CHAPTER 6

Proof by Contradiction

We now introduce a third method of proof, called **proof by contradiction**. This new 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 of this, 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.
Thus 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.
Since 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 $a^2 - 4b = 2$.
We 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 since $c^2 - b \in \mathbb{Z}$, it follows that 1 is even.
Since we know 1 is **not** even, 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. ■

Though you may be a bit suspicious of this line of reasoning, 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)$\wedge \sim$(1 is odd), which has the form $C \wedge \sim C$. Notice that no matter what statement C is, and whether or not it is true, the statement $C \wedge \sim C$ must be false. A statement—like this one—that cannot be true is called a **contradiction**. Contradictions play a key role in our new technique.

6.1 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 $\sim P$ was true, and from this we deduced $C \wedge \sim C$. In other words we proved that $\sim P$ being true forces $C \wedge \sim C$ to be true, and this means that we proved that the *conditional* statement $(\sim P) \Rightarrow (C \wedge \sim C)$ is true. To see that this is the same as proving P is true, look at the following truth table for $(\sim P) \Rightarrow (C \wedge \sim C)$. Notice that the columns for P and $(\sim P) \Rightarrow (C \wedge \sim C)$ are exactly the same, so P is logically equivalent to $(\sim P) \Rightarrow (C \wedge \sim C)$.

P	C	$\sim P$	$C \wedge \sim C$	$(\sim P) \Rightarrow (C \wedge \sim C)$
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 $(\sim P) \Rightarrow (C \wedge \sim C)$. This can be done with direct proof: Assume $\sim P$ and deduce $C \wedge \sim C$. Here is the outline.

Outline for Proof by Contradiction.

Proposition P.

Proof. Suppose $\sim P$.

$\vdots$

Therefore $C \wedge \sim C$. ■

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 $\sim P$ is true, then deduce new statements until you have deduced some statement C *and* its negation $\sim C$.

If this method seems confusing, look at it this way. In the first line of the proof we suppose $\sim P$ 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 to transform the non-obvious contradiction $P \wedge \sim P$ to an obvious contradiction $C \wedge \sim C$.

The idea of proof by contradiction is quite ancient, and goes 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 as a fraction of two integers. Here is the exact definition.

Definition 6.1 A real number x is **rational** if $x = \frac{a}{b}$, for some $a, b \in \mathbb{Z}$. The number 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 in writing the proof, 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

$$\sqrt{2} = \frac{a}{b}. \tag{6.1}$$

Let this fraction be fully reduced. In particular, this means a and b are not both even, for if they were, the fraction could be further reduced by factoring 2's from the numerator and denominator and canceling. Squaring both sides of Equation 6.1 gives $2 = \frac{a^2}{b^2}$, and therefore

$$a^2 = 2b^2. \tag{6.2}$$

From this it follows that a^2 is even. But we proved at the beginning of this chapter 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 6.2, 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 that $\sqrt{2}$ is irrational without it. Where would we begin? What would

be our initial assumption? There are no clear answers to these questions. Proof by contradiction gives us a starting point: assume $\sqrt{2}$ is rational, and work from there.

In the above proof we got the contradiction (b is even) $\wedge \sim$(b is even) which has the form $C \wedge \sim C$. 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 $4|2$, 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, has at least one prime divisor, and that means $p_k | a$ 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. These numbers can't be equal, so 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 $\sim \forall x, P(x)$, which as we know from Section 2.10 is equivalent to $\exists x, \sim P(x)$. This gives us a specific x for which $\sim P(x)$ is true, and often that is enough to produce a contradiction. Here is an example.

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 $0 \le \sin x + \cos x < 1$.
Thus $0^2 \le (\sin x + \cos x)^2 < 1^2$, which gives $0^2 \le \sin^2 x + 2\sin x \cos x + \cos^2 x < 1^2$.
As $\sin^2 x + \cos^2 x = 1$, this becomes $0 \le 1 + 2\sin x \cos x < 1$, 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. ■

6.2 Proving Conditional Statements by Contradiction

Since the previous two chapters dealt exclusively with proving conditional statements, we now formalize the procedure in which contradiction is used to prove a conditional statement. Suppose we want to prove a proposition of the following 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 $\sim(P \Rightarrow Q)$ it true, that is that $P \Rightarrow Q$ is false. But we know that $P \Rightarrow Q$ being false means that P is true and Q is false. Thus the first step in the proof it to assume P and $\sim Q$. Here is an outline.

Outline for Proving a Conditional Statement with Contradiction.

Proposition If P, then Q.

Proof. Suppose P and $\sim Q$.
⋮
Therefore $C \wedge \sim C$. ■

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 "Suppose for the sake of contradiction that 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. (And since we have arrived at a contradiction, our original supposition that a^2 is even and a is odd could not be true.) ■

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 $ad - ac = 1$, or $a(d-c) = 1$.
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. ■

6.3 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 result. The overall approach is direct, but inside the direct proof is a separate proof by contradiction.

Proposition Every nonzero rational number can be expressed as a product of two irrational numbers.

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

Suppose r is a nonzero 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 complete the proof we must show $r/\sqrt{2}$ is also irrational.

To show this, assume for the sake of contradiction that $r/\sqrt{2}$ is rational. This means

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

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 of this chapter and then check its solution. That exercise asks you to prove that $\sqrt{3}$ is irrational. This turns out to be slightly trickier than proving that $\sqrt{2}$ is irrational.

6.4 Some Words of Advice

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 and deduces that $a^2 - 2a + 7$ is not even. That is the contrapositive approach! Thus it would be more efficient to proceed as follows, using contrapositive proof.

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. ■

Exercises for Chapter 6

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 rational number x, there is a positive rational number y 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 $a + b \leq 2\sqrt{ab}$.

17. For every $n \in \mathbb{Z}$, $4 \not| (n^2 + 2)$.

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

B. Prove the following statements using any method from chapters 4, 5 or 6.

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 the Cartesian plane 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 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.