Last digit

Last digit

Problem 3.

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution.

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10$$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

$2^4 \equiv 6 \mod 10$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

$2^4 \equiv 6 \mod 10$

$2^5 \equiv 2 \mod 10$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

$2^4 \equiv 6 \mod 10$

$2^5 \equiv 2 \mod 10$

$2^6 \equiv 4 \mod 10$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

$2^4 \equiv 6 \mod 10$

$2^5 \equiv 2 \mod 10$

$2^6 \equiv 4 \mod 10$

. . . . . .

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$$\left.\begin{aligned} 2^1 &\equiv 2 \mod 10 \\ 2^2 &\equiv 4 \mod 10 \\ 2^3 &\equiv 8 \mod 10 \\ 2^4 &\equiv 6 \mod 10 \\ 2^5 &\equiv 2 \mod 10 \\ 2^6 &\equiv 4 \mod 10 \\ &\cdots\cdots\cdots\cdots \end{aligned}\right]$$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

$2^4 \equiv 6 \mod 10$

$2^5 \equiv 2 \mod 10$

$2^6 \equiv 4 \mod 10$

. . . . . .

cycle of length 4

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

$2^4 \equiv 6 \mod 10$

$2^5 \equiv 2 \mod 10$

$2^6 \equiv 4 \mod 10$

.....

cycle of length 4

$2023 \equiv ? \mod 4$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

$2^4 \equiv 6 \mod 10$

$2^5 \equiv 2 \mod 10$

$2^6 \equiv 4 \mod 10$

.....

cycle of length 4

$2023 \equiv ? \mod 4$

$2023 \equiv 3 \mod 4$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

$2^4 \equiv 6 \mod 10$

$2^5 \equiv 2 \mod 10$

$2^6 \equiv 4 \mod 10$

.....

cycle of length 4

$2023 \equiv ? \mod 4$

$2023 \equiv 3 \mod 4$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

$2^4 \equiv 6 \mod 10$

$2^5 \equiv 2 \mod 10$

$2^6 \equiv 4 \mod 10$

.....

cycle of length 4

$2023 \equiv ? \mod 4$

$2023 \equiv 3 \mod 4$

$2^{2023} \equiv 8 \mod 10$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ? \mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

$2^4 \equiv 6 \mod 10$

$2^5 \equiv 2 \mod 10$

$2^6 \equiv 4 \mod 10$

.....

cycle of length 4

$2023 \equiv ? \mod 4$

$2023 \equiv 3 \mod 4$

$2^{2023} \equiv 8 \mod 10$

$2022^{2023} \equiv 8 \mod 10$

Last digit

Problem 3. Find the last digit of 2022^{2023}.

Solution. $2022^{2023} \equiv ?\mod 10$

$$2022 \equiv 2 \mod 10 \implies 2022^{2023} \equiv 2^{2023} \mod 10$$

$$2^{2023} \equiv ? \mod 10$$

$2^1 \equiv 2 \mod 10$

$2^2 \equiv 4 \mod 10$

$2^3 \equiv 8 \mod 10$

$2^4 \equiv 6 \mod 10$

$2^5 \equiv 2 \mod 10$

$2^6 \equiv 4 \mod 10$

.....

cycle of length 4

$2023 \equiv ? \mod 4$

$2023 \equiv 3 \mod 4$

$2^{2023} \equiv 8 \mod 10$

$2022^{2023} \equiv 8 \mod 10$

Answer:

the last digit of 2022^{2023} is 8.

Diophantine equations

Diophantine equations

Problem 3.

Diophantine equations

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$

Diophantine equations

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Diophantine equations

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution.

Diophantine equations

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

Diophantine equations

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

Diophantine equations

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

Diophantine equations

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

$$[x^2]_3 = 2$$

Diophantine equations

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

$$[x^2]_3 = 2$$

$x \mod 3$	$x^2 \mod 3$
0	0
1	1
-1	1

Diophantine equations

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

$$[x^2]_3 = 2$$

$x \mod 3$	$x^2 \mod 3$
0	0
1	1
-1	1

So $x^2 \equiv 0$ or $1 \mod 3$,

Diophantine equations

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

$$[x^2]_3 = 2$$

$x \mod 3$	$x^2 \mod 3$
0	0
1	1
-1	1

So $x^2 \equiv 0$ or $1 \mod 3$, and $x^2 \not\equiv 2 \mod 3$.

