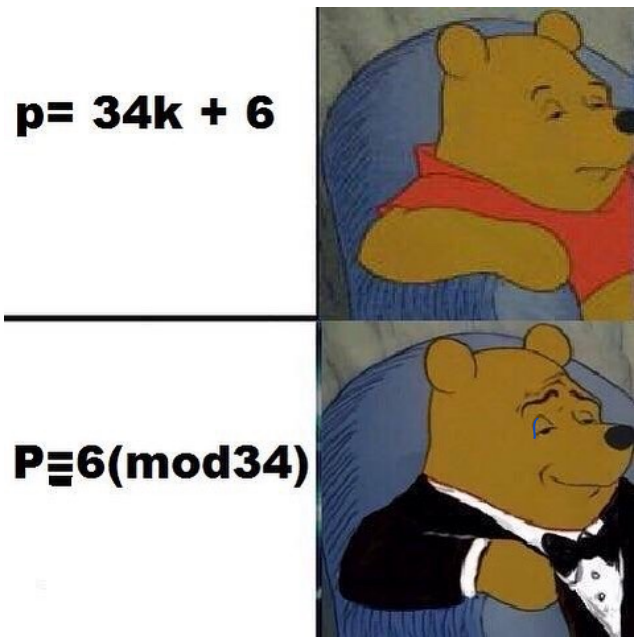
Dis 03B: Modular Arithmetic

- thinking of setting up a discussion discord => hop in while working and ask each other questions (or weekly happy hours?)
  - ↳ would need someone to manage forme (contact me).



For Breakout Rooms

- We'll do some review + icebreakers first (~first ten minutes).
- If you prefer to work solo / want to read questions first, market in your name but feel free to chill in the breakout room (or stay in the main room?)

fun exercise: prove all of these (at the end!)

2 THANK	3 YOU	4 ALL
5 FOR	6 HAVING	7 NOT YOU
8 EASY	9 DIVISIBILITY	10 RULES

@howie_hua

Breakout Room Q's (on my website!)

Icebreaker: names, years, favorite restaurant(s) in Berkeley! (exchange emails / FB?)
↳ ex: Tyler, junior, obviously Chez Panisse (/c probably Cheeseboard / Gregoire's)

review:

1) what does $a \equiv b \pmod m$ mean?

$a = bt + m \cdot k$ for some $k \in \mathbb{Z} \iff m \mid a-b$

2) does $a \equiv b \pmod m$ imply $a^n \equiv b^n \pmod m$?

Yes $m \mid a-b \mid a^n - b^n$.

3) $+, -, \times$ are straightforward in modular arithmetic.

how (or when) can we divide?

More Review

Definition 1. We say that a is *congruent* to $b \pmod m$ if

$$a \equiv b \pmod m \iff m | a - b \iff a - b = m \cdot k, \quad k \in \mathbb{Z}.$$

One interpretation is that mod m gets the remainder when we divide by m, but the mod operator is more powerful than just that. For example, we have that

$$\begin{aligned}
\cdots \equiv -9 \equiv -4 \equiv \boxed{1} \equiv 6 \equiv 11 \equiv \ldots \pmod 5 \\
\cdots \equiv -8 \equiv -3 \equiv \boxed{2} \equiv 7 \equiv 12 \equiv \ldots \pmod 5 \\
\cdots \equiv -7 \equiv -2 \equiv \boxed{3} \equiv 8 \equiv 13 \equiv \ldots \pmod 5
\end{aligned}$$

Given that so many numbers are equivalent to each other when working over a certain modulus, it helps us to agree upon a set of *representatives* for each equivalence class of numbers. In the above example, the representatives for each class has been boxed. In general, the representatives are $\{0, 1, \ldots, m-1\}$.

To drive this point home, compare to how we say that all of the following fractions are the same, but we use the boxed one as their representative (namely $\frac{1}{3}$):

$$\cdots = \frac{-3}{-9} = \frac{-2}{-6} = \frac{-1}{-3} = \boxed{\frac{1}{3}} = \frac{2}{6} = \frac{3}{9} = \cdots$$

Doing math over a modulus is similar to normal arithmetic; addition, subtraction, multiplication, and exponentiation all hold.

when can we divide? when

$ax \equiv 1 \pmod m$

has a solution (inverse), $\iff$ $\gcd(m, x) = 1$.

