Contents

1 7 October 2024

1.1 Well-Ordering Principle

Theorem 1.1. *(Well-Ordering Principle) Every nonempty set S of non-negative integers contains a least element; that is some integer a in S such that $a \leqslant b$ for all b's belonging to S.*

We shall prove this by mathematical induction in Section 1.3

Theorem 1.2. *(Archimedeam property) If $a, b \in \mathbb{N}$, then there exists a positive integer n such that $na \geqslant b$.*

1.2 Mathematical Induction

Theorem 1.3. *(First Principle of Finite Induction) Let S be a set of positive integers with the following properties:*

- *The integer 1 belongs to S.*
- *Whenever the $k \in S$, the next integer $k + 1$ must also be in S.*

Then S is the set of all positive integers.

We shall prove this by Well-Ordering Principle in Section 1.3

Example 1.1. *Prove for all $n \in \mathbb{N}$,*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

- Base case ($n = 1$): $\sum_{k=1}^{1} k = \frac{1(1+1)}{2}$, which is just $1 = 1$. Hence, the base case holds.
- Hypothesis ($n = t$): Suppose $\sum_{k=1}^{t} k = \frac{t(t+1)}{2}$ holds.
- Inductive step ($n = t + 1$): $\sum_{k=1}^{t+1} k = (\sum_{k=1}^{t} k) + (t + 1) = \frac{t(t+1)}{2} + (t + 1) = \frac{(t+1)(t+2)}{2}$, which is what we want.

Hence, by induction, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

1.3 WOP iff MI

Let T be all the positive integers that are not in $S \in \mathbb{N}$

To prove the forward direction (WOP $\rightarrow$ MI), we need to show $T = \varnothing$. To do this, we use proof by contradiction. Now, by Well-Ordering Principle, T possesses a least element, let's call that a. Since $1 \in S$, then $a > 1$, and therefore $0 < a - 1 < a$. The choice of a as the smallest positive integer implies that $a - 1 \notin T$, this can only means that $a - 1 \in S$. By hypothesis, S must also contain $(a - 1) + 1 = a$. Now, we have previously said that T is a set that it's element is not in S, this contradicts the fact that $a \in T$. And therefore, T is empty set, and in consequence, S contains for all positive integers.

Now, let $A \subset \mathbb{N}$ be a nonempty set. And let $P(n)$ be the statement: $n \in A \rightarrow A$ has the smallest element.

To prove the backward direction (MI $\rightarrow$ WOP), we need to prove that $P(n)$ is true for $n \in \mathbb{N}$ using mathematical induction.

- Base case ($n = 1$): $1 \in A$, then this means that for all $x \in A$, we have $x \geqslant 1$ since $x \in \mathbb{N}$.
- Hypothesis ($n = t$): Suppose $P(n)$ is true for $n = 1, 2, 3, ..., t$
- Inductive step ($n = t + 1$): Now, assume $t + 1 \in A$, let $n \in 1, 2, ..., t$, there are two possible cases, which are $n \in A$ and $n \notin A$. Case 1: $n \in A$, then by induction hypothesis, A has a smallest element, and hence $P(t + 1)$ is true. Case 2: $n \notin A$, then for any $x \in A$, we have $x \geqslant t + 1$, this means A has smallest element as well, and therefore $P(t + 1)$ is true.

As we can see, no matter which case is it, $P(t + 1)$ holds. And therefore by mathematical induction, Well-Ordering Principle holds, and we are done.

1.4 The Binomial Theorem

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

Proof. magic. □

Example 1.2. *Show the following identities:*

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} + ... + (-1)^n \binom{n}{n} = 0 \tag{1}$$

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + ... + n\binom{n}{n} = n2^{n-1} \tag{2}$$

$$\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + ... + 2^n\binom{n}{n} = 3^n \tag{3}$$

There are 3 ways that we can tackle of these problems, namely using binomial theorem, mathematical induction, and combinatorial approach. In this note, I will just focus on using the binomial theorem.

