P.9 Proof by Contradiction

I've probably referred to all of our proof techniques as "powerful," but the method of contradiction really is amazingly powerful. Most often, we employ proof by contradiction when proving a claim for which there is no clear beginning for the proof. You'll see some examples soon.

Goals:

- Develop the logic behind proof by contradiction
- Find the contradiction in given proofs by contradiction
- Write proofs using contradiction

We're still working to prove statements of the form $P \Rightarrow Q$. The process of proof by contradiction begins with negating such a statement. You may recall from Intro to Formal Mathematics that

$$\sim (P \Rightarrow Q) \equiv P \wedge \sim Q.$$

1. Confirm that $\sim (P \Rightarrow Q) \equiv P \wedge \sim Q$ using the truth table below.

P	Q	$P \Rightarrow Q$	$\sim (P \Rightarrow Q)$	$\sim Q$	$P \wedge \sim Q$
T	T				
T	F				
F	T				
F	F				

2. Negate the following conditional statements using the form $P \wedge \sim Q$. Remember to negate Q in a *useful* way if possible.

   (a) If $x > 1$, then $x^3 > x$.

   (b) If $a \mid b$, then $a \mid bc$.

(c) If $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, then $b \equiv c \pmod{n}$.

(d) If a is even, then a^2 is even and a^3 is even.

(e) If $x \,|\, yz$, then $x \,|\, y$ or $x \,|\, z$.

It is very possible that you've employed a contradiction argument before as it is common even outside of mathematics. The structure of the method is simple. We begin with a statement R that is true. The statement R itself may be quite complicated. It could be a conjunction, disjunction, conditional statement like $R \equiv (P \Rightarrow Q)$, or any combination thereof. To argue that R is true we begin by supposing that R is false. We then derive a series of statements using correct deductive reasoning. With any luck we manage to derive an *absurdity*, that is, a statement that is always false. Often times the absurdity will take the form $C \wedge \sim C$, but this is not always the case.

3. Complete the following truth table for $C \wedge \sim C$ to show that this statement is an absurdity.

C	$\sim C$	$(C \wedge \sim C)$
T		
F		

4. The general form of the argument in a proof by contradiction is $\sim R \Rightarrow (C \wedge \sim C)$. Fill in the truth table for this argument form to see that it is true precisely when R is true.

R	C	$(C\wedge \sim C)$	$\sim R \Rightarrow (C\wedge \sim C)$
T	T		
T	F		
F	T		
F	F		

5. We need one more step before we really get started. We'll use the following claims as lemmas today. That is, we'll use them while proving other statements. You can prove the following claims with either a direct proof or a proof by contrapositive.

   Claim 1. Suppose $n \in \mathbb{Z}$. If n^3 is even, then n is even.

   Claim 2. Suppose $a, b, c \in \mathbb{Z}$. If $a \,|\, (b + c)$ and $a \,|\, b$, then $a \,|\, c$.

Let's take a look at using contradiction to prove the following claim. The proof given below is adapted from the one given in your text.

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

Here, R is the conditional statement "If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$." Recall then that $\sim R$ will be "$a, b \in \mathbb{Z}$ and $a^2 - 4b - 3 = 0$." This is how our proof will begin.

Notice, that there is no given C. The statement of the claim gives no indication of what the contradicting piece will be. We are forced deduce things from our initial claim seemingly at random until we stumble across a contradiction.

Finally, like contrapositive, we want to tell our reader how we are proving the claim so that he or she is not confused by our proof. Usually, we begin proofs by contradiction with the phrase "Suppose for the sake of contradiction that..." or "By way of contradiction, suppose..." For the purposes of this class, when using contradiction we will also start by writing "(Contradiction)."

