CS 5002: Discrete Structures **Fall 2018**

Lecture 5: October 4, 2018 [1]

Instructors: Tamara Bonaci, Adrienne Slaugther

Number Theory

Readings for this week:
Rosen, Chapter 4.1, 4.2, 4.3, 4.4

5.1 Overview

1. Review: set theory
2. Review: matrices and arrays
3. Number theory: divisibility and modular arithmetic
4. Number theory: prime numbers and greatest common divisor (gcd)
5. Number theory: solving congruences
6. Number theory: modular exponentiation and Fermat's little theorem

5.2 Introduction

In today's lecture, we will dive into the branch of mathematics, studying the set of integers and their properties, known as **number theory**. Number theory has very important practical implications in computer science, but also in our every day life. For example, secure online communication, as we know it today, would not be possible without number theory because many of the encryption algorithms used to enable secure communication rely heavily of some famous (and in some cases, very old) results from number theory.

We will first introduce the notion of divisibility of integers. From there, we will introduce modular arithmetic, and explore and prove some important results about modular arithmetic. We will then discuss prime numbers, and show that there are infinitely many primes. Finaly, we will explain how to solve linear congruences, and systems of linear congruences.

5.3 Review

5.3.1 Set Theory

In the last lecture, we talked about sets, and some of their properties. Here's the quick summary.

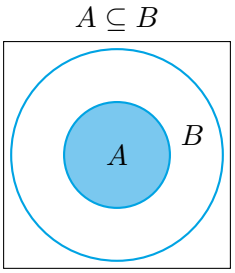
A ***set*** is a group of objects, usually with some relationship or similar property. The objects in the set are called ***elements*** or ***members*** of the set. We use the symbol $\in$ to indicate that an element is or is not in a set:

$$x \in A\text{: } x \text{ is in set } A$$

$$x \notin A\text{: } x \text{ is not in set } A$$

Venn Diagrams

A ***Venn diagram*** is a graphical representation of a set.



Subsets

The set A is a ***subset*** of B if and only if every element of A is also an element of the set B. We use the notation: $A \subseteq B$.

Set Cardinality

Let S be a set. If there are n distinct elements in S (and n is an integer greater than or equal to 0), S is a ***finite set***, and n is the ***cardinality*** or S. The cardinality of S is written $|S|$.

5.3.1.1 Set Operations

- ***Union:*** Let A and B be sets. The **union** of the sets A and B, denoted $A \cup B$ is the set that contains the elements in either A or in B, or in both.
- ***Intersection:*** Let A and B be sets. The **intersection** of the sets A and B, denoted $A \cap B$ is the set that contains the elements in both A and B.

- ***Set complement:*** The **complement** of a set A, denoted A^c is the set of elements that belong to U but which do not belong to A.
- ***Difference of sets:*** The **relative complement** or **difference** of a set B with respect to A, denoted $A \setminus B$ (said A minus B) is the set of elements that belong to A, but which do not belong to B.

5.3.2 Matrices and Arrays

Last lecture, we defined a ***matrix*** as a rectangular array of numbers, and we said that a matrix with m rows and n columns is called an $m \times n$ matrix. Let's recall some matrix operation and properties we mentioned last time.

Matrix Operations and Properties

An ***identity matrix***, denoted as $I \in \mathbb{R}^{n \times n}$ is a square matrix with ones on the diagonal and zeros everywhere else:

$$I_{ij} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$$

A ***diagonal matrix*** is a matrix where all off-diagonal elements are equal to 0, $D = diag(d_1, d_2, \ldots, d_n)$ and

$$D_{ij} = \begin{cases} d_i, i = j \\ 0, i \neq j \end{cases}$$

Note: $I = diag(1, 1, \ldots, 1)$.

Given a matrix $A \in \mathbb{Z}^{m \times n}$, its ***transpose***, denoted $A^T \in \mathbb{Z}^{n \times m}$, is the $n \times m$ matrix whose entries are obtained by "flipping" the rows and the columns of matrix A:

$$(A^T)_{ij} = A_{ji}$$

The following properties of transpose can be easily verified:

- $(A^T)^T = A$
- $(AB)^T = B^T A^T$
- $(A + B)^T = A^T + B^T$

A **square matrix** $A \in \mathbb{Z}^{n \times n}$ is a ***symmetric matrix*** if it holds that:

$$A = A^T$$

A square matrix A is ***anti-symmetric*** if:

$$A = -A^T$$

Matrix Manipulations: The product of two matrices $A \in \mathbb{Z}^{m\times n}$ and $B \in \mathbb{Z}^{n\times p}$ is a new matrix, C, defined as:

$$C = AB := \sum_{k=1}^{n} A_{ik}B_{kj} \in \mathbb{R}^{m\times p}$$

Note: In order for matrix C to exist, the number of columns of matrix A must be equal to the number of rows of matrix B.

