Review 3: Integers modulo n

Peter Mayr

CU, Discrete Math, April 29, 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.]

General facts about inverses

Lemma (Inverses are unique)

If a is invertible, then it has a unique inverse.

Proof. (cf. left and right inverse of bijective functions)

Let b, c be inverses of a. Then

$$b = b1 = b(ac) = (ba)c = 1c = c.$$

The unique inverse of a is denoted as a^{-1}.

Lemma (Product of invertible elements is invertible)

If a and b are invertible, then so is ab.

Proof. (cf. inverse of composition of bijective functions)

$(ab)^{-1} = b^{-1}a^{-1}$ since

$$(ab)b^{-1}a^{-1} = a1a^{-1} = aa^{-1} = 1.$$

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.

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

$\square$

Corollary

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

The number of invertible elements

Definition (Euler's phi-function)

For $n \in \mathbb{N}, n > 1$, define

$$\begin{aligned} \varphi(n) &:= |\{a \in \mathbb{Z}_n \;:\; a \text{ is invertible}\}| \\ &= |\{a \in \{1, \dots, n-1\} \;:\; \gcd(a, n) = 1\}| \end{aligned}$$

Example

$\varphi(4) = 2$ $\qquad$ $\varphi(12) = 4$ [only $1, 5, 7, 11$ have inverses in $\mathbb{Z}_{12}$]
$\varphi(p) = p - 1$ for any prime p.

Euler's Theorem

Let $n \in \mathbb{N}, n > 1$, and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Proof of Euler's Theorem.

$$I := \{x \in \mathbb{Z}_n \;:\; x \text{ is invertible}\}$$

has size $\varphi(n)$.

- **Claim:** $f : I \to I,\; x \mapsto [a]_n x$, is bijective.
  - Since $\gcd(a, n) = 1$, we have $[a]_n^{-1} \in \mathbb{Z}_n$.
  - $I \to I,\; x \mapsto [a]_n^{-1}x$ is the inverse of f, hence f is bijective.
- So $\prod_{x\in I} x = \prod_{x\in I} f(x) = \prod_{x\in I}([a]_n x) = [a]_n^{\varphi(n)} \prod_{x\in I} x$
- Multiply

$$\prod_{x\in I} x = [a]_n^{\varphi(n)} \prod_{x\in I} x$$

by $(\prod_{x\in I} x)^{-1}$ to get $[1]_n = [a]_n^{\varphi(n)}$. □

Corollary (Fermat's Little Theorem)

For any prime p and $a \in \mathbb{Z}$,

$$a^p \equiv a \mod p.$$

Proof.

- Case $p | a$: Then $p | a^p$ and $a^p \equiv 0 \equiv a \mod p$.
- Case $p \not| a$: Then $a^{p-1} \equiv 1 \mod p$ by Euler's Theorem. So $a^p \equiv a \mod p$. $\square$

Corollary (Freshman's Dream)

For $x, y \in \mathbb{Z}_p$,

$$(x+y)^p = x^p + y^p.$$

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