Contents

Section 1. Mathematical induction

1.1 Theorem: well-ordering principle(axiom)

Every nonempty set S of non-negative integers contains a least element, i.e., there exists $a \in S$ such that $a \leq x$ for all $x \in S$.
Consider $S' = \{x - b : x \in S\}$. Then S' must have a least element, say y. Then $y + b$ is the least element of S.

1.2 Theorem: Archimedean property

let a, b be positive integers. Then there exists a positive integer n such that $an \geq b$.

Proof) Suppose by contradiction, $\forall k \in \mathbb{N}, ak < b$. Consider that $S = \{b - ak | k \in \mathbb{N}\}$ consists of integers large than or equal to 1. By well-ordering principle, S contains the minimal element, say $b - am$ $(m \in \mathbb{N})$. Then $0 < b - a(m+1) < b - am \implies b - a(m+1) \in S$, leading to a contradiction. □

1.3 Theorem: First principle of finite induction

Suppose that S is a set of integers satisfying

(a) $1 \in S$;

(b) if $k \in S$, then $k + 1 \in S$.

Then S is the set of all positive integers.

Proof) Let $T = \mathbb{N} \backslash S$. Suppose that T is not empty. By the well-ordering principle, T contains a least element, say n. Then $n \geq 2$ ($\because 1 \in S \implies 1 \notin T$), and $n - 1 \notin T \implies n - 1 \in S$. By (b), $n \in S$, leading to a contradiction. □

Example 1.4 Show that for all $n \in \mathbb{N}$,

$$1 + 3 + 5 + \cdots + (2n-1) = n^2$$

Proof) $n = 1 \implies 1 = 1^2 = 1$. Suppose the assertion holds for $n = k$. Then $1 + 3 + \cdots + (2k-1) + (2k+1) = k^2 + 2k + 1 = (k+1)^2$, holds for $n = k + 1$. □

Remark (b) can be repalced by the condition (b') If k is a positive integer and $1, 2, \ldots, k \in S$, then $k + 1 \in S$.

1.5 Theorem: Second principle of finite induction

Let S be a sef of positive integer satisfying (a),(b'). Then $S = \mathbb{N}$

The proof is similar

Example 1.6 Let $\{a_n\}$ be a sequence with $a_1 = 1$, $a_2 = 2$, $a_3 = 3$ and $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ for all $n \geq 4$. Show that $a_n < 2^n$ for all $n \in \mathbb{N}$

The proof is an exercise.

1.7 Theorem: The binomial theorem

$\binom{n}{k} =_n C_k$: the number of ways of choosing k numbers in $\{1, 2, \ldots\}$.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (0 \leq k \leq n)$$

1.8 Theorem: Pascal's rule

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k} \quad (1 \leq k \leq n)$$

Proof) $\text{LHS} = \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} = \frac{n!}{(k-1)!(n-k)!}\left(\frac{1}{n-k+1} + \frac{1}{k}\right) = \frac{n!}{(k-1)!(n-k)!}\left(\frac{n+1}{(n-k+1)k}\right) = \frac{(n+1)!}{k!(n-k+1)!}$. □

1.9 Theorem: Binomial expansion

Complete exansion of $(a+b)^n \quad (n \geq 1)$ into a sum of poners of a and b.

$$(a+b)^1 = a + b \tag{1}$$
$$(a+b)^2 = a^2 + 2ab + b^2 \tag{2}$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 \tag{3}$$
$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \tag{4}$$

1.10 Theorem

For $n \geq 1$, positive integer

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Proof) Use induction on n. $n=1$: clear. Suppose the equality holds for $n=m$. Then

$$(a+b)(a+b)^m = \left(\sum_{k=0}^{m}(m,k)a^k b^{m-k}\right)(a+b) \tag{5}$$

$$= \sum_{k=0}^{m}(m,k)a^{k+1}b^{m-k} + \sum_{k=0}^{m}(m,k)a^k b^{m-k+1} \tag{6}$$

$$= (m,k)a^{m+1} + \sum_{k=0}^{m-1}(m,k)a^{k+1}b^{m-k} + (m,0)b^{m+1} + \sum_{k=1}^{m}(m,k)a^k b^{m-k+1} \tag{7}$$

$$= a^{m+1} + \sum_{k=1}^{m}\left((m,k-1)+(m,k)\right)a^k b^{m-k+1} + b^{m+1} \tag{8}$$

$$= a^{m+1} + \sum_{k=1}^{m}(m+1,k)a^k b^{m-k+1} + b^{m+1} \tag{9}$$

$$= \sum_{k=0}^{m+1}(m+1,k)a^k b^{m+1-k} \tag{10}$$

□

Example 1.11 For $n \geq 1$,

(a) $\sum_{k=0}^{n}(n,k) = 2^n$

(b) $\sum_{k=0}^{n}(-1)^k(n,k) = 0$

(c) $(n,1)+(n,3)+\cdots = (n,0)+(n,2)+(n,4)+\cdots = 2^{n-1}$

The proof is trivial.

