Note 3. Induction

1 Induction

Imagine you have a long line of dominoes arranged in a row. Your goal is to make sure all the dominoes fall over.

1. First domino falls.
2. Dominoes knock each other over: if k-th falls, it will knock over the next domino $(k+1)$-th

Then all dominoes fall.

Theorem 1.1 (Finite Induction Principle). *Let $S(n)$ denote an open mathematical statement that involves one or more events of variable n, which represents a positive integer.*

1. *(Base case) If $S(1)$ is true;*
2. *(Inductive step:) If whenever $S(k)$ is true, then $S(k+1)$ is true,*

then $S(n)$ is true for all $n \in Z^+$.

Theorem 1.2 (Strong version). *Let $S(n)$ denote an open mathematical statement that involves one or more events of variable n, which represents a positive integer.*

1. *If $S(1)$ is true;*
2. *$S(1), S(2), \cdots, S(k)$ are true $\implies$ $S(k+1)$ is true,*

then $S(n)$ is true for all $n \in Z^+$.

Problem 1. *For any $n \in \mathbb{Z}^+$, show that $\sum_{i=1}^{n} i = n(n+1)/2$.*

Proof. The equality holds for $n = 1$. Assume that the equality holds for some $n = k$, where $k \geq 1$. Then $\sum_{i=1}^{k} i = k(k+1)/2$. We have

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = k(k+1)/2 + (k+1) = (k+1)(k+2)/2.$$

This implies that the equality also holds for $n = k+1$. So, by induction, the equality holds for all $n \in \mathbb{Z}^+$. $\square$

Problem 2. *For any $n \geq 0$, show that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.*

Proof. Base case: the equality holds for $n = 0$.
Inductive step: Assume that the equality holds for some $n = k$, where $k \geq 0$. Then $1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$. $\implies 1 + 2 + 2^2 + \cdots + 2^{k+1} = (2^{k+1} - 1) + 2^{k+1} = 2^{k+2} - 1$. This implies that the equality also holds for $n = k+1$. So by induction, the equality holds for all $n \geq 0$. $\square$

Theorem 1.3 (DeMorgan's Laws). *For two sets A and B,*

- $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Proof of the first one: For each element $x \in \overline{A \cup B} \Leftrightarrow x \notin A \cup B \Leftrightarrow x \notin A$ and $x \notin B \Leftrightarrow x \in \overline{A}$ and $x \in \overline{B} \Leftrightarrow x \in \overline{A} \cap \overline{B}$. Done! $\square$

Problem 3. *(homework)*

- $\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}$.
- $\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}$.

2 Euclidean Algorithm

Definition 2.1. *If $a, b \in \mathbb{Z}$ and $b \neq 0$, we say that b divides a, and we write $b|a$, if there is an integer n such that $a = bn$.*

- *b is a divisor of a*
- *a is a multiple of b*
- *If $b|a$ and $b|c$, the b is a common divisor of a, c. The largest such number is the greatest common divisor of a and c, written $gcd(a, c)$.*
- *If $b|a$ and $d|a$, then a is a common multiple of b and c. The smallest such a is the least common multiple of b and c, written $lcm(b, c)$.*

Theorem 2.2 (The Division Algorithm)**.** *If $a, b \in \mathbb{Z}$ and $b > 0$, then there are the first unique integers q and r such that $a = qb + r$ and $0 \leq r < b$.*

Find $gcd(a, b)$

Theorem 2.3 (Euclidean Algorithm)**.** *If $a, b \in \mathbb{Z}^+$, we apply the division algorithm as follows.*

$$a = q_1 b + r_1, \qquad 0 \leq r_1 < b;$$

$$b = q_2 r_1 + r_2, \qquad 0 \leq r_2 < r_1;$$

$$r_1 = q_3 r_2 + r_3, \qquad 0 \leq r_3 < r_2;$$

$$\cdots$$

$$r_{k-1} = q_{k+1} r_k + 0.$$

Then gcd(a, b)$= r_k$.

Show that: $gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = gcd(r_2, r_3) = \cdots = gcd(r_{k-1}, r_k) = r_k$.

Problem 4. *Find $gcd(22, 8)$.*

3 Recursion

Definition 3.1. *A set of sequences of subjects is recursive if it can be defined*

- *Base*
- *Recursion: A formulation that used the base to generate the rest of the objects*

Example 3.2 (The Fibonnaci Numbers)**.** *1,1,2,3,5,8,13.*

- *Base: $F_0 = F_1 = 1$.*
- *Recursion: $F_n = F_{n-1} + F_{n-2}$.*

Problem 5. *You have a pocket containing n balls. Each time, you can remove either 2 or 3 balls from the pocket. How many different ways can you empty the pocket?*

Solution. Let $f(n)$ represent the number of ways to empty a pocket containing n balls. The recursive relation can be derived as follows:

- If you remove 2 balls first, you're left with $n - 2$ balls, so the number of ways to empty the pocket from there is $f(n - 2)$.

- If you remove 3 balls first, you're left with $n-3$ balls, so the number of ways to empty the pocket from there is $f(n-3)$.

Thus
$$f(n) = f(n-2) + f(n-3), \text{ where } n \geq 5.$$
The base cases are
$$f(0) = 1, \quad f(1) = 0, \quad f(2) = 1.$$
□