sigma a.$ □

Symmetry. $\forall a, b \in X \quad a \sim_\Sigma b \implies b \sim_\Sigma a.$ Obvious. □

Transitivity. $\forall a, b, c \in X \quad a \sim_\Sigma b \wedge b \sim_\Sigma c \implies a \sim_\Sigma c.$

If $a \sim_\Sigma b$ and $b \sim_\Sigma c$, then there are $S, T \in \Sigma$ such that $a, b \in S$ and $b, c \in T$.

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
 which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

or in words:

$x \sim_\Sigma y$ iff x and y belong to the same element of the partition Σ .

For any partition Σ of X , the relation \sim_Σ has the following three properties.

Reflexivity. $\forall a \in X \quad a \sim_\Sigma a.$

Indeed, each $a \in X$ belongs to some element of Σ . Therefore $a \sim_\Sigma a.$ □

Symmetry. $\forall a, b \in X \quad a \sim_\Sigma b \implies b \sim_\Sigma a.$ Obvious. □

Transitivity. $\forall a, b, c \in X \quad a \sim_\Sigma b \wedge b \sim_\Sigma c \implies a \sim_\Sigma c.$

If $a \sim_\Sigma b$ and $b \sim_\Sigma c$, then there are $S, T \in \Sigma$ such that $a, b \in S$ and $b, c \in T$.
 Hence $b \in S \cap T$.

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
 which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

or in words:

$x \sim_\Sigma y$ iff x and y belong to the same element of the partition Σ .

For any partition Σ of X , the relation \sim_Σ has the following three properties.

Reflexivity. $\forall a \in X \quad a \sim_\Sigma a$.

Indeed, each $a \in X$ belongs to some element of Σ . Therefore $a \sim_\Sigma a$. □

Symmetry. $\forall a, b \in X \quad a \sim_\Sigma b \implies b \sim_\Sigma a$. Obvious. □

Transitivity. $\forall a, b, c \in X \quad a \sim_\Sigma b \wedge b \sim_\Sigma c \implies a \sim_\Sigma c$.

If $a \sim_\Sigma b$ and $b \sim_\Sigma c$, then there are $S, T \in \Sigma$ such that $a, b \in S$ and $b, c \in T$.
 Hence $b \in S \cap T$. Therefore $S \cap T \neq \emptyset$ and $S = T$.

Description of a partition by a binary relation

Let X be a set.

How to describe a partition $\Sigma \subset \mathcal{P}(X)$ of X ?

Often this is done by specifying, for each element $a \in X$,
which elements of X belong to the **same** element of the partition.

This is encoded in a binary relation \sim_Σ on X defined by formula

$$x \sim_\Sigma y \iff \exists S \in \Sigma \quad x, y \in S.$$

or in words:

$x \sim_\Sigma y$ iff x and y belong to the same element of the partition Σ .

For any partition Σ of X , the relation \sim_Σ has the following three properties.

Reflexivity. $\forall a \in X \quad a \sim_\Sigma a$.

Indeed, each $a \in X$ belongs to some element of Σ . Therefore $a \sim_\Sigma a$. □

Symmetry. $\forall a, b \in X \quad a \sim_\Sigma b \implies b \sim_\Sigma a$. Obvious. □

Transitivity. $\forall a, b, c \in X \quad a \sim_\Sigma b \wedge b \sim_\Sigma c \implies a \sim_\Sigma c$.

If $a \sim_\Sigma b$ and $b \sim_\Sigma c$, then there are $S, T \in \Sigma$ such that $a, b \in S$ and $b, c \in T$.
Hence $b \in S \cap T$. Therefore $S \cap T \neq \emptyset$ and $S = T$. □

Definition. An **equivalence relation** on a set X

Definition. An **equivalence relation** on a set X is a relation \sim which is

Definition. An **equivalence relation** on a set X is a relation \sim which is

- reflexive: $\forall x \in X \quad x \sim x$

Definition. An **equivalence relation** on a set X is a relation \sim which is

- **reflexive:** $\forall x \in X \quad x \sim x$
- **symmetric:** $\forall x, y \in X \quad x \sim y \implies y \sim x$

Definition. An **equivalence relation** on a set X is a relation \sim which is

- **reflexive:** $\forall x \in X \quad x \sim x$
- **symmetric:** $\forall x, y \in X \quad x \sim y \implies y \sim x$
- **transitive:** $\forall x, y, z \in X \quad x \sim y \wedge y \sim z \implies x \sim z.$

Definition. An **equivalence relation** on a set X is a relation \sim which is

- **reflexive:** $\forall x \in X \quad x \sim x$
- **symmetric:** $\forall x, y \in X \quad x \sim y \implies y \sim x$
- **transitive:** $\forall x, y, z \in X \quad x \sim y \wedge y \sim z \implies x \sim z.$

Example 1. Relation “=” on \mathbb{R} is an equivalence relation, since it is

Equivalence relations

Definition. An **equivalence relation** on a set X is a relation \sim which is

- **reflexive:** $\forall x \in X \quad x \sim x$
- **symmetric:** $\forall x, y \in X \quad x \sim y \implies y \sim x$
- **transitive:** $\forall x, y, z \in X \quad x \sim y \wedge y \sim z \implies x \sim z.$

Example 1. Relation “=” on \mathbb{R} is an equivalence relation, since it is

reflexive: $\forall x \in \mathbb{R} \quad x = x$

Definition. An **equivalence relation** on a set X is a relation \sim which is

- **reflexive:** $\forall x \in X \quad x \sim x$
- **symmetric:** $\forall x, y \in X \quad x \sim y \implies y \sim x$
- **transitive:** $\forall x, y, z \in X \quad x \sim y \wedge y \sim z \implies x \sim z.$

Example 1. Relation “=” on \mathbb{R} is an equivalence relation, since it is

reflexive: $\forall x \in \mathbb{R} \quad x = x$

symmetric: $\forall x, y \in \mathbb{R} \quad x = y \implies y = x,$

Equivalence relations

Definition. An **equivalence relation** on a set X is a relation \sim which is

- **reflexive:** $\forall x \in X \quad x \sim x$
- **symmetric:** $\forall x, y \in X \quad x \sim y \implies y \sim x$
- **transitive:** $\forall x, y, z \in X \quad x \sim y \wedge y \sim z \implies x \sim z .$

Example 1. Relation “=” on \mathbb{R} is an equivalence relation, since it is

reflexive: $\forall x \in \mathbb{R} \quad x = x$

symmetric: $\forall x, y \in \mathbb{R} \quad x = y \implies y = x ,$

transitive: $\forall x, y, z \in \mathbb{R} \quad x = y \wedge y = z \implies x = z .$

Equivalence relations

Definition. An **equivalence relation** on a set X is a relation \sim which is

- **reflexive:** $\forall x \in X \quad x \sim x$
- **symmetric:** $\forall x, y \in X \quad x \sim y \implies y \sim x$
- **transitive:** $\forall x, y, z \in X \quad x \sim y \wedge y \sim z \implies x \sim z .$

Example 1. Relation “=” on \mathbb{R} is an equivalence relation, since it is

reflexive: $\forall x \in \mathbb{R} \quad x = x$

symmetric: $\forall x, y \in \mathbb{R} \quad x = y \implies y = x ,$

transitive: $\forall x, y, z \in \mathbb{R} \quad x = y \wedge y = z \implies x = z .$

Example 2. Relation “to be **congruent**” is an equivalence relation

Equivalence relations

Definition. An **equivalence relation** on a set X is a relation \sim which is

- **reflexive:** $\forall x \in X \quad x \sim x$
- **symmetric:** $\forall x, y \in X \quad x \sim y \implies y \sim x$
- **transitive:** $\forall x, y, z \in X \quad x \sim y \wedge y \sim z \implies x \sim z .$

Example 1. Relation “=” on \mathbb{R} is an equivalence relation, since it is

reflexive: $\forall x \in \mathbb{R} \quad x = x$

symmetric: $\forall x, y \in \mathbb{R} \quad x = y \implies y = x ,$

transitive: $\forall x, y, z \in \mathbb{R} \quad x = y \wedge y = z \implies x = z .$

Example 2. Relation “to be **congruent**” is an equivalence relation
 on the set of all triangles on a plane.

Equivalence relations

Definition. An **equivalence relation** on a set X is a relation \sim which is

- **reflexive:** $\forall x \in X \quad x \sim x$
- **symmetric:** $\forall x, y \in X \quad x \sim y \implies y \sim x$
- **transitive:** $\forall x, y, z \in X \quad x \sim y \wedge y \sim z \implies x \sim z .$

Example 1. Relation “=” on \mathbb{R} is an equivalence relation, since it is

reflexive: $\forall x \in \mathbb{R} \quad x = x$

symmetric: $\forall x, y \in \mathbb{R} \quad x = y \implies y = x ,$

transitive: $\forall x, y, z \in \mathbb{R} \quad x = y \wedge y = z \implies x = z .$

Example 2. Relation “to be **congruent**” is an equivalence relation
 on the set of all triangles on a plane.

Example 3. **Similarity** of triangles is an equivalence relation

Equivalence relations

Definition. An **equivalence relation** on a set X is a relation \sim which is

- **reflexive:** $\forall x \in X \quad x \sim x$
- **symmetric:** $\forall x, y \in X \quad x \sim y \implies y \sim x$
- **transitive:** $\forall x, y, z \in X \quad x \sim y \wedge y \sim z \implies x \sim z .$

Example 1. Relation “=” on \mathbb{R} is an equivalence relation, since it is

reflexive: $\forall x \in \mathbb{R} \quad x = x$

symmetric: $\forall x, y \in \mathbb{R} \quad x = y \implies y = x ,$

transitive: $\forall x, y, z \in \mathbb{R} \quad x = y \wedge y = z \implies x = z .$

Example 2. Relation “to be **congruent**” is an equivalence relation
 on the set of all triangles on a plane.

Example 3. Similarity of triangles is an equivalence relation
 on the set of all triangles on a plane.

Examples of equivalence relations

Example 4.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in Mat_n(\mathbb{R})$ are called **similar**

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in Mat_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in Mat_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $Mat_n(\mathbb{R})$.

Example 6.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation!

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in Mat_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $Mat_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in Mat_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $Mat_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

because it is neither reflexive

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

because it is neither reflexive, nor symmetric

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

because it is neither reflexive, nor symmetric, nor transitive.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in Mat_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $Mat_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

because it is neither reflexive, nor symmetric, nor transitive.

Example 8.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

because it is neither reflexive, nor symmetric, nor transitive.

Example 8. Value,

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

because it is neither reflexive, nor symmetric, nor transitive.

Example 8. **Value**, exchange value in economics.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

because it is neither reflexive, nor symmetric, nor transitive.

Example 8. **Value**, exchange value in economics.

Example 9.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in Mat_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $Mat_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

because it is neither reflexive, nor symmetric, nor transitive.

Example 8. **Value**, exchange value in economics.

Example 9. **Color**,

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

because it is neither reflexive, nor symmetric, nor transitive.

Example 8. **Value**, exchange value in economics.

Example 9. **Color**, being of the same color.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

because it is neither reflexive, nor symmetric, nor transitive.

Example 8. **Value**, exchange value in economics.

Example 9. **Color**, being of the same color.

Example 10.

Examples of equivalence relations

Example 4. Relation “to be **parallel**” is an equivalence relation
on the set of lines on a plane.

Example 5 (from linear algebra).

Two matrices $A, B \in \text{Mat}_n(\mathbb{R})$ are called **similar**
if there exists an invertible matrix C such that $B = C^{-1}AC$.

Similarity is an equivalence relation on $\text{Mat}_n(\mathbb{R})$.

Example 6. Is **friendship** an equivalence relation?

No, **Friendship** is **not** an equivalence relation! Why?

because it is neither reflexive, nor transitive.

Example 7. Is **love** an equivalence relation?

No **Love** is **not** an equivalence relation

because it is neither reflexive, nor symmetric, nor transitive.

Example 8. **Value**, exchange value in economics.

Example 9. **Color**, being of the same color.

Example 10. **Smell**.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X .

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$.

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$.
The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called
the **equivalence class** of a .

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$.
The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called
the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X ,
the equivalence classes form a partition of X .

