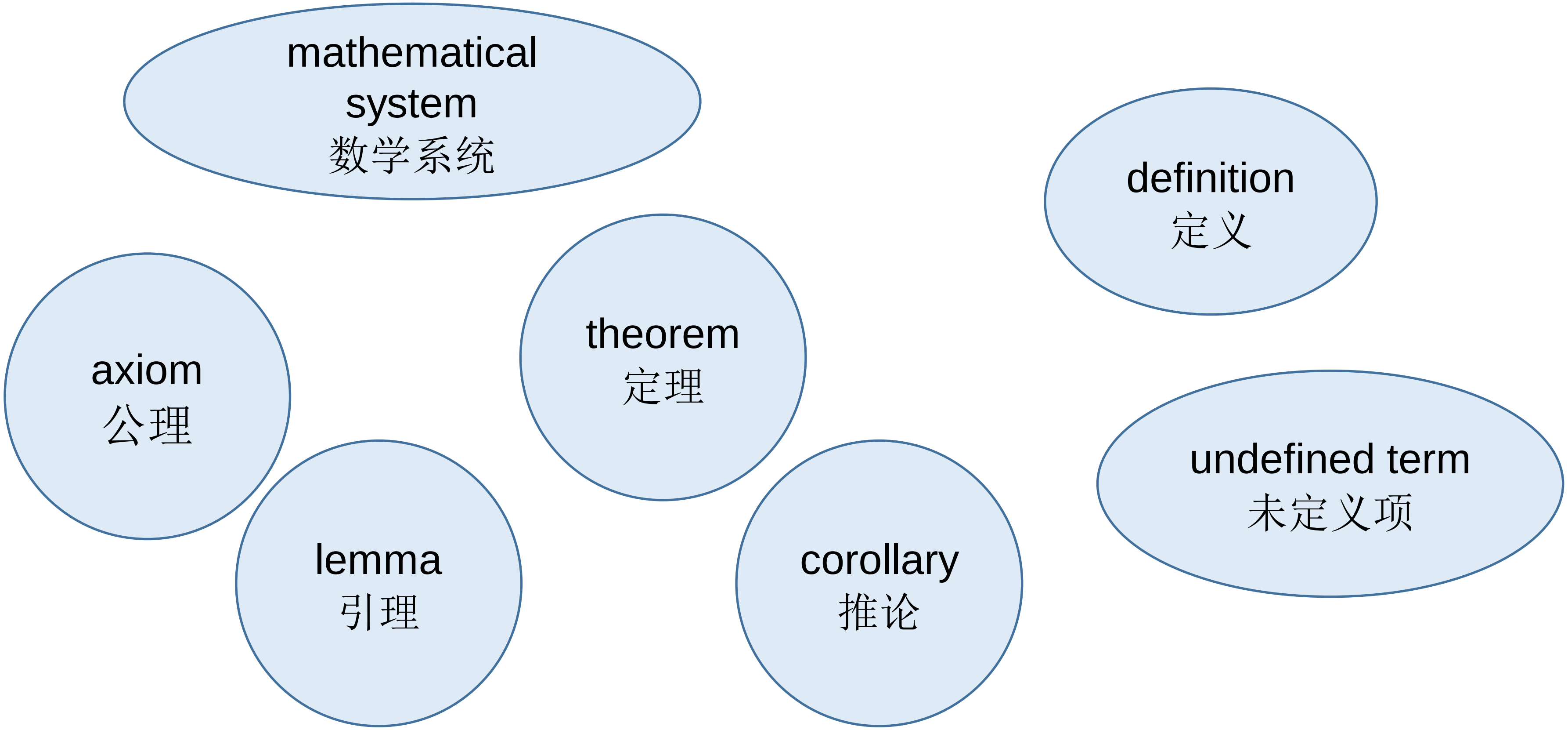
Chapter 2 Proofs 证明

Lu Han

hl@bupt.edu.cn

2.1 Mathematical Systems (数学系统), Direct Proofs (直接证明), and Counterexamples (反例)



mathematical system
数学系统

definition
定义

axiom
公理

theorem
定理

undefined term
未定义项

lemma
引理

corollary
推论

Mathematical Systems 数学系统

A mathematical system consists of

- axioms

Axioms are assumed to be true.

- definitions
- undefined terms.

Mathematical Systems 数学系统

A mathematical system consists of

- axioms
- definitions
- undefined terms.

Axioms are assumed to be true.

- **Sun Rises In The East.**
- **India is a Part of Asia.**
- **Probability lies between 0 to 1.**

- **Given two distinct points, there is exactly one line that contains them.**
- **Given a line and a point not on the line, there is exactly one line parallel to the line through the point.**

Mathematical Systems 数学系统

A mathematical system consists of

- axioms
- definitions
- undefined terms.

Definitions are used to create new concepts in terms of existing ones.

- The absolute value $|x|$ of a real number x is defined to be x is x is positive or 0 and -x otherwise.

Mathematical Systems 数学系统

A mathematical system consists of

- axioms
- definitions
- undefined terms.

Some terms are not explicitly defined but rather are implicitly defined by the axioms.

- **Given two distinct points, there is exactly one line that contains them.**

Theorem 定理

A theorem is a proposition that has been proved to be true.

If two sides of a triangle are equal, then the angles opposite them are equal.

Corollary 推论

A corollary is a theorem that follows easily from another theorem.

If a triangle is equilateral, then it is equiangular.

Lemma 引理

A lemma is a theorem that is usually not too interesting in its won right but is useful in proving another.

If n is a positive integer, then either $n -$ is a positive integer or n-1=0

Direct Proof 直接证明

Theorem are often of the **form**

For all $x_1, x_2,\ldots, x_n$, if $p(x_1, x_2, \ldots, x_n)$ then $q(x_1, x_2, \ldots, x_n)$.

A direct proof assumes that $p(x_1, x_2, \ldots, x_n)$ is true and then using $p(x_1, x_2, \ldots, x_n)$ as well as other axioms, definitions, previously derived theorems, and rules of inference, shows directly that $p(x_1, x_2, \ldots, x_n)$ is true.

Definition 2.1.7 An integer n is even if there exists an integer k such that $n=2k$. An integer n is odd if there exists an integer k such that $n=2k+1$.

Example 2.1.10 Given a direct proof of the following statement: For all integers m and n, if m is odd and n is even, then $m+n$ is odd.

m is odd and n is even (Hypotheses)
…
$m+n$ is odd (Conclusion)

Definition 2.1.7 An integer n is even if there exists an integer k such that $n=2k$. An integer n is odd if there exists an integer k such that $n=2k+1$.

Example 2.1.10 Given a direct proof of the following statement: For all integers m and n, if m is odd and n is even, then $m+n$ is odd.

Proof Let m and n be arbitrary integers, and suppose that m is odd and n is even. We prove that $m + n$ is odd. By definition, since m is odd, there exists an integer k_1 suchthat $m = 2k_1+1$. Also, by definition, since n is even, there exists an integer k_2 such that $n = 2k_2$. Now the sum is

$m + n = (2k_1+1) + (2k_2) = 2(k_1 + k_2) + 1.$

Thus, there exists an integer k (namely $k = k_1 + k_2$) such that $m + n = 2k+1$.

Therefore, $m + n$ is odd.

Example 2.1.11 Give a direct proof of the following statement.

For all sets X, Y, and Z, $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$.

? (Hypotheses)
...
? (Conclusion)

Example 2.1.11 Give a direct proof of the following statement.

For all sets X, Y, and Z, $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$.

X, Y, and Z are sets (Hypotheses)

...

$X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$ (Conclusion)

How to prove two sets are equal ?

Example 2.1.11 Give a direct proof of the following statement.

For all sets X, Y, and Z, $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$.

X, Y, and Z are sets (Hypotheses)
...
$X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$ (Conclusion)

How to prove two sets are equal ?

Two sets A and B are equal and we write $A = B$ if A and B have the same elements.
To put it another way, $A = B$ if the following two conditions hold:

- For every x, if $x \in A$, then $x \in B$,

and

- For every x, if $x \in B$, then $x \in A$.

Example 2.1.11 Give a direct proof of the following statement.

For all sets X, Y, and Z, $X \cap (Y - Z) = (X \bigcap Y) - (X \bigcap Z)$.

$X, Y,$ and Z are sets (Hypotheses)

…

$X \cap (Y - Z) = (X \bigcap Y) - (X \bigcap Z)$ (Conclusion)

For every x,
if $x \in X \cap (Y - Z)$, then $x \in (X \bigcap Y) - (X \bigcap Z)$,
and
if $x \in (X \bigcap Y) - (X \bigcap Z)$, then $x \in X \cap (Y - Z)$.

How to prove two sets are equal ?

Two sets A and B are equal and we write $A = B$ if A and B have the same elements.

To put it another way, $A = B$ if the following two conditions hold:

- For every x, if $x \in A$, then $x \in B$,

and

- For every x, if $x \in B$, then $x \in A$.

Example 2.1.11 Give a direct proof of the following statement.

For all sets X, Y, and Z, $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$.

The set $A - B = \{x \mid x \in A \text{ and } x \notin B\}$ is called the difference.

For every x,

if $x \in X \cap (Y - Z)$, then $x \in (X \cap Y) - (X \cap Z)$,

and

if $x \in (X \cap Y) - (X \cap Z)$, then $x \in X \cap (Y - Z)$.

Example 2.1.13 $X \cup (Y - X) = X \cup Y$ for all sets X and Y.

? (Hypotheses)

...

? (Conclusion)

Example 2.1.13 $X \cup (Y - X) = X \cup Y$ for all sets X and Y.

X and Y are sets (Hypotheses)

...

$X \cup (Y - X) = X \cup Y$ (Conclusion)

Example 2.1.13 $X \cup (Y - X) = X \cup Y$ for all sets X and Y.

X and Y are sets (Hypotheses)

...

$X \cup (Y - X) = X \cup Y$ (Conclusion)

$Y - X = Y \cap (U - X)$

Disproving a Universally Quantified Statement 证明全称量词语句为假

To disprove $\forall x\, P(x)$ we simply need to find one member x in the domain of discourse that makes $P(x)$ false.

Such that a value for x is called a **counterexample (反例)**.

Disproving a Universally Quantified Statement
证明全称量词语句为假

To disprove $\forall x\, P(x)$ we simply need to find one member x in the domain of discourse that makes $P(x)$ false.

Such that a value for x is called a **counterexample (反例)**.

Example 1.5.6 Determine whether the universally quantified statement $\forall x\ (x^2 - 1 > 0)$ is true or false. The domain of discourse is **R**.

Disproving a Universally Quantified Statement
证明全称量词语句为假

To disprove $\forall x\, P(x)$ we simply need to find one member x in the domain of discourse that makes $P(x)$ false.

Such that a value for x is called a **counterexample (反例)**.

Example 1.5.6 Determine whether the universally quantified statement $\forall x\ (x^2 - 1 > 0)$ is true or false. The domain of discourse is **R**.

Value 1 is a counterexample to the statement $\forall x\ (x^2 - 1 > 0)$.

Disproving a Universally Quantified Statement
证明全称量词语句为假

To disprove $\forall x\, P(x)$ we simply need to find one member x in the domain of discourse that makes $P(x)$ false.

Such that a value for x is called a **counterexample (反例)**.

Example 2.1.4 Determine whether the universally quantified statement $\forall n \in \boldsymbol{Z}^{+}\ (2^{n} + 1 \text{ is prime})$ is true or false. If false, give a counterexample.

Disproving a Universally Quantified Statement
证明全称量词语句为假

To disprove $\forall x\ P(x)$ we simply need to find one member x in the domain of discourse that makes $P(x)$ false.

Such that a value for x is called a **counterexample (反例)**.

Example 2.1.4 Determine whether the universally quantified statement $\forall n \in \boldsymbol{Z}^{+}\ (2^{n} + 1 \text{ is prime})$ is true or false. If false, give a counterexample.

