1-3 Proof

魏恒峰

hfwei@nju.edu.cn

2019 年 10 月 31 日

Theorem (First Principle of Mathematical Induction (Theorem 18.1))

For an integer n, let $P(n)$ denote an assertion. Suppose that

(i) *$P(1)$ is true, and*

(ii) *for all positive integers n, if $P(n)$ is true, then $P(n+1)$ is true.*

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

Theorem (First Principle of Mathematical Induction (Theorem 18.1))

For an integer n, let $P(n)$ denote an assertion. Suppose that

(i) $P(1)$ *is true, and*

(ii) *for all positive integers n, if $P(n)$ is true, then $P(n+1)$ is true.*

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

$$\Big[P(1) \land \forall n \in \mathbb{N}^{+} \big(P(n) \to P(n+1)\big)\Big] \to \forall n \in \mathbb{N}^{+} P(n).$$

Theorem (First Principle of Mathematical Induction (Theorem 18.1))

For an integer n, let $P(n)$ denote an assertion. Suppose that

(i) *$P(1)$ is true, and*

(ii) *for all positive integers n, if $P(n)$ is true, then $P(n+1)$ is true.*

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

$$\forall P : \Big[P(1) \land \forall n \in \mathbb{N}^{+} \big(P(n) \to P(n+1)\big)\Big] \to \forall n \in \mathbb{N}^{+} P(n).$$

Theorem (Second Principle of Mathematical Induction (Theorem 18.9))

For an integer n, let $Q(n)$ denote an assertion. Suppose that

(i) *$Q(1)$ is true, and*

(ii) *for all positive integers n, if $Q(1), \cdots, Q(n)$ are true, then $Q(n+1)$ is true.*

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

Theorem (Second Principle of Mathematical Induction (Theorem 18.9))

For an integer n, let $Q(n)$ denote an assertion. Suppose that

(i) *$Q(1)$ is true, and*

(ii) *for all positive integers n, if $Q(1), \cdots, Q(n)$ are true, then $Q(n+1)$ is true.*

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

$$\forall Q : \Big[Q(1) \land \forall n \in \mathbb{N}^+ \Big((Q(1) \land \cdots \land Q(n)) \to Q(n+1)\Big)\Big] \to \forall n \in \mathbb{N}^+ Q(n).$$

PMI(II) $\leftrightarrow$ PMI(I)

$$\forall P : \Big[P(1) \land \forall n \in \mathbb{N}^+ \big(P(n) \to P(n+1)\big)\Big] \to \forall n \in \mathbb{N}^+ P(n).$$

$$\forall Q : \Big[Q(1) \land \forall n \in \mathbb{N}^+ \Big(\big(Q(1) \land \cdots \land Q(n)\big) \to Q(n+1)\Big)\Big] \to \forall n \in \mathbb{N}^+ Q(n).$$

PMI(II) $\leftrightarrow$ PMI(I)

$$\forall P : \Big[P(1) \land \forall n \in \mathbb{N}^+ \big(P(n) \to P(n+1)\big)\Big] \to \forall n \in \mathbb{N}^+ P(n).$$

$$\forall Q : \Big[Q(1) \land \forall n \in \mathbb{N}^+ \Big(\big(Q(1) \land \cdots \land Q(n)\big) \to Q(n+1)\Big)\Big] \to \forall n \in \mathbb{N}^+ Q(n).$$

Let us calculate [calculemus].

PMI(II) $\rightarrow$ PMI(I)

$$\forall Q: \Big[Q(1) \land \forall n \in \mathbb{N}^+ \Big((Q(1) \land \cdots \land Q(n)) \rightarrow Q(n+1) \Big) \Big] \rightarrow \forall n \in \mathbb{N}^+ Q(n).$$

$$\forall P: \Big[P(1) \land \forall n \in \mathbb{N}^+ (P(n) \rightarrow P(n+1)) \Big] \rightarrow \forall n \in \mathbb{N}^+ P(n).$$

