Math 425: Abstract Algebra 1

Section 1.3: Integers mod n

Mckenzie West

Last Updated: September 19, 2022

Last Time.

- Division Algorithm
- GCD
- Bézout's Identity
- Euclidean Algorithm
- Prime Factorization Theorem

Today.

- Congruence modulo n
- Relations and Equivalence Classes
- Integers and Arithmetic modulo n
- Arithmetic Modulo n
- Inverses Modulo n

Definition.

Let $a, b, n \in \mathbb{Z}$ with $n \geq 2$. We say that a and b are `congruent modulo` n if

$$n \mid (a - b).$$

In that case, we write $a \equiv b \pmod{n}$.

Theorem 1.3.1.

Congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Exercise 1.

Write the equivalence classes of $(\mathbb{Z}, \equiv \pmod{2})$.

Exercise 2.

Write the equivalence classes of $(\mathbb{Z}, \equiv \pmod{3})$.

Definition.

If $a \in \mathbb{Z}$, then its equivalence class, $[a]$, with respect to congruence modulo n is called its `residue class modulo` n and we write $\overline{a}$ for convenience.

$$\overline{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}.$$

Definition.

The `set of integers modulo` n is denoted $\mathbb{Z}_n$ and is given by

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

Example.

$\mathbb{Z}_7 =$

Exercise 3.

What is $\overline{47}$ in $\mathbb{Z}_7$? What is $\overline{-16}$?

Claim.

Addition and multiplication in $\mathbb{Z}_n$, as defined below, are well-defined:

(1) $\overline{a} + \overline{b} = \overline{a+b}$

(2) $\overline{a}\,\overline{b} = \overline{ab}$

Note.

The important point here is that any well-defined arithmetic operation on $\mathbb{Z}_n$ should NOT depend on the choice of residue class representative.

Example.

In $\mathbb{Z}_7$, $\overline{48} = \overline{6}$ and $\overline{3} = \overline{10}$. Is it true that $\overline{48} + \overline{3} = \overline{6} + \overline{10}$?

Proof.

It suffices to show that if $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$ in $\mathbb{Z}_n$, then

$$\overline{a_1 + b_1} = \overline{a_2 + b_2} \text{ and } \overline{a_1 b_1} = \overline{a_2 b_2}.$$

Exercise 4.

Fill out the addition and multiplication tables for $\mathbb{Z}_4$.

$+_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$				
$\overline{1}$				
$\overline{2}$				
$\overline{3}$				

$\times_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$				
$\overline{1}$				
$\overline{2}$				
$\overline{3}$				

Claim.

An integer $n \in \mathbb{Z}$ is divisible by 9 if and only if the sum of its digits is divisible by 9.

Summary.

- The set of integers modulo n is

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

- If r is the remainder you get when dividing a by n, then

$$a \equiv r \pmod{n} \text{ or equivalently } \overline{a} = \overline{r}.$$

- Addition in $\mathbb{Z}_n$ is defined by:

$$\overline{a} + \overline{b} = \overline{a+b}.$$

- Multiplication in $\mathbb{Z}_n$ is defined by

$$\overline{a}\,\overline{b} = \overline{ab}.$$

Theorem 1.3.4.

Let $n \geq 2$ be a fixed modulus and let a, b and c denote arbitrary integers. Then the following hold in $\mathbb{Z}_n$.

1. $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ and $\overline{a}\overline{b} = \overline{b}\overline{a}$.
2. $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$ and $\overline{a}(\overline{b}\overline{c}) = (\overline{a}\overline{b})\overline{c}$.
3. $\overline{a} + \overline{0} = \overline{a}$ and $\overline{a}\overline{1} = \overline{a}$.
4. $\overline{a} + \overline{-a} = \overline{0}$.
5. $\overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{ac}$.

Note.

The proof of (5) is in the book. And (2) is proved in a video.

Moral from last Theorem: Arithmetic in $\mathbb{Z}_n$ behaves very similarly to arithmetic in $\mathbb{Z}$!

There's a zero, $\overline{0}$, and unity, $\overline{1}$, in $\mathbb{Z}_n$.

Every $\overline{a} \in \mathbb{Z}_n$ has an negative or additive inverse, $\overline{-a}$, in $\mathbb{Z}_n$, which we write as $-\overline{a}$ and satisfies

$$\overline{a} + \overline{-a} = \overline{0}.$$

Subtraction is then naturally defined as

$$\overline{a} - \overline{b} = \overline{a} + \overline{-b} = \overline{a - b}.$$

Exercise 5.

What is the additive inverse of $\overline{6}$ in $\mathbb{Z}_8$?

Definition.

We call a class $\overline{a} \in \mathbb{Z}_n$ `invertible` if there is some $\overline{b} \in Z_n$ such that $\overline{a}\overline{b} = \overline{1}$.

Example.

Consider $\mathbb{Z}_4$.