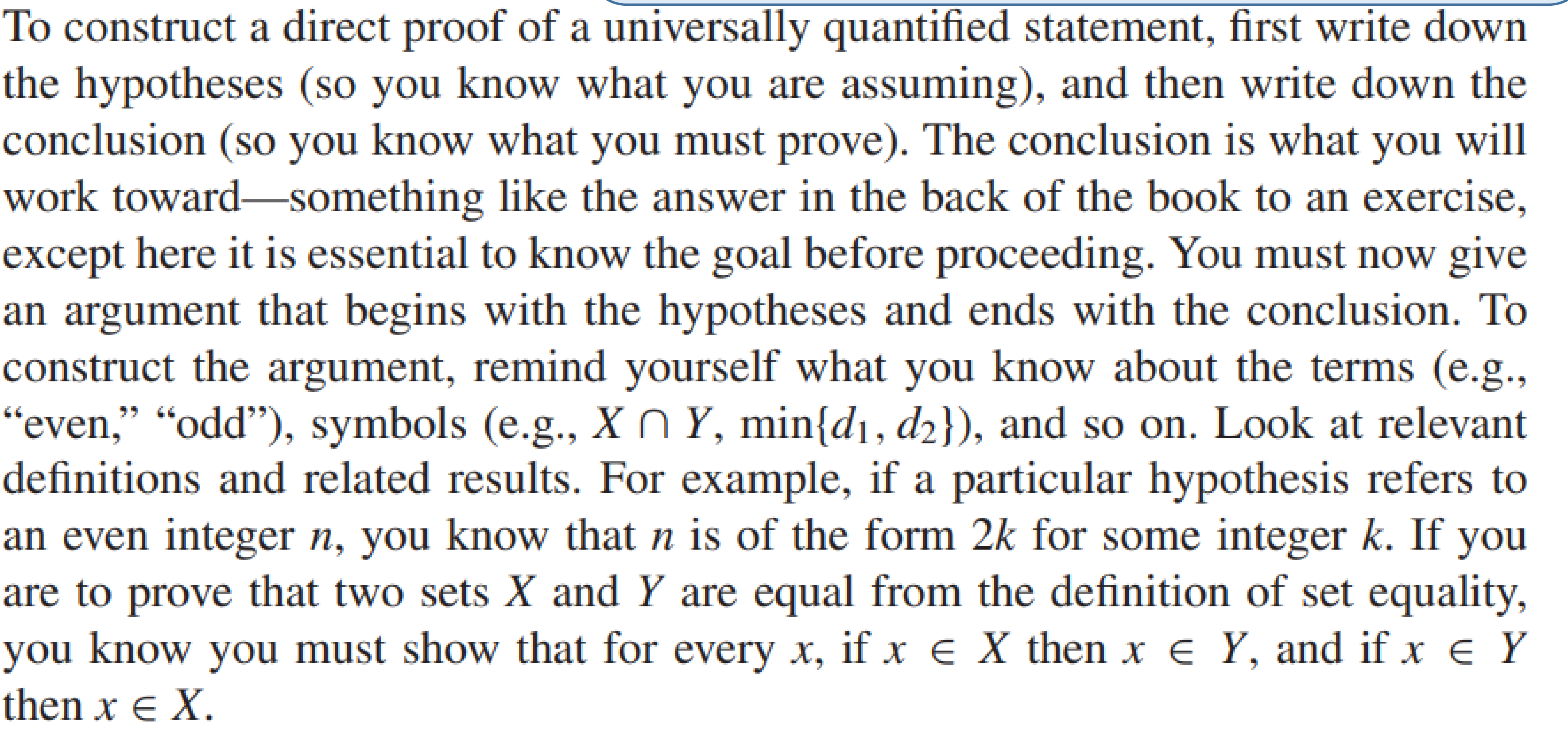
A counterexample is $n = 3$.

Disproving a Universally Quantified Statement
证明全称量词语句为假

Example 2.1.5 If statement $(A \cap B) \cup C = A \cap (B \cup C)$, for all sets $A, B, \text{and } C$ is true, prove it; otherwise, give a counterexample.

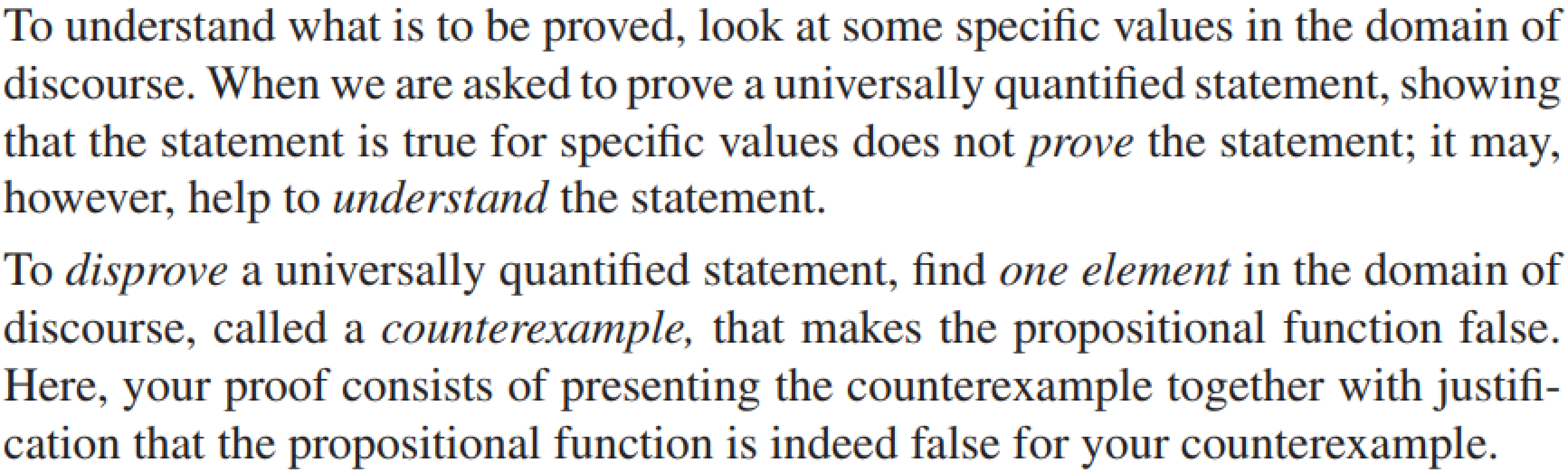
Problem-Solving Tips

Proof Let m and n be arbitrary integers, and suppose that m is odd and n is even. We prove that $m + n$ is odd. By definition, since m is odd, there exists an integer k_1 suchthat $m = 2k_1+1$. Also, by definition, since n is even, there exists an integer k_2 such that $n = 2k_2$. Now the sum is $m + n = (2k_1+1) + (2k_2) = 2(k_1 + k_2) + 1$.
Thus, there exists an integer k (namely $k = k_1 + k_2$) such that $m + n = 2k+1$. Therefore, $m + n$ is odd.



- To construct a direct proof of a universally quantified statement, first write down the hypotheses (so you know what you are assuming), and then write down the conclusion (so you know what you must prove). The conclusion is what you will work toward—something like the answer in the back of the book to an exercise, except here it is essential to know the goal before proceeding. You must now give an argument that begins with the hypotheses and ends with the conclusion. To construct the argument, remind yourself what you know about the terms (e.g., “even,” “odd”), symbols (e.g., $X \cap Y$, $\min\{d_1, d_2\}$), and so on. Look at relevant definitions and related results. For example, if a particular hypothesis refers to an even integer n, you know that n is of the form $2k$ for some integer k. If you are to prove that two sets X and Y are equal from the definition of set equality, you know you must show that for every x, if $x \in X$ then $x \in Y$, and if $x \in Y$ then $x \in X$.

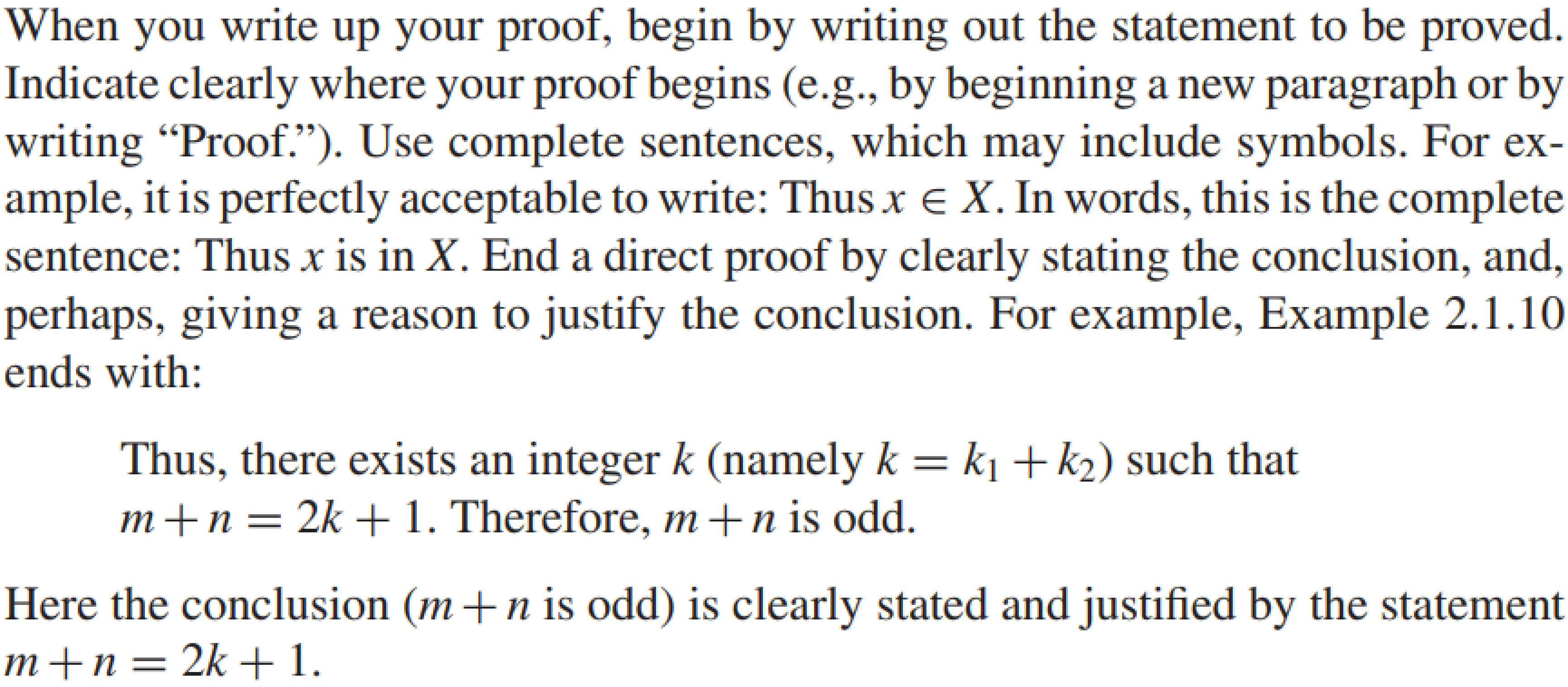
Problem-Solving Tips



- To understand what is to be proved, look at some specific values in the domain of discourse. When we are asked to prove a universally quantified statement, showing that the statement is true for specific values does not *prove* the statement; it may, however, help to *understand* the statement.
- To *disprove* a universally quantified statement, find *one element* in the domain of discourse, called a *counterexample,* that makes the propositional function false. Here, your proof consists of presenting the counterexample together with justification that the propositional function is indeed false for your counterexample.

Problem-Solving Tips

Proof Let m and n be arbitrary integers, and suppose that m is odd and n is even. We prove that $m + n$ is odd. By definition, since m is odd, there exists an integer k_1 suchthat $m = 2k_1+1$. Also, by definition, since n is even, there exists an integer k_2 such that $n = 2k_2$. Now the sum is $m + n = (2k_1+1) + (2k_2) = 2(k_1 + k_2) + 1$.
Thus, there exists an integer k (namely $k = k_1 + k_2$) such that $m + n = 2k+1$. Therefore, $m + n$ is odd.



- When you write up your proof, begin by writing out the statement to be proved. Indicate clearly where your proof begins (e.g., by beginning a new paragraph or by writing "Proof."). Use complete sentences, which may include symbols. For example, it is perfectly acceptable to write: Thus $x \in X$. In words, this is the complete sentence: Thus x is in X. End a direct proof by clearly stating the conclusion, and, perhaps, giving a reason to justify the conclusion. For example, Example 2.1.10 ends with:

  > Thus, there exists an integer k (namely $k = k_1 + k_2$) such that $m + n = 2k + 1$. Therefore, $m + n$ is odd.

  Here the conclusion ($m + n$ is odd) is clearly stated and justified by the statement $m + n = 2k + 1$.

Problem-Solving Tips

- Alert the reader where you are headed. For example, if you are going to prove that $X = Y$, write "We will prove that $X = Y$" before launching into this part of the proof.
- Justify your steps. For example, if you conclude that $x \in X$ or $x \in Y$ because it is known that $x \in X \cup Y$, write "Since $x \in X \cup Y$, $x \in X$ or $x \in Y$," or perhaps even "Since $x \in X \cup Y$, by the definition of union $x \in X$ or $x \in Y$" if, like Richard Nixon, you want to be perfectly clear.
- If you are asked to prove or disprove a universally quantified statement, you can begin by trying to prove it. If you succeed, you are finished—the statement is true and you proved it! If your proof breaks down, look carefully at the point where it fails. The given statement may be false and your failed proof may give insight into how to construct a counterexample (see Example 2.1.15). On the other hand, if you have trouble constructing a counterexample, check where your proposed examples fail. This insight may show why the statement is true and guide construction of a proof.

Exercise 1 Prove that if $X \subseteq Y$, then $X \cap Z \subseteq Y \cap Z$ for all sets X, Y and Z.

A is a subset of B (i.e., $A \subseteq B$) if for every x if $x \in A$, then $x \in B$.

Exercise 1 Prove that if $X \subseteq Y$, then $X \cap Z \subseteq Y \cap Z$ for all sets X, Y and Z.

Proof Let $x \in X \bigcap Z$. From the definition of"intersection," we conclude that Let $x \in X$ and $x \in Z$. Since $X \subseteq Y$ and $x \in X$ and $x \in Y$. Since $x \in Y$ and $x \in Z$, from the definition of"intersection,"we conclude that $x \in Y \bigcap Z$. Therefore $X \bigcap Z \subseteq Y \cap Z$.

A is a subset of B (i.e., $A \subseteq B$) if for every x if $x \in A$, then $x \in B$.

Exercise 2 Prove that if $X \cap Y = X \cap Z$ and $X \cup Y = X \cup Z$, then $Y = Z$ for all sets X, Y and Z.

