CHAPTER 7

Proving Non-Conditional Statements

The last three chapters 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 to prove them. 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 conditional statements are true:

If P, then Q.
If Q, then P.

So to prove *"P if and only if Q,"* we must 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 is odd)⇒(n^2 is odd) using direct proof and (n^2 is odd)⇒(n 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 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 $6 \mid (a-b)$, so there is an integer n for which

$$a-b = 6n.$$

From this we get $a-b = 2(3n)$, which implies $2 \mid (a-b)$, so $a \equiv b \pmod{2}$. But we also get $a-b = 3(2n)$, which implies $3 \mid (a-b)$, 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 $2 \mid (a-b)$, 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 $3 \mid (a-b)$, 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 $6 \mid (a-b)$, 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) The matrix A does not have 0 as an eigenvalue.

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 about the $n \times n$ matrix would be to prove the conditional statement $(a) \Rightarrow (b)$, then $(b) \Rightarrow (c)$, then $(c) \Rightarrow (d)$, then $(d) \Rightarrow (e)$, then $(e) \Rightarrow (f)$ and finally $(f) \Rightarrow (a)$. This pattern is illustrated below.

$$\begin{tikzcd}
(a) \arrow[r, Rightarrow] & (b) \arrow[r, Rightarrow] & (c) \arrow[d, Rightarrow] \\
(f) \arrow[u, Rightarrow] & (e) \arrow[l, Rightarrow] & (d) \arrow[l, Rightarrow]
\end{tikzcd}$$

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 $(b) \Rightarrow (c)$ is true forces (b) to be false. This combined with the truth of $(a) \Rightarrow (b)$ 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:

$$\begin{tikzcd}
(a) \arrow[r, Rightarrow] & (b) \arrow[r, Leftrightarrow] \arrow[d, Rightarrow] & (c) \\
(f) \arrow[u, Rightarrow] & (e) \arrow[l, Rightarrow] \arrow[r, Leftrightarrow] & (d)
\end{tikzcd}$$

$$\begin{tikzcd}
(a) \arrow[r, Leftrightarrow] & (b) \arrow[r, Leftrightarrow] \arrow[d, Leftrightarrow] & (c) \\
(f) \arrow[r, Leftrightarrow] & (e) \arrow[r, Leftrightarrow] & (d)
\end{tikzcd}$$

But a circular pattern yields the fewest 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; Existence and Uniqueness 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. ■

Admittedly, this last proposition was a bit of an oversimplification. The next one is slightly more challenging.

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 single example does not prove a conditional statement.

Often an existence statement will be embedded inside of a conditional statement. Consider the following. (Recall the definition of gcd on page 90.)

If $a,b \in \mathbb{N}$, then there exist integers k and ℓ for which $\gcd(a,b) = ak+b\ell$.

This is a conditional statement that has the form

$$a,b \in \mathbb{N} \implies \exists\, k,\ell \in \mathbb{Z},\ \gcd(a,b) = ak+b\ell.$$

To prove it with direct proof, we would first assume that $a,b \in \mathbb{N}$, then prove the existence statement $\exists\, k,\ell \in \mathbb{Z}$, $\gcd(a,b) = ak+b\ell$. That is, we would produce two integers k and ℓ (which depend on a and b) for which $\gcd(a,b) = ak+b\ell$. Let's carry out this plan. (We will use this fundamental proposition several times later, so it is given a number.)

Proposition 7.1 If $a,b \in \mathbb{N}$, then there exist integers k and ℓ for which $\gcd(a,b) = ak+b\ell$.

Proof. (Direct) Suppose $a,b \in \mathbb{N}$. Consider the set $A = \{ax+by : x,y \in \mathbb{Z}\}$. This set contains both positive and negative integers, as well as 0. (Reason: Let $y=0$ and let x range over all integers. Then $ax+by = ax$ ranges over all multiples of a, both positive, negative and zero.) Let d be the smallest positive element of A. Then, because d is in A, it must have the form $d = ak+b\ell$ for some specific $k,\ell \in \mathbb{Z}$.

To finish, we will show $d = \gcd(a,b)$. We will first argue that d is a common divisor of a and b, and then that it is the *greatest* common divisor.