PMI(II) $\rightarrow$ PMI(I)

$$\forall Q : \Big[Q(1) \land \forall n \in \mathbb{N}^+ \Big((Q(1) \land \cdots \land Q(n)) \rightarrow Q(n+1) \Big) \Big] \rightarrow \forall n \in \mathbb{N}^+ Q(n).$$

$$\forall P : \Big[P(1) \land \forall n \in \mathbb{N}^+ (P(n) \rightarrow P(n+1)) \Big] \rightarrow \forall n \in \mathbb{N}^+ P(n).$$

$$Q(n) \triangleq P(n)$$

PMI(I) $\rightarrow$ PMI(II)

$$\forall P : \Big[P(1) \land \forall n \in \mathbb{N}^+ \big(P(n) \rightarrow P(n+1) \big) \Big] \rightarrow \forall n \in \mathbb{N}^+ P(n).$$

$$\forall Q : \Big[Q(1) \land \forall n \in \mathbb{N}^+ \Big((Q(1) \land \cdots \land Q(n)) \rightarrow Q(n+1) \Big) \Big] \rightarrow \forall n \in \mathbb{N}^+ Q(n).$$

PMI(I) $\rightarrow$ PMI(II)

$$\forall P : \Big[P(1) \land \forall n \in \mathbb{N}^+ (P(n) \to P(n+1))\Big] \to \forall n \in \mathbb{N}^+ P(n).$$

$$\forall Q : \Big[Q(1) \land \forall n \in \mathbb{N}^+ \Big((Q(1) \land \cdots \land Q(n)) \to Q(n+1)\Big)\Big] \to \forall n \in \mathbb{N}^+ Q(n).$$

$$P(n) \triangleq Q(1) \land \cdots \land Q(n)$$

说好的数学归纳法呢?

PMI(I) $\to$ PMI(II) (“标准” 证明示例)

$$P(n) \triangleq Q(1) \wedge \cdots \wedge Q(n)$$

用第一数学归纳法证明 $\forall n \in \mathbb{N}^+ : P(n)$。

PMI(I) $\rightarrow$ PMI(II) ("标准" 证明示例)

$$P(n) \triangleq Q(1) \land \cdots \land Q(n)$$

用第一数学归纳法证明 $\forall n \in \mathbb{N}^+ : P(n)$。

Proof.

By mathematical induction on $\mathbb{N}^+$.

Basis Step: $P(1)$

Inductive Hypothesis: $P(n)$

Inductive Step: $P(n) \rightarrow P(n+1)$

Therefore, $P(n)$ holds for all positive integers. $\square$

Theorem (Second Principle of Mathematical Induction)

For an integer n, let $Q(n)$ denote an assertion. Suppose that

(i) *$Q(1)$ is true, and*

(ii) *for all positive integers n, if $Q(1), \cdots, Q(n)$ are true, then $Q(n+1)$ is true.*

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

Theorem (Well-ordering Principle of $\mathbb{N}$)

Every non-empty subset of the natural numbers contains a minimum.

Theorem (Second Principle of Mathematical Induction)

For an integer n, let $Q(n)$ denote an assertion. Suppose that

(i) *$Q(1)$ is true, and*

(ii) *for all positive integers n, if $Q(1), \cdots, Q(n)$ are true, then $Q(n+1)$ is true.*

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

Theorem (Well-ordering Principle of $\mathbb{N}$)

Every non-empty subset of the natural numbers contains a minimum.

By contradiction.

$\exists S \neq \emptyset : S$ has no minimum element.

Theorem (Second Principle of Mathematical Induction)

For an integer n, let $Q(n)$ denote an assertion. Suppose that

(i) *$Q(1)$ is true, and*

(ii) *for all positive integers n, if $Q(1), \cdots, Q(n)$ are true, then $Q(n+1)$ is true.*

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

Theorem (Well-ordering Principle of $\mathbb{N}$)

Every non-empty subset of the natural numbers contains a minimum.

