CHAPTER 9

Contrapositive Proof

We now examine an alternative to direct proof called **contrapositive proof**. Like direct proof, the technique of contrapositive proof is used to prove conditional statements of the form *"If P, then Q."* Although it is possible to use direct proof exclusively, there are occasions where contrapositive proof is much easier.

9.1 Contrapositive Proof

To understand how contrapositive proof works, imagine that you need to prove a proposition of the following form.

Proposition If P, then Q.

This is a conditional statement of form $P \Rightarrow Q$. Our goal is to show that this conditional statement is true. Recall that in Section 3.6 we observed that $P \Rightarrow Q$ is logically equivalent to $\sim Q \Rightarrow \sim P$. For convenience, we duplicate the truth table that verifies this fact.

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

According to the table, statements $P \Rightarrow Q$ and $\sim Q \Rightarrow \sim P$ are different ways of expressing exactly the same thing. The expression $\sim Q \Rightarrow \sim P$ is called the **contrapositive form** of $P \Rightarrow Q$.[1]

Since $P \Rightarrow Q$ is logically equivalent to $\sim Q \Rightarrow \sim P$, it follows that to prove $P \Rightarrow Q$ is true, it suffices to instead prove that $\sim Q \Rightarrow \sim P$ is true. If we were

[1] Do not confuse the words *contrapositive* and *converse*. Recall from Section 3.4 that the *converse* of $P \Rightarrow Q$ is the statement $Q \Rightarrow P$, which is not logically equivalent to $P \Rightarrow Q$.

to use direct proof to show $\sim Q \Rightarrow \sim P$ is true, we would assume $\sim Q$ is true use this to deduce that $\sim P$ is true. This in fact is the basic approach of contrapositive proof, summarized as follows.

Outline for Contrapositive Proof

Proposition If P, then Q.

Proof. Suppose $\sim Q$.

⋮

Therefore $\sim P$. ■

So the setup for contrapositive proof is very simple. The first line of the proof is the sentence *"Suppose Q is not true."* (Or something to that effect.) The last line is the sentence *"Therefore P is not true."* Between the first and last line we use logic and definitions to transform the statement $\sim Q$ to the statement $\sim P$.

To illustrate this new technique, and to contrast it with direct proof, we now prove a proposition in two ways: first with direct proof and then with contrapositive proof.

Proposition Suppose $x \in \mathbb{Z}$. If $7x + 9$ is even, then x is odd.

Proof. (Direct) Suppose $7x + 9$ is even.
Thus $7x + 9 = 2a$ for some integer a.
Subtracting $6x + 9$ from both sides, we get $x = 2a - 6x - 9$.
Thus $x = 2a - 6x - 9 = 2a - 6x - 10 + 1 = 2(a - 3x - 5) + 1$.
Consequently $x = 2b + 1$, where $b = a - 3x - 5 \in \mathbb{Z}$.
Therefore x is odd. ■

Here is a contrapositive proof of the same statement:

Proposition Suppose $x \in \mathbb{Z}$. If $7x + 9$ is even, then x is odd.

Proof. (Contrapositive) Suppose x is not odd.
Thus x is even, so $x = 2a$ for some integer a.
Then $7x + 9 = 7(2a) + 9 = 14a + 8 + 1 = 2(7a + 4) + 1$.
Therefore $7x + 9 = 2b + 1$, where b is the integer $7a + 4$.
Consequently $7x + 9$ is odd.
Therefore $7x + 9$ is not even. ■

Though the proofs are of equal length, you may feel that the contrapositive proof flowed more smoothly. This is because it is easier to transform information about x into information about $7x+9$ than the other way around. For our next example, consider the following proposition concerning an integer x:

Proposition If x^2-6x+5 is even, then x is odd.

A direct proof would be problematic. We would begin by assuming that x^2-6x+5 is even, so $x^2-6x+5=2a$. Then we would need to transform this into $x=2b+1$ for $b\in\mathbb{Z}$. But it is not quite clear how that could be done, for it would involve isolating an x from the quadratic expression. However the proof becomes very simple if we use contrapositive proof.