Diophantine equations

Problem 3. Prove that the equation $x^2 - 3y^2 = 17$ has no integer solutions.

Solution. $x^2 - 3y^2 = 17$

$$[x^2 - 3y^2]_3 = [17]_3$$

$$[x^2]_3 - [3y^2]_3 = 2$$

$$[x^2]_3 = 2$$

$x \mod 3$	$x^2 \mod 3$
0	0
1	1
-1	1

So $x^2 \equiv 0$ or $1 \mod 3$, and $x^2 \not\equiv 2 \mod 3$.

Therefore, the original equation has **no** integer solutions.

Reduction modulo m

Reduction modulo m

As we know, an equivalence relation on a set X

Reduction modulo m

As we know, an equivalence relation on a set X gives rise to the quotient set $X/_\sim$

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 $X \to X/_\sim,\ x \mapsto [x]$.

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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence 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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m,
then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m,
then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names:

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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m,
then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,

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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m,
then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m,
then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m,
then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient 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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m,
then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ 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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m,
then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ 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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m,
then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ possesses the following two properties:
$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$

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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m, then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ 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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m, then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ 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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m, then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ 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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m, then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ 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, $f(a+b) = [a+b] = [a] + [b]$

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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m, then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ 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, $f(a+b) = [a+b] = [a] + [b] = f(a) + f(b)$

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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m, then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ 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
$f(ab)$

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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m, then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ 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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m, then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ 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
$f(ab) = [ab] = [a][b]$

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 $X \to X/_\sim,\ x \mapsto [x]$.

When $X = \mathbb{Z}$ and the equivalence relation is the congruence modulo m, then the quotient map is $\mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$.

This map has many names: canonical projection,
projection map
reduction modulo m,
quotient map.

This map $\mathbb{Z} \to \mathbb{Z}/_m$ 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
$f(ab) = [ab] = [a][b] = f(a)f(b)$.

Ring homomorphism

Ring homomorphism

Definition. Let R, S be rings.

Ring homomorphism

Definition. Let R, S be rings.
A map $f : R \to S$ is called **ring homomorphism**

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$$f(a+b) = f(a) + f(b)$$

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$$f(a+b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b)$$

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$.

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$.

Remark.

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$.

Remark. $f(a+b) = f(a) + f(b)$.

$\uparrow$ addition in R $\quad$ $\uparrow$ addition in S

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ 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

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ 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. $f(a+b) = f(a) + f(b)$.

$\uparrow$ addition in R $\quad$ $\uparrow$ addition in S

$$f(ab) = f(a)f(b)$$

$\uparrow$ multiplication in R $\quad$ $\uparrow$ multiplication in S

Theorem.

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$.

Remark. $f(a+b) = f(a) + f(b)$.

$\uparrow$ addition in R $\quad$ $\uparrow$ addition in S

$f(ab) = f(a)f(b)$

$\uparrow$ multiplication in R $\quad$ $\uparrow$ multiplication in S

Theorem. The canonical projection $\mathbb{Z} \to \mathbb{Z}/m$

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$.

Remark. $f(a+b) = f(a) + f(b)$.

$\uparrow$ addition in R $\quad$ $\uparrow$ addition in S

$f(ab) = f(a)f(b)$

$\uparrow$ multiplication in R $\quad$ $\uparrow$ multiplication in S

Theorem. The canonical projection $\mathbb{Z} \to \mathbb{Z}/m$ is a ring homomorphism.

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$.

Remark. $f(a+b) = f(a) + f(b)$.

$\uparrow$ addition in R $\quad$ $\uparrow$ addition in S

$f(ab) = f(a)f(b)$

$\uparrow$ multiplication in R $\quad$ $\uparrow$ multiplication in S

Theorem. The canonical projection $\mathbb{Z} \to \mathbb{Z}/m$ is a ring homomorphism.

