$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

We solved $x+1 \equiv 3 \pmod 5$

But what about $2x \equiv 3 \pmod 5$?

Trial and error:

$x=2$? $2 \cdot 2 = 4$

$x=4$? $2 \cdot 4 = 8 \rightarrow 8 \bmod 5 = 3$

$$\boxed{x=4}$$

How do we divide?

$\div$ Modular division $a \oslash b$ is defined to be $a \otimes b^{-1}$

$$4 \div 2 \Rightarrow 4 \times \frac{1}{2}$$

Def'n The multiplicative inverse a^{-1} of an integer $a \in \mathbb{Z}_n$ is the value $a^{-1} \in \mathbb{Z}_n$ s.t. $a \otimes a^{-1} \equiv a^{-1} \otimes a \equiv 1$

Thm For any $a \in \mathbb{Z}_n$, a^{-1} exists iff $\gcd(a, n) = 1$.

To find a^{-1}, use EEA to find x, y s.t. $ax + ny = 1$. Then, $a^{-1} = x$.

Suppose we found $\gcd(a,n)=1$

And then we found $1 = ax + ny$

$$1 \bmod n \equiv ax + ny \bmod n$$

$$1 \equiv ax \pmod{n}$$

$$x = a^{-1}$$

Ex. Find $37^{-1} \in \mathbb{Z}_{1205}$

From Sep. 5 example: $1 = 37(228) + 1205(-7)$

$$37^{-1} = 228$$

Ex. 7^{-1} in $\mathbb{Z}_{16}$

We can either do EA and backtrack by sub'ing

Or we can do the EEA

$$a = bq + r$$

$$16 = 7\cdot(2) + 2 \rightarrow 2 = 16 + 7(-2) \quad ①$$

$$7 = 2\cdot(3) + 1 \rightarrow 1 = 7 + 2(-3) \quad ②$$

$$2 = 1\cdot(2) + 0$$

$$1 = 16x + 7y$$

$$② \; 1 = 7 + [16 + 7(-2)](-3)$$
$$= 7 + 16(-3) + 7(6)$$
$$= 7(7) + 16(-3)$$

$$7^{-1} = 7$$

Ex.: Repeat w/ EEA

Ex. $7x \equiv 2 \pmod{16}$

$$\underline{7^{-1} \otimes 7} x \equiv 7^{-1} \otimes 2 \pmod{16}$$

$$x \equiv 7 \otimes 2 \pmod{16}$$

$$x \equiv 14 \pmod{16}$$

Can we solve $ax \equiv b \pmod{n}$ when $\gcd(a,n) \neq 1$?

Since a^{-1} doesn't exist, we must guess and check

$\gcd(8,12) = 4$

$\Downarrow$

8^{-1} D.N.E in $\mathbb{Z}_{12}$

Ex. $8x \equiv 4 \pmod{12}$

x	0	1	2	3	4	5	6	7	8	9	10	11
x8	0	8	16	24	32	40	48	56	64	72	80	88
mod 12	0	8	4	0	8	4	0	8	4	0	8	4

$\therefore x \equiv 2, 5, 8, 11 \pmod{12}$

$x = [2]_{12}, x = [5]_{12} \ldots$

if

$\mathbb{Z}_n$ is defined as $\{[0], [1], \ldots [n-1]\}$

I wrote the above (inside this rectangle) in response to a question in class. Some textbooks define Z_n as a set of equivalence classes instead of a set of integers. But that is not the notation that our textbook follows, so you don't need to worry about it (it is just extra info).

Ex. From the multiplication table in the prev. ex., we see that

$$8x \equiv 5 \pmod{12}$$

does not have a sol'n.

So, we have seen examples where...

$$ax \equiv b \pmod{n} \begin{cases} \to 1 \text{ sol'n} \\ \to \text{multiple sol'ns} \\ \to \text{no sol'ns} \end{cases}$$

Next class: Solving multiple congruences

① $x \equiv 2 \pmod{3}$

② $x \equiv 4 \pmod{7}$

③ $x \equiv 3 \pmod{11}$