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

Proof. (Contrapositive) Suppose x is not odd.
Thus x is even, so $x=2a$ for some integer a.
So $x^2-6x+5=(2a)^2-6(2a)+5=4a^2-12a+5=4a^2-12a+4+1=2(2a^2-6a+2)+1$.
Therefore $x^2-6x+5=2b+1$, where b is the integer $2a^2-6a+2$.
Consequently x^2-6x+5 is odd.
Therefore x^2-6x+5 is not even. ■

In summary, since x being not odd ($\sim Q$) resulted in x^2-6x+5 being not even ($\sim P$), then x^2-6x+5 being even (P) means that x is odd (Q). Thus we have proved $P\Rightarrow Q$ by proving $\sim Q\Rightarrow\sim P$. Here is another example:

Proposition Suppose $x,y\in\mathbb{R}$. If $y^3+yx^2\le x^3+xy^2$, then $y\le x$.

Proof. (Contrapositive) Suppose it is not true that $y\le x$, so $y>x$.
Then $y-x>0$. Multiply both sides of $y-x>0$ by the positive value x^2+y^2.

$$\begin{aligned}(y-x)(x^2+y^2) &> 0(x^2+y^2)\\ yx^2+y^3-x^3-xy^2 &> 0\\ y^3+yx^2 &> x^3+xy^2\end{aligned}$$

Therefore $y^3+yx^2>x^3+xy^2$, so it is not true that $y^3+yx^2\le x^3+xy^2$. ■

Proving *"If P, then Q,"* with the contrapositive approach necessarily involves the negated statements $\sim P$ and $\sim Q$. In working with these we may have to use the techniques for negating statements (e.g., DeMorgan's laws) discussed in Section 7.4. We consider such an example next.

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

Proof. (Contrapositive) Suppose it is not true that $5 \nmid x$ **and** $5 \nmid y$.
By DeMorgan's law, it is not true that $5 \nmid x$ **or** it is not true that $5 \nmid y$.
Therefore $5 \mid x$ or $5 \mid y$. We consider these possibilities separately.
Case 1. Suppose $5 \mid x$. Then $x = 5a$ for some $a \in \mathbb{Z}$.
From this we get $xy = 5(ay)$, and that means $5 \mid xy$.
Case 2. Suppose $5 \mid y$. Then $y = 5a$ for some $a \in \mathbb{Z}$.
From this we get $xy = 5(ax)$, and that means $5 \mid xy$.
The above cases show that $5 \mid xy$, so it is not true that $5 \nmid xy$. ■

9.2 Congruence of Integers

This is a good time to introduce a new definition. It is not necessarily related to contrapositive proof, but introducing it now ensures that we have a sufficient variety of exercises to practice all our proof techniques on. This new definition occurs in many branches of mathematics, and it will surely play a role in some of your later courses. But our primary reason for introducing it is that it will give us more practice in writing proofs.

Definition 9.1 Given integers a and b and an $n \in \mathbb{N}$, we say a and b are **congruent modulo n** if $n \mid (a - b)$. We express this as $a \equiv b \pmod{n}$. If a and b are not congruent modulo n, we write this as $a \not\equiv b \pmod{n}$.

Example 9.1 Here are some examples:

1. $9 \equiv 1 \pmod{4}$ because $4 \mid (9 - 1)$.
2. $6 \equiv 10 \pmod{4}$ because $4 \mid (6 - 10)$.
3. $14 \not\equiv 8 \pmod{4}$ because $4 \nmid (14 - 8)$.
4. $20 \equiv 4 \pmod{8}$ because $8 \mid (20 - 4)$.
5. $17 \equiv -4 \pmod{3}$ because $3 \mid (17 - (-4))$. ✍

In practical terms, $a \equiv b \pmod{n}$ means that a and b have the same remainder when divided by n. For example, we saw above that $6 \equiv 10 \pmod{4}$ and indeed 6 and 10 both have remainder 2 when divided by 4. Also we saw $14 \not\equiv 8 \pmod{4}$, and sure enough 14 has remainder 2 when divided by 4, while 8 has remainder 0.