Proof.

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ 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. $f(a+b) = f(a) + f(b)$.

$\uparrow$ addition in R $\quad$ $\uparrow$ addition in S

$$f(ab) = f(a)f(b)$$

$\uparrow$ multiplication in R $\quad$ $\uparrow$ multiplication in S

Theorem. The canonical projection $\mathbb{Z} \to \mathbb{Z}/m$ is a ring homomorphism.

Proof. We already know that both $\mathbb{Z}$ and $\mathbb{Z}/m$ are rings.

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$.

Remark. $f(a+b) = f(a) + f(b)$.

$\uparrow$ addition in R $\quad$ $\uparrow$ addition in S

$f(ab) = f(a)f(b)$

$\uparrow$ multiplication in R $\quad$ $\uparrow$ multiplication in S

Theorem. The canonical projection $\mathbb{Z} \to \mathbb{Z}/_m$ 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 $f : \mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$ preserves the ring operations:

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$.

Remark. $f(a+b) = f(a) + f(b)$.

$\uparrow$ addition in R $\quad$ $\uparrow$ addition in S

$f(ab) = f(a)f(b)$

$\uparrow$ multiplication in R $\quad$ $\uparrow$ multiplication in S

Theorem. The canonical projection $\mathbb{Z} \to \mathbb{Z}/_m$ 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 $f : \mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$ preserves the ring operations:

$f(a+b) = f(a) + f(b)$

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$.

Remark. $f(a+b) = f(a) + f(b)$.

$\uparrow$ addition in R $\quad$ $\uparrow$ addition in S

$f(ab) = f(a)f(b)$

$\uparrow$ multiplication in R $\quad$ $\uparrow$ multiplication in S

Theorem. The canonical projection $\mathbb{Z} \to \mathbb{Z}/m$ 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 $f : \mathbb{Z} \to \mathbb{Z}/m,\ x \mapsto x \bmod m$ preserves the ring operations:

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$.

Remark. $f(a+b) = f(a) + f(b)$.

$\uparrow$ addition in R $\quad$ $\uparrow$ addition in S

$f(ab) = f(a)f(b)$

$\uparrow$ multiplication in R $\quad$ $\uparrow$ multiplication in S

Theorem. The canonical projection $\mathbb{Z} \to \mathbb{Z}/_m$ 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 $f : \mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$ preserves the ring operations:

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in \mathbb{Z}$.

Ring homomorphism

Definition. Let R, S be rings.

A map $f : R \to S$ is called **ring homomorphism** if

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in R$.

Remark. $f(a+b) = f(a) + f(b)$.

$\uparrow$ addition in R $\quad$ $\uparrow$ addition in S

$f(ab) = f(a)f(b)$

$\uparrow$ multiplication in R $\quad$ $\uparrow$ multiplication in S

Theorem. The canonical projection $\mathbb{Z} \to \mathbb{Z}/_m$ 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 $f : \mathbb{Z} \to \mathbb{Z}/_m,\ x \mapsto x \bmod m$ preserves the ring operations:

$f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for any $a, b \in \mathbb{Z}$.

Therefore, f is a ring homomorphism. $\square$

Control of calculations

Control of calculations

Problem.

Control of calculations

Problem. Is it true that

Control of calculations

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Control of calculations

Problem. Is it true that $74,218 \cdot 21,363 - 81,835 = 1,585,447,299$?

Solution.

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,

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

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)

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

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 $4 \cdot 6 - 7 = 0$.

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 $24 - 7 \neq 0$.

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 $\mathbb{Z}/_9$,

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 $\mathbb{Z}$.

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. $74,218 \cdot 21,363 - 81,835 \neq 1,585,447,299$.

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 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.

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

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: $2 + 7 \stackrel{?}{=} 18 \quad \stackrel{\text{mod } 9}{\longrightarrow} \quad 0 = 0$.

