Chapter 13

Proving Non-Conditional Statements

We have learned three main proof methods: direct, contrapositive and contradiction. These methods are used to prove statements of the form *"If P, then Q."* As most propositions have this conditional form (or can be reworded to have it), the three main methods are quite important. But some propositions are not conditional statements. For example, they may have form *"P if and only if Q."* These are biconditional statements, not conditional statements. In this chapter we examine ways to prove such statements, and we will also look at two other types of theorems.

13.1 If-and-Only-If Proof

Some propositions have the form

P if and only if Q.

We know from Section 3.4 that this statement asserts that **both** of the following conditional statements are true:

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

So proving *"P if and only if Q,"* involves proving **two** conditional statements. Recall from Section 3.4 that $Q \Rightarrow P$ is called the *converse* of $P \Rightarrow Q$. Thus we need to prove both $P \Rightarrow Q$ and its converse. These are both conditional statements and can be proved with 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. We will prove (n is odd)$\Rightarrow$(n^2 is odd) with direct proof and (n^2 is odd)$\Rightarrow$(n is odd) with contrapositive proof.

Proposition. An 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. Also it's good to remind the reader of what statement that paragraph will prove.

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.

13.2 Equivalent Statements

In other courses you will may encounter a type of theorem that is neither conditional nor biconditional. 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.

So 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 work:

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

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

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.

13.3 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 5.2 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.

Most theorems and propositions are conditional (or if-and-only-if) statements, but 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 easy. (But not always!) Some examples follow.

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.

Assumption 13.1. There exists an integer that can be expressed as the sum of two perfect cubes in two different ways.

Proof. Consider 1729. Note that $1^3 + 12^3 = 1729$ and $9^3 + 10^3 = 1729$. So 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 in a conditional statement. Consider the following. (Recall the definition of gcd on page 242.)

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 13.1. *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 215) to write $a = qd + r$ for integers q and r with $0 \leq r < d$. 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 $0 \leq r < d$ 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 $d \geq \gcd(a, b)$. 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 $\big\{ax + by : x, y \in \mathbb{Z}\big\}$ consists precisely of all the multiples of $\gcd(a, b)$.

Proposition. Suppose $a, b \in \mathbb{N}$. Then there exists a unique $d \in \mathbb{N}$ with following property: 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 13.1 (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:

$$m \text{ is a multiple of } d' \iff m = ax + by \text{ for some } x, y \in \mathbb{Z}. \tag{13.1}$$

We next argue that $d' = d$; that is, d is the *unique* natural number with the stated property. Because of (13.1), $m = a \cdot 1 + b \cdot 0 = a$ 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

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

But also, by (13.1), 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

$$d \leq d'.$$

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

13.4 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 $\big(\sqrt{2}^{\sqrt{2}}\big)^{\sqrt{2}}$ 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 13

Prove the following statements. These exercises are cumulative, covering all techniques addressed in Chapters 9–13.

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 $x^3 + x^2 y = y^2 + xy$ 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 2.9, but uniqueness needs to be established too.)

29. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$. (Suggestion: Use Proposition 13.1.)

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 Proposition 13.1.)

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 $\gcd(ab, c) = 1$. (Hint: Use Proposition 13.1.)

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 $b \mid a$.

37. Suppose A and B are sets. Prove $A \subseteq B$ if and only if $A - B = \emptyset$.

38. Let A and B be sets. Prove that $A \subseteq B$ if and only if $A \cap B = A$.

39. Suppose $A \neq \emptyset$. Prove that $A \times B \subseteq A \times C$, if and only if $B \subseteq C$.

Solutions for Chapter 13

1. Suppose $x \in \mathbb{Z}$. Then x is even if and only if $3x+5$ is odd.

Proof. We first use direct proof to show that if x is even, then $3x+5$ is odd. If x is even, then $x = 2n$ for some integer n, so $3x+5 = 3(2n)+5 = 6n+5 = 6n+4+1 = 2(3n+2)+1$. Thus $3x+5$ is odd because it has form $2k+1$, where $k = 3n+2 \in \mathbb{Z}$.

Conversely, we need to show that if $3x+5$ is odd, then x is even. We will prove this using contrapositive proof. Suppose x is *not* even. Then x is odd, so $x = 2n+1$ for some integer n. Thus $3x+5 = 3(2n+1)+5 = 6n+8 = 2(3n+4)$. This means $3x+5$ is twice the integer $3n+4$, so $3x+5$ is even, not odd. □

3. Given an integer a, then a^3+a^2+a is even if and only if a is even.

Proof. First we will prove that if a^3+a^2+a is even then a is even. This is done with contrapositive proof. Suppose a is not even. Then a is odd, so there is an integer n for which $a = 2n+1$. Then

$$\begin{aligned} a^3+a^2+a &= (2n+1)^3 + (2n+1)^2 + (2n+1) \\ &= 8n^3+12n^2+6n+1+4n^2+4n+1+2n+1 \\ &= 8n^3+16n^2+12n+2+1 \\ &= 2(4n^3+8n^2+6n+1)+1. \end{aligned}$$

This expresses a^3+a^2+a as twice an integer plus 1, so a^3+a^2+a is odd, not even. We have now shown that if a^3+a^2+a is even then a is even.

