Principle of Mathematical Induction 数学归纳法

Suppose that we have a propositional function $S(n)$ whose domain of discourse is the set of positive integers. Suppose that

(1) $S(1)$ is true;

(2) for all $n \geq 1$, if $S(n)$ is true, then $S(n+1)$ is true.

Then $S(n)$ is true for every positive integer n.

Condition (1) is sometimes called the **Basis Step (基本步)**

Condition (2) is sometimes called the **Inductive Step (归纳步)**

Principle of Mathematical Induction 数学归纳法

Suppose that we have a propositional function $S(n)$ whose domain of discourse is the set of positive integers. Suppose that
(1) $S(1)$ is true;
(2) for all $n \geq 1$, if $S(n)$ is true, then $S(n+1)$ is true.
Then $S(n)$ is true for every positive integer n.

Example 2.4.3 Use induction to show that $n! \geq 2^{n-1}$ for all $n \geq 1$.

Basis Step (n = 1)
$1! = 1 \geq 1 = 2^{n-1}$

$$n! = \begin{cases} 1 & \text{if } n = 0 \\ n(n-1)\ldots 2 \times 1 & \text{if } n \geq 1 \end{cases}$$

Inductive Step
We assume that the inequality is true for $n \geq 1$; that is,
we assume that $n! \geq 2^{n-1}$ is true.
We must then prove that the inequality is true for $n+1$; that is
$(n+1)! \geq 2^n$.

Principle of Mathematical Induction 数学归纳法

Suppose that we have a propositional function $S(n)$ whose domain of discourse is the set of positive integers. Suppose that
(1) $S(1)$ is true;
(2) for all $n \geq 1$, if $S(n)$ is true, then $S(n+1)$ is true.
Then $S(n)$ is true for every positive integer n.

$\longrightarrow S(1), S(2), \ldots, S(n)$

If we want to verify that the statements $S(n_0), S(n_0+1), \ldots$, where $n_0 \neq 1$, are true, we must change the **Basis Step** to $S(n_0)$ is true.

The Basis Step is to prove that the propositional function $S(n)$ is true for the smallest value n_0 in the domain of discourse.

The **Inductive Step** then becomes
for all $n \geq n_0$, if $S(n)$ is true, then $S(n+1)$ is true.

$\longrightarrow S(n_0), S(n_0+1), \ldots$

Principle of Mathematical Induction 数学归纳法

Exercise 1 Use induction to show that if $6 \cdot 7^n - 2 \cdot 3^n$ is divisible by 4 for all $n \geq 1$.

Basis Step (n = 1)

Inductive Step

Principle of Mathematical Induction 数学归纳法

Exercise 1 Use induction to show that if $6 \cdot 7^n - 2 \cdot 3^n$ is divisible by 4 for all $n \geq 1$.

Basis Step (n = 1)

If $n = 1$, $6 \cdot 7^n - 2 \cdot 3^n = 6 \cdot 7^1 - 2 \cdot 3^1 = 36$, which is divisible by 4.

Inductive Step

We assume that $6 \cdot 7^n - 2 \cdot 3^n$ is divisible by 4. We must then show that $6 \cdot 7^{n+1} - 2 \cdot 3^{n+1}$ is dibisible by 4.

$$\begin{aligned} 6 \cdot 7^{n+1} - 2 \cdot 3^{n+1} &= 7 \cdot 6 \cdot 7^n - 3 \cdot 2 \cdot 3^n \\ &= 6 \cdot 7^n - 2 \cdot 3^n + 6 \cdot 6 \cdot 7^n - 2 \cdot 2 \cdot 3^n \\ &= 6 \cdot 7^n - 2 \cdot 3^n + 36 \cdot 7^n - 4 \cdot 3^n. \end{aligned}$$

Since 4 divides $6 \cdot 7^n - 2 \cdot 3^n$, $36 \cdot 7^n$ and $-4 \cdot 3^n$, it divides their sum, which is $6 \cdot 7^{n+1} - 2 \cdot 3^{n+1}$.

2.5 Strong Form of Induction (强数学归纳法) and Well-Ordering Property (良序性)

2.5 Strong Form of Induction (强数学归纳法) and Well-Ordering Property (良序性)

Strong Form of Induction: To prove a statement is true, we assume the truth of all of the preceding statement (前趋语句)

Suppose that we have a propositional function $S(n)$ whose domain of discourse is the set of integers greater than or equal to n_0. Suppose that

(1) $S(n_0)$ is true;

(2) for all $n > n_0$, if $S(k)$ is true for all $n_0 \leq k < n$, then $S(n)$ is true.