By contradiction.

$$\exists S \neq \emptyset : S \text{ has no minimum element.}$$

$$Q(n) \triangleq n \notin S$$

Theorem (First Principle of Mathematical Induction)

Theorem (Well-ordering Principle of $\mathbb{N}$)

Every non-empty subset of $\mathbb{N}$ *contains a minimum.*

Theorem (First Principle of Mathematical Induction)

Theorem (Well-ordering Principle of $\mathbb{N}$)

Every non-empty subset of $\mathbb{N}$ *contains a minimum.*

By mathematical induction on the size n of non-empty subsets of $\mathbb{N}$.

$$P(k): \text{All subsets of size } k \text{ contain a minimum.}$$

Theorem (First Principle of Mathematical Induction)

Theorem (Well-ordering Principle of $\mathbb{N}$)

Every non-empty subset of $\mathbb{N}$ *contains a minimum.*

By mathematical induction on the size n of non-empty subsets of $\mathbb{N}$.

$$P(k) : \text{All subsets of size } k \text{ contain a minimum.}$$

$$\begin{aligned} \text{Basis Step:} \quad & P(1) \\ \text{Inductive Hypothesis:} \quad & P(n) \\ \text{Inductive Step:} \quad & P(n) \to P(n+1) \end{aligned}$$

Theorem (First Principle of Mathematical Induction)

Theorem (Well-ordering Principle of $\mathbb{N}$)

Every non-empty subset of $\mathbb{N}$ contains a minimum.

By mathematical induction on the size n of non-empty subsets of $\mathbb{N}$.

$$P(k): \text{All subsets of size } k \text{ contain a minimum.}$$

Basis Step: $P(1)$

Inductive Hypothesis: $P(n)$

Inductive Step: $P(n) \to P(n+1)$

- $A' \leftarrow A \setminus a$
- $x \leftarrow \min A'$
- Compare x with a

Theorem (First Principle of Mathematical Induction)

Theorem (Well-ordering Principle of $\mathbb{N}$)

Every non-empty subset of $\mathbb{N}$ *contains a minimum.*

By mathematical induction on the size n of non-empty subsets of $\mathbb{N}$.

$$P(k) : \text{All subsets of size } k \text{ contain a minimum.}$$

Basis Step: $P(1)$

Inductive Hypothesis: $P(n)$

Inductive Step: $P(n) \to P(n+1)$

$$\forall n \in \mathbb{N} : P(n) \quad vs. \quad P(\infty)$$

Numbers

Suppose $A \subseteq \{1, 2, \cdots, 2n\}$ with $|A| = n + 1$. Please prove that:

(1) There are two numbers in A which are relatively prime.

(2) There are two numbers in A such that one divides the other.

Numbers

Suppose $A \subseteq \{1, 2, \cdots, 2n\}$ with $|A| = n + 1$. Please prove that:

(1) There are two numbers in A which are relatively prime.

(2) There are two numbers in A such that one divides the other.

There must be two numbers
which are only 1 apart.

Numbers

Suppose $A \subseteq \{1, 2, \cdots, 2n\}$ with $|A| = n + 1$. Please prove that:

(1) There are two numbers in A which are relatively prime.

(2) There are two numbers in A such that one divides the other.

$$a = 2^k m \ (k \in \mathbb{N}, m \text{ is odd})$$

There must be two numbers
which are only 1 apart.

Numbers

Suppose $A \subseteq \{1, 2, \cdots, 2n\}$ with $|A| = n + 1$. Please prove that:

(1) There are two numbers in A which are relatively prime.

(2) There are two numbers in A such that one divides the other.

$a = 2^k m$ ($k \in \mathbb{N}, m$ is odd)

Only n different odd parts

There must be two numbers which are only 1 apart.

Numbers

Suppose $A \subseteq \{1, 2, \cdots, 2n\}$ with $|A| = n + 1$. Please prove that:

(1) There are two numbers in A which are relatively prime.

(2) There are two numbers in A such that one divides the other.

$a = 2^k m \ (k \in \mathbb{N}, m \text{ is odd})$

There must be two numbers which are only 1 apart.

Only n different odd parts

$|A| = n + 1$

Numbers

Suppose $A \subseteq \{1, 2, \cdots, 2n\}$ with $|A| = n + 1$. Please prove that:

(1) There are two numbers in A which are relatively prime.

(2) There are two numbers in A such that one divides the other.

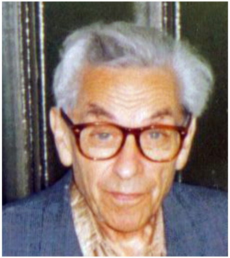
$a = 2^k m$ ($k \in \mathbb{N}, m$ is odd)

There must be two numbers which are only 1 apart.