Conversely, we need to show that if a is even, then a^3+a^2+a is even. We will use direct proof. Suppose a is even, so $a = 2n$ for some integer n. Then $a^3+a^2+a = (2n)^3+(2n)^2+2n = 8n^3+4n^2+2n = 2(4n^3+2n^2+n)$. Therefore, a^3+a^2+a is even because it's twice an integer. □

5. An integer a is odd if and only if a^3 is odd.

Proof. Suppose that a is odd. Then $a = 2n+1$ for some integer n, and $a^3 = (2n+1)^3 = 8n^3+12n^2+6n+1 = 2(4n^3+6n^2+3n)+1$. This shows that a^3 is twice an integer, plus 1, so a^3 is odd. Thus we've proved that if a is odd then a^3 is odd.

Conversely we need to show that if a^3 is odd, then a is odd. For this we employ contrapositive proof. Suppose a is not odd. Thus a is even, so $a = 2n$ for some integer n. Then $a^3 = (2n)^3 = 8n^3 = 2(4n^3)$ is even (not odd). □

7. Suppose $x, y \in \mathbb{R}$. Then $(x+y)^2 = x^2+y^2$ if and only if $x = 0$ or $y = 0$.

Proof. First we prove with direct proof that if $(x+y)^2 = x^2+y^2$, then $x = 0$ or $y = 0$. Suppose $(x+y)^2 = x^2+y^2$. From this we get $x^2+2xy+y^2 = x^2+y^2$, so $2xy = 0$, and hence $xy = 0$. Thus $x = 0$ or $y = 0$.

Conversely, we need to show that if $x = 0$ or $y = 0$, then $(x+y)^2 = x^2+y^2$. This will be done with cases.
Case 1. If $x = 0$ then $(x+y)^2 = (0+y)^2 = y^2 = 0^2+y^2 = x^2+y^2$.

Case 2. If $y = 0$ then $(x+y)^2 = (x+0)^2 = x^2 = x^2 + 0^2 = x^2 + y^2$.
Either way, we have $(x+y)^2 = x^2 + y^2$. □

9. Suppose $a \in \mathbb{Z}$. Prove that $14 \mid a$ if and only if $7 \mid a$ and $2 \mid a$.

Proof. First we prove that if $14 \mid a$, then $7 \mid a$ and $2 \mid a$. Direct proof is used. Suppose $14 \mid a$. This means $a = 14m$ for some integer m. Therefore $a = 7(2m)$, which means $7 \mid a$, and also $a = 2(7m)$, which means $2 \mid a$. Thus $7 \mid a$ and $2 \mid a$.

Conversely, we need to prove that if $7 \mid a$ and $2 \mid a$, then $14 \mid a$. Once again direct proof if used. Suppose $7 \mid a$ and $2 \mid a$. Since $2 \mid a$ it follows that $a = 2m$ for some integer m, and that in turn implies that a is even. Since $7 \mid a$ it follows that $a = 7n$ for some integer n. Now, since a is known to be even, and $a = 7n$, it follows that n is even (if it were odd, then $a = 7n$ would be odd). Thus $n = 2p$ for an appropriate integer p, and plugging $n = 2p$ back into $a = 7n$ gives $a = 7(2p)$, so $a = 14p$. Therefore $14 \mid a$. □

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.

Proof. First we will prove that if $(a-3)b^2$ is even, then a is odd or b is even. For this we use contrapositive proof. Suppose it is not the case that a is odd or b is even. Then by DeMorgan's law, a is even and b is odd. Thus there are integers m and n for which $a = 2m$ and $b = 2n+1$. Now observe $(a-3)b^2 = (2m-3)(2n+1)^2 = (2m-3)(4n^2+4n+1) = 8mn^2+8mn+2m-12n^2-12n-3 = 8mn^2+8mn+2m-12n^2-12n-4+1 = 2(4mn^2+4mn+m-6n^2-6n-2)+1$. This shows $(a-3)b^2$ is odd, so it's not even.

