

## Recitation 5

### Three's Trick

## Review

**Defn 1:** We say that  $a \mid b$  ( $a$  divides  $b$ ) when  $b = ka$  for some  $k \in \mathbb{Z}$ .

**Defn 2:**  $a \equiv b \pmod{m}$  if  $m \mid (b - a)$ . In other words,  $a$  and  $b$  have the same remainder upon division by  $m$ . Convince yourself that these statements are equivalent.

### Properties of Congruence Relations:

For  $a, b \in \mathbb{Z}^+$ , if  $a \equiv b \pmod{m}$ , then

- $a + c \equiv b + c \pmod{m}$  for  $c \in \mathbb{Z}$
- $ac \equiv bc \pmod{m}$  for  $c \in \mathbb{Z}$
- $a^n \equiv b^n \pmod{m}$  for  $n \in \mathbb{Z}^+$

If we also have  $c \equiv d \pmod{m}$ , then

- $a + c \equiv b + d \pmod{m}$
- $ac \equiv bd \pmod{m}$

**Theorem 1:** For any  $a, b \in \mathbb{Z}$  there exists  $u, v \in \mathbb{Z}$  such that  $au + bv = \gcd(a, b)$ . In words, we say that  $a$  and  $b$  can be written as a linear combination of their gcd.

**Theorem 2:** The congruence  $ax \equiv c \pmod{m}$  has a solution if and only if the  $\gcd(a, m)$  divides  $c$ .

$$\gcd(a, m) \mid c.$$

## Warm-Up

- a. Given  $a \equiv b \pmod{m}$ , prove  $a + c \equiv b + c \pmod{m}$  for  $c \in \mathbb{Z}$ .

---

b. Given  $a \equiv b \pmod{m}$ , prove  $ac \equiv bc \pmod{m}$  for  $c \in \mathbb{Z}$ .

c. Given  $a \equiv b \pmod{m}$ , prove  $a^2 \equiv b^2 \pmod{m}$ .

d. For every odd integer  $n$ , prove that  $n^4 - 1$  is divisible by 8.

---

## Section Lesson - Modular Inverses and the Three's Trick

Say we are trying to solve for  $x$  in the equation  $8x = 2$ , how would we do so?

Answer: we would multiply both sides by  $8^{-1} = \frac{1}{8}$ . This is called the inverse of 8.

$$\begin{aligned}\frac{1}{8} \cdot 8 \cdot x &= \frac{1}{8} \cdot 2 \\ \Rightarrow x &= 0.25\end{aligned}$$

And in general, if we are trying to solve for  $x$  in the equation  $ax = c$  we simply multiply both sides by  $a^{-1} = \frac{1}{a}$ .

The  $a^{-1}$  notation indicates that  $a^{-1} \cdot a = 1$ .

However, it is not so simple when we are working with congruence relations.

For example, there is **no solution** for  $x$  in the equation  $8x \equiv 2 \pmod{12}$ .

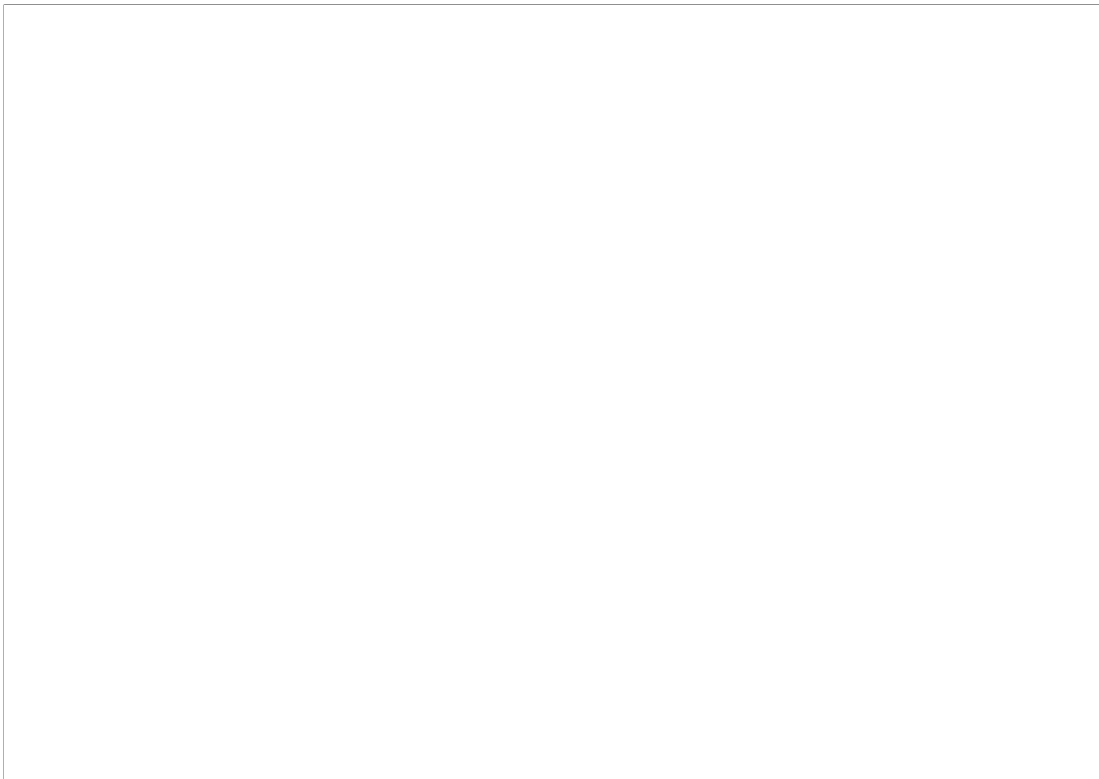
In general,  $ax \equiv c \pmod{m}$  has a solution if and only if  $\gcd(a, m) \mid c$ . (In english: if and only if the gcd of  $a$  and  $m$  divides  $c$ .)

