## Contents

1. What is number theory? ........................................... 2  
2. Intro to proofs: Propositional logic .......................... 13  
3. Intro to proofs: Existential and universal quantifiers ...... 18  
4. Intro to proofs: Basic proof techniques ....................... 25  
5. Divisibility ......................................................... 29  
6. The Division-with-Remainder Theorem ....................... 33  
   6.1 Interlude: Proofs by Mathematical Induction ............ 33  
   6.2 Weak Induction and Strong Induction ..................... 36  
   6.3 Proof of the Division-with-Remainder Theorem .......... 37  
7. Greatest common divisors and the Euclidean Algorithm .... 42
1 What is number theory?

To put it succinctly, number theory is the study of the set of *natural numbers*: the positive integers 1, 2, 3, 4, ….

This may sound overly simplistic. How could an entire subject be built on such a simple premise as the numbers that we all learned about in elementary school? However, it turns out that many deep and fascinating problems arise very quickly from just asking questions about the natural numbers. In this chapter, our goal is just to demonstrate this by showing a few such questions, and give a little bit of the flavor of some of the techniques and concepts that arise in number theory.

The atoms of the natural number universe

One concept that very quickly arises in number theory is that of *prime numbers*. As you probably know, a natural number \( n \), other than 1, is called *prime* if its only factors are 1 and itself\(^1\).

What is the significance of prime numbers? The simple answer is that they are the building blocks of the natural numbers, in the following sense: every natural number can be written as a product of prime numbers, *and* this can be done in one and only one way. For example, \( 12 = 2 \cdot 2 \cdot 3 \), and other than reordering these factors, there is no other way to write 12 as a product of prime numbers. Similarly, \( 75 = 3 \cdot 5 \cdot 5 \), \( 79 = 79 \) (itself prime), and \( 82 = 2 \cdot 41 \). By analogy with the physical world, prime numbers are like the atoms of the natural numbers. Just as every molecule in the universe is made up of atoms, and different arrangements of atoms give rise to different types of molecules, similarly every natural number is made up of prime numbers multiplied together, and different collections of prime numbers will always have different products.

To briefly deal with the number 1, first consider this: if 1 were allowed as a prime number, this would violate the *uniqueness* part of the statement we made above. This is because we can write 6 as \( 2 \cdot 3 \), or \( 1 \cdot 2 \cdot 3 \), or \( 1 \cdot 1 \cdot 1 \cdot 1 \cdot 2 \cdot 3 \). If 1 were considered prime, all of these would be *different* ways of writing 6 as a product of prime numbers. You might also ask how we can write 1 as a product of prime numbers. Note that an empty product of numbers is 1.

---

\(^1\)You might be asking why 1 is explicitly excluded from this definition. Read on for the answer.
This is because, in a sense, 1 is the starting point for forming a product: to multiply 3 numbers, start with 1, then multiply it by the first number, then multiply the result by the second number, then multiply that result by the third number. Try doing this for 2 numbers, then for 1 number. When you get down to a product of 0 numbers, all you have is the starting point, which is 1. So the natural number 1 can also be written uniquely as a product of prime numbers, namely, the product of no prime numbers at all.

“Simple” questions about prime numbers

If prime numbers are important, one question we can ask immediately is how many prime numbers there are. Are there a fixed number of them, or are there infinitely many? Your intuition probably says that there are infinitely many, and that’s correct. This is not hard to prove, and we will do so fairly soon.

Another question that, knowing that there are infinitely many prime numbers, one might ask, is how often they occur within the natural numbers. Looking at the lowest natural numbers, we see primes occurring fairly often:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, ...

However, if we go further out into the natural numbers, they seem to occur much more rarely:

..., 5001, 5002, 5003, 5004, 5005, 5006, 5007, 5008, 5009, 5010, 5011, 5012, 5013, 5014, 5015, 5016, 5017, 5018, 5019, ...

So what can be said about the distribution of the prime numbers within the sequence of natural numbers? There are many, many answers to this question. Indeed, this is a story that has been developing for a few hundred years, and is still far from being completely answered.

One thing that you might notice from the above lists is that pairs of numbers that are two apart sometimes occur as primes. This occurs frequently in the lower numbers: 3 and 5, 5 and 7, 11 and 13, 17 and 19. However, even in the second list, there is still a pair like this: 5009 and 5011.

