Review 3: Integers modulo n

Peter Mayr

CU, Discrete Math, December 7, 2020

Question

Which elements are invertible in $\mathbb{Z}$?
[Which elements can you divide by?]

$1, -1$

Question

Which elements are invertible in $\mathbb{Z}_n$?

Goal: Solve equations like $[a]_n \cdot x = [c]_n$.

Recall

Let $n \in \mathbb{N}, n > 1$, and $a, b \in \mathbb{Z}$.

Definition

$a \equiv b \mod n$ (read: a is **congruent** to b **modulo** n) if $n | a - b$.
Alternative notation: $a \equiv_n b$.

1. $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.
2. The **class** of a mod n is $[a]_n = a + n\mathbb{Z}$.
3. $\mathbb{Z}_n := \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ are the **integers modulo** n.
4. $[a] + [b] := [a + b]$, $-[a] := [-a]$, and $[a] \cdot [b] := [a \cdot b]$ are well-defined on $\mathbb{Z}_n$ and satisfy the same laws as $+, -, \cdot$ on $\mathbb{Z}$.
5. $[1]_n$ is the **multiplicative identity** in $\mathbb{Z}_n$.
6. $[a]_n$ has a **multiplicative inverse** $[b]_n$ in $\mathbb{Z}_n$ if $[a]_n \cdot [b]_n = 1$. Then $[a]_n$ is **invertible**.

If $[a]_n$ has inverse $[b]_n$, we can solve $[a]_n \cdot x = [c]_n$ as $x = [b]_n \cdot [c]_n$.

Operation tables on $\mathbb{Z}_4$

To ease notation we drop the brackets [.] for classes and write 0 for [0].

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

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

Invertible elements in $\mathbb{Z}_4$: 1, 3
[$3 \cdot 3 = 1$, hence 3 is its own inverse.]

When is $[a]_n$ in $\mathbb{Z}_n$ invertible?

Theorem

Let $n \in \mathbb{N}, n > 1$, and $a \in \mathbb{Z}$. Then $[a]_n$ is invertible in $\mathbb{Z}_n$ iff $\gcd(a, n) = 1$.

Proof.

$[a]_n$ is invertible iff $\exists x \in \mathbb{Z}\colon ax \equiv 1 \mod n$ (by definition)
iff $\exists x, y \in \mathbb{Z}\colon ax + ny = 1$ (by def of $\equiv_n$)
iff $\gcd(a, n) = 1$. (by a previous Thm) □

Corollary

Let p be a prime. Then every element in $\mathbb{Z}_p \setminus \{[0]_p\}$ is invertible.

Do you want to know more?

- For applications of $\mathbb{Z}_n$ in cryptography and more see
  Math 3110 – Intro to the Theory of Numbers
- For a general study of algebraic structures like $\mathbb{Z}_n$, polynomials, permutations,...
  Math 3140 – Abstract Algebra 1