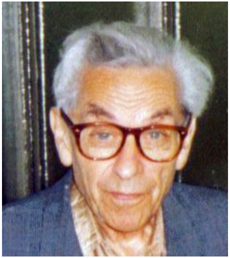
Only n different odd parts

$|A| = n + 1$

There must be two numbers in A with the same odd part.



Paul Erdős (1913 – 1996)



Paul Erdős (1913 – 1996)

Paul Erdős with Terence Tao

Theorem (Erdős-Szekeres Theorem)

Let n be a positive integer.
Every sequence of $n^2 + 1$ distinct integers must contain a monotone subsequence of length $n + 1$.

Theorem (Erdős-Szekeres Theorem)

Let n be a positive integer.
Every sequence of $n^2 + 1$ distinct integers must contain a monotone subsequence of length $n + 1$.

Fail for n^2

Theorem (Erdős-Szekeres Theorem)

Let n be a positive integer.
Every sequence of $n^2 + 1$ distinct integers must contain a monotone subsequence of length $n + 1$.

Fail for n^2

$$n = 3$$

$$7, 8, 9, 4, 5, 6, 1, 2, 3$$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

By Contradiction.

Suppose there are only a finite number of such primes.

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

By Contradiction.

Suppose there are only a finite number of such primes.

$$P = \{p_1, p_2, \cdots, p_r\}$$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

By Contradiction.

Suppose there are only a finite number of such primes.

$$P = \{p_1, p_2, \cdots, p_r\}$$

$$\boxed{A = 4p_1p_2 \cdots p_r + 3}$$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

By Contradiction.

Suppose there are only a finite number of such primes.

$$P = \{p_1, p_2, \cdots, p_r\}$$

$$\boxed{A = 4p_1p_2 \cdots p_r + 3}$$

A is *not* a prime: $A = q_1q_2 \cdots q_s$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

By Contradiction.

Suppose there are only a finite number of such primes.

$$P = \{p_1, p_2, \cdots, p_r\}$$

$$\boxed{A = 4p_1p_2\cdots p_r + 3}$$

A is *not* a prime: $A = q_1q_2\cdots q_s$

$\exists i : q_i \equiv 3 \pmod 4$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

By Contradiction.
Suppose there are only a finite number of such primes.

$$P = \{p_1, p_2, \cdots, p_r\}$$

$$\boxed{A = 4p_1p_2\cdots p_r + 3}$$

A is *not* a prime: $A = q_1q_2\cdots q_s$

$\exists i : q_i \equiv 3 \pmod 4$

(By Contradiction.)

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

By Contradiction.

Suppose there are only a finite number of such primes.

$$P = \{p_1, p_2, \cdots, p_r\}$$

$$\boxed{A = 4p_1p_2\cdots p_r + 3}$$

A is *not* a prime: $A = q_1q_2\cdots q_s$

$\exists i : q_i \equiv 3 \pmod 4$

$q_i \notin P$

(By Contradiction.)

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

By Contradiction.

Suppose there are only a finite number of such primes.

$$P = \{p_1, p_2, \cdots, p_r\}$$

$$\boxed{A = 4p_1p_2\cdots p_r + 3}$$

A is *not* a prime: $A = q_1q_2\cdots q_s$

$\exists i : q_i \equiv 3 \pmod 4$ | $q_i \notin P$

(By Contradiction.) | $(q_i | A, \quad p_i \nmid A)$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

By Contradiction.
Suppose there are only a finite number of such primes.

$$P = \{p_1, p_2, \cdots, p_r\} \quad (3 \notin P)$$

$$\boxed{A = 4p_1p_2 \cdots p_r + 3}$$

A is *not* a prime: $A = q_1q_2 \cdots q_s$

$\exists i : q_i \equiv 3 \pmod 4$ $\qquad$ $q_i \notin P$

(By Contradiction.) $\qquad$ $(q_i | A, \quad p_i \nmid A)$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