Caution

Caution

Example 1.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4)$

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3$

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. But

$f([0]_4) =$

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. But

$f([0]_4) = f([4]_4)$

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. But

$f([0]_4) = f([4]_4) = [4^2]_3$

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. But

$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3$

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. But

$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3$.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. But

$f([0]_4) = f([4]_4) = [4^2]_3 = [16]_3 = [1]_3$.

The element $[0]_4$ has two different images!

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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**.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$ by $[x]_6 \mapsto [x^2]_3$.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$ by $[x]_6 \mapsto [x^2]_3$.

Is this map well-defined?

Solution.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$ 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 $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$ 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 $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$ 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 $x_1 \equiv x_2 \mod 6$.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$ 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 $x_1 \equiv x_2 \mod 6$. We have to check if $x_1^2 \equiv x_2^2 \mod 3$.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$ 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 $x_1 \equiv x_2 \mod 6$. We have to check if $x_1^2 \equiv x_2^2 \mod 3$.
If $x_1 \equiv x_2 \mod 6$, then $x_1 - x_2$ is divisible by 6, and so by 3.

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$ 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 $x_1 \equiv x_2 \mod 6$. We have to check if $x_1^2 \equiv x_2^2 \mod 3$.
If $x_1 \equiv x_2 \mod 6$, 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 $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$ 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 $x_1 \equiv x_2 \mod 6$. We have to check if $x_1^2 \equiv x_2^2 \mod 3$.
If $x_1 \equiv x_2 \mod 6$, 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, $x_1^2 \equiv x_2^2 \mod 3$,

Caution

Example 1. Define a map $f : \mathbb{Z}/_4 \to \mathbb{Z}/_3$ by $[x]_4 \mapsto [x^2]_3$.

The formula looks innocent, let's do some calculations:

$f([0]_4) = [0^2]_3 = [0]_3$. 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 $f : \mathbb{Z}/_6 \to \mathbb{Z}/_3$ 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 $x_1 \equiv x_2 \mod 6$. We have to check if $x_1^2 \equiv x_2^2 \mod 3$.
If $x_1 \equiv x_2 \mod 6$, 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, $x_1^2 \equiv x_2^2 \mod 3$, and the map is well defined.

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 $ab = 0$.

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?

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.

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 $0 < a, b < m$.

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, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$.

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, $[a]_m \cdot [b]_m = [ab]_m = [m]_m = 0$. □

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 $ab = 1$.

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 $ab = 1$.

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}.

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.

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

$$a^{-1}ab = (a^{-1}a)b = 1 \cdot b = b.$$

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

$$0 = a^{-1} \cdot 0 = a^{-1}(ab) = a^{-1}ab = (a^{-1}a)b = 1 \cdot b = b.$$

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**.

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.

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.

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.

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.

Fields $\mathbb{Z}/_p$

Why are fields remarkable?

Fields $\mathbb{Z}/_p$

Why are fields remarkable?

In a field we can divide by any non-zero element.

Fields $\mathbb{Z}/_p$

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 $a \neq 0$.

Fields $\mathbb{Z}/_p$

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.

Fields $\mathbb{Z}/_p$

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.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ has zero-divisors.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ has zero-divisors.
Therefore it cannot be a field.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ has zero-divisors.
Therefore it cannot be a field.

Let us prove that if m is prime, then $\mathbb{Z}/_m$ is a field.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ 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 $0 < a < m$.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ 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-divsor, multiplication by $[a]$ defines a map

$$\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\}\,.$$

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ 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-divsor, multiplication by $[a]$ defines a map
$\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\}$. This map is injective.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ 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-divsor, multiplication by $[a]$ defines a map
$\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\}$. This map is injective.
Indeed, let $b, c \in \mathbb{Z}_m \setminus \{0\}$ and $b \cdot [a] = c \cdot [a]$.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ 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-divsor, multiplication by $[a]$ defines a map
$\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\}$. 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., $b = c$.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ 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-divsor, multiplication by $[a]$ defines a map
$\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\}$. 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 $\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\} : x \mapsto x \cdot [a]$ is injective.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ 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-divsor, multiplication by $[a]$ defines a map
$\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\}$. 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 $\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\} : x \mapsto x \cdot [a]$ is injective.
This is a map of a finite set to itself.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ 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-divsor, multiplication by $[a]$ defines a map
$\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\}$. 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 $\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\} : x \mapsto x \cdot [a]$ 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.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ 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-divsor, multiplication by $[a]$ defines a map
$\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\}$. 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 $\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\} : x \mapsto x \cdot [a]$ 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 $b \cdot [a] = 1$,

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ 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-divsor, multiplication by $[a]$ defines a map
$\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\}$. 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 $\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\} : x \mapsto x \cdot [a]$ 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 $b = [a]^{-1}$.

