Section 1.4

Integers Modulo *n*

SET OF 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 ***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 ***set of integers modulo*** n, and is denoted by $\mathbb{Z}_n$.

An element of $[a]_n$ is called a ***representative of the congruence class***.

ADDITION AN MULTIPLICATION OF CONGRUENCE CLASSES

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:

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

ADDITIVE INVERSE

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

Associativity	$([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$ $([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$
Commutativity	$[a]_n + [b]_n = [b]_n + [a]_n$ $[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$
Distributivity	$[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$
Identities	$[a]_n + [0]_n = [a]_n$ $[a]_n \cdot [1]_n = [a]_n$
Additive Inverses	$[a]_n + [-a]_n = [0]_n$

A DIVISOR OF ZERO

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 ***divisor of zero***.

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 φ-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 top n will be denoted by $\varphi(n)$. This function is called ***Euler's φ-function***, or the ***totient function***.

A FORMULA FOR THE EULER φ-FUNCTION

1.4.8 Proposition. If the prime factorization of n is $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $\alpha_i > 0$ 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 $a^{\varphi(n)} \equiv 1 \pmod{n}$.

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 $a^p \equiv a \pmod{p}$.