Example 1: Please find matrix product AB, if matrices A and B are equal to $A = \begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 4 & 2 \\ 1 & 5 & 3 \end{bmatrix}$.

$$AB = \begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix}\begin{bmatrix} 2 & 4 & 2 \\ 1 & 5 & 3 \end{bmatrix} = \begin{bmatrix} 2\cdot 2+3\cdot 1 & 2\cdot 4+3\cdot 5 & 2\cdot 2+3\cdot 3 \\ 4\cdot 2+1\cdot 1 & 4\cdot 4+1\cdot 5 & 4\cdot 2+1\cdot 3 \end{bmatrix} = \begin{bmatrix} 7 & 23 & 13 \\ 8 & 21 & 11 \end{bmatrix}$$

Some Properties of Matrix-Matrix Manipulation:

- Matrix manipulation is associative: $(AB)C = A(BC)$
- Matrix manipulation is distributive: $A(B + C) = AB + Ac$
- Matrix manipulation in general is **not commutative**, i.e., in general, $AB \neq BA$

Matrix Determinant: The **determinant** of a square matrix $A \in \mathbb{R}^{n\times n}$ is a function $\det : \mathbb{R}^{n\times n} \to \mathbb{R}$, denoted as $|A|$. Before giving the general definition for the determinant, let's define $A \in \mathbb{R}^{n\times n}$ and $A_{\setminus i,\setminus j} \in \mathbb{R}^{(n-1)\times(n-1)}$ as a matrix that results from deleting the i-th row and j-th column from matrix A. The general (recursive) formula for the determinant is now given as:

$$|A| = \sum_{i=1}^{n}(-1)^{i+j}a_{ij}|A_{\setminus i,\setminus j}| = \sum_{j=1}^{n}(-1)^{i+j}a_{ij}|A_{\setminus i,\setminus j}|$$

for any $i, j \in \{1, 2, \ldots, n\}$. The initial case is given as $|A| = a_{11}$ for $A \in \mathbb{R}^{1\times 1}$.

For matrices up to size 3×3, the determinants can be found using the following formulas:

- $|[a_{11}]| = a_{11}$
- $\left|\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\right| = a_{11}a_{22} - a_{12}a_{21}$
- $\left|\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}\right| = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}$

Matrix Inverse: The **inverse** of a square matrix $A \in \mathbb{Z}^{n\times n}$ is denoted as A^{-1}, and it is a **unique** matrix such that:

$$A^{-1}A = AA^{-1} = I \tag{5.1}$$

Note: Not all matrices have an inverse. In particular, we say that matrix A is invertible or **non-singular** if its inverse A^{-1} exits.

5.4 Introduction to Number Theory

Why are numbers beautiful? Its like asking why is Beethoven's Ninth Symphony beautiful. If you dont see why, someone can't tell you. *Paul Erdös(1913–1996)*

After so many math topics we have already explored in this course, you would be perfectly justified to ask why should you care about number theory. There are many important real world reasons, let's mention a few:

- **Secure communication** - many cryptographic algorithms we use today, to make sure our digital communication is confidential, as well as to confirm that some remote entity is who they claim to be, is based on some famous results from number theory.
- **Pseudo random number generators** Many pseudorandom number generators we use today rely on important results from number theory.
- **Digit verification** Many services we use in our regular lives rely on various identification numbers. For example, retail product are often identified by their UPCs (Universal Product Codes). Similarly, books are uniqiely identified by their ISBNs (International Standard Book Numbers). The validity of those numbers is often verified by performing simple modular arithmetic checks on the digits of those numbers.

Let's take a deeper dive into one simple cryptographic example. Let's assume some person, *Alice* wants to send a message to another person, *Bob* over an insecure channel, and that neither *Alice* nor *Bob* want this information to be readable by any other parties.

1. *Alice* takes her original message, referred to as **plaintext**, and encrypts it with a cryptograhic secret, using some encryption function, to generate a secure message, typically referred to as **ciphertext**.
2. She then transmits the ciphertext over the insecure channel.

3. *Bob* knows something about Alice's cryptographic secret, and he has an appropriate **decryption algorithm**.
4. When he receives the ciphertext from Alice, he runs the decryption algorithm, and recovers the original message.

For simplicity, we can assume that Alice and Bob communicate in English, and we know that English alphabet consists of 26 letters. Since our encryption function is just another function, it is often convenient to take those 26 letters of English alpahbet, and map them into some integers. One way to do so is shown in the table below.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 5.1: Mapping of alphabets to numerals

The goal of Alice's encryption function is to take one letter of English alphabet, represented as a number, and map it to some other English letter. For example, Alice may decide to shift every letter of her original message, x_i by some integer K to the right:

$$y_i = x_i + K$$

Let's assume Alice sets her cryptgraphic secret $K = 3$, and does the following:

$$\begin{aligned} \text{Letter A: } & 0 + 3 = 3 \\ \text{Letter B: } & 1 + 3 = 4 \\ & \vdots \\ \text{Letter Y: } & 24 + 3 = 27 \\ \text{Letter Z: } & 25 + 3 = 28 \end{aligned}$$

An important question immediately arises: how does Alice convert these numbers back to some cyphertext, when there do not exist numbers 26, 27, 28 in her table?

