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.

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

Solution:

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

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

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

(d) No. For contradiction, assume $x \in \mathbb{Z}$ is an inverse of 4 modulo 8. Then $4x \equiv 1 \pmod{8}$. Then $8 \mid 4x - 1$, which is impossible.

(e) No. We have $xa \equiv x'a \equiv 1 \pmod{m}$. So

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

Multiply both sides by x, we get

$$xa(x - x') \equiv 0 \cdot x \pmod{m}$$

$$\implies x - x' \equiv 0 \pmod{m}.$$

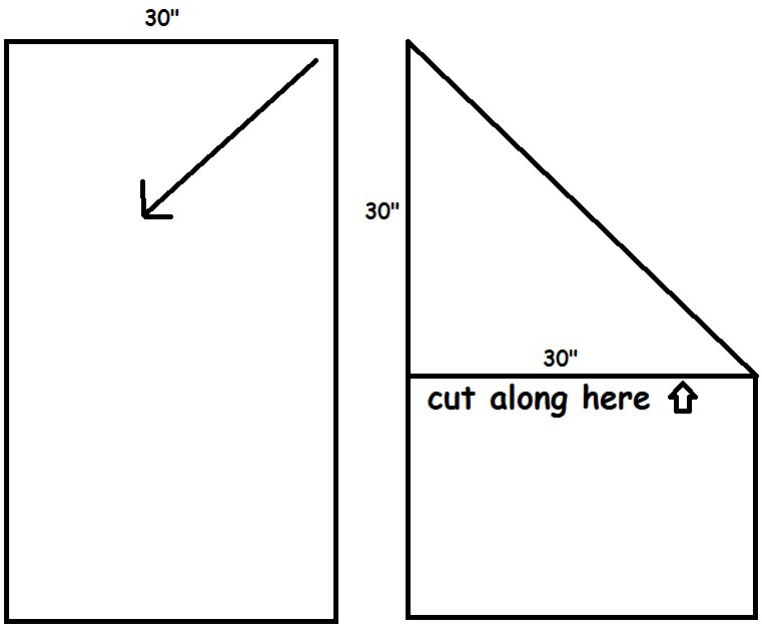
$$\implies x \equiv x' \pmod{m}$$

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.

Solution:

We can fold the smaller side diagonally onto the larger side, and tear the paper from where the fold lands.



If we started with height and width equal to a and b, this gives us a piece of paper with side lengths $a-b$ and b (assuming that $a > b$). Note that if $a-b > b$, the next time we end up with side lengths $a-2b$ and b. So after a few steps we must reach a mod b and b, at which we start subtracting from b.

Continuing this method is similar to the Euclidean algorithm and therefore results in reaching 0 at some point. Right before reaching 0, we must have a square piece of paper whose side lengths are 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) $3^{987654321}$

Solution:

(a) 11 is always 1 mod 10, so the answer to (a) is 1.

(b) 9 is its own inverse mod 10, therefore, if 9 is raised to an odd power, the number will be 9 mod 10. So the answer is 9.

Also notice that $9 \equiv -1 \pmod{10}$ so $9^{10001} \equiv (-1)^{10001} \equiv -1 \equiv 9 \pmod{10}$. In general, $m-1 \equiv -1 \pmod{m}$, so $m-1$ is always its own inverse. This is a useful trick so you can avoid computing the inverse of $m-1$ by hand. You can also check that $(m-1)^2 \equiv m^2 - 2m + 1 \equiv 1 \pmod{m}$, which is another proof that $m-1$ is its own inverse modulo m.

(c) $3^4 = 9^2 = 1$ mod 10. We see that the exponent $987654321 = 1$ mod 4 so the answer is 3.