Chapter 2: Congruence in $\mathbb{Z}$ and Modular Arithmetic

Modular arithmetic is "clock" arithmetic. It is essentially doing arithmetic only using remainders. We introduce a new "equality" on $\mathbb{Z}$ and see how this works.

2.1 Congruence classes:

We begin with the definition that forms the basis for the rest of the chapter.

Def: Let $n \in \mathbb{Z}_{>0}$. We say $a, b \in \mathbb{Z}$ are congruent modulo n and write $a \equiv b \pmod{n}$ if $n \mid (a-b)$.

Examples: 1) $4 \equiv 1 \pmod{3}$

2) $5 \equiv -5 \pmod{10}$

3) $10075610 \equiv 0 \pmod{10}$.

What makes congruence useful to work with is it is an equivalence relation, ie., the following theorem is true.

Theorem 2.1.1: Let $n \in \mathbb{Z}_{>0}$. For all $a, b, c \in \mathbb{Z}$ we have:

1) $a \equiv a \pmod{n}$ (reflexive)

2) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$ (symmetric)

3) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$ (Transitive).

Proof:

1) Clearly we have $n \mid (a-a) = 0$ because every integer divides 0.

2) Suppose $a \equiv b \pmod{n}$. Then $n \mid (a-b)$, so there exists $k \in \mathbb{Z}$ so that $a - b = nk$. Thus, $n(-k) = b - a$ and we have $n \mid (b-a)$, i.e., $b \equiv a \pmod{n}$.

3) Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then there exists $s, t \in \mathbb{Z}$ so that $a - b = ns$ and $b - c = nt$. Adding these equations together we have $a - c = ns + nt = n(s+t)$. Thus, $n \mid (a-c)$ and so $a \equiv c \pmod{n}$. ∎

This result allows us to transfer some important arithmetic properties from "$=$" in $\mathbb{Z}$ to congruence modulo n.

Theorem 2.7.2: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

1) $a + c \equiv b + d \pmod{n}$

2) $ac \equiv bd \pmod{n}$

Proof: 1) Prove in class in groups.

2) We want to show $n \mid (ac - bd)$. Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then exists $s, t \in \mathbb{Z}$ so that $a - b = ns$ and $c - d = nt$. We have

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= (a-b)c + b(c-d) \end{aligned}$$

$= nsc + bnt$

$= n(sc + bt)$.

Thus, $n \mid (ac - bd)$ as desired. ∎

We use this new type of equality to partition $\mathbb{Z}$ into congruence classes.

Def: Let $n \in \mathbb{Z}_{>0}$. For $a \in \mathbb{Z}$ we define the *congruence class of a modulo n*, denoted $[a]_n$ or $[a]$ if n is clear from context, as the collection of integers congruent to a modulo n, i.e.

$$[a]_n = \{ b \in \mathbb{Z} : a \equiv b \pmod{n} \}.$$

Examples: 1) $[0]_n = \{ b \in \mathbb{Z} : b \equiv 0 \pmod{n} \}$

$= \{ b \in \mathbb{Z} : n \mid b \}$.

$= n\mathbb{Z}$.

2) $[1]_5 = \{ b \in \mathbb{Z} : b \equiv 1 \pmod{5} \}$

$= \{ b \in \mathbb{Z} : b \equiv 6 \pmod{5} \}$

$= [6]_5$.

Note we have $[a]_n = \{ b \in \mathbb{Z} : b \equiv a \pmod{n} \}$

$= \{ b \in \mathbb{Z} : b = a + kn \text{ for } k \in \mathbb{Z} \}$

$= \{ a + kn : k \in \mathbb{Z} \}$.

Example:

$$[3]_4 = \{ b \in \mathbb{Z} : b \equiv 3 \pmod 4 \}$$

$$= \{ 3 + k4 : k \in \mathbb{Z} \}$$

$$= \{ \ldots, -9, -5, -1, 3, 7, 10, 13, \ldots \}$$

Theorem 2.1.3: We have $a \equiv b \pmod n$ iff $[a]_n = [b]_n$.

Proof: First, suppose $a \equiv b \pmod n$. Then we have $[a]_n = \{ c \in \mathbb{Z} : a \equiv c \pmod n \}$. However, since we have transitivity of $\equiv$ we have $c \equiv a \pmod n$ iff $c \equiv b \pmod n$. Thus,

$$[a]_n = \{ c \in \mathbb{Z} : a \equiv c \pmod n \}.$$

$$= \{ c \in \mathbb{Z} : b \equiv c \pmod n \}.$$

$$= [b]_n.$$

Now suppose $[a]_n = [b]_n$. Then $a \in [b]_n$ so $a \equiv b \pmod n$. ∎

Theorem 2.1.4: Given $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$, we have

$$[a]_n = [b]_n \text{ or } [a]_n \cap [b]_n = \emptyset.$$

Proof: If $[a]_n \cap [b]_n = \emptyset$ we are done, so assume there exists $c \in [a]_n \cap [b]_n$. Then $a \equiv c \pmod{n}$ and $b \equiv c \pmod{n}$.

