

Discrete Mathematics (151)

*Department of Mathematics
College of Sciences
King Saud University*

Chapter 2: Proof Methods

2.1 Introduction to Proofs (1.7 in book)

Methods of Proving Theorems

Proving mathematical theorems can be difficult. To construct proofs we need all available ammunition, including a powerful battery of different proof methods. These methods provide the overall approach and strategy of proofs. Understanding these methods is a key component of learning how to read and construct mathematical proofs. One we have chosen a proof method, we use axioms, definitions of terms, previously proved results, and rules of inference to complete the proof.

Direct Proofs

A **direct proof** of a conditional statement $p \rightarrow q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true.

A direct proof shows that a conditional statement $p \rightarrow q$ is true by showing that if p is true, then q must also be true, so that the combination p true and q false never occurs. In a direct proof, we assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true.

DEFINITION 1

The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$. (Note that every integer is either even or odd, and no integer is both even and odd.)

Two integers have the same parity when both are even or both are odd; they have opposite parity when one is even and the other is odd.

Example 1

Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

Solution: Note that this theorem states $\forall n (P(n) \rightarrow Q(n))$, where $P(n)$ is " n is an odd integer" and $Q(n)$ is " n^2 is odd." To begin a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that n is odd. By the definition of an odd integer, it follows that $n = 2k + 1$, where k is some integer. We want to show that n^2 is also odd. We can square both sides of the equation $n = 2k + 1$ to obtain a new equation that expresses n^2 . When we do this, we find that $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. We can conclude that n^2 is an odd integer (it is one more than twice an integer). Consequently, we have proved that if n is an odd integer, then n^2 is an odd integer.

Example 1

Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

Solution: Note that this theorem states $\forall n (P(n) \rightarrow Q(n))$, where $P(n)$ is " n is an odd integer" and $Q(n)$ is " n^2 is odd." To begin a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that n is odd. By the definition of an odd integer, it follows that $n = 2k + 1$, where k is some integer. We want to show that n^2 is also odd. We can square both sides of the equation $n = 2k + 1$ to obtain a new equation that expresses n^2 . When we do this, we find that $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. We can conclude that n^2 is an odd integer (it is one more than twice an integer). Consequently, we have proved that if n is an odd integer, then n^2 is an odd integer.

Example 2

Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square. (An integer a is a perfect square if there is an integer b such that $a = b^2$.)

Solution: To produce a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that m and n are both perfect squares. By the definition of a perfect square, it follows that there are integers s and t such that $m = s^2$ and $n = t^2$. The goal of the proof is to show that mn must also be a perfect square when m and n are; looking ahead we see how we can show this by substituting s^2 for m and t^2 for n into mn . This tells us that $mn = s^2t^2$. Hence, $mn = s^2t^2 = (ss)(tt) = (st)(st) = (st)^2$, using commutativity and associativity of multiplication. By the definition of perfect square, it follows that mn is also a perfect square, because it is the square of st , which is an integer. We have proved that if m and n are both perfect squares, then mn is also a perfect square.

Example 2

Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square. (An integer a is a perfect square if there is an integer b such that $a = b^2$.)

Solution: To produce a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that m and n are both perfect squares. By the definition of a perfect square, it follows that there are integers s and t such that $m = s^2$ and $n = t^2$. The goal of the proof is to show that mn must also be a perfect square when m and n are; looking ahead we see how we can show this by substituting s^2 for m and t^2 for n into mn . This tells us that $mn = s^2t^2$. Hence, $mn = s^2t^2 = (ss)(tt) = (st)(st) = (st)^2$, using commutativity and associativity of multiplication. By the definition of perfect square, it follows that mn is also a perfect square, because it is the square of st , which is an integer. We have proved that if m and n are both perfect squares, then mn is also a perfect square.

Proof by Contraposition

We need other methods of proving theorems of the form $\forall x (P(x) \rightarrow Q(x))$. Proofs of theorems of this type that are not direct proofs, that is, that do not start with the premises and end with the conclusion, are called **indirect proofs**.

An extremely useful type of indirect proof is known as **proof by contraposition**. Proofs by contraposition make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$. This means that the conditional statement $p \rightarrow q$ can be proved by showing that its contrapositive, $\neg q \rightarrow \neg p$, is true. In a proof by contraposition of $p \rightarrow q$, we take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow.

Example 3

Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Solution: We first attempt a direct proof. To construct a direct proof, we first assume that $3n + 2$ is an odd integer. This means that $3n + 2 = 2k + 1$ for some integer k . Can we use this fact to show that n is odd? We see that $3n + 1 = 2k$, but there does not seem to be any direct way to conclude that n is odd. Because our attempt at a direct proof failed, we next try a proof by contraposition. The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "If $3n + 2$ is odd, then n is odd" is false; namely, assume that n is even. Then, by the definition of an even integer, $n = 2k$ for some integer k . Substituting $2k$ for n , we find that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. This tells us that $3n + 2$ is even (because it is a multiple of 2), and therefore not odd. This is the negation of the premise of the theorem. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded; we have proved the theorem "If $3n + 2$ is odd, then n is odd."

Example 3

Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Solution: We first attempt a direct proof. To construct a direct proof, we first assume that $3n + 2$ is an odd integer. This means that $3n + 2 = 2k + 1$ for some integer k . Can we use this fact to show that n is odd? We see that $3n + 1 = 2k$, but there does not seem to be any direct way to conclude that n is odd. Because our attempt at a direct proof failed, we next try a proof by contraposition. The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "If $3n + 2$ is odd, then n is odd" is false; namely, assume that n is even. Then, by the definition of an even integer, $n = 2k$ for some integer k . Substituting $2k$ for n , we find that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. This tells us that $3n + 2$ is even (because it is a multiple of 2), and therefore not odd. This is the negation of the premise of the theorem. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded; we have proved the theorem "If $3n + 2$ is odd, then n is odd."

