Chapter 11

Proof by Contradiction

We now explore a third method of proof: **proof by contradiction**. This method is not limited to proving just conditional statements—it can be used to prove any kind of statement whatsoever. The basic idea is to assume that the statement we want to prove is *false*, and then show that this assumption leads to nonsense. We are then led to conclude that we were wrong to assume the statement was false, so the statement must be true. As an example, consider the following proposition and its proof.

Proposition. If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.

Proof. Suppose this proposition is *false*.
This conditional statement being false means there exist numbers a and b for which $a, b \in \mathbb{Z}$ is true, but $a^2 - 4b \neq 2$ is false.
In other words, there exist integers $a, b \in \mathbb{Z}$ for which $\boxed{a^2 - 4b = 2.}$
From this equation we get $a^2 = 4b + 2 = 2(2b + 1)$, so a^2 is even.
Because a^2 is even, it follows that a is even, so $a = 2c$ for some integer c.
Now plug $a = 2c$ back into the boxed equation to get $(2c)^2 - 4b = 2$,
so $4c^2 - 4b = 2$. Dividing by 2, we get $2c^2 - 2b = 1$.
Therefore $1 = 2(c^2 - b)$, and because $c^2 - b \in \mathbb{Z}$, it follows that 1 is even.
We know 1 is **not** even, so something went wrong.
But all the logic after the first line of the proof is correct, so it must be that the first line was incorrect. In other words, we were wrong to assume the proposition was false. Thus the proposition is true. □

You may be a bit suspicious of this line of reasoning, but in the next section we will see that it is logically sound. For now, notice that at the end of the proof we deduced that 1 is even, which conflicts with our knowledge that 1 is odd. In essence, we have obtained the statement (1 is odd)$\wedge\neg$(1 is odd), which has the form $C \wedge \neg C$. Notice that no matter what statement C is, and whether or not it is true, the statement $C \wedge \neg C$ is false. A statement—like this one—that cannot be true is called a **contradiction**. Contradictions play a key role in our new technique.

11.1 Proving Statements with Contradiction

Let's now see why the proof on the previous page is logically valid. In that proof we needed to show that a statement $P : (a, b \in \mathbb{Z}) \Rightarrow (a^2 - 4b \neq 2)$ was true. The proof began with the assumption that P was false, that is that $\neg P$ was true, and from this we deduced $C \wedge \neg C$. In other words we proved that $\neg P$ being true forces $C \wedge \neg C$ to be true, and this means that we proved that the *conditional* statement $(\neg P) \Rightarrow (C \wedge \neg C)$ is true. To see that this is the same as proving P is true, look at the following truth table for $(\neg P) \Rightarrow (C \wedge \neg C)$. Notice that the columns for P and $(\neg P) \Rightarrow (C \wedge \neg C)$ are exactly the same, so P is logically equivalent to $(\neg P) \Rightarrow (C \wedge \neg C)$.

P	C	$\neg P$	$C \wedge \neg C$	$(\neg P) \Rightarrow (C \wedge \neg C)$
T	T	F	F	**T**
T	F	F	F	**T**
F	T	T	F	**F**
F	F	T	F	**F**

Therefore to prove a statement P, it suffices to instead prove the conditional statement $(\neg P) \Rightarrow (C \wedge \neg C)$. This can be done with direct proof: Assume $\neg P$ and deduce $C \wedge \neg C$. Here is the outline:

Outline for Proof by Contradiction

Assumption 11.1. P.

Proof. Suppose $\neg P$.

⋮

Therefore $C \wedge \neg C$. □

One slightly unsettling feature of this method is that we may not know at the beginning of the proof what the statement C is going to be. In doing the scratch work for the proof, you assume that $\neg P$ is true, then deduce new statements until you have deduced some statement C *and* its negation $\neg C$.

If this method seems confusing, look at it this way. In the first line of the proof we suppose $\neg P$ is true, that is we assume P is *false*. But if P is really true then this contradicts our assumption that P is false. But we haven't yet *proved* P to be true, so the contradiction is not obvious. We use logic and reasoning to transform the non-obvious contradiction $\neg P$ to an obvious contradiction $C \wedge \neg C$.