Exercise 6.

Show $\overline{6} \in \mathbb{Z}_8$ has no multiplicative inverse.

Note.

Looking at this question as a polynomial equation, there is no solution to $\overline{6}x = \overline{1}$ in $\mathbb{Z}_8$.

Exercise 7.

(a) Solve $\overline{5}x = \overline{1}$ in $\mathbb{Z}_8$, if possible.
Brute force is a great plan.

(b) Solve $\overline{5}x = \overline{2}$ in $\mathbb{Z}_8$, if possible.

(c) Solve $\overline{6}x = \overline{2}$ in $\mathbb{Z}_8$, if possible.

Note.

Here's some Sage code for some brute force that will print it nicely.

```
Zmod8=Integers(8)
for a in Zmod8:
print(f"5*{a}={5*a} mod 8")
```

Use at `https://sagecell.sagemath.org/`.

Question 8.

What do you notice about the relationship between n and the values in $\mathbb{Z}_n$ that have inverses?
This slide and the next have multiplication tables for $\mathbb{Z}_7$, $\mathbb{Z}_8$, $\mathbb{Z}_9$, and $\mathbb{Z}_{10}$. Identify the rows that have a 1 in them - these are the classes with inverses.

Multiplication in $\mathbb{Z}_7$

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Multiplication in $\mathbb{Z}_8$

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

* Overlines omitted for the sake of visual appearance.

Multiplication in $\mathbb{Z}_9$

$\times$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Multiplication in $\mathbb{Z}_{10}$

0	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4*	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Overlines omitted for the sake of visual appearance.

Theorem 1.3.5.

Let $a, n \in \mathbb{Z}$ with $n \geq 2$. Then $\overline{a}$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if a and n are relatively prime.

Before starting the proof of Theorem 1.3.5, we recall two important Theorems:

Theorem 1.2.4.

Let $m, n \in Z$ not both zero. Then

$$m, n \text{ relatively prime} \Leftrightarrow \exists r, s \in \mathbb{Z} \text{ such that } 1 = rm + sn$$

Theorem 1.3.2.

Given $n \geq 2$, $\overline{a} = \overline{b} \Leftrightarrow a \equiv b \pmod{n}$.

Theorem 1.3.5.

Let $a, n \in \mathbb{Z}$ with $n \geq 2$. Then $\overline{a}$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if a and n are relatively prime.

Note.

The proof of the reverse direction of Theorem 1.3.5 helps us to find inverses.

Example.

Find the inverse of $\overline{16}$ in $\mathbb{Z}_{35}$.

Euclidean Algorithm:

$$\begin{aligned} 35 &= 2(16) + 3 \\ 16 &= 5(3) + 1 \\ 3 &= 3(1) + 0 \end{aligned}$$

Bézout:

$$\begin{aligned} 1 &= 16 - 5(3) \\ &= 16 - 5(35 - 2(16)) \\ &= 11(16) - 5(35) \end{aligned}$$

The equation $1 = 11(16) - 5(35)$ modulo 35 gives:

$$1 \equiv 11 \cdot 16 \pmod{35}.$$

Therefore, the multiplicative inverse of $\overline{16}$ in $\mathbb{Z}_{35}$ is $\overline{11}$.

Exercise 9.

Solve the equation $\overline{16}x = \overline{9}$, in $\mathbb{Z}_{35}$.

Exercise 10.

Solve the system of equations in $\mathbb{Z}_{13}$

$$\begin{cases} \overline{5}x + \overline{2}y = \overline{1} \\ \overline{2}x + \overline{10}y = \overline{2}. \end{cases}$$

Theorem 1.3.6 (The Chinese Remainder Theorem).

Let m and n be relatively prime integers. If s and t are arbitrary integers, then there is an integer b for which

$$b \equiv s \pmod{m} \text{ and } b \equiv t \pmod{n}.$$

Note.

How do we find this b?
Since $\gcd(m, n) = 1$, we can find $p, q \in \mathbb{Z}$ such that $1 = mp + nq$.
$\boxed{\text{why?}}$
Set $b = (mp)t + (nq)s$. $\boxed{\text{why does this work???}}$

Theorem 1.3.7.

The following are equivalent for any integer $n \geq 2$.

1. Every element $\overline{a} \neq \overline{0}$ in $\mathbb{Z}_n$ has a multiplicative inverse.
2. If $\overline{a}\overline{b} = \overline{0}$ in $\mathbb{Z}_n$, then either $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.
3. The integer n is prime.

Wilson's Theorem - A Corollary to 1.3.7.

If p is prime then $(p-1)! \equiv -1 \pmod{p}$.

Note.

Think about how numbers and their inverses mod p appear in the product

$$1 \cdot 2 \cdot 3 \cdots (p-1).$$

Theorem 1.3.8 (Fermat's Theorem).

If p is prime then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$. Moreover, if $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.