

Discrete Structures 2

Lecture 2:

Number Theory

Part 2

Dr Abdullah Alharbi

Second Semester
(1447 AH – 2026 AD)

The lecture content is taken from Discrete Mathematics and Its Applications, 8th edition, by Kenneth H. Rosen. McGraw-Hill, 2019.

Lectures Contents:

- **Number Theory**:
  - Divisibility & Modular Arithmetic
  - Integer Representations & Algorithms
  - **Primes** & **Greatest Common Divisors**
  - Solving Congruences
  - Applications of Congruences

Number Theory

- Introduction
- Primes
- Trial Division
- The Sieve of Eratosthenes:
  - The infinitude of Primes
- Greatest Common Divisor
- Finding the Greatest Common Divisor Using Prime Factorizations
- Least Common Multiple
- Dividing Congruences by an Integer

Introduction

- A **prime** is an integer greater than 1 that is divisible by no positive integers other than 1 and itself.
- **Primes** have become essential in modern cryptographic systems, and we will develop some of their properties important in cryptography.
- For example, finding **large primes** is essential in modern cryptography.
- The "**length of time**" required to factor large integers into their prime factors is the basis for the strength of some important modern cryptographic systems.

Primes

- Every integer greater than 1 is divisible by at least two integers,
  - **Because** a positive integer is divisible by 1 and by itself.
- **Positive integers** that have exactly two different positive integer factors are called **primes**.
- **Definition 1**:

> An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

- ***Remark:*** The **integer 1** is **not prime**, **because** it has only one positive factor.
- **Note** also that **an integer** "***n***" is **composite** if and only if **there exists an integer** "***a***" such that "***a*** | ***n***" and "**1 < *a* < *n***"

Primes

- **Example 1**:
  - The integer **7** is **prime** because its only positive factors are **1** and **7**, whereas the integer **9** is **composite** because it is divisible by **3**.
- The **primes** are the building blocks of positive integers, as the fundamental theorem of arithmetic shows.
- **Theorem 1**:

> **THE FUNDAMENTAL THEOREM OF ARITHMETIC** Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of nondecreasing size.

- **Example 2:** (next slide) gives some prime factorizations of integers.

Primes

EXAMPLE 2 The prime factorizations of 100, 641, 999, and 1024 are given by

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2,$$

$$641 = 641,$$

$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37,$$

$$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}.$$

Trial Division

- It is often important to show that a given **integer** is **prime**.
- For instance, in **cryptology**, large primes are used in some methods for making messages secret.
- One procedure for showing that an **integer** is **prime** is based on the following observation.

- **Theorem 2**:

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

Trial Division

- From "**Theorem 2**", it follows that an **integer** is **prime** if it is **not divisible** by any prime less than or equal to its square root.
  - This leads to the brute-force algorithm known as **trial division**.
- To use **trial division,** we divide "n" by all primes not exceeding $\sqrt{n}$ and conclude that "n" is prime if it is **not divisible** by any of these primes.

- **Example 3**: Show that **101** is prime.
- **Solution**:
- The only primes not exceeding $\sqrt{101}$ are **2**, **3**, **5**, and **7**.
  - Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that **101 is prime**.

Trial Division

- Because "**every integer has a prime factorization**", it would be useful to have a procedure for finding this **prime factorization**.
- Consider the problem of **finding the prime factorization of "n"**.
- Begin by dividing "n" by successive primes, starting with the smallest prime, "**2**".
- If "**n**" has a prime factor, then by **Theorem 3** a **prime factor "p" not exceeding $\sqrt{n}$** will be found.
- So, **if no prime factor not exceeding $\sqrt{n}$ is found, then "n" is prime**.
- Otherwise, **if a prime factor "p" is found, continue by factoring "n / p"**.
- **Note** that "**n / p**" has **no prime factors less than "p"**.
- Again, **if "n / p" has no prime factor greater than or equal to "p" and not exceeding its square root, then it is prime**.
- Otherwise, **if it has a prime factor "q", continue by factoring "n / (pq)"**.
- This procedure is continued until the factorization has been reduced to a **prime**.
- This procedure is illustrated in **Example 4**.

Trial Division

- **Example 4**:

  Find the prime factorization of **7007**

- **Solution**:
  - To find the prime factorization of 7007, first **perform divisions of 7007 by successive primes, beginning with 2**
    - None of the primes **2**, **3**, and **5 divides 7007**
  - However, **7 divides 7007**, with **7007/7 = 1001**
  - Next, **divide 1001 by successive primes, beginning with 7**
  - It is immediately seen that **7 also divides 1001, because 1001/7 = 143**
  - Continue by **dividing 143 by successive primes, beginning with 7**
    - Although **7 does not divide 143**, **11 does divide 143, and 143/11 = 13**
  - Because **13 is prime**, **the procedure is completed**.
  - It follows that **$7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$**
  - Consequently, **the prime factorization of 7007 is $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$**

The Sieve of Eratosthenes

- **Note** that **composite integers not exceeding 100 must have a prime factor not exceeding 10**.
- Because the **only primes less than 10** are **2**, **3**, **5**, and **7**, the primes not exceeding 100 are these four primes and those positive integers greater than 1 and not exceeding 100 that are divisible by none of 2, 3, 5, or 7.
- The **sieve of Eratosthenes** is used to find all primes not exceeding a specified positive integer.
- For instance, the following procedure is used to find the primes not exceeding 100.