2.2 More Methods of Proof 更多的证明方法

- **Proof by Contradiction 反证法**
- **Proof by Contrapositive 逆否证明法**
- **Proof by Cases 分情况证明法**
- **Proofs of Equivalence 等价证明法**
- **Existence Proofs 存在性证明法**

Proof by Contradiction 反证法

A **proof by contraction** establishes $p \rightarrow q$ by assuming that the hypothesis p is true and that the conclusion q is false and then, **using p and $\neg q$** as well as other axioms, definitions, previously derived theorems, and rules of inference, derives a contradiction.

Proof by Contradiction 反证法

A **proof by contraction** establishes p⍰q by assuming that the hypothesis p is true and that the conclusion q is false and then, **using p and $\neg q$** as well as other axioms, definitions, previously derived theorems, and rules of inference, derives a contradiction.

A proof by contradiction is sometimes called an **indirect proof** **（间接证明）**.

Proof by Contradiction 反证法

A **proof by contraction** establishes p□q by assuming that the hypothesis p is true and that the conclusion q is false and then, **using p and $\neg q$** as well as other axioms, definitions, previously derived theorems, and rules of inference, derives a contradiction.

The method of **proof by contradiction** of a theorem p□q consists of the following steps:

1. Assume p is true and q is false
2. Show that $\neg p$ is also true.
3. Then we have that $p \land \neg p$ is true.
4. But this is impossible, since the statement $p \land \neg p$ is always false. There is a contradiction!
5. So, q cannot be false and therefore it is true.

Proof by Contradiction 反证法

Example 2.2.1 Give a proof by contradiction of the following statement:

For every $n \in \mathbf{Z}$, if n^2 is even, then n is even.

Proof by Contradiction 反证法

Example 2.2.1 Give a proof by contradiction of the following statement:

For every $n \in \mathbf{Z}$, if n^2 is even, then n is even.

The method of **proof by contradiction** of a theorem p⍰q consists of the following steps:

1. Assume p is true and q is false
2. Show that $\neg p$ is also true.
3. Then we have that $p \wedge \neg p$ is true.
4. But this is impossible, since the statement $p \wedge \neg p$ is always false. There is a contradiction!
5. So, q cannot be false and therefore it is true.

Proof by Contradiction 反证法

Example 2.2.1 Give a proof by contradiction of the following statement:

For every $n \in \mathbf{Z}$, if n^2 is even, then n is even.

Proof We give a proof by contradiction. Thus we assume the hypothsis n^2 is even and that the conclustion is false n is odd. Since n is odd, there exists an integer k such $n = 2k + 1$. Now

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Thus n^2 is odd, which contradicts the hypothesis n^2 is even.
The proof by contradiction is complete. We have proved that For every $n \in \mathbf{Z}$, if n^2 is even, then n is even.

The method of **proof by contradiction** of a theorem p⍰q consists of the following steps:

1. Assume p is true and q is false
2. Show that $\neg p$ is also true.
3. Then we have that $p \wedge \neg p$ is true.
4. But this is impossible, since the statement $p \wedge \neg p$ is always false. There is a contradiction!
5. So, q cannot be false and therefore it is true.

Proof by Contradiction 反证法

Example 2.2.1 Give a proof by contradiction of the following statement:

For all real numbers x and y, if $x + y \geq 2$, then either $x \geq 1$ or $y \geq 1$.

The method of **proof by contradiction** of a theorem p⍰q consists of the following steps:

1. Assume p is true and q is false
2. Show that $\neg p$ is also true.
3. Then we have that $p \wedge \neg p$ is true.
4. But this is impossible, since the statement $p \wedge \neg p$ is always false. There is a contradiction!
5. So, q cannot be false and therefore it is true.

Proof by Contrapositive 逆否证明法

Suppose that we give a proof by contradiction of $p\square q$ in which, as in Examples 2.2.1and 2.2.2, we deduce $\neg p$. In effect, we have proved $\neg q \rightarrow \neg p$.

Recall that $p\square q$ and $\neg q \rightarrow \neg p$ are equivalent. This special case of proof by contradiction is called **proof by contrapositive**.

Example 2.2.4 Give a proof by contrapositive to prove that
for all $x \in \mathbf{R}$, if x^2 is irrational, then x is irrational.

Proof by Contrapositive 逆否证明法

Suppose that we give a proof by contradiction of p▯q in which, as in Examples 2.2.1and 2.2.2, we deduce $\neg p$. In effect, we have proved $\neg q \rightarrow \neg p$.

Recall that p▯q and $\neg q \rightarrow \neg p$ are equivalent. This special case of proof by contradiction is called **proof by contrapositive**.

Example 2.2.4 Give a proof by contrapositive to prove that
for all $x \in \mathbf{R}$, if x^2 is irrational, then x is irrational.

if x is not irrational, then x^2 is not irrational
⇔ if x is rational, then x^2 is rational

Proof by Contrapositive 逆否证明法

Suppose that we give a proof by contradiction of p□q in which, as in Examples 2.2.1and 2.2.2, we deduce $\neg p$. In effect, we have proved $\neg q \rightarrow \neg p$.

Recall that p□q and $\neg q \rightarrow \neg p$ are equivalent. This special case of proof by contradiction is called **proof by contrapositive**.

Example 2.2.4 Give a proof by contrapositive to prove that
for all $x \in \mathbf{R}$, if x^2 is irrational, then x is irrational.

Proof We begin by letting x be an arbitrary real number. We prove the contrapositive of the given statement, which is
if x is not irrational, then x^2 is not irrational
or, equivalently,
if x is rational, then x^2 is rational.
So suppose that x is rational. Then $x = p/q$ for some integers p and q.
Now $x^2 = p^2/q^2$.Since x^2 is the quotient of integers, x^2 is rational. The proof is complete.

Proof by Contrapositive 逆否证明法

Suppose that we give a proof by contradiction of p□q in which, as in Examples 2.2.1and 2.2.2, we deduce $\neg p$. In effect, we have proved $\neg q \rightarrow \neg p$.

Recall that p□q and $\neg q \rightarrow \neg p$ are equivalent. This special case of proof by contradiction is called **proof by contrapositive**.

Exercise1 Give a proof by contrapositive to prove that

If $3n + 2$ is odd, then n is odd.

Proof by Contrapositive 逆否证明法

Suppose that we give a proof by contradiction of $p \square q$ in which, as in Examples 2.2.1and 2.2.2, we deduce $\neg p$. In effect, we have proved $\neg q \rightarrow \neg p$.

Recall that $p \square q$ and $\neg q \rightarrow \neg p$ are equivalent. This special case of proof by contradiction is called **proof by contrapositive**.

Example 2.2.1 For every $n \in \mathbf{Z}$, if n^2 is even, then n is even.

Exercise2 For every $n \in \mathbf{Z}$, if n is even, then n^2 is even.

Proof by Contrapositive 逆否证明法

Exercise2 For every $n \in \mathbf{Z}$, if n is even, then n^2 is even.

Proof by Contrapositive 逆否证明法

Exercise2 For every $n \in \mathbf{Z}$, if n is even, then n^2 is even.

1. Suppose n^2 is not even.
2. So n^2 is odd.
3. $\exists k \ \ n^2 = 2k + 1$
4. $\exists k \ \ n^2 - 1 = 2k$
5. $\exists k \ \ (n - 1)(n + 1) = 2k$
6. $2 \mid (n - 1)(n + 1)$
7. $2 \mid (n - 1) \ \vee \ 2 \mid (n + 1)$ since 2 is prime
8. $\exists a \ \ n - 1 \ = 2a \ \vee \ \exists b \ \ n+1 \ = 2b$
9. $\exists a \ \ n = 2a + 1 \vee \ \exists b \ \ n \ = 2b - 1$
10. In both cases n is odd
11. So n is not even

Proof by Cases 分情况证明法

Proof by cases is used when the original hypothesis naturally divides itself into various cases.

Proof by Cases 分情况证明法

Proof by cases is used when the original hypothesis naturally divides itself into various cases.

Suppose that the task is to prove $p \rightarrow q$ and that p is equivalent to $p_1 \vee p_2 \vee \ldots p_n$ (p_1, ..., p_n are the cases).
Instead of proving

$$(p_1 \vee p_2 \vee \ldots p_n) \rightarrow q,$$

we prove

Proof by Cases 分情况证明法

Proof by cases is used when the original hypothesis naturally divides itself into various cases.

Suppose that the task is to prove $p \rightarrow q$ and that p is equivalent to $p_1 \vee p_2 \vee \ldots p_n$ (p_1, ..., p_n are the cases).
Instead of proving

$$(p_1 \vee p_2 \vee \ldots p_n) \rightarrow q,$$

we prove

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q).$$

Proof by Cases 分情况证明法

Proof by cases is used when the original hypothesis naturally divides itself into various cases.

Suppose that the task is to prove $p \rightarrow q$ and that p is equivalent to $p_1 \vee p_2 \vee \ldots p_n$ (p_1, ..., p_n are the cases).
Instead of proving

$$(p_1 \vee p_2 \vee \ldots p_n) \rightarrow q,$$

we prove

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q).$$

Sometimes the number of cases to prove is finite and not too large, so we can checkthem all one by one. We call this type of proof **exhaustive proof** （穷举证明）.

Proof by Cases 分情况证明法

Example 2.2.6 Prove that $2m^2 + 3n^2 = 40$ has no solution in positive integers, that is, that $2m^2 + 3n^2 = 40$ is false for all positive integers m and n.

Proof by Cases 分情况证明法

Example 2.2.6 Prove that $2m^2 + 3n^2 = 40$ has no solution in positive integers, that is, that $2m^2 + 3n^2 = 40$ is false for all positive integers m and n.

Proof If $2m^2 + 3n^2 = 40$, we must have $2m^2 \leq 40$. Thus $m^2 \leq 20$ and $m \leq 4$. Similarly, we must have $3n^2 \leq 40$. Thus $n^2 \leq 40/3$ and $n \leq 3$. Therefore it suffices to chech the cases $m = 1, 2, 3, 4$ and $n = 1, 2, 3$.

The entries in the table give the value of $2m^2 + 3n^2$ for the indicated values of m and n.

			m		
		1	2	3	4
	1	5	11	21	35
n	2	14	20	30	44
	3	29	35	45	59

Since $2m^2 + 3n^2 \neq 40$ for $m = 1, 2, 3, 4$ and $n = 1, 2, 3$, and $2m^2 + 3n^2 > 40$ for $m > 4$ or $n > 3$, we conclude that $2m^2 + 3n^2 = 40$ has no solution in positive integers.

Proof by Cases 分情况证明法

Example 2.2.7 We prove that for every real number x, $x \le |x|$.

Proof of Equivalence 等价证明法

Some theorems are of the form p if and only if q. Such theorems are proved by using the equivalence

$$p \leftrightarrow q \equiv (p \longrightarrow q) \land (q \longrightarrow p)$$

that is, to prove “p if and only if q”, prove “if p then q” and “if q then p”.

Proof of Equivalence 等价证明法

Some theorems are of the form p if and only if q. Such theorems are proved by using the equivalence

$$p \leftrightarrow q \equiv (p \longrightarrow q) \wedge (q \longrightarrow p)$$

that is, to prove “p if and only if q”, prove “if p then q” and “if q then p”.

Example 2.2.9 Prove that for every integer n, n is odd if and only if $n - 1$ is even.

Proof of Equivalence 等价证明法

Some theorems are of the form p if and only if q. Such theorems are proved by using the equivalence

$$p \leftrightarrow q \equiv (p \longrightarrow q) \land (q \longrightarrow p)$$

that is, to prove “p if and only if q”, prove “if p then q” and “if q then p”.

Example 2.2.9 Prove that for every integer n, n is odd if and only if $n - 1$ is even.

Proof If n is odd, then $n = 2\mathrm{k} + 1$ for some integer k.
Now $n - 1 = (2k + 1) - 1 = 2k$. Therefore, $n - 1$ is even.
If $n - 1$ is even, then $n - 1 = 2k$ for some integer k.
Now $n = 2k + 1$. Therefore, n is odd. The proof is complete.

Proof of Equivalence 等价证明法

Some theorems are of the form p if and only if q. Such theorems are proved by using the equivalence

$$p \leftrightarrow q \equiv (p \longrightarrow q) \land (q \longrightarrow p)$$

that is, to prove “p if and only if q”, prove “if p then q” and “if q then p”.

To prove that $p_1, p_2, \ldots, p_n$ are equivalent, the usual method is to prove

$$(p_1 \longrightarrow p_2) \land (p_2 \longrightarrow p_3) \land \ldots \land (p_{n-1} \longrightarrow p_n) \land (p_n \longrightarrow p_1).$$

Proof of Equivalence 等价证明法

Example 2.2.11

Let A, B, and C be sets. Prove that the following are equivalent:

(a) $A \subseteq B$

(b) $A \cap B = A$

(c) $A \cup B = B$.

Existence Proofs 存在性证明法

A proof of

$$\exists x\ \mathrm{P}(x)$$

is called an **existence proof**. One way to prove it is to exhibit one member a in the domain of discourse that makes $\mathrm{P}(a)$ true.

Example 2.2.12 Let a and b be real numbers with $a < b$. Prove that there exists a real number x satisfying $a < x < b$.