To see the answer to these and other important question, let's dive into modular arithmetic.

5.5 Divisibility and Modular Arithmetic

5.5.1 Divisibility

We start our exploration of number theory by defining the notion of divisibility.

Definition 5.1 *If a and b are integers such that $a \neq 0$, we say that **a divides b** if if there exist an integer c such that:*

$$b = ac$$

or equivalently, $\frac{b}{a}$ is an integer.

When a divides b, we say that a is a ***factor*** or ***divisor*** of b, and b is ***multiple*** of a.

Notation:

- Notation $a|b$ denotes that a divides b
- Notation $a \not| b$ denotes that a does not divide b

Theorem 5.2 *Let a, b and c be integers, such that $a \neq 0$. Then it holds:*

1. *If $a|b$ and $a|c$, then $a|(b + c)$*
2. *If $a|b$, then $a|bc$ for all integers c*
3. *If $a|b$ and $b|c$, then $a|c$*

An important question arises: what happens when $a \not| b$? Let's introduce the next theorem to see.

Theorem 5.3 (The Division Algorithm) *Let a be some integer, and d some positive integer. Then there always exist unique integers q and r, where $0 \leq r < d$, such that:*

$$a = dq + r$$

*In the given equation, positive integer d is typically referred to as **divisor**, integer a as **dividend**, and integers q and r as **quotient** and **remainder**, respectively.*

We can now write:

$$q = a \text{ div } d$$
$$r = a \bmod d$$

5.5.2 Modular Arithmetic

In many situations, we care only about a remainder of an integer, when it is divided by some other positive integer, and we have a special notation for it.

Definition 5.4 (Congruence) *Let a and b be integers, $a, b \in \mathbb{Z}$ and let m be a positive integer, $m \in \mathbb{N}$. If m divides $(a - b)$, we can write:*

$$a \equiv b \pmod{m}, \quad or \tag{5.2}$$
$$m|(a - b) \tag{5.3}$$

*The operator $\equiv$ is called congruence and $a \equiv b \pmod{m}$ is read: "a **is congruent to** b **modulo** m." The positive integer m is known as the **modulus**.*

Example 2: Determine whether or not 19 is congruent to 7 modulo 4. We start solving this problem by subtracting 7 from 19, 19 - 7 = 12. We immediately observe that 12 is divisible by 4, such that the quotient $q = 3$, and remainder $r = 0$. Therefore, 19 is congruent ot 7 modulo 4.

Theorem 5.5 *Let m be a positive integer. Then some integers a and b are congruent modulo m if and only if there exists some integer k such that:*

$$a = b + km$$

When working with congruences, we need to be rather careful, since some properties we would expect to hold are actually not valid. Let's explore some of the properties that do hold.

5.5.2.1 Some Properties of Modulo Arithmetic

Let $\mathbb{Z}_m$ denote the set of integers $\{0, 1, 2, \ldots, m - 1\}$.

1. $a \equiv b \pmod{m}$ if and only if $a \pmod{m} = b \pmod{m}$, i.e. the remainders of a and b modulo m are equal.
2. Addition is *closed*: for any $a, b \in \mathbb{Z}_m,\ a + b \in \mathbb{Z}_m$.
3. Addition is *commutative*: for any $a, b \in \mathbb{Z}_m, a + b = b + a$.
4. Addition is *associative*: for any $a, b, c \in \mathbb{Z}_m, (a + b) + c = a + (b + c)$.
5. 0 is an additive identity: for any $a \in \mathbb{Z}_m, a + 0 = 0 + a = a$.
6. The *additive inverse* of any $a \in \mathbb{Z}_m$ is $m - a$: that is $a + (m - a) = (m - a) + a = 0,\ \forall a \in \mathbb{Z}_m$.
7. Multiplication is *closed*: for any $a, b \in \mathbb{Z}_m, ab \in \mathbb{Z}_m$.
8. Multiplication is *commutative*: for any $a, b \in \mathbb{Z}_m, ab = ba$.
9. Multiplication is *associative*: for any $a, b, c \in \mathbb{Z}_m, (ab)c = a(bc)$.
10. 1 is the multiplicative identity: for any $a \in \mathbb{Z}_m, a \times 1 = 1 \times a = a$.
11. The *distributive* property is satisfied: for any $a, b, c \in \mathbb{Z}_m, (a+b)c = (ac) + (bc)$ and $a(b+c) = (ab) + (ac)$.