To see that this is true in general, note that if a and b both have the same remainder r when divided by n, then $a = kn + r$ and $b = \ell n + r$ for some $k, \ell \in \mathbb{Z}$. Then $a - b = (kn + r) - (\ell n + r) = n(k - \ell)$. But $a - b = n(k - \ell)$ means $n \mid (a - b)$, so $a \equiv b \pmod{n}$. Conversely, Exercise 9.32 asks you to show that if $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n.

We conclude this section with several proofs involving congruence of integers, but you will also test your skills with other proofs in the exercises.

Proposition Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.

Proof. We will use direct proof. Suppose $a \equiv b \pmod{n}$.
By definition of congruence of integers, this means $n \mid (a - b)$.
Then by definition of divisibility, there is an integer c for which $a - b = nc$.
Now multiply both sides of this equation by $a + b$.

$$\begin{aligned} a - b &= nc \\ (a - b)(a + b) &= nc(a + b) \\ a^2 - b^2 &= nc(a + b) \end{aligned}$$

Since $c(a + b) \in \mathbb{Z}$, the above equation tells us $n \mid (a^2 - b^2)$.
According to Definition 9.1, this gives $a^2 \equiv b^2 \pmod{n}$. ■

Let's pause to consider this proposition's meaning. It says $a \equiv b \pmod{n}$ implies $a^2 \equiv b^2 \pmod{n}$. In other words, it says that if integers a and b have the same remainder when divided by n, then a^2 and b^2 also have the same remainder when divided by n. As an example of this, 6 and 10 have the same remainder (2) when divided by $n = 4$, and their squares 36 and 100 also have the same remainder (0) when divided by $n = 4$. The proposition promises this will happen for all a, b and n. In our examples we tend to concentrate more on how to prove propositions than on what the propositions mean. This is reasonable since our main goal is to learn how to prove statements. But it is helpful to sometimes also think about the meaning of what we prove.

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

Proof. We employ direct proof. Suppose $a \equiv b \pmod{n}$. By Definition 9.1, it follows that $n \mid (a - b)$. Therefore, by definition of divisibility, there exists an integer k for which $a - b = nk$. Multiply both sides of this equation by c to get $ac - bc = nkc$. Thus $ac - bc = n(kc)$ where $kc \in \mathbb{Z}$, which means $n \mid (ac - bc)$. By Definition 9.1, we have $ac \equiv bc \pmod{n}$. ■

Contrapositive proof seems to be the best approach in the next example, since it will eliminate the symbols $\nmid$ and $\neq$.

Proposition Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $12a \not\equiv 12b \pmod{n}$, then $n \nmid 12$.

Proof. (Contrapositive) Suppose $n \mid 12$, so there is an integer c for which $12 = nc$. Now reason as follows.

$$\begin{aligned} 12 &= nc \\ 12(a-b) &= nc(a-b) \\ 12a - 12b &= n(ca - cb) \end{aligned}$$

Since $ca - cb \in \mathbb{Z}$, the equation $12a - 12b = n(ca - cb)$ implies $n \mid (12a - 12b)$. This in turn means $12a \equiv 12b \pmod{n}$. ■

9.3 Mathematical Writing

Now that we have begun writing proofs, it is a good time to contemplate the craft of writing. Unlike logic and mathematics, where there is a clear-cut distinction between what is right or wrong, the difference between good and bad writing is sometimes a matter of opinion. But there are some standard guidelines that will make your writing clearer. Some are listed below.

1. **Begin each sentence with a word, not a mathematical symbol.** The reason is that sentences begin with capital letters, but mathematical symbols are case sensitive. Because x and X can have entirely different meanings, putting such symbols at the beginning of a sentence can lead to ambiguity. Here are some examples of bad usage (marked with ×) and good usage (marked with ✓).

   A is a subset of B. ×
   The set A is a subset of B. ✓

   x is an integer, so $2x+5$ is an integer. ×
   Because x is an integer, $2x+5$ is an integer. ✓

   $x^2 - x + 2 = 0$ has two solutions. ×
   $X^2 - x + 2 = 0$ has two solutions. × (and silly too)
   The equation $x^2 - x + 2 = 0$ has two solutions. ✓

2. **End each sentence with a period,** even when the sentence ends with a mathematical symbol or expression.