Example 4

Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Solution: Because there is no obvious way of showing that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ directly from the equation $n = ab$, where a and b are positive integers, we attempt a proof by contraposition.

The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ " is false. That is, we assume that the statement $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$ is false. Using the meaning of disjunction together with De Morgans law, we see that this implies that both $a \leq \sqrt{n}$ and $b \leq \sqrt{n}$ are false. This implies that $a > \sqrt{n}$ and $b > \sqrt{n}$. We can multiply these inequalities together (using the fact that if $0 < s < t$ and $0 < u < v$, then $su < tv$) to obtain $ab > \sqrt{n}\sqrt{n} = n$. This shows that $ab \neq n$, which contradicts the statement $n = ab$. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded; we have proved that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Example 4

Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Solution: Because there is no obvious way of showing that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ directly from the equation $n = ab$, where a and b are positive integers, we attempt a proof by contraposition.

The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ " is false. That is, we assume that the statement $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$ is false. Using the meaning of disjunction together with De Morgans law, we see that this implies that both $a \leq \sqrt{n}$ and $b \leq \sqrt{n}$ are false. This implies that $a > \sqrt{n}$ and $b > \sqrt{n}$. We can multiply these inequalities together (using the fact that if $0 < s < t$ and $0 < u < v$, then $su < tv$) to obtain $ab > \sqrt{n}\sqrt{n} = n$. This shows that $ab \neq n$, which contradicts the statement $n = ab$. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded; we have proved that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Example 5 (8 in book)

Prove that if n is an integer and n^2 is odd, then n is odd.

Solution: We first attempt a direct proof. Suppose that n is an integer and n^2 is odd. Then, there exists an integer k such that $n^2 = 2k + 1$. Can we use this information to show that n is odd?

There seems to be no obvious approach to show that n is odd because solving for n produces the equation $n = \pm\sqrt{2k+1}$, which is not terribly useful. Because this attempt to use a direct proof did not give result, we next attempt a proof by contraposition. We take as our hypothesis the statement that n is not odd.

Because every integer is odd or even, this means that n is even. This implies that there exists an integer k such that $n = 2k$. To prove the theorem, we need to show that this hypothesis implies the conclusion that n^2 is not odd, that is, that n^2 is even. Can we use the equation $n = 2k$ to achieve this? By squaring both sides of this equation, we obtain $n^2 = 4k^2 = 2(2k^2)$, which implies that n^2 is also even because $n^2 = 2t$, where $t = 2k^2$. We have proved that if n is an integer and n^2 is odd, then n is odd. Our attempt to find a proof by contraposition succeeded.

Example 5 (8 in book)

Prove that if n is an integer and n^2 is odd, then n is odd.

Solution: We first attempt a direct proof. Suppose that n is an integer and n^2 is odd. Then, there exists an integer k such that $n^2 = 2k + 1$. Can we use this information to show that n is odd?

There seems to be no obvious approach to show that n is odd because solving for n produces the equation $n = \pm\sqrt{2k+1}$, which is not terribly useful. Because this attempt to use a direct proof did not give result, we next attempt a proof by contraposition. We take as our hypothesis the statement that n is not odd.

Because every integer is odd or even, this means that n is even. This implies that there exists an integer k such that $n = 2k$. To prove the theorem, we need to show that this hypothesis implies the conclusion that n^2 is not odd, that is, that n^2 is even. Can we use the equation $n = 2k$ to achieve this? By squaring both sides of this equation, we obtain $n^2 = 4k^2 = 2(2k^2)$, which implies that n^2 is also even because $n^2 = 2t$, where $t = 2k^2$. We have proved that if n is an integer and n^2 is odd, then n is odd. Our attempt to find a proof by contraposition succeeded.

Proofs by Contradiction

Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true. Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true. How can we find a contradiction q that might help us prove that p is true in this way?

Because the statement $r \wedge \neg r$ is a contradiction whenever r is a proposition, we can prove that p is true if we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true for some proposition r . Proofs of this type are called proofs by contradiction. Because a proof by contradiction does not prove a result directly, it is another type of indirect proof.

Example 6 (9 in book)

Show that at least four of any 22 days must fall on the same day of the week.

Solution: Let p be the proposition "At least four of 22 chosen days fall on the same day of the week". Suppose that $\neg p$ is true. This means that at most three of the 22 days fall on the same day of the week. Because there are seven days of the week, this implies that at most 21 days could have been chosen, as for each of the days of the week, at most three of the chosen days could fall on that day. This contradicts the premise that we have 22 days under consideration. That is, if r is the statement that 22 days are chosen, then we have shown that $\neg p \rightarrow (r \wedge \neg r)$. Consequently, we know that p is true. We have proved that at least four of 22 chosen days fall on the same day of the week.

Example 6 (9 in book)

Show that at least four of any 22 days must fall on the same day of the week.

