Notation 1. For a positive integer $n > 1$, let $\mathbb{Z}_n$ denote the set $\{0, 1, \ldots, n-1\}$ and let $\mathbb{Z}$ denote the set of all integers. We will denote integers by the letters x, y, z and elements of $\mathbb{Z}_n$ by a, b, c. The number n will be fixed throughout.

Remark 1. $\mathbb{Z}_n$ can be identified with the set of remainders of integer division by n. For an integer x, denote by $[x]$ its remainder after division by n. Then $[x] \in \mathbb{Z}_n$ for any $x \in \mathbb{Z}$.

Example 1. Let $n = 3$. Then $[5] = [2] = [-1] = 2$. Indeed, $5 = 1 \cdot 3 + 2$, $2 = 0 \cdot 3 + 2$ and $-1 = (-1) \cdot 3 + 2$.

Definition 1. (Addition on $\mathbb{Z}_n$). Let $a, b \in \mathbb{Z}_n$. Choose $x, y \in \mathbb{Z}$ so that $[x] = a$ and $[y] = b$. Then define $a + b = [x + y]$.

Theorem 1. *Addition is well-defined.*

Proof. We need to show that: (i) the choice of x and y is always possible and (ii) that the result $[x + y]$ does not depend on the choices of x and y, as long as $[x] = a$ and $[y] = b$.

Let us first prove (i). This is obvious, since we could, for example, choose $x = a$ and $y = b$.

Let us now prove (ii). If x' and y' are two other integers, so that $[x] = [x'] = a$ and $[y] = [y'] = b$, then we must have

$$\begin{aligned} x &= rn + a \\ y &= sn + b \\ x' &= r'n + b \\ y' &= s'n + b \end{aligned}$$

for some integers r, r', s, s'. But then

$$(x + y) - (x' + y') = (r - r' + s - s')n,$$

so that the remainder of $x + y$ after dividing by n is the same as the remainder of $x' + y'$ after dividing by n. Thus $[x + y] = [x' + y']$, so that the choices of x and y are irrelevant. □

Definition 2. (Negation) For $a \in \mathbb{Z}_n$, define $-a = [-a]$.

Example 2. Let $n = 3$, $a = 1$. Then $-a = [-1] = 2$.

Exercise 1. Prove that for any $a \in \mathbb{Z}_n$, $a + (-a) = 0$. Prove that for any $a, b \in \mathbb{Z}_n$, $a + b = b + a$. Prove that for any $a, b, c \in \mathbb{Z}_n$, $a + (b + c) = (a + b) + c$. Prove that $a + 0 = 0$ for all $a \in \mathbb{Z}_n$. Finally, prove that if $a = 1$, then $-a = n - 1$.

Definition 3. (Multiplication on $\mathbb{Z}_n$) For $a, b \in \mathbb{Z}_n$, let x and y be integers such that $[x] = a$ and $[y] = b$. The product $a \cdot b$ is then defined to be $[xy]$.

Exercise 2. State and prove a theorem, showing that multiplication is well-defined. Prove that for any $a, b \in \mathbb{Z}_n$, $a \cdot b = b \cdot a$. Prove that for any $a, b, c \in \mathbb{Z}_n$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Prove that $a \cdot 1 = a$. Finally, prove that $a \cdot (b + c) = a \cdot b + a \cdot c$, for all $a, b, c \in \mathbb{Z}_n$.

Definition 4. (Multiplicative inverse). Let $a \in \mathbb{Z}_n$. An element $b \in \mathbb{Z}_n$ is called a *multiplicative inverse of* a, if $a \cdot b = 1$.

Proposition 1. *If a multiplicative inverse of $a \in \mathbb{Z}_n$ exists, it is unique.*

Proof. Let $b, b' \in \mathbb{Z}_n$ be such that $a \cdot b = a \cdot b' = 1$. But then

$$\begin{aligned} b' &= 1 \cdot b' = (a \cdot b) \cdot b' \\ &= a \cdot (b \cdot b') = a \cdot (b' \cdot b) \\ &= (a \cdot b') \cdot b = 1 \cdot b = b \end{aligned}$$

so that $b = b'$. □

Fact 1. *Let r and s be integers. Then there exist integers k and l so that*

$$k \cdot r + l \cdot s = g.c.d(r, s),$$

where $g.c.d(r, s)$ stands for the Greatest Common Divisor.

Example 3. Let $r = 4$ and $s = 6$. Then $g.c.d(4, 6) = 2$, and $(-1) \cdot 4 + 1 \cdot 6 = 2$, so that $k = -1$, $l = 1$. Let $r = 4$, $s = 7$. Then $g.c.d(4, 7) = 1$, and indeed $1 = 2 \cdot 4 + (-1) \cdot 7$, so that $k = 2$ and $l = -1$.

Exercise 3. Show that $b \cdot 0 = 0$ for all $b \in \mathbb{Z}_n$. Prove that if $a = 0$, then a cannot have a multiplicative inverse.

Definition 5. A nonzero element a of $\mathbb{Z}_n$ so that $a \cdot b = 0$ for some non-zero $b \in \mathbb{Z}_n$ is called a *zero divisor.*

Lemma 1. *If $a \in \mathbb{Z}_n$ is a zero divisor, then a cannot have a multiplicative inverse.*

Proof. Assume that a is a zero divisor, so that $a \cdot b = 0$ for some $b \neq 0$. Let c be a multiplicative inverse of a. Then $0 = c \cdot 0 = c \cdot (a \cdot b) = (c \cdot a) \cdot b = 1 \cdot b = b$, which contradicts the assumption that $b \neq 0$. □

Theorem 2. *(i) If n is a prime number, then every non-zero element $a \in \mathbb{Z}_n$ has an inverse. (ii) Conversely, if every nonzero element of $\mathbb{Z}_n$ has an inverse, then n is a prime number.*

Proof. Let us first prove (i). Assume that $a \neq 0$ is in $\mathbb{Z}_n$. Since n is prime, a (which satisfies $0 \leq a \leq n - 1$) and n are relatively prime, i.e., $g.c.d(a, n) = 1$. Thus for some integers k and l, we have

$$k \cdot a + l \cdot n = g.c.d(a, n) = 1,$$

so that

$$k \cdot a = 1 - l \cdot n.$$

Let $b = [k]$. Then

$$a \cdot b = [k \cdot a] = [1 - l \cdot n] = 1,$$

since $l \cdot n$ is obviously divisible by n. Thus b is a multiplicative inverse of a.

We assume now that (ii) fails. Thus we assume that for some non-prime n, every nonzero element has a multiplicative inverse. We'll show this cannot happen, so that (ii) cannot fail. Since n is not prime, $n = k \cdot l$ with $k, l < n$. Let $a = k$, $b = l$. Then $a \cdot b = [kl] = [n] = 0$. On the other hand, neither a nor b is zero. Thus a is a zero divisor. But then a cannot have a multiplicative inverse, by Lemma 1. □

Remark 2. The preceeding theorem shows that $\mathbb{Z}_n$ is a *field* if and only if n is a prime number.