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 $p_1 p_2 \dots p_k$ is a prime factorisation of n and $q_1 q_2 \dots q_l$ is a prime factorisation of m, then $p_1 p_2 \dots p_k q_1 q_2 \dots q_l$ is a prime factorisation of nm. The **uniqueness** is derived from another observation: if a prime number p divides a product of primes $p_1 p_2 \dots p_k$ then one of the primes $p_1, \dots, p_k$ 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 $b_1 b_2 \dots b_n$.