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$.
The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called
the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X ,
the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

(a) Any equivalence class is not empty.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

This means that $c \sim a$ and $c \sim b$

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

This means that $c \sim a$ and $c \sim b$, therefore $a \sim b$.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

This means that $c \sim a$ and $c \sim b$, therefore $a \sim b$. Let us prove that $[a] = [b]$.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

This means that $c \sim a$ and $c \sim b$, therefore $a \sim b$. Let us prove that $[a] = [b]$. Take any $x \in [a]$.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

This means that $c \sim a$ and $c \sim b$, therefore $a \sim b$. Let us prove that $[a] = [b]$. Take any $x \in [a]$. Then $x \sim a$,

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

This means that $c \sim a$ and $c \sim b$, therefore $a \sim b$. Let us prove that $[a] = [b]$. Take any $x \in [a]$. Then $x \sim a$, but $a \sim b$,

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

This means that $c \sim a$ and $c \sim b$, therefore $a \sim b$. Let us prove that $[a] = [b]$. Take any $x \in [a]$. Then $x \sim a$, but $a \sim b$, by transitivity $x \sim b$

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

This means that $c \sim a$ and $c \sim b$, therefore $a \sim b$. Let us prove that $[a] = [b]$. Take any $x \in [a]$. Then $x \sim a$, but $a \sim b$, by transitivity $x \sim b$ so $x \in [b]$.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

This means that $c \sim a$ and $c \sim b$, therefore $a \sim b$. Let us prove that $[a] = [b]$. Take any $x \in [a]$. Then $x \sim a$, but $a \sim b$, by transitivity $x \sim b$ so $x \in [b]$. Therefore, $[a] \subset [b]$.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

This means that $c \sim a$ and $c \sim b$, therefore $a \sim b$. Let us prove that $[a] = [b]$. Take any $x \in [a]$. Then $x \sim a$, but $a \sim b$, by transitivity $x \sim b$ so $x \in [b]$. Therefore, $[a] \subset [b]$. Symmetrically, $[b] \subset [a]$.

Equivalence classes

Definition. Let \sim be an equivalence relation on a set X . Let $a \in X$. The set $[a] = \{x \in X \mid x \sim a\}$ of all elements equivalent to a is called the **equivalence class** of a .

Theorem. For any equivalence relation \sim on X , the equivalence classes form a partition of X .

Proof. We have to prove the following three statements:

- (a) Any equivalence class is not empty.
- (b) Any element of X belongs to some equivalence class.
- (c) Any two equivalence classes either coincide or are disjoint.

Proof of (a): Any equivalence class $[a]$ is not empty, because $a \in [a]$. □

Proof of (b): Any $a \in X$ belongs to the equivalence class $[a]$. □

Proof of (c): Take any $a, b \in X$ and assume that $[a] \cap [b] \neq \emptyset$.

Then $\exists c \in X$ such that $c \in [a]$ and $c \in [b]$.

This means that $c \sim a$ and $c \sim b$, therefore $a \sim b$. Let us prove that $[a] = [b]$. Take any $x \in [a]$. Then $x \sim a$, but $a \sim b$, by transitivity $x \sim b$ so $x \in [b]$. Therefore, $[a] \subset [b]$. Symmetrically, $[b] \subset [a]$.

Together this gives us that $[a] = [b]$. □

We have seen **two constructions**:

We have seen **two constructions**:

1. each **partition** Σ of a set X gives rise to the **equivalence relation** \sim_Σ on X

We have seen **two constructions**:

1. each **partition** Σ of a set X gives rise to the **equivalence relation** \sim_Σ on X
2. and each **equivalence relation** on X gives rise to the **partition**
formed by equivalence classes.

We have seen **two constructions**:

1. each **partition** Σ of a set X gives rise to the **equivalence relation** \sim_Σ on X
2. and each **equivalence relation** on X gives rise to the **partition**
formed by equivalence classes.

It is easy to see that these constructions defines **bijections**

We have seen **two constructions**:

1. each **partition** Σ of a set X gives rise to the **equivalence relation** \sim_Σ on X
2. and each **equivalence relation** on X gives rise to the **partition**
formed by equivalence classes.

It is easy to see that these constructions defines **bijections**
between the set of all **equivalence relations** on a set X

We have seen **two constructions**:

1. each **partition** Σ of a set X gives rise to the **equivalence relation** \sim_Σ on X
2. and each **equivalence relation** on X gives rise to the **partition**
formed by equivalence classes.

It is easy to see that these constructions defines **bijections**

between the set of all **equivalence relations** on a set X
and the set of all **partitions** on X

We have seen **two constructions**:

1. each **partition** Σ of a set X gives rise to the **equivalence relation** \sim_Σ on X
2. and each **equivalence relation** on X gives rise to the **partition**
formed by equivalence classes.

It is easy to see that these constructions defines **bijections**

between the set of all **equivalence relations** on a set X
and the set of all **partitions** on X
inverse to each other.

We have seen **two constructions**:

1. each **partition** Σ of a set X gives rise to the **equivalence relation** \sim_Σ on X
2. and each **equivalence relation** on X gives rise to the **partition**
formed by equivalence classes.

It is easy to see that these constructions defines **bijections**

between the set of all **equivalence relations** on a set X
and the set of all **partitions** on X
inverse to each other.

Exercise. Verify that these two maps are really inverse to each other.

Definition. Let \sim be an equivalence relation on a set X .

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

In other words, the quotient set X/\sim
is the **partition** of X by equivalence classes for \sim .

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

In other words, the quotient set X/\sim
is the **partition** of X by equivalence classes for \sim .

The **partition** and the **quotient set** are

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

In other words, the quotient set X/\sim
is the **partition** of X by equivalence classes for \sim .

The **partition** and the **quotient set** are
sets which consist of the same elements,

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

In other words, the quotient set X/\sim
is the **partition** of X by equivalence classes for \sim .

The **partition** and the **quotient set** are
sets which consist of the same elements,
hence they coincide.

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

In other words, the quotient set X/\sim
is the **partition** of X by equivalence classes for \sim .

The **partition** and the **quotient set** are
sets which consist of the same elements,
hence they coincide.

Why the same set has two names?

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

In other words, the quotient set X/\sim
is the **partition** of X by equivalence classes for \sim .

The **partition** and the **quotient set** are
sets which consist of the same elements,
hence they coincide.

Why the same set has two names? partition and quotient set.

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

In other words, the quotient set X/\sim
is the **partition** of X by equivalence classes for \sim .

The **partition** and the **quotient set** are
sets which consist of the same elements,
hence they coincide.

Why the same set has two names? partition and quotient set.

There is a **stylistic difference** between usage of these terms.

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

In other words, the quotient set X/\sim
is the **partition** of X by equivalence classes for \sim .

The **partition** and the **quotient set** are
sets which consist of the same elements,
hence they coincide.

Why the same set has two names? partition and quotient set.

There is a **stylistic difference** between usage of these terms.

If we remember that the equivalence classes are subsets of X
and keep track of their internal structure, then we speak on a **partition**.

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

In other words, the quotient set X/\sim
is the **partition** of X by equivalence classes for \sim .

The **partition** and the **quotient set** are
sets which consist of the same elements,
hence they coincide.

Why the same set has two names? partition and quotient set.

There is a **stylistic difference** between usage of these terms.

If we remember that the equivalence classes are subsets of X
and keep track of their internal structure, then we speak on a **partition**.

If we think of them as atoms, ignoring their possible internal structure,
then we speak about a **quotient set**.

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

In other words, the quotient set X/\sim
is the **partition** of X by equivalence classes for \sim .

The **partition** and the **quotient set** are
sets which consist of the same elements,
hence they coincide.

Why the same set has two names? partition and quotient set.

There is a **stylistic difference** between usage of these terms.

If we remember that the equivalence classes are subsets of X
and keep track of their internal structure, then we speak on a **partition**.

If we think of them as atoms, ignoring their possible internal structure,
then we speak about a **quotient set**.

Moreover, for a partition Σ of X , we use notation X/Σ .

Quotient set

Definition. Let \sim be an equivalence relation on a set X .
The set of all equivalence classes is called
the **quotient set** of X with respect to \sim
and denoted by X/\sim .

By definition, $X/\sim = \{[x] \mid x \in X\}$.

In other words, the quotient set X/\sim
is the **partition** of X by equivalence classes for \sim .

The **partition** and the **quotient set** are
sets which consist of the same elements,
hence they coincide.

Why the same set has two names? partition and quotient set.

There is a **stylistic difference** between usage of these terms.

If we remember that the equivalence classes are subsets of X
and keep track of their internal structure, then we speak on a **partition**.

If we think of them as atoms, ignoring their possible internal structure,
then we speak about a **quotient set**.

Moreover, for a partition Σ of X , we use notation X/Σ .

Thus, formally speaking, $\Sigma = X/\Sigma$!

Quotient projection

Quotient projection

Let \sim be an equivalence relation on a set X .

Quotient projection

Let \sim be an equivalence relation on a set X . It defines the quotient set X/\sim ,

Quotient projection

Let \sim be an equivalence relation on a set X . It defines the quotient set X/\sim , whose elements are the equivalence classes.

Quotient projection

Let \sim be an equivalence relation on a set X . It defines the quotient set X/\sim , whose elements are the equivalence classes.

The map $\text{pr}_\sim : X \rightarrow X/\sim$

Quotient projection

Let \sim be an equivalence relation on a set X . It defines the quotient set X/\sim , whose elements are the equivalence classes.

The map $\text{pr}_\sim : X \rightarrow X/\sim$ defined by $x \mapsto [x]$

Quotient projection

Let \sim be an equivalence relation on a set X . It defines the quotient set X/\sim , whose elements are the equivalence classes.

The map $\text{pr}_\sim : X \rightarrow X/\sim$ defined by $x \mapsto [x]$ is called the **quotient projection**.

Let \sim be an equivalence relation on a set X . It defines the quotient set X/\sim , whose elements are the equivalence classes.

The map $\text{pr}_\sim : X \rightarrow X/\sim$ defined by $x \mapsto [x]$ is called the **quotient projection**.

The quotient projection is surjective.

Quotient projection

Let \sim be an equivalence relation on a set X . It defines the quotient set X/\sim , whose elements are the equivalence classes.

The map $\text{pr}_\sim : X \rightarrow X/\sim$ defined by $x \mapsto [x]$ is called the **quotient projection**.

The quotient projection is surjective.

Example.

Quotient projection

Let \sim be an equivalence relation on a set X . It defines the quotient set X/\sim , whose elements are the equivalence classes.

The map $\text{pr}_\sim : X \rightarrow X/\sim$ defined by $x \mapsto [x]$ is called the **quotient projection**.

The quotient projection is surjective.

Example. The quotient projection $\mathbb{Z} \rightarrow \mathbb{Z}_m$, $x \mapsto x \bmod m$

Quotient projection

Let \sim be an equivalence relation on a set X . It defines the quotient set X/\sim , whose elements are the equivalence classes.

The map $\text{pr}_\sim : X \rightarrow X/\sim$ defined by $x \mapsto [x]$ is called the **quotient projection**.

The quotient projection is surjective.

Example. The quotient projection $\mathbb{Z} \rightarrow \mathbb{Z}_m$, $x \mapsto x \bmod m$ is called the **reduction modulo m** .

Quotient maps

Let $f : X \rightarrow Y$ be a map, and \sim be an equivalence relation in X .

Let $f : X \rightarrow Y$ be a map, and \sim be an equivalence relation in X .

Assume that $\forall x_1, x_2 \in X \quad x_1 \sim x_2 \implies f(x_1) = f(x_2)$.

Let $f : X \rightarrow Y$ be a map, and \sim be an equivalence relation in X .

Assume that $\forall x_1, x_2 \in X \quad x_1 \sim x_2 \implies f(x_1) = f(x_2)$.

Then f is constant on every equivalence class.

Let $f : X \rightarrow Y$ be a map, and \sim be an equivalence relation in X .

Assume that $\forall x_1, x_2 \in X \quad x_1 \sim x_2 \implies f(x_1) = f(x_2)$.

Then f is constant on every equivalence class.

Define $f/\sim : X/\sim \rightarrow Y$

Let $f : X \rightarrow Y$ be a map, and \sim be an equivalence relation in X .

Assume that $\forall x_1, x_2 \in X \quad x_1 \sim x_2 \implies f(x_1) = f(x_2)$.

Then f is constant on every equivalence class.

Define $f/\sim : X/\sim \rightarrow Y : [x] \mapsto f(x)$,

Let $f : X \rightarrow Y$ be a map, and \sim be an equivalence relation in X .

Assume that $\forall x_1, x_2 \in X \quad x_1 \sim x_2 \implies f(x_1) = f(x_2)$.

Then f is constant on every equivalence class.

Define $f/\sim : X/\sim \rightarrow Y : [x] \mapsto f(x)$,

where $[x]$ denotes the equivalence class that contains x .

Let $f : X \rightarrow Y$ be a map, and \sim be an equivalence relation in X .

Assume that $\forall x_1, x_2 \in X \quad x_1 \sim x_2 \implies f(x_1) = f(x_2)$.

Then f is constant on every equivalence class.

Define $f/\sim : X/\sim \rightarrow Y : [x] \mapsto f(x)$,

where $[x]$ denotes the equivalence class that contains x .

Notice that $f/\sim([x])$ does not depend on the choice of x from $[x]$.

Let $f : X \rightarrow Y$ be a map, and \sim be an equivalence relation in X .

Assume that $\forall x_1, x_2 \in X \quad x_1 \sim x_2 \implies f(x_1) = f(x_2)$.

Then f is constant on every equivalence class.

Define $f/\sim : X/\sim \rightarrow Y : [x] \mapsto f(x)$,

where $[x]$ denotes the equivalence class that contains x .

Notice that $f/\sim([x])$ does not depend on the choice of x from $[x]$.

The map f/\sim is called a **quotient map** of f .

