

①

Ch.5 - Math Induction & Recursive Definition

§1 The First Principle of Mathematical Induction

Recall that the natural numbers were special sets that were defined as follows.

$$0 = \emptyset, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\}$$

$$4 = \{0, 1, 2, 3\}, \quad 5 = \{0, 1, 2, 3, 4\}, \text{ and in}$$

$$\text{general } n = \{0, 1, 2, 3, \dots, n-1\}.$$

The set of natural numbers \mathbb{N} has an important property called the Well-ordering Principle which follows from its set-theoretical definition.

Well-ordering Principle for \mathbb{N} : Every non-empty subset of \mathbb{N} has a smallest element.

Theorem 1 (First Principle of Mathematical Induction for \mathbb{N})

Let $P(n)$ be a formula of First logic with free variable n .

Then $\{P(0) \wedge (\forall n \in \mathbb{N})[P(n) \rightarrow P(n+1)]\} \Rightarrow (\forall n \in \mathbb{N})[P(n)]$.

Proof: Let $P(0) \wedge (\forall n \in \mathbb{N})[P(n) \rightarrow P(n+1)]$ be true. Now assume that $(\forall n \in \mathbb{N}) P(n)$ is false. Then $(\exists n \in \mathbb{N})[P(n) \text{ is false}]$. Let

$$E = \{n \in \mathbb{N} : P(n) \text{ is false}\}$$

Then E is a non-empty subset of \mathbb{N} . So by the Well-ordering Principle for \mathbb{N} , E has a smallest element, n_0 say. Since $P(0)$ is true n_0 cannot be 0. So $n_0 \geq 1$. Now consider $n_0 - 1$. Since n_0 was the smallest element of E , $P(n_0 - 1)$ must be true (otherwise, n_0 won't be the smallest element).

(2)

of E). Now $(\forall n \in \mathbb{N})[P(n) \rightarrow P(n+1)]$. So in particular for $n = n_0 - 1$, we get $P(n_0 - 1) \rightarrow P(n_0)$. Since $P(n_0 - 1)$ is true, it follows that $P(n_0)$ must also be true. But $P(n_0)$ was false because $n_0 \notin E$. Hence we have a contradiction. So our assumption that $(\forall n \in \mathbb{N})P(n)$ is false cannot be true. Hence $(\forall n \in \mathbb{N})P(n)$ is true.
 $\therefore \{P(0) \wedge (\forall n \in \mathbb{N})[P(n) \rightarrow P(n+1)]\} \models \Rightarrow (\forall n \in \mathbb{N})[P(n)]$.

Ex. 1 Prove that $(\forall n \in \mathbb{N})(2^0 + 2^1 + 2^2 + \dots + 2^n = 2^{n+1} - 1)$

Define $S_0 = 1$ & $S_n = S_{n-1} + 2^n$. $(\forall n \in \mathbb{N})(S_n = 2^{n+1} - 1)$

Sol. Let $P(n)$ be the statement, " $2^0 + 2^1 + 2^2 + \dots + 2^n = 2^{n+1} - 1$ ".

(a) Now $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$. So $P(0)$ is true.

(b) Also suppose $P(n)$ is true. Then $2^0 + 2^1 + 2^2 + \dots + 2^n = 2^{n+1} - 1$, So

$$\begin{aligned} 2^0 + 2^1 + 2^2 + \dots + 2^n + 2^{n+1} &= (2^0 + 2^1 + \dots + 2^n) + 2^{n+1} \\ &= (2^{n+1} - 1) + 2^{n+1} \\ &= (2 \cdot 2^{n+1}) - 1 = 2^{(n+1)+1} - 1 \end{aligned}$$

Hence if $P(n)$ is true, then $P(n+1)$ will be true.

Since n was arbitrary, it follows that

$(\forall n \in \mathbb{N})[P(n) \rightarrow P(n+1)]$ is true.

(c) Hence by the First Principle of Math Induction for \mathbb{N} $(\forall n \in \mathbb{N})P(n)$ is true. Thus

$$(\forall n \in \mathbb{N})[2^0 + 2^1 + 2^2 + \dots + 2^n = 2^{n+1} - 1]$$

Ex. 2 Prove that $(\forall n \in \mathbb{N})[5^n - 4n - 1]$ is an integer multiple of 16.

$$(\forall n \in \mathbb{N})[(\exists k \in \mathbb{Z})(5^n - 4n - 1 = 16k)]$$

Sol. Let $P(n)$ be the statement, " $5^n - 4n - 1$ is an integer multiple of 16."