\(^2\)Note that pairs of consecutive numbers, other than 2 and 3, can never both be prime. This is because with two consecutive numbers, one must be even and the other odd, and an even number larger than 2 can never be prime.
Pairs of prime numbers such as these, separated by a distance of 2, are called twin primes. Here are some even larger pairs of twin primes: 9857 and 9859, 71,261 and 71,263, 104,681 and 104,683. As far out as mankind has been able to look into the prime numbers, we have always found more of them. So it is natural to ask, are there infinitely many pairs of twin primes? The answer is believed to be yes. But remarkably, even with all the sophistication of modern mathematics, no one has yet been able to prove this simple-sounding statement.

In a fascinating development to this story, some significant progress has been made on this problem very recently. In 2013, a mathematician named Yitang Zhang became the first to prove that there are infinitely many pairs of consecutive prime numbers separated by at most a certain finite distance. Specifically, if we let $p_n$ denote the $n^{th}$ prime number, Zhang proved that there are infinitely many pairs of consecutive primes $(p_n, p_{n+1})$ for which

$$p_{n+1} - p_n \leq 70,000,000.$$  
While that number 70,000,000 seems rather huge, this was the first time in history that anyone had been able to prove that there was any fixed bound for which such a statement is true. (Note that the twin prime conjecture is exactly this statement, with the number 70,000,000 replaced with the number 2.)

Immediately after Zhang announced his proof, mathematicians from around the world set out to whittle away at that number 70,000,000, and see if this bound could be made smaller. Before long, a worldwide, internet-organized project called Polymath was established to see how small the bound could be made. The project was organized and led largely by famed UCLA mathematician Terence Tao, but with contributions from literally hundreds of people all over the world. Over a period of months, they managed to bring the bound down from 70,000,000 all the way to 246. That is, the following is now a theorem; its proof is credited to an entire community of mathematicians$^3$:

**Theorem.** There are infinitely many pairs of consecutive primes $(p_n, p_{n+1})$ for which

$$p_{n+1} - p_n \leq 246.$$  

$^3$To hear more about this story, from Tao himself, see [https://www.youtube.com/watch?v=pp06oGD4m00](https://www.youtube.com/watch?v=pp06oGD4m00)
Another simple-sounding question that we can ask about the distribution of the prime numbers is how many primes there are in any particular interval of numbers. For this, we start by defining the prime-counting function:

\[ \pi(x) = \text{the number of prime numbers less than or equal to } x \]

Note that with this function, the number of primes in any half-open interval of real numbers \((x_1, x_2]\) is just \(\pi(x_2) - \pi(x_1)\).

Using a list of all the prime numbers up to 200 (on the left), or up to 10,000 (on the right), we can graph the function \(\pi(x)\):

![Graph of \(\pi(x)\)](image)

Obviously, the value of \(\pi(x)\) should “jump” by 1 exactly when \(x\) is a prime number, so it makes sense that the graph of this function has a stair-step shape, as the graph on the left shows. However, if we zoom out far enough on this picture, as we have done with the right graph, it starts to look like a smooth curve. One might be tempted to ask: is there a formula for a curve that closely approximates that graph?

Around the turn of the nineteenth century, Adrien-Marie Legendre conjectured that this curve is approximated by the function

\[ L(x) = \frac{x}{\log(x)} \]

where \(\log\) denotes the natural log function. Almost exactly 100 years later, in 1896, this was finally proved by two mathematicians, independently: Jacques Hadamard and Charles Jean de la Vallée-Poussin. More specifically, they proved that the function \(\pi(x)\) asymptotically approaches \(L(x)\), in the sense that the relative error (percent error) between the two functions tends to 0 as \(x\) goes to infinity:

\[ \lim_{x \to \infty} \frac{\pi(x) - L(x)}{x} = 0 \]
Finding good bounds on the error term, $|\pi(x) - f(x)|$, is an active area of research today. Indeed, perhaps the most famous unsolved problem in all of mathematics, known as the Riemann Hypothesis, is known to be equivalent to a certain bound on this type of error in approximations to the prime-counting function.

**Natural number solutions to equations**

Another type of problem studied in number theory is to find solutions to algebraic equations using only natural numbers. These are often referred to as *Diophantine problems*. For example, you are no doubt familiar with the formula

\[a^2 + b^2 = c^2\]

that occurs in the Pythagorean Theorem. In that theorem from geometry, $a$, $b$, and $c$ represent the lengths of the sides of a right triangle, so we usually think of them as being any positive real numbers. But are there solutions to this equation where $a$, $b$, and $c$ are all natural numbers?