   Euler proved that $\displaystyle\sum_{k=1}^{\infty} \frac{1}{k^s} = \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}}$ ×
   Euler proved that $\displaystyle\sum_{k=1}^{\infty} \frac{1}{k^s} = \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}}$. ✓

Mathematical statements (equations, etc.) are like English phrases that happen to contain special symbols, so use normal punctuation.

3. **Separate mathematical symbols and expressions with words.** Not doing this can cause confusion by making distinct expressions appear to merge into one. Compare the clarity of the following examples.

   Because $x^2 - 1 = 0$, $x = 1$ or $x = -1$. ×
   Because $x^2 - 1 = 0$, it follows that $x = 1$ or $x = -1$. ✓

   Unlike $A \cup B$, $A \cap B$ equals $\emptyset$. ×
   Unlike $A \cup B$, the set $A \cap B$ equals $\emptyset$. ✓

4. **Avoid misuse of symbols.** Symbols such as $=$, $\leq$, $\subseteq$, $\in$, etc., are not words. While it is appropriate to use them in mathematical expressions, they are out of place in other contexts.

   Since the two sets are $=$, one is a subset of the other. ×
   Since the two sets are equal, one is a subset of the other. ✓

   The empty set is a $\subseteq$ of every set. ×
   The empty set is a subset of every set. ✓

   Since a is odd and x odd $\Rightarrow$ x^2 odd, a^2 is odd. ×
   Since a is odd and any odd number squared is odd, then a^2 is odd. ✓

5. **Avoid using unnecessary symbols.** Mathematics is confusing enough without them. Don't muddy the water even more.

   No set X has negative cardinality. ×
   No set has negative cardinality. ✓

6. **Use the first person plural.** In mathematical writing, it is common to use the words "we" and "us" rather than "I," "you" or "me." It is as if the reader and writer are having a conversation, with the writer guiding the reader through the details of the proof.

7. **Use the active voice.** This is just a suggestion, but the active voice makes your writing more lively.

   The value $x = 3$ is obtained through the division of both sides by 5. ×
   Dividing both sides by 5, we get the value $x = 3$. ✓

8. **Explain each new symbol.** In writing a proof, you must explain the meaning of every new symbol you introduce. Failure to do this can lead to ambiguity, misunderstanding and mistakes. For example, consider the following two possibilities for a sentence in a proof, where a and b have been introduced on a previous line.

Since $a \mid b$, it follows that $b = ac$. ×
Since $a \mid b$, it follows that $b = ac$ for some integer c. ✓

If you use the first form, then a reader who has been carefully following your proof may momentarily scan backwards looking for where the c entered into the picture, not realizing at first that it came from the definition of divides.

9. **Watch out for "it."** The pronoun "it" can cause confusion when it is unclear what it refers to. If there is any possibility of confusion, you should avoid the word "it." Here is an example:

   Since $X \subseteq Y$, and $0 < |X|$, we see that it is not empty. ×

   Is "it" X or Y? Either one would make sense, but which do we mean?

   Since $X \subseteq Y$, and $0 < |X|$, we see that Y is not empty. ✓

10. **Since, because, as, for, so.** In proofs, it is common to use these words as conjunctions joining two statements, and meaning that one statement is true and as a consequence the other true. The following statements all mean that P is true (or assumed to be true) and as a consequence Q is true also.

Q since P	Q because P	Q, as P	Q, for P	P, so Q
Since P, Q	Because P, Q	as P, Q		

    Notice that the meaning of these constructions is different from that of *"If P, then Q,"* for they are asserting not only that P implies Q, but **also** that P is true. Exercise care in using them. It must be the case that P and Q are both statements **and** that Q really does follow from P.