Injective quotient map

Injective quotient map

Let $f : X \rightarrow Y$ be a map.

Injective quotient map

Let $f : X \rightarrow Y$ be a map. Consider the relation on X defined as follows:

Injective quotient map

Let $f : X \rightarrow Y$ be a map. Consider the relation on X defined as follows:

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2) \text{ for } x_1, x_2 \in X.$$

Injective quotient map

Let $f : X \rightarrow Y$ be a map. Consider the relation on X defined as follows:

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2) \text{ for } x_1, x_2 \in X.$$

Obviously, \sim_f is an equivalence relation.

Injective quotient map

Let $f : X \rightarrow Y$ be a map. Consider the relation on X defined as follows:

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2) \text{ for } x_1, x_2 \in X.$$

Obviously, \sim_f is an equivalence relation. What is the quotient set X/\sim_f ?

Injective quotient map

Let $f : X \rightarrow Y$ be a map. Consider the relation on X defined as follows:

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2) \text{ for } x_1, x_2 \in X.$$

Obviously, \sim_f is an equivalence relation. What is the quotient set X/\sim_f ?

Its elements are equivalence classes,

Injective quotient map

Let $f : X \rightarrow Y$ be a map. Consider the relation on X defined as follows:

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2) \text{ for } x_1, x_2 \in X.$$

Obviously, \sim_f is an equivalence relation. What is the quotient set X/\sim_f ?

Its elements are equivalence classes,

the representatives of each class are mapped to the same element in Y .

Injective quotient map

Let $f : X \rightarrow Y$ be a map. Consider the relation on X defined as follows:

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2) \text{ for } x_1, x_2 \in X.$$

Obviously, \sim_f is an equivalence relation. What is the quotient set X/\sim_f ?

Its elements are equivalence classes,

the representatives of each class are mapped to the same element in Y .

That is, $[x] = f^{-1}f(x)$.

Injective quotient map

Let $f : X \rightarrow Y$ be a map. Consider the relation on X defined as follows:

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2) \text{ for } x_1, x_2 \in X.$$

Obviously, \sim_f is an equivalence relation. What is the quotient set X/\sim_f ?

Its elements are equivalence classes,

the representatives of each class are mapped to the same element in Y .

That is, $[x] = f^{-1}f(x)$.

Therefore, the map $f/ : X/\sim_f \rightarrow Y$

Injective quotient map

Let $f : X \rightarrow Y$ be a map. Consider the relation on X defined as follows:

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2) \text{ for } x_1, x_2 \in X.$$

Obviously, \sim_f is an equivalence relation. What is the quotient set X/\sim_f ?

Its elements are equivalence classes,

the representatives of each class are mapped to the same element in Y .

That is, $[x] = f^{-1}f(x)$.

Therefore, the map $f/ : X/\sim_f \rightarrow Y$ defined by $[x] \mapsto f(x)$

Injective quotient map

Let $f : X \rightarrow Y$ be a map. Consider the relation on X defined as follows:

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2) \text{ for } x_1, x_2 \in X.$$

Obviously, \sim_f is an equivalence relation. What is the quotient set X/\sim_f ?

Its elements are equivalence classes,

the representatives of each class are mapped to the same element in Y .

That is, $[x] = f^{-1}f(x)$.

Therefore, the map $f/ : X/\sim_f \rightarrow Y$ defined by $[x] \mapsto f(x)$ is an injection.

Injective quotient map

Let $f : X \rightarrow Y$ be a map. Consider the relation on X defined as follows:

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2) \text{ for } x_1, x_2 \in X.$$

Obviously, \sim_f is an equivalence relation. What is the quotient set X/\sim_f ?

Its elements are equivalence classes,

the representatives of each class are mapped to the same element in Y .

That is, $[x] = f^{-1}f(x)$.

Therefore, the map $f/ : X/\sim_f \rightarrow Y$ defined by $[x] \mapsto f(x)$ is an injection.

It is called the **injective quotient** of f .

Canonical factorization of a map

Canonical factorization of a map

Let us put all pieces together.

Canonical factorization of a map

Let us put all pieces together.

Given a map $f : X \rightarrow Y$,

Canonical factorization of a map

Let us put all pieces together.

Given a map $f : X \rightarrow Y$, one can define the quotient set X/\sim_f

Canonical factorization of a map

Let us put all pieces together.

Given a map $f : X \rightarrow Y$, one can define the quotient set X/\sim_f
and the quotient map $f/ : X/\sim_f \rightarrow \text{Im } f$.

Canonical factorization of a map

Let us put all pieces together.

Given a map $f : X \rightarrow Y$, one can define the quotient set X/\sim_f
and the quotient map $f/\sim_f : X/\sim_f \rightarrow \text{Im } f$.

Beside this, there is the quotient projection $\text{pr}_{\sim_f} : X \rightarrow X/\sim_f$

Let us put all pieces together.

Given a map $f : X \rightarrow Y$, one can define the quotient set X/\sim_f
and the quotient map $f/ : X/\sim_f \rightarrow \text{Im } f$.

Beside this, there is the quotient projection $\text{pr}_{\sim_f} : X \rightarrow X/\sim_f$
and the inclusion map $\text{Im } f \rightarrow Y$.

Let us put all pieces together.

Given a map $f : X \rightarrow Y$, one can define the quotient set X/\sim_f
and the quotient map $f/ : X/\sim_f \rightarrow \text{Im } f$.

Beside this, there is the quotient projection $\text{pr}_{\sim_f} : X \rightarrow X/\sim_f$
and the inclusion map $\text{Im } f \rightarrow Y$.

These maps are organized in the following **commutative** diagram:

Canonical factorization of a map

Let us put all pieces together.

Given a map $f : X \rightarrow Y$, one can define the quotient set X/\sim_f and the quotient map $f/\sim_f : X/\sim_f \rightarrow \text{Im } f$.

Beside this, there is the quotient projection $\text{pr}_{\sim_f} : X \rightarrow X/\sim_f$ and the inclusion map $\text{Im } f \rightarrow Y$.

These maps are organized in the following **commutative** diagram:

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 \text{pr}_{\sim_f} \downarrow & & \uparrow \text{in} \\
 X/\sim_f & \xrightarrow{f/\sim_f} & \text{Im } f
 \end{array}$$

Canonical factorization of a map

Let us put all pieces together.

Given a map $f : X \rightarrow Y$, one can define the quotient set X/\sim_f and the quotient map $f/ : X/\sim_f \rightarrow \text{Im } f$.

Beside this, there is the quotient projection $\text{pr}_{\sim_f} : X \rightarrow X/\sim_f$ and the inclusion map $\text{Im } f \rightarrow Y$.

These maps are organized in the following **commutative** diagram:

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 \text{pr}_{\sim_f} \downarrow & & \uparrow \text{in} \\
 X/\sim_f & \xrightarrow{f/} & \text{Im } f
 \end{array}
 \qquad
 f = \text{in} \circ f/ \circ \text{pr}_{\sim_f}$$

Canonical factorization of a map

Let us put all pieces together.

Given a map $f : X \rightarrow Y$, one can define the quotient set X/\sim_f and the quotient map $f/ : X/\sim_f \rightarrow \text{Im } f$.

Beside this, there is the quotient projection $\text{pr}_{\sim_f} : X \rightarrow X/\sim_f$ and the inclusion map $\text{Im } f \rightarrow Y$.

These maps are organized in the following **commutative** diagram:

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 \text{pr}_{\sim_f} \downarrow & & \uparrow \text{in} \\
 X/\sim_f & \xrightarrow{f/} & \text{Im } f
 \end{array}
 \qquad
 f = \text{in} \circ f/ \circ \text{pr}_{\sim_f}$$

Therefore, any map can be presented

Canonical factorization of a map

Let us put all pieces together.

Given a map $f : X \rightarrow Y$, one can define the quotient set X/\sim_f and the quotient map $f/ : X/\sim_f \rightarrow \text{Im } f$.

Beside this, there is the quotient projection $\text{pr}_{\sim_f} : X \rightarrow X/\sim_f$ and the inclusion map $\text{Im } f \rightarrow Y$.

These maps are organized in the following **commutative** diagram:

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 \text{pr}_{\sim_f} \downarrow & & \uparrow \text{in} \\
 X/\sim_f & \xrightarrow{f/} & \text{Im } f
 \end{array}
 \qquad
 f = \text{in} \circ f/ \circ \text{pr}_{\sim_f}$$

Therefore, any map can be presented

as a composition of a surjection, bijection and injection:

Canonical factorization of a map

Let us put all pieces together.

Given a map $f : X \rightarrow Y$, one can define the quotient set X/\sim_f and the quotient map $f/ : X/\sim_f \rightarrow \text{Im } f$.

Beside this, there is the quotient projection $\text{pr}_{\sim_f} : X \rightarrow X/\sim_f$ and the inclusion map $\text{Im } f \rightarrow Y$.

These maps are organized in the following **commutative** diagram:

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 \text{pr}_{\sim_f} \downarrow & & \uparrow \text{in} \\
 X/\sim_f & \xrightarrow{f/} & \text{Im } f
 \end{array}
 \qquad
 f = \text{in} \circ f/ \circ \text{pr}_{\sim_f}$$

Therefore, any map can be presented

as a composition of a surjection, bijection and injection:

$$f = \underbrace{\text{in}}_{\text{injection}} \circ \underbrace{f/}_{\text{bijection}} \circ \underbrace{\text{pr}_{\sim_f}}_{\text{surjection}}$$

Canonical factorization of a map

Let us put all pieces together.

Given a map $f : X \rightarrow Y$, one can define the quotient set X/\sim_f and the quotient map $f/ : X/\sim_f \rightarrow \text{Im } f$.

Beside this, there is the quotient projection $\text{pr}_{\sim_f} : X \rightarrow X/\sim_f$ and the inclusion map $\text{Im } f \rightarrow Y$.

These maps are organized in the following **commutative** diagram:

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 \text{pr}_{\sim_f} \downarrow & & \uparrow \text{in} \\
 X/\sim_f & \xrightarrow{f/} & \text{Im } f
 \end{array}
 \qquad
 f = \text{in} \circ f/ \circ \text{pr}_{\sim_f}$$

Therefore, any map can be presented

as a composition of a surjection, bijection and injection:

$$f = \underbrace{\text{in}}_{\text{injection}} \circ \underbrace{f/}_{\text{bijection}} \circ \underbrace{\text{pr}_{\sim_f}}_{\text{surjection}}$$

This presentation is called the **canonical factorization** of f .

In this section we will see how
the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

In this section we will see how
the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$.

In this section we will see how
the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$. We call it **modulus**.

In this section we will see how the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$. We call it **modulus**.

Definition. Integers a, b are said to be **congruent** modulo m

In this section we will see how the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$. We call it **modulus**.

Definition. Integers a, b are said to be **congruent** modulo m if $m \mid (a - b)$.

In this section we will see how the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$. We call it **modulus**.

Definition. Integers a, b are said to be **congruent** modulo m if $m \mid (a - b)$.

Notation: $a \equiv b \pmod{m}$

In this section we will see how the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$. We call it **modulus**.

Definition. Integers a, b are said to be **congruent** modulo m if $m \mid (a - b)$.

Notation: $a \equiv b \pmod{m}$

By definition, $a \equiv b \pmod{m} \iff m \mid (a - b) \iff$

In this section we will see how the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$. We call it **modulus**.

Definition. Integers a, b are said to be **congruent** modulo m if $m \mid (a - b)$.

Notation: $a \equiv b \pmod{m}$

By definition, $a \equiv b \pmod{m} \iff m \mid (a - b) \iff$
 a and b have the same remainder when divided by m .

In this section we will see how the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$. We call it **modulus**.

Definition. Integers a, b are said to be **congruent** modulo m if $m \mid (a - b)$.

Notation: $a \equiv b \pmod{m}$

By definition, $a \equiv b \pmod{m} \iff m \mid (a - b) \iff$
 a and b have the same remainder when divided by m .

Examples.

In this section we will see how the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$. We call it **modulus**.

Definition. Integers a, b are said to be **congruent** modulo m if $m \mid (a - b)$.

Notation: $a \equiv b \pmod{m}$

By definition, $a \equiv b \pmod{m} \iff m \mid (a - b) \iff$
 a and b have the same remainder when divided by m .

Examples. $7 \equiv 2 \pmod{5}$

In this section we will see how the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$. We call it **modulus**.

Definition. Integers a, b are said to be **congruent** modulo m if $m \mid (a - b)$.

Notation: $a \equiv b \pmod{m}$

By definition, $a \equiv b \pmod{m} \iff m \mid (a - b) \iff$
 a and b have the same remainder when divided by m .

Examples. $7 \equiv 2 \pmod{5}$ since $5 \mid (7 - 2)$.

In this section we will see how the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$. We call it **modulus**.

Definition. Integers a, b are said to be **congruent** modulo m if $m \mid (a - b)$.

Notation: $a \equiv b \pmod{m}$

By definition, $a \equiv b \pmod{m} \iff m \mid (a - b) \iff$
 a and b have the same remainder when divided by m .