You probably have seen some such solutions before. Probably the most well known is $3^2 + 4^2 = 5^2$, which gives the so-called “3-4-5 triangle”. Another well-known example is $5^2 + 12^2 = 13^2$. Let’s make a quick definition to make it easier to discuss these:

**Definition.** A triple of three natural numbers $(a, b, c)$ that satisfies $a^2 + b^2 = c^2$ is called a *Pythagorean triple*.

Here are a few Pythagorean triples:

\[
(3, 4, 5) \quad (5, 12, 13) \quad (6, 8, 10) \\
(8, 15, 17) \quad (15, 20, 25) \quad (28, 45, 53)
\]

Once again, after studying these for a little while, some natural questions arise: How many Pythagorean triples are there? Are there only finitely many, or infinitely many? Can we list them all in some way?

An easy way to see that there are infinitely many Pythagorean triples is to start with one, and scalar multiply the ordered triple by any number to get another Pythagorean triple. This works because, if $a^2 + b^2 = c^2$ and $d$ is any number, then

\[(da)^2 + (db)^2 = d^2a^2 + d^2b^2 = d^2(a^2 + b^2) = d^2c^2 = (dc)^2.\]
For example, starting with the Pythagorean triple \((3, 4, 5)\), doubling all three numbers gives the Pythagorean triple \((6, 8, 10)\). Multiplying by 3 gives \((9, 12, 15)\), which is another. Continuing in this way will obviously give infinitely many distinct Pythagorean triples.

But this also does not give all of them. As we can see from the above list, there are triples like \((5, 12, 13)\) and \((8, 15, 17)\) that are not scalar multiples of \((3, 4, 5)\). Starting with one of these other triples and scalar multiplying will give another infinite series of Pythagorean triples:

\[
\begin{align*}
(5, 12, 13) \text{ gives } & (10, 24, 26), \ (15, 36, 39), \ (20, 48, 52), \ldots \\
(8, 15, 17) \text{ gives } & (16, 30, 34), \ (24, 45, 51), \ (32, 60, 68), \ldots
\end{align*}
\]

Since this is an obvious way of getting many infinite lists of Pythagorean triples, let’s try to focus on just the Pythagorean triples that are the “starting points” of these lists. The thing that distinguishes these starting triples from the ones that have been scalar multiplied by some number is that in the latter type of triple, all three numbers share a common factor. For example, in \((6, 8, 10)\), all three numbers are multiples of 2; in \((15, 36, 39)\), all three numbers are multiples of 3. So we are more interested in the Pythagorean triples that don’t have a common factor.

**Definition.** A Pythagorean triple \((a, b, c)\) is called **primitive** if \(a\), \(b\), and \(c\) have no common factor.

It is not hard to prove that if any two of the numbers in a Pythagorean triple share a common factor, then the third number will also be a multiple of that same factor. By contrapositive, this definition is equivalent to saying that no two of \(a\), \(b\), and \(c\) have a common factor. (The fancy math way of saying this is that \(a\), \(b\), and \(c\) are **pair-wise relatively prime**.)

To study the primitive Pythagorean triples in greater depth, we will employ a clever geometric trick. Notice that if \(a^2 + b^2 = c^2\), then dividing both sides of this equation by \(c^2\) yields

\[
\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.
\]

Thus, for any Pythagorean triple \((a, b, c)\), we can let \(X = \frac{a}{c}\) and \(Y = \frac{b}{c}\), and the pair \((X, Y)\) will be a pair of **rational** numbers (because \(a\), \(b\), and \(c\) are integers) that satisfy the equation

\[
X^2 + Y^2 = 1.
\]
As everyone knows, this is the equation for the unit circle in the XY-plane. We will call a point in the XY-plane with rational coordinates a rational point. Since \(a, b,\) and \(c\) are positive integers, \(X\) and \(Y\) will also be positive numbers. So what we have just said is that

Every Pythagorean triple \((a, b, c)\) yields a rational point \((X, Y)\) on the unit circle with \(X > 0, Y > 0\), via the map

\[
(a, b, c) \mapsto (X, Y) = \left(\frac{a}{c}, \frac{b}{c}\right).
\]

It is easy to see that two Pythagorean triples that are scalar multiples of one another give rise to the same rational point on the circle, so it again makes sense to restrict our attention to the primitive Pythagorean triples.