Existence Proofs 存在性证明法

A proof of

$$\exists x \ \mathrm{P}(x)$$

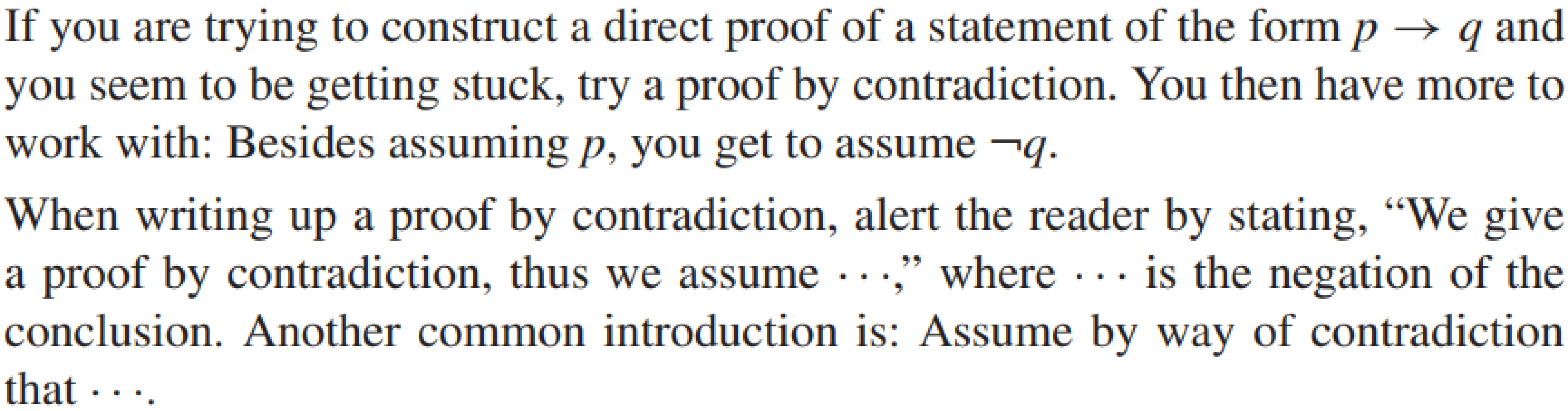
is called an **existence proof**. One way to prove it is to exhibit one member a in the domain of discourse that makes $\mathrm{P}(a)$ true.

Example 2.2.14 Let

$$A = \frac{s_1 + s_2 + \ldots + s_n}{n}$$

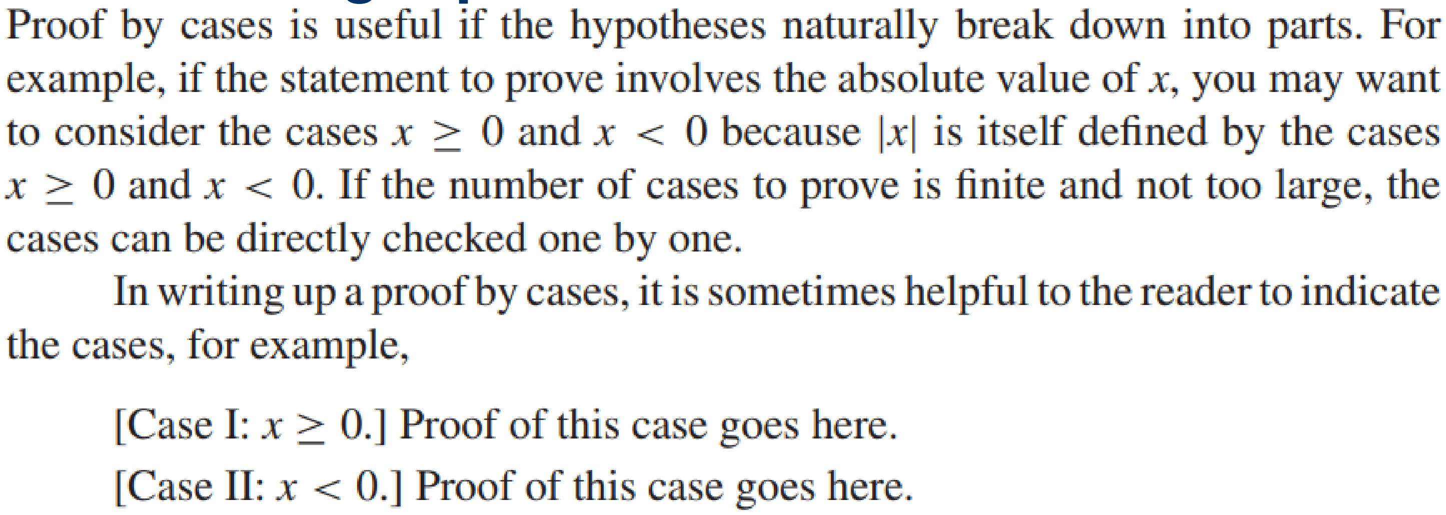
be the average of the real numbers $s_1, s_2, \ldots, s_n$. Prove that there exists i such that $s_i \geq A$.

Problem-Solving Tips



- If you are trying to construct a direct proof of a statement of the form $p \to q$ and you seem to be getting stuck, try a proof by contradiction. You then have more to work with: Besides assuming p, you get to assume $\neg q$.
- When writing up a proof by contradiction, alert the reader by stating, "We give a proof by contradiction, thus we assume $\cdots$," where $\cdots$ is the negation of the conclusion. Another common introduction is: Assume by way of contradiction that $\cdots$.

Problem-Solving Tips

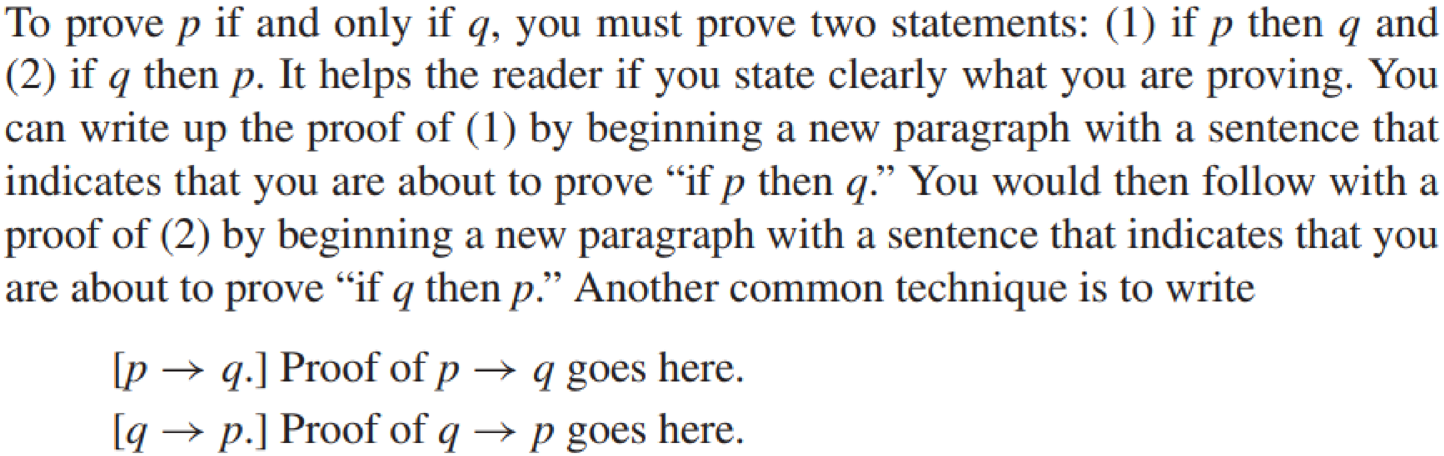
- 

  Proof by cases is useful if the hypotheses naturally break down into parts. For example, if the statement to prove involves the absolute value of x, you may want to consider the cases $x \geq 0$ and $x < 0$ because $|x|$ is itself defined by the cases $x \geq 0$ and $x < 0$. If the number of cases to prove is finite and not too large, the cases can be directly checked one by one.

  In writing up a proof by cases, it is sometimes helpful to the reader to indicate the cases, for example,

  [Case I: $x \geq 0$.] Proof of this case goes here.

  [Case II: $x < 0$.] Proof of this case goes here.

- 

  To prove p if and only if q, you must prove two statements: (1) if p then q and (2) if q then p. It helps the reader if you state clearly what you are proving. You can write up the proof of (1) by beginning a new paragraph with a sentence that indicates that you are about to prove "if p then q." You would then follow with a proof of (2) by beginning a new paragraph with a sentence that indicates that you are about to prove "if q then p." Another common technique is to write

  [$p \to q$.] Proof of $p \to q$ goes here.

  [$q \to p$.] Proof of $q \to p$ goes here.

Problem-Solving Tips

- To prove that several statements, say $p_1, \ldots, p_n$, are equivalent, prove $p_1 \to p_2$, $p_2 \to p_3, \ldots, p_{n-1} \to p_n, p_n \to p_1$. The statements can be ordered in any way and the proofs may be easier to construct for one ordering than another. For example, you could swap p_2 and p_3 and prove $p_1 \to p_3, p_3 \to p_2, p_2 \to p_4, p_4 \to p_5, \ldots, p_{n-1} \to p_n, p_n \to p_1$. You should indicate clearly what you are about to prove. One common form is

  [$p_1 \to p_2$.] Proof of $p_1 \to p_2$ goes here.

  [$p_2 \to p_3$.] Proof of $p_2 \to p_3$ goes here.

  And so forth.

- If the statement is existentially quantified (i.e., there exists $x \ldots$), the proof, called an existence proof, consists of showing that there exists at least one x in the domain of discourse that makes the statement true. One type of existence proof exhibits a value of x that makes the statement true (and proves that the statement is indeed true for the specific x). Another type of existence proof indirectly proves (e.g., using proof by contradiction) that a value of x exists that makes the statement true without specifying any particular value of x for which the statement is true.

Exercise

1. Define the *sign of the real number x*, sgn(x), as

$$\operatorname{sgn}(x) = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0. \end{cases}$$

Use proof by cases to prove that $|x| = \operatorname{sgn}(x)x$ for every real number x.

2. Prove that the following are equivalent for the integer n:

(a) n is odd. (b) There exists $k \in \mathbf{Z}$ such that $n = 2k - 1$.
(c) $n^2 + 1$ is even.

2.3 Resolution Proofs 消解证明 / 归结证明

Due to J. A. Robinson (1965)

If $p \lor q$ and $\neg p \lor r$ are both true, then $q \lor r$ is true.

2.3 Resolution Proofs 消解证明 / 归结证明

Due to J. A. Robinson (1965)

If $p \vee q$ and $\neg p \vee r$ are both true, then $q \vee r$ is true.

Example 2.3.4 Prove the following using resolution：

$$\begin{array}{ll} 1, & a \vee b \\ 2, & \neg a \vee c \\ 3, & \neg c \vee d \\ \hline \therefore & b \vee d \end{array}$$

2.3 Resolution Proofs 消解证明 / 归结证明

Due to J. A. Robinson (1965)

If $p \vee q$ and $\neg p \vee r$ are both true, then $q \vee r$ is true.

Special Case of Rule

If $p \vee q$ and $\neg p$ are both true, then q is true.
If $\neg p \vee q$ and p are both true, then q is true.

2.3 Resolution Proofs 消解证明 / 归结证明

Due to J. A. Robinson (1965)

If $p \vee q$ and $\neg p \vee r$ are both true, then $q \vee r$ is true.

Example 2.3.5 Prove the following using resolution：

$$\begin{array}{ll} 1, & a \\ 2, & \neg a \vee c \\ 3, & \neg c \vee d \\ \hline \therefore & d \end{array}$$

2.4 Mathematical Induction 数学归纳法

Example Let S_n denote the sum of the first n positive integers:

$$S_n = 1 + 2 + \ldots + n.$$

Someone claims that $S_n = \frac{n(n+1)}{2}$.

The first equation is true.

For all n, if equation n is true, then equation $n + 1$ is also true.

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.

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 $n \geq 1$.

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

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 $n \geq 1$.

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

Basis Step ($n = 1$)

$1! = 1 \geq 1 = 2^{n-1}$

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 $n \geq 1$.

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

Basis Step ($n = 1$)

$1! = 1 \geq 1 = 2^{n-1}$

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

Example Prove $\forall n \geq 1\ S(n)$ where

$S(n)$ = “The sum of the first n positive odd numbers is the n^{th} perfect square.”

Principle of Mathematical Induction 数学归纳法

Example Prove $\forall n \geq 1\ S(n)$ where

$S(n)$ = "The sum of the first n positive odd numbers is the n^{th} perfect square."

$$S(n): \sum_{i=1}^{n}(2i-1) = n^2$$

Principle of Mathematical Induction 数学归纳法

Example Prove $\forall n \geq 1\ S(n)$ where

$S(n)$ = "The sum of the first n positive odd numbers is the n^{th} perfect square."