Examples. $7 \equiv 2 \pmod{5}$ since $5 \mid (7 - 2)$.

$$-1 \equiv 13 \pmod{7}$$

Congruence modulo m

In this section we will see how the notion of **equivalence classes** helps to **reason** and **calculate** very **efficiently**.

Fix a positive integer $m \geq 2$. We call it **modulus**.

Definition. Integers a, b are said to be **congruent** modulo m if $m \mid (a - b)$.

Notation: $a \equiv b \pmod{m}$

By definition, $a \equiv b \pmod{m} \iff m \mid (a - b) \iff$
 a and b have the same remainder when divided by m .

Examples. $7 \equiv 2 \pmod{5}$ since $5 \mid (7 - 2)$.
 $-1 \equiv 13 \pmod{7}$ since $7 \mid (-1 - 13)$.

Congruence modulo m is an equivalence relation

MAT 250
Lecture 10
Modular Arithmetic

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof.

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is reflexive:

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

$\equiv \pmod{m}$ is **symmetric**:

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

$\equiv \pmod{m}$ is **symmetric**: $\forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

$\equiv \pmod{m}$ is **symmetric**: $\forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ since
 $m \mid (a - b) \implies m \mid (b - a)$.

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

$\equiv \pmod{m}$ is **symmetric**: $\forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ since
 $m \mid (a - b) \implies m \mid (b - a)$.

$\equiv \pmod{m}$ is **transitive**:

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

$\equiv \pmod{m}$ is **symmetric**: $\forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ since
 $m \mid (a - b) \implies m \mid (b - a)$.

$\equiv \pmod{m}$ is **transitive**:

$\forall a, b, c \in \mathbb{Z} \quad (a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

$\equiv \pmod{m}$ is **symmetric**: $\forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ since
 $m \mid (a - b) \implies m \mid (b - a)$.

$\equiv \pmod{m}$ is **transitive**:

$\forall a, b, c \in \mathbb{Z} \quad (a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$

Indeed, $a \equiv b \pmod{m} \iff m \mid (a - b)$

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

$\equiv \pmod{m}$ is **symmetric**: $\forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ since
 $m \mid (a - b) \implies m \mid (b - a)$.

$\equiv \pmod{m}$ is **transitive**:

$\forall a, b, c \in \mathbb{Z} \quad (a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$

Indeed, $a \equiv b \pmod{m} \iff m \mid (a - b)$ and $b \equiv c \pmod{m} \iff m \mid (b - c)$.

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

$\equiv \pmod{m}$ is **symmetric**: $\forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ since
 $m \mid (a - b) \implies m \mid (b - a)$.

$\equiv \pmod{m}$ is **transitive**:

$$\forall a, b, c \in \mathbb{Z} \quad (a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$$

Indeed, $a \equiv b \pmod{m} \iff m \mid (a - b)$ and $b \equiv c \pmod{m} \iff m \mid (b - c)$.

$$\text{Hence, } a - c = \underbrace{(a - b)}_{\text{div. by } m} + \underbrace{(b - c)}_{\text{div. by } m}$$

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

$\equiv \pmod{m}$ is **symmetric**: $\forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ since
 $m \mid (a - b) \implies m \mid (b - a)$.

$\equiv \pmod{m}$ is **transitive**:

$\forall a, b, c \in \mathbb{Z} \quad (a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$

Indeed, $a \equiv b \pmod{m} \iff m \mid (a - b)$ and $b \equiv c \pmod{m} \iff m \mid (b - c)$.

Hence, $a - c = \underbrace{(a - b)}_{\text{div. by } m} + \underbrace{(b - c)}_{\text{div. by } m}$ is divisible by m .

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

$\equiv \pmod{m}$ is **symmetric**: $\forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ since
 $m \mid (a - b) \implies m \mid (b - a)$.

$\equiv \pmod{m}$ is **transitive**:

$$\forall a, b, c \in \mathbb{Z} \quad (a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$$

Indeed, $a \equiv b \pmod{m} \iff m \mid (a - b)$ and $b \equiv c \pmod{m} \iff m \mid (b - c)$.

Hence, $a - c = \underbrace{(a - b)}_{\text{div. by } m} + \underbrace{(b - c)}_{\text{div. by } m}$ is divisible by m .

Therefore, $a \equiv c \pmod{m}$.

Congruence modulo m is an equivalence relation

Theorem. Congruence modulo m is an equivalence relation on \mathbb{Z} .

Proof. $\equiv \pmod{m}$ is **reflexive**: $\forall a \in \mathbb{Z} \quad a \equiv a \pmod{m}$
since $m \mid (a - a)$.

$\equiv \pmod{m}$ is **symmetric**: $\forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ since
 $m \mid (a - b) \implies m \mid (b - a)$.

$\equiv \pmod{m}$ is **transitive**:

$$\forall a, b, c \in \mathbb{Z} \quad (a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$$

Indeed, $a \equiv b \pmod{m} \iff m \mid (a - b)$ and $b \equiv c \pmod{m} \iff m \mid (b - c)$.

Hence, $a - c = \underbrace{(a - b)}_{\text{div. by } m} + \underbrace{(b - c)}_{\text{div. by } m}$ is divisible by m .

Therefore, $a \equiv c \pmod{m}$. □

Equivalence classes modulo m

Equivalence classes modulo m

There are m equivalence classes modulo m :

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m :

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Example.

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Example. If $m = 3$,

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Example. If $m = 3$, then there are three classes:

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Example. If $m = 3$, then there are three classes: $[0], [1], [2]$.

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
 sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Example. If $m = 3$, then there are three classes: $[0], [1], [2]$.

$$[0] = \{3k \mid k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \dots\}$$

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
 sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Example. If $m = 3$, then there are three classes: $[0], [1], [2]$.

$$[0] = \{3k \mid k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \dots\}$$

$$[1] = \{1 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\}$$

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
 sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Example. If $m = 3$, then there are three classes: $[0], [1], [2]$.

$$[0] = \{3k \mid k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \dots\}$$

$$[1] = \{1 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\}$$

$$[2] = \{2 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
 sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Example. If $m = 3$, then there are three classes: $[0], [1], [2]$.

$$[0] = \{3k \mid k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \dots\}$$

$$[1] = \{1 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\}$$

$$[2] = \{2 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

Any element of a congruence class is called a **representative** for this class.

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
 sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Example. If $m = 3$, then there are three classes: $[0], [1], [2]$.

$$[0] = \{3k \mid k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \dots\}$$

$$[1] = \{1 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\}$$

$$[2] = \{2 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

Any element of a congruence class is called a **representative** for this class.

For example, 5 is a representative of class $[2]$ since $5 \in [2]$.

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
 sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Example. If $m = 3$, then there are three classes: $[0], [1], [2]$.

$$[0] = \{3k \mid k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \dots\}$$

$$[1] = \{1 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\}$$

$$[2] = \{2 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

Any element of a congruence class is called a **representative** for this class.

For example, 5 is a representative of class $[2]$ since $5 \in [2]$.

Any element of a congruence class may serve as a class representative.

Equivalence classes modulo m

There are m **equivalence classes** modulo m :

$$[0], [1], [2], \dots, [m-1]$$

They are called **congruence classes**.

Sometimes, they are denoted with index m : $[0]_m, [1]_m, [2]_m, \dots, [m-1]_m$,
 sometimes, like this: $0 \bmod m, 1 \bmod m, \dots$

Each class contains infinitely many integers.

Example. If $m = 3$, then there are three classes: $[0], [1], [2]$.

$$[0] = \{3k \mid k \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \dots\}$$

$$[1] = \{1 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\}$$

$$[2] = \{2 + 3k \mid k \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

Any element of a congruence class is called a **representative** for this class.

For example, 5 is a representative of class $[2]$ since $5 \in [2]$.

Any element of a congruence class may serve as a class representative.

For example, $[5] = [2]$.

Addition in \mathbb{Z}/m

The quotient set (the set of all congruence classes modulo m)

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes?

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows:

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

We have to prove that the addition is **well defined**,

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

We have to prove that the addition is **well defined**, that is,

the result of addition doesn't depend on the choice of class representatives.

Addition in \mathbb{Z}/m

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

We have to prove that the addition is **well defined**, that is,

the result of addition doesn't depend on the choice of class representatives.

Theorem 1. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$

Addition in \mathbb{Z}/m

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

We have to prove that the addition is **well defined**, that is,

the result of addition doesn't depend on the choice of class representatives.

Theorem 1. If $a \equiv a_1 \pmod{m}$ and

$$b \equiv b_1 \pmod{m}$$

then $a + b \equiv a_1 + b_1 \pmod{m}$

Addition in \mathbb{Z}/m

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

We have to prove that the addition is **well defined**, that is,

the result of addition doesn't depend on the choice of class representatives.

Theorem 1. If $a \equiv a_1 \pmod{m}$ and

$$b \equiv b_1 \pmod{m}$$

then $a + b \equiv a_1 + b_1 \pmod{m}$

Proof.

Addition in \mathbb{Z}/m

The quotient set (the set of all congruence classes modulo m) is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

We have to prove that the addition is **well defined**, that is,
 the result of addition doesn't depend on the choice of class representatives.

Theorem 1. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
 then $a + b \equiv a_1 + b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

Addition in \mathbb{Z}/m

The quotient set (the set of all congruence classes modulo m) is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

We have to prove that the addition is **well defined**, that is,
 the result of addition doesn't depend on the choice of class representatives.

Theorem 1. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
 then $a + b \equiv a_1 + b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

Addition in \mathbb{Z}/m

The quotient set (the set of all congruence classes modulo m) is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

We have to prove that the addition is **well defined**, that is,
 the result of addition doesn't depend on the choice of class representatives.

Theorem 1. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
 then $a + b \equiv a_1 + b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

Therefore, $(a + b) - (a_1 + b_1)$

The quotient set (the set of all congruence classes modulo m)

is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

We have to prove that the addition is **well defined**, that is,

the result of addition doesn't depend on the choice of class representatives.

Theorem 1. If $a \equiv a_1 \pmod{m}$ and

$$b \equiv b_1 \pmod{m}$$

then $a + b \equiv a_1 + b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

Therefore, $(a + b) - (a_1 + b_1) = (a - a_1) + (b - b_1)$

The quotient set (the set of all congruence classes modulo m) is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

We have to prove that the addition is **well defined**, that is,
the result of addition doesn't depend on the choice of class representatives.

Theorem 1. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
then $a + b \equiv a_1 + b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

Therefore, $(a + b) - (a_1 + b_1) = (a - a_1) + (b - b_1)$ is divisible by m .

Addition in \mathbb{Z}/m

The quotient set (the set of all congruence classes modulo m) is denoted by \mathbb{Z}/m :

$$\mathbb{Z}/m = \{[0], [1], [2], \dots, [m-1]\}$$

What can we do with congruence classes? Add, multiply, and raise to a power.

Define addition in \mathbb{Z}/m as follows: $[a] + [b] = [a + b]$

We have to prove that the addition is **well defined**, that is, the result of addition doesn't depend on the choice of class representatives.

Theorem 1. If $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$ then $a + b \equiv a_1 + b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

Therefore, $(a + b) - (a_1 + b_1) = (a - a_1) + (b - b_1)$ is divisible by m .

By this, $a + b \equiv a_1 + b_1 \pmod{m}$. □

Example: addition

Example: addition

Example.

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5 .

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution.

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5 .

Solution. $2018 \equiv$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5 .

Solution. $2018 \equiv -2 \pmod{5}$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5 .

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5 .

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5 .

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$ since $5 \mid 876543 - 3$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$ since $5 \mid 876543 - 3$

Overall,

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$ since $5 \mid 876543 - 3$

Overall,

$2018 + 123456789 + 876543 \equiv$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$ since $5 \mid 876543 - 3$

Overall,

$$2018 + 123456789 + 876543 \equiv -2 - 1 + 3 \equiv$$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$ since $5 \mid 876543 - 3$

Overall,

$2018 + 123456789 + 876543 \equiv -2 - 1 + 3 \equiv 0 \pmod{5}$.

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$ since $5 \mid 876543 - 3$

Overall,

$2018 + 123456789 + 876543 \equiv -2 - 1 + 3 \equiv 0 \pmod{5}$.

Answer: the remainder is 0.

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$ since $5 \mid 876543 - 3$

Overall,

$2018 + 123456789 + 876543 \equiv -2 - 1 + 3 \equiv 0 \pmod{5}$.

Answer: the remainder is 0.

Remark. The solution can be written as follows:

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$ since $5 \mid 876543 - 3$

Overall,

$2018 + 123456789 + 876543 \equiv -2 - 1 + 3 \equiv 0 \pmod{5}$.

Answer: the remainder is 0.

Remark. The solution can be written as follows:

$[2018 + 123456789 + 876543]_5 =$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$ since $5 \mid 876543 - 3$

Overall,

$2018 + 123456789 + 876543 \equiv -2 - 1 + 3 \equiv 0 \pmod{5}$.

Answer: the remainder is 0.

