Math.3336: Discrete Mathematics

Solving Linear Congruences and Cryptography

Instructor: Dr. Blerina Xhabli

Department of Mathematics, University of Houston

https://www.math.uh.edu/~blerina
Email: blerina@math.uh.edu

Fall 2019
Course Information/Office Hours

- Instructor’s office hours:
  
  MWF 10:00am – 11:00am, 1:00pm – 2:00pm (202 PGH)

- An’s office hours:
  
  Friday 3:00pm – 5:00pm at Fleming, Room 11

- Course webpage:
  
  http://www.math.uh.edu/~blerina/Math3336F19.html

  The class webpage contains contact info, office hours, slides from lectures, and important announcements.

  Homeworks can be found in your CASA accounts.
Assignments to work on

- Homework #6 due Wednesday, 10/09, 11:59pm
  - No credit unless turned in by 11:59pm on due date
  - Late submissions not allowed, but lowest homework score dropped when calculating grades

- Homework will be submitted online in your CASA accounts.
  - You can find the instructions on how to upload your homework in our class webpage.
Chapter 4 – Number Theory and Cryptography

Chapter 4 – Overview

Section 4.1: Divisibility and Modular Arithmetic ✓

Section 4.2: Integer Representations and Algorithms*

Section 4.3: Primes and Greatest Common Divisors ✓

Section 4.4: Solving Congruences

Section 4.5: Applications of Congruences*

Section 4.6: Cryptography
Prime Numbers

- A positive integer $p$ that is greater than 1 and divisible only by 1 and itself is called a **prime number**, otherwise $p$ is called a **composite number**.

- **Fundamental Thm:** Every positive integer greater than 1 is either prime or can be written **uniquely** as a product of primes. This unique product of prime numbers for $x$ is called the **prime factorization** of $x$.

- **Theorem:** If $n$ is composite, then it has a prime divisor less than or equal to $\sqrt{n}$.

- **Corollary:** If $n$ does not have a prime divisor $\leq \sqrt{n}$, then $n$ is prime.

- **Theorem:** There are infinitely many prime numbers.
Greatest Common Divisors and Least Common Multiples

- Suppose $a$ and $b$ are integers, not both 0. Then, the largest integer $d$ such that $d|a$ and $d|b$ is called greatest common divisor of $a$ and $b$, written $\text{gcd}(a,b)$.

- Two numbers whose gcd is 1 are called relatively prime.

- The least common multiple of $a$ and $b$, written $\text{lcm}(a,b)$, is the smallest integer $c$ such that $a|c$ and $b|c$.

- **Theorem:** Let $a$ and $b$ be positive integers. Then, 
  \[ ab = \text{gcd}(a, b) \cdot \text{lcm}(a, b) \]
Euclidean Algorithm

- **Theorem:** Let \( a = bq + r \). Then, \( \gcd(a, b) = \gcd(b, r) \)

Here is how this algorithm functions:
GCD as Linear Combination

- **gcd**$(a, b)$ can be expressed as a linear combination of $a$ and $b$

- **Bezout’s Theorem**: If $a$ and $b$ are positive integers, then there exist integers $s$ and $t$ such that:

\[
gcd(a, b) = s \cdot a + t \cdot b.
\]

- This is called the **Bezout’s identity**, and $s$ and $t$ are the **Bezout’s coefficients**.

- Euclidean algorithm gives us a way to compute these integers $s$ and $t$, which we call the **Extended Euclidean Algorithm**.
A Useful Result

**Lemma:** If $a, b$ are relatively prime and $a \mid bc$, then $a \mid c$.

**Proof:** Since $a, b$ are relatively prime $\gcd(a, b) = 1$

By previous theorem, there exists $s, t$ such that $1 = s \cdot a + t \cdot b$

Multiply both sides by $c$: $c = csa + ctb$

By earlier theorem, since $a \mid bc, a \mid ctb$

Also, by earlier theorem, $a \mid csa$

Therefore, $a \mid csa + ctb$, which implies $a \mid c$ since $c = csa + ctb$
Lemma: If $a, b$ are relatively prime and $a \mid bc$, then $a \mid c$.

