The Integers Modulo n

Table of contents

The set $\mathbb{Z}_n$ 1
Adding and multiplying classes 2
$(\mathbb{Z}_n, +)$ is a group 4
Multiplication: $\mathbb{Z}_n - \{[0]\}$ 4
$\mathbb{Z}_p$ is a field 5
Notation 6
Common mistakes 7
See also 7

$\mathbb{Z}_n$ is the set of equivalence classes of congruence mod n. It is a number system with exactly n elements, in which addition and multiplication are done on classes. Congruence itself is in modular-arithmetic[1], and equivalence classes in equivalence-classes-and-partitions[2]. Under addition $\mathbb{Z}_n$ is one of the course's standard groups[3], and when n is prime it is a field, with division by every non-zero class (fields[4]). First met in 2026-09-24-definitions-and-examples-of-groups[5].

The set $\mathbb{Z}_n$

Fix $n \in \mathbb{Z}^+$. Congruence mod n is an equivalence relation on $\mathbb{Z}$,

$$m \; R \; k \iff m \equiv k \pmod{n} \iff n \mid (m-k),$$

and its classes partition $\mathbb{Z}$. $\mathbb{Z}_n$ is the set of those classes:

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}.$$

[1] courses/math1061/modular-arithmetic.pdf
[2] courses/math1061/equivalence-classes-and-partitions.pdf
[3] courses/math1061/groups.pdf
[4] courses/math1061/fields.pdf
[5] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

For $n = 10$:

$$\mathbb{Z}_{10} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9]\}$$

$$[0] = \{\dots, -30, -20, -10, 0, 10, 20, 30, \dots\}, \qquad [1] = \{\dots, -29, -19, -9, 1, 11, 21, 31, \dots\}$$

- $\mathbb{Z}_n$ **has exactly** n **elements.** Every integer leaves exactly one of the remainders $0, 1, \dots, n-1$ on division by n (modular-arithmetic[6]), so every integer is in exactly one of the n classes.
- **Each element is an infinite set of integers.** [1] is not the number 1. It is the set of all integers congruent to 1.
- **Each class has many names.** $[0] = [10] = [30]$ and $[1] = [21] = [-9]$. In general $[a] = [b]$ exactly when $a \equiv b \pmod{n}$ (equivalence-classes-and-partitions[7]).

We usually use $[0], [1], \dots, [n-1]$ as representatives for the equivalence classes of $\mathbb{Z}_n$.

	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
	−10	−9	−8	−7	−6	−5	−4	−3	−2	−1
usual names	0	1	2	3	4	5	6	7	8	9
	10	11	12	13	14	15	16	17	18	19
	20	21	22	23	24	25	26	27	28	29
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Figure 1: The integers from −10 to 29 written in rows of ten. Each column is one element of $\mathbb{Z}_{10}$: going down a column adds 10, so everything in a column is congruent mod 10. The whole of $\mathbb{Z}$ is sorted into these ten columns, and $\mathbb{Z}_{10}$ is the set of the ten columns. The shaded row holds the usual representatives, 0 to 9. Any other number in a column names the same class, so $[21] = [1]$ and $[-1] = [9]$.

Adding and multiplying classes

Define binary operations + (plus/addition) and · (times/multiplication) on $\mathbb{Z}_n$ as follows. For all $[a], [b] \in \mathbb{Z}_n$,

$$[a] + [b] = [a + b] \qquad \text{and} \qquad [a] \cdot [b] = [ab].$$

[6] courses/math1061/modular-arithmetic.pdf
[7] courses/math1061/equivalence-classes-and-partitions.pdf

To combine two classes, combine a representative of each in the ordinary way and take the class of the result. In $\mathbb{Z}_{10}$: $[8]+[9]=[17]=[7]$ and $[8]\cdot[9]=[72]=[2]$.

Any representative can be used

> when doing arithmetic in $\mathbb{Z}_n$, any representative of the equivalence classes can be used.

The definition $[a]+[b]=[a+b]$ computes with the particular names a and b, and each class has infinitely many names. The boxed sentence says the result does not depend on which names are used.

The reason is the lemma of modular-arithmetic[8]: if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$$a+b \equiv a'+b' \pmod{n} \qquad \text{and} \qquad ab \equiv a'b' \pmod{n}.$$

In the language of classes, if $[a]=[a']$ and $[b]=[b']$ then $[a+b]=[a'+b']$ and $[ab]=[a'b']$.