Then $S(n)$ is true for every positive integer $n \geq n_0$.

Exercise Every integer >1 is a product of primes or itself is a prime.

Basis Step (n_0 = 2)

Inductive Step

Suppose that we have a propositional function $S(n)$ whose domain of discourse is the set of integers greater than or equal to n_0. Suppose that

(1) $S(n_0)$ is true;

(2) for all $n > n_0$, if $S(k)$ is true for all $n_0 \leq k < n$, then $S(n)$ is true.

Then $S(n)$ is true for every positive integer $n \geq n_0$.

Example 2.5.1 Use mathematical induction to show that postage of 4 cents or more can be achieved by using only 2-cent and 5-cent stamps.

Suppose that we have a propositional function $S(n)$ whose domain of discourse is the set of integers greater than or equal to n_0. Suppose that

(1) $S(n_0)$ is true;

(2) for all $n > n_0$, if $S(k)$ is true for all $n_0 \leq k < n$, then $S(n)$ is true.

Then $S(n)$ is true for every positive integer $n \geq n_0$.

Example 2.5.1 Use mathematical induction to show that postage of 4 cents or more can be achieved by using only 2-cent and 5-cent stamps.

Proof:

Basis Steps (n = 4, n = 5)

We can make 4-cents postage by using two 2-cent stamps. We can make 5-cents postage by using one 5-cent stamp. The Basis Steps are verified.

Inductive Step

We assume that $n \geq 6$ and that postage of k cents or more can be achieved by using only 2-cent and 5-cent stamps for $4 \leq k < n$.

By the inductive assumption, we can make postage of $n-2$ cents. We add a 2-cent stamp to make n-cents postage.

The Inductive Step is complete.

Example 2.5.1 Use mathematical induction to show that postage of 4 cents or more can be achieved by using only 2-cent and 5-cent stamps.

Extension

Given an unlimited supply of 5 cent and 7 cent stamps, what postages are possible?

Example 2.5.2 Suppose that the sequence $c_1,c_2,\ldots c_n$ is given by

$$c_1=0,\ c_n=c_{\lfloor n/2\rfloor}+n \text{ for all } n>1$$

use strong induction to prove that

$$c_n<2n \text{ for all } n\geq 1.$$

$c_1=$

$c_2=$

$c_3=$

$c_4=$

$c_5=$

Example 2.5.2 Suppose that the sequence $c_1,c_2,\ldots c_n$ is given by

$$c_1=0,\ c_n=c_{\lfloor n/2\rfloor}+n \text{ for all } n>1$$

use strong induction to prove that

$$c_n<2n \text{ for all } n\geq 1.$$

Proof:

Basis Steps (n=)

Inductive Step

Example 2.5.2 Suppose that the sequence $c_1, c_2, \ldots c_n$ is given by

$$c_1=0,\ c_n=c_{\lfloor n/2 \rfloor}+n \text{ for all } n>1$$

use strong induction to prove that

$$c_n<2n \text{ for all } n\geq 1.$$

Proof:

Basis Steps (n= 1)

Since $c_1 = 0 < 2 = 2 \cdot 1$, the Basis Step is verified.

Inductive Step

We assume that $c_k < 2k$, for all k, $1 \leq k < n$, and prove that $c_n < 2n$, $n > 1$. Since $1 < n$, $2 \leq n$. Thus $1 \leq n/2 < n$. Therefore $1 \leq [n/2]< n$ and taking $k = [n/2]$, we see that $1 \leq k< n$. By the inductive assumption

$$c_{[n/2]} = c_k < 2k = 2[n/2].$$

Now

$$c_n = c_{[n/2]} + n < 2[n/2] + n \leq 2(n/2) + n = 2n.$$

The Inductive Step is complete.

Example 2.5.4 Suppose that we insert parentheses and then multiply the n numbers $a_1 a_2 \ldots a_n$. Use strong induction to prove that if we insert parentheses in any manner whatsoever and then multiply the n numbers $a_1 a_2 \ldots a_n$, we perform $n-1$ multiplications.

For example, if $n = 4$, we might insert the parentheses as shown:

$$(a_1 a_2)(a_3 a_4)$$

Here we would first multiply a_1 by a_2 to obtain $a_1 a_2$ and a_3 by a_4 to obtain $a_3 a_4$. We would then multiply $a_1 a_2$ by $a_3 a_4$ to obtain $(a_1 a_2)(a_3 a_4)$. Notice that the number of multiplications is three.