The idea of proof by contradiction is ancient, going back at least as far as the Pythagoreans, who used it to prove that certain numbers are irrational. Our next example follows their logic to prove that $\sqrt{2}$ is irrational. Recall that a number is *rational* if it equals a fraction of two integers, and it is *irrational* if it cannot be expressed this way. Here is the exact definition.

Definition 11.1. A real number x is **rational** if $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$. Also, x is **irrational** if it is not rational, that is if $x \neq \frac{a}{b}$ for every $a, b \in \mathbb{Z}$.

We are now ready to use contradiction to prove that $\sqrt{2}$ is irrational. According to the outline, the first line of the proof should be "Suppose that it is not true that $\sqrt{2}$ is irrational." But it is helpful (though not mandatory) to tip our reader off to the fact that we are using proof by contradiction. One standard way of doing this is to make the first line "*Suppose for the sake of contradiction that it is not true that $\sqrt{2}$ is irrational.*"

Proposition. The number $\sqrt{2}$ is irrational.

Proof. Suppose for the sake of contradiction that it is not true that $\sqrt{2}$ is irrational. Then $\sqrt{2}$ is rational, so there are integers a and b for which

$$\sqrt{2} = \frac{a}{b}. \tag{11.1}$$

Let this fraction be fully reduced; in particular, this means that a and b are not both even. (If they were both even, the fraction could be further reduced by factoring 2's from the numerator and denominator and canceling.) Squaring both sides of Equation 11.1 gives $2 = \frac{a^2}{b^2}$, and therefore

$$a^2 = 2b^2. \tag{11.2}$$

From this it follows that a^2 is even. But we proved earlier (Exercise 1 on page 265) that a^2 being even implies a is even. Thus, as we know that a and b are not both even, it follows that b **is odd.** Now, since a is even there is an integer c for which $a = 2c$. Plugging this value for a into Equation (11.2), we get $(2c)^2 = 2b^2$, so $4c^2 = 2b^2$, and hence $b^2 = 2c^2$. This means b^2 is even, so b is even also. But previously we deduced that b is odd. Thus we have the contradiction b is even **and** b is odd. □

To appreciate the power of proof by contradiction, imagine trying to prove $\sqrt{2}$ is irrational without it. Where would we begin? What would be our initial assumption? There are no clear answers. Proof by contradiction gives a starting point: Assume $\sqrt{2}$ is rational, and work from there.

In the above proof we got the contradiction (b is even) $\wedge\neg$(b is even) which has the form $C \wedge \neg C$. In general, your contradiction need not necessarily be of this form. Any statement that is clearly false is sufficient. For example $2 \neq 2$ would be a fine contradiction, as would be $4 \mid 2$, provided that you could deduce them.

Here is another ancient example, dating back at least as far as Euclid:

Proposition. There are infinitely many prime numbers.

Proof. For the sake of contradiction, suppose there are only finitely many prime numbers. Then we can list all the prime numbers as $p_1, p_2, p_3, \ldots p_n$, where $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ and so on. Thus p_n is the nth and largest prime number. Now consider the number $a = (p_1 p_2 p_3 \cdots p_n) + 1$, that is, a is the product of all prime numbers, plus 1. Now a, like any natural number greater than 1, has at least one prime divisor, and that means $p_k \mid a$ for at least one of our n prime numbers p_k. Thus there is an integer c for which $a = cp_k$, which is to say

$$(p_1 p_2 p_3 \cdots p_{k-1} p_k p_{k+1} \cdots p_n) + 1 = cp_k.$$

Dividing both sides of this by p_k gives us

$$(p_1 p_2 p_3 \cdots p_{k-1} p_{k+1} \cdots p_n) + \frac{1}{p_k} = c,$$

so

$$\frac{1}{p_k} = c - (p_1 p_2 p_3 \cdots p_{k-1} p_{k+1} \cdots p_n).$$

The expression on the right is an integer, while the expression on the left is not an integer. This is a contradiction. □

Proof by contradiction often works well in proving statements of the form $\forall x, P(x)$. The reason is that the proof set-up involves assuming $\neg\forall x, P(x)$, which as we know from Section 5.4 is equivalent to $\exists\, x, \neg P(x)$. This gives us a specific x for which $\neg P(x)$ is true, and often that is enough to produce a contradiction.