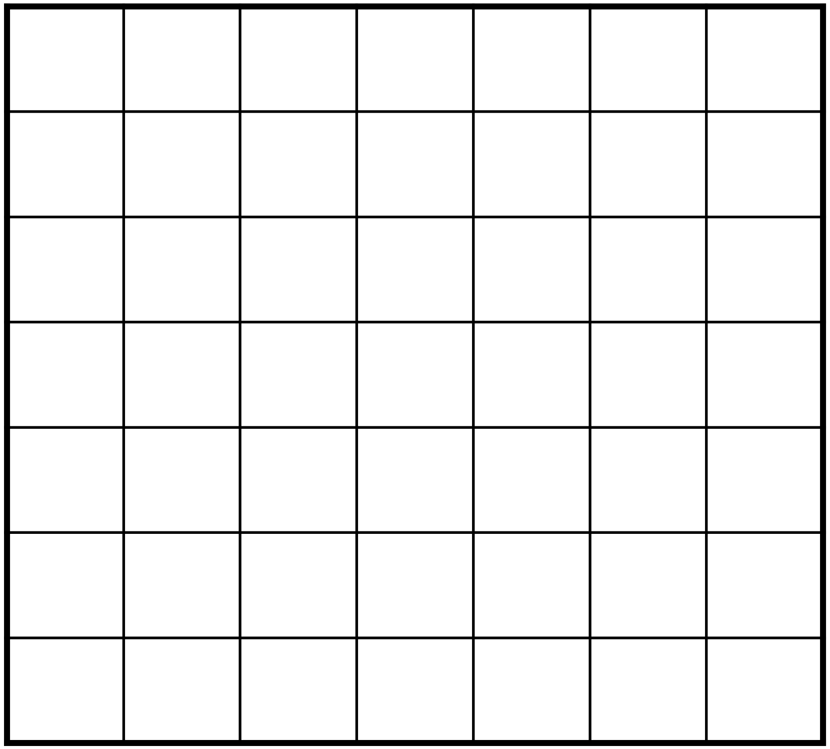
$$S(n): \sum_{i=1}^{n}(2i-1) = n^2$$

Geometric interpretation.
To get next square, need
to add next odd number:

Principle of Mathematical Induction 数学归纳法

Example Prove $\forall n \geq 1\ S(n)$ where
$S(n)$ = “The sum of the first n positive odd numbers is the n^{th} perfect square.”

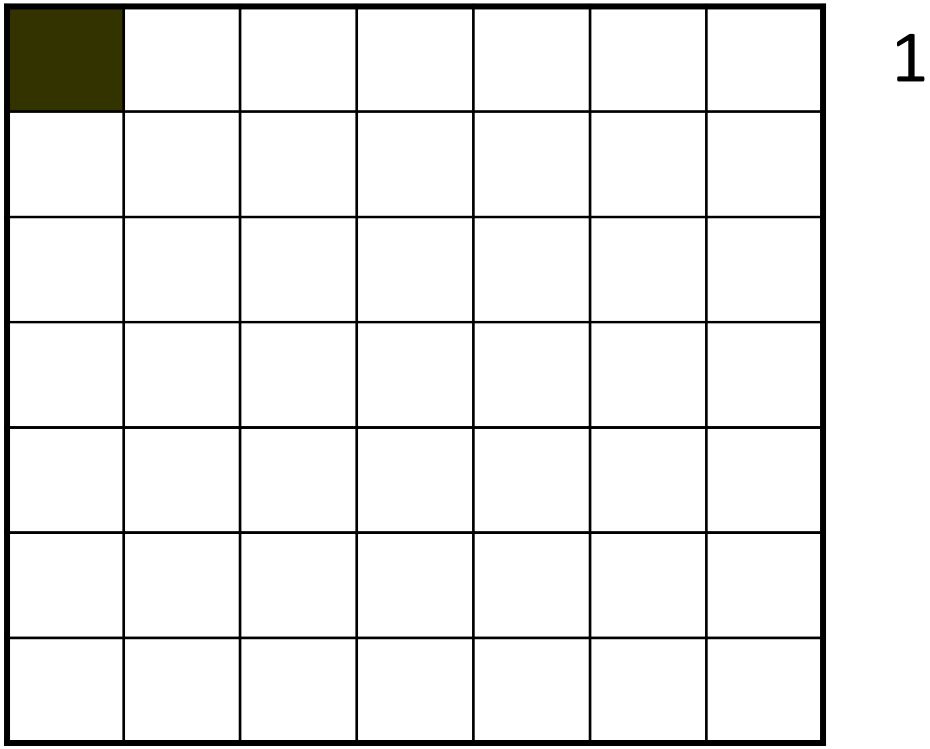
Geometric interpretation.
To get next square, need
to add next odd number:



Principle of Mathematical Induction 数学归纳法

Example Prove $\forall n \geq 1 \; S(n)$ where
$S(n)$ = "The sum of the first n positive odd numbers is the n^{th} perfect square."

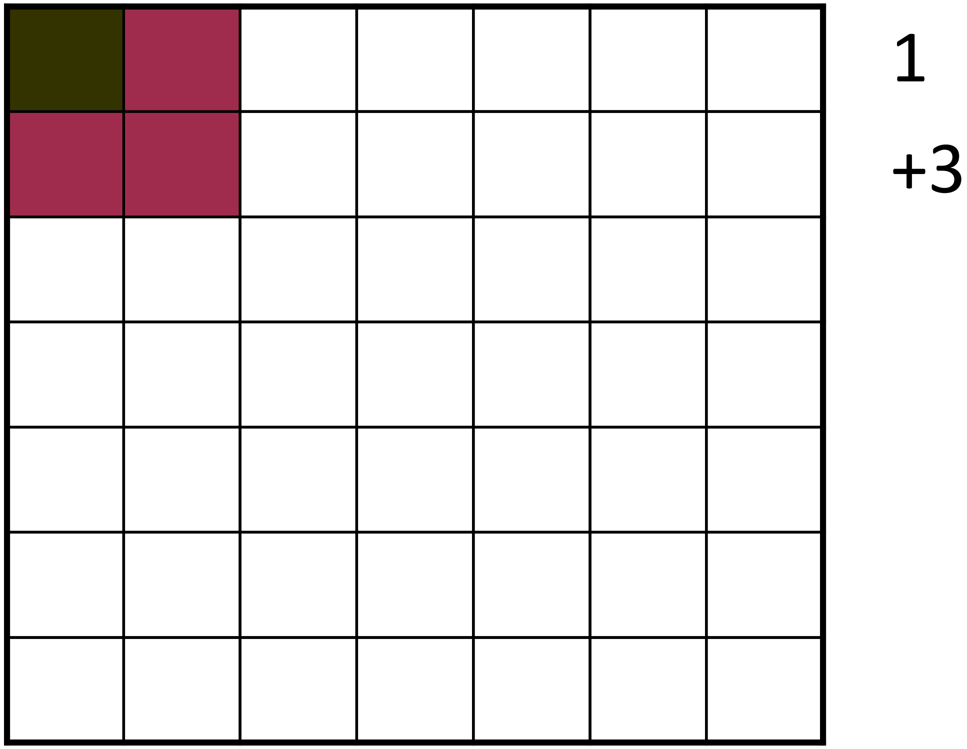
Geometric interpretation. To get next square, need to add next odd number:



Principle of Mathematical Induction 数学归纳法

Example Prove $\forall n \geq 1\ S(n)$ where
$S(n)$ = “The sum of the first n positive odd numbers is the n^{th} perfect square.”

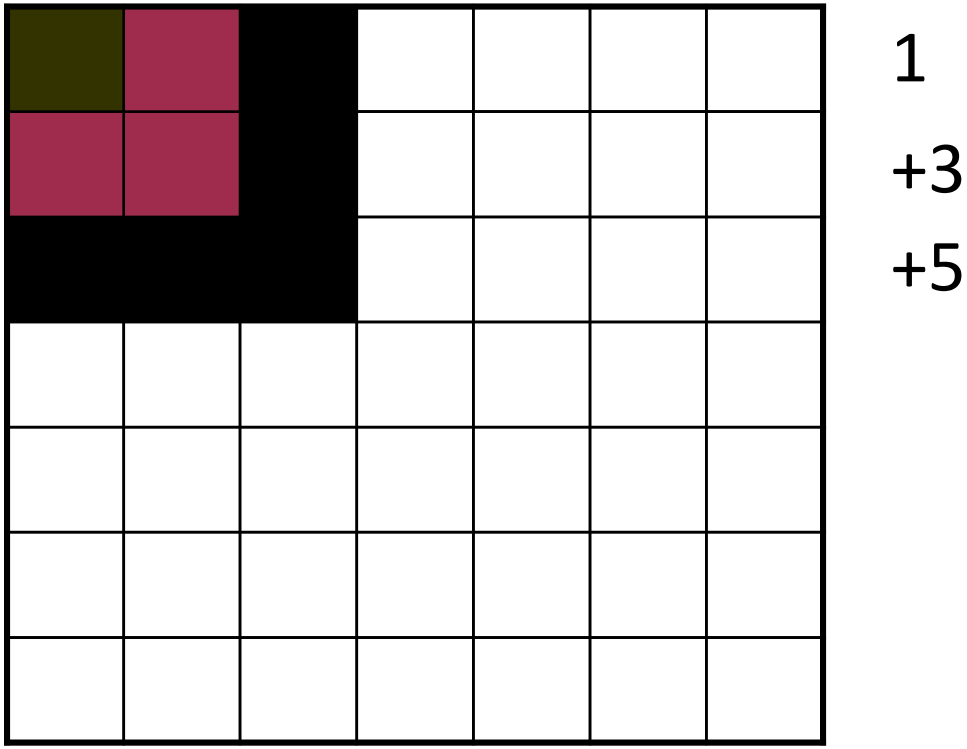
Geometric interpretation.
To get next square, need
to add next odd number:



Principle of Mathematical Induction 数学归纳法

Example Prove $\forall n \geq 1\ S(n)$ where
$S(n)$ = “The sum of the first n positive odd numbers is the n^{th} perfect square.”

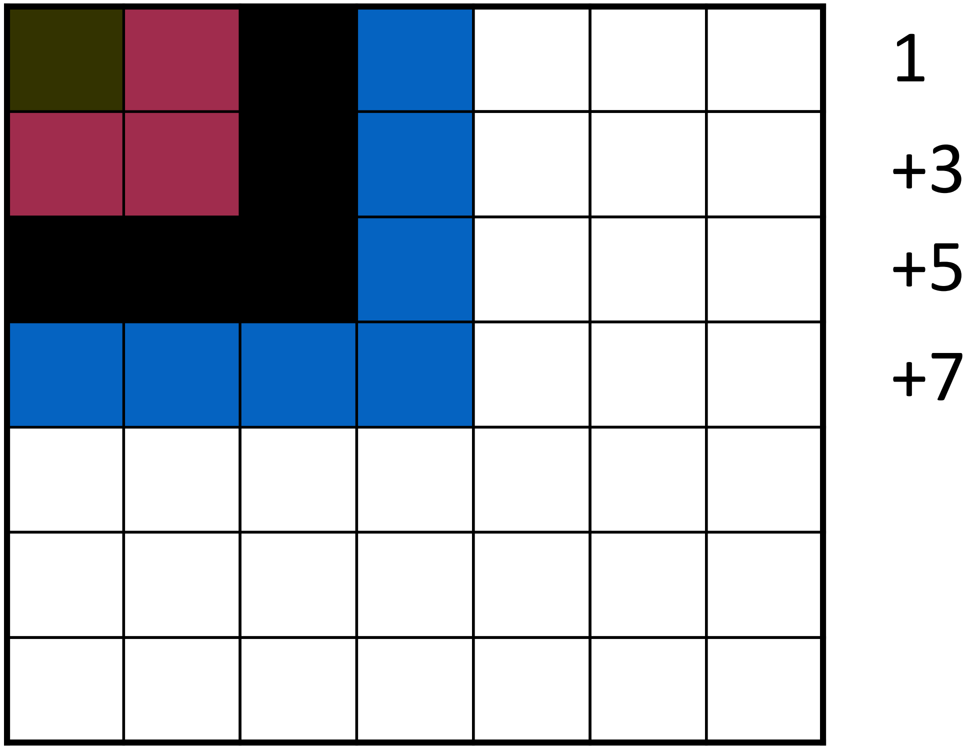
Geometric interpretation.
To get next square, need
to add next odd number:



Principle of Mathematical Induction 数学归纳法

Example Prove $\forall n \geq 1\ S(n)$ where
$S(n)$ = “The sum of the first n positive odd numbers is the n^{th} perfect square.”

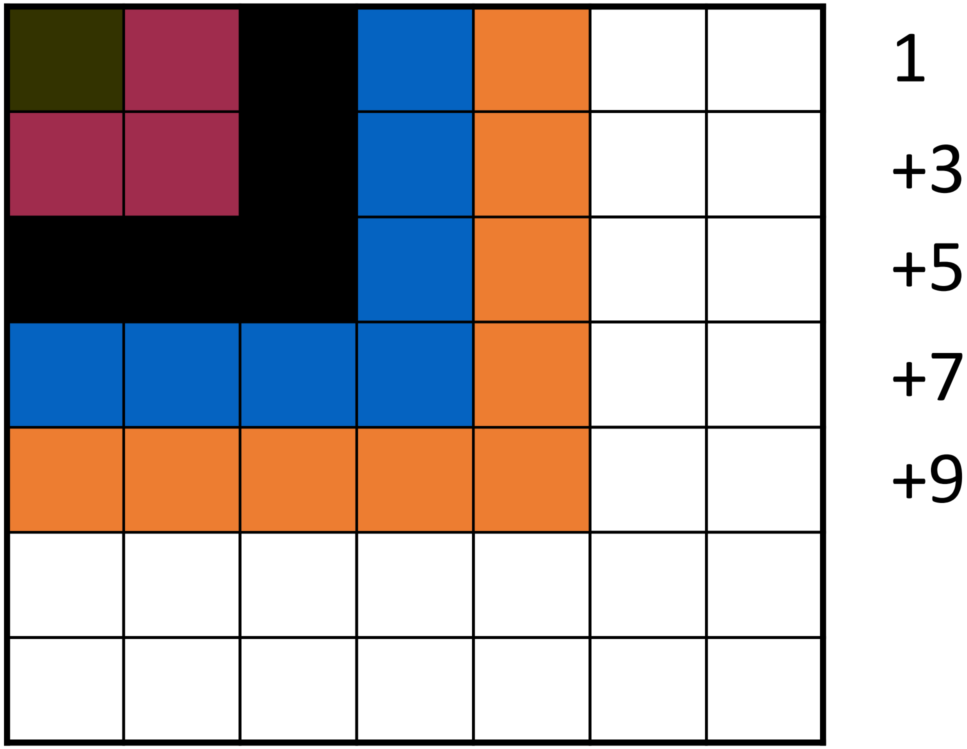
Geometric interpretation. To get next square, need to add next odd number:



Principle of Mathematical Induction 数学归纳法

Example Prove $\forall n \geq 1\ S(n)$ where
$S(n)$ = “The sum of the first n positive odd numbers is the n^{th} perfect square.”

