Recitation 6

Number Theory

Number Theory

Definition 1. For $a, b \in \mathbb{Z}$, we say that $a \mid b$ (a divides b) when $b = ka$ for some $k \in \mathbb{Z}$.

Definition 2. The division theorem says that any integer n with respect to some d can be written as $n = qd + r$, where $0 \leq r \leq d - 1$.

The function $\text{qcnt}(n, d)$ returns q. The function $\text{rem}(n, d)$ returns r.

Proposition 3. Let x, y, z be integers. If $x \mid y$ and $x \mid z$, then $x \mid (sy + tz)$ for any integers s and t. That is, any common divisor of y and z divides a linear combination of y and z (we call $sy + tz$ a linear combination of y and z).

Task 1

a. Using the division theorem, provide q and r for the following numbers:

i. $n = 10$, $d = 5$

Solution:
$10 = 2 \cdot 5 + 0$, $q = 2$, $r = 0$

ii. $n = 10$, $d = 6$

Solution:
$10 = 1 \cdot 6 + 4$, $q = 1$, $r = 4$

iii. $n = 10$, $d = 11$

Solution:
$10 = 0 \cdot 11 + 10$, $q = 0$, $r = 10$

b. Determine the output of the following:

i. $\text{qcnt}(52, 13)$

Solution:
4

ii. rem$(15, 4)$

Solution:
3

iii. rem$(93812129481, 2)$

Solution:
1

iv. *Optional:* qcnt$(24912, 5)$

Solution:
4982 (solving for $r = 2$ first will make this easier)

c. Given $3 \mid 9$ and $3 \mid 33$, use proposition 3 to show that $3 \mid 57$.

Solution:
We can re-write 57 as a linear combination of 9 and 33; for example, $9 \cdot (-1) + 33 \cdot 2 = 57$. Thus, $3 \mid 57$ by the water jug theorem.

d. Similarly, use proposition 3 to prove that we *cannot* write 4 as a linear combination of 9 and 15.

Solution:
Assume for the sake of contradiction that there exists s, t such that $4 = 9s+15t$. We know that $3 \mid 9$ and $3 \mid 15$, so by the water jug theorem, $3 \mid 9s + 15t$. However, $3 \nmid 4$, so this is a contradiction.

Modular Congruence

So far, we've worked with rem as a *function* that outputs the remainder. Now, we will look at the concept of remainders as a relation. We say that two numbers are related (mod m) if they have the same remainder when divided by m. We denote this relation with $\pmod m$.

Definition 4. If m is a positive integer, we say the integers a and b are congruent modulo m, and write $a \equiv b \pmod m$, iff they have the same remainder on division by m.

For instance,

$$5 \equiv 2 \pmod 3$$

since their remainders are both 2 when divided by 3.

Proposition 5. $a \equiv b \pmod m$ if and only if $m \mid (b - a)$. In other words, a and b have the same remainder upon division by n. *Proving this is an optional task below!*

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.

Task 2

a. What is 4 congruent to mod 2? Write out three solutions for $a \equiv 4 \pmod 2$.

Solution:

{..., -4, -2, 0, 2, 4,...}

b. Write out three solutions for $a \equiv 9 \pmod 5$.

Solution:

{..., -6, -1, 4, 9, 14,...}

c. Write out three solutions for $a \equiv -3 \pmod 7$.

Solution:

{..., -10, -3, 4, 11, 18...}

d. Prove that proposition 5 above is true; that is, $a \equiv b \pmod m$ if and only if $m \mid (b - a)$.

Solution:

We break the proof into two parts for the biconditional:

If $a \equiv b \pmod m$, then there are integers q, q' and r, with $a = qm + r$ and $b = q'm + r$. So, $b - a = (q'm + r) - (qm + r) = (q' - q)m$, which means $m \mid b - a$.

If $m \mid (b - a)$, then there is an x with $b - a = xm$; that is, $b = a + xm$. We

can write a in its divisibility algorithm form as $a = qm + r$. Substitute this and we have $b = qm + r + xm = m(q + x) + r$. This shows that b has the same remainder as a when divided by m, so we have shown that $a \equiv b \pmod{m}$ if $m \mid (b - a)$.

e. *Optional Challenge:*

Solve for x in $2x \equiv 1 \pmod{5}$. Are there multiple answers?