Solution: Let p be the proposition "At least four of 22 chosen days fall on the same day of the week". Suppose that $\neg p$ is true. This means that at most three of the 22 days fall on the same day of the week. Because there are seven days of the week, this implies that at most 21 days could have been chosen, as for each of the days of the week, at most three of the chosen days could fall on that day. This contradicts the premise that we have 22 days under consideration. That is, if r is the statement that 22 days are chosen, then we have shown that $\neg p \rightarrow (r \wedge \neg r)$. Consequently, we know that p is true. We have proved that at least four of 22 chosen days fall on the same day of the week.

Example 7 (10 in book)

Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Solution: Let p be the proposition " $\sqrt{2}$ is irrational." To start a proof by contradiction, we suppose that $\neg p$ is true. Note that $\neg p$ is the statement "It is not the case that $\sqrt{2}$ is irrational," which says that $\sqrt{2}$ is rational. We will show that assuming that $\neg p$ is true leads to a contradiction. If $\sqrt{2}$ is rational, there exist integers a and b with $\sqrt{2} = \frac{a}{b}$, where $b \neq 0$ and a and b have no common factors (so that the fraction $\frac{a}{b}$ is in lowest terms.) (Here, we are using the fact that every rational number can be written in lowest terms.) Because $\sqrt{2} = \frac{a}{b}$, when both sides of this equation are squared, it follows that $2 = \frac{a^2}{b^2}$. Hence, $2b^2 = a^2$. By the definition of an even integer it follows that a^2 is even. We next use the fact that if a^2 is even, a must also be even.

Example 7 (10 in book)

Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Solution: Let p be the proposition " $\sqrt{2}$ is irrational." To start a proof by contradiction, we suppose that $\neg p$ is true. Note that $\neg p$ is the statement "It is not the case that $\sqrt{2}$ is irrational," which says that $\sqrt{2}$ is rational. We will show that assuming that $\neg p$ is true leads to a contradiction. If $\sqrt{2}$ is rational, there exist integers a and b with $\sqrt{2} = \frac{a}{b}$, where $b \neq 0$ and a and b have no common factors (so that the fraction $\frac{a}{b}$ is in lowest terms.) (Here, we are using the fact that every rational number can be written in lowest terms.) Because $\sqrt{2} = \frac{a}{b}$, when both sides of this equation are squared, it follows that $2 = \frac{a^2}{b^2}$. Hence, $2b^2 = a^2$. By the definition of an even integer it follows that a^2 is even. We next use the fact that if a^2 is even, a must also be even.

Introduction to Proofs

Furthermore, because a is even, by the definition of an even integer, $a = 2c$ for some integer c . Thus, $2b^2 = 4c^2$. Dividing both sides of this equation by 2 gives $b^2 = 2c^2$. By the definition of even, this means that b^2 is even. Again using the fact that if the square of an integer is even, then the integer itself must be even, we conclude that b must be even as well. We have now shown that the assumption of $\neg p$ leads to the equation $\sqrt{2} = \frac{a}{b}$, where a and b have no common factors, but both a and b are even, that is, 2 divides both a and b . Note that the statement that $\sqrt{2} = \frac{a}{b}$, where a and b have no common factors, means, in particular, that 2 does not divide both a and b . Because our assumption of $\neg p$ leads to the contradiction that 2 divides both a and b and 2 does not divide both a and b , $\neg p$ must be false. That is, the statement p , " $\sqrt{2}$ is irrational," is true. We have proved that $\sqrt{2}$ is irrational.

Example 8 (11 in book)

Give a proof by contradiction of the theorem "If $3n + 2$ is odd, then n is odd."

Solution: Let p be " $3n + 2$ is odd" and q be " n is odd." To construct a proof by contradiction, assume that both p and $\neg q$ are true. That is, assume that $3n + 2$ is odd and that n is not odd. Because n is not odd, we know that it is even. Because n is even, there is an integer k such that $n = 2k$. This implies that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. Because $3n + 2$ is $2t$, where $t = 3k + 1$, $3n + 2$ is even. Note that the statement " $3n + 2$ is even" is equivalent to the statement $\neg p$, because an integer is even if and only if it is not odd. Because both p and $\neg p$ are true, we have a contradiction. This completes the proof by contradiction, proving that if $3n + 2$ is odd, then n is odd.

Example 8 (11 in book)

Give a proof by contradiction of the theorem "If $3n + 2$ is odd, then n is odd."

Solution: Let p be " $3n + 2$ is odd" and q be " n is odd." To construct a proof by contradiction, assume that both p and $\neg q$ are true. That is, assume that $3n + 2$ is odd and that n is not odd. Because n is not odd, we know that it is even. Because n is even, there is an integer k such that $n = 2k$. This implies that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. Because $3n + 2$ is $2t$, where $t = 3k + 1$, $3n + 2$ is even. Note that the statement " $3n + 2$ is even" is equivalent to the statement $\neg p$, because an integer is even if and only if it is not odd. Because both p and $\neg p$ are true, we have a contradiction. This completes the proof by contradiction, proving that if $3n + 2$ is odd, then n is odd.

Note that we can also prove by contradiction that $p \rightarrow q$ is true by assuming that p and $\neg q$ are true, and showing that q must be also be true. This implies that $\neg q$ and q are both true, a contradiction. This observation tells us that we can turn a direct proof into a proof by contradiction.

Proofs of Equivalence

To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true. The validity of this approach is based on the tautology $(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$.

Example 9 (12 in book)

Prove the theorem "If n is an integer, then n is odd if and only if n^2 is odd."