To see that $d \mid a$, use the division algorithm (page 29) to write $a = qd+r$ for integers q and r with $0 \le r < d$. The equation $a = qd+r$ yields

$$\begin{aligned} r &= a-qd \\ &= a-q(ak+b\ell) \\ &= a(1-qk)+b(-q\ell). \end{aligned}$$

Therefore r has form $r = ax+by$, so it belongs to A. But $0 \le r < d$ and d is the smallest positive number in A, so r can't be positive; hence $r=0$. Updating our equation $a = qd+r$, we get $a = qd$, so $d \mid a$. Repeating this argument with $b = qd+r$ shows $d \mid b$. Thus d is indeed a common divisor of a and b. It remains to show that it is the *greatest* common divisor.

As $\gcd(a,b)$ divides a and b, we have $a = \gcd(a,b)\cdot m$ and $b = \gcd(a,b)\cdot n$ for some $m,n \in \mathbb{Z}$. So $d = ak+b\ell = \gcd(a,b)\cdot mk + \gcd(a,b)\cdot n\ell = \gcd(a,b)\big(mk+n\ell\big)$, and thus d is a multiple of $\gcd(a,b)$. Therefore $d \ge \gcd(a,b)$. But d can't be a larger common divisor of a and b than $\gcd(a,b)$, so $d = \gcd(a,b)$. ■

We conclude this section with a discussion of so-called *uniqueness proofs*. Some existence statements have form "*There is a* unique x *for which* $P(x)$." Such a statement asserts that there is *exactly one* example x for which $P(x)$ is true. To prove it, you must produce an example $x = d$ for which $P(d)$ is true, **and** you must show that d is the only such example. The next proposition illustrates this. In essence, it asserts that the set $\{ax+by : x,y \in \mathbb{Z}\}$ consists precisely of all the multiples of $\gcd(a,b)$.

Proposition Suppose $a,b \in \mathbb{N}$. Then there exists a unique $d \in \mathbb{N}$ for which: An integer m is a multiple of d if and only if $m = ax+by$ for some $x,y \in \mathbb{Z}$.

Proof. Suppose $a,b \in \mathbb{N}$. Let $d = \gcd(a,b)$. We now show that an integer m is a multiple of d if and only if $m = ax+by$ for some $x,y \in \mathbb{Z}$. Let $m = dn$ be a multiple of d. By Proposition 7.1 (on the previous page), there are integers k and ℓ for which $d = ak+b\ell$. Then $m = dn = (ak+b\ell)n = a(kn)+b(\ell n)$, so $m = ax+by$ for integers $x = kn$ and $y = \ell n$.

Conversely, suppose $m = ax+by$ for some $x,y \in \mathbb{Z}$. Since $d = \gcd(a,b)$ is a divisor of both a and b, we have $a = dc$ and $b = de$ for some $c,e \in \mathbb{Z}$. Then $m = ax+by = dcx+dey = d(cx+ey)$, and this is a multiple of d.

We have now shown that there is a natural number d with the property that m is a multiple of d if and only if $m = ax+by$ for some $x,y \in \mathbb{Z}$. It remains to show that d is the *unique* such natural number. To do this, suppose d' is *any* natural number with the property that d has:

$$m \text{ is a multiple of } d' \iff m = ax+by \text{ for some } x,y \in \mathbb{Z}. \tag{7.1}$$

We next argue that $d' = d$; that is, d is the *unique* natural number with the stated property. Because of (7.1), $m = a\cdot 1+b\cdot 0 = a$ is a multiple of d'. Likewise $m = a\cdot 0+b\cdot 1 = b$ is a multiple of d'. Hence a and b are both multiples of d', so d' is a common divisor of a and b, and therefore

$$d' \le \gcd(a,b) = d.$$

But also, by (7.1), the multiple $m = d'\cdot 1 = d'$ of d' can be expressed as $d' = ax+by$ for some $x,y \in \mathbb{Z}$. As noted in the second paragraph of the proof, $a = dc$ and $b = de$ for some $c,e \in \mathbb{Z}$. Thus $d' = ax+by = dcx+dey = d(cx+ey)$, so d' is a multiple d. As d' and d are both positive, it follows that

$$d \le d'.$$

We've now shown that $d' \le d$ and $d \le d'$, so $d = d'$. The proof is complete. ■

7.4 Constructive Versus Non-Constructive Proofs

Existence proofs fall into two categories: constructive and non-constructive. Constructive proofs display an explicit example that proves the theorem; non-constructive proofs prove an example exists without actually giving it. We illustrate the difference with two proofs of the same fact: There exist *irrational* numbers x and y (possibly equal) for which x^y is *rational*.