Given $d \in [a]_n$, we have $d \equiv a \pmod{n}$
$\equiv c \pmod{n}$
$\equiv b \pmod{n}$.

Thus, $d \in [b]_n$. Similarly, if $e \in [b]_n$, then $e \equiv b \pmod{n}$
$\equiv c \pmod{n}$
$\equiv a \pmod{n}$

so $e \in [a]_n$. Thus, $[a]_n = [b]_n$. ∎

Our next step is to show these congruence classes partition $\mathbb{Z}$ and pick a nice representative for each congruence class.

Cor 2.1.5: Let $n \in \mathbb{Z}_{>1}$.

1) If $a \in \mathbb{Z}$ and r is the remainder when a is divided by n, then $[a]_n = [r]_n$.
2) There are exactly n distinct congruence classes $[0]_n, [1]_n, \ldots, [n-1]_n$.

Proof: 1) Write $a = nq + r$ with $0 \leq r < n$. Then $a - r = nq$

so $a \equiv r \pmod{n}$. Thus, $[a]_n = [r]_n$.

2) Let $a \in \mathbb{Z}$. Then we have $[a]_n = [r]_n$ for r the remainder as in 1). This gives every $[a]_n$ is exactly one of the n listed. We now just need to show these are distinct.

Suppose there exists $0 \leq b < c < n$ so that $[b]_n = [c]_n$.

This gives $b \equiv c \pmod{n}$, ie, $n \mid (c - b)$. This is a contradiction as $0 < c - b < n$. Thus, the congruence classes are distinct. ∎

Given $n \in \mathbb{Z}_{>1}$, we denote the collection of $[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n$ by $\mathbb{Z}/n\mathbb{Z}$, ie.

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

Note the textbook writes this as $\mathbb{Z}_n$. We will NOT use that notation as it is truly horrible notation (we will see at least one reason why later.)

In the next section we will see that we can add and multiply in the set $\mathbb{Z}/n\mathbb{Z}$!

2.2 Modular Arithmetic:

As mentioned before, we now want to define addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$.

We define $[a]_n + [b]_n = [a+b]_n$ and $[a]_n[b]_n = [ab]_n$.

The issue here is that we can have $[a]_n = [c]_n$, so then are these operations well-defined, namely, does the addition and mult. depend on the representative chosen? Before we prove this is okay, lets look at an example.

Example: Let $n = 5$.

$$[2]_5 + [3]_5 = [2+3]_5 = [5]_5 = [0]_5.$$

We also have $[2]_5 = [7]_5$ and $[3]_5 = [-2]_5 = [-7]_5 = [-12]_5$,

so observe

$$[0]_5 = [2]_5 + [3]_5 = [7]_5 + [-12]_5 = [-5]_5 = [0]_5,$$

so it works in this case for addition.

$$[2]_5[3]_5 = [6]_5 = [1]_5$$

We also have

$$[2]_5[3]_5 = [7]_5[8]_5 = [56]_5 = [1]_5$$

so it works ok in this case as well.

Theorem 2.2.1: Let $[a]_n = [b]_n$ and $[c]_n = [d]_n$. Then

$[a]_n + [c]_n = [b]_n + [d]_n$ and $[a]_n [c]_n = [b]_n [d]_n$,

ie., addition and multiplication is well-defined.

Proof: To show $[a]_n + [c]_n = [b]_n + [d]_n$ we must show

$[a+c]_n = [b+d]_n$ and similarly we must show $[ac]_n = [bd]_n$.

Since $[a]_n = [b]_n$, we have $a \equiv b \pmod n$ so there exists

$s \in \mathbb{Z}$ s.t. $a - b = sn$ and similarly there exists $t \in \mathbb{Z}$

s.t. $c - d = tn$. Thus, we have

$$a + c - (b+d) = n(s+t),$$

ie. $$n \mid ((a+c) - (b+d))$$

ie, $$a+c \equiv b+d \pmod n.$$

Thus, $$[a+c]_n = [b+d]_n.$$

For multiplication, we have

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= (a-b)c + b(c-d) \\ &= snc + tnb \\ &= n(sc + tb). \end{aligned}$$

Thus, $ac \equiv bd \pmod n$, ie.

$$[ac]_n = [bd]_n.$$

∎

Example: We can write out addition and multiplication for $\mathbb{Z}/3\mathbb{Z}$:

+	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

·	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

.

cln groups: Write out addition and multiplication tables for $\mathbb{Z}/4\mathbb{Z}$.

