

# Session 59: GCD and LCM

- Greatest Common Divisor
- Least Common Multiple

# 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  **$\gcd(a, b)$** .

**Example:**

$$\gcd(24, 36) = 12$$

$$\gcd(17, 22) = 1$$

# Relatively Prime

**Definition:** The integers  $a$  and  $b$  are **relatively prime** if  $\gcd(a, b) = 1$

**Definition:** The integers  $a_1, a_2, \dots, a_n$  are **pairwise relatively prime** if  $\gcd(a_i, a_j) = 1$  whenever  $1 \leq i < j \leq n$ .

# Examples

17 and 22 are relatively prime

The integers 10, 17 and 21 are pairwise relatively prime.

$$\gcd(10, 17) = 1$$

$$\gcd(10, 21) = 1$$

$$\gcd(17, 21) = 1$$

The integers 10, 19, and 24 are not pairwise relatively prime.

$$\gcd(10, 24) = 2$$

# Finding the Greatest Common Divisor

Suppose the prime factorizations of  $a$  and  $b$  are:

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

where each exponent is a nonnegative integer.

Then:

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

- 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.

# Example

$$120 = 2^3 \cdot 3 \cdot 5 = 2^3 \cdot 3^1 \cdot 5^1$$

$$500 = 2^2 \cdot 5^3 = 2^2 \cdot 3^0 \cdot 5^3$$

# 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  **$\text{lcm}(a, b)$** .

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

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

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

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

# Euclidean Algorithm

The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers.

It is based on the idea that  $\gcd(a, b)$  is equal to  $\gcd(r, b)$  when  $a > b$  and  $r$  is the remainder when  $a$  is divided by  $b$ .

## Example:

Find  $\gcd(91, 287)$ :

$$287 = 91 \cdot 3 + 14, \text{ therefore } \gcd(287, 91) = \gcd(14, 91) = \gcd(91, 14)$$

$$91 = 14 \cdot 6 + 7, \text{ therefore } \gcd(91, 14) = \gcd(7, 14) = \gcd(14, 7)$$

$$14 = 7 \cdot 2 + 0, \text{ therefore } \gcd(14, 7) = 7$$



# Correctness of Euclidean Algorithm

**Lemma 1:** Let  $a = bq + r$ , where  $a$ ,  $b$ ,  $q$ , and  $r$  are integers.  
Then  $\gcd(a, b) = \gcd(b, r)$ .

**Proof:**

- Suppose that  $d$  divides both  $a$  and  $b$ . Then  $d$  also divides  $a - bq = r$ .
  - Hence, any common divisor of  $a$  and  $b$  must also be a common divisor of  $b$  and  $r$ .
- Suppose that  $d$  divides both  $b$  and  $r$ . Then  $d$  also divides  $bq + r = a$ .
  - Hence, any common divisor of  $a$  and  $b$  must also be a common divisor of  $b$  and  $r$ .
- Therefore,  $\gcd(a, b) = \gcd(b, r)$ . ☒

# Euclidean Algorithm

```
procedure gcd(a, b: positive integers,  $a > b$ )  
x := a  
y := b  
while  $y \neq 0$   
    r := x mod y  
    x := y  
    y := r  
return x
```

```
procedure gcd(a, b: positive integers,  $a > b$ )  
if  $b = 0$  then return a  
    else return gcd(a mod b, b)
```

# Correctness of Euclidean Algorithm

Suppose that  $a$  and  $b$  are positive integers with  $a \geq b$ . Let  $r_0 = a$  and  $r_1 = b$ .

Successive applications of the division algorithm yields:

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3 & 0 \leq r_3 < r_2, \\ &\vdots \\ &\vdots \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n. \end{aligned}$$

Eventually, a remainder of zero occurs in the sequence of terms:  $a = r_0 > r_1 > r_2 > \cdots \geq 0$ .

The sequence can't contain more than  $a$  terms.

By Lemma 1  $\gcd(a, b) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$ .

Hence the greatest common divisor is the last nonzero remainder in the sequence of divisions.

# Complexity of Euclidean Algorithm

**Theorem (Lamé's theorem):** Let  $a$  and  $b$  be positive integers with  $a \geq b$ . Then the number of divisions used by the Euclidean algorithm to find  $\gcd(a, b)$  is less than or equal to five times the number of decimal digits in  $b$ .

Therefore the Euclidean algorithm has complexity  $O(\log b)$ .

# Summary

- Greatest common divisor
- Least common Multiple
- Euclidean Algorithm