$$P = \{7\}$$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

$$P = \{7\}$$

$$A = 4 \cdot 7 + 3 = 31$$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

$$P = \{7\}$$

$$A = 4 \cdot 7 + 3 = 31$$

$$P = \{7, 31\}$$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

$$P = \{7\}$$

$$A = 4 \cdot 7 + 3 = 31$$

$$P = \{7, 31\}$$

$$A = 4 \cdot 7 \cdot 31 + 3 = 871 = 13 \cdot 67$$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

$$P = \{7\}$$

$$A = 4 \cdot 7 + 3 = 31$$

$$P = \{7, 31\}$$

$$A = 4 \cdot 7 \cdot 31 + 3 = 871 = 13 \cdot 67$$

$$P = \{7, 31, 67\}$$

Theorem (Primes 3 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 3 modulo 4.

Theorem (Primes 3 (Mod 4) Theorem)

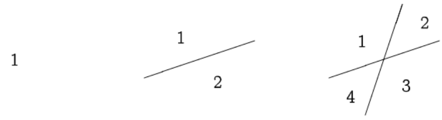
There are infinitely many primes that are congruent to 3 modulo 4.

Theorem (Primes 1 (Mod 4) Theorem)

There are infinitely many primes that are congruent to 1 modulo 4.

Lines in the Plane

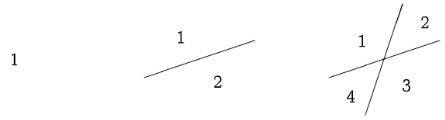
(1) What is the maximum number L_n of regions determined by n straight lines in the plane?



$L_0 = 1$ $\quad$ $L_1 = 2$ $\quad$ $L_2 = 4$

Lines in the Plane

(1) What is the maximum number L_n of regions determined by n straight lines in the plane?

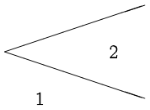


$L_0 = 1$ $L_1 = 2$ $L_2 = 4$

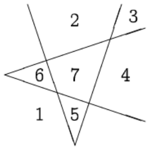
$$L_n = L_{n-1} + n = \frac{1}{2}n(n+1) + 1$$

Lines in the Plane

(2) What is the maximum number Z_n of regions determined by n bent lines, each containing one "zig", in the plane?



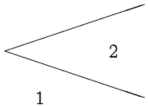
$Z_1 = 2$



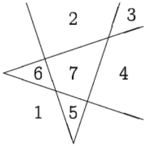
$Z_2 = 7$

Lines in the Plane

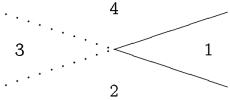
(2) What is the maximum number Z_n of regions determined by n bent lines, each containing one "zig", in the plane?



$Z_1 = 2$

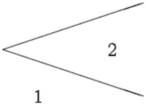


$Z_2 = 7$

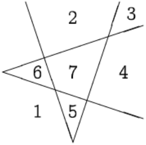


Lines in the Plane

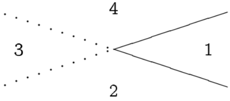
(2) What is the maximum number Z_n of regions determined by n bent lines, each containing one "zig", in the plane?



$Z_1 = 2$



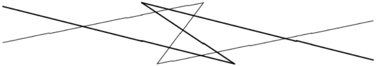
$Z_2 = 7$



$$Z_n = L_{2n} - 2n = 2n^2 - n + 1$$

Lines in the Plane

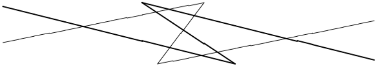
(3) What's the maximum number ZZ_n of regions determined by n "zig-zag" lines in the plane?



$ZZ_2 = 12$

Lines in the Plane

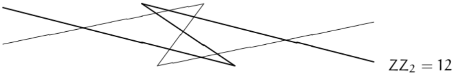
(3) What's the maximum number ZZ_n of regions determined by n "zig-zag" lines in the plane?



$$ZZ_n = ZZ_{n-1} + 9n - 8 = \frac{9}{2}n^2 - \frac{7}{2}n + 1$$

Lines in the Plane

(3) What's the maximum number ZZ_n of regions determined by n "zig-zag" lines in the plane?



$$ZZ_n = ZZ_{n-1} + 9n - 8 = \frac{9}{2}n^2 - \frac{7}{2}n + 1$$

$$9n - 8 = 9(n-1) + 1$$


Thank You!