3 Amaze Your Friends

It's been a long week, and you're finally in the Friday Zoom hangout that you've been looking forward to. You eschew conversations about Professor Rao's updated facial hair, that sourdough starter that's all the rage, or the new season of "Pose". Instead, you decide to invoke wonder (or possibly fear) in your friends by tricking them into thinking you can perform mental arithmetic with very large numbers.

So, what are the last digit of the following numbers? $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$

(a) 11^{2017}

$11^{2017} \equiv 1^{2017} \equiv 1 \pmod{10}$

(b) 9^{10001}

$9^{10001} \equiv (-1)^{10001} \equiv -1 \equiv 9 \pmod{10}$

$(-1)^1 \equiv -1$, $(-1)^2 \equiv 1$, $(-1)^3 \equiv -1$

mod 10

(c) $3^{987654321}$

$3^{987654321} \equiv 3^{1+4\cdot k} \pmod{10}$.

$987654321 \equiv 1 \pmod 4$.

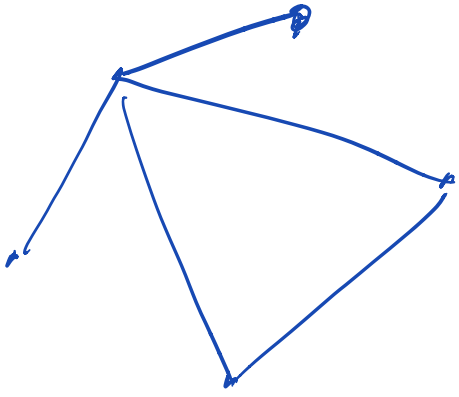
$\equiv 3^1 \equiv 3 \pmod{10}$

$3^1 \equiv 3$

$3^2 \equiv 9$

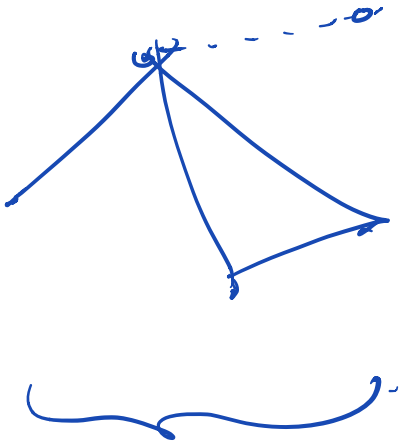
$3^3 \equiv 7$

$3^4 \equiv 81 \equiv 1 \pmod{10}$



$k+1$

$\Rightarrow$



1 Modular Inverses

Recall the definition of inverses from lecture: let $a, m \in \mathbb{Z}$ and $m > 0$; if $x \in \mathbb{Z}$ satisfies $ax \equiv 1 \pmod{m}$, then we say x is an **inverse of** a **modulo** m.

Now, we will investigate the existence and uniqueness of inverses.

(a) Is 3 an inverse of 5 modulo 10?

(b) Is 3 an inverse of 5 modulo 14?

(c) Is each $3 + 14n$ where $n \in \mathbb{Z}$ an inverse of 5 modulo 14?

(d) Does 4 have inverse modulo 8?

(e) Suppose $x, x' \in \mathbb{Z}$ are both inverses of a modulo m. Is it possible that $x \not\equiv x' \pmod{m}$?

$a \cdot x \equiv 1$

$3 \cdot \frac{1}{3} = 1$.

$a \equiv b \pmod{m} \iff m \mid a - b$.

(a), $3 \cdot 5 = 15 \equiv 5 \pmod{10}$, so No.

(b) $3 \cdot 5 = 15 \equiv 1 \pmod{14}$, so Yes.

(c), $(3 + 14n) \cdot 5 = 3 \cdot 5 + 14 \cdot 5 \cdot n \equiv 15 \equiv 1 \pmod{14}$, so Yes.

(d), $4 \cdot k \equiv 1 \pmod{8} \iff 4k \equiv 1 + 8 \cdot l$

$\Rightarrow 0 \equiv 1 \pmod{4}$ X no sol.

(e). No.

$ax \equiv ax' \equiv 1 \pmod{m}$

$\Rightarrow ax - ax' \equiv 0 \pmod{m}$

$\Rightarrow a(x - x') \equiv 0 \pmod{m}$.

$xy \equiv 0 \pmod{6}$. $\Rightarrow$ ~~x~~ $a(x - x') \equiv x \cdot 0 \pmod{m}$

$\Rightarrow x - x' \equiv 0$

$x \equiv x' \pmod{m}$