

Modular arithmetic / Congruences.

$$a, b \in \mathbb{Z} \quad n \in \mathbb{Z}$$

$$a \equiv b \pmod{n}$$

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

$$\Leftrightarrow \begin{aligned} &\underline{b = a + qn} \text{ for some } q \in \mathbb{Z} \\ &\underline{a = b + q'n} \end{aligned}$$

$$n \mid a \Leftrightarrow a \equiv 0 \pmod{n}$$

Main power:

$$\begin{aligned} &a \equiv a' \pmod{n} \text{ and } b \equiv b' \pmod{n} \\ \Rightarrow &a + b \equiv a' + b' \pmod{n} \text{ and } ab \equiv a'b' \pmod{n} \end{aligned}$$

Example $387 \cdot 911 \equiv 1 \pmod{2}$

because $387 \equiv 1 \pmod{2}$
 $911 \equiv 1 \pmod{2}.$

so $387 \cdot 911 \equiv 1 \cdot 1 \pmod{2}$
 $\equiv 1 \pmod{2}.$

$387 \cdot 911 \equiv ? \pmod{3}.$

$387 \equiv 0 \pmod{3}$
 $\equiv 0 \pmod{3}$

$911 \equiv 2 \pmod{3}$

$\mathbb{Z}/n\mathbb{Z} :=$ set of symbols $0, \dots, n-1$

$a b$ is the unique number $0 \leq k < n$ such that
 $ab \equiv k \pmod{n}.$

I.e. to multiply $a, b \rightarrow$ take ab as an integer
then replace with the
remainder for division by n

Similarly for addition.

Example: $3 \cdot 5$ in $\mathbb{Z}/6\mathbb{Z}$

is $15 \sim \text{remainder for } 6 \overline{)15}$
 $= 3$

Exercise: Write down times tables
for $\mathbb{Z}/n\mathbb{Z}$ $n=2, 3, 4, 5, \dots, 13$

$$n=3$$

$\mathbb{Z}/n\mathbb{Z}$

0, 1, 2

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$3 \cdot 2 = 6 \equiv 2 \pmod{4}$$

$$n=4$$

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

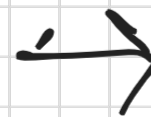
$$3 \cdot 3 = 9 \equiv 1 \pmod{4}$$

$$n=5$$

	0	1	2	3	4
0	0.0	0.1	0.2	0.3	0.4
1	1.0	1.1	1.2	1.3	1.4
2	2.0	2.1	2.2	2.3	2.4
3	3.0	3.1	3.2	3.3	3.4
4	4.0	4.1	4.2	4.3	4.4

Multiplication

done in
 $\mathbb{Z}/5\mathbb{Z}$



	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

When does an element of $\mathbb{Z}/n\mathbb{Z}$
have a multiplicative inverse?

(\Leftrightarrow)

Given $a, n \in \mathbb{Z}$, when is there $b \in \mathbb{Z}$
such that $ab \equiv 1 \pmod{n}$?

In any number system $(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z})$

we say an element x has a multiplicative inverse
if there is y such that $xy = 1$.

Example: Any nonzero $x \in \mathbb{Q}$ has a mult. inverse in \mathbb{Q}

$$x = \frac{a}{b}$$

$$y = \frac{b}{a}$$

$$xy = \frac{ab}{ba} = 1.$$

Question: Which $x \in \mathbb{Z}$ have a mult. inverse that is in \mathbb{Z} ?

1 and -1

$$1 \cdot 1 = 1$$

$$(-1)(-1) = 1.$$

← These are the only ones.

Exercise 1-(2) - Which $a \in \mathbb{Z} \setminus \{0\}$ have a mult. inverse?

Guess a simple condition on a and n , then try to justify it using things we have done.