Conversely, we need to show that if a is odd or b is even, then $(a-3)b^2$ is even. For this we use direct proof, with cases.
Case 1. Suppose a is odd. Then $a = 2m+1$ for some integer m. Thus $(a-3)b^2 = (2m+1-3)b^2 = (2m-2)b^2 = 2(m-1)b^2$. Thus in this case $(a-3)b^2$ is even.
Case 2. Suppose b is even. Then $b = 2n$ for some integer n. Thus $(a-3)b^2 = (a-3)(2n)^2 = (a-3)4n^2 = 2(a-3)2n^2 =$. Thus in this case $(a-3)b^2$ is even.
Therefore, in any event, $(a-3)b^2$ is even. □

13. Suppose $a, b \in \mathbb{Z}$. If $a+b$ is odd, then a^2+b^2 is odd.
Hint: Use direct proof. Suppose $a+b$ is odd. Argue that this means a and b have opposite parity. Then use cases.

15. Suppose $a, b \in \mathbb{Z}$. Prove that $a+b$ is even if and only if a and b have the same parity.

Proof. First we will show that if $a+b$ is even, then a and b have the same parity. For this we use contrapositive proof. Suppose it is not the case that a and b have the same parity. Then one of a and b is even and the other is odd. Without loss of generality, let's say that a is even and b is odd. Thus there are integers m and n for which $a = 2m$ and $b = 2n+1$. Then $a+b = 2m+2n+1 = 2(m+n)+1$, so $a+b$ is odd, not even.

Conversely, we need to show that if a and b have the same parity, then $a+b$ is even. For this, we use direct proof with cases. Suppose a and b have the same parity.
Case 1. Both a and b are even. Then there are integers m and n for which $a = 2m$

and $b = 2n$, so $a + b = 2m + 2n = 2(m + n)$ is clearly even.
Case 2. Both a and b are odd. Then there are integers m and n for which $a = 2m + 1$ and $b = 2n + 1$, so $a + b = 2m + 1 + 2n + 1 = 2(m + n + 1)$ is clearly even.

Either way, $a + b$ is even. This completes the proof. □

17. There is a prime number between 90 and 100.

Proof. Simply observe that 97 is prime. □

19. If $n \in \mathbb{N}$, then $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \cdots + 2^n = 2^{n+1} - 1$.

Proof. We use direct proof. Suppose $n \in \mathbb{N}$. Let S be the number

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

In what follows, we will solve for S and show $S = 2^{n+1} - 1$. Multiplying both sides of (1) by 2 gives

$$2S = 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + \cdots + 2^n + 2^{n+1}. \tag{2}$$

Now subtract Equation (1) from Equation (2) to obtain $2S - S = -2^0 + 2^{n+1}$, which simplifies to $S = 2^{n+1} - 1$. Combining this with Equation (1) produces $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \cdots + 2^n = 2^{n+1} - 1$, so the proof is complete. □

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

Proof. Suppose for the sake of contradiction that this polynomial has a rational solution $\frac{a}{b}$. We may assume that this fraction is fully reduced, so a and b are not both even. We have $\left(\frac{a}{b}\right)^3 + \frac{a}{b} + 3 = 0$. Clearing the denominator gives

$$a^3 + ab^2 + 3b^3 = 0.$$

Consider two cases: First, if both a and b are odd, the left-hand side is a sum of three odds, which is odd, meaning 0 is odd, a contradiction. Second, if one of a and b is odd and the other is even, then the middle term of $a^3 + ab^2 + 3b^3$ is even, while a^3 and $3b^2$ have opposite parity. Then $a^3 + ab^2 + 3b^3$ is the sum of two evens and an odd, which is odd, again contradicting the fact that 0 is even. □

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

Proof. (Direct) Suppose $a \mid b$ and $a \mid (b^2 - c)$. This means that $b = ad$ and $b^2 - c = ae$ for some integers d and e. Squaring the first equation produces $b^2 = a^2d^2$. Subtracting $b^2 - c = ae$ from $b^2 = a^2d^2$ gives $c = a^2d^2 - ae = a(ad^2 - e)$. As $ad^2 - e \in \mathbb{Z}$, it follows that $a \mid c$. □

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.

Proof. (Contrapositive) Suppose that p is not prime, so it factors as $p = mn$ for $1 < m, n < p$.

Observe that it is not the case that both $m > \sqrt{p}$ and $n > \sqrt{p}$, because if this were true the inequalities would multiply to give $mn > \sqrt{p}\sqrt{p} = p$, which contradicts $p = mn$.

