

MTHSC 412 SECTION 2.3 – THE STRUCTURE OF $\mathbb{Z}_p$ WHEN p IS PRIME

Kevin James

EXAMPLE

First, let us consider a nonprime example. Let $n = 6$. Note that $[2] \neq [0]$ and $[3] \neq [0]$, but $[2][3] = [0]$. This is very different from $\mathbb{Z}$.

THEOREM

If $p > 1$ is an integer then the following are equivalent.

- ① *p is prime.*
- ② *For any $[0] \neq [a] \in \mathbb{Z}_p$, the equation $[a][x] = 1$ has a solution in $\mathbb{Z}_p$.*
- ③ *Whenever $[a][b] = 0$, either $[a] = 0$ or $[b] = 0$.*

PROOF.

(1 $\Rightarrow$ 2): Suppose that p is prime and that $[0] \neq [a] \in \mathbb{Z}_p$.

Then $(a, p) = 1$.

Thus there are $x, y \in \mathbb{Z}$ such that

$$ax + py = 1 \Rightarrow ax - 1 = p(-y) \Rightarrow ax \equiv 1 \pmod{p}.$$

Thus $[a][x] = [1]$.

(2 $\Rightarrow$ 3): Suppose that (2) holds and that $[a][b] = 0$.

If $[a] = 0$, then the theorem holds.

Suppose that $[a] \neq 0$.

By (2), there is $[x] \in \mathbb{Z}_p$ such that $[a][x] = 1$.

$$\text{So, } [a][b] = 0 \Rightarrow [b] = [b]([a][x]) = ([b][a])[x] = ([a][b])[x] = 0[x] = 0..$$

(3 $\Rightarrow$ 1): Suppose that (3) holds and that $d|p$.

Then $p = dk$ for some $k \in \mathbb{Z}$.

Thus, $[d][k] = [p] = [0]$.

So, by (3), $[d] = 0 \Rightarrow p|d \Rightarrow d = \pm p$ or

$$[k] = 0 \Rightarrow p|k \Rightarrow k = \pm p \Rightarrow d = \pm 1.$$

Thus p is prime.

COROLLARY

Let $p > 1$ be prime. For any $[0] \neq [a] \in \mathbb{Z}_p$ and $[b] \in \mathbb{Z}_p$, the equation $[a]x = [b]$ has a unique solution in $\mathbb{Z}_p$.

PROOF.

(Existence): From our theorem, we know that there is a solution to $[a]x = [1]$, say $x = [u]$.

That is, $[a][u] = 1$.

Thus $[a][ub] = [b]$.

So, $x = [ub]$ is a solution to $[a]x = [b]$ in $\mathbb{Z}_p$.

(Uniqueness): Suppose that $[u]$ and $[w]$ are both solutions.

Then $[a][u] = [a][w]$ in $\mathbb{Z}_p$.

Thus $[a]([u] - [w]) = 0$ in $\mathbb{Z}_p$.

Since $[a] \neq [0]$, $[u] - [w] = 0 \Rightarrow [u] = [w]$ in $\mathbb{Z}_p$. □

COROLLARY

Suppose that $a, b, n \in \mathbb{Z}$ with $n > 1$ and $(a, n) = 1$. Then the equation $[a]x = [b]$ has a solution in $\mathbb{Z}_n$.

PROOF.

Since $(a, n) = 1$, there exists $z, y \in \mathbb{Z}$ such that $az + ny = 1 \Rightarrow az - 1 = n(-y)$.

Thus, $[a][z] = 1 \Rightarrow [a][zb] = [b]$ in $\mathbb{Z}_n$.

So, $x = [zb]$ is a solution. □

THEOREM

Suppose that $a, b, n \in \mathbb{Z}$ with $n > 1$ and $(a, n) = d$.

- 1 The equation $[a]x = [b]$ has a solution in $\mathbb{Z}_n$ if and only if $d \mid b$.
- 2 In the case that $d \mid b$ the equation $[a]x = [b]$ has d distinct solutions in $\mathbb{Z}_n$.

PROOF.

Exercise. □