Lecture 0909

Section 2. Divisibility theory in the integers

The division algorithm

2.1 Theorem

Suppose $a, b \in \mathbb{Z}$ and $b > 0$. Then there exists unique integers q and r such that $a = qb + r$ and $0 \leq r < b$. q,r is called the ***quotient*** and ***remainder*** respectively.

Proof) Let $S = \{a - kb : k \in \mathbb{Z}, a - kb \geq 0\}$. Clearly $S \neq \varnothing$. By the well-ordering pinrciple, S has the minimal element, say r. Assume $r = a - qb$. We claim that $0 \leq r < b$. Suppose to the contrary $r \geq b$. Then $0 \leq a-(q+1)b = a - qb - b < a - qb$, whci contradicts to the minimality of r. The existance of such q, r follows. To prove uniqueness, suppose $a = q_1 b + r_1 = q_2 b + r_2$. Then $|b(q_1 - q_2)| = |r_1 - r_2|$. Since $|r_1 - r_2| < b$ and $b|(r_1 - r_2)$, $r_1 = r_2$. □

2.2 Corollary

Suppose a, b are integers and $b \neq 0$. Then there exists unique $q, r \in \mathbb{Z}$ such that

(a) $a = qb + r$.

(b) $0 \leq r < |b|$.

Proof) The case $b > 0$ holds by the previous theorem. If $b < 0$, there exists $q', r' \in \mathbb{Z}$ such that $a = q'|b| + r' = b(-q') + r' = bq + r$ where $0 \leq r' < |b|$. By the uniqueness of q, r, $q' = -q$ and $r = r'$. □

Example 2.3 Let $a \in \mathbb{Z}$ and $b = 2$. Division algorithm says that a is of the form $2q$ or $2q+1$.

Example 2.4 a^2 leaves the remainder 0 or 1 when divided by 4(remainder 0,1,or 4 when divided by 8). $a = 2q \implies a^2 = 4q^2$. $a = 2q+1 \implies a^2 = 4q^2 + 4q + 1 = 4q(q+1) + 1 = 8k + 1$.

Example 2.5 a^4 is of the form $5k$ or $5k+1$. $a = 5q + r \quad 0 \leq r \leq 4$. $a^4 = (5q = r)^4 = (5q)^4 + \cdots + \binom{4}{4}r^4$. $r^4 \equiv 1 \mod 5$.

Example 2.6 More generally, if p is a prime, then a^{r-1} is of the form pk or $pk+1$ (Fermat's little theorem).

Section 3. The greatest common divisor

3.1 Definition

An integer b is said to be ***divisible*** by $a \neq 0$ if $\exists c \in \mathbb{Z}$ such that $b = ac$, we write $a \mid b$. We write $x \nmid y$ to mean b is not divisible by a.

3.2 Theorem

Suppose $a, b, c \in \mathbb{Z}$ and $a \neq 0$. Then

(a) $a \mid 0$, $1 \mid b$, and $a \mid a$.

(b) $a \mid 1 \iff a = 1$ or $a = -1$.

(c) $a \mid b$, $c \mid d \implies ac \mid db$.

(d) $a \mid b$, $b \mid c \implies a \mid c$.

(e) $a \mid b$, $b \mid a \iff a = b$ or $a = -b$.

(f) $a \mid b$, $b \neq 0 \implies |a| \leq |b|$.

(g) $a \mid x_1, a \mid x_2, \ldots, a \mid x_n$, then $a \mid (b_1x_1 + b_2x_2 + \cdots + b_nx_n)$ with $b_i \in \mathbb{Z}$

Proof) (f) $b = ac \quad (c \neq 0)$. Then $|b| = |ac| = |a||c| \geq |a|$. □

3.3 Definition

Suppose a, b are integers. An integer d such that $d \mid a$ and $d \mid b$ is called a ***common divisor*** of a and b.

3.4 Definition

Suppose $a, b \in \mathbb{Z}$ and $a \neq 0$ or $b \neq 0$. Then the greatest common divisor(g.c.d) a and b, denoted by $gcd(a, b)$, is the positive integer d satisfying

(a) $d \mid a$ and $d \mid b$.

(b) If $c \mid a$ and $c \mid b$, then $c \leq d$.

Remark For any nonzero interger b, there are only finitely many divisors. Therefore, $gcd(a, b)$ exists if $a \neq 0$ or $b \neq 0$.

3.5 Theorem

Suppose $a, b \in \mathbb{Z}$, $a \neq 0$ or $b \neq 0$, and $d = gcd(a, b)$. Then there exists $x, y \in \mathbb{Z}$ such that $ax + by = d$.

Proof) Consider a set $S = \{am + bn \mid m, n \in \mathbb{Z}, am + bn > 0\}$. By the Archimedean property, $S \neq \varnothing$. By the well-ordering principle, the smallest element $\exists s \in S$. Claim $s = d = gcd(a, b)$. To prove s is a common divisor, use division algorithm: $a = qs + r$ with $0 \leq r < s$. If $r \neq 0$, then $r = a - qs = a - q(ax + by) = a(1 - qx) + b(-qy) \in S$. It is a contradiction, so $r = 0$ and $s \mid a$. Similarly, $s \mid b$. Let c be common divisor of a and b. Then $c \mid ax + by = s \implies |c| \leq |s| = s$. Thus $s = d = \gcd(a, b)$. □

3.6 Corollary

Supppose $a, b \in \mathbb{Z}$, $a \neq 0$ or $b \neq 0$. Then $T = \{ax + by \mid x, y \in \mathbb{Z}\}$ is precisely the set of all multiples of $\gcd(a, b) = d$.

