MATH 433

Applied Algebra

Lecture 3:
Prime factorisation (continued).
Congruence classes.
Modular arithmetic.

Unique prime factorisation

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

Prime factorisation of a positive integer $n \geq 2$ is a decomposition of n into a product of primes.

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

The **existence** of the factorisation is derived from a simple fact: if $p_1 p_2 \ldots p_k$ is a prime factorisation of n and $q_1 q_2 \ldots q_l$ is a prime factorisation of m, then $p_1 p_2 \ldots p_k q_1 q_2 \ldots q_l$ is a prime factorisation of nm. The **uniqueness** is derived from another observation: if a prime number p divides a product of primes $p_1 p_2 \ldots p_k$ then one of the primes $p_1, \ldots, p_k$ 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)** a divides b if and only if $n_i \le m_i$ for $i = 1, 2, \dots, k$.

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

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

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

Fermat and Mersenne primes

Proposition For any integer $k \geq 2$ and any $x, y \in \mathbb{R}$,

$$x^k - y^k = (x - y)(x^{k-1} + x^{k-2}y + \cdots + xy^{k-2} + y^{k-1}).$$

If, in addition, k is odd, then

$$x^k + y^k = (x + y)(x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1}).$$

Corollary 1 (Mersenne) The number $2^n - 1$ is composite whenever n is composite.

(Hint: use the first formula with $x = 2^{n/k}$, $y = 1$, and k a prime divisor of n.)

Corollary 2 (Fermat) Let $n \geq 2$ be an integer. Then the number $2^n + 1$ is composite whenever n is not a power of 2.

(Hint: use the second formula with $x = 2^{n/k}$, $y = 1$, and k an odd prime divisor of n.)

Mersenne primes are primes of the form $2^p - 1$, where p is prime. **Fermat primes** are primes of the form $2^{2^n} + 1$. Only finitely many Fermat and Mersenne primes are known.

Congruences

Let n be a postive integer. The integers a and b are called **congruent modulo** n if they have the same remainder when divided by n. An equivalent condition is that n divides the difference $a - b$.

Notation. $a \equiv b \mod n$ or $a \equiv b \pmod{n}$.

Proposition If $a \equiv b \mod n$ then for any integer c,
(i) $a + cn \equiv b \mod n$;
(ii) $a + c \equiv b + c \mod n$;
(iii) $ac \equiv bc \mod n$.

Modular arithmetic

Given an integer a, the **congruence class of a modulo n** is the set of all integers congruent to a modulo n.

Notation. $[a]_n$ or simply $[a]$.
Also, $\overline{a}$ and $a + n\mathbb{Z}$.

For any integers a and b, we let

$$[a]_n + [b]_n = [a+b]_n,$$
$$[a]_n \times [b]_n = [ab]_n,$$