Going the other direction, suppose we are given a rational point \((X, Y)\) on the unit circle, in the first quadrant. Since \(X\) and \(Y\) are rational numbers, we can choose a common denominator for them, and thereby write \(X = \frac{a}{c}\) and \(Y = \frac{b}{c}\) for some natural numbers \(a, b,\) and \(c\). Then since

\[
X^2 + Y^2 = \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1,
\]

we can multiply both sides by \(c^2\) to get \(a^2 + b^2 = c^2\). That is, \((a, b, c)\) is a Pythagorean triple. Furthermore, dividing out any common factor among them, we can make this into primitive Pythagorean triple, and as we just pointed out, this primitive Pythagorean triple will correspond to the same \((X, Y)\) that we started with.

In other words, we have now established a one-to-one correspondence between two sets: the set of primitive Pythagorean triples, and the set of rational points on the unit circle in the first quadrant. We will now proceed to parametrize the latter, which will in turn give us a parametrization of the former.

To parametrize the rational points on the unit circle, we will use a classic method called stereographic projection. Let \((X, Y)\) be any point on the unit circle other than \((-1, 0)\), and consider the line \(L\) through the point \((X, Y)\) and the point \((-1, 0)\), as in the following figure.
We will use the slope $m$ of the line $\mathcal{L}$ to parametrize the points $(X,Y)$. It is easy to see from the figure that points on the unit circle in the first quadrant will correspond to slopes between 0 and 1. What we need now is to find equations for $X$ and $Y$ in terms of the slope $m$.

From the point-slope formula, the equation for the line $\mathcal{L}$ is $Y = m(X+1)$. So to find $X$ and $Y$, we need to solve simultaneously the system of equations

\[
\begin{align*}
X^2 + Y^2 &= 1 \\
Y &= m(X + 1)
\end{align*}
\]

Substituting the second equation into the first gives

\[X^2 + m^2(X + 1)^2 = 1,\]

which can be simplified to

\[(1 + m^2)X^2 + 2m^2X + (m^2 - 1) = 0.\]  \hspace{1cm} (1)

We could try solving for $X$ using the quadratic formula, but there is an easier way. Solving Equation (1) should give us both points of intersection between the line and the circle, and we already know that one of those points is $(-1,0)$. So we already know that $X = -1$ is a solution to this equation, which means that we can factor out $(X+1)$ from it. The other factor will give us the other solution, which is the $X$ value of the other point of intersection, the one we’re actually interested in.

Equation (1) factors as

\[(X + 1)\left((1 + m^2)X + (m^2 - 1)\right) = 0.\]
So the solution we want is \( X = \frac{1 - m^2}{1 + m^2} \). Substituting this back into the equation for the line gives
\[
Y = m(X + 1) = m \left( \frac{1 - m^2}{1 + m^2} + 1 \right) = \frac{2m}{1 + m^2}.
\]
So the coordinates of the point on the circle, in terms of the slope \( m \), are
\[
(X, Y) = \left( \frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2} \right).
\]  
(2)

Now, since the slope of the line is \( m = \frac{Y - 0}{X - (-1)} = \frac{Y}{X+1} \), it is easy to see that when \( X \) and \( Y \) are rational numbers, \( m \) is also rational. And conversely, from Equation (2), it is easy to see that when \( m \) is rational, \( X \) and \( Y \) will be rational as well. Thus, Equation (2) establishes a one-to-one correspondence between the following two sets:
\[
\begin{align*}
\{ \text{rational points } (X,Y) \text{ on the} & \text{ unit circle with } X > 0, Y > 0 \} \\
\text{and} & \quad \{ \text{rational numbers } m \text{ with } 0 < m < 1 \}
\end{align*}
\]

Since we previously gave a one-to-one correspondence between the first of these sets and the set of primitive Pythagorean triples, we can now conclude the following:

**Theorem.** There are infinitely many primitive Pythagorean triples. To find all of them, let \( m \) be any rational number with \( 0 < m < 1 \), and compute \( X = \frac{1 - m^2}{1 + m^2} \) and \( Y = \frac{2m}{1 + m^2} \). Write \( X = \frac{a}{c} \) and \( Y = \frac{b}{c} \) for some natural numbers \( a \), \( b \), and \( c \), with no common factor among them. Then \( (a,b,c) \) is a primitive Pythagorean triple, and this process gives all of them.