This happened in the proof that $\sqrt{2}$ is irrational on page 273. The statement "$\sqrt{2}$ *is irrational*" is logically equivalent to $\forall a, b \in \mathbb{Z},\ 2 \neq \left(\frac{a}{b}\right)^2$. Proof by contradiction involved assuming this was false, that is, we assumed $\neg \left(\forall a, b \in \mathbb{Z},\ 2 \neq \left(\frac{a}{b}\right)^2\right)$, which became $\exists\, a, b \in \mathbb{Z},\ 2 = \left(\frac{a}{b}\right)^2$. This gave a concrete *equation* $2 = \left(\frac{a}{b}\right)^2$ to work with, and that was what led to the contradiction.

Let's look at another example another example of form $\forall x, P(x)$.

Proposition. For every real number $x \in [0, \pi/2]$, we have $\sin x + \cos x \geq 1$.

Proof. Suppose for the sake of contradiction that this is not true.
Then there exists an $x \in [0, \pi/2]$ for which $\sin x + \cos x < 1$.

Since $x \in [0, \pi/2]$, neither $\sin x$ nor $\cos x$ is negative, so $0 \leq \sin x + \cos x < 1$.
Thus $0^2 \leq (\sin x + \cos x)^2 < 1^2$, which gives $0^2 \leq \sin^2 x + 2 \sin x \cos x + \cos^2 x < 1^2$.
As $\sin^2 x + \cos^2 x = 1$, this becomes $0 \leq 1 + 2 \sin x \cos x < 1$, so $1 + 2 \sin x \cos x < 1$.
Subtracting 1 from both sides gives $2 \sin x \cos x < 0$.
But this contradicts the fact that neither $\sin x$ nor $\cos x$ is negative. □

11.2 Proving Conditional Statements by Contradiction

As the previous two chapters dealt with proving conditional statements, we now formalize the method for proving conditional statements with contradiction. Suppose we want to prove a proposition of this form:

Proposition. If P, then Q.

Thus we need to prove that $P \Rightarrow Q$ is a true statement. Proof by contradiction begins with the assumption that $\neg(P \Rightarrow Q)$ is true, that is, that $P \Rightarrow Q$ is false. But we know that $P \Rightarrow Q$ being false means that it is possible that P can be true while Q is false. Thus the first step in the proof is to assume P and $\neg Q$. Here is an outline:

Outline for Proving a Conditional Statement with Contradiction

Proposition. If P, then Q.
Proof. Suppose P and $\neg Q$.
$\vdots$
Therefore $C \wedge \neg C$. □

To illustrate this new technique, we revisit a familiar result: If a^2 is even, then a is even. According to the outline, the first line of the proof should be "For the sake of contradiction, suppose a^2 is even and a is not even."

Proposition. Suppose $a \in \mathbb{Z}$. If a^2 is even, then a is even.

Proof. For the sake of contradiction, suppose a^2 is even and a is not even.
Then a^2 is even, and a is odd.
Since a is odd, there is an integer c for which $a = 2c + 1$.
Then $a^2 = (2c+1)^2 = 4c^2 + 4c + 1 = 2(2c^2 + 2c) + 1$, so a^2 is odd.
Thus a^2 is even and a^2 is not even, a contradiction. □

Here is another example.

Proposition. If $a, b \in \mathbb{Z}$ and $a \geq 2$, then $a \nmid b$ or $a \nmid (b+1)$.

Proof. Suppose for the sake of contradiction there exist $a, b \in \mathbb{Z}$ with $a \geq 2$, and for which it is not true that $a \nmid b$ or $a \nmid (b+1)$.
By DeMorgan's law, we have $a \mid b$ and $a \mid (b+1)$.
The definition of divisibility says there are $c, d \in \mathbb{Z}$ with $b = ac$ and $b + 1 = ad$.
Subtracting one equation from the other gives $ad - ac = 1$, so $a(d - c) = 1$.
Since a is positive, $d - c$ is also positive (otherwise $a(d - c)$ would be negative).
Then $d - c$ is a positive integer and $a(d - c) = 1$, so $a = 1/(d - c) < 2$.
Thus we have $a \geq 2$ and $a < 2$, a contradiction. □

11.3 Combining Techniques

Often, especially in more complex proofs, several proof techniques are combined within a single proof. For example, in proving a conditional statement $P \Rightarrow Q$, we might begin with direct proof and thus assume P to be true with the aim of ultimately showing Q is true. But the truth of Q might hinge on the truth of some other statement R which—together with P—would imply Q. We would then need to prove R, and we would use whichever proof technique seems most appropriate. This can lead to "proofs inside of proofs." Consider the following example. The overall approach is direct, but inside the direct proof is a separate proof by contradiction.