(3)

Ex 2 (a)

$$\text{Now } 5^0 - 4(0) - 1 = 1 - 0 - 1 = 0 = 16(0).$$

So $5^0 - 4(0) - 1$ is an integer multiple of 16 because $0 \in \mathbb{Z}$. Hence $P(0)$ is true.

(b) Also suppose $P(n)$ is true. Then $5^n - 4n - 1 = 16k$ for some $k \in \mathbb{Z}$. So $5^{n+1} - 4(n+1) - 1$

$$= \{5 \cdot (5^n - 4n - 1) + 5(4n+1)\} - 4(n+1) - 1$$

$$= 5 \cdot (16k) + (20n+5) - 4n - 4 - 1$$

$$= 5 \cdot (16k) + 16n = 16(5k+n)$$

Since $5k+n \in \mathbb{Z}$, $5^{n+1} - 4(n+1) - 1$ is an integer multiple of 16. So if $P(n)$ is true, $P(n+1)$ will be true. Since n was arbitrary, it follows that $(\forall n \in \mathbb{N}) [P(n) \rightarrow P(n+1)]$.

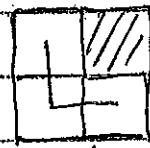
(c) Hence by the First Principle of Math Induction for \mathbb{N} , $(\forall n \in \mathbb{N}) P(n)$ is true. Thus

$(\forall n \in \mathbb{N}) [(5^n - 4n - 1) \text{ is an integer multiple of 16}]$

Def A 2^n -chess board is a 2^n by 2^n grid which consists of 2^{2n} squares. (For example, the standard chess board is a $2^3 \times 2^3$ grid which consists of $2^3 \times 2^3 = 8 \times 8 = 64$ squares.)

Def An L-shaped tile is a tile which consists of 3 squares in the shape of an L as .

We can easily see that the following grids can be tiled completely by using whole L-shaped tiles



$2^1 \times 2^1$ -one cell



$2^2 \times 2^2$ -one cell

Ex.3

(4)

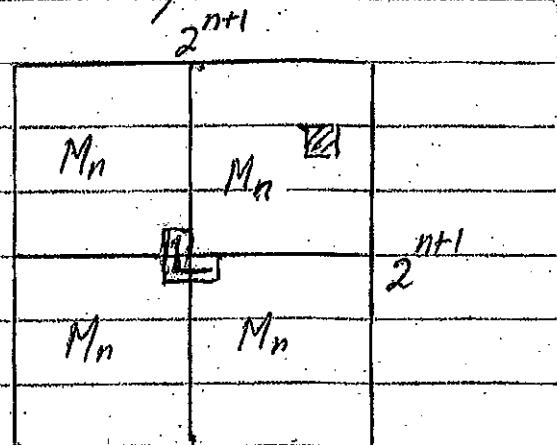
Let M_n be any 2^n by 2^n chessboard with one square (cell) removed. Prove that $(\forall n \in \mathbb{N}) [M_n \text{ can be tiled with only whole L-shaped tiles}]$.

Sol. Let $P(n)$ be, " M_n can be tiled with only whole L-shaped tiles."

(a) Since $M_0 = \boxed{\square} = 2^0 \times 2^0$ grid with one cell removed, M_0 can be tiled with zero L-shaped tiles. So $P(0)$ is true.

(b) Now suppose $P(n)$ is true. Then any M_n -type chessboard can be tiled with L-shaped tiles.

Consider any M_{n+1} -type chessboard (with the one cell removed). Then the removed cell must be in one of the four quadrants shown on the right.



Without loss of generality, assume that the removed tile is in the first quadrant. We use one L-shaped tile to tile the three cells from the other 3 quadrants that are nearest to the center. Then we will be left with 4 M_n -type chessboards. Since $P(n)$ is true, we can tile all 4 of these M_n -type boards with L-shaped tiles. Thus any M_{n+1} -type board can be completely tiled with whole L-shaped tiles.

Since n was arbitrary, $(\forall n \in \mathbb{N}) [P(n) \rightarrow P(n+1)]$

(c) So by the First Principle of Math induction for \mathbb{N} , $(\forall n \in \mathbb{N}) P(n)$. Thus any M_n -type chessboard can be completely tiled with only whole L-shaped tiles.

(5)

§2. More Induction Principles & Recursive definitions

Theorem 1' (First Principle of Math Induction for $\mathbb{N} + k_0$)

Let k_0 be any fixed integer and $P(n)$ be a formula of First Order Logic with free variable n . Then

$$P(k_0) \wedge (\forall n \in \mathbb{Z} \text{ with } n \geq k_0) [P(n) \rightarrow P(n+1)] \\ \Rightarrow (\forall n \in \mathbb{Z} \text{ with } n \geq k_0) P(n).$$

Proof. Do for H.W. The proof is the same as that of Theorem 1. The only thing we need to do is to replace 0 by k_0 everywhere in that proof & $(\forall n \in \mathbb{N})$ by $(\forall n \in \mathbb{Z} \text{ with } n \geq k_0)$.