Fields $\mathbb{Z}/_p$

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, them $\mathbb{Z}/_m$ 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-divsor, multiplication by $[a]$ defines a map
$\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\}$. 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 $\mathbb{Z}/_m \setminus \{0\} \to \mathbb{Z}/_m \setminus \{0\} : x \mapsto x \cdot [a]$ 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 $b = [a]^{-1}$. □

Injective vs. surjective self-maps

Theorem, If a set X is finite, then any injection $f : X \to X$ is surjective.

Injective vs. surjective self-maps

Theorem, If a set X is finite, then any injection $f : X \to X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}$ is called the **orbit** of a.

Injective vs. surjective self-maps

Theorem, If a set X is finite, then any injection $f : X \to X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}$ is called the **orbit** of a. It is finite, as a subset of finite X.

Injective vs. surjective self-maps

Theorem, If a set X is finite, then any injection $f : X \to X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}$ 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 $m \neq p$.

Injective vs. surjective self-maps

Theorem, If a set X is finite, then any injection $f : X \to X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}$ 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, $\quad (f^m(a) = f^p(a)) \implies (f^{m-1}(a) = f^{p-1}(a))$.

Injective vs. surjective self-maps

Theorem, If a set X is finite, then any injection $f : X \to X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}$ 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, $\quad (f^m(a) = f^p(a)) \implies (f^{m-1}(a) = f^{p-1}(a))$.
Therefore, each orbit looks as $\{a, f(a), f^2(a), \ldots, f^p(a)\}$ for some $p \in \mathbb{N}$ with $a = f^{p+1}(a)$.

Injective vs. surjective self-maps

Theorem, If a set X is finite, then any injection $f : X \to X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}$ 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, $\quad (f^m(a) = f^p(a)) \implies (f^{m-1}(a) = f^{p-1}(a))$.
Therefore, each orbit looks as $\{a, f(a), f^2(a), \ldots, f^p(a)\}$ for some $p \in \mathbb{N}$ with $a = f^{p+1}(a)$.

On each orbit, f is surjective.

Injective vs. surjective self-maps

Theorem, If a set X is finite, then any injection $f : X \to X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}$ 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, $\quad (f^m(a) = f^p(a)) \implies (f^{m-1}(a) = f^{p-1}(a))$.
Therefore, each orbit looks as $\{a, f(a), f^2(a), \ldots, f^p(a)\}$ for some $p \in \mathbb{N}$ with $a = f^{p+1}(a)$.

On each orbit, f is surjective. Orbits cover the whole X.

Injective vs. surjective self-maps

Theorem, If a set X is finite, then any injection $f : X \to X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}$ 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, $\quad (f^m(a) = f^p(a)) \Longrightarrow (f^{m-1}(a) = f^{p-1}(a))$.
Therefore, each orbit looks as $\{a, f(a), f^2(a), \ldots, f^p(a)\}$ 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.

Injective vs. surjective self-maps

Theorem, If a set X is finite, then any injection $f : X \to X$ is surjective.

Proof. Let $a \in X$. The set $\{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}$ 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, $\quad (f^m(a) = f^p(a)) \Longrightarrow (f^{m-1}(a) = f^{p-1}(a))$.
Therefore, each orbit looks as $\{a, f(a), f^2(a), \ldots, f^p(a)\}$ 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. $\square$

Questions for future

Now we leave **Modular Arithmetics**,

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

There are many further questions in this subjects to think about. Here are some:

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

There are many further questions in this subjects to think about. Here are some:

We have learned how to **add**, **subtract** and **multiply** in $\mathbb{Z}/_m$.