Proof) $T' = \{dn \mid n \in \mathbb{Z}\}$. WTS: $T = T'$
($\supset$) $d = am + bk$ for $m, k \in \mathbb{Z}$. $dn = a(mn) + b(kn) \in T$.
($\subset$) $\forall ax + by \in T$ is a multiple of $d \implies T \subset T'$. □

3.7 Definition

Suppose $a, b \in \mathbb{Z}$ and $a \neq 0$ or $b \neq 0$. Then a, b are said to be ***relatively prime*** if $\gcd(a, b) = 1$

3.8 Theorem

suppose $a, b \in \mathbb{Z}$ and $a \neq 0$ or $b \neq 0$.

$$\gcd(a, b) = 1 \iff \exists m, n \in \mathbb{Z} \text{ such that } 1 = am + ba$$

3.9 Proposition

($\Rightarrow$) Follows from the previous thm.
($\Leftarrow$) If c is a common divisor of a and b, then $c \mid 1$ and $c = +-1 \leq 1 \implies \gcd(a, b) = 1$.

3.10 Corollary

If $\gcd(a, b) = d$, then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof) $\exists m, n \in \mathbb{Z}$, $am + bn = d \implies (\frac{a}{d}m + (\frac{b}{d})n = 1) \implies \gcd(\frac{a}{d}, \frac{b}{d}) = 1$. □

3.11 Corollary

If $a \mid c$, $b \mid c$ and $\gcd(a, b) = 1$, then $ab \mid c$.

Proof) $\gcd(a, b) = 1 \implies \exists m, n \in \mathbb{Z}$ such that $1 = am + bn$. Then $c = 1c = (am + bn)c = acm + cbn = abrm + absm$ ($\because c = br = as$ for some $r, s \in \mathbb{Z}$). □

3.12 Theorem: Euclid's lemma

If $a \mid bc$ and $gcd(a, b) = 1$, then $a \mid c$.

Proof) $1 = am + bn$ for some $m, n \in \mathbb{Z}$. Then $c = 1c = c(am + bn) = acm + bcn$, which is divisible by a. □

3.13 Theorem: Alternative definition of gcd

Suppose $a, b \in \mathbb{Z}$ and $a \neq 0$ or $b \neq 0$. For a positive integer d, $d = gcd(a,b) \iff$

(a) $d \mid a$ and $d \mid d$

(b) If $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof) ($\Leftarrow$) Clear as (b) implies that if $c \mid a$ and $c \mid b$, then $c \leq |c| \leq |d| = d$.
($\Rightarrow$) If $c \mid a$ and $c \mid b$, then $c \mid ax + by$ for any $x, y \in \mathbb{Z}$. $\exists m, n \in \mathbb{Z}$ such that $am + bn = d$. $\square$

Remark $\gcd(a,b) = \gcd(c,d) \iff$

(a) Every common divisor of a and b is a common divisor of c and d.

(b) Every common divisor of c and d is a comoon divisor of a and b.

Example 3.14 $\gcd(a,b) = \gcd(a,-b) = \gcd(-a,b) = \gcd(-a,-b)$.

Section 4. Euclidean algorithm

Example 4.1

(a) Find $\gcd(a,b)$

(b) $\gcd(a,b) = d$. We know $\exists x, y \in \mathbb{Z}$ such that $d = ax + by$.

The Euclidean algorithm gives us x, y. Suppose $a, b \in \mathbb{Z}$ and $a \neq 0$ or $b \neq 0$. $\gcd(a,b) = gcd(|a|,|b|)$. We may assume $a, b > 0$. $a = q_1 b + r_1$ for $(0 \leq r_1 < b)$. If $r_1 = 0$, $\gcd(a,b) = b$. If $r_1 \neq 0$, then for b and r_1, $b = q_2 r_1 + r_2 \quad (0 \leq r_2 < r_1)$. The algorithm terminate when we arrive at $r_{n+1} = 0$. Then $gcd(a,b) = r_n$.

4.2 Theorem

If $a = qb + r$, then $\gcd(a,b) = \gcd(b,r)$.

Proof) $c \mid a, b \implies c \mid r \implies c \mid b, r$. Thus, $\gcd(a,b) \mid \gcd(b,r)$. Similarly if $c' \mid b, r$, then $c' \mid a = qb + r$. $\square$

Example 4.3

$$\begin{aligned} \gcd(a,b) = r_n = & r_{n-2} - q_n r_{n-1} && (11) \\ = & r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) && (12) \\ & \vdots && (13) \\ = & a(X) + b(Y) && (14) \end{aligned}$$