Solution: This theorem has the form " p if and only if q ," where p is " n is odd" and q is " n^2 is odd." (As usual, we do not explicitly deal with the universal quantification.) To prove this theorem, we need to show that $p \rightarrow q$ and $q \rightarrow p$ are true. We have already shown (in Example 1) that $p \rightarrow q$ is true and (in Example 5 (8 in book)) that $q \rightarrow p$ is true. Because we have shown that both $p \rightarrow q$ and $q \rightarrow p$ are true, we have shown that the theorem is true.

Example 9 (12 in book)

Prove the theorem "If n is an integer, then n is odd if and only if n^2 is odd."

Solution: This theorem has the form " p if and only if q ," where p is " n is odd" and q is " n^2 is odd." (As usual, we do not explicitly deal with the universal quantification.) To prove this theorem, we need to show that $p \rightarrow q$ and $q \rightarrow p$ are true. We have already shown (in Example 1) that $p \rightarrow q$ is true and (in Example 5 (8 in book)) that $q \rightarrow p$ is true. Because we have shown that both $p \rightarrow q$ and $q \rightarrow p$ are true, we have shown that the theorem is true.

2.2 Proof Methods and Strategy (1.8 in book)

Introduction

- In Section 1.4 (1.7 in book) we introduced many methods of proof and illustrated how each method can be used. In this section we continue this effort. We will introduce several other commonly used proof methods, including the method of proving a theorem by considering different cases separately. We will also discuss proofs where we prove the existence of objects with desired properties.
- In Section 1.4 (1.7 in book) we briefly discussed the strategy behind constructing proofs. This strategy includes selecting a proof method and then successfully constructing an argument step by step, based on this method.

Introduction

- In this section, after we have developed a versatile arsenal of proof methods, we will study some aspects of the art and science of proofs.
- We will provide advice on how to find a proof of a theorem. We will describe some tricks of the trade, including how proofs can be found by working backward and by adapting existing proofs.
- When mathematicians work, they formulate conjectures and attempt to prove or disprove them.

Exhaustive Proofs

- Some theorems can be proved by examining a relatively small number of examples. Such proofs are called **exhaustive proofs**, or **proofs by exhaustion** because these proofs proceed by exhausting all possibilities.
- An exhaustive proof is a special type of proof by cases where each case involves checking a single example.
- We now provide some illustrations of exhaustive proofs.

To prove a conditional statement of the form $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$ the tautology

$[(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)]$
can be used as a rule of inference.

Example 1

Prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Solution: We use a proof by exhaustion. We only need verify the inequality $(n + 1)^3 \geq 3^n$ when $n = 1, 2, 3$, and 4 .

For $n = 1$, we have $(n + 1)^3 = 2^3 = 8$ and $3^n = 3^1 = 3$;

for $n = 2$, we have $(n + 1)^3 = 3^3 = 27$ and $3^n = 3^2 = 9$;

for $n = 3$, we have $(n + 1)^3 = 4^3 = 64$ and $3^n = 3^3 = 27$;

and for $n = 4$, we have $(n + 1)^4 = 5^4 = 625$ and $3^n = 3^4 = 81$.

In each of these four cases, we see that $(n + 1)^3 \geq 3^n$. We have used the method of exhaustion to prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Example 1

Prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Solution: We use a proof by exhaustion. We only need verify the inequality $(n + 1)^3 \geq 3^n$ when $n = 1, 2, 3$, and 4 .

For $n = 1$, we have $(n + 1)^3 = 2^3 = 8$ and $3^n = 3^1 = 3$;

for $n = 2$, we have $(n + 1)^3 = 3^3 = 27$ and $3^n = 3^2 = 9$;

for $n = 3$, we have $(n + 1)^3 = 4^3 = 64$ and $3^n = 3^3 = 27$;

and for $n = 4$, we have $(n + 1)^4 = 5^4 = 625$ and $3^n = 3^4 = 81$.

In each of these four cases, we see that $(n + 1)^3 \geq 3^n$. We have used the method of exhaustion to prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Example 2

Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9. (An integer is a **perfect power** if it equals n^a , where a is an integer greater than 1.)

Solution: We use a proof by exhaustion. In particular, we can prove this fact by examining positive integers n not exceeding 100, first checking whether n is a perfect power, and if it is, checking whether $n + 1$ is also a perfect power. A quicker way to do this is simply to look at all perfect powers not exceeding 100 and checking whether the next largest integer is also a perfect power. The squares of positive integers not exceeding 100 are 1, 4, 9, 16, 25, 36, 49, 64, 81, and 100. The cubes of positive integers not exceeding 100 are 1, 8, 27, and 64. The fourth powers of positive integers not exceeding 100 are 1, 16, and 81.

Example 2

Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9. (An integer is a **perfect power** if it equals n^a , where a is an integer greater than 1.)

Solution: We use a proof by exhaustion. In particular, we can prove this fact by examining positive integers n not exceeding 100, first checking whether n is a perfect power, and if it is, checking whether $n + 1$ is also a perfect power. A quicker way to do this is simply to look at all perfect powers not exceeding 100 and checking whether the next largest integer is also a perfect power. The squares of positive integers not exceeding 100 are 1, 4, 9, 16, 25, 36, 49, 64, 81, and 100. The cubes of positive integers not exceeding 100 are 1, 8, 27, and 64. The fourth powers of positive integers not exceeding 100 are 1, 16, and 81.

Proof Methods and Strategy

The fifth powers of positive integers not exceeding 100 are 1 and 32. The sixth powers of positive integers not exceeding 100 are 1 and 64. There are no powers of positive integers higher than the sixth power not exceeding 100, other than 1.

