Mathematical Proofs
A Transition to Advanced Mathematics

Chapter 6
Mathematical Induction

Gary Chartrand   Albert D. Polimeni   Ping Zhang

The Principle of Mathematical Induction

Definition

A number m in a (nonempty) set $A \subseteq \mathbf{R}$ is called a **least** (or **minimum** or **smallest**) element of A if $x \geq m$ for every $x \in A$.

Some nonempty sets of real numbers have a least element and some do not.

$\mathbf{N}$ has a smallest element, namely 1.

$[0, 1]$ has a minimum element, namely 0.

$(0, 1)$ has no minimum element.

$A = \left\{ \frac{1}{n} : \ n \in \mathbf{N} \right\}$ has no least element.

Theorem

If a set A of real numbers has a least element, then A has a unique least element.

Proof. Let m_1 and m_2 be least elements of A. Since m_1 is a least element, $m_2 \geq m_1$. Also, since m_2 is a least element, $m_1 \geq m_2$. Therefore, $m_1 = m_2$. □

Definition

A nonempty set S of real numbers is said to be **well-ordered** if every nonempty subset of S has a least element.

$S = \{2, 3, 6, 10\}$ is a well-ordered set. In fact, every nonempty finite set of real numbers is well-ordered.

$S = [0, 1]$ is not well-ordered since, for example, $(0, 1)$ is a nonempty subset of S having no least element.

Although it may appear evident that the set **N** of positive integers is well-ordered, this statement cannot be proved from the properties of positive integers that we have used and derived thus far. Consequently, this statement is accepted as an axiom, which we state below.

The Well-Ordering Principle

The set **N** of positive integers is well-ordered.

A consequence of the Well-Ordering Principle is another principle, which serves as the foundation for another and important proof technique.

The Principle of Mathematical Induction

Theorem

For each positive integer n, let $P(n)$ be a statement. If

(1) $P(1)$ is true and

(2) the implication

$$\text{If } P(k), \text{ then } P(k+1).$$

is true for every positive integer k,

then $P(n)$ is true for every positive integer n.

Proof. Assume, to the contrary, that the theorem is false. Then conditions (1) and (2) are satisfied but there exist some positive integers n for which $P(n)$ is a false statement.

Proof (continued)

Let

$$S = \{n \in \mathbf{N} : \ P(n) \text{ is false}\}.$$

Since S is a nonempty subset of $\mathbf{N}$, it follows by the Well-Ordering Principle that S contains a least element s. Since $P(1)$ is true, $1 \notin S$. Thus, $s \geq 2$ and $s - 1 \in \mathbf{N}$. Therefore, $s - 1 \notin S$ and so $P(s-1)$ is a true statement. By condition (2), $P(s)$ is also true and so $s \notin S$. This, however, contradicts our assumption that $s \in S$. □

The Principle of Mathematical Induction

As a consequence of the Principle of Mathematical Induction, the quantified statement $\forall n \in \mathbf{N},\ P(n)$ can be proved to be true if

(1) we can show that the statement $P(1)$ is true and

(2) we can establish the truth of the implication

$$\text{If } P(k), \text{ then } P(k+1).$$

for every positive integer k.

Definition

A proof using the Principle of Mathematical Induction is called an **induction proof** or a **proof by induction**.

The verification of the truth of $P(1)$ in an induction proof is called the **base step**, **basis step** or the **anchor** of the induction.

In the implication

$$\text{If } P(k), \text{ then } P(k+1).$$

for an arbitrary positive integer k, the statement $P(k)$ is called the **inductive** (or **induction**) **hypothesis**.

The Principle of Mathematical Induction

Often we use a direct proof to verify

$$\forall k \in \mathbf{N},\ P(k) \Rightarrow P(k+1), \tag{1}$$

although any proof technique is acceptable. That is, we typically assume that the inductive hypothesis $P(k)$ is true for an arbitrary positive integer k and attempt to show that $P(k+1)$ is true.

Definition

Establishing the truth of (1) is called the **inductive step** in the induction proof.

We illustrate this proof technique by showing that the sum of the first n positive integers is given by $n(n+1)/2$ for every positive integer n, that is,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Example 1

Result Let

$$P(n):\ 1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

where $n \in \mathbf{N}$. Then $P(n)$ is true for every positive integer n.

