

Equivalence modulo n and \mathbb{Z}_n

Throughout, let n be some fixed element of \mathbb{N} with $n \geq 2$.

Definition 1 For $x, y \in \mathbb{Z}$,

$$x \equiv_n y \quad \text{if} \quad n|y - x.$$

Proposition 1 Suppose that $a_1 \equiv_n a_2$ and $b_1 \equiv_n b_2$. Then $a_1 + b_1 \equiv_n a_2 + b_2$, $a_1 \cdot b_1 \equiv_n a_2 \cdot b_2$ and $-a_1 \equiv_n -a_2$.

Definition 2 For $x \in \mathbb{Z}$, $[x]_n = \{z \in \mathbb{Z} : z \equiv_n x\}$. (That is, $[x]_n = \{z \in \mathbb{Z} : n|z - x\}$.)

Proposition 2 The relation \equiv_n is an equivalence relation with distinct equivalence classes $[0]_n, [1]_n, \dots, [n-1]_n$.

Definition 3 The set of **integers modulo n** is the set $\mathbb{Z}_n = \{[x]_n : x \in \mathbb{Z}\} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$.

We define the binary operations of addition (+) and multiplication (\cdot) on \mathbb{Z}_n by

$$[x]_n + [y]_n = [x + y]_n$$

and

$$[x]_n \cdot [y]_n = [x \cdot y]_n.$$

Note that we needed the proposition above for the definitions of + and \cdot to be independent of the representatives used.

Proposition 3 The structure $(\mathbb{Z}_n, +, \cdot, [0]_n, [1]_n)$ satisfies the following statements.

1. The operation + is commutative and associative. The element $[0]$ is an identity for +, that is, $[0] + X = X$ for any $X \in \mathbb{Z}_n$. For any $x \in \mathbb{Z}$, $[-x]$ is an additive inverse for $[x]$. That is, $[-x] + [x] = [0]$.
2. The operation \cdot is commutative and associative. The element $[1]$ is an identity for \cdot . That is, $[1] \cdot X = X$ for any $X \in \mathbb{Z}_n$.
3. The operation \cdot distributes over the operation +.

Definition 4 An element X of \mathbb{Z}_n is a **zero-divisor** if there is $Y \in \mathbb{Z}_n$, $Y \neq [0]$ such that $X \cdot Y = [0]$.

Note that the only zero-divisor in each of the structures $(\mathbb{Z}, +, \cdot, 0, 1)$ and $(\mathbb{Q}, +, \cdot, 0, 1)$ is 0 itself.

Definition 5 An element X of \mathbb{Z}_n is a **unit** if it has a **multiplicative inverse** in \mathbb{Z}_n , i.e. an element Y of \mathbb{Z}_n , such that $X \cdot Y = [1]$. In this case, we also say that X is **invertible**.

Note that the only units in the structure $(\mathbb{Z}, +, \cdot, 0, 1)$ are 1 and -1 (hence the name “unit”). In contrast, in $(\mathbb{Q}, +, \cdot, 0, 1)$, every nonzero element is a unit.

We ask ourselves what are the units in \mathbb{Z}_n ? The answer pulls together many of the ideas we have explored so far.

Theorem 4 Let $n \in \mathbb{N}$. Let $k \in \mathbb{Z}$. The following statements are equivalent.

1. The equation $nx + ky = 1$ has a solution in \mathbb{Z} .
2. $\gcd(n, k) = 1$
3. If $k|nm$ then $k|m$.
4. $[k]_n$ is not a zero-divisor in \mathbb{Z}_n .
5. $[k]_n$ is a unit in \mathbb{Z}_n .

Theorem 5 If p is prime, then every nonzero element of \mathbb{Z}_p is a unit.