Proposition. Every non-zero rational number can be expressed as a product of two irrational numbers.

Proof. This proposition can be reworded as follows: If r is a non-zero rational number, then r is a product of two irrational numbers. In what follows, we prove this with direct proof.

Suppose r is a non-zero rational number. Then $r = \frac{a}{b}$ for integers a and b. Also, r can be written as a product of two numbers as follows:

$$r = \sqrt{2} \cdot \frac{r}{\sqrt{2}}.$$

We know $\sqrt{2}$ is irrational, so to finish the proof we must show $r/\sqrt{2}$ is irrational too. For this, assume for the sake of contradiction that $r/\sqrt{2}$ is rational. Then

$$\frac{r}{\sqrt{2}} = \frac{c}{d}$$

for integers c and d, so

$$\sqrt{2} = r\frac{d}{c}.$$

But we know $r = a/b$, which combines with the above equation to give

$$\sqrt{2} = r\frac{d}{c} = \frac{a}{b}\frac{d}{c} = \frac{ad}{bc}.$$

This means $\sqrt{2}$ is rational, which is a contradiction because we know it is irrational. Therefore $r/\sqrt{2}$ is irrational.

Consequently $r = \sqrt{2} \cdot r/\sqrt{2}$ is a product of two irrational numbers. □

For another example of a proof-within-a-proof, try Exercise 5 at the end of this chapter (or see its solution). Exercise 5 asks you to prove that $\sqrt{3}$ is irrational. This turns out to be slightly trickier than proving that $\sqrt{2}$ is irrational.

Despite the power of proof by contradiction, it's best to use it only when the direct and contrapositive approaches do not seem to work. The reason for this is that a proof by contradiction can often have hidden in it a simpler contrapositive proof, and if this is the case it's better to go with the simpler approach. Consider the following example.

Proposition. Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proof. To the contrary, suppose $a^2 - 2a + 7$ is even and a is not odd.
That is, suppose $a^2 - 2a + 7$ is even and a is even.
Since a is even, there is an integer c for which $a = 2c$.
Then $a^2 - 2a + 7 = (2c)^2 - 2(2c) + 7 = 2(2c^2 - 2c + 3) + 1$, so $a^2 - 2a + 7$ is odd.
Thus $a^2 - 2a + 7$ is both even and odd, a contradiction. □

Though there is nothing really wrong with this proof, notice that part of it assumes a is not odd, then deduces that a^2-2a+7 is not even. That's contrapositive proof! So it would be simpler to just take the contrapositive approach, as follows.

Proposition. Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proof. (Contrapositive) Suppose a is not odd.
Then a is even, so there is an integer c for which $a = 2c$.
Then $a^2 - 2a + 7 = (2c)^2 - 2(2c) + 7 = 2(2c^2 - 2c + 3) + 1$, so $a^2 - 2a + 7$ is odd.
Thus $a^2 - 2a + 7$ is not even. □

11.4 Case Study: The Halting Problem

The ancient greeks used contradiction to prove that $\sqrt{2}$ is not a fraction of integers, or (as we would say today) it is irrational. This truth was shocking and unsettling, for it shattered their fundamental conception of what a number was.

Millennia later, contradiction again rocked mathematics. Before 1930, mathematicians were of the mindset that any *true* mathematical statement could be *proved*. They also believed—roughly speaking—that any problem in discrete mathematics could be solved with an algorithm. Then Alan Turing proved that there are problems that no algorithm can solve. We now examine such a problem, and use contradiction to prove it is really insolvable.

Imagine a computer program (or algorithm) called `LoopCheck`. Its purpose is to decide whether any program would go into an infinite loop if run. Think of `LoopCheck` as being similar to a spell check program that reads in a document and finds the spelling errors. `LoopCheck` would read in a computer program and find "infinite loop" errors.

Turing discovered that it is absolutely impossible to write `LoopCheck`. No such algorithm can possibly exist. The problem of writing one is simply unsolvable. In computer science this is known as the **halting problem**, as a `LoopCheck` program would decide whether or not any program *halts*.