Ex. 1 Prove that $(\forall n \in \mathbb{Z} \text{ with } n \geq 5) [2^n > n^2]$.

Sol. Let $P(n)$ be the statement, " $2^n > n^2$ ".

(a) Since $2^5 = 32 > 25 = 5^2$, $P(5)$ is true.

(b) Suppose that $n \geq 5$ and $P(n)$ is true. Then $2^n > n^2$. We will show that $2^{n+1} > (n+1)^2$. Now

$$\begin{aligned} 2^{n+1} &= 2^n + 2^n \\ &> n^2 + n^2 \quad \text{because } 2^n > n^2 \\ &= n^2 + n \cdot n \\ &\geq n^2 + 5 \cdot n \quad \text{because } n \geq 5 \\ &= n^2 + 2n + 3n \\ &> n^2 + 2n + 1 \quad \text{because } n \geq 5 \\ &= (n+1)^2 \end{aligned}$$

$\therefore 2^{n+1} > (n+1)^2$. So $P(n) \rightarrow P(n+1)$. Since n was arbitrary $(\forall n \in \mathbb{Z} \text{ with } n \geq 5) [P(n) \rightarrow P(n+1)]$. So by the F.P.M.I

(c) for $\mathbb{N} + 5$, $(\forall n \in \mathbb{Z} \text{ with } n \geq 5) P(n)$, i.e. $(\forall n \in \mathbb{Z} \text{ with } n \geq 5) [2^n > n^2]$.

Ex.2 Let $x \in \mathbb{R}$ with $x > -1$. Prove that $(\forall n \in \mathbb{N}) [(1+x)^n > nx]$. (6)

Sol. (Failed attempt). Fix $x \in \mathbb{R}$ with $x > -1$. Let $P(n)$ be the statement, " $(1+x)^n > nx$ ".

(a) Since $(1+x)^0 = 1 > 0 = 0(x)$, $P(0)$ is true.

(b) Suppose $P(n)$ is true. Then $(1+x)^n > nx$. We want to prove $P(n+1)$, i.e., $(1+x)^{n+1} > (n+1)x$. Now

$$\begin{aligned}(1+x)^{n+1} &= (1+x) \cdot (1+x)^n \\ &> (1+x) \cdot nx \quad \text{bec. } (1+x)^n > nx \\ &= nx + nx^2\end{aligned}$$

$\geq ?$ $nx + x$ does not follow!

$$= (n+1)x$$

Since we do not know that $nx^2 \geq x$, we cannot conclude that $(1+x)^{n+1} > (n+1)x$. Hence our attempt to prove the result failed — but this does not mean that the result is false.

Sol. (Successful attempt). We will show that

$(\forall n \in \mathbb{N}) [(1+x)^n \geq 1+nx]$. Since $1+nx > nx$, it will follow that $(\forall n \in \mathbb{N}) [(1+x)^n > nx]$.

Let $P(n)$ be the statement, " $(1+x)^n \geq 1+nx$ ".

(a) Since $(1+x)^0 = 1 \geq 1+0(x)$, $P(0)$ is true.

(b) Suppose $P(n)$ is true. Then $(1+x)^n \geq 1+nx$. Now

$$\begin{aligned}(1+x)^{n+1} &= (1+x)(1+x)^n \geq (1+x)(1+nx) \\ &= 1+x+nx+nx^2 \\ &\geq 1+nx+x = 1+(n+1)x\end{aligned}$$

So $(1+x)^{n+1} \geq 1+(n+1)x$. $\therefore P(n) \rightarrow P(n+1)$. Since n is arb.

$(\forall n \in \mathbb{N}) [P(n) \rightarrow P(n+1)]$. By the F.P.M.I. for \mathbb{N} (with parameter

(c) x), it follows that $(\forall n \in \mathbb{N}) P(n)$. So $(\forall n \in \mathbb{N}) [(1+x)^n \geq 1+nx]$.