Properties 1, 3-5, say that $\mathbb{Z}_m$ forms a *group*. Since property 2 also holds, the group is called an *abelian group*. Properties 1-10 make $\mathbb{Z}_m$ a *ring*.

We can also define subtraction in $\mathbb{Z}_m$ as $(a - b) \mod m$.

5.6 Prime Numbers and Greatest Common Divisors

A few important concepts, based on the concept of divisibility are those of **prime, coprime, and composite numbers**. Let's investigate them next.

5.6.1 Prime and Composite Numbers

Definition 5.6 *Some integer p greater than one is called **prime** if its only positive factors are 1 and p. A positive integer that is not a prime is called **composite**.*

When thinking about prime and composite numbers, several questions immediately come to mind. For example:

- How do we show that some positive integer is a prime?
- If an integer isn't a prime, how do we find all of its divisors (factors)?
- How many primes are there anyway?

Let's address all of these questions in order, and in doing so, let's start by introducing an important theorem, **the fundamental theorem of arithmetic**.

5.6.1.1 Unique Prime Factorization

Theorem 5.7 (*Fundamental Theorem of Arithmetic*) *For any integer $m > 1$, there exists an integer n, a set of distinct primes $p_1, \ldots, p_n$, and a set of integers $e_1, \ldots, e_n$ satisfying*

$$m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \tag{5.4}$$

Furthermore, the sequences $p_1, \ldots, p_n$ and $e_1, \ldots, e_n$ are unique up to reordering of the p_i's.

While we won't prove the fundamental theorem of arithmetic, let's take a moment to restate what this theorem says: **every integer greater than 1 can be uniquely written as a prime, or a product of two or more primes.**

Example 3: For $x = 432$,

$$432 = 2^4 \cdot 3^3. \tag{5.5}$$

This factorization is unique up to a rearrangement of the terms on the right hand side (i.e., we can write $3^3 \times 2^4$ instead).

The fundamental theorem of arithmetic has many important consequences, and one such consequence can be expressed as follows.

Theorem 5.8 *If n is a composite integer, then it has a prime divisor less than or equal to $\sqrt{n}$.*

Trivial division: From theorem 5.8, it follows that an integer is a prime if it isn't divisible by any prime less than or equal to its square root. This leads to a brute-force algorithm to check whether or not an integer is a prime.

Note: (The cost of primality testing vs. the cost of prime factorization) In addition to the trivial division, there exist many other algorithms to check whether or not some integer is a prime number. The fastest such algorithm run in polynomial time in the size of the input. Unlike primality testing, however, prime factorization of some integer is considered to be a computationally difficult problem, which cannot be solved nowhere near polynomail time. This fact is used in some of the most popular cryptogrpahic algorithms that we have today.

Let's answer our last question about prime numbers - how many prime numbers there are?

Theorem 5.9 *There are infinitely many prime numbers.*

Proof: To prove theorem 5.9, we will start by assuming the contradiction, that there are only finitely many primes, $p_1, p_2, \ldots, p_n$. Let now define a new integer:

$$Q = p_1 p_2 \ldots p_n + 1$$

By the fundamental theorem of arithmetic, integer Q is either a prime, or it can be written as the product of primes $p_1, p_2, \ldots, p_{mn}$. However, by construction, none of our known primes $p_i, 1 \leq i \leq n$ divides Q, since $Q - p_1 p_2 \ldots p_n = 1$. Therefore, there exists some prime that is not on our finite list of known primes, and that prime is either Q itself, or some other prime that divides Q. **But, that is a contradiction, since we said that there are only finitely many primes,** $p_1, p_2, \ldots, p_n$.
■

5.7 Coprimes and Greatest Common Divisors

A concept closely related to that of prime and composite numbers is that of **coprime** or **relatively prime** numbers. To define it, however, we first need to define the concept if a **greatest common divisor**.

Definition 5.10 *Given two integers $a \neq 0$ and $b \neq 0$, the **greatest common divisor** of a and b (denoted $\gcd(a, b)$) is equal to the largest integer c that divides both a and b.*

Definition 5.11 *Two integers $a \geq 1$ and $m \geq 2$ are said to be **relatively prime** or **coprime** if their greatest common divisor is equal to $gcd(a, m) = 1$.*

Two important questions one can ask, when thiking about relatively prime numbers are:

- Given some positive integer a, how many integers from the set $\mathbb{Z}_a = \{1, 2, \ldots, a-1\}$ are coprime with a?
- How would we generally check whether or not two integers a and b are coprime?

Let's answer those questions next.

5.7.1 Euler Totient Function

As it turn out, the number of integers in $\mathbb{Z}_a$ that are relatively prime to a is known as the ***Euler-phi function***, denoted by $\phi(m)$, and the following theorem holds for it.