Before proving that `LoopCheck` is impossible, let's pause to lay out its exact specifications, so we'll know what we're dealing with. Note that if we run a program on some input, one of two things will happen: either it gets hung up in an infinite loop, or it eventually halts. There may be several reasons for halting. Maybe it finishes its appointed task and returns some output. Or maybe it stops because of some internal error like division by zero, or some other meaningless operation. Maybe the input simply makes no sense for the program. When a program halts under such circumstances it may return garbage for output, but it *still halts*.

`LoopCheck` does not make any evaluation about whether or not a program's output is garbage. Its purpose is only to decide whether or not a program goes into an infinite loop when run on certain input.

Think of it as a procedure `LoopCheck(prog,input)` that reads in a program `prog` and some input `input` for `prog`. Let `prog(input)` mean that `prog` is run with input `input`. Then `LoopCheck(prog,input)` simply returns the words "GOOD" or "BAD," as follows.

$$\texttt{LoopCheck(prog,input)} = \begin{cases} \text{GOOD if } \texttt{prog(input)} \text{ halts,} \\ \text{BAD if } \texttt{prog(input)} \text{ loops infinitely.} \end{cases}$$

We're ready for Turing's famous proof that `LoopCheck` is impossible. In the proof you will see the expression `LoopCheck(prog,prog)`, which means `LoopCheck` is asked to decide whether or not a program `prog` halts with itself as input. Keep in mind that lots of programs can use themselves as input. Consider a program that counts the number of characters in a file. You could certainly run it on itself (or at least a copy of itself) and the output would be the number of characters in the program. Granted, most programs would come to a crashing halt if they read in themselves as input. And if they didn't halt, they'd run forever (i.e., they'd be stuck in an infinite loop).

Theorem 11.2. *The program* `LoopCheck` *is impossible to write.*
(That is, the halting problem cannot be solved.)

Proof. For sake of contradiction, suppose that `LoopCheck` *can* be written, and it has been implemented. Now make the following procedure called `Test` that reads in a program `prog` as input. In running, it makes a call to `LoopCheck`.

Procedure Test(`prog`) *(input* `prog` *is a program)*

```
begin
    if LoopCheck(prog,prog) = GOOD then
        i := 1
        while (i > 0) do
            i := i + 1 ................................. this is an infinite loop
        end
    else
        if LoopCheck(prog,prog) = BAD then
            return UGLY .............. i.e., return the word "UGLY" and halt
        end
    end
end
```

We will get a contradiction by running `Test(Test)`. In other words, we will run the above procedure `Test` with the input `prog` replaced by `Test`.

Let's run `Test(Test)`. Consider the following two cases.

Case 1. Suppose that in line 2, `LoopCheck(Test,Test)` = GOOD. Then the while loop runs forever, so `Test(Test)` does not halt. But at the same time, `LoopCheck(Test,Test)` = GOOD means that `Test(Test)` halts. Therefore `Test(Test)` halts and does not halt. Contradiction!

Case 2. Suppose that in line 2, `LoopCheck(Test,Test)` = BAD. Then `Test(Test)` halts at line 9 (and returns the word "UGLY"). But the fact `LoopCheck(Test,Test)` = BAD means `Test(Test)` does not halt. Therefore `Test(Test)` halts and does not halt. Contradiction!

In either case, `Test(Test)` halts and does not halt, a contradiction. □

The fact that `LoopCheck` is impossible has some significant theoretical implications. For one, it means that certain strategies for proving theorems are hopeless. For example, consider Fermat's last theorem, from page 47:

For all numbers $a, b, c, n \in \mathbb{N}$ with $n > 2$, it is the case that $a^n + b^n \neq c^n$.

It would easy to write an algorithm with nested while loops that runs through all possible combinations of a, b, c and n, and stops only when and if $a^n + b^n = c^n$. This algorithm reads in no input (that is, its input is $\emptyset$), but it either halts or loops forever. Moreover, this algorithm (call it `Fermat`) halts if Fermat's last theorem is false, and it loops forever if Fermat's last theorem is true. If `LoopCheck` were possible, and if it were written, we could prove or disprove Fermat's last theorem by running

`LoopCheck( Fermat,` $\emptyset$ `).`

If it returned "GOOD," then Fermat's last theorem would be false. If it returned "BAD," then Fermat's last theorem would be true. The fact that `LoopCheck` is impossible means that we can't hope to prove Fermat's last theorem (or any other theorem) this way.

