3.6: Review of Proof Methods

This section is different from others in the text. It is meant primarily as a review of the proof methods studied in Chapter 3. So the first part of the section will be a description of some of the main proof techniques introduced in Chapter 3. The most important part of this section is the set of exercises since these exercises will provide an opportunity to use the proof techniques that we have studied so far.

We will now give descriptions of three of the most common methods used to prove a conditional statement.

**Direct Proof of a Conditional Statement \((P \to Q)\)**

- **When is it indicated?** This type of proof is often used when the hypothesis and the conclusion are both stated in a “positive” manner. That is, no negations are evident in the hypothesis and conclusion. That is, no negations are evident in the hypothesis and conclusion.

- **Description of the process.** Assume that \(\neg(P)\) is true and use this to conclude that \(\neg(Q)\) is true. That is, we use the forward-backward method and work forward from \(\neg(P)\) and backward from \(\neg(Q)\).

- **Why the process makes sense.** We know that the conditional statement \((P \to Q)\) is automatically true when the hypothesis is false. Therefore, because our goal is to prove that \(\neg(P \to Q)\) is true, there is nothing to do in the case that \(\neg(P)\) is false. Consequently, we may assume that \(\neg(P)\) is true. Then, in order for \(\neg(P \to Q)\) to be true, the conclusion \(\neg(Q)\) must also be true. (When \(\neg(P)\) is true, but \(\neg(Q)\) is false, \(\neg(P \to Q)\) is false.) Thus, we must use our assumption that \(\neg(P)\) is true to show that \(\neg(Q)\) is also true.

**Proof of a Conditional Statement \((P \to Q)\) Using the Contrapositive**

- **When is it indicated?** This type of proof is often used when both the hypothesis and the conclusion are stated in
the form of negations. This often works well if the conclusion contains the operator “or”; that is, if the conclusion is in the form of a disjunction. In this case, the negation will be a conjunction.

- **Description of the process.** We prove the logically equivalent statement \(\urcorner Q \to \urcorner P\). The forward-backward method is used to prove \(\urcorner Q \to \urcorner P\). That is, we work forward from \(\urcorner Q\) and backward from \(\urcorner P\).

- **Why the process makes sense.** When we prove \(\urcorner Q \to \urcorner P\), we are also proving \(P \to Q\) because these two statements are logically equivalent. When we prove the contrapositive of \(P \to Q\), we are doing a direct proof of \(\urcorner Q \to \urcorner P\). So we assume \(\urcorner Q\) because, when doing a direct proof, we assume the hypothesis, and \(\urcorner Q\) is the hypothesis of the contrapositive. We must show \(\urcorner P\) because it is the conclusion of the contrapositive.

**Proof of \(P \to Q\) Using a Proof by Contradiction**

- When is it indicated? This type of proof is often used when the conclusion is stated in the form of a negation, but the hypothesis is not. This often works well if the conclusion contains the operator “or”; that is, if the conclusion is in the form of a disjunction. In this case, the negation will be a conjunction.

- **Description of the process.** Assume \(P\) and \(\urcorner Q\) and work forward from these two assumptions until a contradiction is obtained.

- **Why the process makes sense.** The statement \(P \to Q\) is either true or false. In a proof by contradiction, we show that it is true by eliminating the only other possibility (that it is false). We show that \(P \to Q\) cannot be false by assuming it is false and reaching a contradiction. Since we assume that \(P \to Q\) is false, and the only way for a conditional statement to be false is for its hypothesis to be true and its conclusion to be false, we assume that \(P\) is true and that \(Q\) is false (or, equivalently, that \(\urcorner Q\) is true). When we reach a contradiction, we know that our original assumption that \(P \to Q\) is false is incorrect. Hence, \(P \to Q\) cannot be false, and so it must be true.

**Other Methods of Proof**

The methods of proof that were just described are three of the most common types of proof. However, we have seen other methods of proof and these are described below.

**Proofs that Use a Logical Equivalency**

As was indicated in Section 3.2, we can sometimes use a logical equivalency to help prove a statement. For example, in order to prove a statement of the form

\[P \to (Q \vee R)\]

it is sometimes possible to use the logical equivalency

\[(P \to (Q \vee R)) \equiv ([P \to Q) \to (Q \to R)]\]

We would then prove the statement

\[([P \to Q) \to (Q \to R)]\]

Most often, this would use a direct proof for statement (3.6.1) but other methods could also be used. Because of the logical equivalency, by proving statement (3.6.3), we have also proven the statement (3.6.1).
Proofs that Use Cases

When we are trying to prove a proposition or a theorem, we often run into the problem that there does not seem to be enough information to proceed. In this situation, we will sometimes use cases to provide additional assumptions for the forward process of the proof. When this is done, the original proposition is divided into a number of separate cases that are proven independently of each other. The cases must be chosen so that they exhaust all possibilities for the hypothesis of the original proposition. This method of case analysis is justified by the logical equivalency

\[(P \lor Q) \rightarrow R \equiv (P \rightarrow R) \land (Q \rightarrow R).\]

which was established in Preview Activity \(\PageIndex{1}\) in Section 3.4.