Theorem 5.12 *Let*

$$m = \prod_{i=1}^{n} p_i^{e_i}, \tag{5.6}$$

where p_i are distinct primes and $e_i > 0, 1 \leq i \leq n$. Then

$$\phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1}). \tag{5.7}$$

Some properties of the Euler's-phi function:

1. If p is a prime, then numbers $\{1, 2, ..., p-1\}$ are all relatively prime to p, so $\phi(p) = p - 1$.
2. $\phi(p^2) = p^2 - \frac{p^2}{p} = p(p-1)$, since every p^{th} element is divided by p.
3. Similarly, $\phi(p^{e_1}) = p^{e_1}(1 - \frac{1}{p})$, where $e_1 \geq 1$.
4. If m, n are two integers such that $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.
5. As a special case, if p, q are two distinct primes, then $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right). \tag{5.8}$$

Example 4: Let's see how many integers there exist, that are coprime with:

- $\phi(2) = |\{1\}| = 1$.
- $\phi(3) = |\{1, 2\}| = 2$.
- $\phi(4) = |\{1, 3\}| = 2$.
- $\phi(6) = |\{1, 5\}| = 2$.
- $\phi(7) = |\{1, 2, 3, 4, 5, 6\}| = 6$.

How many integers there exist that are coprime with $m = 60$:

$$60 = 2^2 \cdot 3^1 \cdot 5^1, \tag{5.9}$$

and,

$$\phi(m) = (4 - 2) \cdot (3 - 1) \cdot (5 - 1) = 16. \tag{5.10}$$

5.7.2 Euclidean Algorithm

There exist several algorithms that can be used to find the greatest common divisor of two integers. One such algorithm is ***the Euclidean algorithm***, and we are going to exlore it next.

Let's start by showing the Euclidean algorithm in action first, and then we'll explain how it works, and why.

Example 5: Let's find the gcd of $a = 87$ and $b = 24$. Using the Euclidean algorithm, we can write:

$$\begin{aligned} 87 &= 3(24) + 15 \\ 24 &= 1(15) + 9 \\ 15 &= 1(9) + 6 \\ 9 &= 1(6) + 3 \\ 6 &= 2(3) \end{aligned}$$

It follows that $\gcd(87, 24) = 3$.

This Euclidean algorithm finds the gcd of two integers a and b through repeated integer division. First, $r_0 = a$ is divided by $r_1 = b$, and the remainder r_2 is found. In the next step, $r_1 = b$ is divided by r_2 and the remainder r_3 is found. The process continues until the remainder of r_{m-1} divided by r_m is zero. The $\gcd(a, b) = \gcd(r_0, r_1)$ is the last non-zero divisor, namely r_m. The general steps of the division algorithm are as follows:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ r_2 &= q_3 r_3 + r_4 \\ \cdots &\quad \cdots \\ r_{m-2} &= q_{m-1} r_{m-1} + r_m \\ r_{m-1} &= q_m r_m \end{aligned}$$

And the pseudocode of the algorithm is given below:

EUCLIDEAN ALGORITHM
Input: Positive integers a and b
Output: Greatest common divisor d of a and b
$r_0 \leftarrow a$
$r_1 \leftarrow b$
$m \leftarrow 1$
while $r_m \neq 0$
  $q_m \leftarrow \lfloor \frac{r_{m-1}}{r_m} \rfloor$
  $r_{m+1} \leftarrow r_{m-1} - q_m r_m$
  $m \leftarrow m + 1$
end while
$m \leftarrow m - 1$
$d \leftarrow r_{m-1}$
return d

Figure 5.1: The Euclidean algorithm. Finds the greatest common divisor of a and b, where $a > b$.

The Euclidean algorithm is based on the following result about greatest common divisors and the division algorithm.

Theorem 5.13 *Let $a = bq + r$, where a, b, q and r are integrs. Then* $\gcd(a, b) = \gcd(b, r)$.

Using theorem 5.13, let's now consider the equation $r_i = q_{i+1}r_{i+1} + r_{i+2}$. It follows that the relationship between the divisor r_{i+1} and the remainder r_{i+2} is given by $0 \leq r_{i+2} < r_{i+1}$. We also assumed that $r_0 > r_1$. Hence, we can write $r_0 > r_1 > r_2 > \cdots r_m$.

