Chapter 27 Modular Arithmetic

Now that we have introduced $\mathbb{Z}_n$ (a collection of equivalence classes), can we treat it like a number system and do things like add and multiply.

Question How do we define $[r]_n + [s]_n$ or $[r]_n \cdot [s]_n$ or $-[r]_n$ or $[r]_n^{-1}$?

Example Consider $[7]_6$ and $[4]_6$. Could we define $[7]_6 \cdot [4]_6$ to be $[28]_6$? Notice $[7]_6 = [19]_6$. So couldn't $[7_6] \cdot [4]_6$ be $[76]_6$? Is that ok or are we getting different outputs for the same input? What about $[7]_6 + [4]_6$? Is it $[11]_6$ or $[23]_6$?

Proposition Let $m : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ be given by $m([r]_n, [s]_n) = [rs]_n$. Then m is a well-defined function. We'll take this to be our definition of multiplication in $\mathbb{Z}_n$. That is $[r]_n \cdot [s]_n = [rs]_n$.

Proof We must show (1) for each $x \in \mathbb{Z}_n \times \mathbb{Z}_n$, there exists $y \in \mathbb{Z}_n$ such that $m(x) = y$ and (2) if $x = x'$, then $m(x) = m(x')$.

Let $x \in \mathbb{Z}_n \times \mathbb{Z}_n$. Then $x = ([r]_n, [s]_n)$ for some $r, s \in \mathbb{Z}$. Since $rs \in \mathbb{Z}$, $m(x) = [rs]_n \in \mathbb{Z}_n$.

Let $x = ([r]_n, [s]_n)$ and $x = ([u]_n, [v]_n)$ be two representations of x for some $r, s, u, v \in \mathbb{Z}$ such that $r \equiv u \pmod{n}$ and $s \equiv v \pmod{n}$.

Our goal is to show $[rs]_n = [uv]_n$. To do this we must show $rs \equiv uv \pmod{n}$, which means showing $n \mid (rs - uv)$. Since $r \equiv u \pmod{n}$ and $s \equiv v \pmod{n}$, then exist $j, k \in \mathbb{Z}$ such that $r - u = nj$ and $s - v = nk$. Observe that

$$\begin{aligned} rs - uv &= rs - us + us - uv \\ &= s(r-u) + u(s-v) \\ &= snj + unk \\ &= n(sj + uk). \end{aligned}$$

Since $sj + uk \in \mathbb{Z}$, $n \mid (rs - uv)$.

Recall that $\forall\ m, n \in \mathbb{Z}$ not both zero, $\exists\ k, l \in \mathbb{Z}$ such that $\gcd(m,n) = km + ln$.

Corollary Let $n \in \mathbb{Z}$ with $n > 1$. Then for every $a \in \mathbb{Z}$ with $\gcd(a,n) = 1$, there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$.

Proof Let $a \in \mathbb{Z}$ with $\gcd(a,n) = 1$. Then $1 = ak + nl$ for some $k, l \in \mathbb{Z}$. Observe that $1 - ak = nl$, which implies $n \mid (1-ak)$, and so $ak \equiv 1 \pmod{n}$. Therefore $\exists\ b \in \mathbb{Z}$ (namely $b = k$) so that $ab \equiv 1 \pmod{n}$.

Def Let $n \in \mathbb{Z}$ with $n > 1$. Let $a \in \mathbb{Z}$ with $\gcd(a,n) = 1$. We say that $b \in \mathbb{Z}$ is the reciprocal modulo n of a if $ab \equiv 1 \pmod{n}$ and write $b \equiv a^{-1} \pmod{n}$.

Lemma Let $n \in \mathbb{Z}$ with $n > 1$. Suppose $a, c \in \mathbb{Z}$ are such that $a \equiv c \pmod{n}$. Then

① $\gcd(a,n) = 1$ if and only if $\gcd(c,n) = 1$.

② if $ab \equiv 1 \pmod{n}$ and $cd \equiv 1 \pmod{n}$, then $b \equiv d \pmod{n}$.

This lemma tells us that $[a]_n^{-1} = [b]_n$ where $b \in \mathbb{Z}$ is the reciprocal of a mod n is a well-

defined function with the property $[a]_n^{-1} \cdot [a]_n = [1]_n$.

Proof ① ($\Rightarrow$) Suppose $\gcd(c,n) \neq 1$. We must show $\gcd(a,n) \neq 1$. Let $k = \gcd(c,n) > 1$. We claim k is a divisor of a and n, and since $\gcd(a,n)$ is the greatest common divisor of a and n, thus will show $\gcd(a,n) \geq k > 1$. Since $a \equiv c \pmod n$ $a = nj + c$ for some $j \in \mathbb{Z}$. Since $k \mid n$, $k \mid nj$. Since $k \mid c$ and $k \mid nj$, $k \mid a$. Thus k is a divisor of a and n. The ($\Leftarrow$) is the same.

② Observe that $ab \equiv 1 \pmod n$ means $[ab]_n = [1]_n$ and similarly we have $[cd]_n = [1]_n$. and $[a]_n = [c]_n$. Therefore

$$\begin{aligned} [b]_n &= [b \cdot 1]_n \\ &= [b\,cd]_n \\ &= [b\,ad]_n \\ &= [ab\,d]_n \\ &= [1 \cdot d]_n \\ &= [d]_n, \end{aligned}$$

which means $b \equiv d \pmod n$.

Example Find reciprocals modulo 7 of 3, 5, and 6.

① $[3]_7^{-1} = [5]_7$ since $[3]_7 \cdot [5]_7 = [15]_7 = [1]_7$.

② $[5]_7^{-1} = [3]_7$

③ $[6]_7^{-1} = [6]_7$ since $[6]_7 \cdot [6]_7 = [36]_7 = [1]_7$.

Example Which elements of $\mathbb{Z}_6$ have reciprocals modulo 6? Only $[1]_6$ and $[5]_6$

since $\gcd(1,6) = 1 = \gcd(5,6) = 1$ but

$\gcd(m,6) \neq 1$ when $m = 0, 2, 3, 4$.