    $x \in \mathbb{N}$, so $\mathbb{Z}$ ×
    $x \in \mathbb{N}$, so $x \in \mathbb{Z}$ ✓

11. **Thus, hence, therefore consequently.** These adverbs precede a statement that follows logically from previous sentences or clauses. Be sure that a statement follows them.

    Therefore $2k + 1$. ×
    Therefore $a = 2k + 1$. ✓

12. **Clarity is the gold standard of mathematical writing.** If you believe breaking a rule makes your writing clearer, then break the rule.

Your mathematical writing will evolve with practice usage. One of the best ways to develop a good mathematical writing style is to read other people's proofs. Adopt what works and avoid what doesn't.

9.4 The Euclidean Algorithm

Proofs and algorithms intersect in various ways. As we will see later in this book, one can *prove* that a given algorithm works correctly. In another direction, propositions and theorems that have been proved may be used in algorithms. This section explores an example of such an algorithm – the famous Euclidean algorithm for computing the greatest common divisor of two numbers.

This algorithm is named after Euclid, who recorded it more than 2000 years ago (although it is unlikely that he himself discovered it). It is based on the following proposition.

Proposition If a and b are integers, then $\gcd(a,b) = \gcd(a-b,b)$.

Proof. (Direct) Suppose $a, b \in \mathbb{Z}$. We will first prove $\gcd(a,b) \leq \gcd(a-b,b)$, then $\gcd(a,b) \geq \gcd(a-b,b)$. Together these will imply $\gcd(a,b) = \gcd(a-b,b)$.

So let's prove $\gcd(a,b) \leq \gcd(a-b,b)$. Put $d = \gcd(a,b)$. As d is a divisor of both a and b, we have $a = dx$ and $b = dy$ for some integers x and y. Then $a - b = dx - dy = d(x-y)$, which means d divides $a-b$. Thus d is divisor of both $a-b$ and b. But it can't be greater than the *greatest* common divisor of $a-b$ and b, which is to say $\gcd(a,b) = d \leq \gcd(a-b,b)$.

Next let $e = \gcd(a-b,b)$. Then e divides both $a-b$ and b, so $a-b = ex$ and $b = ey$ for integers x and y. Then $a = (a-b)+b = ex+ey = e(x+y)$, so now we see that e is a divisor of both a and b. But it is not more than their *greatest* common divisor, that is, $\gcd(a-b,b) = e \leq \gcd(a,b)$.

The previous two paragraphs show $\gcd(a,b) = \gcd(a-b,b)$. ■

This proposition means that if we need to compute $\gcd(a,b)$, then we will get the same answer by computing $\gcd(a-b,b)$, which might be easier, as it involves smaller numbers.

For a concrete example, suppose we wanted to compute $\gcd(30,12)$. (Pretend for the moment that you don't see what the answer will be.) The proposition says $\gcd(30,12) = \gcd(30-12,12) = \gcd(18,12)$, so we have reduced our problem to that of finding $\gcd(18,12)$. For *this*, we can use the proposition *again* to get $\gcd(18,12) = \gcd(18-12,12) = \gcd(6,12)$. Using it a third time would give the negative value $6-12$, but we *can* interchange the numbers to get $\gcd(6,12) = \gcd(12,6)$, and the proposition applied twice to this yields $\gcd(12,6) = \gcd(12-6,6) = \gcd(6,6) = \gcd(6-6,6) = \gcd(0,6) = 6$. (Recall $\gcd(0,6) = 6$, as *every* integer is a divisor of 0, but the greatest divisor of 6 is 6. Similarly, $\gcd(0,b) = b$ when $b \neq 0$.) Multiple applications of the proposition have given $\gcd(30,12) = 6$.