Example 6: Let's use the **Euclidean algorithm** to find the greatest common divisor (gcd) of the following pairs of numbers:

1. $a = 96, b = 15$,
2. $a = 96, b = 16$, and
3. $a = 96, b = 17$,

1. Numbers $a = 96$ and $b = 15$ are both divisible by three, but not by six or nine, so by inspection, we conclude that their gcd is 3. Let's check that using the Euclidean algorithm:

$$96 = 6(15) + 6 \tag{5.11}$$
$$15 = 2(6) + 3 \tag{5.12}$$
$$6 = 2(3) \tag{5.13}$$

   From equation (5.13), we see that $\gcd(96, 15)$ indeed is three.
2. Number $a = 96$ is divisible by $b = 16$ without remainder, so again by inspection, we conclude that their greatest common divisor is 16:

$$96 = 6(16) + 0 \tag{5.14}$$

3. Number $b = 17$ is a prime number (divisible only by one and by itself), so it should be the case that the greatest common divisor of numbers $a = 96$ and $b = 17$ is one. Let's check if that is true using the Euclidean algorithm:

$$\begin{aligned} 96 &= 5(17) + 11 && (5.15)\\ 17 &= 1(11) + 6 && (5.16)\\ 11 &= 1(6) + 5 && (5.17)\\ 6 &= 1(5) + 1 && (5.18)\\ 5 &= 5(1) && (5.19) \end{aligned}$$

From equation (5.19) it now clearly follows that $\gcd(96, 17)$ is one.

5.7.3 gcds as Linear Combination

An important result that we will use in the rest of this lecture is the fact that the greatest common divisor of some integers a and b can be expressed as a **linear combination of a and b**, and their corresponding linear coefficients. Let's explore this fact further, to see how might that be possible, and how do we use it.

Theorem 5.14 ***(Bezout's theorem)*** *Let a and b be positive integers, and let $d = \gcd(a, b)$. Then there exist integers x and y such that*

$$ax + by = d \tag{5.20}$$

and integers x and y are called ***Bezout's coefficients****.*

One algorithm that we can use to find x and y is the **extended Euclidean algorithm**, with the pseudocode given below. We will see some more examples of how to use Extended Euclidean algorithm, and the importance of the Bezout's coefficents in the next section.

5.8 Linear Congruences and Modular Inverses

Definition 5.15 ***(Linear congruence)*** *A congruence of the form:*

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

where m is a positive integer, a and b are integers, and x is a variable is called a **linear congruence**.

The question arises: how does one solve such linear congruences? We know what we would do if this was a regular linear equation - we would try to find an inverse of a, and apply it to the both sides of the equation. As it turns out, we do something similar with linear congruences too. Let's explore.

Definition 5.16 ***(Modular multiplicative inverse)*** *The modular multiplicative inverse of an integer $a \in \mathbb{Z}_m$ modulo m, denoted as $a^{-1} \pmod{m}$, is an element $a' \in \mathbb{Z}_m$ such that:*

$$a \cdot a' \equiv a' \cdot a \equiv 1 \pmod{m} \tag{5.21}$$

EXTENDED EUCLIDEAN ALGORITHM
Input: Positive integers a and b
Output: Integers r, s, and t such that $r = \gcd(a, b)$ and $sa + tb = r$

$a_0 \leftarrow a$
$b_0 \leftarrow b$
$t_0 \leftarrow 0$
$t \leftarrow 1$
$s_0 \leftarrow 1$
$s \leftarrow 0$
$q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor$
$r \leftarrow a_0 - qb_0$
while $r > 0$
  $temp \leftarrow t_0 - qt$
  $t_0 \leftarrow t$
  $t \leftarrow temp$
  $temp \leftarrow s_0 - qs$
  $s_0 \leftarrow s$
  $s \leftarrow temp$
  $a_0 \leftarrow b_0$
  $b_0 \leftarrow r$
  $q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor$
  $r \leftarrow a_0 - qb_0$
end while
$r \leftarrow b_0$
return (r, s, t)

Figure 5.2: The extended Euclidean algorithm.

Given the modular multiplicative inverse, some congruence $ax \equiv b \pmod{m}$ can be solved for x as follows:

$$\begin{aligned} ax &\equiv b \pmod{m} \\ \underbrace{a^{-1}(ax)}_{x} &\equiv a^{-1}(b) \pmod{m} \end{aligned}$$

5.8.1 Problems with Modular Inverses

Not all integers $a \in \mathbb{Z}_m$ have a modular multiplicative inverse under modulo m. As an example, integers $a = 2$ and $a = 13$ do not have a multiplicative inverse in $\mathbb{Z}_{26}$.
That opens up some important questions:

- When does an integer $a \in \mathbb{Z}_m$ have a modular multiplicative inverse under modulo m?
- If an integer $a \in \mathbb{Z}_m$ have a modular multiplicative inverse under modulo m, how do we find it?

Let's answer them in order.