Our discussion of the halting problem has been somewhat informal. Most careful treatments of it use mathematical constructions called *Turing machines*, which are theoretical versions of computers. If this kind of thing piques your interest, you should definitely consider taking a computer science class in the theory of computation. You will need a command of all proof techniques covered in this book, including contradiction.

Exercises for Chapter 11

A. Use the method of proof by contradiction to prove the following statements. (In each case, you should also think about how a direct or contrapositive proof would work. You will find in most cases that proof by contradiction is easier.)

1. Suppose $n \in \mathbb{Z}$. If n is odd, then n^2 is odd.

2. Suppose $n \in \mathbb{Z}$. If n^2 is odd, then n is odd.

3. Prove that $\sqrt[3]{2}$ is irrational.

4. Prove that $\sqrt{6}$ is irrational.

5. Prove that $\sqrt{3}$ is irrational.

6. If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 2 \neq 0$.

7. If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$.

8. Suppose $a, b, c \in \mathbb{Z}$. If $a^2 + b^2 = c^2$, then a or b is even.

9. Suppose $a, b \in \mathbb{R}$. If a is rational and ab is irrational, then b is irrational.

10. There exist no integers a and b for which $21a + 30b = 1$.

11. There exist no integers a and b for which $18a + 6b = 1$.

12. For every positive $x \in \mathbb{Q}$, there is a positive $y \in \mathbb{Q}$ for which $y < x$.

13. For every $x \in [\pi/2, \pi]$, $\sin x - \cos x \geq 1$.

14. If A and B are sets, then $A \cap (B - A) = \emptyset$.

15. If $b \in \mathbb{Z}$ and $b \nmid k$ for every $k \in \mathbb{N}$, then $b = 0$.

16. If a and b are positive real numbers, then $a + b \geq 2\sqrt{ab}$.

17. For every $n \in \mathbb{Z}$, $4 \nmid (n^2 + 2)$.

18. Suppose $a, b \in \mathbb{Z}$. If $4 \mid (a^2 + b^2)$, then a and b are not both odd.

B. Prove the following statements using any method from Chapters 9, 10 or 11.

19. The product of any five consecutive integers is divisible by 120. (For example, the product of 3,4,5,6 and 7 is 2520, and $2520 = 120 \cdot 21$.)

20. We say that a point $P = (x, y)$ in $\mathbb{R}^2$ is **rational** if both x and y are rational. More precisely, P is rational if $P = (x, y) \in \mathbb{Q}^2$. An equation $F(x, y) = 0$ is said to have a **rational point** if there exists $x_0, y_0 \in \mathbb{Q}$ such that $F(x_0, y_0) = 0$. For example, the curve $x^2 + y^2 - 1 = 0$ has rational point $(x_0, y_0) = (1, 0)$. Show that the curve $x^2 + y^2 - 3 = 0$ has no rational points.

21. Exercise 20 (above) involved showing that there are no rational points on the curve $x^2 + y^2 - 3 = 0$. Use this fact to show that $\sqrt{3}$ is irrational.

22. Explain why $x^2 + y^2 - 3 = 0$ not having any rational solutions (Exercise 20) implies $x^2 + y^2 - 3^k = 0$ has no rational solutions for k an odd, positive integer.

23. Use the above result to prove that $\sqrt{3^k}$ is irrational for all odd, positive k.

24. The number $\log_2 3$ is irrational.

Solutions for Chapter 11

1. Suppose n is an integer. If n is odd, then n^2 is odd.

Proof. Suppose for the sake of contradiction that n is odd and n^2 is not odd. Then n^2 is even. Now, since n is odd, we have $n = 2a + 1$ for some integer a. Thus $n^2 = (2a+1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$. This shows $n^2 = 2b + 1$, where b is the integer $b = 2a^2 + 2a$. Therefore we have n^2 is odd and n^2 is even, a contradiction. □