Example 2.5.4 Suppose that we insert parentheses and then multiply the n numbers $a_1 a_2 \ldots a_n$. Use strong induction to prove that if we insert parentheses in any manner whatsoever and then multiply the n numbers $a_1 a_2 \ldots a_n$, we perform $n - 1$ multiplications.

For example, if $n = 4$, we might insert the parentheses as shown:

$$(a_1 a_2)(a_3 a_4)$$

Here we would first multiply a_1 by a_2 to obtain $a_1 a_2$ and a_3 by a_4 to obtain $a_3 a_4$. We would then multiply $a_1 a_2$ by $a_3 a_4$ to obtain $(a_1 a_2)(a_3 a_4)$. Notice that the number of multiplications is three.

Proof:

Basis Steps (n= 1)

Inductive Step

Assume that for all k, $1 \le k < n$, it takes $k - 1$ multiplications to compute the product of k numbers if parentheses are inserted in any manner whatsoever.

Well-Ordering Property (良序性)

The **well-ordering property for nonnegative integers** states that ***every nonempty set of nonnegative integers has a least element*****.**

Well-Ordering Property (良序性)

The **well-ordering property for nonnegative integers** states that ***every nonempty set of nonnegative integers has a least element*.**

Q1: What's the smallest element of the set
$\{ 16.99+1/n \mid n \in \mathbf{Z+} \}$?

Q2: How about $\{ \lfloor 16.99+1/n \rfloor \mid n \in \mathbf{Z+} \}$?

Well-Ordering Property (良序性)

The **well-ordering property for nonnegative integers** states that ***every nonempty set of nonnegative integers has a least element*.**

Q1: What's the smallest element of the set
$\{ 16.99+1/n \mid n \in \mathbf{Z+} \}$?

A1: $\{ 16.99+1/n \mid n \in \mathbf{Z}^+ \}$ doesn't have a smallest element (though it does have limit-point 16.99)!

Q2: How about $\{ \lfloor 16.99+1/n \rfloor \mid n \in \mathbf{Z+} \}$?

Well-Ordering Property (良序性)

The **well-ordering property for nonnegative integers** states that ***every nonempty set of nonnegative integers has a least element*.**

Q1: What's the smallest element of the set

$\{ 16.99+1/n \mid n \in \mathbf{Z+} \}$?

A1: $\{ 16.99+1/n \mid n \in \mathbf{Z}^+ \}$ doesn't have a smallest element (though it does have limit-point 16.99)!

Q2: How about $\{ \lfloor 16.99+1/n \rfloor \mid n \in \mathbf{Z+} \}$?

A2: 16 is the smallest element of $\{ \lfloor 16.99+1/n \rfloor \mid n \in Z+ \}$.
(EG: set n = 101)

Quotient-Remainder Theorem 商和余数定理

If d and n are integers, $d > 0$, there exist integers q (quotient) and r (remainder) satisfying $n = dq + r \quad (0 \leq r < d)$

Furthermore, q and r are unique; that is, if

$$n = dq_1 + r_1 \ (0 \leq r_1 < d)$$

and

$$n = dq_2 + r_2 \ (0 \leq r_2 < d),$$

then $q_1 = q_2$ and $r_1 = r_2$.

Quotient-Remainder Theorem 商和余数定理

If d and n are integers, $d > 0$, there exist integers q (quotient) and r (remainder) satisfying $n = dq + r \ \ (0 \leq r < d)$

Furthermore, q and r are unique; that is, if

$$n = dq_1 + r_1 \, (0 \leq r_1 < d)$$

and

$$n = dq_2 + r_2 \, (0 \leq r_2 < d),$$

then $q_1 = q_2$ and $r_1 = r_2$.

Example 2.5.5 When we divide n =74 by $d = 13$.

Quotient-Remainder Theorem 商和余数定理

If d and n are integers, $d > 0$, there exist integers q (quotient) and r (remainder) satisfying $n = dq + r \ \ (0 \le r < d)$

Furthermore, q and r are unique; that is, if

$$n = dq_1 + r_1 \ (0 \le r_1 < d)$$

and

$$n = dq_2 + r_2 \ (0 \le r_2 < d),$$

then $q_1 = q_2$ and $r_1 = r_2$.

Proof:

(i) First, show that, for each n, there is at least one pair of integers q, r satisfying $n = dq + r \ \ (0 \le r < d)$.

(ii) Then show that this pair q, r is unique.