Remark. The solution can be written as follows:

$$[2018 + 123456789 + 876543]_5 = [2018]_5 + [123456789]_5 + [876543]_5$$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$ since $5 \mid 876543 - 3$

Overall,

$2018 + 123456789 + 876543 \equiv -2 - 1 + 3 \equiv 0 \pmod{5}$.

Answer: the remainder is 0.

Remark. The solution can be written as follows:

$$\begin{aligned} [2018 + 123456789 + 876543]_5 &= [2018]_5 + [123456789]_5 + [876543]_5 \\ &= [-2]_5 + [-1]_5 + [3]_5 = \end{aligned}$$

Example: addition

Example. Find the remainder when

$2018 + 123456789 + 876543$ is divided by 5.

Solution. $2018 \equiv -2 \pmod{5}$ since $5 \mid \underbrace{2018 - (-2)}_{2020}$

$123456789 \equiv -1 \pmod{5}$ since $5 \mid 123456789 - (-1)$

$876543 \equiv 3 \pmod{5}$ since $5 \mid 876543 - 3$

Overall,

$2018 + 123456789 + 876543 \equiv -2 - 1 + 3 \equiv 0 \pmod{5}$.

Answer: the remainder is 0.

Remark. The solution can be written as follows:

$$\begin{aligned} [2018 + 123456789 + 876543]_5 &= [2018]_5 + [123456789]_5 + [876543]_5 \\ &= [-2]_5 + [-1]_5 + [3]_5 = [-2 - 1 + 3]_5 = [0]_5. \end{aligned}$$

Multiplication in \mathbb{Z}/m

Multiplication in \mathbb{Z}/m

Define multiplication in \mathbb{Z}/m as follows:

Multiplication in \mathbb{Z}/m

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
on the choice of class representatives,

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
on the choice of class representatives, as the theorem below states:

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
on the choice of class representatives, as the theorem below states:

Theorem 2. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
on the choice of class representatives, as the theorem below states:

Theorem 2. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
then $ab \equiv a_1b_1 \pmod{m}$

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
on the choice of class representatives, as the theorem below states:

Theorem 2. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
then $ab \equiv a_1b_1 \pmod{m}$

Proof.

Multiplication in \mathbb{Z}/m

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
 on the choice of class representatives, as the theorem below states:

Theorem 2. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
 then $ab \equiv a_1b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

Multiplication in \mathbb{Z}/m

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
 on the choice of class representatives, as the theorem below states:

Theorem 2. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
 then $ab \equiv a_1b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
on the choice of class representatives, as the theorem below states:

Theorem 2. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
then $ab \equiv a_1b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

Therefore, $ab - a_1b_1$

Multiplication in \mathbb{Z}/m

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
 on the choice of class representatives, as the theorem below states:

Theorem 2. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
 then $ab \equiv a_1b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

Therefore, $ab - a_1b_1 = ab - ab_1 + ab_1 - a_1b_1$

Multiplication in \mathbb{Z}/m

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
 on the choice of class representatives, as the theorem below states:

Theorem 2. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
 then $ab \equiv a_1b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

Therefore, $ab - a_1b_1 = ab - ab_1 + ab_1 - a_1b_1 = \underbrace{a(b - b_1)}_{\text{div. by } m} + \underbrace{(a - a_1)b_1}_{\text{div. by } m}$

Multiplication in \mathbb{Z}/m

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
 on the choice of class representatives, as the theorem below states:

Theorem 2. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
 then $ab \equiv a_1b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

$$\text{Therefore, } ab - a_1b_1 = ab - ab_1 + ab_1 - a_1b_1 = \underbrace{a(b - b_1)}_{\text{div. by } m} + \underbrace{(a - a_1)b_1}_{\text{div. by } m}$$

is divisible by m .

Multiplication in \mathbb{Z}/m

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
 on the choice of class representatives, as the theorem below states:

Theorem 2. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
 then $ab \equiv a_1b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

Therefore, $ab - a_1b_1 = ab - ab_1 + ab_1 - a_1b_1 = a \underbrace{(b - b_1)}_{\text{div. by } m} + \underbrace{(a - a_1)}_{\text{div. by } m} b_1$

is divisible by m .

Hence, $ab \equiv a_1b_1 \pmod{m}$.

Multiplication in \mathbb{Z}/m

Define multiplication in \mathbb{Z}/m as follows: $[a] \cdot [b] = [ab]$

The result of multiplication doesn't depend
 on the choice of class representatives, as the theorem below states:

Theorem 2. If $a \equiv a_1 \pmod{m}$ and
 $b \equiv b_1 \pmod{m}$
 then $ab \equiv a_1b_1 \pmod{m}$

Proof. Let $a \equiv a_1 \pmod{m}$ and $b \equiv b_1 \pmod{m}$.

It means that both $a - a_1$ and $b - b_1$ are divisible by m .

Therefore, $ab - a_1b_1 = ab - ab_1 + ab_1 - a_1b_1 = a \underbrace{(b - b_1)}_{\text{div. by } m} + \underbrace{(a - a_1)}_{\text{div. by } m} b_1$

is divisible by m .

Hence, $ab \equiv a_1b_1 \pmod{m}$. □

Example: multiplication

Example: multiplication

Problem.

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3 .

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3 .

Solution.

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3 .

Solution. $235 \equiv 1 \pmod{3}$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3 .

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$$9923 \equiv 2 \pmod{3}$$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

$757 \equiv 1 \pmod{3}$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

$757 \equiv 1 \pmod{3}$ since $757 = 3 \cdot 252 + 1$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

$757 \equiv 1 \pmod{3}$ since $757 = 3 \cdot 252 + 1$

Therefore, $234 \cdot 9823 \cdot 757$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

$757 \equiv 1 \pmod{3}$ since $757 = 3 \cdot 252 + 1$

Therefore, $234 \cdot 9823 \cdot 757 \equiv 1 \cdot 2 \cdot 1$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

$757 \equiv 1 \pmod{3}$ since $757 = 3 \cdot 252 + 1$

Therefore, $234 \cdot 9823 \cdot 757 \equiv 1 \cdot 2 \cdot 1 \equiv 2 \pmod{3}$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

$757 \equiv 1 \pmod{3}$ since $757 = 3 \cdot 252 + 1$

Therefore, $234 \cdot 9823 \cdot 757 \equiv 1 \cdot 2 \cdot 1 \equiv 2 \pmod{3}$

Answer: the remainder is 2.

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

$757 \equiv 1 \pmod{3}$ since $757 = 3 \cdot 252 + 1$

Therefore, $234 \cdot 9823 \cdot 757 \equiv 1 \cdot 2 \cdot 1 \equiv 2 \pmod{3}$

Answer: the remainder is 2.

Remark. The solution can be written as follows:

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

$757 \equiv 1 \pmod{3}$ since $757 = 3 \cdot 252 + 1$

Therefore, $234 \cdot 9823 \cdot 757 \equiv 1 \cdot 2 \cdot 1 \equiv 2 \pmod{3}$

Answer: the remainder is 2.

Remark. The solution can be written as follows:

$$[235 \cdot 9823 \cdot 757]_3 =$$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

$757 \equiv 1 \pmod{3}$ since $757 = 3 \cdot 252 + 1$

Therefore, $234 \cdot 9823 \cdot 757 \equiv 1 \cdot 2 \cdot 1 \equiv 2 \pmod{3}$

Answer: the remainder is 2.

Remark. The solution can be written as follows:

$$[235 \cdot 9823 \cdot 757]_3 = [235]_3 \cdot [9823]_3 \cdot [757]_3 =$$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

$757 \equiv 1 \pmod{3}$ since $757 = 3 \cdot 252 + 1$

Therefore, $234 \cdot 9823 \cdot 757 \equiv 1 \cdot 2 \cdot 1 \equiv 2 \pmod{3}$

Answer: the remainder is 2.

Remark. The solution can be written as follows:

$$[235 \cdot 9823 \cdot 757]_3 = [235]_3 \cdot [9823]_3 \cdot [757]_3 = [1]_2 \cdot [2]_3 \cdot [1]_3 =$$

Example: multiplication

Problem. Find the remainder when $235 \cdot 9823 \cdot 757$ is divided by 3.

Solution. $235 \equiv 1 \pmod{3}$ since $235 = 3 \cdot 78 + 1$

$9923 \equiv 2 \pmod{3}$ since $9923 = 3 \cdot 3307 + 2$

$757 \equiv 1 \pmod{3}$ since $757 = 3 \cdot 252 + 1$

Therefore, $234 \cdot 9823 \cdot 757 \equiv 1 \cdot 2 \cdot 1 \equiv 2 \pmod{3}$

Answer: the remainder is 2.

Remark. The solution can be written as follows:

$$[235 \cdot 9823 \cdot 757]_3 = [235]_3 \cdot [9823]_3 \cdot [757]_3 = [1]_3 \cdot [2]_3 \cdot [1]_3 = [1 \cdot 2 \cdot 1]_3 = [2]_3.$$

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

$$[a]^n = [a^n], \quad n \in \mathbb{N}$$

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

The result doesn't depend
on the choice of the class representative,

$$[a]^n = [a^n], \quad n \in \mathbb{N}$$

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

$$[a]^n = [a^n], \quad n \in \mathbb{N}$$

The result doesn't depend

on the choice of the class representative, as the theorem below states:

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

$$[a]^n = [a^n], \quad n \in \mathbb{N}$$

The result doesn't depend

on the choice of the class representative, as the theorem below states:

Theorem 3. If $a \equiv b \pmod{m}$

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

$$[a]^n = [a^n], \quad n \in \mathbb{N}$$

The result doesn't depend

on the choice of the class representative, as the theorem below states:

Theorem 3. If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$.

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

$$[a]^n = [a^n], \quad n \in \mathbb{N}$$

The result doesn't depend

on the choice of the class representative, as the theorem below states:

Theorem 3. If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$.

Proof.

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

$$[a]^n = [a^n], \quad n \in \mathbb{N}$$

The result doesn't depend

on the choice of the class representative, as the theorem below states:

Theorem 3. If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$.

Proof. Let $a \equiv b \pmod{m}$. It means that $m \mid a - b$.

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

$$[a]^n = [a^n], \quad n \in \mathbb{N}$$

The result doesn't depend

on the choice of the class representative, as the theorem below states:

Theorem 3. If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$.

Proof. Let $a \equiv b \pmod{m}$. It means that $m \mid a - b$.

Then

$$a^n - b^n =$$

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

$$[a]^n = [a^n], \quad n \in \mathbb{N}$$

The result doesn't depend

on the choice of the class representative, as the theorem below states:

Theorem 3. If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$.

Proof. Let $a \equiv b \pmod{m}$. It means that $m \mid a - b$.

Then

$$a^n - b^n = \underbrace{(a - b)}_{\text{div. by } m} (a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$$

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

$$[a]^n = [a^n], \quad n \in \mathbb{N}$$

The result doesn't depend

on the choice of the class representative, as the theorem below states:

Theorem 3. If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$.

Proof. Let $a \equiv b \pmod{m}$. It means that $m \mid a - b$.

Then

$$a^n - b^n = \underbrace{(a - b)}_{\text{div. by } m} (a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1}) \text{ is divisible by } m.$$

Powers in \mathbb{Z}/m

Define a positive integer **power** of an element in \mathbb{Z}/m as follows:

$$[a]^n = [a^n], \quad n \in \mathbb{N}$$

The result doesn't depend

on the choice of the class representative, as the theorem below states:

Theorem 3. If $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$.

Proof. Let $a \equiv b \pmod{m}$. It means that $m \mid a - b$.

Then

$$a^n - b^n = \underbrace{(a - b)}_{\text{div. by } m} (a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1}) \text{ is divisible by } m.$$

Therefore, $a^n \equiv b^n \pmod{m}$. □

Theorem.

Theorem. \mathbb{Z}/m with operations of addition and multiplication defined by
 $[a] + [b] = [a + b]$ and $[a][b] = [ab]$

Theorem. \mathbb{Z}/m with operations of addition and multiplication defined by $[a] + [b] = [a + b]$ and $[a][b] = [ab]$ is a commutative ring with unity.

Theorem. \mathbb{Z}/m with operations of addition and multiplication defined by $[a] + [b] = [a + b]$ and $[a][b] = [ab]$ is a commutative ring with unity.

It is called the **ring of congruence classes modulo m**
or **ring of integers modulo m** .

Theorem. \mathbb{Z}/m with operations of addition and multiplication defined by $[a] + [b] = [a + b]$ and $[a][b] = [ab]$ is a commutative ring with unity.

It is called the **ring of congruence classes modulo m** or **ring of integers modulo m** .

Proof

Theorem. \mathbb{Z}/m with operations of addition and multiplication defined by $[a] + [b] = [a + b]$ and $[a][b] = [ab]$ is a commutative ring with unity.

It is called the **ring of congruence classes modulo m** or **ring of integers modulo m** .

Proof is by checking the ring axioms.

Theorem. \mathbb{Z}/m with operations of addition and multiplication defined by $[a] + [b] = [a + b]$ and $[a][b] = [ab]$ is a commutative ring with unity.

It is called the **ring of congruence classes modulo m**

or **ring of integers modulo m** .