Geometric interpretation.
To get next square, need
to add next odd number:



1

+3

+5

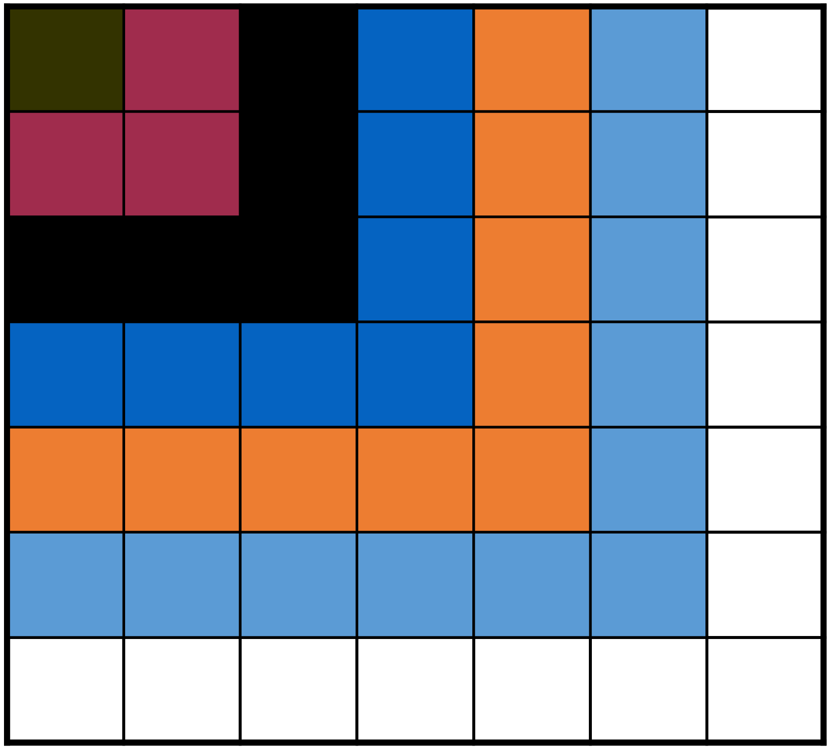
+7

+9

Principle of Mathematical Induction 数学归纳法

Example Prove $\forall n \geq 1\ S(n)$ where
$S(n)$ = “The sum of the first n positive odd numbers is the n^{th} perfect square.”

Geometric interpretation. To get next square, need to add next odd number:



1

+3

+5

+7

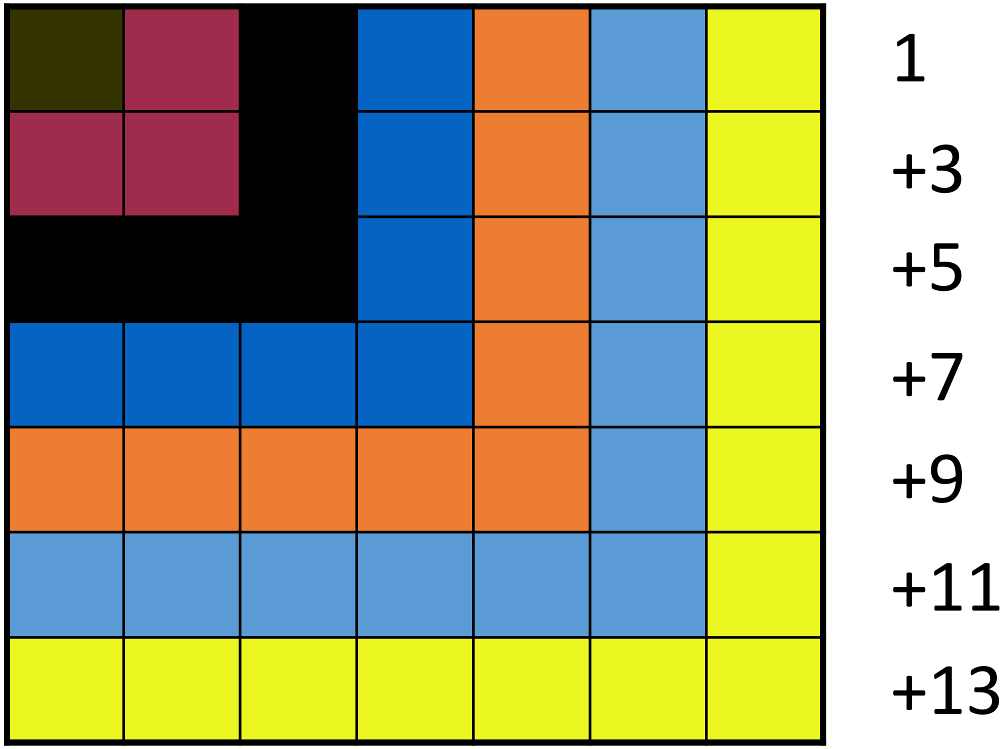
+9

+11

Principle of Mathematical Induction 数学归纳法

Example Prove $\forall n \geq 1\ S(n)$ where
$S(n)$ = “The sum of the first n positive odd numbers is the n^{th} perfect square.”

Geometric interpretation. To get next square, need to add next odd number:



Principle of Mathematical Induction 数学归纳法

Example Prove $\forall n \geq 1\ S(n)$ where
$S(n)$ = “The sum of the first n positive odd numbers is the n^{th} perfect square.”

$$S(n): \sum_{i=1}^{n}(2i-1) = n^2$$

Basis Step ($n = 1$)

Inductive Step

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.

All horses are the same color.

$\boldsymbol{S(n)}$: **any set of $\boldsymbol{n}$ horses have the same color.**

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.

All horses are the same color.

$\boldsymbol{S(n)}$**: any set of** $\boldsymbol{n}$ **horses have the same color.**

Basis Step ($n = 1$)

Inductive Step

Assume any n horses have the same color.
Prove that any $n+1$ horses have the same color.

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.

All horses are the same color.

$\boldsymbol{S(n)}$: any set of $\boldsymbol{n}$ horses have the same color.

Basis Step ($n = 1$)

Inductive Step

Assume any n horses have the same color.
Prove that any $n+1$ horses have the same color.

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.

All horses are the same color.

$\boldsymbol{S(n)}$: **any set of $\boldsymbol{n}$ horses have the same color.**

Is this proof correct?

Basis Step ($n = 1$)

Inductive Step

Assume any n horses have the same color.
Prove that any $n+1$ horses have the same color.

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.

All horses are the same color.

$S(n)$: any set of n horses have the same color.

Basis Step ($n = 1$)

Inductive Step

Assume any n horses have the same color.
Prove that any $n + 1$ horses have the same color.

Is this proof correct?

Proof that $S(n) \rightarrow S(n+1)$ is false if n = 1, because the two horse groups do not overlap.

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.

All horses are the same color.

$S(n)$: any set of n horses have the same color.

But proof works for all $n \neq 1$.

Basis Step ($n = 1$)

Inductive Step

Assume any n horses have the same color.
Prove that any $n + 1$ horses have the same color.

Proof that $S(n) \rightarrow S(n+1)$ is false if $n = 1$, because the two horse groups do not overlap.

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.

→ $S(1), S(2), \ldots, S(n)$

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.

→ $S(1), S(2), \ldots, S(n)$

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.

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

Example 2.4.4 Geometric Sum 几何级数求和

Use induction to show that if $r \neq 1$,

$$a + ar^1 + ar^2 + \ldots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1}$$

for all $n \geq 0$.

Principle of Mathematical Induction 数学归纳法

Example 2.4.4 Geometric Sum 几何级数求和

Use induction to show that if $r \neq 1$,

$$a + ar^1 + ar^2 + \ldots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1}$$

for all $n \geq 0$.

Basis Step ($n = 0$)

Inductive Step

Principle of Mathematical Induction 数学归纳法

Example 2.4.5 Use induction to show that if $5^n - 1$ is divisible by 4 for all $n \geq 1$.

Basis Step ($n = 1$)

Inductive Step

Principle of Mathematical Induction 数学归纳法

Example 2.4.5 Use induction to show that if $5^n - 1$ is divisible by 4 for all $n \geq 1$.

Basis Step ($n = 1$)

If $n = 1, 5^n - 1 = 5^1 - 1 = 4$, which is divisible by 4.

Inductive Step

Fact: If p and q are each divisible by k, then $p + q$ is also divisible by k. (Exercise 74)

Principle of Mathematical Induction 数学归纳法

Example 2.4.5 Use induction to show that if $5^n - 1$ is divisible by 4 for all $n \geq 1$.

Basis Step ($n = 1$)

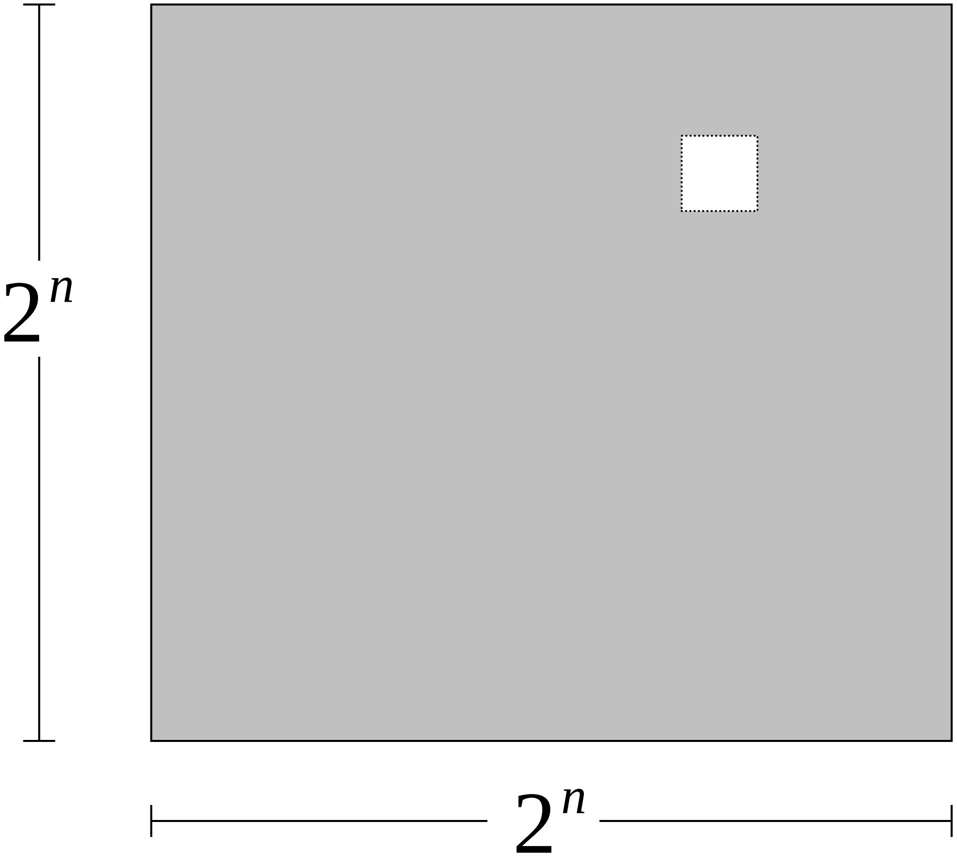
If $n = 1, 5^n - 1 = 5^1 - 1 = 4$, which is divisible by 4.

Inductive Step

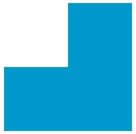
Fact: If p and q are each divisible by k, then $p + q$ is also divisible by k. (Exercise 74)

Principle of Mathematical Induction 数学归纳法

Example 2.4.7 A Tiling Problem



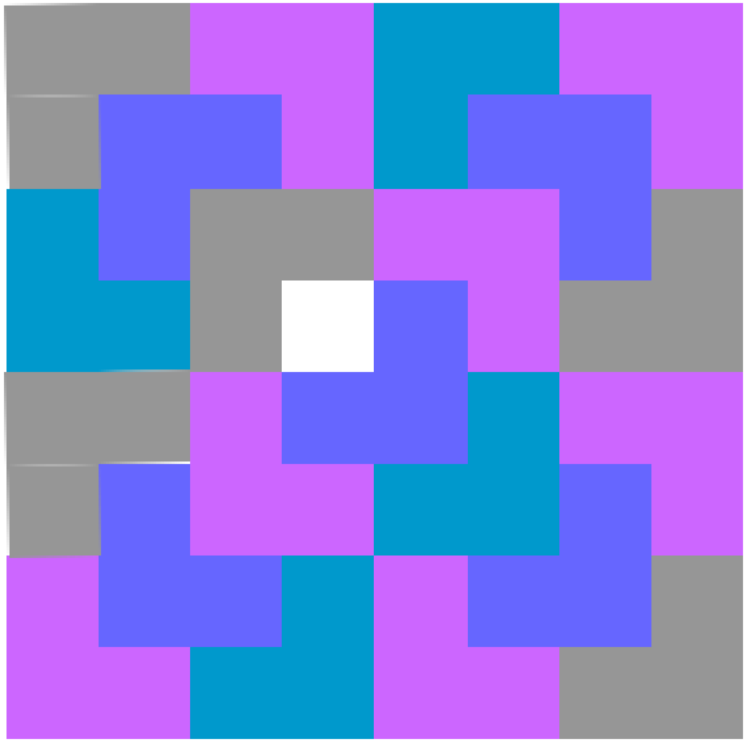
There are only L-shaped tiles covering three squares:



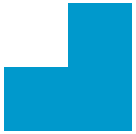
Goal: tile the board with one square missing.

