Republic of Iraq
Ministry of Higher Education and Scientific Research
Al- Mustaqbal University
Collage of science - Department of Cyber Security

1st class

2024- 2025

Number Theory

Lecture 4

Asst. Lect. Mohammed Jabbar
mohammed.jabbar.obaid@uomus.edu.iq

الرياضيات :المرحلة الاولى

نظرية الاعداد

المحاضرة الرابعة

استاذ المادة: م.م محمد جبار

Cybersecurity Department
قسم الأمن السيبراني

Contents

1 Great Common Divisor and Euclidean Algorithm

1.1 Great Common Divisor

Greatest Common Divisor (GCD)

Definition 1.1. The **GCD** of two integers a and b, denoted as $\gcd(a, b)$, is the largest positive integer that divides both a and b without leaving a remainder.

$$\gcd(a, b) = \max\{d \in \mathbb{Z} : d \mid a \text{ and } d \mid b\}.$$

For example, $\gcd(1, 2) = 1$, $\gcd(6, 27) = 3$, and for any a, $\gcd(0, a) = \gcd(a, 0) = a$.

Remark 1.1. unless both a and b are 0 in which case $\gcd(0, 0) = 0$.

Definition 1.2 (Co-Prime Numbers)**.** Two integers a and b are **co-prime** (or relatively prime) if the only positive integer that divides both of them is 1; equivalently, their greatest common divisor is 1:

$$\gcd(a, b) = 1.$$

For examples: $(8, 15), (7, 9), (13, 27)$ are co-prime pairs.

Lemma 1.1. For any integers a,b and n, we have

$$\gcd(a, b) = \gcd(b, a) = \gcd(\pm a, \pm b) = \gcd(a, b - a) = \gcd(a, b + a) = \gcd(a, b - na).$$

Lemma 1.2. For any integers a, b, and n, we have

$$\gcd(an, bn) = |n| \cdot \gcd(a, b).$$

Lemma 1.3. Suppose a, b, and n are integers such that $n \mid a$ and $n \mid b$. Then

$$n \mid \gcd(a, b).$$

Theorem 1.1. *For any integers a and b, there exist integers x and y such that*

$$d = \gcd(a, b) = ax + by.$$

Theorem 1.2. *If* $\gcd(a, b) = d$*, then* $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof. (1). Assume that k is a positive common divisor such that $k \mid a/d$ and $k \mid b/d$.

$$\Rightarrow ad = km \quad \text{and} \quad bd = kn, \quad n, m \in \mathbb{Z}$$

$$\Rightarrow a = kmd \quad \text{and} \quad b = knd.$$

Hence, $kd \mid a$ and $kd \mid b$. Also, $kd \mid d$. However, d is the GCD of a and b, so $kd \leq d$.

Since $kd \mid d \Rightarrow kd = d \Rightarrow k = 1$.

Thus, the only common divisor of a/d and b/d is 1.

$$\therefore \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

□

Proof. (2). $d = ax + by \Rightarrow 1 = \frac{a}{d}x + \frac{b}{d}y \Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

1.2 Euclidean Algorithm

Lemma 1.4. Let $a, b \in \mathbb{Z}$, such that $a = bq + r$ for some integers q, r. Then

$$\gcd(a, b) = \gcd(b, r).$$

Proof. Let $d = \gcd(a, b) \Rightarrow d \mid a, d \mid b$. Since $a = bq + r$, we have $r = a - bq$.

$\Rightarrow d \mid a - bq$, which means $d \mid r$. Thus, d is a common divisor of b and r, so $d \leq \gcd(b, r)$.

Conversely, let $d' = \gcd(b, r)$. Since $d' \mid b, d' \mid r \Rightarrow d' \mid a = bq + r$

Thus, d' is a common divisor of a and b, so $d' \leq \gcd(a, b)$. We have $d' = d$ □

Euclidean algorithm

Theorem 1.3. *Let a, b be nonzero integers. Repeatedly apply the division algorithm as follows:*

$$a = bq_1 + r_1, \quad 0 \leq r_1 < |b|$$

$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2$$

$$\vdots$$

Continue this process until some remainder $r_n = 0$, at which point the greatest common divisor is given by:

$$\gcd(a, b) = r_{n-1}.$$

Example 1.1. Let $a = 75$ and $b = 45$. We apply the Euclidean algorithm:

$$75 = 45 \times 1 + 30$$

$$45 = 30 \times 1 + 15$$

$$30 = 15 \times 2 + 0$$

Since the remainder is now 0, we conclude that:

$$\gcd(75, 45) = 15.$$

Example 1.2. Let $a = 517$ and $b = 89$. We apply the Euclidean algorithm:

$$517 = 89 \times 5 + 72$$

$$89 = 72 \times 1 + 17$$

$$72 = 17 \times 4 + 4$$

$$17 = 4 \times 4 + 1$$

$$4 = 1 \times 4 + 0$$

Since the remainder is now 0, we conclude that:

$$\gcd(517, 89) = 1.$$

Least Common Multiple (LCM)

Definition 1.3. The **Least Common Multiple (LCM)** of two integers a and b is the smallest positive integer that is divisible by both a and b.

$$\text{LCM}(a, b) = \frac{|a \times b|}{\gcd(a, b)}$$

Properties of LCM

- $\text{LCM}(a, b) \times \gcd(a, b) = |a \times b|$
- $\text{LCM}(a, b) \geq \max(a, b)$
- If a divides b, then $\text{LCM}(a, b) = b$.

Example

For $a = 12$ and $b = 18$:

$$\gcd(12, 18) = 6$$
$$\text{LCM}(12, 18) = \frac{12 \times 18}{6} = 36$$

Thus, $\text{LCM}(12, 18) = 36$.

1.3 Exercises of Great Common Divisor and Euclidean Algorithm

Exercises

1. Let a and b be two positive even integers. Prove that $\gcd(a, b) = 2\gcd(a/2, b/2)$.
2. By Euclidean Algorithm to find
   (a) $\gcd(12378, 3054)$.
   (b) $\gcd(51, 288)$.
   (c) $\gcd(7544, 115)$.
3. Show that if a and b are positive integers where a is even and b is odd, then $\gcd(a, b) = \gcd(a/2, b)$
4. Let $a, b, c \in \mathbb{Z}$ such that $a \mid bc$ and $\gcd(a, c) = 1$. Prove that $a \mid b$.
5. If $a \mid b$ and $a > 0$, prove that $\gcd(a, b) = a$.
6. If $n \in \mathbb{Z}$ prove that n and $n + 1$ co-prime i.e $\gcd(n, n + 1) = 1$.
7. Find $lcm(15, 20)$ and $lcm(51, 288)$
8. Let $a, b \in \mathbb{Z}$, if $lcm(a, b) = ab$, prove that $\gcd(a, b) = 1$.