Theorem 5.17 ***(Existance of modular multiplicative inverse)*** *Consider some integers a and $m > 1$. If $gcd(a, m) = 1$, then a has a unique modular multiplicative inverse under module m.*

Theorem 5.18 ***(Modular inverse and Bezout's coefficients)*** *An integer a has an inverse $\pmod{m}$ if and only if there exist numbers p and q such thar*

$$ap + qm = 1 \pmod{m} \tag{5.22}$$

Proof: Let's rewrite equation (5.22) as:

$$1 \equiv ap \pmod{m} \tag{5.23}$$

Equation (5.23) implies that a has a modular multiplicative inverse $p \pmod{m}$. Let's now recall that some number $r \equiv 1 \pmod{m}$ if and only we can write:

$$r + bm = 1 \tag{5.24}$$

for some b, implying that $ap \equiv 1 \pmod{m}$ if and only if it holds that:

$$ap + mq = 1 \tag{5.25}$$

for some q. Equation (5.25) is, in turn, valid only if $\gcd(a, m) = 1$. To see why, let $c = \gcd(a, m)$ and suppose $c > 1$. Then there exist positive integers α, β satisfying $a = \alpha c$ and $m = \beta c$. If $ap + mq = 1$ for some p, q, then $pc\alpha + qc\alpha = 1$, hence $c(p\alpha + q\alpha) = 1$. This is a contradiction since there are no positive integers that divide 1 (except 1 itself).
The other direction of the theorem is also true: if $\gcd(a, m) = 1$, then there exist integers p, q satisfying equation (5.22). These integers can be computed using the extended Euclidean algorithm, and integer p is a modular multiplicative inverse of $a \pmod{m}$. ■
Now that we know when some integer a has a modular multiplicative inverse, a question that immediately comes to mind is: suppose we have Bezout's coefficients, p and q. Can we use them to find the inverse of a modulo b?

The answer is **we can use the Extended Euclidean algorithm.** Let's see how on the following example.

Example: Let $a = 7$, $m = 26$. Find $a^{-1} \bmod m$.
First, let's look at the Euclidean algorithm.

$$26 = 3(7) + 5 \tag{5.26}$$
$$7 = 1(5) + 2 \tag{5.27}$$
$$5 = 2(2) + 1 \tag{5.28}$$

Now, let's rewrite the last equation to put the gcd (which is 1) on to the left-hand side of the equation.

$$1 = 5 - 2(2) \tag{5.29}$$

From Eq. (5.28), we have:

$$2 = 7 - 5 \tag{5.30}$$

Substituting Eq. (5.30) into Eq. (5.29) yields

$$1 = 5 - 2(7 - 5) = 3(5) - 2(7) \tag{5.31}$$

We're almost there; the last step is to use Eq. (5.27), as follows:

$$5 = 26 - 3(7) \tag{5.32}$$

so that

$$1 = 3(26 - 3(7)) - 2(7) = 3(26) - 11(7) \tag{5.33}$$

And so $7^{-1} \bmod 26 = -11 \bmod 26 = 15 \bmod 26$.
Example 7: Let $a = 9$, $m = 26$. Find $a^{-1} \bmod m$.
We first use the Euclidean algorithm to check whether or not the multiplicative modular inverse exists.

$$26 = 2(9) + 8 \tag{5.34}$$
$$9 = 1(8) + 1 \tag{5.35}$$
$$8 = 8(1) \tag{5.36}$$
$$\tag{5.37}$$

Since $\gcd(9, 26) = 1$, the modular multiplicative inverse exists, and we can use the Extended Euclidean algoirthm to find it. First, let's rewrite the last equation to put the gcd (which is 1) on to the left-hand side of the equation.

$$1 = 9 - 1(8) \tag{5.38}$$

From Eq. (5.34), we have:

$$8 = 26 - 2(9) \tag{5.39}$$

Substituting equation (5.39) into equation (5.38), we get:

$$1 = 9 - 1\{26 - 2(9)\} = 3(9) - 26 \tag{5.40}$$

From equation (5.40), we can read off the modular multiplicative inverse of $a = 9$ to be $a^{-1} = 3$ under modulo $m = 26$ arithmetic.
Let's see one more example.
Example 8: Let's use the Extended Euclidean algorithm again to find the modular multiplicative inverse of number $a = 27$ under modulo $b = 5$.

We start by first using the Euclidean algorithm as follows:

$$27 = 5(5) + 2 \tag{5.41}$$
$$5 = 2(2) + 1 \tag{5.42}$$

Equation (5.42) can now be rewritten as:

$$1 = 5 - 2(2) \tag{5.43}$$

Similarly, equation (5.42) can be rewritten as:

$$2 = 27 - 5(5) \tag{5.44}$$

By plugging equation (5.44) into equation (5.43), we get:

$$1 = 5 - 2(27 - 5(5)) \tag{5.45}$$
$$1 = 5 - 2(27) + 5(5) \tag{5.46}$$
$$1 = 6(5) - 2(27) \tag{5.47}$$

We now apply modulo (5) on equation (5.47):

$$1 = 6(5) - 2(27)(\text{mod}5) \tag{5.48}$$
$$1 \equiv -2(27)(\text{mod}5) \tag{5.49}$$

From equation (5.49), it follows that -2 is modular multiplicative inverse of 27 under modulo 5 arithmetic:

$$a^{-1} = -2 \equiv 3(\text{mod}5) \tag{5.50}$$

5.8.2 Systems of Congruences and the Chinese Remainder Theorem

We now know when one linear congruence has a solution, and how to find it using the Extended Euclidean algorithm. Interesting questions to ask are:

- When does a system of linear congruences have a solution?
- If the system of linear congruences has a solution, how do we find it?