Proof. We employ induction. Since $1=(1\cdot 2)/2$, the statement $P(1)$ is true. Assume that $P(k)$ is true for an arbitrary positive integer k, that is, assume that

$$1+2+3+\cdots+k=\frac{k(k+1)}{2}.$$

We show that $P(k+1)$ is true, that is, we show that

$$1+2+3+\cdots+(k+1)=\frac{(k+1)(k+2)}{2}.$$

Example 1 (continued)

Thus,

$$
\begin{aligned}
1+2+3+\cdots+(k+1) &= (1+2+3+\cdots+k)+(k+1) \\
&= \frac{k(k+1)}{2}+(k+1) \\
&= \frac{k(k+1)+2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2},
\end{aligned}
$$

as desired.

By the Principle of Mathematical Induction, $P(n)$ is true for every positive integer n. □

Example 2

Result For every positive integer n,

$$\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{(n+1)(n+2)}=\frac{n}{2n+4}.$$

Proof. We use induction. Since

$$\frac{1}{2\cdot 3}=\frac{1}{2\cdot 1+4}=\frac{1}{6},$$

the formula holds for $n=1$.

Example 2 (continued)

Assume that

$$\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{(k+1)(k+2)}=\frac{k}{2k+4}$$

for a positive integer k. We show that

$$\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{(k+2)(k+3)}=\frac{k+1}{2(k+1)+4}=\frac{k+1}{2k+6}.$$

Example 2 (continued)

Observe that

$$\begin{aligned}
&\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{(k+2)(k+3)}\\
&=\left[\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{(k+1)(k+2)}\right]+\frac{1}{(k+2)(k+3)}\\
&=\frac{k}{2k+4}+\frac{1}{(k+2)(k+3)}=\frac{k}{2(k+2)}+\frac{1}{(k+2)(k+3)}\\
&=\frac{k(k+3)+2}{2(k+2)(k+3)}=\frac{k^2+3k+2}{2(k+2)(k+3)}\\
&=\frac{(k+1)(k+2)}{2(k+2)(k+3)}=\frac{k+1}{2(k+3)}=\frac{k+1}{2k+6},
\end{aligned}$$

giving us the desired result.

Example 2 (continued)

By the Principle of Mathematical Induction,

$$\frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(n+1)(n+2)} = \frac{n}{2n+4}$$

for every positive integer n. □

A More General Principle of Mathematical Induction

Theorem

For each integer m, the set

$$S = \{i \in \mathbf{Z} : \ i \geq m\}$$

is well-ordered.

The Principle of Mathematical Induction

For a fixed integer m, let $S = \{i \in \mathbf{Z} : \ i \geq m\}$. For each integer $n \in S$, let $P(n)$ be a statement. If

(1) $P(m)$ is true and

(2) the implication

$$\text{If } P(k), \text{ then } P(k+1).$$

is true for every integer $k \in S$,

then $P(n)$ is true for every integer $n \in S$.

A More General Principle of Mathematical Induction

Example 3

Result For every nonnegative integer n,

$$2^n > n.$$

Proof. We proceed by induction. The inequality holds for $n = 0$ since $2^0 > 0$. Assume that $2^k > k$, where k is a nonnegative integer. We show that $2^{k+1} > k + 1$. When $k = 0$, we have

$$2^{k+1} = 2 > 1 = k + 1.$$

We therefore assume that $k \geq 1$. Then

$$2^{k+1} = 2 \cdot 2^k > 2k = k + k \geq k + 1.$$

By the Principle of Mathematical Induction, $2^n > n$ for every nonnegative integer n. □

Example 4

Result For every integer $n \geq 5$,

$$2^n > n^2.$$

Proof. We proceed by induction. Since $2^5 > 5^2$, the inequality holds for $n = 5$. Assume that $2^k > k^2$ where $k \geq 5$. We show that

$$2^{k+1} > (k+1)^2.$$

Observe that

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k > 2k^2 = k^2 + k^2 \geq k^2 + 5k \\ &= k^2 + 2k + 3k \geq k^2 + 2k + 15 \\ &> k^2 + 2k + 1 = (k+1)^2. \end{aligned}$$

