Recitation 4

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.

When you are working on number theory problems, start by writing out what you know. If you have that two numbers are equivalent mod another, write that out in terms on divisibility, and write out what the divisibility means. It will often be easier to work this way.

Properties of Congruence Relations:

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

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

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

- $a + c \equiv b + d \mod m$
- $ac \equiv bd \mod m$

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 $c \in \mathbb{Z}$.

$a \equiv b \pmod{m} \implies m|(b-a) \implies m * k = b - a$ for some integer k
$b - a = b - a + (c - c) = (b + c) - (a + c)$, so $m * k = (b + c) - (a + c)$
Thus, as $(b + c) - (a + c)$ is m times some integer, $m|((b + c) - (a + c)) \implies$
$a + c \equiv b + c \pmod{m}$

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

$a \equiv b \pmod{m} \implies m|(b-a) \implies m * k = b - a$ for some integer k
$m * k = b - a \implies m * k * c = c(b - a) \implies m * k * c = bc - ac$
As the integers are closed under addition, $k * c$ is an integer, so $bc - ac$ is m times some integer.
Thus, $m|bc - ac \implies ac \equiv bc \pmod{m}$

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

$a \equiv b \pmod{m} \implies m|(b-a) \implies m * k = b - a$ for some integer k
$\implies m * k * (a + b) = (b - a) * (b + a)$
$\implies m * k * (a + b) = b^2 - a^2$
As k, a, and b are integers, so is $k * (a + b)$. Then $b^2 - a^2$ is m times some integer.
Thus, $m|b^2 - a^2 \implies a^2 \equiv b^2 \pmod{m}$

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

$n^4 - 1 = (n^2 - 1)(n^2 + 1) = (n - 1)(n + 1)(n^2 + 1)$
n is odd $\implies n = 2k + 1$ for some integer k
$n^4-1 = ((2k+1)-1)((2k+1)+1)((2k+1)^2+1) = 2k*(2k+2)(4k^2+4k+1+1) =$
$2k*2(k+1)(4k^2+4k+2) = 4k(k+1)*2(2k^2+2k+1) = 8k(k+1)(2k^2+2k+1)$
$k(k + 1)(2k^2 + 2k + 1)$ is an integer, so $8|n^4 - 1$

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.

$$\frac{1}{8} \cdot 8 \cdot x = \frac{1}{8} \cdot 2$$
$$\Rightarrow x = 0.25$$

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. Not every congruence relation of the form $ax \equiv c \pmod{m}$ has a solution.

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

Why does this make sense? Well, 12 is a multiple of 4. For a number to be equivalent to 2 mod 12, it must be 2 greater than some multiple of 4. However, $8x$ will also be a multiple of 4. We can't have a multiple of 4 that is 2 larger than another multiple of 4–these must be at least 4 apart.

Some equations will have solutions though. For instance, a solution for x in the equation $5x \equiv 2 \pmod{12}$ is $x = 10$. It was possible for there to be a multiple of 5 which is 2 greater than a multiple of 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.)

Finding Solutions

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 $k \in \mathbb{Z}$

Hint: What does it mean for $ax \equiv c \pmod{m}$ to have a solution?

Let $d = \gcd(a, m)$. If $d|c$, then $c = kd$ for some $k \in \mathbb{Z}$.
By Theorem 1, $d = au + mv$ for some $u, v \in \mathbb{Z}$. So, $c = k(au + mv)$. Then $c = auk + mvk \implies mvk = c - auk$. $ax \equiv c \pmod{m}$ having a solution means there exists an integer x such that $m|c - ax$.
As u, v, k are integers, so are vk and uk. Let $x = uk$. $mvk = c - ax$, so m times some integer is $c - ax \implies m|c - ax$

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

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

$gcd(4, 14) = 2$, and $4 \cdot 4 + (-1) \cdot 14 = 2$. $2|6$ since $2 * 3 = 6$.
So $k = 3$, $u = 4$, $v = -1$. By part a, $x = k * u = 3 * 4 = 12$
To verify: $14|(6 - 4 * 12) \implies 14|(6 - 48) \implies 14| - 42$ which is true.

Modular Inverses Explained

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

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

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

1

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.

$28 - 27 = 1 \implies 4 * 7 + 9 * (-3) = 1$, so $u = 7$ and $v = -3$
Here, $k = 1$ since c and d are both 1.
Then $x = k * u = 1 * 7 = 7$
To verify, $4 * 7 = 28$ and $9|(1 - 28)$
So, $4^{-1} = 7$

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

We know $4 * 7 \equiv 1 \pmod 9$. By what we proved in the warmup, this means $4 * 7 * 3 \equiv 3 \pmod 9$, so $x = 7 * 3 = 21$
$4 * 21 = 84$, $3 - 84 = -81 = 9 * (-9)$ so it is true $9|(3 - 4 * 21$

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?

> $10 \equiv 1 \pmod 3$, and if we raise both sides to the k congruence still holds $\implies 10^k \equiv 1^k \pmod 3 \implies 10^k \equiv 1 \pmod 3$

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

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

> 1

h. Prove the "Threes trick" by expanding a number in terms of its digits. That is, represent the number abc as $a * 10^2 + b * 10^1 + c * 10^0$

> Consider the integer $a_m * 10^m + a_{m-1} * 10^{m-1} + ... + a_1 * 10^1 + a_0 * 10^0$. As for any positive integer k, $10^k \equiv 1 \pmod 3$, by what was proven in warmup $a_k * 10^k \equiv a_k$.
> Adding it all up as we also proved was possible in the warmup, $a_m * 10^m + a_{m-1} * 10^{m-1} + ... + a_1 * 10^1 + a_0 * 10^0 \equiv a_m + a_{m-1} + ... + a_1 + a_0 \pmod 3$. So, if the sum of the digits is divisible by 3 (equivalent to 0 mod 3), so will the full number.

i. Can we do a similar trick for other numbers when working in base 10? Does the Threes trick work when we are not in base 10? What numbers does it apply for in base b?

> The trick works for a in base b when $b \equiv 1 \pmod a$

Challenge: This One Goes to 11

By the property you found in the last section, the "add all the digits" trick won't work for 11 in base 10. However, there's another trick we can use! Instead of adding all of the digits, we alternate between adding and subtracting.

For example, to check if 6195704592 is divisible by 11, we do $-6+1-9+5-7+0-4+5-9+2=-22$. As -22 is divisible by 11, so is 6195704592.

In general, to check if

$$\sum_{k=0}^{n} a_k * 10^k$$

is divisible by 11, we compute

$$\sum_{k=0}^{n} a_k * (-1)^k$$

and check if it is divisible by 11.

Why does this work? You will want to use a similar strategy as you did for 3. In base b, for what numbers can we do this alternating sum trick?

$10 \equiv -1 \pmod{11}$, so for any k, $10^k \equiv (-1)^k \pmod{11}$
Then $a_k * 10^k \equiv a_k * (-1)^k \pmod{11}$
Adding these all up,

$$\sum_{k=0}^{n} a_k * 10^k \equiv \sum_{k=0}^{n} a_k * (-1)^k \pmod{11}$$

In general, in base b this will work for any n such that $b \equiv -1 \pmod{n}$