- Suppose $15 \mid 16 \cdot x$
- Here 15 and 16 are relatively prime
- Thus, previous theorem implies: $15 \mid x$
Question

- Recall the multiplication of a congruences by an integer: If \( a \equiv b \pmod{m} \), then \( ca \equiv cb \pmod{m} \) for any \( c \in \mathbb{Z} \).

- Suppose \( ca \equiv cb \pmod{m} \). Does this imply \( a \equiv b \pmod{m} \)? No.

- **Counterexample:** Consider \( 14 \equiv 8 \pmod{6} \)

- Thus, \( 2 \cdot 7 \equiv 2 \cdot 4 \pmod{6} \)

- But \( 7 \not\equiv 4 \pmod{6} \)

- Therefore, this implication does not hold in the general case!

- However, if \( c \) and \( m \) are relatively prime, it does hold.
Dividing Congruences by an Integer

- **Theorem:** If $ca \equiv cb \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$

- **Proof:** Since $ca \equiv cb \pmod{m}$, we have $m | ca - cb$

- Rewriting, we get: $m | c(a - b)$

- Since $m, c$ are relatively prime, previous thm implies $m | a - b$

- By definition of congruence, $a \equiv b \pmod{m}$
Examples

- If $15x \equiv 15y \pmod{4}$, is $x \equiv y \pmod{4}$?
  
  Yes, because $15, 4$ are relatively prime

- If $8x \equiv 8y \pmod{4}$, is $x \equiv y \pmod{4}$?

  No, because $8$ and $4$ are NOT relatively prime
  
  Counterexample: $8 \cdot 2 \equiv 8 \cdot 3 \pmod{4}$, but $2 \not\equiv 3 \pmod{4}$
Section 4.4 – Linear Congruences

Highlights of Section 4.4

- Linear Congruences
- The Chinese Remainder Theorem
- Fermat’s Little Theorem and Applications
Section 4.4 – Linear Congruences

- A congruence of the form $ax \equiv b \pmod{m}$ where $a$, $b$, $m$ are integers and $x$ a variable is called a linear congruence.

- Given such a linear congruence, often need to answer:
  1. Are there any solutions?
  2. What are the solutions?

- The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers $x$ that satisfy the congruence.

- Observe: Determining if this congruence has a solution is the same as determining if the equality $ax - mk = b$ has integer solutions.
Theorem: The linear congruence $ax \equiv b \pmod{m}$ has solutions iff $\gcd(a, m) | b$.

Proof involves two steps:

1. If $ax \equiv b \pmod{m}$ has solutions, then $\gcd(a, m) | b$.

2. If $\gcd(a, m) | b$, then $ax \equiv b \pmod{m}$ has solutions.

First prove (1), then (2).
If $ax \equiv b \pmod{m}$ has solutions, then $\gcd(a, m) | b$.

- Suppose $c$ is a solution to $ax \equiv b \pmod{m}$, i.e., $ac \equiv b \pmod{m}$, and denote $d = \gcd(a, m)$.

- Then, $m | (ac - b)$, i.e. there is a $k$ such that $ac - b = mk$.

- Rewrite as $b = ac - mk$.

- We have $d | a$ and $d | m$; hence, $d | (ac - mk)$.

- Since $b = ac - mk$, we have $d | b$, i.e. $\gcd(a, m) | b$. 

\[ \square \]
If \( \gcd(a, m) | b \), then \( ax \equiv b \pmod{m} \) has solutions.