**A few words about applications**

At this point, you may be asking, “What good is any of this? How do whole-number solutions to equations, or even the fact that natural numbers can all be written as products of prime numbers, relate to anything in the real world?” One answer is that number theory is one of the branches of mathematics farthest from any application to science. To most mathematicians, this makes it no less worthy of study. Artists create and study art, poets write verses, and musicians make music, all because these pursuits give them and others some sense of satisfaction, or because they find beauty in it. The
same is true of pure mathematics, the title given to mathematics that is not
directly concerned with applications to real world problems.

Number theory has often been called the purest branch of pure math,
precisely because of this lack of relevance to the real world. Some number
theorists may even take comfort in this lack of applicability. Indeed, the
famous twentieth century number theorist G. H. Hardy once wrote,

“No one has yet discovered any warlike purpose to be served by
the theory of numbers...and it seems unlikely that anyone will
do so for many years.”

However, Hardy’s prediction did turn out to be premature. Only a few
decades after he wrote this, number theory suddenly came to the forefront
of the blossoming subject of cryptography, a field which had been in its
infancy at the time of Hardy’s quote. Since the late 1970’s, number theory
has found extensive applications in cryptography. Moreover, since the late
1990’s, as the internet has proliferated into everyone’s homes, lifestyles, and
even pockets, certain aspects of computational number theory have become
an essential behind-the-scenes part of our everyday life. Indeed, today, when
you do almost anything on the internet, whether with your phone or tablet
or laptop, the privacy of that internet communication depends upon that
device doing some number theoretic calculations involving prime numbers.

We will learn all about this eventually. The number theory needed to
understand the basics of it is not all that advanced. But for now, we can
summarize the idea behind this as follows. Much of cryptography, the study
of secure communication, is based on the concept of mathematical functions
that can be computed easily, but whose inverse is extremely difficult to com-
pute without knowing some special piece of additional information. A classic
example of this is computing a product of two given numbers, versus the
inverse problem of factoring the resulting product back into the two original
numbers.

To be more specific, suppose that $p$ and $q$ are two prime numbers, and for
the sake of making this realistic, assume that they are both huge numbers,
perhaps 300 digits long each. It is not hard at all for a computer to multiply
these two numbers and find the product $n = pq$. A modern computer can
handle this in a fraction of a millisecond. However, if you give the computer
the resulting number $n$, without giving it any extra information about the
values of $p$ or $q$, then it is extremely difficult for the computer to find the
original numbers $p$ and $q$ that are the unique prime factors of $n$. What do we
mean by difficult? If all of the computers in the entire world worked together on the problem, all running the most sophisticated factoring algorithms currently known to mankind, it would still take them millions of years to find \( p \) and \( q \).
2 Intro to proofs: Propositional logic

A proposition is a statement that has a well-defined truth value, either true or false. We will use capital letters $P$, $Q$, $R$, ... to denote propositions.

Example 1.

$P = \text{It is raining.}$

$Q = \text{I brought an umbrella to school.}$

$R = \text{I ate cereal for breakfast today.}$

We can combine propositions with logical connectors, such as and, or, not, and implies (or “if-then”). This produces a propositional expression. The truth values of the propositions $P$ and $Q$ determine the truth value of a propositional expression such as $P \lor Q$ in fairly obvious ways: $P \lor Q$ is true if either $P$ is true, or $Q$ is true, or both, and is false otherwise (if both $P$ and $Q$ are false).

There are standard symbols for all of these logical connectors, as follows:

- $P \land Q$ means $P \text{ and } Q$
- $P \lor Q$ means $P \text{ or } Q$
- $\neg P$ means $P \text{ not}$ (or equivalently, “$P \text{ is false}”$)
- $P \rightarrow Q$ means $P \text{ implies } Q$ (or equivalently, “$P \text{ if } Q$”)
- $P \leftrightarrow Q$ means $P \text{ if and only if } Q$

Parentheses are often used in propositional expressions as well, such as in the expression

$$(P \land Q) \lor (\neg P \land \neg Q)$$

A simple way to understand the meanings of these logical connectors is using truth tables. For example, here is the truth table for $P \lor Q$:

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \lor Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
</tbody>
</table>

Here are the truth tables for the other logical connectors:
Perhaps the one of these which is the least obvious is the truth table for $P \rightarrow Q$. Certainly if $P$ is true and $Q$ is false, then $P \rightarrow Q$ must be false, and it makes sense that if both $P$ and $Q$ are true, then $P \rightarrow Q$ is true. But in the other cases, when $P$ is false, the statement $P \rightarrow Q$ says nothing about whether $Q$ should be true or false. So if $P$ is false, then no matter what truth value $Q$ has, we say that $P \rightarrow Q$ is true.