Proposition There exist irrational numbers x, y for which x^y is rational.

Proof. Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We know y is irrational, but it is not clear whether x is rational or irrational. On one hand, if x is irrational, then we have an irrational number to an irrational power that is rational:

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^{2} = 2.$$

On the other hand, if x is rational, then $y^y = \sqrt{2}^{\sqrt{2}} = x$ is rational. Either way, we have a irrational number to an irrational power that is rational. ■

The above is a classic example of a **non-constructive** proof. It shows that there exist irrational numbers x and y for which x^y is rational without actually producing (or constructing) an example. It convinces us that one of $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$ or $\sqrt{2}^{\sqrt{2}}$ is an irrational number to an irrational power that is rational, but it does not say which one is the correct example. It thus proves that an example exists without explicitly stating one.

Next comes a **constructive proof** of this statement, one that produces (or constructs) two explicit irrational numbers x, y for which x^y is rational.

Proposition There exist irrational numbers x, y for which x^y is rational.

Proof. Let $x = \sqrt{2}$ and $y = \log_2 9$. Then

$$x^y = \sqrt{2}^{\log_2 9} = \sqrt{2}^{\log_2 3^2} = \sqrt{2}^{2\log_2 3} = \left(\sqrt{2}^{2}\right)^{\log_2 3} = 2^{\log_2 3} = 3.$$

As 3 is rational, we have shown that $x^y = 3$ is rational.

We know that $x = \sqrt{2}$ is irrational. The proof will be complete if we can show that $y = \log_2 9$ is irrational. Suppose for the sake of contradiction that $\log_2 9$ is rational, so there are integers a and b for which $\frac{a}{b} = \log_2 9$. This means $2^{a/b} = 9$, so $\left(2^{a/b}\right)^b = 9^b$, which reduces to $2^a = 9^b$. But 2^a is even, while 9^b is odd (because it is the product of the odd number 9 with itself b times). This is a contradiction; the proof is complete. ■

This existence proof has inside of it a separate proof (by contradiction) that $\log_2 9$ is irrational. Such combinations of proof techniques are, of course, typical.

Be alert to constructive and non-constructive proofs as you read proofs in other books and articles, as well as to the possibility of crafting such proofs of your own.

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 $14 \mid a$ if and only if $7 \mid a$ and $2 \mid a$.

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 $a^2 \mid a$ 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 $2^0+2^1+2^2+2^3+2^4+\cdots+2^n = 2^{n+1}-1$.

20. There exists an $n \in \mathbb{N}$ for which $11 \mid (2^n-1)$.

21. Every real solution of $x^3+x+3=0$ is irrational.

22. If $n \in \mathbb{Z}$, then $4 \mid n^2$ or $4 \mid (n^2-1)$.

23. Suppose a, b and c are integers. If $a \mid b$ and $a \mid (b^2-c)$, then $a \mid c$.

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.

28. Prove the division algorithm: If $a, b \in \mathbb{N}$, there exist *unique* integers q, r for which $a = bq + r$, and $0 \leq r < b$. (A proof of existence is given in Section 1.9, but uniqueness needs to be established too.)

29. If $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.
(Suggestion: Use the proposition on page 126.)

30. Suppose $a, b, p \in \mathbb{Z}$ and p is prime. Prove that if $p \mid ab$ then $p \mid a$ or $p \mid b$.
(Suggestion: Use the proposition on page 126.)

31. If $n \in \mathbb{Z}$, then $\gcd(n, n+1) = 1$.

32. If $n \in \mathbb{Z}$, then $\gcd(n, n+2) \in \{1, 2\}$.

33. If $n \in \mathbb{Z}$, then $\gcd(2n+1, 4n^2+1) = 1$.

34. If $\gcd(a,c) = \gcd(b,c) = 1$, then $\gcd(ab, c) = 1$.
(Suggestion: Use the proposition on page 126.)

35. Suppose $a, b \in \mathbb{N}$. Then $a = \gcd(a,b)$ if and only if $a \mid b$.

36. Suppose $a, b \in \mathbb{N}$. Then $a = \operatorname{lcm}(a,b)$ if and only if $b \mid a$.