2.3 The Structure of $\mathbb{Z}/p\mathbb{Z}$ (p Prime) and $\mathbb{Z}/m\mathbb{Z}$

New Notation

So far, we have been using $[a]$ to denote the congruence class of a modulo m. But this notation can be cumbersome, so we generally drop the brackets when it is clear from context that we are talking about congruence classes. For example, we can say "$x = 3$ is a solution to $2x = 1$ in $\mathbb{Z}/5\mathbb{Z}$" rather than "$x = [3]$ is a solution to $[2]x = [1]$ in $\mathbb{Z}/5\mathbb{Z}$."

This will usually cause no confusion. However, it is worth remembering that exponents are normal integers, not elements of $\mathbb{Z}/m\mathbb{Z}$. For example, consider $[3]^3$ in $\mathbb{Z}/5\mathbb{Z}$; we will now be writing that as 3^3, but the two 3's are very different. The lower 3 is really $[3]$, an element of $\mathbb{Z}/5\mathbb{Z}$, and can therefore be replaced with any other element of $[3]$. The upper 3 is the integer 3, and cannot be replaced with another element of $[3]$. That is, we have $3^3 = 8^3 = 13^3$ in $\mathbb{Z}/5\mathbb{Z}$, but you can check that $3^3 \neq 3^8$ in $\mathbb{Z}/5\mathbb{Z}$.

Inverses and units in $\mathbb{Z}/m\mathbb{Z}$

Definition. We say that $a, b \in \mathbb{Z}/m\mathbb{Z}$ are *inverses* if $ab = 1$. If a has an inverse, we say that a is a *unit*.

Equivalently, a is a unit if the equation $ax = 1$ has a solution.

Example. Note that 3 and 5 are inverses in $\mathbb{Z}/7\mathbb{Z}$ because $3 \cdot 5 = 1$ in $\mathbb{Z}/7\mathbb{Z}$. Therefore 3 and 5 are both units in $\mathbb{Z}/7\mathbb{Z}$.

Example. You can check (by brute force, or using the following theorem) that 3 does not have an inverse in $\mathbb{Z}/6\mathbb{Z}$. Therefore 3 is not a unit in $\mathbb{Z}/6\mathbb{Z}$.

The following theorem allows us to easily determine whether a is a unit in $\mathbb{Z}/m\mathbb{Z}$.

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

In other words, $[a]$ is a unit in $\mathbb{Z}/m\mathbb{Z}$ if and only if $(a, m) = 1$.

Proof. First suppose that $(a, m) = 1$. By Bézout's identity, there exist $u, v \in \mathbb{Z}$ such that $au + mv = 1$. It follows that $x = [u]$ is a solution to $[a]x = [1]$.

Conversely, suppose that $[a]x = [1]$ has a solution $x = [u]$ in $\mathbb{Z}/m\mathbb{Z}$. This means that $ax \equiv 1 \pmod{m}$. In other words, $ax = 1 + mk$ for some $k \in \mathbb{Z}$. Thus 1 can be written as a linear combination of a and m, so $(a, m) = 1$. $\square$

One of the nice things about units is that they have the cancellation property:

Theorem. *Let a be a unit in $\mathbb{Z}/m\mathbb{Z}$. If $b, c \in \mathbb{Z}/m\mathbb{Z}$ such that $ab = ac$, then $b = c$.*

Proof. Let u be the inverse of a. Then

$$b = 1b = (ua)b = u(ab) = u(ac) = (ua)c = 1c = c. \qquad \square$$

Structure of $\mathbb{Z}/p\mathbb{Z}$ for p prime

Theorem. *If $p > 1$ is an integer, then the following are equivalent:*

(1) p is prime.

(2) For any $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, the equation $ax = 1$ has a solution in $\mathbb{Z}/p\mathbb{Z}$.

(3) If $bc = 0$ in $\mathbb{Z}/p\mathbb{Z}$, then $b = 0$ or $c = 0$.

Proof. We prove (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1).

Suppose p is prime. Fix any $[a] \neq [0]$ in $\mathbb{Z}/p\mathbb{Z}$. Then $p \nmid a$, so $(a, p) = 1$. By the previous theorem, $ax = 1$ has a solution in $\mathbb{Z}/p\mathbb{Z}$. Thus (1) $\Rightarrow$ (2).

Now assume (2) holds. Suppose $bc = 0$ and $b \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. By (2), there exists some $u \in \mathbb{Z}/p\mathbb{Z}$ such that $bu = 1$. Hence

$$c = 1c = (bu)c = u(bc) = u \cdot 0 = 0,$$

which proves that (2) $\Rightarrow$ (3).

Finally, we prove that (3) $\Rightarrow$ (1). Assume (3) holds. By Theorem 1.5 from the textbook, we can prove that p is prime by proving that if $p \mid bc$, then $p \mid b$ or $p \mid c$. If $p \mid bc$, then $[b][c] = [0]$ in $\mathbb{Z}/p\mathbb{Z}$. By (3), it follows that $[b]$ or $[c]$ is $[0]$, so $p \mid b$ or $p \mid c$. $\square$

Zero divisors in $\mathbb{Z}/m\mathbb{Z}$

Definition. A nonzero element a of $\mathbb{Z}/m\mathbb{Z}$ is called a *zero divisor* if the equation $ax = 0$ has a nonzero solution.

Example. 2 and 3 are zero divisors in $\mathbb{Z}/6\mathbb{Z}$ because $2 \cdot 3 = 0$. Also, 2 is a zero divisor in $\mathbb{Z}/4\mathbb{Z}$ because $2 \cdot 2 = 0$.

Our theorem about $\mathbb{Z}/p\mathbb{Z}$ says that $\mathbb{Z}/p\mathbb{Z}$ has no zero divisors if p is prime. Knowing that $\mathbb{Z}/p\mathbb{Z}$ has no zero divisors is a very nice fact. To see why, remember that you're used to solving real-number equations by saying that if, say, $f(X)g(X)h(X) = 0$, then $f(X) = 0$ or $g(X) = 0$ or $h(X) = 0$. The reason this is valid is because $\mathbb{R}$ has no zero divisors. Now that we know $\mathbb{Z}/p\mathbb{Z}$ has no zero divisors, you can do the same thing to solve equations in $\mathbb{Z}/p\mathbb{Z}$. For example, suppose you want to find all solutions in $\mathbb{Z}/7\mathbb{Z}$ to $X^2 - 1 = 0$. You can factor it as $(X + 1)(X - 1) = 0$ and conclude that $X = \pm 1$.

You cannot do this in $\mathbb{Z}/m\mathbb{Z}$ if $\mathbb{Z}/m\mathbb{Z}$ has zero divisors. For example, there are four solutions to $(X + 1)(X - 1) = 0$ in $\mathbb{Z}/8\mathbb{Z}$.

You will prove for homework that every nonzero element of $\mathbb{Z}/m\mathbb{Z}$ is either a unit or a zero divisor.