If that’s confusing, think about this with some actual statements in place of $P$ and $Q$, such as the statements from Example 1 above. Suppose I make a declaration that “if it is raining, then I bring an umbrella to school”. That is, let’s pretend that in my life, this statement is always true. What does this say about whether or not I bring an umbrella on days when it’s not raining? Perhaps I always bring an umbrella, regardless. Perhaps I never bring an umbrella when it’s not raining. Perhaps when it’s not raining, I flip a coin and decide whether or not to bring my trusty umbrella. In any of those cases, the statement “if it is raining, then I bring an umbrella to school” is still true. The one way it would be false is if there were a day when it did rain, and I did not bring an umbrella.

We say that two propositional expressions are equivalent (or logically equivalent) if they have the same truth value for all possible truth values of the propositional variables in each formula. For example, $P \leftrightarrow Q$ is logically equivalent to the formula

$$ (P \land Q) \lor (\neg P \land \neg Q) $$

mentioned earlier. We can see why by looking at the truth table for each formula. Here is a truth table for expression (3), built up step by step from left to right:
\begin{tabular}{cccccccc}
  & & & & & & & \\
P & Q & P \land Q & \neg P & \neg Q & \neg P \land \neg Q & (P \land Q) \lor (\neg P \land \neg Q) \\
F & F & F & T & T & T & T \\
F & T & F & T & F & F & F \\
T & F & F & F & T & F & F \\
T & T & T & F & F & F & T \\
\end{tabular}

Note that the last column is exactly the same as the column for \( P \iff Q \) in the truth tables above. This shows that these two propositional expressions are logically equivalent.

**Theorem 2.1.** Each of the following is true:

1. \( P \rightarrow Q \) is logically equivalent to \( \neg Q \rightarrow \neg P \).
2. \( P \leftrightarrow Q \) is logically equivalent to \( (P \rightarrow Q) \land (Q \rightarrow P) \).
3. \( \neg (P \lor Q) \) is logically equivalent to \( \neg P \land \neg Q \).
4. \( \neg (P \land Q) \) is logically equivalent to \( \neg P \lor \neg Q \).
5. \( \neg (\neg P) \) is logically equivalent to \( P \).

**Proof.** 1. (Proof by Faith T.)

\[
\begin{array}{cccccccc}
  & & & & & \neg Q & \neg P & \neg Q \rightarrow \neg P & P \rightarrow Q \\
P & Q & & & & & & & \\
F & F & T & T & T & T \\
F & T & T & T & T & T \\
T & F & T & F & F & F \\
T & T & F & F & T & T \\
\end{array}
\]

The last two columns are the same.

2. (Proof by Maddie Y.)

\[
\begin{array}{cccccccc}
  & & & & & \neg Q & \neg P & \neg Q \rightarrow \neg P & P \leftrightarrow Q \\
P & Q & P \rightarrow Q & Q \rightarrow P & (P \rightarrow Q) \land (Q \rightarrow P) & & & & \\
F & F & T & T & T & T & T \\
F & T & T & F & F & F & F \\
T & F & F & T & F & F & F \\
T & T & T & T & T & T & T \\
\end{array}
\]
The last two columns are the same.

3. (Proof by Aidan S.)

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Q</td>
<td>¬P</td>
<td>¬Q</td>
<td>P ∨ Q</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

The last two columns are the same.

4. (Proof by Christine D.)

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Q</td>
<td>¬P</td>
<td>¬Q</td>
<td>P ∧ Q</td>
<td>¬P ∨ ¬Q</td>
<td>¬(P ∧ Q)</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

The last two columns are the same.

5. (Proof by Leilani D.)

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>¬P</td>
<td>¬(¬P)</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

The first and last columns are the same.

Remark.
- In part (1), the if-then statement \( \neg Q \rightarrow \neg P \) is called the contrapositive of the if-then statement \( P \rightarrow Q \). Part (1) shows that a statement and its contrapositive are always logically equivalent. This will be a useful proof technique in some situations: instead of proving \( P \rightarrow Q \) directly, you might instead prove \( \neg Q \rightarrow \neg P \).
• Part (2) shows that to prove an if-and-only-if statement $P \leftrightarrow Q$, you can prove $P \rightarrow Q$ and $Q \rightarrow P$. Indeed, this is the standard strategy for proving an if-and-only-if statement.