Theorem 2 (Second Principle of Mathematical Induction for \mathbb{N})⁽⁷⁾
 Let $P(n)$ be a formula of First Order Logic with free variable n . Then

$$\begin{aligned} P(0) \wedge (\forall n \in \mathbb{N}) [P(0) \wedge P(1) \wedge \dots \wedge P(n) \rightarrow P(n+1)] \\ \Rightarrow (\forall n \in \mathbb{N}) P(n). \end{aligned}$$

Proof: Let $Q(n)$ be $P(0) \wedge P(1) \wedge \dots \wedge P(n)$. Then $Q(0)$ is $P(0)$. Now suppose that $P(0) \wedge (\forall n \in \mathbb{N}) [P(0) \wedge \dots \wedge P(n) \rightarrow P(n+1)]$ is true. Then $Q(0) \wedge (\forall n \in \mathbb{N}) [Q(n) \rightarrow P(n+1)]$. But $(\forall n \in \mathbb{N}) [Q(n) \rightarrow Q(n)]$, so $(\forall n \in \mathbb{N}) [Q(n) \rightarrow Q(n) \wedge P(n+1)]$. $\therefore Q(0) \wedge (\forall n \in \mathbb{N}) [Q(n) \rightarrow Q(n+1)]$ is true. $= Q(n+1)$
 So by the First Principle of Math Induction for \mathbb{N} , we get $(\forall n \in \mathbb{N}) Q(n)$ is true. Hence $(\forall n \in \mathbb{N}) [P(0) \wedge P(1) \wedge \dots \wedge P(n)]$ is true. From this it follows that $(\forall n \in \mathbb{N}) [P(n)]$ is true. Therefore $P(0) \wedge (\forall n \in \mathbb{N}) [P(0) \wedge \dots \wedge P(n) \rightarrow P(n+1)] \Rightarrow (\forall n \in \mathbb{N}) [P(n)]$.

Ex. 3 Prove that $(\forall n \in \mathbb{Z}^+) [n \text{ is a product of primes}]$

Sol. First of all a prime is any positive integer with exactly two positive divisors. Now let $P(n)$ be the statement, "n is a product of primes".

- (a) Since 1 is the empty product of primes, $P(1)$ is true.
 [If you don't believe this, then start the induction at $n=2$. $P(2)$ is true because 2 is a product of 1 prime]
- (b) Suppose $P(1) \wedge P(2) \wedge \dots \wedge P(n)$ is true, then every positive integer $\leq n$ is a product of primes. We will show that $n+1$ is a product of primes. There are two cases.

(8)

Ex.3

Case (i) : $n+1$ is prime. In this case $n+1$ is a product of 1 prime. So $P(n+1)$ is true.

Case (ii) : $n+1$ is not prime. In this case we can find positive integers $a > 1$ & $b > 1$ such that $n+1 = a \cdot b$. Since $a > 1$ & $b > 1$, both $a < n+1$ & $b < n+1$. So $a \leq n$ & $b \leq n$. Since every positive integer $\leq n$ is a product of primes, it follows that a and b are product of primes. So $n+1 = a \cdot b =$ a product of primes. Hence $P(n+1)$ is true again.

Thus in either case $P(0) \wedge P(1) \wedge \dots \wedge P(n) \rightarrow P(n+1)$

Since n was arbitrary it follows that $P(1) \wedge (\forall n \in \mathbb{Z}^+) [P(1) \wedge \dots \wedge P(n) \rightarrow P(n+1)]$

(c) So by the Second Principle of Math Induction for \mathbb{Z}^+ it follows that $(\forall n \in \mathbb{Z}^+) [P(n)]$. Hence $(\forall n \in \mathbb{Z}^+) [n \text{ is a product of primes}]$.

Theorem 3 (Principle of Definition by Recursion)

Let $a_0 \in \mathbb{N}$ and $g: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ be a binary function. Then there is a unique function $f: \mathbb{N} \rightarrow \mathbb{N}$ that is defined by $f(0) = a_0 \wedge f(n+1) = g(n, f(n))$ for $n \in \mathbb{N}$.

Proof: We will show that $(\forall n \in \mathbb{N}) [f(n) \text{ is a single value}]$.

Let $P(n)$ be the statement, " $f(n)$ is a single value."

(a) Since $f(0) = a_0$, a single value, $P(0)$ is true.

(b) Now suppose $P(n)$ is true. Then $f(n)$ is a single value. So $f(n+1) = g(n, f(n)) =$ a single value, because g is a function. $\therefore P(n+1)$.

(b) Hence $P(n) \rightarrow P(n+1)$. Since n was arbitrary, it follows that $(\forall n \in \mathbb{N}) [P(n) \rightarrow P(n+1)]$ (9)

(c) $\therefore P(0) \wedge (\forall n \in \mathbb{N}) [P(n) \rightarrow P(n+1)]$. Hence by the First Principle of Math Induction, it follows that $(\forall n \in \mathbb{N}) P(n)$. So $(\forall n \in \mathbb{N}) [f(n) \text{ is a single value}]$. Thus there is a unique function $f: \mathbb{N} \rightarrow \mathbb{N}$ with $f(0) = q_0$ and $(\forall n \in \mathbb{N}) [f(n+1) = g(n, f(n))]$.