Constructive Proof

This is a technique that is often used to prove a so-called existence theorem. The objective of an existence theorem is to prove that a certain mathematical object exists. That is, the goal is usually to prove a statement of the form

There exists an \(\exists x\) such that \(P(x)\).

For a constructive proof of such a proposition, we actually name, describe, or explain how to construct some object in the universe that makes \(P(x)\) true.

Nonconstructive Proof

This is another type of proof that is often used to prove an existence theorem is the so-called nonconstructive proof. For this type of proof, we make an argument that an object in the universal set that makes \(P(x)\) true must exist but we never construct or name the object that makes \(P(x)\) true.

Exercises for Section 3.6

1. Let \(h\) and \(k\) be real numbers and let \(r\) be a positive number. The equation for a circle whose center is at the point \((h, k)\) and whose radius is \(r\) is

\[(x - h)^2 + (y - k)^2 = r^2.\]

We also know that if \(a\) and \(b\) are real numbers, then

- The point \((a, b)\) is inside the circle if \((a - h)^2 + (b - k)^2 < r^2\).
- The point \((a, b)\) is on the circle if \((a - h)^2 + (b - k)^2 = r^2\).
- The point \((a, b)\) is outside the circle if \((a - h)^2 + (b - k)^2 > r^2\).

Prove that all points on or inside the circle whose equation is \((x - 1)^2 + (y - 2)^2 = 4\) are inside the circle whose equation is \((x^2 + y^2 = 26)\).

2. Let \(r\) be a positive real number. The equation for a circle of radius \(r\) whose center is the origin is \(x^2 + y^2 = r^2\).
(a) Use implicit differentiation to determine \(\frac{dy}{dx}\).

(b) Let \(((a,b))\) be a point on the circle with \((a \neq 0)\) and \((b \neq 0)\). Determine the slope of the line tangent to the circle at the point \(((a,b))\).

(c) Prove that the radius of the circle to the point \(((a,b))\) is perpendicular to the line tangent to the circle at the point \(((a,b))\). Hint: Two lines (neither of which is horizontal) are perpendicular if and only if the products of their slopes is equal to 1.

3. Are the following statements true or false? Justify your conclusions.

(a) For each integer \(a\), if 3 does not divide \(a\), then 3 divides \(2a^2 + 1\).

(b) For each integer \(a\), if 3 divides \(2a^2 + 1\), then 3 does not divide \(a\).

(c) For each integer \(a\), 3 does not divide \(a\) if and only if 3 divides \(2a^2 + 1\).

4. Prove that for each real number \(x\) and each irrational number \(q\), \((x + q)\) is irrational or \((x - q)\) is irrational.

5. Prove that there exist irrational numbers \(u\) and \(v\) such that \((uv)\) is a rational number. Hint: We have proved that \((\sqrt{2})\) is irrational. For the real number \(q = \sqrt{2}^{\sqrt{2}}\), either \((q)\) is rational or \((q)\) is irrational. Use this disjunction to set up two cases.

6. Let \(a\) and \(b\) be natural numbers such that \(a^2 = b^3\). Prove each of the propositions in Parts (6a) through (6d).

(a) If \(a\) is even, then 4 divides \(a\).

(b) If 4 divides \(a\), then 4 divides \(b\).

(c) If 4 divides \(b\), then 8 divides \(a\).

(d) If \(a\) is even, then 8 divides \(a\).

(e) Give an example of natural numbers \(a\) and \(b\) such that \(a^2 = b^3\), but \(b\) is not divisible by 8.

7. Prove the following proposition:

Let \(a\) and \(b\) be integers with \((a \leq 0)\). If \(a\) does not divide \(b\), then the equation \((ax + bx + (b + a) = 0)\) does not have a solution that is a natural number. Hint: It may be necessary to factor a sum of cubes. Recall that

\([u^3 + v^3 = (u + v)(u^2 - uv + v^2)].\]

8. Recall that a Pythagorean triple consists of three natural numbers \(a\), \(b\), and \(c\) such that \((a + b < c)\) and \((a^2 + b^2 = c^2)\). Are the following propositions true or false? Justify your conclusions.

(a) For all \(a, b, c \in \mathbb{N}\) such that \((a + b < c)\), if \(a\), \(b\), and \(c\) form a Pythagorean triple, then 3 divides \(a\) or 3 divides \(b\).

(b) For all \(a, b, c \in \mathbb{N}\) such that \((a + b < c)\), if \(a\), \(b\), and \(c\) form a Pythagorean triple, then 5
divides \(a\) or 5 divides \(b\) or 5 divides \(c\).

9. (a) Prove that there exists a Pythagorean triple \(a\), \(b\), and \(c\), where \(a = 5\) and \(b\) and \(c\) are consecutive natural numbers.
(b) Prove that there exists a Pythagorean triple \(a\), \(b\), and \(c\), where \(a = 7\) and \(b\) and \(c\) are consecutive natural numbers.
(c) Let \(m\) be an odd natural number that is greater than 1. Prove that there exists a Pythagorean triple \(a\), \(b\), and \(c\), where \(a = m\) and \(b\) and \(c\) are consecutive natural numbers.