Principle of Mathematical Induction 数学归纳法

Example 2.4.7 A Tiling Problem



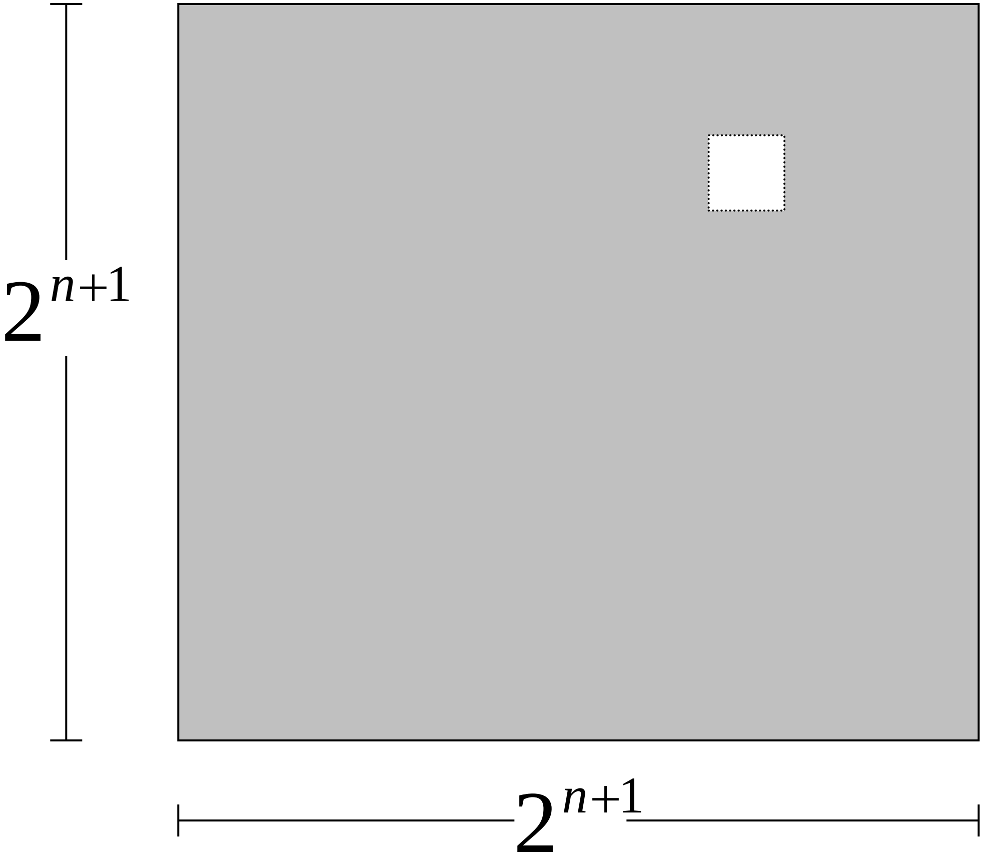
There are only L-shaped tiles covering three squares:



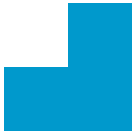
Goal: tile the board with one square missing.

Principle of Mathematical Induction 数学归纳法

Example 2.4.7 A Tiling Problem



There are only L-shaped tiles covering three squares:

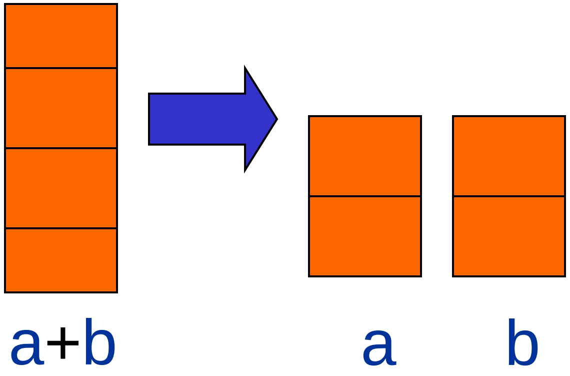


Goal: tile the board with one square missing.

Unstacking Game

- Start: a stack of boxes
- Move: split any stack into two stacks of sizes *a*,*b*>0
- Scoring: *ab* points
- Keep moving: until stuck
- Overall score: sum of move scores

What is the best way to play this game?

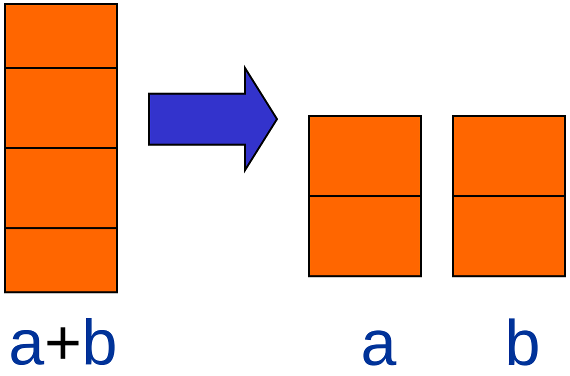


Unstacking Game

Start: a stack of boxes
Move: split any stack into two stacks of sizes *a*,*b*>0
Scoring: *ab* points
Keep moving: until stuck
Overall score: sum of move scores

Suppose there are n boxes.

What is the score if we just take the box one at a time?



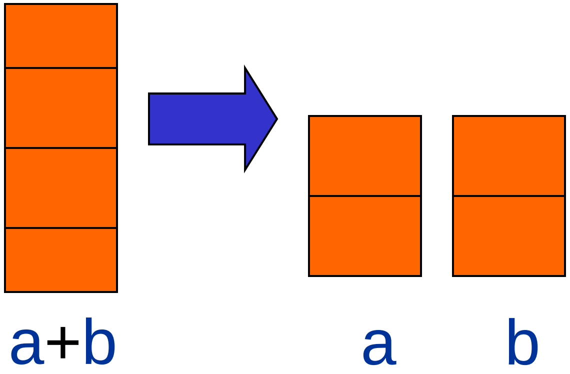
Unstacking Game

Start: a stack of boxes
Move: split any stack into two stacks of sizes *a*,*b*>0
Scoring: *ab* points
Keep moving: until stuck
Overall score: sum of move scores

Suppose there are n boxes.

What is the score if we just take the box one at a time?

$$\sum_{i=1}^{n-1}(n-i) = \frac{n(n-1)}{2}$$



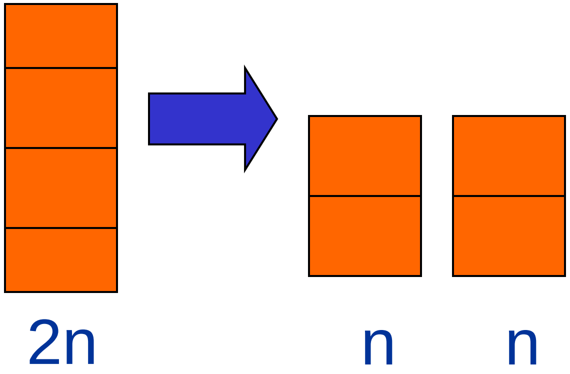
Unstacking Game

Start: a stack of boxes
Move: split any stack into two stacks of sizes *a*,*b*>0
Scoring: *ab* points
Keep moving: until stuck
Overall score: sum of move scores

Suppose there are n boxes.

What is the score if we cut the stack into half each time?

say n=8, then the score is ?



Start: a stack of boxes
Move: split any stack into two stacks of sizes *a*,*b*>0
Scoring: *ab* points
Keep moving: until stuck
Overall score: sum of move scores

Unstacking Game

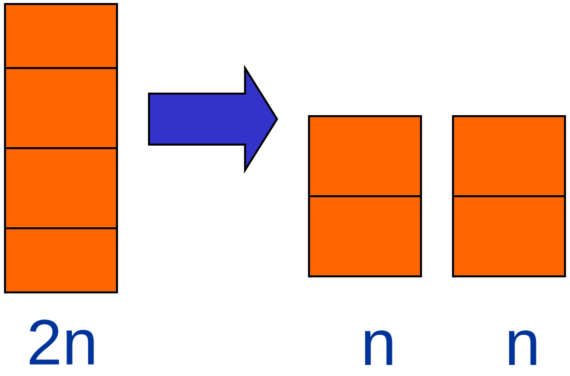
Suppose there are n boxes.

What is the score if we cut the stack into half each time?

say n=8, then the score is

$$\underbrace{1x4x4}_{\textbf{first round}} + \underbrace{2x2x2}_{\textbf{second}} + \underbrace{4x1}_{\textbf{third}} = 28$$

say n=16, then the score is ?



Unstacking Game

Start: a stack of boxes
Move: split any stack into two stacks of sizes *a*,*b*>0
Scoring: *ab* points
Keep moving: until stuck
Overall score: sum of move scores

Suppose there are n boxes.

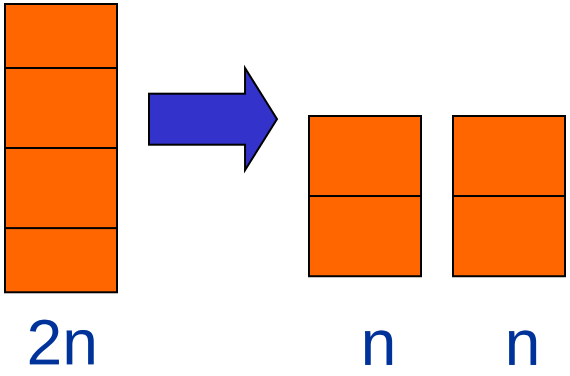
What is the score if we cut the stack into half each time?

say n=8, then the score is

$$\underbrace{1x4x4}_{\textbf{first round}} + \underbrace{2x2x2}_{\textbf{second}} + \underbrace{4x1}_{\textbf{third}} = 28$$

say n=16, then the score is

8x8 + 2x28 = 120



Unstacking Game

Start: a stack of boxes
Move: split any stack into two stacks of sizes *a*,*b*>0
Scoring: *ab* points
Keep moving: until stuck
Overall score: sum of move scores

Which Strategy do you think is better？

(A) the first one

(B) the second one

(C) it depends

(D) they are the same

Unstacking Game

Start: a stack of boxes
Move: split any stack into two stacks of sizes *a*,*b*>0
Scoring: *ab* points
Keep moving: until stuck
Overall score: sum of move scores

Which Strategy do you think is better？

(A) the first one

(B) the second one

(C) it depends

(D) they are the same

say n=8, then the score is

1x4x4 + 2x2x2 + 4x1 = 28

say n=16, then the score is

8x8 + 2x28 = 120

Unstacking Game

Claim: Every way of unstacking gives the same score.

⇕

Claim: Starting with size n stack, final score will be $\frac{\boldsymbol{n(n-1)}}{\mathbf{2}}$

Unstacking Game

Claim: Every way of unstacking gives the same score.

⇕

Claim(*n*)*:* Starting with size n stack, final score will be $\frac{\boldsymbol{n(n-1)}}{\mathbf{2}}$

Proof: by Induction with *Claim*(*n*) as hypothesis

Basis Step ($n = 1$)

score = 0 = $\frac{1(1-1)}{2}$

Unstacking Game

Claim: Every way of unstacking gives the same score.

⇕

Claim(*n*)*:* Starting with size n stack, final score will be $\frac{n(n-1)}{2}$

Inductive Step assume for *n*-stack, and then prove *Claim*(*n*+1)

Claim(*n*+1): (*n*+1)-stack score = $\frac{(n+1)n}{2}$

Claim(n+1): (n+1)-stack score = $\frac{(n+1)n}{2}$

Unstacking Game

Claim(n): Starting with size n stack, final score will be $\frac{n(n-1)}{2}$

Case n+1 > 1. So split into an a-stack and b-stack, where $a + b = n + 1$.

(a + b)-stack score = ab + a-stack score + b-stack score

by induction:

a-stack score =$\frac{a(a-1)}{2}$

b-stack score =$\frac{b(b-1)}{2}$

Claim(n+1): (n+1)-stack score = $\frac{(n+1)n}{2}$

Unstacking Game

Claim(n): Starting with size n stack, final score will be $\frac{n(n-1)}{2}$

Case n+1 > 1. So split into an a-stack and b-stack, where $a + b = n + 1$.

(a + b)-stack score = ab + a-stack score + b-stack score

$$ab + \frac{a(a-1)}{2} + \frac{b(b-1)}{2} \overset{?}{=} \frac{(n+1)n}{2}$$

Unstacking Game

Claim(n+1): (n+1)-stack score = $\frac{(n+1)n}{2}$

Claim(n): Starting with size n stack, final score will be $\frac{n(n-1)}{2}$

Case n+1 > 1. So split into an a-stack and b-stack, where $a + b = n + 1$.