• Parts (3) and (4) are called De Morgan’s Laws, named after the 19th-century British mathematician Augustus De Morgan. They give the standard way to negate a statement involving $\land$ or $\lor$.

• Part (5) is fairly obvious, but it says that a double negative $\neg \neg$ can be removed from a propositional expression.

**Exercise 1.** Find a propositional expression using only $\land$, $\lor$, and $\neg$ that is equivalent to $P \rightarrow Q$. Use this (and perhaps the rules from the previous theorem) to find a simple expression, again using only $\land$, $\lor$, and $\neg$, that is logically equivalent to $\neg(P \rightarrow Q)$.

**Solution.** (Solution of first part by Wei C.)

$$
\begin{array}{cccc}
P & Q & P \rightarrow Q & \neg P & \neg P \lor Q \\
F & F & T & T & T \\
F & T & T & T & T \\
T & F & F & F & F \\
T & T & T & F & T \\
\end{array}
$$

The third and last columns are the same.

(Solution of second part by Omar H.) The following expressions are all logically equivalent:

\[
\begin{align*}
\neg(P \rightarrow Q) \\
\neg(\neg P \lor Q) & \quad \text{(from the first part)} \\
\neg(\neg P) \land \neg Q & \quad \text{(by De Morgan’s Law for $\lor$)} \\
P \land \neg Q & \quad \text{(by Theorem 1 (5))}
\end{align*}
\]

**Remark.** This exercise shows that to disprove an if-then statement $P \rightarrow Q$, it is enough to find a situation where $P$ is true but $Q$ is false. This is referred to as finding a *counterexample*. (This is particularly true in the case where this if-then is preceded by a “For all . . .”. See the next section for more on that.)
3 Intro to proofs: Existential and universal quantifiers

In this section, we will need to start dealing with sets a little bit. Roughly speaking, in mathematics a set is just a collection of things. We use curly brackets \{ and \} to denote sets, as in

\[
S = \{2, 4, 6, 8, 10\} \\
P = \{2, 3, 5, 7, 11, 13, 17, 19, \ldots\} \\
B = \{\text{bears}\}
\]

Here the set \(S\) is a set of just five numbers, the even numbers between 2 and 10. The set \(P\) is intended to be the set of prime numbers. And the set \(B\) is the set of all bears.

We use the symbol \(\in\) to mean “is an element of”, so that \(6 \in S\), and \(13 \in P\), and Paddington \(\in B\). We can also write \(5 \notin S\) to mean that 5 is not an element of the set \(S\).

There are a few sets that have quite standard notation, which we’ll want to use from time to time. Since we are studying number theory, we will often want to refer to the set of all integers, denoted \(\mathbb{Z}\):

\[
\mathbb{Z} = \{-\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}.
\]

Although we won’t use them as much throughout this text, three other sets that have standard names and symbols are the set of all rational numbers, \(\mathbb{Q}\), the set of all real numbers, \(\mathbb{R}\), and the set of all complex numbers, \(\mathbb{C}\).

Of course, since number theory is the study of the natural numbers, we should have a symbol to denote the set of natural numbers as well. In this text, we will let \(\mathbb{N}\) denote the set of all natural numbers:

\[
\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}.
\]

Remark. The notation \(\mathbb{N}\) for the natural numbers is common, but unlike the other symbols mentioned above (\(\mathbb{Z}, \mathbb{Q}, \mathbb{R}\), and \(\mathbb{C}\)), this use of \(\mathbb{N}\) is not completely standard. Much worse, the precise notion of what one means by a natural number is also not completely standardized, due to one small discrepancy: whether or not 0 is considered a natural number. In this text, we are defining the natural numbers to exclude 0, however this is just a
convention. Many other textbooks (and other classes/instructors) define the
natural numbers exactly as we have here, but others (in particular in the
subject of mathematical logic) define the natural numbers to start from 0.
There is no definitive standard for this! Fortunately, in practice, it won’t
matter much whether 0 is included or not. But for the precise statements of
theorems and definitions, do make sure you know what convention is being
followed in any textbook or other source that you’re reading.