10. One of the most famous unsolved problems in mathematics is a conjecture made by Christian Goldbach in a letter to Leonhard Euler in 1742. The conjecture made in this letter is now known as \textbf{Goldbach’s Conjecture}. The conjecture is as follows: 
\textit{Every even integer greater than 2 can be expressed as the sum of two (not necessarily distinct) prime numbers.}
Currently, it is not known if this conjecture is true or false.

(a) Write 50, 142, and 150 as a sum of two prime numbers
(b) Prove the following:
If Goldbach’s Conjecture is true, then every integer greater than 5 can be written as a sum of three prime numbers.
(c) Prove the following:
If Goldbach’s Conjecture is true, then every odd integer greater than 7 can be written as a sum of three odd prime numbers.

11. Two prime numbers that differ by 2 are called \textbf{twin primes}. For example, 3 and 5 are twin primes, 5 and 7 are twin primes, and 11 and 13 are twin primes. Determine at least two other pairs of twin primes. Is the following proposition true or false? Justify your conclusion.

For all natural numbers \(p\) and \(q\) if \(p\) and \(q\) are twin primes other than 3 and 5, then \((pq + 1)\) is a perfect square and 36 divides \((pq + 1)\).

12. Are the following statements true or false? Justify your conclusions.

(a) For all integers \(a\) and \(b\), \((a + b)^2 \equiv (a^2 + b^2) \pmod{2}\).
(b) For all integers \(a\) and \(b\), \((a + b)^3 \equiv (a^3 + b^3) \pmod{3}\).
(c) For all integers \(a\) and \(b\), \((a + b)^4 \equiv (a^4 + b^4) \pmod{4}\).
(d) For all integers \(a\) and \(b\), \((a + b)^5 \equiv (a^5 + b^5) \pmod{5}\).

If any of the statements above are false, write a new statement of the following form that is true (and prove that it is true):

For all integers \(a\) and \(b\), \((a + b)^n \equiv (a^n + \text{something} + b^n) \pmod{n}\).

13. Let \(a\), \(b\), \(c\), and \(d\) be real numbers with \(a \neq 0\) and let \(f(x) = ax^3 + bx^2 + cx + d\).
(a) Determine the derivative and second derivative of the cubic function \( f \).

(b) Prove that the cubic function \( f \) has at most two critical points and has exactly one inflection point.

**Explorations and Activities**

14. **A Special Case of Fermat’s Last Theorem.** We have already seen examples of Pythagorean triples, which are natural numbers \( (a), (b), \) and \( (c) \) where \( a^2 + b^2 = c^2 \). For example, 3, 4, and 5 form a Pythagorean triple as do 5, 12, and 13. One of the famous mathematicians of the 17th century was Pierre de Fermat (1601 – 1665). Fermat made an assertion that for each natural number \( n \) with \( n \ge 3 \), there are no integers \( a, b, \) and \( c \) for which \( a^n + b^n = c^n \). This assertion was discovered in a margin of one of Fermat’s books after his death, but Fermat provided no proof. He did, however, state that he had discovered truly remarkable proof but the margin did not contain enough room for the proof.

This assertion became known as Fermat’s Last Theorem but it more properly should have been called Fermat’s Last Conjecture. Despite the efforts of mathematicians, this “theorem” remained unproved until Andrew Wiles, a British mathematician, first announced a proof in June of 1993. However, it was soon recognized that this proof had a serious gap, but a widely accepted version of the proof was published by Wiles in 1995. Wiles’ proof uses many concepts and techniques that were unknown at the time of Fermat. We cannot discuss the proof here, but we will explore and prove the following proposition, which is a (very) special case of Fermat’s Last Theorem.

**Proposition.** There do not exist prime numbers \( a, b, \) and \( c \) such that
\[ a^3 + b^3 = c^3. \]

Although Fermat’s Last Theorem implies this proposition is true, we will use a proof by contradiction to prove this proposition. For a proof by contradiction, we assume that

there exist prime numbers \( (a), (b), \) and \( (c) \) such that \( a^3 + b^3 = c^3 \).

Since 2 is the only even prime number, we will use the following cases: (1) \( a = b = 2 \); (2) \( a \) and \( b \) are both odd; and (3) one of \( a \) and \( b \) is odd and the other one is 2.

(a) Show that the case where \( a = b = 2 \) leads to a contradiction and hence, this case is not possible.
(b) Show that the case where \( a \) and \( b \) are both odd leads to a contradiction and hence, this case is not possible.
(c) We now know that one of \( a \) or \( b \) must be equal to 2. So we assume that \( b = 2 \) and that \( a \) is an odd prime. Substitute \( b = 2 \) into the equation \( b^3 = c^3 - a^3 \) and then factor the expression \( c^3 - a^3 \). Use this to obtain a contradiction.
(d) Write a complete proof of the proposition.

**Answer**

Add texts here. Do not delete this text first.