Then, try solving it again with $4y \equiv 1 \pmod{7}$.

Solution:

$x = \{\ldots, 3, 8, 13, \ldots\}$ $y = \{\ldots, 2, 9, 16, \ldots\}$

Pseudo-Random Generators

Many computer applications use random numbers. However, truly random numbers are not actually that easy to generate. As a substitute for random numbers, computers use functions called *pseudo-random number generators* that produce numbers having many of the statistical properties of random numbers but are in fact deterministically generated.

Devising good pseudo-random number generators is an on-going research topic in computer science. Meanwhile, there are a variety of pseudo-random number generators that are regularly used in practice.

One of the oldest and best known pseudo-random number generators is the linear congruential generator. The linear congruential generator starts with an initial value X_0 and generates each subsequent value as a function of the previous value according to the function

$$X_{n+1} = aX_n + c \pmod{m}$$

The parameters c, a, and m are chosen for efficiency and performance based on statistical tests. Each number generated lies in the range 0 through $m-1$ and can be scaled if a different range is desired.

Optional: Task 3

Let $a = 2$, $c = 7$, $m = 13$, $X_0 = 9$.

Find the first five pseudo-random integers X_1 to X_5.

Solution:

We will use $X_{n+1} = 2X_n + 7 \pmod{13}$ to find $X_1 ... X_5$, where $X_0 = 9$.

$X_1 = 2 \cdot 9 + 7 \pmod{13} = 12$

$X_2 = 2 \cdot 12 + 7 \pmod{13} = 5$

$X_3 = 2 \cdot 5 + 7 \pmod{13} = 4$

$X_4 = 2 \cdot 4 + 7 \pmod{13} = 2$

$X_5 = 2 \cdot 2 + 7 \pmod{13} = 11$

Checkpoint 1 — call over a TA!

More Properties and Theorems

Definition 6. Two integers a and b are relatively prime if $\gcd(a, b) = 1$, i.e., their largest common factor is 1.

Definition 7 (Euler's Phi Function)**.** Euler's ϕ function is defined mathematically as follows:

$$\phi(n) = |\{k \in \mathbb{Z} \mid 1 \leq k \leq n \text{ s.t. } \gcd(n, k) = 1\}|.$$

That is, it counts the number of integers between 1 and n (inclusive of 1) that are relatively prime to n itself.

Proposition 8. If p is a prime number, then $\phi(p) = p - 1$. This is because every number from 1 to $p - 1$ are relatively prime to p itself.

Proposition 9. Euler's ϕ function is *multiplicative* on prime numbers. That is, for prime numbers p and q,

$$\phi(pq) = \phi(p)\phi(q) = (p - 1)(q - 1)$$

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 10. 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 the gcd can always be written as a linear combination of a and b.

Theorem 11. The congruence $ax \equiv c \pmod m$ has a solution if and only if the $\gcd(a, m)$ divides c.

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

Theorem 12 (Fermat's Little Theorem)**.** Let p be a prime. If $gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod p$

Theorem 13 (Euler-Fermat Theorem)**.** If $gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod m$.

Task 4

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

Solution:

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

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

Solution:

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

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

Solution:

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

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

Solution:

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

Task 5

GCD Practice

In lecture, we discussed using both prime factorization and the Euclidean algorithm as two methods to calculate the gcd. We will practice using these two methods to find $\gcd(44, 96)$.

a. Write out the prime factorization of 44 and 96.

Example: $36 = 2^2 \cdot 3^2$

Solution:

$44 = 2^2 \cdot 11$

$96 = 2^5 \cdot 3$

b. Use the prime factorization of 44 and 96 to find $\gcd(44, 96)$.

Solution:

The gcd involves all shared primes with the minimum multiplicity, thus, $\gcd(44, 96) = 2^2 = 4$.

c. Use the Euclidean algorithm to find $\gcd(44, 96)$.

Hint: Recall that $\gcd(x, y) = \gcd(\text{rem}(y, x), x)$.

Solution:

$$96 = 2 \cdot 44 + 8$$
$$44 = 5 \cdot 8 + 4$$
$$8 = 2 \cdot 4 + 0$$

Thus, $\gcd(44, 96) = 4$.

d. Use your equations from part (c) to write $\gcd(44, 96)$ as a linear combination of 44 and 96. Doing so involves substituting remainders from one equation into where it appears in another, until the gcd is in the same equation as 44 and 96.