- a. Prove that if  $\gcd(a, m) \mid c$  then  $ax \equiv c \pmod{m}$  has a solution.

**Hint:** Let  $d = \gcd(a, m)$ . From Theorem 1 above we know that  $d = au + mv$  for some  $u, v \in \mathbb{Z}$ .

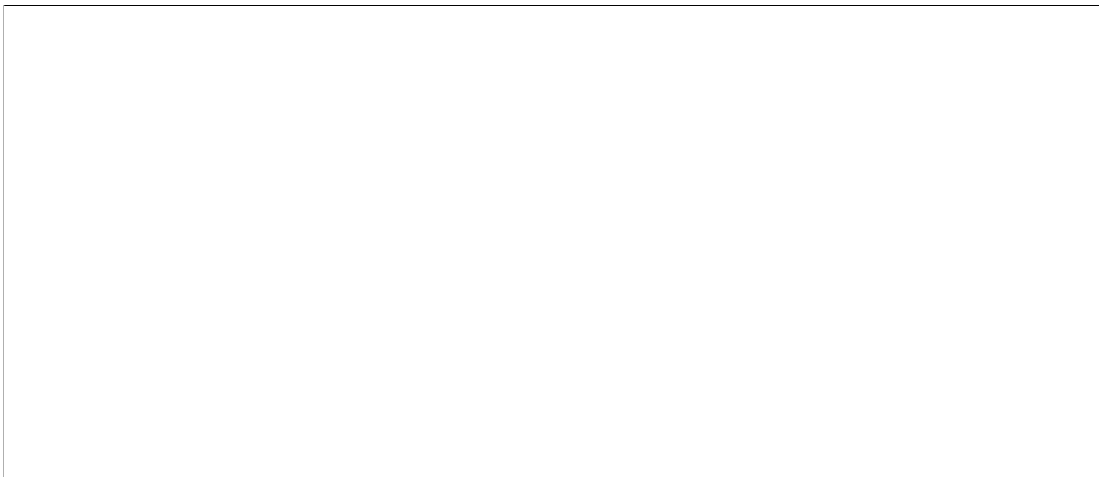
**Hint:** Since  $d \mid c$  then  $c = kd$  for some  $k \in \mathbb{Z}$

---



b. Use the strategy you found above to solve for  $4x \equiv 6 \pmod{14}$ .

Use the fact that  $4 \cdot 4 + (-1) \cdot 14 = 2$ .



## Modular Inverses Explained

A modular inverse for  $a \pmod{m}$  is a number  $a^{-1}$  such that  $a \cdot a^{-1} \equiv 1 \pmod{m}$ .

In other words, a modular inverse for  $a \pmod{m}$  is the  $x$  which solves  $ax \equiv 1 \pmod{m}$ .

- 
- c. If  $a$  has a modular inverse mod  $m$  then what is  $\gcd(a, m)$ .

A modular inverse is extremely helpful in solving equations  $ax \equiv b \pmod{m}$ .

If  $a$  has a modular inverse mod  $m$  then  $x \equiv a^{-1}b \pmod{m}$ .

- d. Use the technique from question “a” to find the modular inverse of 4 mod 9.

**Hint:** Use the fact that  $28-27 = 1$ .

- e. Use  $4^{-1}$  to solve for  $x$  in the equation  $4x \equiv 3 \pmod{9}$ . Verify your answer.

## The Threes Trick

Here is a trick to determine if a number  $n$  is divisible by 3:

*“If the sum of the digits of  $n$  is divisible by 3, so is  $n$ .”*

For example, 261 is divisible by 3 since  $2 + 6 + 1 = 9$ .

You are going to prove this.

- f. For any  $k \in \mathbb{N}$ , what is  $10^k$  congruent to mod 3?

- 
- g. For any  $k \in \mathbb{N}$ , what is the modular inverse of  $10^k \pmod{3}$ ?

Recall the modular inverse is the  $x$  which solves  $10^k x \equiv 1 \pmod{3}$

- h. Prove the “Threes trick” by expanding a number in terms of its digits.

- i. Does the Threes trick work when we are not in Base 10? What numbers does it apply for in base  $b$ ?