P.8 Contrapositive and Proof by Contrapositive

Proof by contrapositive is a very powerful proof technique. Technically speaking, any statement that can be proven with a direct proof can be proven with a contrapositive proof and vice versa. However, it is almost always the case that one proof is significantly easier to write.

Goals:

- Negate statements in a useful manner
- Construct contrapositive statements
- Write proofs using contrapositive statements.

Before we start working on writing proofs by contrapositive, let's review negating statements. Consider the following statements.

P : The number 2 is even.
Q : $x < y$.
R : Set $A = \emptyset$.

Recall that negating these statements is essentially putting the phrase "It is not true that" in front of the statement.

$\sim P$: It is not true that 2 is even. $\equiv$ The number 2 is odd.
$\sim Q$: It is not true that $x < y$. $\equiv$ $x \geq y$.
$\sim R$: It is not true that $A = \emptyset$. $\equiv$ $|A| > 0$.

Notice that two forms of the above statements are given. The first is the direct negation, while the second is, in some sense, a more helpful version of the negation.

1. Negate the following simple statements and open sentences. Express the negation in a more natural way if possible. That is, don't simple write "It is not true that" in front of the original statement.

   (a) The sum of a and b is odd.

   (b) $a \nmid 2b$.

   (c) $x \geq 1$.

It can be more complicated to negate a complicated statement or open sentence. Consider the statement below.

$$R: \text{ Integer } a \text{ is even and integer } b \text{ is odd.}$$
$$\sim R: \text{ It is not true that } a \text{ is even and } b \text{ is odd.}$$

Notice that the statement given for $\sim R$ does not tell us anything specific about a or b. Thus, it is the correct negation, but of no practical use. We can see that $R \equiv P \wedge Q$ if P : "Integer a is even" and Q : "Integer b is odd." Recall that by DeMorgan's Laws, $\sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q)$. Then we can express $\sim R$ as follows.

$$\sim R: \text{ Integer } a \text{ is odd } \textit{or} \text{ integer } b \text{ is even.}$$

2. Negate the following complicated statements using DeMorgan's Laws and the negation of a conditional statement.

   (a) $2 \mid a$ or $2 \nmid b$.

   (b) Integer 2 is a divisor of 10 and 20.

   (c) $x < 1$ or $x \geq 2$.

   (d) $-2 < x < 3$.

Now that we feel comfortable negating statements, let's recall what the contrapositive actually is. Fill in the following truth table.

P	Q	$P \Rightarrow Q$	$\sim Q$	$\sim P$	$\sim Q \Rightarrow \sim P$
T	T				
T	F				
F	T				
F	F				

Notice that the statements $P \Rightarrow Q$ and $\sim Q \Rightarrow \sim P$ are logically equivalent. That is, they produce they same truth values for any given P and Q. This means that if we are asked to prove a statement of the form $P \Rightarrow Q$, we can instead prove the statement $\sim Q \Rightarrow \sim P$. This probably doesn't seem like much of an improvement. Like integration by parts in Calculus 2, this seems to make things more difficult rather than less difficult. However, like integration by parts, contrapositive can be very handy in practice. Consider the following example.

$$P : n^2 \text{ is even}$$
$$Q : n \text{ is even}$$

If asked to prove this statement, we might start out with something like

"Suppose n^2 is even. Then $n^2 = 2a$ for $a \in \mathbb{Z}$."

Unfortunately, there's no clear way to turn this into a statement about n. (Give some thought as to why you can't just take the square root of each side of the equation.) On the other hand, the contrapositive is quite simple to prove.

3. (a) For the statements P and Q listed above, give the contrapositive of $P \Rightarrow Q$. Remember to restate the negations in a useful manner.

(b) Prove the contrapositive found in part (a) using a direct proof.

Before we really start writing proofs by contrapositive, we need to discuss two conventions that we'll use in this class. The first is used almost universally by mathematicians, and the second is just for the purposes of our class.

Let the reader know it's a contrapositive proof: Keep in mind that our proof reader is either someone who is skeptical of our claim or someone who doesn't fully understand our claim. If we decide to write a contrapositive proof rather than a direct proof, then our reader could quickly become very confused. For that reason, we always inform the reader at the start of the proof that we are writing a proof by contrapositive. The two most common ways to do this are as follows.

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

(i) *Proof.* (By Contrapositive) Suppose n is odd. Then ... □

(ii) *Proof.* We proceed by contrapositive, so suppose n is odd. Then ... □

Dr. J Wright prefers the first method be used by his students, and Dr. E Wright prefers the second.

Give the contrapositive: This convention is only for the purposes of this course, and shouldn't be used otherwise. Because you're new at this, it is a good idea to state the thing that you are trying to prove outright. This will prevent Dr. Wright from trying to decide if you're proving the wrong thing correctly or the right thing incorrectly if there's a problem. Our proof should appear as follows.

Proof. (By Contrapositive) [If n is odd, then n^2 is odd.] Suppose n is odd. Then ... □

4. You're finally ready. Prove the following claims using a proof by contrapositive. Follow all conventions.

Claim 2. Suppose $x \in \mathbb{Z}$. If $x^2 - 6x + 5$ is even, then x is odd.

Claim 3. Suppose $x, y \in \mathbb{Z}$. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.

Claim 4. Suppose a and b are integers. If $a + b$ is even and ab is even, then a and b are both even.

With a new proof technique comes new definitions.

Definition. Given integers a and b and an $n \in \mathbb{N}$, we say that a and b are **congruent modulo n** if (and only if) $n|(a - b)$. We express this as $a \equiv b \pmod{n}$. If a and b are not congruent modulo n, we write this as $a \not\equiv b \pmod{n}$. Here, n is referred to as the **modulus**.

5. This new definition really isn't so bad. We can think of it as saying $a \equiv b \pmod{n}$ if a and b have the same remainder when divided by n. For instance, $8 \equiv 14 \pmod{3}$ because $8 = 3(2) + \boxed{2}$ and $14 = 3(4) + \boxed{2}$. Determine if the following statements are true or false.

   (a) $7 \equiv 17 \pmod{5}$

(b) $24 \equiv 6 \pmod{6}$

(c) $-1 \equiv 4 \pmod{5}$

(d) $8 \equiv -2 \pmod{4}$

6. Prove the following claim using both direct proof and proof by contrapositive. Which proof is easier to write? Which is easier to understand? To prove the claim, you may apply the following variation of a result known as *Euclid's Lemma*.

   Lemma. Let $a, b, p \in \mathbb{Z}$. If p is prime and $p \,|\, ab$, then $p \,|\, a$ or $p \,|\, b$.

   Claim 5. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, then $c \equiv b \pmod{n}$.

7. There are no distinct rules about when to use a direct proof versus when to use proof by contrapositive. However, you may have developed some intuition about where you may want to start. List some ideas you have of how to decide between direct proof or proof by contrapositive.