Let's compute gcd(310,90) this way. We begin by continually subtracting 90 from 310 until getting gcd(40,90). At that point $40-90$ would be negative. So we swap the order of the numbers to get gcd(90,40), and continue the pattern, subtracting multiples of 40 from 90, as follows.

$$
\begin{array}{rl}
 & \left.\begin{array}{l}\gcd(310,90)\\ =\ \gcd(220,90)\\ =\ \gcd(130,90)\\ =\ \gcd(\ 40,90)\end{array}\right\} \text{keep subtracting 90 from number on left}\\
 & \text{swap numbers}\\
 & \left.\begin{array}{l}\gcd(90,40)\\ =\ \gcd(50,40)\\ =\ \gcd(10,40)\end{array}\right\} \text{keep subtracting 40 from number on left}\\
 & \text{swap numbers}\\
 & \left.\begin{array}{l}\gcd(40,10)\\ =\ \gcd(30,10)\\ =\ \gcd(20,10)\\ =\ \gcd(10,10)\\ =\ \gcd(\ 0,10)\end{array}\right\} \text{keep subtracting 10 from number on left}\\
= & \mathbf{10} \quad \longleftarrow \text{This is } \gcd(310,90).
\end{array}
$$

Eventually we get down to $\gcd(0,10)=10$, and stop. Thus $\gcd(310,90)=10$.

The Euclidean algorithm executes this exact pattern to compute $\gcd(a,b)$. It decrements a by b until $a<b$, then swaps a and b, and continues in this pattern until $a=0$, at which point it is down to $\gcd(0,b)=b$. (This new b is smaller than its original value.) Here it is.

Algorithm 10: Euclidean Algorithm

Input: Two positive integers a and b.
Output: $\gcd(a,b)$
begin
  while $a \neq 0$ **do**
    if $a<b$ **then**
      $c := a$
      $a := b$
      $b := c$ ..... swap a and b, so now $a \geq b$
    end
    while $a \geq b$ **do**
      $a := a-b$ ..... keep subtracting b from a until $a<b$
    end
  end
  output b
end

For pedagogical honesty we point out that the Euclidean algorithm is not used in a substantial way for the remainder of the book, though it is a good case study in some important ideas. We consider one of those ideas now: the idea that we can *prove* that an algorithm terminates (i.e., it does not go into an infinite loop).

Proposition If its input numbers a, b are positive, then the Euclidean algorithm terminates.

Proof. (Direct) Suppose a and b are positive. As the algorithm starts, the main while loop begins its first iteration, because $a \neq 0$.

Let's trace the first iteration of this loop. As it begins, if $a < b$ then a and b are interchanged. Regardless, we have $a \geq b$ after the if command. Then, in the second (inner) while loop begins and continually decrements a by b as long as $a \geq b$. As $a \geq b$, the value $a := a - b$ that is assigned to a is never negative. Thus, at the end of the first iteration we have $0 \leq a < b$.

If $a = 0$ there are no further iterations, and the algorithm finishes. Otherwise in the second iteration a and b are swapped because $a < b$. This decreases the value of b, and makes $a \geq b$. Then the inner while loop decreases the value of a until $a < b$. But also $0 \leq a$ because the assignment $a := a - b$ is only performed if $a \geq b$. Thus after the second iteration both a and b have decreased and $0 \leq a < b$.

This pattern continues in all further iterations. The iteration begins with $0 < a < b$. Then a and b are swapped, decreasing the value of b. Then a is decreased until $0 \leq a < b$.

So each iteration after the first decreases both of the integers a and b, resulting in $0 \leq a < b$. Thus after a finite number of iterations we must reach $a = 0$, at which point the algorithm terminates. ■

Notice that Euclidean algorithm does its job with just one arithmetic operation – subtraction. Given that subtraction is an easy operation, the Euclidean algorithm is very straightforward, efficient and fast, especially compared to other methods of computing greatest common divisors.

For instance, you are probably familiar with the technique of finding $\gcd(a, b)$ by comparing the prime factorizations of a and b. Given, say, 310 and 90, we prime factor them as

$$310 = 2 \cdot 5 \cdot 31 \qquad \text{and} \qquad 90 = 2 \cdot 3^2 \cdot 5.$$

The common prime factors are 2 and 5, and so $\gcd(310, 90) = 2 \cdot 5 = 10$. If we were going to write a gcd algorithm that took this approach, it would have to

find the prime factors of each number, compare them to each other, collect the common ones and multiply. Such an algorithm would be nowhere as simple as the Euclidean algorithm.