Quotient-Remainder Theorem 商和余数定理

If d and n are integers, $d > 0$, there exist integers q (quotient) and r (remainder) satisfying $n = dq + r \;\; (0 \leq r < d)$
Furthermore, q and r are unique; that is, if
$n = dq_1 + r_1 \; (0 \leq r_1 < d)$ and $n = dq_2 + r_2 \; (0 \leq r_2 < d)$,
then $q_1 = q_2$ and $r_1 = r_2$.

Proof:

Quotient-Remainder Theorem 商和余数定理

If d and n are integers, $d > 0$, there exist integers q (quotient) and r (remainder) satisfying $n = dq + r \ \ (0 \leq r < d)$
Furthermore, q and r are unique; that is, if
$n = dq_1 + r_1 \ (0 \leq r_1 < d)$ and $n = dq_2 + r_2 \ (0 \leq r_2 < d)$,
then $q_1 = q_2$ and $r_1 = r_2$.

Proof: We show that X is nonempty using proof by cases. If $n \geq 0$, then $n - d \cdot 0 = n \geq 0$ so n is in X. Suppose that $n < 0$. Since d is a positive integer, $1 - d \leq 0$. Thus $n - dn = n(1-d) \geq 0$. In this case, $n - dn$ is in X. Therefore X is nonempty.

Since X is a nonempty set of nonnegative integers, by the Well-Ordering Property, X has a smallest element, which we denote r. We let q denote the specific value of k for which $r = n - dq$. Then $n = dq + r$.

Since r is in X, $r \geq 0$. We use proof by contradiction to show that $r < d$. Suppose that $r \geq d$. Then

$$n - d(q+1) = n - dq - d = r - d \geq 0.$$

Thus $n - d(q+1)$ is in X. Also, $n - d(q+1) = r - d < r$. But r is the smallest integer in X. This contradiction shows that $r < d$.

We have shown that if d and n are integers, $d > 0$, there exist integers q and r satisfying

$$n = dq + r \qquad 0 \leq r < d.$$

Quotient-Remainder Theorem 商和余数定理

If d and n are integers, $d > 0$, there exist integers q (quotient) and r (remainder) satisfying $n = dq + r \ \ (0 \le r < d)$
Furthermore, q and r are unique; that is, if
$n = dq_1 + r_1\ (0 \le r_1 < d)$ and $n = dq_2 + r_2\ (0 \le r_2 < d)$,
then $q_1 = q_2$ and $r_1 = r_2$.

Proof: We turn now to the uniqueness of q and r. Suppose that

$$n = dq_1 + r_1 \qquad 0 \le r_1 < d$$

and

$$n = dq_2 + r_2 \qquad 0 \le r_2 < d.$$

We must show that $q_1 = q_2$ and $r_1 = r_2$. Subtracting the previous equations, we obtain

$$0 = n - n = (dq_1 + r_1) - (dq_2 + r_2) = d(q_1 - q_2) - (r_2 - r_1),$$

which can be rewritten

$$d(q_1 - q_2) = r_2 - r_1.$$

The preceding equation shows that d divides $r_2 - r_1$. However, because $0 \le r_1 < d$ and $0 \le r_2 < d$,

$$-d < r_2 - r_1 < d.$$

But the only integer strictly between $-d$ and d divisible by d is 0. Therefore, $r_1 = r_2$. Thus, $d(q_1 - q_2) = 0$; hence, $q_1 = q_2$. The proof is complete. ◀

Problem-Solving Tips

In the Inductive Step of the Strong Form of Mathematical Induction, your goal is to prove case n. To do so, you can assume *all* preceding cases (not just the immediately preceding case as in Section 2.4). You could always use the Strong Form of Mathematical Induction. If it happens that you needed only the immediately preceding case in the Inductive Step, you merely used the form of mathematical induction of Section 2.4. However, assuming all previous cases potentially gives you more to work with in proving case n.

In the Inductive Step of the Strong Form of Mathematical Induction, when you assume that the statement $S(k)$ is true, you must be sure that k is in the domain of discourse of the propositional function $S(n)$. In the terminology of this section, you must be sure that $n_0 \leq k$ (see Examples 2.5.1 and 2.5.2).

In the Inductive Step of the Strong Form of Mathematical Induction, if you assume that case $n-p$ is true, there will be p Basis Steps: $n = n_0, n = n_0+1, \ldots, n = n_0+p-1$.

In general, the key to devising a proof using the Strong Form of Mathematical Induction is to find smaller cases "within" case n. For example, the smaller cases in Example 2.5.4 are the parenthesized products $(a_1 \cdots a_t)$ and $(a_{t+1} \cdots a_n)$ for $1 \leq t < n$.