Primes and Greatest Common Divisors

Course Code: CSC 1204 Course Title: Discrete Mathematics

Dept. of Computer Science
Faculty of Science and Technology

Lecture No:	**10**	**Week No:**	**5**	**Semester:**	**Summer 2021-2022**
Lecturer:	S.M. Abdur Rouf Bhuiyan (arouf@aiub.edu)				

Lecture Outline

3.5 Primes and Greatest Common Divisors

- Prime and Composite numbers
- Fundamental Theorem of Arithmetic
- Greatest Common Divisors (gcd)
- Least Common Multiple (lcm)
- Finding gcd & lcm of two integers using Prime Factorization

Objectives and Outcomes

- **Objectives**: To understand prime and composite numbers, greatest common divisor (gcd) and least common multiple (lcm), how to find gcd and lcm of two integers using prime factorization.

- **Outcomes**: Students are expected to be able explain the terms prime number, composite number, greatest common divisor, least common multiple; be able to determine whether an integer is prime or composite; be able to find the greatest common divisor and least common multiple of two integers using prime factorization.

Primes and Composite Numbers

- Definition 1: A positive 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***.
- Note: The integer n is composite if and only if there exists an integer a such that $a|n$ and $1 < a < n$.
- Theorem 3: There are infinitely many primes.

Example 1 (p. 223)

- 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.

- Question: What are the primes less than 100?

Fundamental Theorem of Arithmetic

- Theorem 1(Fundamental Theorem of Arithmetic): Every positive 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 non-decreasing size.

- Example 2 (p.224) : Prime factorization of 100, 641, 999, and 1024 are given by

  $100 = 2.2.5.5 = 2^2.5^2$

  $641 = 641$

  $999 = 3.3.3.37 = 3^3.37$

  $1024 = 2.2.2.2.2.2.2.2.2.2 = 2^{10}$

Determining whether a given integer is Prime or Composite

- Theorem 2: If *n* is a **composite** integer, then *n* has a prime divisor less than or equal to $\sqrt{n}$.

- 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.

Determining whether a given integer is Prime or Composite

- Example 3 [p.224]: Show that 101 is prime.
- **Solution**: The only primes not exceeding √101 are 2, 3, 5, 7. Because 101 is not divisible by 2, 3, 5, or 7, it follows that **101 is prime**.
- Exercise 1(e)[p.230]: Determine whether 111 is prime.
- **Solution**: The only primes not exceeding √111 are 2, 3, 5, 7. Because 111 is divisible by 3, it follows that **111 is not prime**.
- Exercise 1(f)[p.230]: Determine whether 143 is prime.
- **Solution:** The only primes not exceeding √143 are 2, 3, 5, 7,11. Because 143 is divisible by 11, it follows that **143 is not prime**.
- Extra example: Test if 139 is prime.

Greatest Common Divisor(gcd)

- **Definition 2**: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b.
  - The *greatest common divisor* of a and b is denoted by gcd(a, b)

- Example 10 (p.228): What is the greatest common divisor of 24 and 36?

- Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence **gcd(24,36) = 12**

Relatively Prime

- Definition 3: The integers *a* and *b* are ***relatively prime*** if their gcd is 1.

- Example 11 (p.228): What is the gcd of 17 and 22?
- Solution: The integers 17 and 22 have no positive common divisors other than 1, so that gcd(17,22) = 1
- By Example 11, it follows that the integers 17 & 22 are **relatively prime**, because gcd(17,22) = 1

Least Common Multiple(lcm)

- Definition 5: The *least common multiple* of positive integers a and b is the smallest positive integer that is divisible by both a and b.
  - The least common multiple of a and b is denoted by **lcm(a, b)**

- Theorem 5: Let a and b be positive integers. Then

  $$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$$

Finding **gcd & lcm** of two integers using **Prime Factorization**

- We can find the greatest common divisor (gcd), or least common multiple (lcm) of two integers using the prime factorization of these integers.
- Let prime factorization of the integers *a* and *b*, neither equal to zero, are $a = p_1^{a_1} p_2^{a_2} \ldots\ldots p_n^{a_n}$,

$$b = p_1^{b_1} p_2^{b_2} \ldots\ldots p_n^{b_n}$$

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

$$\mathbf{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \ldots\ldots p_n^{\max(a_n, b_n)}$$

Example 14(p. 229)

- What is the gcd of 120 and 500?
- **Solution**: Because the prime factorization of 120 and 500 are $120 = 2^3.3.5$ and $500 = 2^2.5^3$, the greatest common divisor is

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

$$= 2^2\ 3^0\ 5^1$$

$$= 20$$

[Note: $500 = 2^2.5^3 = 2^2.\ 3^0.5^3$]

[$3^0 = 1$]

Class Work

1. Find the **lcm(120,500)**, and then prove the theorem $ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$, where $a = 120$, and $b = 500$.

2. Find the gcd and lcm of 200 and 700 using prime factorization.

Example 15(p. 230)

- What is the least common multiple(lcm) of $2^3 3^5 7^2$ and $2^4 3^3$?

- **Solution**:

  $\text{lcm}\,(2^3 3^5 7^2\,,\, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)}$

  $= 2^4 3^5 7^2$

  [Note: $7^0 = 1$]

Practice @ Home

- **Relevant odd-numbered Exercises** from your text book

Books

1. *Discrete Mathematics and its applications with combinatorics and graph theory (7th edition)* by Kenneth H. Rosen [Indian Adaptation by KAMALA KRITHIVASAN], published by McGraw-Hill

References

1. Discrete Mathematics, *Richard Johnsonbaugh*, Pearson education, Inc.
2. Discrete Mathematical Structures, *Bernard Kolman*, *Robert C. Busby*, *Sharon Ross,* Prentice-Hall, Inc.
3. *SCHAUM'S outlines Discrete Mathematics(2nd edition)*, by *Seymour Lipschutz*, *Marc Lipson*