

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 $x \not\equiv x' \pmod{m}$?

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.

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}

(b) 9^{10001}

(c) $3^{987654321}$