The Sieve of Eratosthenes

- The ***Sieve of Erastosthenes*** can be used to find all primes not exceeding a specified positive integer.
- For example, **begin** with the list of integers between 1 and 100.
  a. **Delete** all the integers, other than 2, divisible by 2.
  b. **Delete** all the integers, other than 3, divisible by 3.
  c. Next, **delete** all the integers, other than 5, divisible by 5.
  d. Next, **delete** all the integers, other than 7, divisible by 7.
  e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the **primes** are:

{2, 3, 5, 7, 11, 15, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97}

The Sieve of Eratosthenes

- In **Table 1**, the panels display those integers deleted at each stage,
  - each integer **divisible by 2**, **other than 2**, is underlined in the **first** panel.
  - each integer **divisible by 3**, **other than 3**, is underlined in the **second** panel.
  - each integer **divisible by 5**, **other than 5**, is underlined in the **third** panel.
  - each integer **divisible by 7**, **other than 7**, is underlined in the **fourth** panel.
  - The **integers not underlined** are the **primes** not exceeding 100.
- We conclude that the **primes less than 100** are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97

TABLE 1 **The Sieve of Eratosthenes.**

Integers divisible by 2 other than 2 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 3 other than 3 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 5 other than 5 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

The infinitude of Primes

- It has long been known that there are "**infinitely many primes**".
- This *means* that **whenever p_1, p_2,…, p_n are the "n" smallest primes**, we know there is a **larger prime not listed**.

- **THEOREM 3**:

There are infinitely many primes.

The infinitude of Primes

- Because there are **infinitely many primes**, given any positive integer there are **primes greater than this integer**.
- There is an ongoing quest to discover larger and larger prime numbers; for almost all the last 300 years, the **largest prime** known has been an integer of the special form $\mathbf{2^p - 1}$, where "**p**" is also prime.
- Note that $\mathbf{2^n - 1}$ **cannot** be prime when "**n**" is not prime.
- Such primes are called **Mersenne primes**, after the French monk Marin Mersenne, who studied them in the seventeenth century.
- The reason that the largest known prime has usually been a Mersenne prime is that there is an extremely efficient test, known as the **Lucas–Lehmer test**, for determining whether $\mathbf{2^p - 1}$ is **prime**.

The infinitude of Primes

- **Example 5**:
- The following **numbers** are **Mersenne primes**
  - $2^2 - 1 = 3$
  - $2^3 - 1 = 7$
  - $2^5 - 1 = 31$
  - $2^7 - 1 = 127$
- But "$2^{11} - 1 = 2047$" is **not** a Mersenne prime because "$2047 = 23 \cdot 89$"
- A commonly used quality control test for supercomputers is to replicate the "Lucas–Lehmer test" that establishes the primality of a large Mersenne prime.

Greatest Common Divisor

- **Definition**:

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the **greatest common divisor** of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

- One can find greatest common divisors of small numbers by inspection.
- **Example**: What is the greatest common divisor of 24 and 36?
- **Solution**: gcd(24, 36) = 12
- **Example**: What is the greatest common divisor of 17 and 22?
- **Solution**: gcd(17,22) = 1

Greatest Common Divisor

- **Definition:** The integers a and b are "*relatively prime*" if their greatest common divisor is 1.
- **Example:** 17 and 22
- **Definition:** The integers $a_1, a_2, \ldots, a_n$ are ***pairwise relatively prime*** if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
- **Example:** Determine whether the integers 10, 17 and 21 are pairwise relatively prime.
- **Solution:** Because gcd(10, 17) = 1, gcd(10, 21) = 1, and gcd(17, 21) = 1, then 10, 17, and 21 are *pairwise relatively prime*.
- **Example**: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.
- **Solution:** Because gcd(10, 24) = 2, 10, 19, and 24 are not pairwise relatively prime.

Finding the **Greatest Common Divisor** Using **Prime Factorizations**

- Suppose the prime factorizations of *a* and *b* are:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each exponent is a **nonnegative integer**, and where all primes occurring in either prime factorization are included in both. Then:

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,bn)},$$

- This formula is valid since the **integer** on the right (of the equals sign) divides both "*a*" and "*b*".
- No larger integer can divide both *a* and *b*.

Finding the Greatest Common Divisor Using Prime Factorizations

- **Example**: $120 = 2^3 \cdot 3 \cdot 5$ $500 = 2^2 \cdot 5^3$

$$\gcd(120, 500) = \mathbf{2}^{\min(3,2)} \cdot \mathbf{3}^{\min(1,0)} \cdot \mathbf{5}^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

- Finding the **gcd** of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Least Common Multiple

- **Definition**: The least common multiple of the positive integers *a* and *b* is the **smallest positive integer** that is *divisible* by both *a* and *b*. It is denoted by lcm(*a*, *b*).

- The **least common multiple** can also be computed from the prime factorizations.

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,bn)},$$

- This **number** is divided by both "*a*" and "*b*" and no smaller number is divided by "*a*" and "*b*".

Least Common Multiple

- **Example:** $\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2$
- The **greatest common divisor** and the **least common multiple** of two integers are related by:
- **Theorem 5:** Let **a** and **b** be positive integers. Then $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$

Dividing Congruences by an Integer

- **Dividing** both sides of a valid **congruence** by **an integer** does not always produce a valid congruence.
- **But** *dividing by an integer "relatively prime" to the modulus* ***does*** *produce a valid congruence*:
- **Theorem 7**:

Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Any Questions?

- Have a look at the "Extra Examples" on the textbook's website.
- Keep reviewing this lecture *regularly, as well as other lectures*.
- Have a look at the *exercises* at the end of the sections we covered in this lecture in Chapter 4 and do your best with those ones similar to what we presented in this lecture.
  - You should get more *examples* and *exercises* in the *tutorials*.
- Ask *me or ask your peers* if you have any questions.
  - Please, do not wait until the end of the semester or even right before exams.

All the best!