Looking at this list of perfect powers not exceeding 100, we see that $n = 8$ is the only perfect power n for which $n + 1$ is also a perfect power. That is, $2^3 = 8$ and $3^2 = 9$ are the only two consecutive perfect powers not exceeding 100.

Proof by Cases

- A proof by cases must cover all possible cases that arise in a theorem.
- We illustrate proof by cases with a couple of examples. In each example, you should check that all possible cases are covered.

Example 3

Prove that if n is an integer, then $n^2 \geq n$.

Solution: We can prove that $n^2 \geq n$ for every integer by considering three cases, when $n = 0$, when $n \geq 1$, and when $n \leq -1$. We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.

Proof by Cases

- A proof by cases must cover all possible cases that arise in a theorem.
- We illustrate proof by cases with a couple of examples. In each example, you should check that all possible cases are covered.

Example 3

Prove that if n is an integer, then $n^2 \geq n$.

Solution: We can prove that $n^2 \geq n$ for every integer by considering three cases, when $n = 0$, when $n \geq 1$, and when $n \leq -1$. We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.

Proof Methods and Strategy

- Case (i): When $n = 0$, because $0^2 = 0$, we see that $0^2 \geq 0$. It follows that $n^2 \geq n$ is true in this case.
- Case (ii): When $n \geq 1$, when we multiply both sides of the inequality $n \geq 1$ by the positive integer n , we obtain $n \cdot n \geq n \cdot 1$. This implies that $n^2 \geq n$ for $n \geq 1$.
- Case (iii): In this case $n \leq -1$. However, $n^2 \geq 0$. It follows that $n^2 \geq n$.

Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$.

Example 4

Use a proof by cases to show that $|xy| = |x||y|$, where x and y are real numbers. (Recall that $|a|$, the absolute value of a , equals a when $a \geq 0$ and equals $-a$ when $a \leq 0$.)

Solution: In our proof of this theorem, we remove absolute values using the fact that $|a| = a$ when $a \geq 0$ and $|a| = -a$ when $a < 0$. Because both $|x|$ and $|y|$ occur in our formula, we will need four cases: (i) x and y both nonnegative, (ii) x nonnegative and y is negative, (iii) x negative and y nonnegative, and (iv) x negative and y negative. We denote by p_1 , p_2 , p_3 , and p_4 , the proposition stating the assumption for each of these four cases, respectively.

(Note that we can remove the absolute value signs by making the appropriate choice of signs within each case.)

Example 4

Use a proof by cases to show that $|xy| = |x||y|$, where x and y are real numbers. (Recall that $|a|$, the absolute value of a , equals a when $a \geq 0$ and equals $-a$ when $a \leq 0$.)

Solution: In our proof of this theorem, we remove absolute values using the fact that $|a| = a$ when $a \geq 0$ and $|a| = -a$ when $a < 0$. Because both $|x|$ and $|y|$ occur in our formula, we will need four cases: (i) x and y both nonnegative, (ii) x nonnegative and y is negative, (iii) x negative and y nonnegative, and (iv) x negative and y negative. We denote by p_1 , p_2 , p_3 , and p_4 , the proposition stating the assumption for each of these four cases, respectively.

(Note that we can remove the absolute value signs by making the appropriate choice of signs within each case.)

Proof Methods and Strategy

- Case (i): We see that $p_1 \rightarrow q$ because $xy \geq 0$ when $x \geq 0$ and $y \geq 0$, so that $|xy| = xy = |x||y|$.
- To see that $p_2 \rightarrow q$, note that if $x \geq 0$ and $y < 0$, then $xy \leq 0$, so that $|xy| = -xy = x(-y) = |x||y|$. (Here, because $y < 0$, we have $|y| = -y$.)
- Case (iii): To see that $p_3 \rightarrow q$, we follow the same reasoning as the previous case with the roles of x and y reversed.
- Case (iv): To see that $p_4 \rightarrow q$, note that when $x < 0$ and $y < 0$, it follows that $xy > 0$. Hence, $|xy| = xy = (-x)(-y) = |x||y|$.

Because $|xy| = |x||y|$ holds in each of the four cases and these cases exhaust all possibilities, we can conclude that $|xy| = |x||y|$, whenever x and y are real numbers.

Example 5 (7 in book)

Show that if x and y are integers and both xy and $x + y$ are even, then both x and y are even.

Solution: We will use proof by contraposition, the notion of without loss of generality, and proof by cases. First, suppose that x and y are not both even. That is, assume that x is odd or that y is odd (or both). Without loss of generality, we assume that x is odd, so that $x = 2m + 1$ for some integer m .

To complete the proof, we need to show that xy is odd or $x + y$ is odd. Consider two cases: (i) y even, and (ii) y odd.

Example 5 (7 in book)

Show that if x and y are integers and both xy and $x + y$ are even, then both x and y are even.

Solution: We will use proof by contraposition, the notion of without loss of generality, and proof by cases. First, suppose that x and y are not both even. That is, assume that x is odd or that y is odd (or both). Without loss of generality, we assume that x is odd, so that $x = 2m + 1$ for some integer m .

To complete the proof, we need to show that xy is odd or $x + y$ is odd. Consider two cases: (i) y even, and (ii) y odd.

Proof Methods and Strategy

- In (i), $y = 2n$ for some integer n , so that $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.
- In (ii), $y = 2n + 1$ for some integer n , so that $xy = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$ is odd.

This completes the proof by contraposition. (Note that our use of without loss of generality within the proof is justified because the proof when y is odd can be obtained by simply interchanging the roles of x and y in the proof we have given.)