+	−1	9	19
−2	−3	7	17
8	7	17	27
18	17	27	37

every sum is $\equiv 7 \pmod{10}$
$[8]+[9]=[7]$

·	−1	9	19
−2	2	−18	−38
8	−8	72	152
18	−18	162	342

every product is $\equiv 2 \pmod{10}$
$[8]\cdot[9]=[2]$

Figure 2: $[8]+[9]$ and $[8]\cdot[9]$ in $\mathbb{Z}_{10}$, computed with three different representatives of each class: -2, 8 and 18 for $[8]$ down the side, and -1, 9 and 19 for $[9]$ across the top. The sums are not all the same integer, but every one of them is congruent to 7. The products are not all the same integer, but every one is congruent to 2. Whichever representatives are used, $[8]+[9]=[7]$ and $[8]\cdot[9]=[2]$.

Choosing a convenient representative

Since any representative will do, pick the one that makes the arithmetic easy, and reduce at any stage. For example:

$$\begin{aligned}([8]+[9])\cdot([6]+[7]) &= ([8]+[-1])\cdot([6]+[-3]) \\ &= [7]\cdot[3]=[21]=[1].\end{aligned}$$

[8] courses/math1061/modular-arithmetic.pdf

[9] became [−1] and [7] became [−3]. A representative just below a multiple of n is often better written as a small negative number. Without the swap the same calculation is $[17] \cdot [13] = [221] = [1]$.

$(\mathbb{Z}_n, +)$ is a group

For every $n \in \mathbb{Z}^+$, $(\mathbb{Z}_n, +)$ is a group. The check of the four properties (groups[9]):

- **Closure.** $[a] + [b] = [a + b]$, which is a class in $\mathbb{Z}_n$.
- **Associativity.** $([a] + [b]) + [c] = [(a + b) + c] = [a + (b + c)] = [a] + ([b] + [c])$. It is inherited from addition of integers.
- **Identity.** $[0]$, since $[0] + [a] = [a] + [0] = [a]$.
- **Inverses.** $[a]^{-1} = [-a]$, since $[a] + [-a] = [-a] + [a] = [0]$. With the usual names, $[-a] = [n - a]$.

It is abelian, because $[a] + [b] = [a + b] = [b + a] = [b] + [a]$.

For $n = 3$, one of the eight candidates of groups[10]:

$+$	$[0]$	$[1]$	$[2]$
$[\mathbf{0}]$	$[0]$	$[1]$	$[2]$
$[\mathbf{1}]$	$[1]$	$[2]$	$[0]$
$[\mathbf{2}]$	$[2]$	$[0]$	$[1]$

Here the group inverse of $[1]$ is $[2]$, because $[1] + [2] = [0]$. In an additive group the "inverse" is the negative.

Multiplication: $\mathbb{Z}_n - \{[0]\}$

Multiplication of classes is closed, associative and commutative on $\mathbb{Z}_n$, with identity $[1]$. But $(\mathbb{Z}_n, \cdot)$ is not a group when $n > 1$: $[0] \cdot [a] = [0]$ for every $[a]$, so $[0]$ has no inverse. This is the same obstacle as 0 in $(\mathbb{R}, \cdot)$, and the same repair is tried, removing it.

	Group under multiplication?	Worked in
$\mathbb{Z}_5 - \{[0]\}$	**yes**	2026-09-24-definitions-and-examples-of-groups[11]; table in practice-problems[12], Q4

[9] courses/math1061/groups.pdf
[10] courses/math1061/groups.pdf
[11] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[12] courses/math1061/practice-problems.pdf

	Group under multiplication?	Worked in
$\mathbb{Z}_7 - \{[0]\}$	**yes**	2026-09-24-definitions-and-examples-of-groups[13]
$\mathbb{Z}_9 - \{[0]\}$	**no**: not closed, $[3] \cdot [3] = [9] = [0]$	the same practice set, Q1
$\{[1], [2], [4], [5], [7], [8]\}$ in $\mathbb{Z}_9$	**yes**	the same practice set, Q3
$\mathbb{Z}_4 - \{[0]\}$	**no**: not closed, $[2] \cdot [2] = [4] = [0]$	2026-10-08-definitions-and-examples-of-fields[14]
$\mathbb{Z}_{15} - \{[0]\}$	**no**: not closed, $[3] \cdot [5] = [15] = [0]$	2026-10-08-definitions-and-examples-of-fields[15]

For $n = 9$, removing $[0]$ is not enough. $[3]$ and $[6]$ multiply into $[0]$, and removing those as well leaves a group.