We want some basic properties of the addition and multiplication for $\mathbb{Z}/n\mathbb{Z}$.

Theorem 2.2.2: Let $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$.

1) $[a]+[b] \in \mathbb{Z}/n\mathbb{Z}$
2) $[a]+([b]+[c]) = ([a]+[b])+[c]$
3) $[a]+[b] = [b]+[a]$
4) $[a]+[0] = [a] = [0]+[a]$
5) For each $[a] \in \mathbb{Z}/n\mathbb{Z}$, the equation $[a]+x=[0]$ has a solution in $\mathbb{Z}/n\mathbb{Z}$.
6) $[a][b] \in \mathbb{Z}/n\mathbb{Z}$
7) $[a]([b][c]) = ([a][b])[c]$

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

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

9) $[a][b] = [b][a]$

10) $[a][1] = [a] = [1][a]$.

Proof: These are left as exercises. Will let students pick ones to do in groups in class. ∎

Given $k \in \mathbb{Z}_{>0}$, we define

$$[a]^0 = [1]$$

and

$$[a]^k = \underbrace{[a]\cdot[a]\cdots[a]}_{k\text{-times}}.$$

Example: (ISBN Numbers) Each book is given an ISBN-10 number of the form $x_1 - x_2x_3x_4 - x_5x_6x_7x_8x_9 - x_{10}$ where the x_i are single digits. Note if $x_{10} = X$, that X stands for a 10. The x_{10} is a check digit; it is chosen so that

$$10x_1 + 9x_2 + 8x_3 + \cdots + 2x_9 + x_{10} \equiv 0 \pmod{11}.$$

For example, our book has ISBN number 1-111-52962-2.

Observe we have

$$10(1) + 9(1) + 8(1) + 7(1) + 6(5) + 5(2) + 4(9) + 3(6) + 2(2) + 1(2)$$

$= 10 + 9 + 8 + 7 + 30 + 30 + 36 + 18 + 4 + 2$

$= 19 + 15 + 60 + 36 + 24$

$\equiv 8 + 4 + 5 + 3 + 2 \pmod{11}$

$\equiv 1 + 10 \pmod{11}$

$\equiv 0 \pmod{11}$.

So our book has a valid ISBN number.

What if we had transposed two digits? As we wrote

$N = 10x_3 + 9x_2 + 8x_1 + 7x_4 + \cdots + 2x_9 + x_{10}$? We know that

$$10x_1 + 9x_2 + 8x_3 + \cdots + 2x_9 + x_{10} \equiv 0 \pmod{11}.$$

Then,

$$N = (10x_1 + 9x_2 + 8x_3 + \cdots + x_{10}) + 2x_3 - 2x_1$$

$$\equiv 0 + 2(x_3 - x_1) \pmod{11}$$

$$\equiv 2(x_3 - x_1) \pmod{11}.$$

For this to be 0 we must have $11 \mid 2(x_3 - x_1)$. Thus, $11 \mid 2$ or $11 \mid x_3 - x_1$. Since $11 \nmid 2$, we would need $11 \mid x_3 - x_1$. However, $0 \le x_3 \le 9$ and $0 \le x_1 \le 9 \Rightarrow -9 \le -x_1 \le 0$ so $-9 \le x_3 - x_1 \le 9$. Thus, $11 \mid x_3 - x_1$ iff $x_3 - x_1 = 0$, i.e, if $x_3 = x_1$. So we can actually detect there is an error if two numbers are transposed! This works for all transpositions of numbers.

Example: We can solve equations modulo n by first substituting in all possibilities. For example, suppose we want to find solutions of

$$X^2 = [-1]$$

in $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.

In $\mathbb{Z}/3\mathbb{Z}$:
$$[0]_3^2 = [0]_3$$
$$[1]_3^2 = [1]_3$$
$$[2]_3^2 = [4]_3 = [1]_3.$$

In $\mathbb{Z}/3\mathbb{Z}$ we have $[-1]_3 = [2]_3$, so there are no solutions in this case.

What about $\mathbb{Z}/5\mathbb{Z}$? Here we have $[-1]_5 = [4]_5$, so

$$[0]_5^2 = [0]_5$$
$$[1]_5^2 = [1]_5$$
$$[2]_5^2 = [4]_5$$
$$[3]_5^2 = [9]_5 = [4]_5$$
$$[4]_5^2 = [16]_5 = [1]_5.$$

Then, $[2]_5$ and $[3]_5$ are solutions, i.e.,

$$X^2 + [1]_5 = (X - [2]_5)(X - [3]_5)$$
$$= (X + [3]_5)(X + [2]_5)$$

because $-[2]_5 = [3]_5$ and $-[3]_5 = [2]_5$.