2.3 Mathematical Induction (5.1 in book)

- Many mathematical statements assert that a property is true for all positive integers.

Examples of such statements are that for every positive integer n : $n! \leq n^n$, $n^3 - n$ is divisible by 3; a set with n elements has 2^n subsets; and the sum of the first n positive integers is $\frac{n(n+1)}{2}$.

- A major goal of this chapter, is to give the student a thorough understanding of mathematical induction, which is used to prove results of this kind.
- Proofs using mathematical induction have two parts. First, they show that the statement holds for the positive integer 1. Second, they show that if the statement holds for a positive integer then it must also hold for the next larger integer.

- Mathematical induction is based on the rule of inference that tells us that if $P(1)$ and $\forall k (P(k) \rightarrow P(k + 1))$ are true for the domain of positive integers, then $\forall n P(n)$ is true.
- Mathematical induction can be used to prove a huge variety of results.
- Understanding how to read and construct proofs by mathematical induction is a key goal of learning discrete mathematics.

Mathematical Induction

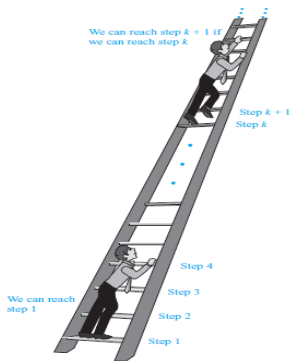


Figure 1: Infinite Ladder.

Suppose that we have an infinite ladder, as shown in Figure 1, and we want to know whether we can reach every step on this ladder. We know two things:

- 1 We can reach the first rung of the ladder.
- 2 If we can reach a particular rung of the ladder, then we can reach the next rung.

Can we conclude that we can reach every rung? By (1), we know that we can reach the first rung of the ladder. Moreover, because we can reach the first rung, by (2), we can also reach the second rung; it is the next rung after the first rung. Applying (2) again, because we can reach the second rung, we can also reach the third rung.

Mathematical Induction

Continuing in this way, we can show that we can reach the fourth rung, the fifth rung, and so on. For example, after 100 uses of (2), we know that we can reach the 101st rung. But can we conclude that we are able to reach every rung of this infinite ladder? The answer is yes, something we can verify using an important proof technique called **mathematical induction**. That is, we can show that $P(n)$ is true for every positive integer n , where $P(n)$ is the statement that we can reach the n th rung of the ladder. Mathematical induction is an extremely important proof technique that can be used to prove assertions of this type. As we will see in this section and in subsequent sections of this chapter and later chapters, mathematical induction is used extensively to prove results about a large variety of discrete objects.

Mathematical Induction

Mathematical Induction:

In general, mathematical induction, can be used to prove statements that assert that $P(n)$ is true for all positive integers n , where $P(n)$ is a propositional function. A proof by mathematical induction has two parts, a basis step, where we show that $P(1)$ is true, and an inductive step, where we show that for all positive integers k , if $P(k)$ is true, then $P(k + 1)$ is true.

PRINCIPLE OF MATHEMATICAL INDUCTION

To prove that $P(n)$ is true for all positive integers n , where $P(n)$ is a propositional function, we complete two steps:

- 1 **BASIS STEP:** We verify that $P(1)$ is true.
- 2 **INDUCTIVE STEP:** We show that the conditional statement $P(k) \rightarrow P(k + 1)$ is true for all positive integers k .

Expressed as a rule of inference, this proof technique can be stated as

$$(P(1) \wedge \forall k (P(k) \rightarrow P(k + 1))) \rightarrow \forall n P(n)$$

Remark:

In a proof by mathematical induction it is not assumed that $P(k)$ is true for all positive integers! It is only shown that if it is assumed that $P(k)$ is true, then $P(k + 1)$ is also true. Thus, a proof by mathematical induction is not a case of begging the question, or circular reasoning.

When we use mathematical induction to prove a theorem, we first show that $P(1)$ is true. Then we know that $P(2)$ is true, because $P(1)$ implies $P(2)$. Further, we know that $P(3)$ is true, because $P(2)$ implies $P(3)$. Continuing along these lines, we see that $P(n)$ is true for every positive integer n .

EXAMPLE 1

Show that if n is a positive integer, then $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Solution: Let $P(n)$ be the proposition that the sum of the first n positive integers, $1 + 2 + \cdots + n$, is $\frac{n(n+1)}{2}$. We must do two things to prove that $P(n)$ is true for $n = 1, 2, 3, \dots$. Namely, we must show that $P(1)$ is true and that the conditional statement $P(k)$ implies $P(k+1)$ is true for $k = 1, 2, 3, \dots$.

BASIS STEP: $P(1)$ is true, because $1 = \frac{1(1+1)}{2}$. (The lefthand side of this equation is 1 because 1 is the sum of the first positive integer. The right-hand side is found by substituting 1 for n in $\frac{n(n+1)}{2}$).

INDUCTIVE STEP: For the inductive hypothesis we assume that $P(k)$ holds for an arbitrary positive integer k . That is, we assume that

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

EXAMPLE 1

Show that if n is a positive integer, then $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Solution: Let $P(n)$ be the proposition that the sum of the first n positive integers, $1 + 2 + \cdots + n$, is $\frac{n(n+1)}{2}$. We must do two things to prove that $P(n)$ is true for $n = 1, 2, 3, \dots$. Namely, we must show that $P(1)$ is true and that the conditional statement $P(k)$ implies $P(k + 1)$ is true for $k = 1, 2, 3, \dots$.

