
Proving Non-conditional Statements

The past three chapters have introduced three major proof techniques: direct, contrapositive and contradiction. These three techniques are used to prove statements of the form “*If P , then Q .*” As we know, most theorems and propositions have this conditional form or they can be reworded to have this form. Thus the three main techniques are quite important. But some theorems and propositions cannot be put into conditional form. For example, some theorems have form “ *P if and only if Q .*” Such theorems are biconditional statements, not conditional statements. In this chapter we examine ways of proving theorems of this form. In addition to learning how to prove if-and-only-if theorems, we will also look at two other types of theorems.

7.1 If-And-Only-If Proof

Some propositions have the form

P if and only if Q .

We know from Section 2.4 that this statement asserts that **both** of the following two conditional statements are true.

If P , then Q .

If Q , then P .

So to prove “ *P if and only if Q ,*” we need to prove **two** conditional statements. Recall from Section 2.4 that $Q \Rightarrow P$ is called the *converse* of $P \Rightarrow Q$. Thus we need to prove both $P \Rightarrow Q$ and its converse. Since these are both conditional statements we may prove them with either direct, contrapositive or contradiction proof. Here is an outline.

Outline for If-And-Only-If Proof.

Proposition P if and only if Q .

Proof.

[Prove $P \Rightarrow Q$ using direct, contrapositive or contradiction proof.]

[Prove $Q \Rightarrow P$ using direct, contrapositive or contradiction proof.] ■

Let's start with a very simple example. You already know that an integer n is odd if and only if n^2 is odd, but let's prove it anyway, just to illustrate the outline. In this example we prove $(n \text{ is odd}) \Rightarrow (n^2 \text{ is odd})$ using direct proof and $(n^2 \text{ is odd}) \Rightarrow (n \text{ is odd})$ using contrapositive proof.

Proposition The integer n is odd if and only if n^2 is odd.

Proof. First we show that n being odd implies that n^2 is odd. Suppose n is odd. Then, by definition of an odd number, $n = 2a + 1$ for some integer a . Thus $n^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$. This expresses n^2 as twice an integer, plus 1, so n^2 is odd.

Conversely, we need to prove that n^2 being odd implies that n is odd. We use contrapositive proof. Suppose n is not odd. Then n is even, so $n = 2a$ for some integer a (by definition of an even number). Thus $n^2 = (2a)^2 = 2(2a^2)$, so n^2 is even because it's twice an integer. Thus n^2 is not odd. We've now proved that if n is not odd, then n^2 is not odd, and this is a contrapositive proof that if n^2 is odd then n is odd. ■

In proving " P if and only if Q ," you should always begin a new paragraph when starting the proof of $Q \Rightarrow P$. Since this is the converse of $P \Rightarrow Q$, it's a good idea to begin the paragraph with the word "Conversely" (as we did above) to remind the reader that you've finished the first part of the proof and are moving on to the second. Likewise, it's a good idea to remind the reader of exactly what statement that paragraph is proving.

The next example uses direct proof in both parts of the proof.

Proposition Suppose a and b are integers. Then $a \equiv b \pmod{6}$ if and only if $a \equiv b \pmod{2}$ and $a \equiv b \pmod{3}$.

Proof. First we prove that if $a \equiv b \pmod{6}$, then $a \equiv b \pmod{2}$ and $a \equiv b \pmod{3}$. Suppose $a \equiv b \pmod{6}$. This means $6|(a - b)$, so there is an integer n for which

$$a - b = 6n.$$

From this we get $a - b = 2(3n)$, which implies $2|(a - b)$, so $a \equiv b \pmod{2}$. But we also get $a - b = 3(2n)$, which implies $3|(a - b)$, so $a \equiv b \pmod{3}$. Therefore $a \equiv b \pmod{2}$ and $a \equiv b \pmod{3}$.

Conversely, suppose $a \equiv b \pmod{2}$ and $a \equiv b \pmod{3}$. Since $a \equiv b \pmod{2}$ we get $2|(a - b)$, so there is an integer k for which $a - b = 2k$. Therefore $a - b$ is even. Also, from $a \equiv b \pmod{3}$ we get $3|(a - b)$, so there is an integer ℓ for which

$$a - b = 3\ell.$$

But since we know $a - b$ is even, it follows that ℓ must be even also, for if it were odd then $a - b = 3\ell$ would be odd. (Because $a - b$ would be the product of two odd integers.) Hence $\ell = 2m$ for some integer m . Thus $a - b = 3\ell = 3 \cdot 2m = 6m$. This means $6|(a - b)$, so $a \equiv b \pmod{6}$. ■

Since if-and-only-if proofs simply combine methods with which we are already familiar, we will not do any further examples in this section. However it is of utmost importance that you practice your skill on some of this chapter's exercises.