For (1), we can substitute $a = 1$ and $b = -1$, then we can straight away get the answer. For (3), substitute $a = 1$, $b = 2$ and we are done. For (2), things are a bit more tricky. Instead of using our old binomial theorem, we need to differentiate both sides respect to b (or a).

$$\begin{aligned}
(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\
\frac{d}{db}(a+b)^n &= \frac{d}{db} \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\
n(a+b)^{n-1} &= \sum_{k=1}^{n} k\binom{n}{k} a^{n-k} b^{k-1}
\end{aligned}$$

From here, we just substitute $a = 1$ and $b = 1$ and we are done.

$$\begin{aligned}
n(1+1)^{n-1} &= \sum_{k=1}^{n} k\binom{n}{k} 1^{n-k}(1^{k-1}) \\
n2^{n-1} &= \sum_{k=1}^{n} k\binom{n}{k}
\end{aligned}$$

1.5 Euclidean division

Theorem 1.4. *(Euclidean division) For any two integers $a, b \in \mathbb{N}$, there exists two unique $q \in \mathbb{N}$, $r \in \mathbb{W}$, with $0 \leqslant r < b$ such that $a = qb + r$. This theorem is also known as the Division Algorithm.*

Proof. We now define a set $S = \{a - xb \mid x \text{ is an integer}; a - xb \geqslant 0\}$. There are three things that we need to proof, which are:

- $S \neq \varnothing$,
- $r < b$, and
- Uniqueness of q, r.

First, we prove $S \neq \varnothing$. To prove it, we just need to find value x such that $a - xb \geqslant 0$. Now, since $b \geqslant 1$, we get $|a|b \geqslant |a|$. So, we can choose $x = -|a|$, so that $a - (-|a|)b = a + |a|b$, which leads to $a + |a|b \geqslant a + |a| \geqslant 0$. Therefore, when $x = -|a|$, we get $a - xb = a + |a|b \geqslant 0$, which is an element in S. With this, we have shown that $S \neq \varnothing$.

Next, we show $r < b$. By WOP, let r be the smallest element in S. By definition of S, there exist q satisfying $r = a - qb$ and $0 \leqslant r$. Now, we need to use contradiction to show that $r < b$. Suppose $r \geqslant b$, then $0 \leqslant r - b$, and $r - b = (a - qb) - b = a - (q + 1)b$. This means that $a - (q + 1)b \in S$. However, $a - (q + 1)b = r - b < r$, meaning, $r - b \in S$. This is a contradiction as we previously had defined r to be the smallest element in S. Therefore, $r < b$.

Finally, we prove the uniqueness of q and r. Now, suppose $a = qb + r = q'b + r'$, where $0 \leqslant r < b$ and $0 \leqslant r' < b$. Then, $r' - r = b(q - q')$, this means that $|r' - r| = b|q - q'|$. From $0 \leqslant r < b$ and $0 \leqslant r' < b$, we can add them together and get $-b < r' - r < b$, which is just $|r' - r| < b$. This implies $b|q - q'| < b$, which also means $0 \leqslant |q - q'| < 1$. Since $|q - q'| \in \mathbb{N}$, this means that $q - q' = 0$, hence, $q = q'$ and $r = r'$. And we are done. □

1.6 a divides b

Definition 1.1. An integer b is said to be divisible by an integer $a \neq 0$, in symbols $a \mid b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

Theorem 1.5. *For integers a, b, c, the following hold:*

1. $a \mid 0$, $1 \mid a$, $a \mid a$
2. $a \mid 1$ *iff* $a = \pm 1$
3. $a \mid b$ *and* $c \mid d$, *then* $ac \mid bd$
4. $a \mid b$ *and* $b \mid c$, *then* $a \mid c$
5. $a \mid b$ *and* $b \mid a$, *then* $a = \pm b$
6. $a \mid b$ *and* $b \neq 0$, *then* $|a| \leqslant |b|$
7. $a \mid b$ *and* $a \mid c$, *then* $a \mid (bx + cy)$ *for some arbitrary* $x, y \in \mathbb{Z}$

2 9 October 2024

2.1 The Greatest Common Divisor

Definition 2.1. (Definition of gcd) Given $a, b \in \mathbb{Z}$, not both zero. $gcd(a, b)$ is the positive integer d that satisfies the following:

1. $d \mid a$ and $d \mid b$
2. If $c \mid a$ and $c \mid b$, then $c \leqslant d$

We usually write this as $gcd(a, b) = d$, or $(a, b) = d$.

There are a few trivial values of gcd:

- $gcd(a, 1) = 1$
- $gcd(a, 0) = |a|$

Theorem 2.1. *(Bezout's Identity) let $a, b \in \mathbb{Z}$, not both zero. Then there exists $x, y \in \mathbb{Z}$ such that $gcd(a, b) = d = ax + by$.*

Proof. Suppose $a, b \neq 0$ at the same time, define $S = \{au + bv \mid au + bv > 0; u, v \in \mathbb{Z}\}$. Now, there are two things that we need to prove:

- $S \neq \varnothing$, and
- $gcd(a, b) = d = ax + by$

The proof for $S \neq \varnothing$ is pretty trivial, just choose $u = 1$ or $u = -1$ and we are done.