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

There are many further questions in this subjects to think about. Here are some:

We have learned how to **add**, **subtract** and **multiply** in $\mathbb{Z}/_m$.

If m is prime, then it is possible to **divide**.

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

There are many further questions in this subjects to think about. Here are some:

We have learned how to **add**, **subtract** and **multiply** in $\mathbb{Z}/_m$.

If m is prime, then it is possible to **divide**.

How to do this?

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

There are many further questions in this subjects to think about. Here are some:

We have learned how to **add**, **subtract** and **multiply** in $\mathbb{Z}/_m$.

If m is prime, then it is possible to **divide**.

How to do this?

How to solve **linear equations** in $\mathbb{Z}/_m$?

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

There are many further questions in this subjects to think about. Here are some:

We have learned how to **add**, **subtract** and **multiply** in $\mathbb{Z}/_m$.

If m is prime, then it is possible to **divide**.

How to do this?

How to solve **linear equations** in $\mathbb{Z}/_m$?

What about **square roots**?

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

There are many further questions in this subjects to think about. Here are some:

We have learned how to **add**, **subtract** and **multiply** in $\mathbb{Z}/_m$.

If m is prime, then it is possible to **divide**.

How to do this?

How to solve **linear equations** in $\mathbb{Z}/_m$?

What about **square roots**? And **quadratic equations**?

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

There are many further questions in this subjects to think about. Here are some:

We have learned how to **add**, **subtract** and **multiply** in $\mathbb{Z}/_m$.

If m is prime, then it is possible to **divide**.

How to do this?

How to solve **linear equations** in $\mathbb{Z}/_m$?

What about **square roots**? And **quadratic equations**?
The modern approach to modular arithmetic was developed by Gauss.

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

There are many further questions in this subjects to think about. Here are some:

We have learned how to **add**, **subtract** and **multiply** in $\mathbb{Z}/_m$.

If m is prime, then it is possible to **divide**.

How to do this?

How to solve **linear equations** in $\mathbb{Z}/_m$?

What about **square roots**? And **quadratic equations**?
The modern approach to modular arithmetic was developed by Gauss.
The symbol $\equiv$ for congruences appeared in Gauss' book

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

There are many further questions in this subjects to think about. Here are some:

We have learned how to **add**, **subtract** and **multiply** in $\mathbb{Z}/_m$.

If m is prime, then it is possible to **divide**.

How to do this?

How to solve **linear equations** in $\mathbb{Z}/_m$?

What about **square roots**? And **quadratic equations**?
The modern approach to modular arithmetic was developed by Gauss.
The symbol $\equiv$ for congruences appeared in Gauss' book "Disquisitiones Arithmeticae"
("Arithmetical Investigations") in 1801,

Questions for future

Now we leave **Modular Arithmetics**, but we **will be back**.

There are many further questions in this subjects to think about. Here are some:

We have learned how to **add**, **subtract** and **multiply** in $\mathbb{Z}/_m$.

If m is prime, then it is possible to **divide**.

How to do this?

How to solve **linear equations** in $\mathbb{Z}/_m$?

What about **square roots**? And **quadratic equations**?
The modern approach to modular arithmetic was developed by Gauss.
The symbol $\equiv$ for congruences appeared in Gauss' book "Disquisitiones Arithmeticae"
("Arithmetical Investigations") in 1801,
where he answered the questions above and much more. Then he was 24.