The rule: $\mathbb{Z}_n - \{[0]\}$ is a group under multiplication exactly when n is prime. When $n = rs$ is composite, with $1 < r, s < n$, the non-zero classes $[r]$ and $[s]$ have $[r] \cdot [s] = [n] = [0]$, and closure fails, as for $9 = 3 \cdot 3$, $4 = 2 \cdot 2$ and $15 = 3 \cdot 5$. When n is prime, no product of non-zero classes is $[0]$ and every non-zero class has an inverse. Why is in fields[16].

$\mathbb{Z}_p$ is a field

$(\mathbb{Z}_p, +, \cdot)$ is a field when p is prime. All three conditions of fields[17] hold:

1. $(\mathbb{Z}_p, +)$ is an abelian group, as above.
2. $(\mathbb{Z}_p - \{[0]\}, \cdot)$ is an abelian group, by the rule just stated.
3. The distributive laws are inherited from the integers: $[a] \cdot ([b] + [c]) = [a(b + c)] = [ab + ac] = [a][b] + [a][c]$.

So in $\mathbb{Z}_p$ every class can be subtracted and every non-zero class divided by, and every equation $[a]x + [b] = [c]$ with $[a] \neq [0]$ has exactly one solution (fields[18]). For composite n, $\mathbb{Z}_n$ is not a field. $\mathbb{Z}_7$ is, and $\mathbb{Z}_4$ and $\mathbb{Z}_{15}$ are not (2026-10-08-definitions-and-examples-of-fields[19]).

[13] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[14] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[15] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[16] courses/math1061/fields.pdf
[17] courses/math1061/fields.pdf
[18] courses/math1061/fields.pdf
[19] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf

Finding a multiplicative inverse

The inverse of $[a]$ is the class $[b]$ with $ab \equiv 1 \pmod{n}$. Read it from the Cayley table, as in 2026-09-24-definitions-and-examples-of-groups[20], or search: in $\mathbb{Z}_7$, $[3] \cdot [5] = [15] = [1]$, so $[3]^{-1} = [5]$. This is the relation $xy \equiv 1 \pmod{7}$, whose arrow diagram is in 2026-09-17-relations-reflexivity-symmetry-transitivity[21]: each non-zero number is joined to its inverse.

When there is no table, there are three ways in:

- **List the multiples.** Write $a, 2a, 3a, \ldots$ mod p, each one the previous plus a, reduced, until 1 appears. For $[10]$ in $\mathbb{Z}_{17}$ the list is $10, 3, 13, 6, 16, 9, 2, 12, 5, 15, 8, 1$, so $10 \cdot 12 \equiv 1$ and $[10]^{-1} = [12]$. The search is drawn in 2026-10-08-definitions-and-examples-of-fields[22]. In $\mathbb{Z}_p$ it always succeeds within $p-1$ steps, because the multiples of a non-zero class run through every non-zero class.
- **Stop at -1.** If $ab \equiv -1$, then $a \cdot (-b) \equiv 1$, so $[a]^{-1} = [-b]$. In the same list, $10 \cdot 5 = 50 \equiv 16 = -1 \pmod{17}$, so $[10]^{-1} = [-5] = [12]$ after five steps instead of twelve.
- **Quick cases.** $[1]^{-1} = [1]$ and $[p-1]^{-1} = [p-1]$, since $(-1)(-1) = 1$. For odd p, $[2]^{-1} = [\frac{p+1}{2}]$, since $2 \cdot \frac{p+1}{2} = p + 1 \equiv 1$. In $\mathbb{Z}_{11}$ that gives $[2]^{-1} = [6]$.

The inverses in three small fields, each pair being inverses of each other:

p	Own inverse	Pairs
5	[1], [4]	$[2] \leftrightarrow [3]$
7	[1], [6]	$[2] \leftrightarrow [4]$, $[3] \leftrightarrow [5]$
11	[1], [10]	$[2] \leftrightarrow [6]$, $[3] \leftrightarrow [4]$, $[5] \leftrightarrow [9]$, $[7] \leftrightarrow [8]$

In a composite $\mathbb{Z}_n$ the search can fail. The multiples of $[2]$ in $\mathbb{Z}_6$ are $[2], [4], [0], [2], \ldots$, and $[1]$ never appears, so $[2]$ has no inverse there.