To answer these questions, let's take a look at the very old, and very famous **Chinese reminder theorem**.

5.8.3 The Chinese Remainder Theorem

Theorem 5.19 ***(Chinese Remainder Theorem)*** *Let $m_1, m_2, \ldots, m_r$ be integers such that every m_i, m_j where $i \neq j$ are relatively prime, i.e.gcd$(m_i, m_j) = 1$. Then for any integers $a_1, a_2, \ldots, a_r$ the set of congruences:*

$$X \equiv a_i \mod m_i, \quad i = 1, 2, \ldots, r \tag{5.51}$$

has a unique solution modulo M, where $M = m_1 m_2 \ldots m_r = \prod_{i=1}^{r} m_i$. The solution is given as:

$$X = \left(\sum_{i=1}^{r} a_i M_i y_i \right) \mod M \tag{5.52}$$

where $M_i = \frac{M}{m_i}$ and $y_i = M_i^{-1} \mod m_i$

Proof: Let $M_i = \frac{M}{m_i}$. Note that $\gcd(M_i, m_i) = 1$.Let $y_i = M_i^{-1} \pmod{m_i} \rightarrow M_i y_i = 1 \pmod{m_i}$ (The inverse exists because $\gcd(M_i, m_i) = 1$, and can be found using the Extended Euclidean Algorithm). Let $\rho(a_1, a_2, \ldots, a_r) = \sum_{i=1}^{r} a_i M_i y_i \pmod{M}$. We can then write $\rho(a_1, a_2, \ldots, a_r) = \sum_{i=1}^{r} a_i M_i y_i + \lambda M$, where λ is an integer. Note that $M = 0 \pmod{m_i}, 1 \leq i \leq r$.

Set $X = \rho(a_1, a_2, \ldots, a_r)$ and let $1 \leq j \leq r$. Consider a term of ρ reduced modulo m_j. If $i = j$, then $a_i M_i y_i = a_i \pmod{m_i}$, because $M_i y_i \equiv 1 \pmod{m_i}$. If $i \neq j$, then $a_i M_i y_i \equiv 0 \pmod{m_j}$ since $m_j | M_i$. Hence $X = (\sum_{i=1}^{r} a_i M_i y_i) \pmod{m_j} \equiv a_j \pmod{m_j}$. This is true for all j and hence X is a solution to the system of congruences. This solution can also be shown to be unique modulo M since the cardinalities of the domain and the range are equal. ■

Example 9: Solve the system of congruences:

$$X \equiv 5 \pmod 7 \tag{5.53}$$
$$X \equiv 3 \pmod{11} \tag{5.54}$$
$$X \equiv 10 \pmod{13} \tag{5.55}$$
$$\tag{5.56}$$

Step 1 Let's setup the problem. We have three congruences, where $m_1 = 7, m_2 = 11, m_3 = 13, a_1 = 5, a_2 = 3, a_3 = 10$. We can compute M to be equal to $M = 7 \cdot 11 \cdot 13 = 1001$.
Step 2 Now we can compute $M_1 = \frac{M}{m_1} = 143, M_2 = 91, M_3 = 77$.
Step 3 Using the extended Euclidean algorithm, we can find modular multiplicative inverses of M_i-s to be equal to $y_1 = 5, y_2 = 4$ and $y_3 = 12$. Please note here that modular multiplicative inverse y_i of M_i is found with respect to modulo m_i.
Step 4 We can compute the solution X as follows:

$$X = (5 \cdot 143 \cdot 5) + (3 \cdot 91 \cdot 4) + (10 \cdot 77 \cdot 12) \mod 1001 = 894$$

Step 5 Finally, we can check our solution, and verify that:

$$894 \equiv 5 \pmod 7$$
$$894 \equiv 3 \pmod{11}$$
$$894 \equiv 10 \pmod{13}$$

5.9 Euler's Theorem

Theorem 5.20 (Euler's Theorem:) *Given two integers, a and n such that* $\gcd(a, n) = 1$*, then:*

$$a^{\phi(n)} = 1 \ \ mod \ \ n. \tag{5.57}$$

Theorem 5.21 (Fermat's Little Theorem) *Let's consider two integers a and p. If p is a prime, and p does not divide a, then:*

$$a^{p-1} = 1 \bmod p \tag{5.58}$$

Proof: Follows from the proof of the Euler's theorem by noting that if $n = p$, a prime, then $\phi(n) = p - 1$. ■