Ex. 4 Let $f(0) = 1$ and $f(n+1) = g(n, f(n))$ where $g: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is the function defined by $g(x, y) = (x+1) \cdot y$. Find $f(n)$.

Sol. We have $f(0) = 1$ & $f(n+1) = (n+1) \cdot f(n)$. So

$$f(1) = (0+1), f(0) = 1(1) = 1$$

$$f(2) = (1+1), f(1) = 2(1) = 2$$

$$f(3) = (2+1) \cdot f(2) = 3(2) = 6$$

$$f(4) = (3+1) \cdot f(3) = 4(6) = 24$$

It is now easy to see that $f(n) = n!$

Ex. 5 Let $f(0) = 0$ & $f(n+1) = g(n, f(n))$ where $g: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is defined by $g(x, y) = 2y + 1$. Find $f(n)$.

Sol. We have $f(0) = 0$ & $f(n+1) = 2f(n) + 1$. So

$$f(1) = 2 \cdot f(0) + 1 = 2(0) + 1 = 1, \quad f(2) = 2 \cdot f(1) + 1 = 2(1) + 1 = 3$$

$$f(3) = 2f(2) + 1 = 2(3) + 1 = 7, \quad f(4) = 2f(3) + 1 = 2(7) + 1 = 15$$

It is now easy to see that $f(n) = 2^n - 1$.

Ex 6 Let $f(0) = 0$ & $f(n+1) = g(n, f(n))$ where $g(x, y) = y + 2x + 1$. Then $f(n+1) = f(n) + 2n + 1$. Check that $f(n) = n^2$.

Def. A set I is inductive if $\emptyset \in I$ and $x \in I \rightarrow x \cup \{x\} \in I$. According to the Axiom of Infinity (from ZFC) there exists at least one ^{set} inductive.

(10)

Def. The set ^{of} natural numbers \mathbb{N} is defined by
 $\mathbb{N} = \cap \{I : I \text{ is an inductive set}\}$

Note. $\mathbb{N} \subseteq$ any inductive set, and

$$0 = \emptyset \in \mathbb{N}, \quad 1 = \emptyset \cup \{\emptyset\} = \{\emptyset\} \in \mathbb{N}$$

$$2 = 1 \cup \{1\} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} \in \mathbb{N}.$$

$$3 = \{0, 1, 2\} \in \mathbb{N}, \quad 4 = \{0, 1, 2, 3\} \in \mathbb{N}.$$

$$n = \{0, 1, 2, \dots, n-1\}$$

Def. The successor function $s: \mathbb{N} \rightarrow \mathbb{N}$ is defined by
 $s(n) = n \cup \{n\} = \{0, 1, 2, \dots, n-1\} \cup \{n\} = \{0, 1, 2, \dots, n\} = n+1$

Def. Addition is the function $\text{ADD}: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ that is defined recursively by (a) $\text{ADD}(n, 0) = n$, (b) $\text{ADD}(n, s(k)) = s(\text{ADD}(n, k))$

Def. Multiplication is the function $\text{MULT}: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ define rec. by (a) $\text{MULT}(n, 0) = 0$, (b) $\text{MULT}(n, s(k)) = \text{ADD}(\text{MULT}(n, k), n)$

Def. Exponentiation is defined recursively by

a) $\exp_n(0) = 1$, (b) $\exp_n(s(k)) = \text{MULT}(\exp_n(k), n)$

$$n^0 = 1$$

$$n^{k+1} = n^k \cdot n$$

Def. Tetration is defined recursively by

(a) $\text{tow}_n(0) = 1$, (b) $\text{tow}_n(s(k)) = \exp_n(\text{tow}_n(k))$

$$n^{\overbrace{n}^{k+1}} = n^{n^k}$$

Ex. $\text{tow}_2(0) = 1$, $\text{tow}_2(1) = 2$, $\text{tow}_2(2) = 2^2$, $\text{tow}_2(3) = 2^2 = 16$
 $\text{tow}_2(4) = 2^2 = 2^4 = 2^{16} = 65,536$, $\text{tow}_2(5) = 2^{65,536}$

Note: $V_1 = \{\emptyset\}$ and $V_{n+1} = P(V_n)$, so from this $|V_{n+1}| = \text{tow}_2(n)$.