BASIS STEP: $P(1)$ is true, because $1 = \frac{1(1+1)}{2}$. (The lefthand side of this equation is 1 because 1 is the sum of the first positive integer. The right-hand side is found by substituting 1 for n in $\frac{n(n+1)}{2}$).

INDUCTIVE STEP: For the inductive hypothesis we assume that $P(k)$ holds for an arbitrary positive integer k . That is, we assume that

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

Mathematical Induction

Under this assumption, it must be shown that $P(k + 1)$ is true, namely,

$$1 + 2 + \cdots + k + (k + 1) = \frac{(k + 1)[(k + 1) + 1]}{2} = \frac{(k + 1)(k + 2)}{2}$$

is also true. We add $k + 1$ to both sides of the equation in $P(k)$, we obtain

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

This last equation shows that $P(k + 1)$ is true under the assumption that $P(k)$ is true. This completes the inductive step.

We have completed the basis step and the inductive step, so by mathematical induction we know that $P(n)$ is true for all positive integers n . That is, we have proven that $1 + 2 + \cdots + n = \frac{n(n + 1)}{2}$ for all positive integers n .

Mathematical Induction

EXAMPLE 2 (6 in book)

Use mathematical induction to prove that $2^n < n!$ for every integer n with $n \geq 4$. (Note that this inequality is false for $n = 1, 2$, and 3 .)

Solution: Let $P(n)$ be the proposition that $2^n < n!$.

BASIS STEP: To prove the inequality for $n \geq 4$ requires that the basis step be $P(4)$. Note that $P(4)$ is true, because $2^4 = 16 < 24 = 4!$.

INDUCTIVE STEP: For the inductive step, we assume that $P(k)$ is true for an arbitrary integer k with $k \geq 4$. That is, we assume that $2^k < k!$ for the positive integer k with $k \geq 4$. We must show that under this hypothesis, $P(k + 1)$ is also true. That is, we must show that if $2^k < k!$ for an arbitrary positive integer k where $k \geq 4$, then $2^{k+1} < (k + 1)!$. We have

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k && \text{by definition of exponent} \\ &< 2 \cdot k! && \text{by the inductive hypothesis} \\ &< (k + 1)k! && \text{because } 2 < k + 1 \\ &= (k + 1)! && \text{by definition of factorial function.} \end{aligned}$$

Mathematical Induction

EXAMPLE 2 (6 in book)

Use mathematical induction to prove that $2^n < n!$ for every integer n with $n \geq 4$. (Note that this inequality is false for $n = 1, 2$, and 3 .)

Solution: Let $P(n)$ be the proposition that $2^n < n!$.

BASIS STEP: To prove the inequality for $n \geq 4$ requires that the basis step be $P(4)$. Note that $P(4)$ is true, because $2^4 = 16 < 24 = 4!$.

INDUCTIVE STEP: For the inductive step, we assume that $P(k)$ is true for an arbitrary integer k with $k \geq 4$. That is, we assume that $2^k < k!$ for the positive integer k with $k \geq 4$. We must show that under this hypothesis, $P(k + 1)$ is also true. That is, we must show that if $2^k < k!$ for an arbitrary positive integer k where $k \geq 4$, then $2^{k+1} < (k + 1)!$. We have

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k && \text{by definition of exponent} \\ &< 2 \cdot k! && \text{by the inductive hypothesis} \\ &< (k + 1)k! && \text{because } 2 < k + 1 \\ &= (k + 1)! && \text{by definition of factorial function.} \end{aligned}$$

Mathematical Induction

This shows that $P(k + 1)$ is true when $P(k)$ is true. This completes the inductive step of the proof.

We have completed the basis step and the inductive step. Hence, by mathematical induction $P(n)$ is true for all integers n with $n \geq 4$. That is, we have proved that $2^n < n!$ is true for all integers n with $n \geq 4$.

Mathematical Induction

EXAMPLE 3

Use mathematical induction to show that

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

for all nonnegative integers n .

Solution: Let $P(n)$ be the proposition that

$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for the integer n .

BASIS STEP: $P(0)$ is true because $2^0 = 1 = 2^1 - 1$. This completes the basis step.

INDUCTIVE STEP: For the inductive hypothesis, we assume that $P(k)$ is true for an arbitrary nonnegative integer k . That is, we assume that

$$1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$$

To carry out the inductive step using this assumption, we must show that when we assume that $P(k)$ is true, then $P(k+1)$ is also true. That is, we must show that

$$1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} = 2^{(k+1)+1} - 1 = 2^{k+2} - 1$$

assuming the inductive hypothesis $P(k)$.

Mathematical Induction

EXAMPLE 3

Use mathematical induction to show that

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

for all nonnegative integers n .

Solution: Let $P(n)$ be the proposition that

$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for the integer n .

BASIS STEP: $P(0)$ is true because $2^0 = 1 = 2^1 - 1$. This completes the basis step.

INDUCTIVE STEP: For the inductive hypothesis, we assume that $P(k)$ is true for an arbitrary nonnegative integer k . That is, we assume that

$$1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$$

To carry out the inductive step using this assumption, we must show that when we assume that $P(k)$ is true, then $P(k+1)$ is also true. That is, we must show that

$$1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} = 2^{(k+1)+1} - 1 = 2^{k+2} - 1$$

assuming the inductive hypothesis $P(k)$.