Therefore, $2^{k+1} > (k+1)^2$. By the Principle of Mathematical Induction, $2^n > n^2$ for every integer $n \geq 5$. □

Example 5

Result For every nonnegative integer n,

$$9 \mid \left(4^{3n} - 1\right).$$

Proof. We proceed by induction. When $n = 0$, $4^{3n} - 1 = 0$. Since $9 \mid 0$, the statement is true when $n = 0$. Assume that

$$9 \mid \left(4^{3k} - 1\right), \text{ where } k \text{ is a nonnegative integer.}$$

We now show that

$$9 \mid \left(4^{3k+3} - 1\right).$$

Example 5 (continued)

Since $9 \mid \left(4^{3k} - 1\right)$, it follows that $4^{3k} - 1 = 9x$ for some integer x. Hence, $4^{3k} = 9x + 1$. Now, observe that

$$\begin{aligned} 4^{3k+3} - 1 &= 4^3 \cdot 4^{3k} - 1 = 64(9x + 1) - 1 \\ &= 64 \cdot 9x + 64 - 1 = 64 \cdot 9x + 63 \\ &= 9(64x + 7). \end{aligned}$$

Since $64x + 7$ is an integer, $9 \mid \left(4^{3k+3} - 1\right)$.

By the Principle of Mathematical Induction, $9 \mid \left(4^{3n} - 1\right)$ for every nonnegative integer n. □

A More General Principle of Mathematical Induction

Theorem

If A is a finite set of cardinality $n \geq 0$, then the cardinality of its power set $\mathcal{P}(A)$ is 2^n.

Proof. We proceed by induction. If A is a set with $|A| = 0$, then $A = \emptyset$. Thus, $\mathcal{P}(A) = \{\emptyset\}$ and so $|\mathcal{P}(A)| = 1 = 2^0$. Therefore, the theorem is true for $n = 0$. Assume that if B is any set with $|B| = k$ for some nonnegative integer k, then $|\mathcal{P}(B)| = 2^k$. We show that if C is a set with $|C| = k + 1$, then $|\mathcal{P}(C)| = 2^{k+1}$. Let

$$C = \{c_1, c_2, \ldots, c_{k+1}\}.$$

A More General Principle of Mathematical Induction

Proof (continued)

By the inductive hypothesis, there are 2^k subsets of the set $\{c_1, c_2, \ldots, c_k\}$, that is, there are 2^k subsets of C not containing c_{k+1}. Any subset of C containing c_{k+1} can be expressed as $D \cup \{c_{k+1}\}$, where $D \subseteq \{c_1, c_2, \ldots, c_k\}$. Again, by the inductive hypothesis, there are 2^k such subsets D. Therefore, there are $2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$ subsets of C.

By the Principle of Mathematical Induction, it follows for every nonnegative integer n that if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$. □

The Strong Principle of Mathematical Induction

For each positive integer n, let $P(n)$ be a statement. If

(*a*) $P(1)$ is true and

(*b*) the implication

If $P(i)$ for every integer i with $1 \leq i \leq k$, then $P(k+1)$

is true for every positive integer k,

then $P(n)$ is true for every positive integer n.

Suppose that we are considering a sequence $a_1, a_2, a_3, \ldots$ of numbers, also expressed as $\{a_n\}$. One way of defining a sequence $\{a_n\}$ is to specify explicitly the nth term a_n (as a function of n).

For example, we might have

$$a_n = \frac{1}{n}, a_n = \frac{(-1)^n}{n^2} \text{ or } a_n = n^3 + n$$

for each $n \in \mathbf{N}$.

Definition

A sequence can also be **defined recursively**. In a **recursively-defined sequence** $\{a_n\}$, only the first term or perhaps the first few terms are defined specifically, say $a_1, a_2, \ldots, a_k$ for some fixed $k \in \mathbf{N}$. These are called the **initial values**. Then a_{k+1} is expressed in terms of $a_1, a_2, \ldots, a_k$ and, more generally, for $n > k$, a_n is expressed in terms of $a_1, a_2, \ldots, a_{n-1}$. This is called the **recurrence relation**.