(a + b)-stack score = ab + a-stack score + b-stack score

$$ab + \frac{a(a-1)}{2} + \frac{b(b-1)}{2} =$$

$$\frac{2ab + a^2 - a + b^2 - b}{2} = \frac{(a+b)^2 - (a+b)}{2} =$$

$$\frac{(a+b)((a+b)-1)}{2} = \frac{(n+1)n}{2}$$

so *Claim*(n+1) is okay.

Unstacking Game

Claim(*n*): Starting with size n stack, final score will be $\frac{n(n-1)}{2}$

Wait: we *assumed* *C*(*a*) and *C*(*b*) where 1 *a*, *b* *n.*

But by induction can only assume *C*(*n*)

(Here "*C*" means "*Claim*".)

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.

Unstacking Game

Claim(*n*)*:* Starting with size n stack, final score will be $\frac{n(n-1)}{2}$

Wait: we *assumed* *C*(*a*) and *C*(*b*) where 1 *a*, *b* *n*.

But by induction can only assume *C*(*n*)

We need Strong Form of Induction (强数学归纳法)！

Unstacking Game

Claim(*n*): Starting with size n stack, final score will be $\frac{n(n-1)}{2}$

Wait: we *assumed* *C*(*a*) and *C*(*b*) where 1 *a*, *b* *n*.

But by induction can only assume *C*(*n*)

the fix: revise the induction hypothesis to

$$Q(n) ::=$$

$$\forall m \leq n.\, C(m)$$

Proof goes through fine using *Q*(*n*) instead of *C*(*n*).

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

Induction: To prove a statement is true, we assume the truth of its immediate predecessor (直接前驱命题)

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 $n \geq n_0$, if $S(n)$ is true, then $S(n+1)$ is true.
Then $S(n)$ is true for every positive integer $n \geq n_0$.

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)

Induction: To prove a statement is true, we assume the truth of its immediate predecessor (直接前驱命题)

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 $n \geq n_0$, if $S(n)$ is true, then $S(n+1)$ is true.
Then $S(n)$ is true for every positive integer $n \geq n_0$.

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 $n_0 \le k < n$, then $S(n)$ is true.

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

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* ≥ 6 and that postage of *k* cents or more can be achieved by using only 2-cent and 5-cent stamps for 4 ≤ *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.

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.

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

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

use strong induction to prove that

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

$c_1=$

$c_2=$

$c_3=$

$c_4=$

$c_5=$

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

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

use strong induction to prove that

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

Proof:

Basis Steps (n=   )

Inductive Step

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

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

use strong induction to prove that

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

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 $\{ \lfloor 16.99+1/\mathrm{n} \rfloor \mid \mathrm{n} \in \mathrm{Z+} \}$.
(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 $n = dq + r$ $(0 \leq r < d)$

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 $n = dq + r \ (0 \leq r < d)$

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:

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

(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

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

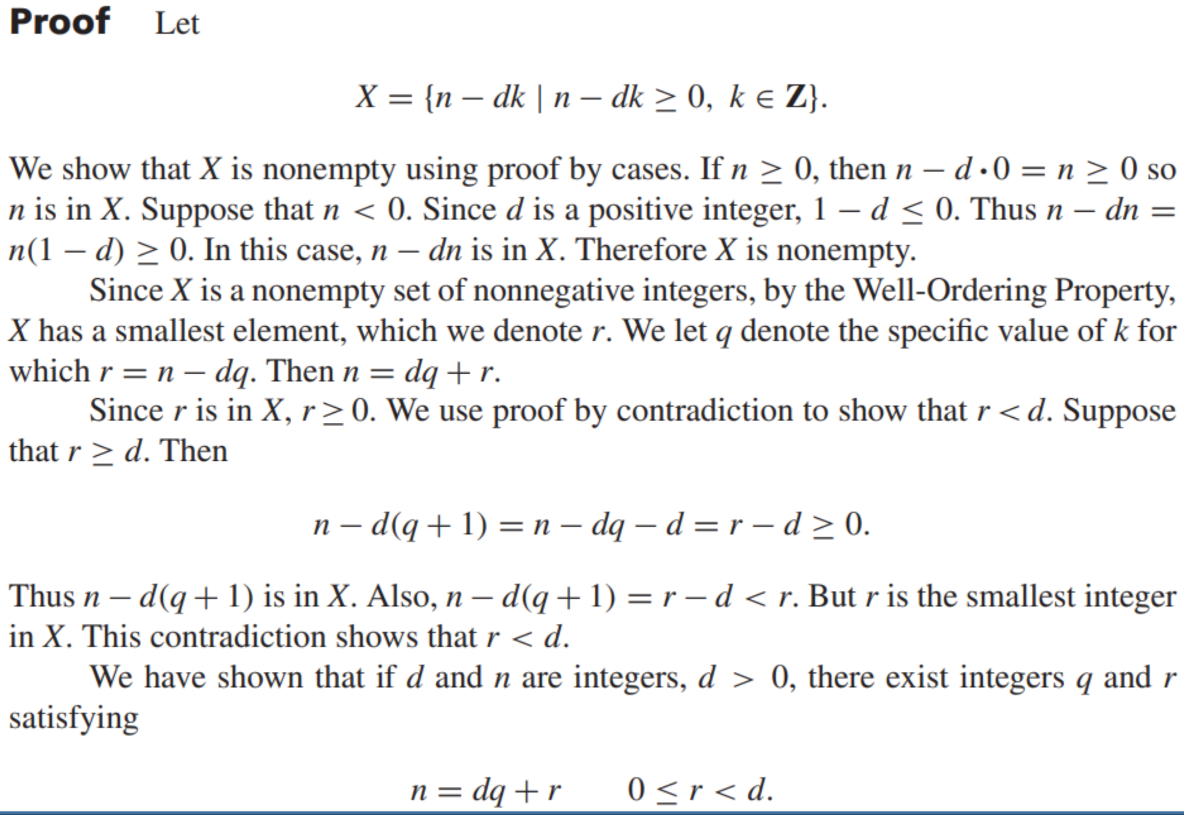
and

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

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

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 $n = dq + r \quad (0 \le r < d)$
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 Let

$$X = \{n - dk \mid n - dk \ge 0,\ k \in \mathbf{Z}\}.$$

We show that X is nonempty using proof by cases. If $n \ge 0$, then $n - d \cdot 0 = n \ge 0$ so n is in X. Suppose that $n < 0$. Since d is a positive integer, $1 - d \le 0$. Thus $n - dn = n(1 - d) \ge 0$. 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, $r \ge 0$. We use proof by contradiction to show that $r < d$. Suppose that $r \ge d$. Then

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

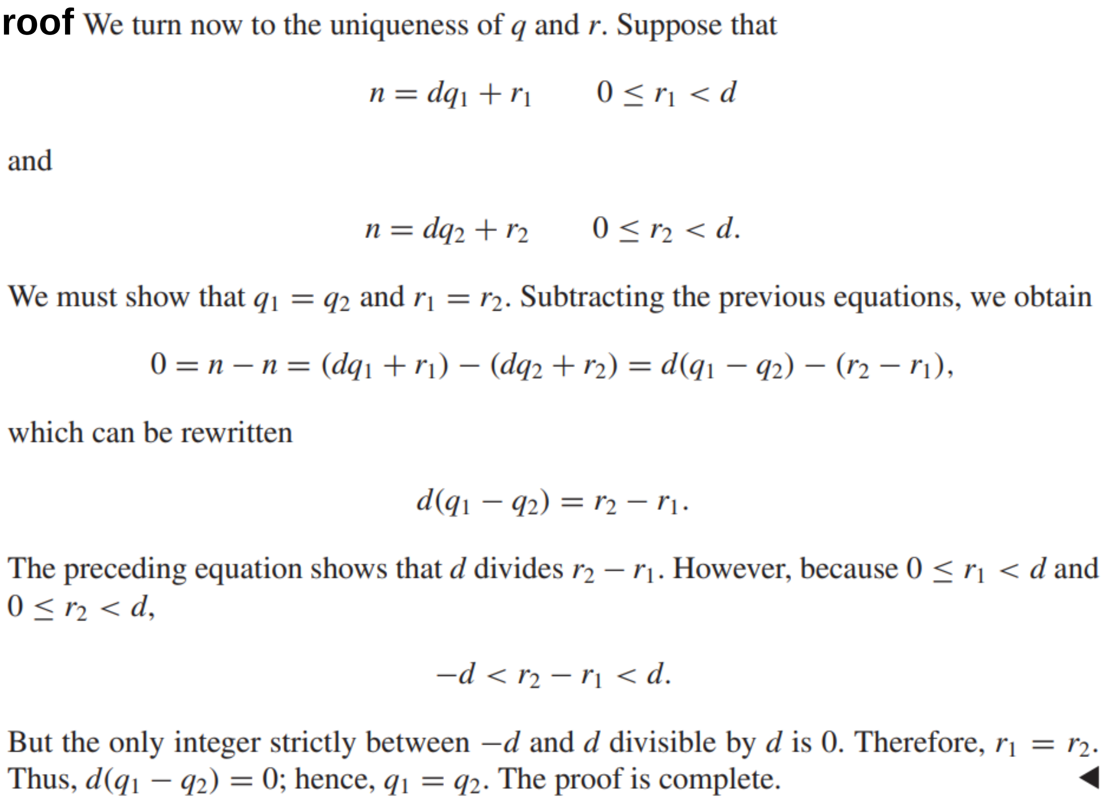
Thus $n - d(q + 1)$ is in X. Also, $n - d(q + 1) = r - d < r$. But r is the smallest integer in X. This contradiction shows that $r < d$.

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

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

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 $n = dq + r \quad (0 \le r < d)$
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

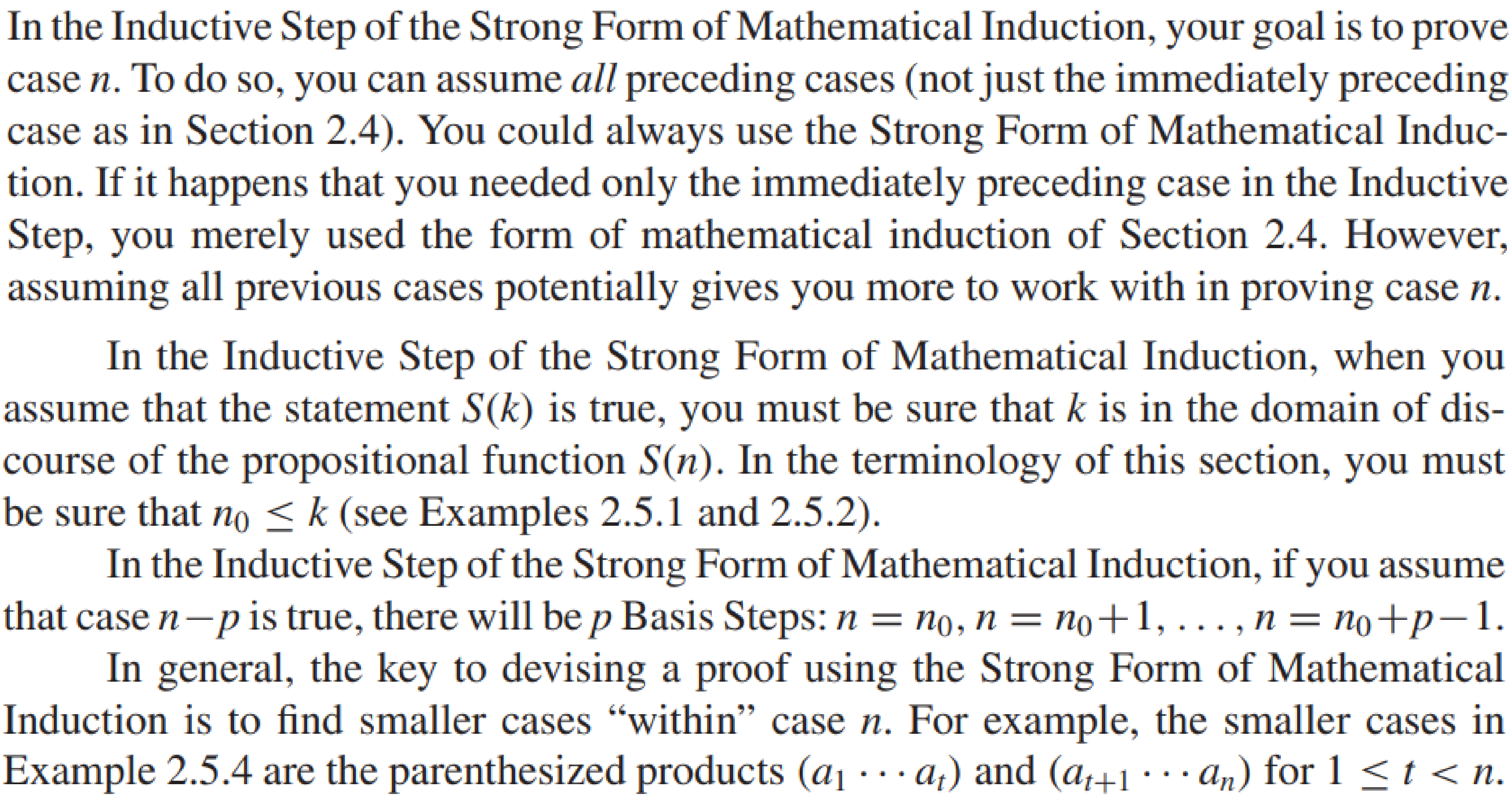
$$d(q_1 - q_2) = r_2 - r_1.$$

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 $1 \leq t < n$.