7.2 Equivalent Statements

In other courses you will sometimes encounter a certain kind of theorem that is neither a conditional nor a biconditional statement. Instead, it asserts that a list of statements is “equivalent.” You saw this (or will see it) in your linear algebra textbook, which featured the following theorem.

Theorem Suppose A is an $n \times n$ matrix. The following statements are equivalent.

- (a) The matrix A is invertible.
- (b) The equation $A\mathbf{x} = \mathbf{b}$ has a unique solution for every $\mathbf{b} \in \mathbb{R}^n$.
- (c) The equation $A\mathbf{x} = \mathbf{0}$ has only the trivial solution.
- (d) The reduced row echelon form of A is I_n .
- (e) $\det(A) \neq 0$.
- (f) Matrix A does not have $\mathbf{0}$ as an eigenvector.

When a theorem asserts that a list of statements is “equivalent,” it is asserting that either the statements are all true, or they are all false. Thus the above theorem tells us that whenever we are dealing with a particular $n \times n$ matrix A , then either the statements (a) through (f) are all true for A , or statements (a) through (f) are all false for A . For example, if we happen to know that $\det(A) \neq 0$, the theorem assures us that in addition to statement (e) being true, **all** the statements (a) through (f) are true. On the other hand, if it happens that $\det(A) = 0$, the theorem tells us that all statements (a) through (f) are false. In this way, the theorem multiplies our knowledge of A by a factor of six. Obviously that can be very useful.

What method would we use to prove such a theorem? In a certain sense, the above theorem is like an if-and-only-if theorem. An if-and-only-if theorem of form $P \Leftrightarrow Q$ asserts that P and Q are either both true or both false, that is that P and Q are equivalent. To prove $P \Leftrightarrow Q$ we prove $P \Rightarrow Q$ followed by $Q \Rightarrow P$, essentially making a “cycle” of implications from P to Q

and back to P . Similarly, one approach to proving the theorem cited at the beginning of this section would be to prove $(\mathbf{a}) \Rightarrow (\mathbf{b})$, then $(\mathbf{b}) \Rightarrow (\mathbf{c})$, then $(\mathbf{c}) \Rightarrow (\mathbf{d})$, then $(\mathbf{d}) \Rightarrow (\mathbf{e})$, then $(\mathbf{e}) \Rightarrow (\mathbf{f})$, and finally $(\mathbf{f}) \Rightarrow (\mathbf{a})$. This pattern is illustrated below.

$$\begin{array}{ccccc} (a) & \Rightarrow & (b) & \Rightarrow & (c) \\ & \Uparrow & & & \Downarrow \\ (f) & \Leftarrow & (e) & \Leftarrow & (d) \end{array}$$

Notice that if these six implications have been proved, then it really does follow that the statements (a) through (f) are either all true or all false. If one of them is true then the circular chain of implications forces them all to be true. On the other hand, if one of them (say (c)) is false, the fact that $(\mathbf{b}) \Rightarrow (\mathbf{c})$ is true forces (b) to be false. This combined with the truth of $(\mathbf{a}) \Rightarrow (\mathbf{b})$ makes (a) false, and so on counterclockwise around the circle.

Thus to prove that n statements are equivalent, it suffices to prove n conditional statements showing each statement implies another, in circular pattern. But it is not necessary that the pattern be circular. The following schemes would also do the job.

$$\begin{array}{ccccc} (a) & \Rightarrow & (b) & \Leftarrow & (c) \\ & \Uparrow & & \Downarrow & \\ (f) & \Leftarrow & (e) & \Leftarrow & (d) \end{array}$$

$$\begin{array}{ccccc} (a) & \Leftarrow & (b) & \Leftarrow & (c) \\ & & \Updownarrow & & \\ (f) & \Leftarrow & (e) & \Leftarrow & (d) \end{array}$$

However, a circular pattern results in the fewest number of conditional statements that must be proved. Whatever the pattern, each conditional statement can be proved with either direct, contrapositive or contradiction proof.

Though we shall not do any of these proofs in this text, you are sure to encounter them in subsequent courses.

7.3 Existence Proofs

Up until this point, we have dealt with proving conditional statements or with statements that can be expressed with two or more conditional statements. Generally, these conditional statements have form $P(x) \Rightarrow Q(x)$. (Possibly with more than one variable.) We saw in Section 2.8 that this can be interpreted as a universally quantified statement $\forall x, P(x) \Rightarrow Q(x)$.

