NUMBER THEORY

Lecture 16

PRIMES AND GREATEST COMMON DIVISOR

PRIME

- Definition: 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.
- Every integer greater than 1 is divisible by at least two integers, because a positive integer is divisible by 1 and itself.
- Integer 1 is not prime, it has only 1 positive factor.
- Example: Integer 7 is prime as its only positive factors are 1 and 7.
- Primes are the building blocks of positive integers, as the fundamental theorem of arithmetic's shows.

FUNDAMENTAL THEOREM OF ARITHMETIC

- Every integer greater than 1 can be written uniquely as a prime or as a product of two or more primes, where the prime factors are written in order of nondecreasing size.
- Every positive integer is either prime or a unique product of primes i.e., composite

$$m = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_l^{k_l}$$

FUNDAMENTAL THEOREM OF ARITHMETIC

- If n is composite, then it has a prime divisor such that

Prime factorization examples: $100 = 2^5 \cdot 5^2$

$999 = 3^3 \cdot 37$

$7007 = 7^2 \cdot 11 \cdot 13$

- **Trial Division(brute-force algorithm):** If n is a composite integer, then n has a prime divisor less than or equal to its square root. $p \le \sqrt{n}$
    - To use trial division, we divide n by all primes not exceeding square root n and conclude that n is prime if it not divisible by any other primes.

GREATEST COMMON DIVISOR

Definition : Let a and b be integers, not both zero. The largest integer d such that d | a and also d | 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).

Easy to find GCD 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

DEFINITIONS

- **<u>Definition</u>** : The integers a and b are ***relatively prime*** if their greatest common divisor is 1.

Example: 17 and 22

- **<u>Definition</u>** : The integers $a_1, a_2, \ldots, a_n$ are ***pairwise relatively prime*** if
  $\gcd(a_i, a_j) = 1$ whenever $1 \le i < j \le n$.

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, 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.

LEAST COMMON MULTIPLE

- **Definition**
  - LCM of two positive integers a and b is the smallest positive integer that is divisible by both a and b.
  - Denoted by lcm(a,b).

- LCM can also be computed from the prime factorizations.

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

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

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

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

EUCLIDEAN ALGORITHM

- Efficient method for computing the GCD of two integers.
- Based on the idea that
  - gcd(a,b) = gcd(b,c) where a > b and c = a mod b.

Example: Find gcd(91, 287):

- $287 = 91 \cdot 3 + 14$ Divide 287 by 91
- $91 = 14 \cdot 6 + 7$ Divide 91 by 14
- $14 = 7 \cdot 2 + 0$ Divide 14 by 7

- gcd(287, 91) = gcd(91, 14) = gcd(14, 7) = 7

The Euclidean algorithm is expressed in pseudocode in Algorithm 1.

ALGORITHM 1 The Euclidean Algorithm.

procedure *gcd*(a, b: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b)$ is $x\}$

BÉZOUT'S THEOREM

- If a and b are positive integers, then there exist integers s and t such that gcd(a,b) = sa + tb.

Definition :

- If a and b are positive integers, then integers s and t such that gcd(a,b) = sa + tb are called **Bézout coefficients** of a and b.
- The equation gcd(a,b) = sa + tb is called **Bézout's identity**.

- By Bézout's Theorem, the gcd of integers a and b can be expressed in the form sa + tb where s and t are integers.
- This is a **linear combination** with integer coefficients of a and b.
  - $\gcd(6,14) = (-2)\cdot 6 + 1\cdot 14$

FINDING GCDS AS LINEAR COMBINATIONS

Example: Express gcd(252,198) = 18 as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show gcd(252,198) = 18

i. $252 = 1 \cdot 198 + 54$

ii. $198 = 3 \cdot 54 + 36$

iii. $54 = 1 \cdot 36 + 18$

iv. $36 = 2 \cdot 18$

- Now working backwards, from iii and ii above
  - $18 = 54 - 1 \cdot 36$
  - $36 = 198 - 3 \cdot 54$
- Substituting the 2nd equation into the 1st yields:
  - $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$
- Substituting $54 = 252 - 1 \cdot 198$ (from i) yields:
  - $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

BÉZOUT'S THEOREM: CONSEQUENCES

- **Lemma 2**:
  - If a, b, and c are positive integers such that gcd(a, b) = 1 and a | bc, then a | c.
- **Proof**: Assume gcd(a, b) = 1 and a | bc
  - Since gcd(a, b) = 1, by Bézout's Theorem, there are integers s and t such that sa + tb = 1.
  - Multiplying both sides of the equation by c, yields sac + tbc = c.
  - Now, (a|bc ⇒ a|tbc) and (a|sac) ⇒ a|(sac + tbc)
  - We conclude a | c, since sac + tbc = c.
- **Lemma 3**:
  - If p is prime and p | $a_1 a_2 \cdots a_n$, then p | a_i for some i.