Notation

- **Three ways to say one thing.** $n \mid (a-b)$, $a \equiv b \pmod{n}$, and $[a] = [b]$ in $\mathbb{Z}_n$ are the same statement. The first is about divisibility, the second about integers, the third about classes.
- **$=$ for classes, $\equiv$ for integers.** $[7] = [0]$ in $\mathbb{Z}_7$ is true. $7 = 0$ is false. $7 \equiv 0 \pmod{7}$ is true.

[20] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[21] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf
[22] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf

- **Brackets are often dropped.** The practice problems write $\mathbb{Z}_9 - \{0\} = \{1, 2, \ldots, 8\}$ and "$2 \cdot 5 = 10 \equiv 1 \pmod 9$" for what is written here as $\mathbb{Z}_9 - \{[0]\}$ and $[2] \cdot [5] = [10] = [1]$. It is the same arithmetic.
- **The $-$ in $\mathbb{Z}_7 - \{[0]\}$ is set difference** (sets-and-set-notation[23]): the set $\mathbb{Z}_7$ with the one element $[0]$ removed.
- mod **again.** The remainder $a \bmod n$ is the usual representative of $[a]$ (modular-arithmetic[24]).

Common mistakes

- **Treating $[a]$ as the integer a.** $[9] = [-1]$ in $\mathbb{Z}_{10}$, but $9 \neq -1$.
- **Thinking $\mathbb{Z}_n$ is infinite.** It has n elements. Each element is an infinite set.
- **Using the wrong inverse.** In $(\mathbb{Z}_7, +)$ the inverse of $[3]$ is $[4]$. In $(\mathbb{Z}_7 - \{[0]\}, \cdot)$ it is $[5]$. Look at the operation first.
- **Dividing.** There is no $[\frac{1}{2}]$. An "inverse of $[2]$" under multiplication means a class $[b]$ with $[2][b] = [1]$, and it may not exist. In $\mathbb{Z}_p$ it always does: in $\mathbb{Z}_{11}$ it is $[6]$, so "dividing by 2" there means multiplying by $[6]$.
- **Mixing up the two inverses.** To undo $+[3]$ in $\mathbb{Z}_{11}$, add $-[3] = [8]$. To undo $[2]\cdot$, multiply by $[2]^{-1} = [6]$.
- **Not checking closure after removing elements.** $\mathbb{Z}_9 - \{[0]\}$ is the example.

See also

- modular-arithmetic[25] — congruence, remainders, and the lemma that makes class arithmetic work
- equivalence-classes-and-partitions[26] — classes and representatives in general
- groups[27] — the definition $\mathbb{Z}_n$ is checked against
- fields[28] — why $\mathbb{Z}_n$ is a field exactly when n is prime, and solving equations in $\mathbb{Z}_p$
- subgroups-and-cyclic-groups[29] — cyclic subgroups and cyclic groups; $(\mathbb{Z}_n, +)$ is cyclic, generated by $[1]$
- cayley-tables[30] — the tables for $\mathbb{Z}_7 - \{[0]\}$ and $\mathbb{Z}_5 - \{[0]\}$ and how to read them
- 2026-09-24-definitions-and-examples-of-groups[31] — Lecture 26 · 2026-09-21-equivalence-relations[32] — Lecture 24, where the classes of congruence mod 3 are drawn

[23] courses/math1061/sets-and-set-notation.pdf
[24] courses/math1061/modular-arithmetic.pdf
[25] courses/math1061/modular-arithmetic.pdf
[26] courses/math1061/equivalence-classes-and-partitions.pdf
[27] courses/math1061/groups.pdf
[28] courses/math1061/fields.pdf
[29] courses/math1061/subgroups-and-cyclic-groups.pdf
[30] courses/math1061/cayley-tables.pdf
[31] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[32] courses/math1061/2026-09-21-equivalence-relations.pdf

- 2026-10-06-elementary-properties-of-groups[33] — Lecture 27, where powers and cyclic subgroups are worked in $\mathbb{Z}_7 - \{[0]\}$, $\mathbb{Z}_{11} - \{[0]\}$ and $\mathbb{Z}_8$
- 2026-10-08-definitions-and-examples-of-fields[34] — Lecture 28, where $\mathbb{Z}_4$, $\mathbb{Z}_7$ and $\mathbb{Z}_{15}$ are tested and equations are solved in $\mathbb{Z}_{11}$ and $\mathbb{Z}_{17}$
- practice-problems[35] — §33, with full worked solutions
- practice-problems[36] — §36, equations in $\mathbb{Z}_5$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$ and $\mathbb{Z}_{19}$

[33] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[34] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[35] courses/math1061/practice-problems.pdf
[36] courses/math1061/practice-problems.pdf