A specific example of this is the sequence $\{a_n\}$ defined by

$$a_1 = 1, a_2 = 3 \text{ and } a_n = 2a_{n-1} - a_{n-2} \text{ for } n \geq 3.$$

In this case, there are two initial values, namely $a_1 = 1$ and $a_2 = 3$. The recurrence relation here is

$$a_n = 2a_{n-1} - a_{n-2} \text{ for } n \geq 3.$$

Letting $n = 3$, we find that $a_3 = 2a_2 - a_1 = 5$; while letting $n = 4$, we have $a_4 = 2a_3 - a_2 = 7$. Similarly, $a_5 = 9$ and $a_6 = 11$. From this information, one might well conjecture (guess) that $a_n = 2n - 1$ for every $n \in \mathbf{N}$.

Example 6

Result A sequence $\{a_n\}$ is defined recursively by

$$a_1 = 1, a_2 = 3 \text{ and } a_n = 2a_{n-1} - a_{n-2} \text{ for } n \geq 3.$$

Then $a_n = 2n - 1$ for all $n \in \mathbf{N}$.

Proof. We proceed by induction. Since $a_1 = 2 \cdot 1 - 1 = 1$, the formula holds for $n = 1$. Assume for an arbitrary positive integer k that $a_i = 2i - 1$ for all integers i with $1 \leq i \leq k$.

Example 6 (continued)

We show that

$$a_{k+1} = 2(k+1) - 1 = 2k + 1.$$

If $k = 1$, then $a_{k+1} = a_2 = 2 \cdot 1 + 1 = 3$. Since $a_2 = 3$, it follows that $a_{k+1} = 2k + 1$ when $k = 1$. Hence, we may assume that $k \geq 2$. Since $k + 1 \geq 3$, it follows that

$$a_{k+1} = 2a_k - a_{k-1} = 2(2k-1) - (2k-3) = 2k + 1,$$

which is the desired result. By the Strong Principle of Mathematical Induction, $a_n = 2n - 1$ for all $n \in \mathbf{N}$. □

Example 7

Result A sequence $\{a_n\}$ is defined recursively by

$$a_1 = 1, a_2 = 4 \text{ and } a_n = 2a_{n-1} - a_{n-2} + 2 \text{ for } n \geq 3.$$

Then $a_n = n^2$ for all $n \in \mathbf{N}$.

Proof. We proceed by induction. Since $a_1 = 1 = 1^2$, the formula holds for $n = 1$. Assume for an arbitrary positive integer k that $a_i = i^2$ for every integer i with $1 \leq i \leq k$.

Example 7 (continued)

We show that

$$a_{k+1} = (k+1)^2.$$

Since $a_2 = 4$, it follows that $a_{k+1} = (k+1)^2$ when $k = 1$. Thus, we may assume that $k \geq 2$. Hence, $k+1 \geq 3$ and so

$$\begin{aligned} a_{k+1} &= 2a_k - a_{k-1} + 2 = 2k^2 - (k-1)^2 + 2 \\ &= 2k^2 - (k^2 - 2k + 1) + 2 = k^2 + 2k + 1 \\ &= (k+1)^2. \end{aligned}$$

By the Strong Principle of Mathematical Induction, $a_n = n^2$ for all $n \in \mathbf{N}$. □

Example 8

Result For each integer $n \geq 8$, there are nonnegative integers a and b such that $n = 3a + 5b$.

Proof. We proceed by induction. Since $8 = 3 \cdot 1 + 5 \cdot 1$, the statement is true for $n = 8$. Assume for each integer i with $8 \leq i \leq k$, where $k \geq 8$ is an arbitrary integer, that there are nonnegative integers s and t such that $i = 3s + 5t$. Consider the integer $k + 1$. We show that there are nonnegative integers x and y such that $k + 1 = 3x + 5y$. Since

$$9 = 3 \cdot 3 + 5 \cdot 0 \text{ and } 10 = 3 \cdot 0 + 5 \cdot 2,$$

this is true if $k + 1 = 9$ and $k + 1 = 10$. Hence, we may assume that $k + 1 \geq 11$. Thus, $8 \leq (k + 1) - 3 < k$.