3. Prove that $\sqrt[3]{2}$ is irrational.

Proof. Suppose for the sake of contradiction that $\sqrt[3]{2}$ is not irrational. Therefore it is rational, so there exist integers a and b for which $\sqrt[3]{2} = \frac{a}{b}$. Let us assume that this fraction is reduced, so a and b are not both even. Now we have $\sqrt[3]{2}^3 = \left(\frac{a}{b}\right)^3$, which gives $2 = \frac{a^3}{b^3}$, or $2b^3 = a^3$. From this we see that a^3 is even, from which we deduce that a is even. (For if a were odd, then $a^3 = (2c+1)^3 = 8c^3 + 12c^2 + 6c + 1 = 2(4c^3 + 6c^2 + 3c) + 1$ would be odd, not even.) Since a is even, it follows that $a = 2d$ for some integer d. The equation $2b^3 = a^3$ from above then becomes $2b^3 = (2d)^3$, or $2b^3 = 8d^3$. Dividing by 2, we get $b^3 = 4d^3$, and it follows that b^3 is even. Thus b is even also. (Using the same argument we used when a^3 was even.) At this point we have discovered that both a and b are even, contradicting the fact (observed above) that the a and b are not both even. □

Here is an alternative proof.

Proof. Suppose for the sake of contradiction that $\sqrt[3]{2}$ is not irrational. Therefore there exist integers a and b for which $\sqrt[3]{2} = \frac{a}{b}$. Cubing both sides, we get $2 = \frac{a^3}{b^3}$. From this, $a^3 = b^3 + b^3$, which contradicts Fermat's last theorem. □

5. Prove that $\sqrt{3}$ is irrational.

Proof. Suppose for the sake of contradiction that $\sqrt{3}$ is not irrational. Therefore it is rational, so there exist integers a and b for which $\sqrt{3} = \frac{a}{b}$. Let us assume that this fraction is reduced, so a and b have no common factor. Notice that $\sqrt{3}^2 = \left(\frac{a}{b}\right)^2$, so $3 = \frac{a^2}{b^2}$, or $3b^2 = a^2$. This means $3 \mid a^2$.

Now we are going to show that if $a \in \mathbb{Z}$ and $3 \mid a^2$, then $3 \mid a$. (This is a proof-within-a-proof.) We will use contrapositive proof to prove this conditional statement. Suppose $3 \nmid a$. Then there is a remainder of either 1 or 2 when 3 is divided into a.
Case 1. There is a remainder of 1 when 3 is divided into a. Then $a = 3m + 1$ for some integer m. Consequently, $a^2 = 9m^2 + 6m + 1 = 3(3m^2 + 2m) + 1$, and this means 3 divides into a^2 with a remainder of 1. Thus $3 \nmid a^2$.
Case 2. There is a remainder of 2 when 3 is divided into a. Then $a = 3m + 2$ for some integer m. Consequently, $a^2 = 9m^2 + 12m + 4 = 9m^2 + 12m + 3 + 1 = 3(3m^2 + 4m + 1) + 1$, and this means 3 divides into a^2 with a remainder of 1. Thus $3 \nmid a^2$.
In either case we have $3 \nmid a^2$, so we've shown $3 \nmid a$ implies $3 \nmid a^2$. Therefore, if $3 \mid a^2$, then $3 \mid a$.

Now go back to $3 \mid a^2$ in the first paragraph. This combined with the result of the second paragraph implies $3 \mid a$, so $a = 3d$ for some integer d. Now also in the first paragraph we had $3b^2 = a^2$, which now becomes $3b^2 = (3d)^2$ or $3b^2 = 9d^2$, so $b^2 = 3d^2$. But this means $3 \mid b^2$, and the second paragraph implies $3 \mid b$. Thus we have concluded that $3 \mid a$ and $3 \mid b$, but this contradicts the fact that the fraction $\frac{a}{b}$ is reduced. □

7. If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$.

Proof. Suppose for the sake of contradiction that $a, b \in \mathbb{Z}$ but $a^2 - 4b - 3 = 0$. Then we have $a^2 = 4b + 3 = 2(2b + 1) + 1$, which means a^2 is odd. Therefore a is odd also, so $a = 2c + 1$ for some integer c. Plugging this back into $a^2 - 4b - 3 = 0$ gives us

$$\begin{aligned}(2c+1)^2 - 4b - 3 &= 0\\ 4c^2 + 4c + 1 - 4b - 3 &= 0\\ 4c^2 + 4c - 4b &= 2\\ 2c^2 + 2c - 2b &= 1\\ 2(c^2 + c - b) &= 1.\end{aligned}$$