We close with one final remark. Look at the inner while loop in the Euclidean algorithm. It shares a striking resemblance to part of the division algorithm on page 176.

while $a \geq b$ **do**
  $a := a - b$
end

Before the while loop starts, we have $a = qb + r$ with $0 \leq r < b$, that is, b goes into a, q times with remainder r. When the while loop finishes, the q b's have been subtracted from a, and a has been replaced with r. In some versions of the Euclidean algorithm (in other texts), this while loop is replaced with the command

$a := r$ ..... where $a = qb + r$, by the division algorithm.

We have opted to code the computation of r directly into the Euclidean algorithm. See Exercise 9.31 below for a proposition leading to the alternate form of the Euclidean algorithm.

Exercises for Chapter 9

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

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

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

3. Suppose $a, b \in \mathbb{Z}$. If $a^2(b^2 - 2b)$ is odd, then a and b are odd.

4. Suppose $a, b, c \in \mathbb{Z}$. If a does not divide bc, then a does not divide b.

5. Suppose $x \in \mathbb{R}$. If $x^2 + 5x < 0$ then $x < 0$.

6. Suppose $x \in \mathbb{R}$. If $x^3 - x > 0$ then $x > -1$.

7. Suppose $a, b \in \mathbb{Z}$. If both ab and $a + b$ are even, then both a and b are even.

8. Suppose $x \in \mathbb{R}$. If $x^5 - 4x^4 + 3x^3 - x^2 + 3x - 4 \geq 0$, then $x \geq 0$.

9. Suppose $n \in \mathbb{Z}$. If $3 \nmid n^2$, then $3 \nmid n$.

10. Suppose $x, y, z \in \mathbb{Z}$ and $x \neq 0$. If $x \nmid yz$, then $x \nmid y$ and $x \nmid z$.

11. Suppose $x, y \in \mathbb{Z}$. If $x^2(y + 3)$ is even, then x is even or y is odd.

12. Suppose $a \in \mathbb{Z}$. If a^2 is not divisible by 4, then a is odd.

13. Suppose $x \in \mathbb{R}$. If $x^5 + 7x^3 + 5x \geq x^4 + x^2 + 8$, then $x \geq 0$.

B. Prove the following statements using either direct or contrapositive proof. Sometimes one approach will be much easier than the other.

14. If $a, b \in \mathbb{Z}$ and a and b have the same parity, then $3a + 7$ and $7b - 4$ do not.

15. Suppose $x \in \mathbb{Z}$. If $x^3 - 1$ is even, then x is odd.

16. Suppose $x \in \mathbb{Z}$. If $x + y$ is even, then x and y have the same parity.

17. If n is odd, then $8 \mid (n^2 - 1)$.

18. For any $a, b \in \mathbb{Z}$, it follows that $(a + b)^3 \equiv a^3 + b^3 \pmod 3$.

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

20. If $a \in \mathbb{Z}$ and $a \equiv 1 \pmod 5$, then $a^2 \equiv 1 \pmod 5$.

21. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod n$, then $a^3 \equiv b^3 \pmod n$

22. Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$. If a has remainder r when divided by n, then $a \equiv r \pmod n$.

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

24. If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $ac \equiv bd \pmod n$.

25. If $n \in \mathbb{N}$ and $2^n - 1$ is prime, then n is prime.

26. If $n = 2^k - 1$ for $k \in \mathbb{N}$, then every entry in Row n of Pascal's Triangle is odd.

27. If $a \equiv 0 \pmod 4$ or $a \equiv 1 \pmod 4$, then $\binom{a}{2}$ is even.

28. If $n \in \mathbb{Z}$, then $4 \nmid (n^2 - 3)$.

29. Write a recursive procedure to compute $\gcd(a, b)$. (This is the only exercise in this section that is not a proof.)

30. If $a \equiv b \pmod n$, then $\gcd(a, n) = \gcd(b, n)$.

31. Suppose the division algorithm applied to a and b yields $a = qb + r$. Then $\gcd(a, b) = \gcd(r, b)$.

32. If $a \equiv b \pmod n$, then a and b have the same remainder when divided by n.