Reading Summary 2.2 and 2.3

Evan Hughes

January 2023

2.2 Properties of Modular Arithmetic

Review of Properties of $\mathbb{Z}$

For all $a, b, c \in \mathbb{Z}$,

1. Closure under addition: $a + b \in \mathbb{Z}$
2. Associative addition: $(a + b) + c = a + (b + c)$
3. Commutative addition: $a + b = b + a$
4. Additive Identity: $a + 0 = a$
5. There is a solution to $a + x = 0$ in $\mathbb{Z}$.
6. Closure under multiplication: $ab \in \mathbb{Z}$
7. Associative multiplication: $(ab)c = a(bc)$
8. Distributive Law: $a(b + c) = ab + ac$
9. Commutative multiplication: $ab = ba$
10. Multiplicative Identity: $a \cdot 1 = a$
11. If $ab = 0$, then $a = 0$ or $b = 0$.

Theorem 2.7

For any classes $[a]$,$[b]$,$[c]$ of $\mathbb{Z}$,

1. $[a] \oplus [b] \in \mathbb{Z}$
2. $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$
3. $[a] \oplus [b] = [b] \oplus [a]$
4. $[a] \oplus [0] = [a]$
5. $[a] \oplus X = [0]$ has a solution in $[\mathbb{Z}]$.
6. $[a] \odot [b] \in \mathbb{Z}$
7. $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$
8. $[a] \odot ([b] \oplus [c]) = [a] \odot [b] \oplus [a] \odot [c]$
9. $[a] \odot [b] = [b] \odot [a]$
10. $[a] \odot [1] = [a]$

Example:

(from the book) in $\mathbb{Z}_5$, $[3]^2 = [3] \odot [3] = [4] \in \mathbb{Z}_5$ and $[3]^4 = [3] \odot [3] \odot [3] \odot [3] = [1] \in \mathbb{Z}_5$.

2.3 The Structure of $\mathbb{Z}_p$ (p Prime) and $\mathbb{Z}_n$

New Notation: Basically we are writing classes and arithmetic of them in the way we write normal integers. The context will make it clear which world we are in.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Figure 1: New notation for $\mathbb{Z}_3$

The structure of $\mathbb{Z}_p$ when p is Prime

Not all $\mathbb{Z}_n$ share the same properties of $\mathbb{Z}$, in $\mathbb{Z}$ the product of and nonzero integer is nonzero, however in $\mathbb{Z}_6$ we have $2 \cdot 3 = 0$. On the other hand in $\mathbb{Z}_5$ we have that the product of nonzero elements is always nonzero. $\mathbb{Z}_5$ has, for any $a \neq 0$, the equation $ax = 1$ has a solution in $\mathbb{Z}_5$.

Theorem 2.8

If $p > 1$ is an integer, the following conditions are equivalent:

1. p is prime
2. For any $a \neq 0$, the equation $ax = 1$ has a solution in $\mathbb{Z}_p$.
3. Whenever $bc = 0$ in $\mathbb{Z}_p$, at least one of b and c is zero.

Example:

In $\mathbb{Z}_3$ if $a = 2$ then $ax = 1$ has a solution in $\mathbb{Z}_3$ of 2. And $0 \cdot 1 = 0$ and $0 \cdot 2 = 0$ and $1 \cdot 2 = 2$.

The structure of $\mathbb{Z}_n$

When n is not prime, the equation doesn't have to have a solution to $ax = 1$. For an example, the equation $2x = 1$ has no solution in $\mathbb{Z}_4$

Theorem 2.9

Let a and n be integers with $n > 1$. Then

The equation $[a]x = [1]$ has a solution in $\mathbb{Z}_n$ if and only if $(a, n) = 1$ in $\mathbb{Z}$.

Units and Zero Divisors

An element a in $\mathbb{Z}_n$ is a unit if $[a]x = [1]$ has a solution in $\mathbb{Z}_n$. In other words a is a unit if there is another element b in $\mathbb{Z}_n$ such that $ab = 1$. In this case we say that b is the inverse of a.

Theorem 2.10

Let a and n be integers with $n > 1$. Then

$[a]$ is a unit of $\mathbb{Z}_n$ if and only if $(a, n) = 1$ in $\mathbb{Z}$.

A nonzero element a in $\mathbb{Z}_n$ is a zero divisor if $[a]x = [0]$ has a *nonzero* solution in $\mathbb{Z}_n$(That is, if there is a nonzero element c in $\mathbb{Z}_n$ such that $ac = 0$).