Proof is by checking the ring axioms. For any $a, b, c \in \mathbb{Z}/m$

1. $a + b \in \mathbb{Z}/m$
2. $a \cdot b \in \mathbb{Z}/m$
3. $(a + b) + c = a + (b + c)$
4. $a + b = b + a$
5. $\exists 0 \in \mathbb{Z}/m \quad a + 0 = a$
6. $\exists -a \in \mathbb{Z}/m \quad a + (-a) = 0$
7. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$
 - $a \cdot b = b \cdot a$
 - $\exists 1 \in \mathbb{Z}/m \quad 1 \cdot a = a \cdot 1 = a$

Modular arithmetic for divisibility

MAT 250
Lecture 10
Modular Arithmetic

Problem 1.

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution.

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$$7^n + 5 \equiv 1 + 5$$

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$$7^n + 5 \equiv 1 + 5 \equiv 6$$

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}.$$

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 2.

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 2. Prove that $7^{2n+1} + 17^n$ is divisible by 8 for all $n = 0, 1, 2, \dots$.

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 2. Prove that $7^{2n+1} + 17^n$ is divisible by 8 for all $n = 0, 1, 2, \dots$.

Solution.

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 2. Prove that $7^{2n+1} + 17^n$ is divisible by 8 for all $n = 0, 1, 2, \dots$.

Solution. $7 \equiv -1 \pmod{8}$

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 2. Prove that $7^{2n+1} + 17^n$ is divisible by 8 for all $n = 0, 1, 2, \dots$.

Solution. $7 \equiv -1 \pmod{8}$

$$7^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{8}$$

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 2. Prove that $7^{2n+1} + 17^n$ is divisible by 8 for all $n = 0, 1, 2, \dots$.

Solution. $7 \equiv -1 \pmod{8}$

$$7^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{8}$$

$$17 \equiv 1 \pmod{8}$$

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 2. Prove that $7^{2n+1} + 17^n$ is divisible by 8 for all $n = 0, 1, 2, \dots$.

Solution. $7 \equiv -1 \pmod{8}$

$$7^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{8}$$

$$17 \equiv 1 \pmod{8}$$

$$17^n \equiv 1^n$$

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 2. Prove that $7^{2n+1} + 17^n$ is divisible by 8 for all $n = 0, 1, 2, \dots$.

Solution. $7 \equiv -1 \pmod{8}$

$$7^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{8}$$

$$17 \equiv 1 \pmod{8}$$

$$17^n \equiv 1^n \equiv 1 \pmod{8}$$

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 2. Prove that $7^{2n+1} + 17^n$ is divisible by 8 for all $n = 0, 1, 2, \dots$.

Solution. $7 \equiv -1 \pmod{8}$

$$7^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{8}$$

$$17 \equiv 1 \pmod{8}$$

$$17^n \equiv 1^n \equiv 1 \pmod{8}$$

Therefore, $7^{2n+1} + 17^n \equiv -1 + 1$

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 2. Prove that $7^{2n+1} + 17^n$ is divisible by 8 for all $n = 0, 1, 2, \dots$.

Solution. $7 \equiv -1 \pmod{8}$

$$7^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{8}$$

$$17 \equiv 1 \pmod{8}$$

$$17^n \equiv 1^n \equiv 1 \pmod{8}$$

Therefore, $7^{2n+1} + 17^n \equiv -1 + 1 \equiv 0 \pmod{8}$,

Problem 1. Prove that $7^n + 5$ is divisible by 3 for any $n \in \mathbb{N}$.

Solution. $7 \equiv 1 \pmod{3}$

$$7^n \equiv \underbrace{1^n}_1 \pmod{3} \quad \text{for any } n \in \mathbb{N}$$

$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod{3}$. Therefore, $3 \mid 7^n + 5$ for any $n \in \mathbb{N}$.

Problem 2. Prove that $7^{2n+1} + 17^n$ is divisible by 8 for all $n = 0, 1, 2, \dots$.

Solution. $7 \equiv -1 \pmod{8}$

$$7^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{8}$$

$$17 \equiv 1 \pmod{8}$$

$$17^n \equiv 1^n \equiv 1 \pmod{8}$$

Therefore, $7^{2n+1} + 17^n \equiv -1 + 1 \equiv 0 \pmod{8}$, as required. □

Problem 3.

Problem 3. Find the last digit of 2022^{2023} .

Problem 3. Find the last digit of 2022^{2023} .

Solution.

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

$$2^6 \equiv 4 \pmod{10}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

$$2^6 \equiv 4 \pmod{10}$$

.....

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

$$2^6 \equiv 4 \pmod{10}$$

.....



Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

$$2^6 \equiv 4 \pmod{10}$$

.....

cycle of length 4

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

$$2^6 \equiv 4 \pmod{10}$$

.....



cycle of length 4

$$2023 \equiv ? \pmod{4}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

$$2^6 \equiv 4 \pmod{10}$$

.....



cycle of length 4

$$2023 \equiv ? \pmod{4}$$

$$2023 \equiv 3 \pmod{4}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

$$2^6 \equiv 4 \pmod{10}$$

.....



cycle of length 4

$$2023 \equiv ? \pmod{4}$$

$$2023 \equiv 3 \pmod{4}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

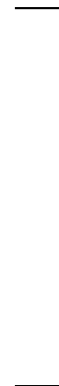
$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

$$2^6 \equiv 4 \pmod{10}$$

.....



cycle of length 4

$$2023 \equiv ? \pmod{4}$$

$$2023 \equiv 3 \pmod{4}$$

$$2^{2023} \equiv 8 \pmod{10}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

$$2^6 \equiv 4 \pmod{10}$$

.....



cycle of length 4

$$2023 \equiv ? \pmod{4}$$

$$2023 \equiv 3 \pmod{4}$$

$$2^{2023} \equiv 8 \pmod{10}$$

$$2022^{2023} \equiv 8 \pmod{10}$$

Problem 3. Find the last digit of 2022^{2023} .

Solution. $2022^{2023} \equiv ? \pmod{10}$

$$2022 \equiv 2 \pmod{10} \implies 2022^{2023} \equiv 2^{2023} \pmod{10}$$

$$2^{2023} \equiv ? \pmod{10}$$

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10}$$

$$2^5 \equiv 2 \pmod{10}$$

$$2^6 \equiv 4 \pmod{10}$$

.....



cycle of length 4

$$2023 \equiv ? \pmod{4}$$

$$2023 \equiv 3 \pmod{4}$$

$$2^{2023} \equiv 8 \pmod{10}$$

$$2022^{2023} \equiv 8 \pmod{10}$$

Answer:

the last digit of 2022^{2023} is 8.

Diophantine equations

MAT 250
Lecture 10
Modular Arithmetic

Problem 3.

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution.

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

$$[x^2]_3 = 2$$

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

$$[x^2]_3 = 2$$

$x \pmod 3$	$x^2 \pmod 3$
0	0
1	1
-1	1

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

$$[x^2]_3 = 2$$

$x \pmod 3$	$x^2 \pmod 3$
0	0
1	1
-1	1

So $x^2 \equiv 0$ or $1 \pmod 3$,

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

$$[x^2]_3 = 2$$

$x \pmod 3$	$x^2 \pmod 3$
0	0
1	1
-1	1

So $x^2 \equiv 0$ or $1 \pmod 3$, and $x^2 \not\equiv 2 \pmod 3$.

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

$$[x^2]_3 = 2$$

$x \pmod 3$	$x^2 \pmod 3$
0	0
1	1
-1	1

So $x^2 \equiv 0$ or $1 \pmod 3$, and $x^2 \not\equiv 2 \pmod 3$.

Therefore, the original equation has **no** integer solutions.

As we know, an equivalence relation on a set X

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m ,

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names:

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
 projection map
 reduction modulo m ,

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
 projection map
 reduction modulo m ,
 quotient map.

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m ,
quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m ,
quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:
 $f(a + b) = f(a) + f(b)$

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
 projection map
 reduction modulo m ,
 quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:
 $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m ,
quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:
 $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in \mathbb{Z}$.

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
 projection map
 reduction modulo m ,
 quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:
 $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in \mathbb{Z}$.

Indeed, $f(a + b)$

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
 projection map
 reduction modulo m ,
 quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:
 $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in \mathbb{Z}$.

Indeed, $f(a + b) = [a + b]$

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
 projection map
 reduction modulo m ,
 quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in \mathbb{Z}.$$

$$\text{Indeed, } f(a + b) = [a + b] = [a] + [b]$$

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
 projection map
 reduction modulo m ,
 quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in \mathbb{Z}.$$

$$\text{Indeed, } f(a + b) = [a + b] = [a] + [b] = f(a) + f(b)$$

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
 projection map
 reduction modulo m ,
 quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:
 $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in \mathbb{Z}$.

Indeed, $f(a + b) = [a + b] = [a] + [b] = f(a) + f(b)$ and
 $f(ab) = [ab] = [a][b] = f(a)f(b)$

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
 projection map
 reduction modulo m ,
 quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:
 $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in \mathbb{Z}$.

Indeed, $f(a + b) = [a + b] = [a] + [b] = f(a) + f(b)$ and
 $f(ab) = [ab]$

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
 projection map
 reduction modulo m ,
 quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in \mathbb{Z}.$$

Indeed, $f(a + b) = [a + b] = [a] + [b] = f(a) + f(b)$ and
 $f(ab) = [ab] = [a][b]$

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set X/\sim and the quotient map $X \rightarrow X/\sim, x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m , then the quotient map is $\mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$.

This map has many names: canonical projection,
 projection map
 reduction modulo m ,
 quotient map.

This map $\mathbb{Z} \rightarrow \mathbb{Z}/m$ possesses the following two properties:

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in \mathbb{Z}.$$

Indeed, $f(a + b) = [a + b] = [a] + [b] = f(a) + f(b)$ and
 $f(ab) = [ab] = [a][b] = f(a)f(b)$.

Definition. Let R, S be rings.

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism**

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b)$$

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b)$$

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark.

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

↑ ↑
addition in R addition in S

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{addition in } R & & \text{addition in } S \end{array}$$

$$\begin{array}{ccc} f(ab) = f(a)f(b) \\ \uparrow \quad \quad \uparrow \\ \text{multiplication in } R & & \text{multiplication in } S \end{array}$$

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{addition in } R & & \text{addition in } S \end{array}$$

$$f(ab) = f(a)f(b)$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{multiplication in } R & & \text{multiplication in } S \end{array}$$

Theorem.

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{addition in } R & & \text{addition in } S \end{array}$$

$$f(ab) = f(a)f(b)$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{multiplication in } R & & \text{multiplication in } S \end{array}$$

Theorem. The canonical projection $\mathbb{Z} \rightarrow \mathbb{Z}/m$

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{addition in } R & & \text{addition in } S \end{array}$$

$$f(ab) = f(a)f(b)$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{multiplication in } R & & \text{multiplication in } S \end{array}$$

Theorem. The canonical projection $\mathbb{Z} \rightarrow \mathbb{Z}/m$ is a ring homomorphism.

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{addition in } R & & \text{addition in } S \end{array}$$

$$f(ab) = f(a)f(b)$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{multiplication in } R & & \text{multiplication in } S \end{array}$$

Theorem. The canonical projection $\mathbb{Z} \rightarrow \mathbb{Z}/m$ is a ring homomorphism.

Proof.

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{addition in } R & & \text{addition in } S \end{array}$$

$$f(ab) = f(a)f(b)$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{multiplication in } R & & \text{multiplication in } S \end{array}$$

Theorem. The canonical projection $\mathbb{Z} \rightarrow \mathbb{Z}/m$ is a ring homomorphism.

Proof. We already know that both \mathbb{Z} and \mathbb{Z}/m are rings.

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

↑ ↑
addition in R addition in S

$$f(ab) = f(a)f(b)$$

↑ ↑
multiplication in R multiplication in S

Theorem. The canonical projection $\mathbb{Z} \rightarrow \mathbb{Z}/m$ is a ring homomorphism.

Proof. We already know that both \mathbb{Z} and \mathbb{Z}/m are rings.

We proved also that the canonical projection $f : \mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$ preserves the ring operations:

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{addition in } R & & \text{addition in } S \end{array}$$

$$f(ab) = f(a)f(b)$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{multiplication in } R & & \text{multiplication in } S \end{array}$$

Theorem. The canonical projection $\mathbb{Z} \rightarrow \mathbb{Z}/m$ is a ring homomorphism.

Proof. We already know that both \mathbb{Z} and \mathbb{Z}/m are rings.

We proved also that the canonical projection $f : \mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$

preserves the ring operations:

$$f(a + b) = f(a) + f(b)$$

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{addition in } R & & \text{addition in } S \end{array}$$

$$f(ab) = f(a)f(b)$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{multiplication in } R & & \text{multiplication in } S \end{array}$$

Theorem. The canonical projection $\mathbb{Z} \rightarrow \mathbb{Z}/m$ is a ring homomorphism.

Proof. We already know that both \mathbb{Z} and \mathbb{Z}/m are rings.