Thus, conditional statements are universally quantified statements, so in proving a conditional statement—whether we use direct, contrapositive or contradiction proof—we are really proving a universally quantified statement.

But how would we prove an *existentially* quantified statement? What technique would we employ to prove a theorem of the following form?

$$\exists x, R(x)$$

This statement asserts that there exists some specific object x for which $R(x)$ is true. To prove $\exists x, R(x)$ is true, all we would have to do is find and display an *example* of a specific x that makes $R(x)$ true.

Though most theorems and propositions are conditional (or if-and-only-if) statements, a few have the form $\exists x, R(x)$. Such statements are called **existence statements**, and theorems that have this form are called **existence theorems**. To prove an existence theorem, all you have to do is provide a particular example that shows it is true. This is often quite simple. (But not always!) Here are some examples.

Proposition There exists an even prime number.

Proof. Observe that 2 is an even prime number. ■

Proposition There exists an integer that can be expressed as the sum of two perfect cubes in two different ways.

Proof. Consider the number 1729. Note that $1^3 + 12^3 = 1729$ and $9^3 + 10^3 = 1729$. Thus the number 1729 can be expressed as the sum of two perfect cubes in two different ways. ■

Sometimes in the proof of an existence statement, a little verification is needed to show that the example really does work. For example, the above proof would be incomplete if we just asserted that 1729 can be written as a sum of two cubes in two ways without showing *how* this is possible.

WARNING: Although an example suffices to prove an existence statement, a mere example *never* proves a conditional statement.

Exercises for Chapter 7

Prove the following statements. These exercises are cumulative, covering all techniques addressed in Chapters 4–7.

1. Suppose $x \in \mathbb{Z}$. Then x is even if and only if $3x + 5$ is odd.
2. Suppose $x \in \mathbb{Z}$. Then x is odd if and only if $3x + 6$ is odd.
3. Given an integer a , then $a^3 + a^2 + a$ is even if and only if a is even.
4. Given an integer a , then $a^2 + 4a + 5$ is odd if and only if a is even.
5. An integer a is odd if and only if a^3 is odd.
6. Suppose $x, y \in \mathbb{R}$. Then $x^3 + x^2y = y^2 + xy$ if and only if $y = x^2$ or $y = -x$.
7. Suppose $x, y \in \mathbb{R}$. Then $(x + y)^2 = x^2 + y^2$ if and only if $x = 0$ or $y = 0$.
8. Suppose $a, b \in \mathbb{Z}$. Prove that $a \equiv b \pmod{10}$ if and only if $a \equiv b \pmod{2}$ and $a \equiv b \pmod{5}$.
9. Suppose $a \in \mathbb{Z}$. Prove that $14|a$ if and only if $7|a$ and $2|a$.
10. If $a \in \mathbb{Z}$, then $a^3 \equiv a \pmod{3}$.
11. Suppose $a, b \in \mathbb{Z}$. Prove that $(a - 3)b^2$ is even if and only if a is odd or b is even.
12. There exist a positive real number x for which $x^2 < \sqrt{x}$.
13. Suppose $a, b \in \mathbb{Z}$. If $a + b$ is odd, then $a^2 + b^2$ is odd.
14. Suppose $a \in \mathbb{Z}$. Then $a^2|a$ if and only if $a \in \{-1, 0, 1\}$.
15. Suppose $a, b \in \mathbb{Z}$. Prove that $a + b$ is even if and only if a and b have the same parity.
16. Suppose $a, b \in \mathbb{Z}$. If ab is odd, then $a^2 + b^2$ is even.
17. There is a prime number between 90 and 100.
18. There is a set X for which $\mathbb{N} \in X$ and $\mathbb{N} \subseteq X$.
19. If $n \in \mathbb{N}$, then $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \dots + 2^n = 2^{n+1} - 1$.
20. There exists an $n \in \mathbb{N}$ for which $11|(2^n - 1)$.
21. Every real solution of $x^3 + x + 3 = 0$ is irrational.
22. If $n \in \mathbb{Z}$, then $4|n^2$ or $4|(n^2 - 1)$.
23. Suppose a, b and c are integers. If $a|b$ and $a|(b^2 - c)$, then $a|c$.
24. If $a \in \mathbb{Z}$, then $4 \nmid (a^2 - 3)$.
25. If $p > 1$ is an integer and $n \nmid p$ for each integer n for which $2 \leq n \leq \sqrt{p}$, then p is prime.
26. The product of any n consecutive positive integers is divisible by $n!$.
27. Suppose $a, b \in \mathbb{Z}$. If $a^2 + b^2$ is a perfect square, then a and b are not both odd.