## 2.2 Modular Arithmetic

We have already noted that addition works nicely with congruences. This inspires us to define addition of congruence classes:

**Definition.** We define addition in $\mathbb{Z}/m\mathbb{Z}$ by $[a] + [c] = [a + c]$.

Note that the plus sign on the left-hand side denotes addition in $\mathbb{Z}/m\mathbb{Z}$, while the plus sign on the right-hand side denotes addition in $\mathbb{Z}$. In order to distinguish these, the textbook temporarily uses $\oplus$ to denote addition in $\mathbb{Z}/m\mathbb{Z}$ before switching to the standard notation that simply uses $+$.

We need to check that addition in $\mathbb{Z}/m\mathbb{Z}$ is well-defined. For example, in $\mathbb{Z}/4\mathbb{Z}$,

$$\{\dots, -3, 1, 5, \dots\} = [1] = [5]$$

and

$$\{\dots, -2, 2, 6, \dots\} = [2] = [6].$$

So what is $\{\dots, -3, 1, 5, \dots\} + \{\dots, -2, 2, 6, \dots\}$? We could calculate it as

$$\{\dots, -3, 1, 5, \dots\} + \{\dots, -2, 2, 6, \dots\} = [1] + [2] = [3]$$

or as

$$\{\dots, -3, 1, 5, \dots\} + \{\dots, -2, 2, 6, \dots\} = [5] + [6] = [11]$$

or as

$$\{\dots, -3, 1, 5, \dots\} + \{\dots, -2, 2, 6, \dots\} = [1] + [6] = [7].$$

Fortunately, all of these methods give us the same answer, since $[3] = [11] = [7]$. But how do we know that we will always get the same answer?

We have previously seen that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$. We can rewrite this theorem in terms of congruence classes: if $[a] = [b]$ and $[c] = [d]$, then $[a+c] = [b+d]$. This proves that addition in $\mathbb{Z}/m\mathbb{Z}$ is well-defined: if $[a] = [b]$ and $[c] = [d]$, then we get the same answer whether we calculate $[a] + [c]$ or $[b] + [d]$.

Our theorem from the previous section also says that subtraction and multiplication are well-behaved in congruences. Therefore we can define subtraction and multiplication in $\mathbb{Z}/m\mathbb{Z}$, and prove that these operations are well-defined in the same way.

**Definition.** We define subtraction in $\mathbb{Z}/m\mathbb{Z}$ by $[a] - [c] = [a - c]$. We define multiplication in $\mathbb{Z}/m\mathbb{Z}$ by $[a] \cdot [c] = [ac]$. As with ordinary multiplication, we can omit the dot, or we can use exponential notation as usual to denote repeated multiplication in $\mathbb{Z}/m\mathbb{Z}$, e.g., $[a]^3 = [a][a][a]$.
**Example.** The textbook contains addition and multiplication tables for $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$.

Since addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$ are based on addition and multiplication in $\mathbb{Z}$, it is unsurprising that many nice properties of integer addition/multiplication continue to hold for modular addition/multiplication.

**Theorem.** *For any* $[a], [b], [c] \in \mathbb{Z}/m\mathbb{Z}$*,*

1. $[a] + ([b] + [c]) = ([a] + [b]) + [c]$.
2. $[a] + [b] = [b] + [a]$.
3. $[a] + [0] = [a] = [0] + [a]$.
4. *The equation* $[a] + X = [0]$ *has a solution in* $\mathbb{Z}/m\mathbb{Z}$.
5. $[a]([b][c]) = ([a][b])[c]$.
6. $[a]([b] + [c]) = [a][b] + [a][c]$ *and* $([a] + [b])[c] = [a][c] + [b][c]$.
7. $[a][b] = [b][a]$.
8. $[a][1] = [a] = [1][a]$.

*Proof.* The proofs are all directly from the definitions of modular addition/multiplication, along with the corresponding properties of integer addition/multiplication. As an example, we prove the first property:

$$[a] + ([b] + [c]) = [a] + [b + c] = [a + (b + c)] = [(a + b) + c] = [a + b] + [c] = ([a] + [b]) + [c].$$

The other properties are proven similarly. Make sure you can prove all of them. $\square$

Note that since $[a] + ([b] + [c]) = ([a] + [b]) + [c]$, we can write $[a] + [b] + [c]$ with no risk of ambiguity.

**Example.** Find all solutions in $\mathbb{Z}/6\mathbb{Z}$ to the equation $X^2 - X = [0]$.

There are only six elements of $\mathbb{Z}/6\mathbb{Z}$, so we can check whether they are solutions by brute force: $[0]^2 - [0] = [0]$, $[1]^2 - [1] = [0]$, $[2]^2 - [2] = [2]$, $[3]^2 - [3] = [6] = [0]$, $[4]^2 - [4] = [12] = [0]$, $[5]^2 - [5] = [20] = [2]$. Therefore the solutions are $[0], [1], [3], [4]$.

Note that this is one area where modular arithmetic is very different from real-number arithmetic. A real quadratic polynomial can have at most two roots, yet $X^2 - X$ has four roots in $\mathbb{Z}/6\mathbb{Z}$. Furthermore, we cannot find the roots of the modular polynomial by factoring: even though $X^2 - X = X(X - [1])$, we cannot conclude that $X = [0], [1]$ are the only roots.