We proved also that the canonical projection $f : \mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$ preserves the ring operations:

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b)$$

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

↑ ↑
addition in R addition in S

$$f(ab) = f(a)f(b)$$

↑ ↑
multiplication in R multiplication in S

Theorem. The canonical projection $\mathbb{Z} \rightarrow \mathbb{Z}/m$ is a ring homomorphism.

Proof. We already know that both \mathbb{Z} and \mathbb{Z}/m are rings.

We proved also that the canonical projection $f : \mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$

preserves the ring operations:

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in \mathbb{Z}.$$

Definition. Let R, S be rings.

A map $f : R \rightarrow S$ is called **ring homomorphism** if

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in R.$$

Remark. $f(a + b) = f(a) + f(b)$.

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{addition in } R & & \text{addition in } S \end{array}$$

$$f(ab) = f(a)f(b)$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \text{multiplication in } R & & \text{multiplication in } S \end{array}$$

Theorem. The canonical projection $\mathbb{Z} \rightarrow \mathbb{Z}/m$ is a ring homomorphism.

Proof. We already know that both \mathbb{Z} and \mathbb{Z}/m are rings.

We proved also that the canonical projection $f : \mathbb{Z} \rightarrow \mathbb{Z}/m, x \mapsto x \bmod m$

preserves the ring operations:

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for any } a, b \in \mathbb{Z}.$$

Therefore, f is a ring homomorphism. \square

Problem.

Problem. Is it true that

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution.

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,
then reduction modulo 9

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,
then reduction modulo 9 (common modulus for such a control)

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,
then reduction modulo 9 (common modulus for such a control)
will result in

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,
then reduction modulo 9 (common modulus for such a control)
will result in $4 \cdot 6 - 7 = 0$.

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

then reduction modulo 9 (common modulus for such a control)
will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)

But $24 - 7 \neq 0$.

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

then reduction modulo 9 (common modulus for such a control)
will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)

But $24 - 7 \neq 0$.

Therefore, since the identity doesn't hold true in $\mathbb{Z}/9$,

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

then reduction modulo 9 (common modulus for such a control)
will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)

But $24 - 7 \neq 0$.

Therefore, since the identity doesn't hold true in $\mathbb{Z}/9$, it neither holds true in \mathbb{Z} .

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

then reduction modulo 9 (common modulus for such a control)
will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)

But $24 - 7 \neq 0$.

Therefore, since the identity doesn't hold true in $\mathbb{Z}/9$, it neither holds true in \mathbb{Z} .

Answer. $74,218 \cdot 21,363 - 81,835 \neq 1,585,447,299$.

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

then reduction modulo 9 (common modulus for such a control)
will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)

But $24 - 7 \neq 0$.

Therefore, since the identity doesn't hold true in $\mathbb{Z}/9$, it neither holds true in \mathbb{Z} .

Answer. $74,218 \cdot 21,363 - 81,835 \neq 1,585,447,299$.

Remark. $74,218 \cdot 21,363 - 81,835 = 1,585,437,299$.

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

then reduction modulo 9 (common modulus for such a control)
will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)

But $24 - 7 \neq 0$.

Therefore, since the identity doesn't hold true in $\mathbb{Z}/9$, it neither holds true in \mathbb{Z} .

Answer. $74,218 \cdot 21,363 - 81,835 \neq 1,585,447,299$.

Remark. $74,218 \cdot 21,363 - 81,835 = 1,585,437,299$.

Control question.

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

then reduction modulo 9 (common modulus for such a control)
will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)

But $24 - 7 \neq 0$.

Therefore, since the identity doesn't hold true in $\mathbb{Z}/9$, it neither holds true in \mathbb{Z} .

Answer. $74,218 \cdot 21,363 - 81,835 \neq 1,585,447,299$.

Remark. $74,218 \cdot 21,363 - 81,835 = 1,585,437,299$.

Control question. If the equality under consideration

Control of calculations

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

then reduction modulo 9 (common modulus for such a control)
 will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)

But $24 - 7 \neq 0$.

Therefore, since the identity doesn't hold true in $\mathbb{Z}/9$, it neither holds true in \mathbb{Z} .

Answer. $74,218 \cdot 21,363 - 81,835 \neq 1,585,447,299$.

Remark. $74,218 \cdot 21,363 - 81,835 = 1,585,437,299$.

Control question. If the equality under consideration
survives the reduction modulo 9,

Control of calculations

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

then reduction modulo 9 (common modulus for such a control)
 will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)

But $24 - 7 \neq 0$.

Therefore, since the identity doesn't hold true in $\mathbb{Z}/9$, it neither holds true in \mathbb{Z} .

Answer. $74,218 \cdot 21,363 - 81,835 \neq 1,585,447,299$.

Remark. $74,218 \cdot 21,363 - 81,835 = 1,585,437,299$.

Control question. If the equality under consideration survives the reduction modulo 9, does it mean that the original equality is true?

Control of calculations

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,
 then reduction modulo 9 (common modulus for such a control)
 will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)
 But $24 - 7 \neq 0$.

Therefore, since the identity doesn't hold true in $\mathbb{Z}/9$, it neither holds true in \mathbb{Z} .

Answer. $74,218 \cdot 21,363 - 81,835 \neq 1,585,447,299$.

Remark. $74,218 \cdot 21,363 - 81,835 = 1,585,437,299$.

Control question. If the equality under consideration survives the reduction modulo 9, does it mean that the original equality is true?

No:

Control of calculations

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

then reduction modulo 9 (common modulus for such a control)
 will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)

But $24 - 7 \neq 0$.

Therefore, since the identity doesn't hold true in $\mathbb{Z}/9$, it neither holds true in \mathbb{Z} .

Answer. $74,218 \cdot 21,363 - 81,835 \neq 1,585,447,299$.

Remark. $74,218 \cdot 21,363 - 81,835 = 1,585,437,299$.

Control question. If the equality under consideration survives the reduction modulo 9, does it mean that the original equality is true?

No: $2 + 7 \stackrel{?}{=} 18$

Control of calculations

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution. If the equality is correct,

then reduction modulo 9 (common modulus for such a control)
 will result in $4 \cdot 6 - 7 = 0$.

(As we remember, a number is congruent modulo 9 to the sum of its digits.)

But $24 - 7 \neq 0$.

Therefore, since the identity doesn't hold true in $\mathbb{Z}/9$, it neither holds true in \mathbb{Z} .

Answer. $74,218 \cdot 21,363 - 81,835 \neq 1,585,447,299$.

Remark. $74,218 \cdot 21,363 - 81,835 = 1,585,437,299$.

Control question. If the equality under consideration survives the reduction modulo 9, does it mean that the original equality is true?

No: $2 + 7 \stackrel{?}{=} 18 \xrightarrow{\text{mod } 9} 0 = 0$.

Caution

Caution

Example 1.

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4)$$

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3$$

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3.$$

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) =$$

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4)$$

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3$$

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3$$

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2.

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$

Caution

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$ by $[x]_6 \mapsto [x^2]_3$.

Caution

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Caution

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Solution.

Caution

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Solution. We have to check if the map gives the same value

Caution

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Solution. We have to check if the map gives the same value regardless of which representative is chosen.

Caution

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Solution. We have to check if the map gives the same value

regardless of which representative is chosen.

Let $x_1 \equiv x_2 \pmod{6}$.

Caution

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Solution. We have to check if the map gives the same value regardless of which representative is chosen.

Let $x_1 \equiv x_2 \pmod{6}$. We have to check if $x_1^2 \equiv x_2^2 \pmod{3}$.

Caution

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Solution. We have to check if the map gives the same value regardless of which representative is chosen.

Let $x_1 \equiv x_2 \pmod{6}$. We have to check if $x_1^2 \equiv x_2^2 \pmod{3}$.

If $x_1 \equiv x_2 \pmod{6}$, then $x_1 - x_2$ is divisible by 6, and so by 3.

Caution

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Solution. We have to check if the map gives the same value regardless of which representative is chosen.

Let $x_1 \equiv x_2 \pmod{6}$. We have to check if $x_1^2 \equiv x_2^2 \pmod{3}$.

If $x_1 \equiv x_2 \pmod{6}$, then $x_1 - x_2$ is divisible by 6, and so by 3. In this case

$$x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2)$$

Caution

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Solution. We have to check if the map gives the same value regardless of which representative is chosen.

Let $x_1 \equiv x_2 \pmod{6}$. We have to check if $x_1^2 \equiv x_2^2 \pmod{3}$.

If $x_1 \equiv x_2 \pmod{6}$, then $x_1 - x_2$ is divisible by 6, and so by 3. In this case $x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2)$ is divisible by 3. Therefore, $x_1^2 \equiv x_2^2 \pmod{3}$,

Caution

Example 1. Define a map $f : \mathbb{Z}/4 \rightarrow \mathbb{Z}/3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$$f([0]_4) = [0^2]_3 = [0]_3. \text{ But}$$

$$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3.$$

The element $[0]_4$ has two different images!

Therefore, the formula $f([x]_4) = [x^2]_3$ doesn't define a map.

We say that the map is **not well-defined**.

Example 2. Define a map $f : \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Solution. We have to check if the map gives the same value regardless of which representative is chosen.

Let $x_1 \equiv x_2 \pmod{6}$. We have to check if $x_1^2 \equiv x_2^2 \pmod{3}$.

If $x_1 \equiv x_2 \pmod{6}$, then $x_1 - x_2$ is divisible by 6, and so by 3. In this case

$x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2)$ is divisible by 3. Therefore, $x_1^2 \equiv x_2^2 \pmod{3}$,
and the map is well defined.

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$.

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. □

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. □

Let R be a commutative ring.

Its element a is called **invertible**, $\exists b \in R$ such that $ab = 1$.

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. □

Let R be a commutative ring.

Its element a is called **invertible**, $\exists b \in R$ such that $ab = 1$.

If $a \in R$ is invertible, then there is only one $b \in R$ such that $ab = 1$.

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. □

Let R be a commutative ring.

Its element a is called **invertible**, $\exists b \in R$ such that $ab = 1$.

If $a \in R$ is invertible, then there is only one $b \in R$ such that $ab = 1$,

this element is called (multiplicative) **inverse** to a and denoted by a^{-1} .

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. □

Let R be a commutative ring.

Its element a is called **invertible**, $\exists b \in R$ such that $ab = 1$.

If $a \in R$ is invertible, then there is only one $b \in R$ such that $ab = 1$,

this element is called (multiplicative) **inverse** to a and denoted by a^{-1} .

An invertible element cannot be a zero-divisor.

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. □

Let R be a commutative ring.

Its element a is called **invertible**, $\exists b \in R$ such that $ab = 1$.

If $a \in R$ is invertible, then there is only one $b \in R$ such that $ab = 1$,

this element is called (multiplicative) **inverse** to a and denoted by a^{-1} .

An invertible element cannot be a zero-divisor. Indeed,

if a is invertible and $ab = 0$, then

$$a^{-1}ab = (a^{-1}a)b = 1 \cdot b = b.$$

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. \square

Let R be a commutative ring.

Its element a is called **invertible**, $\exists b \in R$ such that $ab = 1$.

If $a \in R$ is invertible, then there is only one $b \in R$ such that $ab = 1$,

this element is called (multiplicative) **inverse** to a and denoted by a^{-1} .

An invertible element cannot be a zero-divisor. Indeed,

if a is invertible and $ab = 0$, then

$$0 = a^{-1} \cdot 0 = a^{-1}(ab) = a^{-1}ab = (a^{-1}a)b = 1 \cdot b = b.$$

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. \square

Let R be a commutative ring.

Its element a is called **invertible**, $\exists b \in R$ such that $ab = 1$.

If $a \in R$ is invertible, then there is only one $b \in R$ such that $ab = 1$,

this element is called (multiplicative) **inverse** to a and denoted by a^{-1} .

An invertible element cannot be a zero-divisor. Indeed,

if a is invertible and $ab = 0$, then

$$0 = a^{-1} \cdot 0 = a^{-1}(ab) = a^{-1}ab = (a^{-1}a)b = 1 \cdot b = b.$$

A commutative ring in which any non-zero element is invertible is called a **field**.

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. \square

Let R be a commutative ring.

Its element a is called **invertible**, $\exists b \in R$ such that $ab = 1$.

If $a \in R$ is invertible, then there is only one $b \in R$ such that $ab = 1$,

this element is called (multiplicative) **inverse** to a and denoted by a^{-1} .

An invertible element cannot be a zero-divisor. Indeed,

if a is invertible and $ab = 0$, then

$$0 = a^{-1} \cdot 0 = a^{-1}(ab) = a^{-1}ab = (a^{-1}a)b = 1 \cdot b = b.$$

A commutative ring in which any non-zero element is invertible is called a **field**.

Examples. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. \square

Let R be a commutative ring.

Its element a is called **invertible**, $\exists b \in R$ such that $ab = 1$.

If $a \in R$ is invertible, then there is only one $b \in R$ such that $ab = 1$,

this element is called (multiplicative) **inverse** to a and denoted by a^{-1} .