Therefore $m \leq \sqrt{p}$ or $n \leq \sqrt{p}$. Without loss of generality, say $n \leq \sqrt{p}$. Then the equation $p = mn$ gives $n \mid p$, with $1 < n \leq \sqrt{p}$. Therefore it is not true that $n \nmid p$ for each integer n for which $2 \leq n \leq \sqrt{p}$. □

27. Suppose $a, b \in \mathbb{Z}$. If $a^2 + b^2$ is a perfect square, then a and b are not both odd.

Proof. (Contradiction) Suppose $a^2 + b^2$ is a perfect square, and a and b are both odd. As $a^2 + b^2$ is a perfect square, say c is the integer for which $c^2 = a^2 + b^2$. As a and b are odd, we have $a = 2m + 1$ and $b = 2n + 1$ for integers m and n. Then

$$c^2 = a^2 + b^2 = (2m + 1)^2 + (2n + 1)^2 = 4(m^2 + n^2 + mn) + 2.$$

This is even, so c is even also; let $c = 2k$. Now the above equation results in $(2k)^2 = 4(m^2 + n^2 + mn) + 2$, which simplifies to $2k^2 = 2(m^2 + n^2 + mn) + 1$. Thus $2k^2$ is both even and odd, a contradiction. □

29. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Proof. (Direct) Suppose $a \mid bc$ and $\gcd(a, b) = 1$. The fact that $a \mid bc$ means $bc = az$ for some integer z. The fact that $\gcd(a, b) = 1$ means that $ax + by = 1$ for some integers x and y (by Proposition 13.1 on page 307). From this we get $acx + bcy = c$; substituting $bc = az$ yields $acx + azy = c$, that is, $a(cx + zy) = c$. Therefore $a \mid c$. □

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

Proof. Suppose d is a positive integer that is a common divisor of n and $n + 1$. Then $n = dx$ and $n+1 = dy$ for integers x and y. Then $1 = (n+1) - n = dy - dx = d(y - x)$. Now, $1 = d(y - x)$ is only possible if $d = \pm 1$ and $y - x = \pm 1$. Thus the greatest common divisor of n and $n+1$ can be no greater than 1. But 1 does divide both n and $n + 1$, so $\gcd(n, n + 1) = 1$. □

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

Proof. Note that $4n^2+1 = (2n+1)(2n-1)+2$. Therefore, it suffices to show that $\gcd(2n + 1, (2n + 1)(2n - 1) + 2) = 1$. Let d be a common positive divisor of both $2n+1$ and $(2n+1)(2n-1)+2$, so $2n+1 = dx$ and $(2n+1)(2n-1)+2 = dy$ for integers x and y. Substituting the first equation into the second gives $dx(2n - 1) + 2 = dy$, so $2 = dy - dx(2n - 1) = d(y - 2nx - x)$. This means d divides 2, so d equals 1 or 2. But the equation $2n + 1 = dx$ means d must be odd. Therefore $d = 1$, that is, $\gcd(2n + 1, (2n + 1)(2n - 1) + 2) = 1$. □

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

Proof. Suppose $a = \gcd(a, b)$. This means a is a divisor of both a and b. In particular $a \mid b$.

Conversely, suppose $a \mid b$. Then a divides both a and b, so $a \leq \gcd(a, b)$. On the other hand, since $\gcd(a, b)$ divides a, we have $a = \gcd(a, b) \cdot x$ for some integer x. As all integers involved are positive, it follows that $a \geq gcd(a, b)$.

It has been established that $a \leq \gcd(a, b)$ and $a \geq gcd(a, b)$. Thus $a = \gcd(a, b)$. □

37. Suppose A and B are sets. Prove $A \subseteq B$ if and only if $A - B = \emptyset$.

Proof. First we will prove that if $A \subseteq B$, then $A - B = \emptyset$. Contrapositive proof is used. Suppose that $A - B \neq \emptyset$. Thus there is an element $a \in A - B$, which means $a \in A$ but $a \notin B$. Since not every element of A is in B, we have $A \nsubseteq B$.

Conversely, we will prove that if $A - B = \emptyset$, then $A \subseteq B$. Again, contrapositive proof is used. Suppose $A \nsubseteq B$. This means that it is not the case that every element of A is an element of B, so there is an element $a \in A$ with $a \notin B$. Therefore we have $a \in A - B$, so $A - B \neq \emptyset$. □

39. Suppose $A \neq \emptyset$. Prove that $A \times B \subseteq A \times C$, if and only if $B \subseteq C$.

Proof. First we will prove that if $A \times B \subseteq A \times C$, then $B \subseteq C$. Using contrapositive, suppose that $B \nsubseteq C$. This means there is an element $b \in B$ with $b \notin C$. Since $A \neq \emptyset$, there exists an element $a \in A$. Now consider the ordered pair (a, b). Note that $(a, b) \in A \times B$, but $(a, b) \notin A \times C$. This means $A \times B \nsubseteq A \times C$.

Conversely, we will now show that if $B \subseteq C$, then $A \times B \subseteq A \times C$. We use direct proof. Suppose $B \subseteq C$. Assume that $(a, b) \in A \times B$. This means $a \in A$ and $b \in B$. But, as $B \subseteq C$, we also have $b \in C$. From $a \in A$ and $b \in C$, we get $(a, b) \in A \times C$. We've now shown $(a, b) \in A \times B$ implies $(a, b) \in A \times C$, so $A \times B \subseteq A \times C$. □