Carl Friedrich Gauss (1777-1855)

Carl Friedrich Gauss (1777-1855)

Gaussian elimination

Gauss's least square method

Gaussian distribution (normal distribution)

Gauss's theorem (divergence theorem)

Gauss's law for gravity

Gaussian gravitational constant

Gaussian curvature

Carl Friedrich Gauss (1777-1855)

Gaussian elimination

Gauss's least square method

Gaussian distribution (normal distribution)

Gauss's theorem (divergence theorem)

Gauss's law for gravity

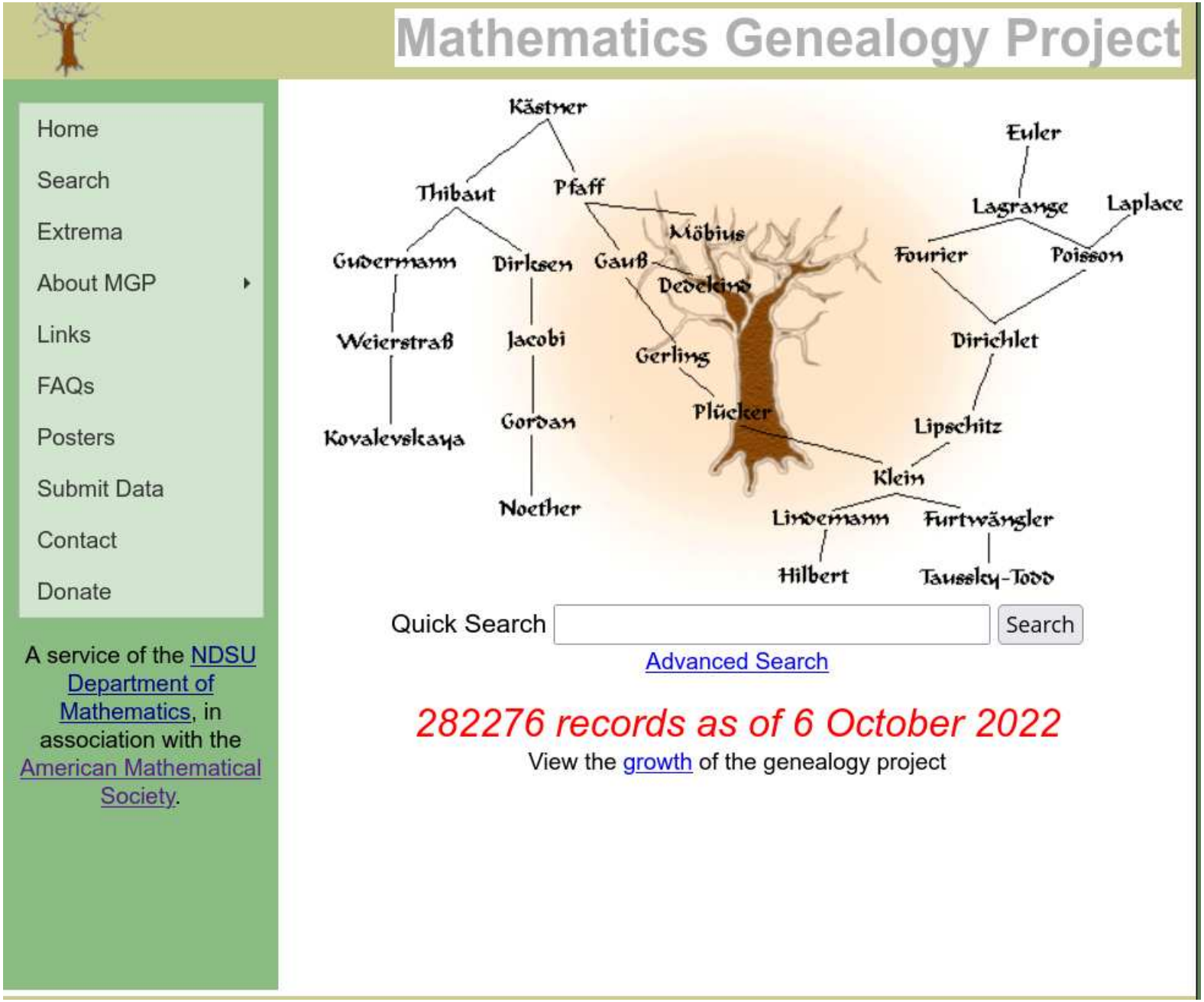
Gaussian gravitational constant

Gaussian curvature

My mathematical ancestors

Mathematics Genealogy Project https://www.genealogy.math.ndsu.nodak.edu/

My mathematical ancestors



My mathematical ancestors