An invertible element cannot be a zero-divisor. Indeed,

if a is invertible and $ab = 0$, then

$$0 = a^{-1} \cdot 0 = a^{-1}(ab) = a^{-1}ab = (a^{-1}a)b = 1 \cdot b = b.$$

A commutative ring in which any non-zero element is invertible is called a **field**.

Examples. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. $\mathbb{Z}/6$ is not a field.

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. \square

Let R be a commutative ring.

Its element a is called **invertible**, $\exists b \in R$ such that $ab = 1$.

If $a \in R$ is invertible, then there is only one $b \in R$ such that $ab = 1$,

this element is called (multiplicative) **inverse** to a and denoted by a^{-1} .

An invertible element cannot be a zero-divisor. Indeed,

if a is invertible and $ab = 0$, then

$$0 = a^{-1} \cdot 0 = a^{-1}(ab) = a^{-1}ab = (a^{-1}a)b = 1 \cdot b = b.$$

A commutative ring in which any non-zero element is invertible is called a **field**.

Examples. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. $\mathbb{Z}/6$ is not a field. $\mathbb{Z}/2$ and $\mathbb{Z}/3$ are fields.

Zero-divisors

Let R be a commutative ring.

Its element $a \neq 0$ is called a **zero-divisor** if $\exists b \in R, b \neq 0$ such that $ab = 0$.

For which m the ring \mathbb{Z}/m does have zero-divisors?

Theorem. If $m \in \mathbb{Z}$ is not prime, then \mathbb{Z}/m has zero-divisors.

Proof. Let m be non-prime, then $m = ab$ with $0 < a, b < m$.

Then $[a]_m$ is a zero-divisor. Indeed, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. □

Let R be a commutative ring.

Its element a is called **invertible**, $\exists b \in R$ such that $ab = 1$.

If $a \in R$ is invertible, then there is only one $b \in R$ such that $ab = 1$,
this element is called (multiplicative) **inverse** to a and denoted by a^{-1} .

An invertible element cannot be a zero-divisor. Indeed,

if a is invertible and $ab = 0$, then

$$0 = a^{-1} \cdot 0 = a^{-1}(ab) = a^{-1}ab = (a^{-1}a)b = 1 \cdot b = b.$$

A commutative ring in which any non-zero element is invertible is called a **field**.

Examples. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. $\mathbb{Z}/6$ is not a field. $\mathbb{Z}/2$ and $\mathbb{Z}/3$ are fields.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Why are fields remarkable?

Why are fields remarkable?

In a field we can divide by any non-zero element.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Why are fields remarkable?

In a field we can divide by any non-zero element.

Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.

And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Therefore it cannot be a field.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.
Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.
Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Any non-zero element of \mathbb{Z}/m is represented as $[a]$ with $0 < a < m$.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Any non-zero element of \mathbb{Z}/m is represented as $[a]$ with $0 < a < m$.

Since $[a]$ is not a zero-divisor, multiplication by $[a]$ defines a map

$$\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\}.$$

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Any non-zero element of \mathbb{Z}/m is represented as $[a]$ with $0 < a < m$.

Since $[a]$ is not a zero-divisor, multiplication by $[a]$ defines a map

$\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\}$. This map is injective.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Any non-zero element of \mathbb{Z}/m is represented as $[a]$ with $0 < a < m$.

Since $[a]$ is not a zero-divisor, multiplication by $[a]$ defines a map

$\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\}$. This map is injective.

Indeed, let $b, c \in \mathbb{Z}/m \setminus \{0\}$ and $b \cdot [a] = c \cdot [a]$.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Any non-zero element of \mathbb{Z}/m is represented as $[a]$ with $0 < a < m$.

Since $[a]$ is not a zero-divisor, multiplication by $[a]$ defines a map

$\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\}$. This map is injective.

Indeed, let $b, c \in \mathbb{Z}_m \setminus \{0\}$ and $b \cdot [a] = c \cdot [a]$. Then $(b - c) \cdot [a] = 0$ and

$b - c = 0$, i.e., $b = c$.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Any non-zero element of \mathbb{Z}/m is represented as $[a]$ with $0 < a < m$.

Since $[a]$ is not a zero-divisor, multiplication by $[a]$ defines a map

$\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\}$. This map is injective.

Indeed, let $b, c \in \mathbb{Z}/m \setminus \{0\}$ and $b \cdot [a] = c \cdot [a]$. Then $(b - c) \cdot [a] = 0$ and

$b - c = 0$, i.e., $b = c$.

Thus, the map $\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\} : x \mapsto x \cdot [a]$ is injective.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Any non-zero element of \mathbb{Z}/m is represented as $[a]$ with $0 < a < m$.

Since $[a]$ is not a zero-divisor, multiplication by $[a]$ defines a map

$\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\}$. This map is injective.

Indeed, let $b, c \in \mathbb{Z}/m \setminus \{0\}$ and $b \cdot [a] = c \cdot [a]$. Then $(b - c) \cdot [a] = 0$ and

$b - c = 0$, i.e., $b = c$.

Thus, the map $\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\} : x \mapsto x \cdot [a]$ is injective.

This is a map of a finite set to itself.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Any non-zero element of \mathbb{Z}/m is represented as $[a]$ with $0 < a < m$.

Since $[a]$ is not a zero-divisor, multiplication by $[a]$ defines a map

$\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\}$. This map is injective.

Indeed, let $b, c \in \mathbb{Z}/m \setminus \{0\}$ and $b \cdot [a] = c \cdot [a]$. Then $(b - c) \cdot [a] = 0$ and

$b - c = 0$, i.e., $b = c$.

Thus, the map $\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\} : x \mapsto x \cdot [a]$ is injective.

This is a map of a finite set to itself. On the next slide we will prove that any injective map of a finite set to itself is surjective.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Any non-zero element of \mathbb{Z}/m is represented as $[a]$ with $0 < a < m$.

Since $[a]$ is not a zero-divisor, multiplication by $[a]$ defines a map

$\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\}$. This map is injective.

Indeed, let $b, c \in \mathbb{Z}/m \setminus \{0\}$ and $b \cdot [a] = c \cdot [a]$. Then $(b - c) \cdot [a] = 0$ and

$b - c = 0$, i.e., $b = c$.

Thus, the map $\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\} : x \mapsto x \cdot [a]$ is injective.

This is a map of a finite set to itself. On the next slide we will prove that any injective map of a finite set to itself is surjective.

It follows that there exists $b \in \mathbb{Z}/m \setminus \{0\}$ such that $b \cdot [a] = 1$,

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Any non-zero element of \mathbb{Z}/m is represented as $[a]$ with $0 < a < m$.

Since $[a]$ is not a zero-divisor, multiplication by $[a]$ defines a map

$\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\}$. This map is injective.

Indeed, let $b, c \in \mathbb{Z}/m \setminus \{0\}$ and $b \cdot [a] = c \cdot [a]$. Then $(b - c) \cdot [a] = 0$ and

$b - c = 0$, i.e., $b = c$.

Thus, the map $\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\} : x \mapsto x \cdot [a]$ is injective.

This is a map of a finite set to itself. On the next slide we will prove that any injective map of a finite set to itself is surjective.

It follows that there exists $b \in \mathbb{Z}/m \setminus \{0\}$ such that $b \cdot [a] = 1$,

that is $b = [a]^{-1}$.

Why are fields remarkable?

In a field we can divide by any non-zero element.
Hence we can solve any linear equation $ax + b = 0$ with $a \neq 0$.
And a solution is unique.

Theorem. \mathbb{Z}/m is a field iff m is prime.

Proof. We have proved that if m is not prime, then \mathbb{Z}/m has zero-divisors.

Therefore it cannot be a field.

Let us prove that if m is prime, then \mathbb{Z}/m is a field.

Any non-zero element of \mathbb{Z}/m is represented as $[a]$ with $0 < a < m$.

Since $[a]$ is not a zero-divisor, multiplication by $[a]$ defines a map

$\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\}$. This map is injective.

Indeed, let $b, c \in \mathbb{Z}/m \setminus \{0\}$ and $b \cdot [a] = c \cdot [a]$. Then $(b - c) \cdot [a] = 0$ and

$b - c = 0$, i.e., $b = c$.

Thus, the map $\mathbb{Z}/m \setminus \{0\} \rightarrow \mathbb{Z}/m \setminus \{0\} : x \mapsto x \cdot [a]$ is injective.

This is a map of a finite set to itself. On the next slide we will prove that any injective map of a finite set to itself is surjective.

It follows that there exists $b \in \mathbb{Z}/m \setminus \{0\}$ such that $b \cdot [a] = 1$,

that is $b = [a]^{-1}$. □

Theorem, If a set X is finite, then any injection $f : X \rightarrow X$ is surjective.

Theorem, If a set X is finite, then any injection $f : X \rightarrow X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \dots, f^n(a), \dots\}$ is called the **orbit** of a .

Theorem, If a set X is finite, then any injection $f : X \rightarrow X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \dots, f^n(a), \dots\}$ is called the **orbit** of a . It is finite, as a subset of finite X .

Theorem, If a set X is finite, then any injection $f : X \rightarrow X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \dots, f^n(a), \dots\}$ is called the **orbit** of a . It is finite, as a subset of finite X . Therefore, $\exists m, p \in \mathbb{N} \quad f^m(a) = f^p(a)$
for some $m \neq p$.

Theorem, If a set X is finite, then any injection $f : X \rightarrow X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \dots, f^n(a), \dots\}$ is called the **orbit** of a . It is finite, as a subset of finite X . Therefore, $\exists m, p \in \mathbb{N} \quad f^m(a) = f^p(a)$
for some $m \neq p$.

By injectivity of f , $(f^m(a) = f^p(a)) \implies (f^{m-1}(a) = f^{p-1}(a))$.

Theorem, If a set X is finite, then any injection $f : X \rightarrow X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \dots, f^n(a), \dots\}$ is called the **orbit** of a . It is finite, as a subset of finite X . Therefore, $\exists m, p \in \mathbb{N} \quad f^m(a) = f^p(a)$ for some $m \neq p$.

By injectivity of f , $(f^m(a) = f^p(a)) \implies (f^{m-1}(a) = f^{p-1}(a))$.

Therefore, each orbit looks as $\{a, f(a), f^2(a), \dots, f^p(a)\}$ for some $p \in \mathbb{N}$ with $a = f^{p+1}(a)$.

Theorem, If a set X is finite, then any injection $f : X \rightarrow X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \dots, f^n(a), \dots\}$ is called the **orbit** of a . It is finite, as a subset of finite X . Therefore, $\exists m, p \in \mathbb{N} \quad f^m(a) = f^p(a)$
for some $m \neq p$.

By injectivity of f , $(f^m(a) = f^p(a)) \implies (f^{m-1}(a) = f^{p-1}(a))$.

Therefore, each orbit looks as $\{a, f(a), f^2(a), \dots, f^p(a)\}$ for some $p \in \mathbb{N}$ with $a = f^{p+1}(a)$.

On each orbit, f is surjective.

Theorem, If a set X is finite, then any injection $f : X \rightarrow X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \dots, f^n(a), \dots\}$ is called the **orbit** of a . It is finite, as a subset of finite X . Therefore, $\exists m, p \in \mathbb{N} \quad f^m(a) = f^p(a)$
for some $m \neq p$.

By injectivity of f , $(f^m(a) = f^p(a)) \implies (f^{m-1}(a) = f^{p-1}(a))$.

Therefore, each orbit looks as $\{a, f(a), f^2(a), \dots, f^p(a)\}$ for some $p \in \mathbb{N}$ with $a = f^{p+1}(a)$.

On each orbit, f is surjective. Orbits cover the whole X .

Theorem, If a set X is finite, then any injection $f : X \rightarrow X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \dots, f^n(a), \dots\}$ is called the **orbit** of a . It is finite, as a subset of finite X . Therefore, $\exists m, p \in \mathbb{N} \quad f^m(a) = f^p(a)$
for some $m \neq p$.

By injectivity of f , $(f^m(a) = f^p(a)) \implies (f^{m-1}(a) = f^{p-1}(a))$.

Therefore, each orbit looks as $\{a, f(a), f^2(a), \dots, f^p(a)\}$ for some $p \in \mathbb{N}$ with $a = f^{p+1}(a)$.

On each orbit, f is surjective. Orbits cover the whole X .

Therefore, f is surjective on the whole X .

Theorem, If a set X is finite, then any injection $f : X \rightarrow X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \dots, f^n(a), \dots\}$ is called the **orbit** of a . It is finite, as a subset of finite X . Therefore, $\exists m, p \in \mathbb{N} \quad f^m(a) = f^p(a)$
for some $m \neq p$.

By injectivity of f , $(f^m(a) = f^p(a)) \implies (f^{m-1}(a) = f^{p-1}(a))$.

Therefore, each orbit looks as $\{a, f(a), f^2(a), \dots, f^p(a)\}$ for some $p \in \mathbb{N}$ with $a = f^{p+1}(a)$.

On each orbit, f is surjective. Orbits cover the whole X .

Therefore, f is surjective on the whole X . □