Mathematical Induction

Under the assumption of $P(k)$, we see that

$$\begin{aligned}1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} &= (1 + 2 + 2^2 + \cdots + 2^k) + 2^{k+1} \\ &\stackrel{IH}{=} (2^{k+1} - 1) + 2^{k+1} \\ &= 2 \cdot 2^{k+1} - 1 \\ &= 2^{k+2} - 1.\end{aligned}$$

Note that we used the inductive hypothesis in the second equation in this string of equalities to replace $1 + 2 + 2^2 + \cdots + 2^k$ by $2^{k+1} - 1$. We have completed the inductive step.

Because we have completed the basis step and the inductive step, by mathematical induction we know that $P(n)$ is true for all nonnegative integers n . That is, $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for all nonnegative integers n .

2.4 Strong Induction (5.2 in book)

Strong Induction

Strong Induction: Before we illustrate how to use strong induction, we state this principle again.

STRONG INDUCTION

To prove that $P(n)$ is true for all positive integers n , where $P(n)$ is a propositional function, we complete two steps:

BASIS STEP: We verify that the proposition $P(1)$ is true.

INDUCTIVE STEP: We show that the conditional statement $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k + 1)$ is true for all positive integers k .

Strong Induction:

EXAMPLE 1 (2 in book)

Show that if n is an integer greater than 1, then n can be written as the product of primes.

Solution: Let $P(n)$ be the proposition that n can be written as the product of primes.

BASIS STEP: $P(2)$ is true, because 2 can be written as the product of one prime, itself. (Note that $P(2)$ is the first case we need to establish.)

INDUCTIVE STEP: The inductive hypothesis is the assumption that $P(j)$ is true for all integers j with $2 \leq j \leq k$, that is, the assumption that j can be written as the product of primes whenever j is a positive integer at least 2 and not exceeding k . To complete the inductive step, it must be shown that $P(k+1)$ is true under this assumption, that is, that $k+1$ is the product of primes.

Strong Induction:

EXAMPLE 1 (2 in book)

Show that if n is an integer greater than 1, then n can be written as the product of primes.

Solution: Let $P(n)$ be the proposition that n can be written as the product of primes.

BASIS STEP: $P(2)$ is true, because 2 can be written as the product of one prime, itself. (Note that $P(2)$ is the first case we need to establish.)

INDUCTIVE STEP: The inductive hypothesis is the assumption that $P(j)$ is true for all integers j with $2 \leq j \leq k$, that is, the assumption that j can be written as the product of primes whenever j is a positive integer at least 2 and not exceeding k . To complete the inductive step, it must be shown that $P(k+1)$ is true under this assumption, that is, that $k+1$ is the product of primes.

Strong Induction:

There are two cases to consider, namely, when $k + 1$ is prime and when $k + 1$ is composite. If $k + 1$ is prime, we immediately see that $P(k + 1)$ is true. Otherwise, $k + 1$ is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b < k + 1$. Because both a and b are integers at least 2 and not exceeding k , we can use the inductive hypothesis to write both a and b as the product of primes. Thus, if $k + 1$ is composite, it can be written as the product of primes, namely, those primes in the factorization of a and those in the factorization of b .

Strong Induction

STRONG INDUCTION

Let b be a fixed integer and j a fixed positive integer. The form of strong induction we need tells us that $P(n)$ is true for all integers n with $n \geq b$ if we can complete these two steps:

BASIS STEP: We verify that the propositions $P(b), P(b+1), \dots, P(b+j)$ are true.

INDUCTIVE STEP: We show that $[P(b) \wedge P(b+1) \wedge \dots \wedge P(k)] \rightarrow P(k+1)$ is true for every integer $k \geq b+j$.

EXAMPLE

Give a recursive definition of the sequence $\{a_n\}_{n \in \mathbb{N}}$, where $a_0 = 1$, $a_1 = 1$ and $a_n = 2a_{n-1} + a_{n-2}$, for all integer $n > 1$. Show that a_n is a an odd integer for all nonnegative integers n .

Solution:

Well-Ordering

THE WELL-ORDERING PROPERTY Every nonempty set of nonnegative integers has a least element.

The well-ordering property can often be used directly in proofs.

EXAMPLE 2 (6 in book)

In a round-robin tournament every player plays every other player exactly once and each match has a winner and a loser. We say that the players p_1, p_2, \dots, p_m form a cycle if p_1 beats p_2 , p_2 beats p_3, \dots, p_{m-1} beats p_m , and p_m beats p_1 . Use the well-ordering principle to show that if there is a cycle of length m ($m \geq 3$) among the players in a round-robin tournament, there must be a cycle of three of these players.

Solution: We assume that there is no cycle of three players. Because there is at least one cycle in the round-robin tournament, the set of all positive integers n for which there is a cycle of length n is nonempty. By the well-ordering property, this set of positive integers has a least element k , which by assumption must be greater than three. Consequently, there exists a cycle of players $p_1, p_2, p_3, \dots, p_k$ and no shorter cycle exists.

Because there is no cycle of three players, we know that $k > 3$. Consider the first three elements of this cycle, p_1, p_2 , and p_3 . There are two possible outcomes of the match between p_1 and p_3 . If p_3 beats p_1 , it follows that p_1, p_2, p_3 is a cycle of length three, contradicting our assumption that there is no cycle of three players. Consequently, it must be the case that p_1 beats p_3 . This means that we can omit p_2 from the cycle $p_1, p_2, p_3, \dots, p_k$ to obtain the cycle $p_1, p_3, p_4, \dots, p_k$ of length $k - 1$, contradicting the assumption that the smallest cycle has length k . We conclude that there must be a cycle of length three.