As for showing $gcd(a, b) = d = ax + by$, we first use WOP to define d as the smallest element in S, then by definition of S, there exists $x, y \in \mathbb{Z}$ such that $d = ax + by$. The only thing that we need to show now is just $d = gcd(a, b)$, which means d is indeed the largest among all the common divisors.

Using Euclidean division, we obtain $q, r \in \mathbb{Z}$ such that $a = qd + r$, $0 \leqslant r < d$. Then, r can be written as follows:

$$\begin{aligned} r &= a - qd \\ &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy) \end{aligned}$$

Now, we have two cases, $r = 0$ and $r \neq 0$. Suppose $r \neq 0$, this means that $r \in S$ and $0 < r < d$. But, this is a contradiction because d is the smallest element in S. Therefore, $r = 0$.

This means that $a = qd + 0 = qd$ which implies $d \mid a$. Similarly, $d \mid b$. Let c be an arbitrary positive common divisor of a and b, by previous theorem in section 1.6, $c \mid (ax + by) \rightarrow c \mid d \rightarrow c = |c| \leqslant |d| = d$. Hence, d is indeed the largest among all the common divisors.

Then, by the definition of gcd, $d = gcd(a, b)$, which means $gcd(a, b) = d = ax + by$, and we are done. □

Definition 2.2. Let $a, b \in \mathbb{Z}$, not both zero. $gcd(a, b) = 1$ iff a and b are coprime (or relatively prime) to each other.

Example 2.1. 36 *and* 49 *are coprime because* $gcd(36, 49) = 1$

Corollary 2.1. *If* $gcd(a, b) = d$*, then* $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof. By using Bezout's identity, we are able to obtain some $x, y \in \mathbb{Z}$ such that $ax + by = d$. Now, divide the whole equation by d, and we get $(\frac{a}{d})x + (\frac{b}{d})y = 1$. Here, note that since $gcd(a, b) = d$, this means that $d \mid a$ and $d \mid b$, which means that $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. Then, by the definition of gcd, we obtain $gcd(\frac{a}{d}, \frac{b}{d}) = 1$. □

2.2 Euclid's lemma

Lemma 2.1. *(Euclid's Lemma) If* $a \mid bc$*, with* $gcd(a, b) = 1$*, then* $a \mid c$.

Proof. Use Bezout's identity (again). □

2.3 The Lowest Common Multiple

Definition 2.3. (Definition of lcm) $lcm(a, b) = m$, such that $m \in \mathbb{N}$ that satisfies the following

1. $a \mid m$ and $b \mid m$
2. If $a \mid c$ and $b \mid c$, with $c > 0$, then $m \leqslant c$

Note that we can also write $lcm(a, b) = m$ as $[a, b] = m$.

This brought us to a famous identity.

Theorem 2.2. *let* $a, b \in \mathbb{N}$, $gcd(a,b) * lcm(a,b) = ab$

Proof. If you have learnt abstract algebra (or group theory), you may try to give this video a watch. It's a very beautiful proof by using the first and second isomorphism theorem.

If not, fear not, we will proceed our usual way to prove this theorem by only using number theory knowledge. First, we let $d = gcd(a,b)$, and we can write a, b as $a = dr$, $b = ds$ for some $r, s \in \mathbb{Z}$. Now, if we let $m = \frac{ab}{d}$, then we will obtain $m = \frac{ab}{d} = \frac{drds}{d} = drs = as$, and similarly, $m = \frac{ad}{b} = rb$. Then, we get $m = as = rb$, which is the common multiple of a and b.

Next, we have to show that m is indeed the lowest common multiple. Now let c be any common multiple of a, b, say $c = au = bv$ for some $u, v \in \mathbb{Z}$. We know there exists $x, y \in \mathbb{Z}$ satisfying $ax + by = d$. So, by using all the information we obtained,

$$\begin{aligned}\frac{c}{m} &= \frac{cd}{ab} \\ &= \frac{c(ax+by)}{ab} \\ &= (\frac{c}{b})x + (\frac{c}{a})y \\ &= vx + uy\end{aligned}$$

From here, we observed that $\frac{c}{m} \in \mathbb{Z}$, this means that $m \leqslant c$, hence allow us to conclude m is indeed the lowest among all the common multiples. And by definition,

$$\begin{aligned}lcm(a,b) &= m \\ lcm(a,b) &= \frac{ab}{gcd(a,b)} \\ gcd(a,b) * lcm(a,b) &= ab\end{aligned}$$

□