- Let \( d = \gcd(a, m) \) and suppose \( d | b \)

- Then, there is a \( k \) such that \( b = dk \)

- By earlier theorem, there exist \( s, t \) such that \( d = s \cdot a + t \cdot m \)

- Multiply both sides by \( k \): \( dk = a \cdot (sk) + m \cdot (tk) \)

- Since \( b = dk \), we have \( b - a \cdot (sk) = m \cdot tk \)

- Thus, \( b \equiv a \cdot (sk) \pmod{m} \)

- Hence, \( sk \) is a solution.
Examples

- Does $5x \equiv 7 \pmod{15}$ have any solutions? No because $5 \nmid 7$

- Does $3x \equiv 4 \pmod{7}$ have any solutions? Yes because $1 \mid 4$, one solution is 6

- **Note**: This result generalizes to linear Diophantine equations

- Equality $a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = b$ has integer solutions iff
  \[
  \gcd(a_1, a_2, \ldots, a_n) \mid b
  \]

- Previous result just an instance of this because
  $ax \equiv b \pmod{m}$ can be written as $ax - mk = b$
Examples

- Does $77x + 42y = 35$ have integer solutions?
  - Yes because $7 | 35$

- Does $6x + 9y + 12z = 7$ have integer solutions?
  - No because $3 \nmid 7$
Inverse Modulo $m$

- The inverse of $a$ modulo $m$, written $\bar{a}$ has the property:
  \[ a\bar{a} \equiv 1 \pmod{m} \]

- **Theorem**: Inverse of $a$ modulo $m$ exists if and only if $a$ and $m$ are relatively prime.

- **Proof**: Inverse must satisfy $ax \equiv 1 \pmod{m}$

  By previous thm, this equation has a solution iff $\gcd(a, m) | 1$

  Thus, $\gcd(a, m)$ must be 1

- Does 3 have an inverse modulo 7? Yes because $\gcd(3,7) = 1$
Finding Solutions to $ax \equiv 1 \pmod{m}$

1. Find an inverse of 3 modulo 7.

- An inverse is any solution to $3x \equiv 1 \pmod{7}$
- Apply Euclidean algorithm: $7 = 2 \cdot 3 + 1$ and $3 = 3 \cdot 1 + 0$
- Thus $\gcd(3, 7) = 1 = 3 \cdot (-2) + 7 \cdot (1) \Rightarrow s = -2 \& t = 1$.
- Thus, $-2$ is an inverse of 3 modulo 7
- $5, 12, -9, \ldots$ are also inverses, or in other words they are solutions to $3x \equiv 1 \pmod{7}$.
- **Observe:** All inverses of $a$ modulo $m$ are congruent modulo $m$. 
The solution to $3x \equiv 1 \pmod{7}$ is

$$x = -2 + 7u, \ u \in \mathbb{Z}.$$ 

Checking that $x = -2 + 7u$ is a solution to the given linear congruence is easy:

$$3x = 3(-2 + 7u)$$
$$= -6 + 21u$$
$$\equiv -6 + 0 \pmod{7}$$
$$\equiv 1 \pmod{7}$$
Finding Solutions to $ax \equiv 1 \pmod{m}$

2. Find inverse of 2 modulo 5.

- Need to solve the congruence $2x \equiv 1 \pmod{5}$

- What are $s, t$ such that $2s + 5t = 1$?

- Using Euclidean algorithm, one can easily calculate $\text{gcd}(2, 5) = 1 = 2 \cdot (3) + 5 \cdot (-1) \Rightarrow s = 3 \land t = -1$.

- Thus, 3 is an inverse of 2 modulo 5.

- 8, 13, −2, −7 . . . are also inverses, or in other words they are solutions to $2x \equiv 1 \pmod{7}$. 
The solution to $2x \equiv 1 \pmod{5}$ is

$$x = 3 + 5u, \ u \in \mathbb{Z}.$$ 

Checking that $x = 3 + 5u$ is a solution to the given linear congruence is easy:

$$2x = 2(3 + 5u) = 6 + 10u \equiv 1 + 0 \pmod{5} \equiv 1 \pmod{5}$$
Finding Solutions to \( ax \equiv 1 \pmod{m}, \ \gcd(a, m) = 1 \)

- The linear congruence \( ax \equiv 1 \pmod{m} \) has a solution iff \( \gcd(a, m) = 1 \).