Example 8 (continued)

By the induction hypothesis, there are nonnegative integers a and b such that

$$(k+1) - 3 = 3a + 5b \text{ and so } k+1 = 3(a+1) + 5b.$$

Letting $x = a + 1$ and $y = b$, we have the desired conclusion.

By the Strong Principle of Mathematical Induction, for every integer $n \geq 8$, there are nonnegative integers a and b such that $n = 3a + 5b$. □

Proof by Minimum Counterexample

If we wish to prove a statement of the type

$$\forall n \in \mathbf{N},\ \ P(n),$$

the first proof technique that could probably occur to us now is induction. However, there is always the possibility that this technique does not work (or does not work well). Another possible approach that one can try is related to induction and is a consequence of the Well-Ordering Principle.

Here, we try a proof by contradiction. In this case, we assume that

$$\forall n \in \mathbf{N}, P(n) \text{ is false},$$

obtaining

$$\exists n \in \mathbf{N}, \sim P(n),$$

that is, there are positive integers n such that $P(n)$ is false.

Proof by Minimum Counterexample

By the Well-Ordering Principle, there exists a smallest positive integer n (which we will call m) such that $P(n)$ is a false statement. Therefore, $P(m)$ is false and if $m \geq 2$, then $P(k)$ is true for every integer k with $1 \leq k < m$.

Definition

The integer m is referred to as a **minimum counterexample** of the statement $\forall n \in \mathbf{N}, P(n)$.

If a proof (by contradiction) of $\forall n \in \mathbf{N}, P(n)$ can be given using the fact that m is a minimum counterexample, then such a proof is called a **proof by minimum counterexample**.

Proof by Minimum Counterexample

Example 9

Result For every positive integer n,

$$6 \mid \left(n^3 - n\right).$$

Proof. Assume, to the contrary, that there are positive integers n such that $6 \nmid (n^3 - n)$. Then there is a smallest positive integer n such that $6 \nmid \left(n^3 - n\right)$. Let m be this integer. If $n = 1$, then $n^3 - n = 0$; while if $n = 2$, then $n^3 - n = 6$. Since $6 \mid 0$ and $6 \mid 6$, it follows that $6 \mid \left(n^3 - n\right)$ for $n = 1$ and $n = 2$. Therefore $m \geq 3$. So, we can write $m = k + 2$, where $1 \leq k < m$.

Example 9 (continued)

Observe that

$$m^3 - m = (k+2)^3 - (k+2) = (k^3 + 6k^2 + 12k + 8) - (k+2)$$
$$= (k^3 - k) + (6k^2 + 12k + 6).$$

Since $k < m$, it follows that $6 \mid \left(k^3 - k\right)$. Hence, $k^3 - k = 6x$ for some integer x. So, we have

$$m^3 - m = 6x + 6(k^2 + 2k + 1) = 6(x + k^2 + 2k + 1).$$

Since $x + k^2 + 2k + 1$ is an integer, $6 \mid \left(m^3 - m\right)$, which produces a contradiction. □

Example 10

Result For every nonnegative integer n,

$$3 \mid \left(2^{2n} - 1\right).$$

Proof. Assume, to the contrary, that there are nonnegative integers n for which $3 \nmid \left(2^{2n} - 1\right)$. By a theorem in this chapter, there is a smallest nonnegative integer n such that $3 \nmid \left(2^{2n} - 1\right)$. Denote this integer by m. Thus $3 \nmid \left(2^{2m} - 1\right)$ and $3 \mid \left(2^{2n} - 1\right)$ for all nonnegative integers n for which $0 \le n < m$. Since $3 \mid \left(2^{2n} - 1\right)$ when $n = 0$, it follows that $m \ge 1$. Hence, m can be expressed by $m = k + 1$, where $0 \le k < m$. Thus, $3 \mid \left(2^{2k} - 1\right)$, which implies that $2^{2k} - 1 = 3x$ for some integer x. Consequently, $2^{2k} = 3x + 1$.

Example 10 (continued)

Observe that

$$2^{2m} - 1 = 2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^2 \cdot 2^{2k} - 1$$
$$= 4(3x + 1) - 1 = 12x + 3 = 3(4x + 1).$$

Since $4x + 1$ is an integer, $3 \mid \left(2^{2m} - 1\right)$, which produces a contradiction. □