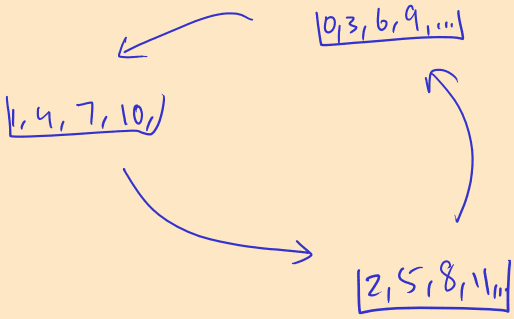
equiv

$2 \equiv 5 \pmod 3$

mod 3

$-2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad \ldots$



$(a+b) \bmod m$

$= a \bmod m + b \bmod m$

mod 5

|0,5,10,|

|1,6,11,16|

|2,7,12|

|3,8,13|

|4,9,14|

$4^{-1} \equiv 4 \pmod 5$

$4 \times 4 = 16 \equiv 1 \pmod 5$

$9 \times 4 = 36 \equiv 1 \pmod 5$

$\equiv$

$4 \times 4 \pmod 5$

$2^{-1} \equiv 3 \pmod 5$

$3 \times 2 = 6 \equiv 1 \pmod 5$

$3^{-1} \equiv 2 \pmod 5$

$a^{-1} \pmod m$

$\gcd(a, m) = 1 = d$

$a = kd$

$m = ld$

$kdx + ldy = 1$

$d(kx + ly) = 1$

$(kx + ly) = \frac{1}{d}$ ← not int, $d > 1$

$40 \cdot 5 + 51 \cdot (-3) = 47$

$x \equiv 40^{-1} \pmod{51}$

$1 \equiv 40x \pmod{51}$

mod inv

$40x + 51y = 1 \pmod{51}$

$51 \overline{)200}$ quotient 3, 153, remainder 47

$51 \overline{)40x}$ quotient y, remainder $\to 1$

$40(-5) + 51(4) = 4$

$40(1) + 51(1) = 11$

$40(4) + 51(-3) = 7$

$40(9) + 51(-7) = 3$

$40(-14) + 51(11) = 1$

$7 - 4 = 3$

$4 - 3 = 1$

$51y = 1 + 40x$

$51 - 14 = 37$

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 DIS 3B

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.

3, 3+14, 3+28, ...

(a) Is 3 an inverse of 5 modulo 10? No, $3 \times 5 \equiv 5 \pmod{10}$

(b) Is 3 an inverse of 5 modulo 14? Yes, $15 \equiv 1 \pmod{14}$

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

(d) Does 4 have inverse modulo 8? $4^{-1} \pmod 8$ No! $\gcd(4,8) = 4 > 1$

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

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

$(ax - ax') \equiv 1 - 1 \equiv 0 \pmod m$

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

$a \equiv 0$ → not possible! 0^{-1} DNE

$x - x' \equiv 0$

$\Rightarrow ax(x - x') \equiv 0$

$\Rightarrow 1 \cdot (x - x') \equiv 0$

$\Rightarrow x \equiv x' \pmod m$

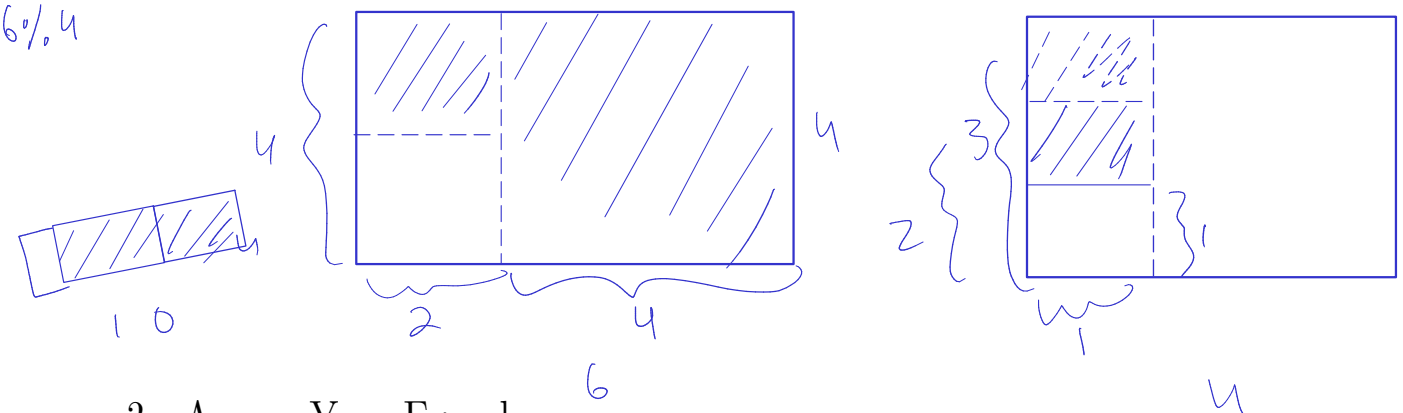
3, 17, $3 \cdot 17 \equiv 0 \pmod{51}$

$m = 51$

2 Paper GCD

Given a sheet of paper such as this one, and no rulers, describe a method to find the GCD of the width and the height of the paper. You can fold or tear the paper however you want, and ultimately you should produce a square piece whose side lengths are equal to the GCD.

6 % 4



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) 11^{2017} 1 11 121 1331 $11^{2017} \bmod 10 \equiv 1^{2017} \bmod 10$

1
9
81
729
6561

(b) 9^{10001} $9^2 = 81 \equiv 1 \bmod 10$

$9^{10001} \bmod 10 \equiv 9 \cdot (9^2)^{5000} \bmod 10$

$\equiv 9 \cdot (81)^{5000} \bmod 10 \equiv 9 \bmod 10$

(c) $3^{987654321}$

3

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

$3^{987654321} \bmod 10 \equiv 3 \cdot (3^4)^{\square} \bmod 10$


Always has been
1
11
121
1331
14641
161051
1771561
19487171
214358881
2357947691
25937424601
285311670611
3138428376721
34522712143931
379749833583241
(mod 10)
Wait it's all 1?