- By using Euclidean algorithm, one can find \( s \) and \( t \) such that

\[
\gcd(a, m) = 1 = a \cdot s + m \cdot t
\]

where \( s \) is the inverse of \( a \) modulo \( m \).

- Then, the solution to \( ax \equiv 1 \pmod{m} \) is

\[
x = s + mu, \ u \in \mathbb{Z}
\]
Finding Solutions to $ax \equiv b \pmod{m}$, $\gcd(a, m) = 1$

- We can solve the linear congruence $ax \equiv b \pmod{m}$, by multiplying both sides by the inverse of $a$ modulo $m$.

- Since $\gcd(a, m) = 1 = a \cdot s + m \cdot t$, then we know $s$ is the inverse of $a$ modulo $m$.

- Thus we multiply both sides of $ax \equiv b \pmod{m}$ by $s$:

$$s \cdot ax \equiv s \cdot b \pmod{m}$$

- Because $s \cdot a \equiv 1 \pmod{m}$, we get

$$x \equiv s \cdot b \pmod{m}$$

- The solution to $ax \equiv b \pmod{m}$ is

$$x = sb + mu, \ u \in \mathbb{Z}.$$
Example 3

- Find the solutions to the linear congruence $3x \equiv 4 \pmod{7}$.

  - We have $\gcd(3, 7) = 1 = 3 \cdot (-2) + 7 \cdot (1)$, i.e. $-2$ is an inverse of $3$ modulo $7$.

  - Then multiplying both sides of $3x \equiv 4 \pmod{7}$ by $-2$, we get
    
    $$x \equiv -2 \cdot 4 \pmod{7} \rightarrow x \equiv 6 \pmod{7}$$

  - As a result, the solution to $3x \equiv 4 \pmod{7}$ is
    
    $$x = 6 + 7u, \ u \in \mathbb{Z}.$$
Example 4

- Find the solutions to the linear congruence $5x \equiv 3 \pmod{6}$.

- We have $\gcd(5, 6) = 1 = 5 \cdot (-1) + 6 \cdot (1)$, i.e. $-1$ is an inverse of $5$ modulo $6$.

- Then multiplying both sides of $5x \equiv 3 \pmod{6}$ by $-1$, we get
  
  $$x \equiv -1 \cdot 3 \pmod{6} \rightarrow x \equiv 3 \pmod{6}$$

- As a result, the solution to $5x \equiv 3 \pmod{6}$ is
  
  $$x = 3 + 6u, \ u \in \mathbb{Z}.$$
Example 5

- Find the solution to the linear congruence $6x \equiv 8 \pmod{14}$.

  - Note that $\gcd(6, 14) = 2$ and $2|8$, therefore there is a solution to this congruence.

  - Since $\gcd(6, 14) \neq 1$, then we cannot apply the method we did previously.

  - Instead we will show that $6x \equiv 8 \pmod{14}$ is equivalent to $3x \equiv 4 \pmod{7}$. Dividing the congruence modulo $m$ by the $\gcd$, produces a new equivalent congruence modulo $m/\gcd$.

  - **Lemma**: Let $d = \gcd(a, m) = as + mt$. If $d|b$, then the linear congruences

    
    $$ax \equiv b \pmod{m} \text{ and } \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

    

    have exactly the same solutions.
Lemma: Let $d = \gcd(a, m) = as + mt$. If $d \mid b$, then the linear congruences

$$ax \equiv b \pmod{m} \quad \text{and} \quad \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

have exactly the same solutions.

Note that if $\gcd(a, m) = d$, then $\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$.

Based on this result, it is enough to find the solutions to

$$3x \equiv 4 \pmod{7}.$$ 

As done in Example 3, the solution is $x = 6 + 7u$, $u \in \mathbb{Z}$. 
Solving Systems of Linear Congruences

- To be continued on Wednesday, 10/09.