2.3 The Structure of $\mathbb{Z}/n\mathbb{Z}$:

Recall in our tables for addition and multiplication tables for $\mathbb{Z}/4\mathbb{Z}$ we saw $[2]_4 \cdot [2]_4 = [0]_4$. Thus, in this set where can multiply two non-zero elements and get zero! This means we have to be very careful about things we normally take for granted. For instance, we can't just cancel. In $\mathbb{Z}$ if we have $ab = ac$, then we have $ab - ac = 0$, i.e., $a(b-c) = 0$. Since in $\mathbb{Z}$ if we multiply two elements and get zero one of the other must be 0, we conclude if $a \neq 0$ then $b = c$. However, consider $\mathbb{Z}/6\mathbb{Z}$. In this set we have

$$[2]_6 [4]_6 = [2]_6 [1]_6$$

but we do NOT have $[4]_6 = [1]_6$.

Def: Let $[a]_n \in \mathbb{Z}/n\mathbb{Z}$. We call $[a]_n$ a *zero divisor* if there exists a nonzero element $[b]_n \in \mathbb{Z}/n\mathbb{Z}$ so that $[a]_n [b]_n = [0]_n$.

Example: We saw above $[2]_6$ and $[3]_6$ are both zero divisors in $\mathbb{Z}/6\mathbb{Z}$.

One thing to notice here is that $\gcd(2,6) = 2 > 1$ and $\gcd(3,6) = 3 > 1$.

Suppose we have $\gcd(a,n) = 1$. Then we know there exists $r, s \in \mathbb{Z}$ so that

$$as + tn = 1.$$

Thinking of this in $\mathbb{Z}/n\mathbb{Z}$, we have

$$[a]_n [5]_n = [1]_n$$

since $[n]_n = [0]_n$.

Def: Let $[a]_n \in \mathbb{Z}/n\mathbb{Z}$. If there exists $[b]_n \in \mathbb{Z}/n\mathbb{Z}$ so that $[a]_n [b]_n = [1]_n$ we say $[a]_n$ is a unit modulo n. We denote the set of units in $\mathbb{Z}/n\mathbb{Z}$ by $(\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem 2.3.1: Let $n \in \mathbb{Z}_{>1}$. Let $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ with $\gcd(a,n) = 1$. Then $[a]_n$ is a unit modulo n. Conversely, if $\gcd(a,n) > 1$ then $[a]_n$ is a zero divisor.

Proof: We saw above that if $\gcd(a,n) = 1$ then $[a]_n$ is a unit modulo n. Suppose that $\gcd(a,n) = d > 1$. Then there exists $e \in \mathbb{Z}$ with $e > 1$ and $ed = a$ and $f \in \mathbb{Z}$ with $f > 1$ and $fd = n$. Then we have

$$\begin{aligned} fa &= fed \\ &= fde \\ &= ne, \end{aligned}$$

and so

$$[f]_n [a]_n = [n]_n [e]_n = [0]_n.$$

Thus, $[a]_n$ is a zero divisor since $1 < f < n$. ∎

Cor 2.3.2: Let $p \in \mathbb{Z}$ be a prime. Then $(\mathbb{Z}/p\mathbb{Z})^\times$ consists of all the non-zero elements of $\mathbb{Z}/p\mathbb{Z}$, ie. all non-zero elements are units and there are no zero-divisors.

Note: One cannot have an element that is a unit and zero divisor. If $[a]_n$ is a unit, then suppose there exists $[b]_n$ so that $[a]_n[b]_n = [0]_n$. Let $[c]_n \in \mathbb{Z}/n\mathbb{Z}$ so that $[a]_n[c]_n = [1]_n$.

Then $[b]_n([a]_n[c]_n) = [b]_n[1]_n = [b]_n$ and

$[b]_n([a]_n[c]_n) = ([b]_n[a]_n)[c]_n = [0]_n$

so $[b]_n = [0]_n$.

We can rephrase these result in terms of solutions to equations as well.

Cor 2.3.3: 1) The equation $[a]_n x = [1]_n$ has a solution in $\mathbb{Z}/n\mathbb{Z}$ iff $[a]_n$ is a unit in $(\mathbb{Z}/n\mathbb{Z})$. iff $\gcd(a,n) = 1$.

2) The equation $[a]_n x = [0]_n$ has a non-zero solution in $\mathbb{Z}/n\mathbb{Z}$ iff $[a]_n$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$ iff $\gcd(a,n) > 1$.

Proof: Exercise. ∎