Solution:

From parts *a* and *b*, we found that $\gcd(44, 96)$. We can use the extended

Euclidean Algorithm to write 4 as a linear combination of 44 and 96.

$$\begin{aligned} 4 &= 44 - 5 \cdot 8 \\ 4 &= 44 - 5 \cdot (96 - 2 \cdot 44) \\ 4 &= 44 - 5 \cdot 96 + 10 \cdot 44 \\ 4 &= 11 \cdot 44 - 5 \cdot 96 \end{aligned}$$

Alternatively, starting from the first equation:

$$\begin{aligned} 8 &= 96 - 2 \cdot 44 \\ 44 &= 5 \cdot (96 - 2 \cdot 44) + 4 \\ 44 &= 5 \cdot 96 - 10 \cdot 44 + 4 \\ 4 &= 11 \cdot 44 - 5 \cdot 96 \end{aligned}$$

Checkpoint 2 — call over a TA!

Multiplicative Inverses

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

Answer: We would multiply both sides by $8^{-1} = \frac{1}{8}$. It is called the multiplicative 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 that happen? Well, 12 is a multiple of 4. For a number to be congruent to 2 mod 12, it must be 2 greater than some multiple of 12 (which is a multiple of 4). However, any $8x$ will be an exact multiple of 4. We can't have a multiple of 4 that is 2 larger than another multiple of 4 — they 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 that is 2 greater than a multiple of 12.

Proposition 14. In general, $ax \equiv c \pmod{m}$ has a solution x if and only if $\gcd(a, m) \mid c$. (In English: if and only if the gcd of a and m divides c.)

We'll prove this fact in the next part of this recitation.

Finding Solutions

Task 6

a. Goal: If $d = \gcd(a, m)$, prove that if $d \mid c$, $ax \equiv c \pmod{m}$ has a solution.

i. Come up with two different equations that involve d. One should come from Definition 1, and the other comes from Theorem 1.

Solution:

$c = kd$ for some $k \in \mathbb{Z}$ (divisibility)

$d = au + mv$ for some $u, v \in \mathbb{Z}$ (the gcd can be written as a linear combination of the two numbers)

ii. Write $ax \equiv c \pmod{m}$ in another equivalent form. Definitions 1 or 4 may help here.

Solution:

$m \mid c - ax$, or equivalently $c - ax = qm$ for some $q \in \mathbb{Z}$

iii. Use your two equations from part (i) to find a solution to x from part (ii).

Solution:

Substituting, we have $c = k(au+mv)$. Rearranging, we get $c-auk = mvk$. Let $x = uk$ and $q = vk$, which forms a solution.

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

You can use the linear combination $4 \cdot 4 + (-1) \cdot 14 = 2$.

Solution:

$\gcd(4, 14) = 2$, and $4 \cdot 4 + (-1) \cdot 14 = 2$. $2 \mid 6$ since $2 \cdot 3 = 6$, so we can use the strategy.

So $k = 3$, $u = 4$, $v = -1$. By part a, $x = k \cdot u = 3 \cdot 4 = 12$

To verify: $14|(6 - 4 \cdot 12) \rightarrow 14|(6 - 48) \rightarrow 14| - 42$ which is true.

Multiplicative Inverses Explained

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

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

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

Solution:

1

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

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

b. Use the technique from part (a) to find the multiplicative inverse of $4 \pmod{9}$.

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

Solution:

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

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

Solution:

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

In lecture, we also talked about using Fermat's Little Theorem and the Euler Phi Function to find multiplicative inverses. They aren't covered in this recitation, but they are very much related, so keep them in mind.

Optional: 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 fact.

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

   Hint: See the third property of modular congruence.

Solution:

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

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

   Recall the multiplicative inverse is the x that solves $10^k x \equiv 1 \pmod 3$.

Solution:

1

c. Prove the "Threes trick" by expanding a number in terms of its digits. That is, represent the number 792 as $7 \cdot 10^2 + 9 \cdot 10^1 + 2 \cdot 10^0$.

Solution:

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

d. 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?

Solution:

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

🏁 Final Checkoff — call over a TA!