Section 1.4

Integers Modulo $n$

1.4.1 Definition. Let $a$ and $n > 0$ be integers. The set of all integers which have the same remainder as $a$ when divided by $n$ is called the \textit{congruence class of $a$ modulo} $n$, and is denoted by $[a]_n$, where

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$$

The collection of all congruence classes modulo $n$ is called the \textit{set of integers modulo} $n$, and is denoted by $\mathbb{Z}_n$.

An element of $[a]_n$ is called a \textit{representative of the congruence class}.

1.4.2 Proposition. Let $n$ be a positive integer, and let $a, b$ be any integers. Then the addition and multiplication of congruence classes are well-defined:

$$[a]_n + [b]_n = [a + b]_n, \quad [a]_n \cdot [b]_n = [ab]_n$$

1.4.3 Definition. If $[a]_n$ belongs to $\mathbb{Z}_n$, and $[a]_n \cdot [b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a \textit{divisor of zero}. 

### ADDITION AN MULTIPLICATION OF CONGRUENCE CLASSES

#### Addition

**Additive Inverse**

If $[a]_n, [b]_n \in \mathbb{Z}_n$ and $[a]_n + [b]_n = [0]_n$, then $[b]_n$ is called the \textit{additive inverse} of $[a]_n$.

### ARITHMETIC WITH CONGRUENCES

For any elements $[a]_n, [b]_n, [c]_n$ in $\mathbb{Z}_n$, the following laws hold.

<table>
<thead>
<tr>
<th>Property</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associativity</td>
<td>$([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$</td>
</tr>
<tr>
<td>Commutativity</td>
<td>$[a]_n + [b]_n = [b]_n + [a]_n$</td>
</tr>
<tr>
<td>Distributivity</td>
<td>$[a]_n \cdot ([b]_n + [c]_n) = ([a]_n \cdot [b]_n) + ([a]_n \cdot [c]_n)$</td>
</tr>
<tr>
<td>Identities</td>
<td>$[a]_n + [0]_n = [a]_n$</td>
</tr>
<tr>
<td>Additive Inverses</td>
<td>$[a]_n + [-a]_n = [0]_n$</td>
</tr>
</tbody>
</table>
MULTIPlicative INVERSes

1.4.4 Definition. If \([a]_n\) belongs to \(\mathbb{Z}_n\), and \([a]_n \cdot [b]_n = [1]_n\), then \([b]_n\) is called a multiplicative inverse of \([a]_n\) and is denoted by \([a]_n^{-1}\).

In this case, we say that \([a]_n\) is an invertible element of \(\mathbb{Z}_n\), or \(a\) is a unit of \(\mathbb{Z}_n\).

DIVISORS OF ZERO AND MULTIPlicative INVERSes

1.4.5 Proposition. Let \(n\) be a positive integer.

(a) The congruence class \([a]_n\) has a multiplicative inverse in \(\mathbb{Z}_n\) if and only if \(\gcd(a, n) = 1\).

(b) Any nonzero element of \(\mathbb{Z}_n\) either has a multiplicative inverse or is a divisor of zero.

A CorOLLARY

1.4.6 Corollary. The following conditions on the modulus \(n > 0\) are equivalent.

(1) The number \(n\) is prime.
(2) \(\mathbb{Z}_n\) has no divisors of zero except \([0]_n\).
(3) Every nonzero element of \(\mathbb{Z}_n\) has a multiplicative inverse.

Euler’s \(\varphi\)-FUNCTIon

1.4.7 Definition. Let \(n\) be a positive integer. The number of positive integers less than or equal to \(n\) which are relatively prime to \(n\) will be denoted by \(\varphi(n)\). This function is called Euler’s \(\varphi\)-function, or the totient function.

A FORMula For The Euler \(\varphi\)-FUNCTION

1.4.8 Proposition. If the prime factorization of \(n\) is \(n = p_1^{a_1}p_2^{a_2} \cdots p_k^{a_k}\), where \(a_i > 0\) for \(1 \leq i \leq k\), then

\[
\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).
\]

THE SET OF UNITS

1.4.9 Definition. The set of units of \(\mathbb{Z}_n\), the congruence classes \([a]\) such that \(\gcd(a, n) = 1\), will be denoted by \(\mathbb{Z}_n^\times\).

1.4.10 Proposition. The set \(\mathbb{Z}_n^\times\) of units of \(\mathbb{Z}_n\) is closed under multiplication.
### Euler’s Theorem

1.4.11 Theorem (Euler). If \( \gcd(a, n) = 1 \), then \( a^{\phi(n)} \equiv 1 \pmod{n} \).

### Fermat’s Little Theorem

The following corollary of Euler’s Theorem is known as “Fermat’s Little Theorem.”

1.4.12 Corollary (Fermat). If \( p \) is a prime number, then for any integer \( a \) we have \( a^p \equiv a \pmod{p} \).