MATH 433

Applied Algebra

Lecture 2: Mathematical induction. Prime numbers. Unique factorisation theorem.

Mathematical induction

Well-ordering principle: any nonempty set of positive integers has the smallest element. (Equivalently, any decreasing sequence of positive integers is finite.)

Induction principle: Let $P(n)$ be an assertion depending on the positive integer variable n. Suppose that

- $P(1)$ holds,
- whenever $P(k)$ holds, so does $P(k+1)$.

Then $P(n)$ holds for all positive integers n.

Remarks. The assertion $P(1)$ is called the **basis of induction**. The implication $P(k) \implies P(k+1)$ is called the **induction step**.

Examples of assertions $P(n)$:

(a) $1 + 2 + \cdots + n = n(n+1)/2$,
(b) $n(n+1)(n+2)$ is divisible by 6,
(c) $n = 2p + 3q$ for some $p, q \in \mathbb{Z}$.

Theorem The well-ordering principle implies the induction principle.

Proof: Let $P(n)$ be an assertion depending on the positive integer variable n such that $P(1)$ holds and $P(k)$ implies $P(k+1)$ for any integer $k > 0$.

Consider the set $S = \{n \in \mathbb{P} : P(n) \text{ does not hold}\}$. Assume that S is not empty. By the well-ordering principle, the set S has the smallest element m. Since $P(1)$ holds, $m \neq 1$ so that $m - 1 > 0$. Clearly, $m - 1 \notin S$, therefore $P(m-1)$ holds. But $P(m-1) \implies P(m)$ so that $P(m)$ holds as well.

The contradiction means that the assumption was wrong. Thus the set S is empty.

Theorem $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

Proof: Let us use the induction principle.

Basis of induction: check the formula for $n = 1$.

In this case, $1 = 1(1+1)/2$, which is true.

Induction step: assume that the formula is true for $n = m$ and derive it for $n = m + 1$.

Inductive assumption: $1 + 2 + \cdots + m = m(m+1)/2$.

Then

$$1 + 2 + \cdots + m + (m+1) = \frac{m(m+1)}{2} + (m+1)$$

$$= (m+1)\Big(\frac{m}{2} + 1\Big) = \frac{(m+1)(m+2)}{2}.$$

Strong induction principle: Let $P(n)$ be an assertion depending on the positive integer variable n. Suppose that $P(n)$ holds whenever $P(k)$ holds for all $k < n$. Then $P(n)$ holds for all positive integers n.

For $n = 1$, this means that $P(1)$ holds unconditionally.

For $n = 2$, this means that $P(1)$ implies $P(2)$.

For $n = 3$, this means that $P(1)$ and $P(2)$ imply $P(3)$.

And so on.

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 is proved in the same way as in the case $n = 2$ (proved in the previous lecture). 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 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 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.

Remark. The existence is proved by strong induction on n. The uniqueness is proved by (normal) induction on the number of factors.

Corollary There are infinitely many prime numbers.

Idea of the proof: Let $p_1, p_2, \ldots, p_n$ be the first n primes. Consider the number $N = p_1 p_2 \cdots p_n + 1$. This number has a prime divisor different from $p_1, p_2, \ldots, p_n$.