From this last equation, we see that 1 is an even number, a contradiction. □

9. Suppose $a, b \in \mathbb{R}$ and $a \neq 0$. If a is rational and ab is irrational, then b is irrational.

Proof. Suppose for the sake of contradiction that a is rational and ab is irrational and b is **not** irrational. Thus we have a and b rational, and ab irrational. Since a and b are rational, we know there are integers c, d, e, f for which $a = \frac{c}{d}$ and $b = \frac{e}{f}$. Then $ab = \frac{ce}{df}$, and since both ce and df are integers, it follows that ab is rational. But this is a contradiction because we started out with ab irrational. □

11. There exist no integers a and b for which $18a + 6b = 1$.

Proof. Suppose for the sake of contradiction that there do exist integers a and b for which $18a+6b = 1$. Then $1 = 2(9a+3b)$, which means 1 is even, a contradiction. □

13. For every $x \in [\pi/2, \pi]$, $\sin x - \cos x \geq 1$.

Proof. Suppose for the sake of contradiction that $x \in [\pi/2, \pi]$, but $\sin x - \cos x < 1$. Since $x \in [\pi/2, \pi]$, we know $\sin x \geq 0$ and $\cos x \leq 0$, so $\sin x - \cos x \geq 0$. Therefore we have $0 \leq \sin x - \cos x < 1$. Now the square of any number between 0 and 1 is still a number between 0 and 1, so we have $0 \leq (\sin x - \cos x)^2 < 1$, or $0 \leq \sin^2 x - 2 \sin x \cos x + \cos^2 x < 1$. Using the fact that $\sin^2 x + \cos^2 x = 1$, this becomes $0 \leq -2 \sin x \cos x + 1 < 1$. Subtracting 1, we obtain $-2 \sin x \cos x < 0$. But above we remarked that $\sin x \geq 0$ and $\cos x \leq 0$, and hence $-2 \sin x \cos x \geq 0$. We now have the contradiction $-2 \sin x \cos x < 0$ and $-2 \sin x \cos x \geq 0$. □

15. If $b \in \mathbb{Z}$ and $b \nmid k$ for every $k \in \mathbb{N}$, then $b = 0$.

Proof. Suppose for the sake of contradiction that $b \in \mathbb{Z}$ and $b \nmid k$ for every $k \in \mathbb{N}$, but $b \neq 0$.

Case 1. Suppose $b > 0$. Then $b \in \mathbb{N}$, so $b|b$, contradicting $b \nmid k$ for every $k \in \mathbb{N}$.

Case 2. Suppose $b < 0$. Then $-b \in \mathbb{N}$, so $b|(-b)$, again a contradiction □

17. For every $n \in \mathbb{Z}$, $4 \nmid (n^2 + 2)$.

Proof. Assume there exists $n \in \mathbb{Z}$ with $4 \mid (n^2 + 2)$. Then for some $k \in \mathbb{Z}$, $4k = n^2 + 2$ or $2k = n^2 + 2(1 - k)$. If n is odd, this means $2k$ is odd, and we've reached a contradiction. If n is even then $n = 2j$ and we get $k = 2j^2 + 1 - k$ for some $j \in \mathbb{Z}$. Hence $2(k - j^2) = 1$, so 1 is even, a contradiction. □

Remark. It is fairly easy to see that two more than a perfect square is always either $2 \pmod 4$ or $3 \pmod 4$. This would end the proof immediately.

19. The product of 5 consecutive integers is a multiple of 120.

Proof. Starting from 0, every fifth integer is a multiple of 5, every fourth integer is a multiple of 4, every third integer is a multiple of 3, and every other integer is a multiple of 2. It follows that any set of 5 consecutive integers must contain a multiple of 5, a multiple of 4, at least one multiple of 3, and at least two multiples of 2 (possibly one of which is a multiple of 4). It follows that the product of five consecutive integers is a multiple of $5 \cdot 4 \cdot 3 \cdot 2 = 120$. □

21. Hints for Exercises 20–23. For Exercises 20, first show that the equation $a^2 + b^2 = 3c^2$ has no solutions (other than the trivial solution $(a, b, c) = (0, 0, 0)$) in the integers. To do this, investigate the remainders of a sum of squares $\pmod 4$. After you've done this, prove that the only solution is indeed the trivial solution. Next assume that the equation $x^2 + y^2 - 3 = 0$ has a rational solution. Use the definition of rational numbers to yield a contradiction.