

MATH 433

Applied Algebra

Lecture 4:

More on greatest common divisor.

Prime numbers.

Unique factorisation theorem.

Greatest common divisor

Given positive integers a_1, a_2, \dots, a_n , the **greatest common divisor** $\gcd(a_1, a_2, \dots, a_n)$ is the largest positive integer that divides a_1, a_2, \dots, a_n .

Theorem (i) $\gcd(a_1, a_2, \dots, a_n)$ is the smallest positive integer represented as an integral linear combination of a_1, a_2, \dots, a_n .

(ii) $\gcd(a_1, a_2, \dots, a_n)$ is divisible by any other common divisor of a_1, a_2, \dots, a_n .

Remark. The theorem can be proved in the same way as in the case $n = 2$ (see Lecture 2). Another approach is by induction on n using the fact that $\gcd(a_1, a_2, \dots, a_n) = \gcd(a_1, \gcd(a_2, \dots, a_n))$.

Prime numbers

A positive integer p is **prime** if it has exactly two positive divisors, namely, 1 and p .

Examples. 2, 3, 5, 7, 29, 41, 101.

A positive integer n is **composite** if it is a product of two strictly smaller positive integers.

Examples. $6 = 2 \cdot 3$, $16 = 4 \cdot 4$, $125 = 5 \cdot 25$.

Any positive integer is either prime or composite or 1. **Prime factorisation** of a positive integer $n \geq 2$ is a decomposition of n into a product of primes.

Examples.

- $120 = 12 \cdot 10 = (2 \cdot 6) \cdot (2 \cdot 5)$
 $= (2 \cdot (2 \cdot 3)) \cdot (2 \cdot 5) = 2^3 \cdot 3 \cdot 5$.
- $144 = 12^2 = (2^2 \cdot 3)^2 = 2^4 \cdot 3^2$.

Sieve of Eratosthenes

The **sieve of Eratosthenes** is a method to find all primes from 2 to n :

- (1) Write down all integers from 2 to n .
- (2) Select the smallest integer k that is not selected or crossed out yet.
- (3) Cross out all multiples of k .
- (4) If not all numbers are selected or crossed out, return to step (2).

The prime numbers are those selected in the process.

Unique factorisation theorem

Theorem Any positive integer $n \geq 2$ admits a prime factorisation. This factorisation is unique up to rearranging the factors.

Corollary There are infinitely many prime numbers.

Idea of the proof: Let p_1, p_2, \dots, p_k be the first k primes. Consider the number $N = p_1 p_2 \dots p_k + 1$. By construction, this number is not divisible by p_1, p_2, \dots, p_k . But it does have a prime divisor, due to the theorem.

Problem. Suppose m is a positive integer such that

$$m = 2^4 p_1 p_2 p_3,$$

$$m + 100 = 5 q_1 q_2 q_3,$$

$$m + 200 = 23 r_1 r_2 r_3 r_4,$$

where p_i, q_j, r_k are prime numbers and, moreover, $p_i \neq 2$, $q_j \neq 5$, $r_k \neq 23$. Find m .

The prime decomposition of 100 is $2^2 \cdot 5^2$. Since the numbers $m + 100$ and 100 are divisible by 5, so are their difference m and their sum $m + 200$.

The prime decomposition of 200 is $2^3 \cdot 5^2$. Since the number m is divisible by $2^4 = 16$, it follows that $m + 100$ is divisible by $2^2 = 4$ while $m + 200$ is divisible by $2^3 = 8$.

By the above the prime decomposition of $m + 200$ contains $2^3 \cdot 5 \cdot 23$. As there are only 5 factors in this decomposition, the number $m + 200$ is exactly $2^3 \cdot 5 \cdot 23 = 920$. Then $m + 100 = 820 = 2^2 \cdot 5 \cdot 41$ and $m = 720 = 2^4 \cdot 3^2 \cdot 5$.

Unique prime factorisation

Theorem Any positive integer $n \geq 2$ admits a prime factorisation. This factorisation is unique up to rearranging the factors.

Ideas of the proof: The **existence** is proved by strong induction on n . It is based on a simple fact: if $p_1 p_2 \dots p_s$ is a prime factorisation of k and $q_1 q_2 \dots q_t$ is a prime factorisation of m , then $p_1 p_2 \dots p_s q_1 q_2 \dots q_t$ is a prime factorisation of km .

The **uniqueness** is proved by (normal) induction on the number of prime factors. It is based on a (not so simple) fact: if a prime number p divides a product of primes $q_1 q_2 \dots q_t$ then one of the primes q_1, \dots, q_t coincides with p .

Coprime numbers

Positive integers a and b are **relatively prime** (or **coprime**) if $\gcd(a, b) = 1$.

Theorem Suppose that a and b are coprime integers. Then

- (i) $a|bc$ implies $a|c$;
- (ii) $a|c$ and $b|c$ imply $ab|c$.

Idea of the proof: Since $\gcd(a, b) = 1$, there are integers m and n such that $ma + nb = 1$. Then $c = mac + nbc$.

Corollary 1 If a prime number p divides the product $a_1 a_2 \dots a_n$, then p divides one of the integers a_1, \dots, a_n .

Corollary 2 If an integer a is divisible by pairwise coprime integers b_1, b_2, \dots, b_n , then a is divisible by the product $b_1 b_2 \dots b_n$.

Let $a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ and $b = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$, where p_1, p_2, \dots, p_k are distinct primes and n_i, m_i are nonnegative integers.

Theorem (i) $ab = p_1^{n_1+m_1} p_2^{n_2+m_2} \dots p_k^{n_k+m_k}$.

(ii) a divides b if and only if $n_i \leq m_i$ for $i = 1, 2, \dots, k$.

(iii) $\gcd(a, b) = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$, where $s_i = \min(n_i, m_i)$.

(iv) $\text{lcm}(a, b) = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$, where $t_i = \max(n_i, m_i)$.

Here $\text{lcm}(a, b)$ denotes the **least common multiple** of a and b , that is, the smallest positive integer divisible by both a and b .