Proof. (Contradiction) Suppose for the sake of contradiction that $a, b \in \mathbb{Z}$ and $a^2 - 4b - 3 = 0$. Then

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

Since $2b + 1$ is an integer, we have that a^2 is odd by definition. Recall from a previous proof that if a^2 is odd then a is odd, so $a = 2c + 1$ for $c \in \mathbb{Z}$. By substitution, we have

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

Since $(c^2 + c - b) \in \mathbb{Z}$, the last equality gives us that 1 is an even integer. Since we know 1 to be an odd integer, we have a contradiction. □

There are definitely a few things to point out about this process and this proof now that we've seen an example. First, notice that the contradiction didn't exactly take the form $C\wedge \sim C$, though we could have phrased it that way. Either way, we did arrive at a clearly false statement. Second, no planning went in to decide to use $\sim R$ to show that 1 is even. After several lines of manipulation it became clear that this contradiction was possible. Arguably the hardest part of proof by contradiction is recognizing your contradiction when you find it. Third, it is very likely that there are many other contradictions that can be derived from assuming $\sim R$. In general, there is no one way to write a contradiction proof. Finally, our proof ends with an explanation to our reader of why we have a contradiction. Unfortunately, this aspect is often left out of proofs by contradiction and it is the reader's responsibility to recognize the contradiction for what it is.

When we write proofs by hand, we have a few common symbols people employ to indicate the line their contradiction appears on. The most common that Dr. Wright has seen is the opposing arrows symbol ($\rightarrow\!\leftarrow$). Another popular symbols is the "blitzkrieg" or lightning symbol ($\lightning$). Neither symbol has any business in a formal proof and you won't find either one in standard LaTeX, so don't try typing them.

We'll need the following definition as we go forward.

Definition. (Rational) A number n is *rational*, denoted $n \in \mathbb{Q}$, if there exist integers a and b such that $n = {}^{a}/_{b}$. The number n is called *irrational* if no such integers exist.

6. The following proofs are written using contradiction, but no explanation is given as to what the contradiction is. Read the proof and find the contradiction.

   (a) There is no greatest even integer.

   Proof. Suppose for sake of contradiction that there is a greatest even integer N. Then for all $k \in \mathbb{Z}$, $n = 2k \leq N$. Let $M = N + 2$. □

   (b) The sum of any rational number and any irrational number is irrational.

   Proof. For the sake of contradiction, suppose there exists rational number x and irrational number y such that $(x + y)$ is rational. Then $x = {}^{a}/_{b}$ for $a, b \in \mathbb{Z}$ and

$b \neq 0$ and $(x+y) = {}^{c}/_{d}$ for $c, d \in \mathbb{Z}$ and $d \neq 0$. Using substitution,

$$\begin{aligned} x + y &= \frac{c}{d}, \\ \frac{a}{b} + y &= \frac{c}{d}, \\ y &= \frac{a}{b} - \frac{c}{d}, \\ y &= \frac{ad - bc}{bd}. \end{aligned}$$

□

(c) The cube root of 2 is irrational.

Proof. Suppose for sake of contradiction that $\sqrt[3]{2}$ is rational. Then there exist integers a and $b \neq 0$ such that $\sqrt[3]{2} = (a/b)$ and we may assume that (a/b) is fully reduced. Using algebra, we see

$$\begin{aligned} 2 &= \frac{a^3}{b^3} \\ 2b^3 &= a^3. \end{aligned}$$

Since $b^3 \in \mathbb{Z}$, we have that a^3 is even which we have seen previously means that a is even. Then $a = 2c$ for $c \in \mathbb{Z}$ and using substitution again,

$$\begin{aligned} 2b^3 &= (2c)^3, \\ 2b^3 &= 8c^3, \\ b^3 &= 4c^3. \end{aligned}$$

□

7. It's time to write some contradiction proofs of your own. As you work on each of the following, carefully consider how you might prove the claim without contradiction.

Claim 4. Suppose $n \in \mathbb{Z}$. If n is odd, then n^2 is odd.

Claim 5. Suppose $a, b \in \mathbb{R}$. If a is rational and ab is irrational, then b is irrational.

Claim 6. For every $x \in [^{\pi}/_{2}, \pi]$, $\sin(x) - \cos(x) \geq 1$.

(Hint: If $x \in [^{\pi}/_{2}, \pi]$, then $\sin(x) - \cos(x) > 0$.)

A point $P = (x, y) \in \mathbb{R}^2$ is called **rational** if both x and y are rational. That is, $P = (x, y)$ is rational if $P \in \mathbb{Q}^2$. 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 $F(x_0, y_0) = 0$.

Claim 7. The curve $x^2 + y^2 - 3 = 0$ has no rational points.