Returning to the topic of the previous chapter, we will often want to deal
with the logic of expressions such as \( x^2 < 1 \). However, this is not a proposition
(which must have a specific truth value), because we don’t know what the
value of \( x \) is. For some values of \( x \), \( x^2 < 1 \) is true, but for other values of \( x \), \( x^2 < 1 \) is false, whereas for other values of \( x \) (such as \( x = \text{Paddington} \)),
\( x^2 < 1 \) is completely meaningless. So to deal with logical expressions like
this, we introduce the following concept.

**Definition 3.1.** A *propositional function* is a function of one or more vari-
ables whose output is always a proposition. Given a propositional function
of some variable \( x \), the *universal set* for \( x \) (or just the *universe* of \( x \)) is the set
of all values of \( x \) that can be used as inputs to this function. That is, if the
propositional function is a function of a single variable, then the universal
set for that variable is just the domain of the propositional function.

**Examples.**

\[
\begin{align*}
P(x) &= \text{“}x^2 + 1 > 0\text{”} & \text{Universe: } x \in \mathbb{R} \\
Q(a,b) &= \text{“(}a < b\text{) } \lor \text{“(}b < a\text{)”} & \text{Universe: } a \in \mathbb{Z}, b \in \mathbb{Z} \\
R(x,y) &= \text{“}x \text{ loves } y\text{”} & \text{Universe: } x,y \in \{\text{people}\}
\end{align*}
\]

This means that \( P(5) \) is the proposition “\( 5^2 + 1 > 0 \)”, and \( P(-42) \) is the
proposition “\((-42)^2 + 1 > 0\)”. Note that here we are just plugging values
into a function, without worrying yet about whether or not the resulting
proposition is true. For example, \( R(\text{Professor Conley}, \text{Donald Trump}) \) is the
proposition “Professor Conley loves Donald Trump”. This proposition is
certainly false! But we can still plug these two values into the function \( R \) to
produce a valid proposition, regardless of its truth value.

If \( P(x) \) is a propositional function of a variable \( x \), and *every* element in
the universe of the variable \( x \) yields a proposition that is True, then we say
that the statement

\[
\text{For all } x, \ P(x)
\]
is true. Of course, we have some notation for this:

\[ \forall x \ P(x) \quad \text{means} \quad \text{For all } x, \ P(x) \]

The symbol \( \forall \) is called the **universal quantifier**, but you can just read it as “for all”, “for each”, “for any”, or “for every”.

If \( P(x) \) is a propositional function of a variable \( x \), and there is some element in the universe of the variable \( x \) for which the proposition \( P(x) \) is True, then we say that the statement

There exists \( x \) such that \( P(x) \)

is true. Once again, we have some notation for this as well:

\[ \exists x \ P(x) \quad \text{means} \quad \text{There exists } x \text{ such that } P(x) \]

The symbol \( \exists \) is called the **existential quantifier**, but you can just read it as “there exists” or “for some”.

**Examples.**

1. Universal set for \( x \): \( \mathbb{R} \)
   
   \[ P(x) = "x^2 + 1 > 0" \]
   
   \( \forall x \ P(x) \) is True.

2. Universal set for \( x \): \( \mathbb{R} \)
   
   \[ Q(x) = "x^2 = -1" \]
   
   \( \exists x \ Q(x) \) is False.

Note that the universal set matters! If in both of the preceding examples, we change the universe from \( \mathbb{R} \) to \( \mathbb{C} \), the truth values of the statements both change:

3. Universal set for \( x \): \( \mathbb{C} \)
   
   \[ P(x) = "x^2 + 1 > 0" \]
   
   \( \forall x \ P(x) \) is now False. (Consider \( x = i \), for example.)

4. Universal set for \( x \): \( \mathbb{C} \)
   
   \[ Q(x) = "x^2 = -1" \]
   
   \( \exists x \ Q(x) \) is now True. (Again, \( x = i \) works.)

**Note.** As the examples above show, the choice of the universal set often matters too much to be just guessed from the context of the statement.
So, although formal languages in the subject of mathematical logic usually prescribe these notations strictly as \( \forall x \, P(x) \) and \( \exists x \, P(x) \), most of the time in regular usage, mathematicians specify the universal set for each variable immediately after the quantifier, as in the following examples:

1. \( \forall x \in \mathbb{R} \, x^2 + 1 > 0 \)
2. \( \exists x \in \mathbb{R} \, x^2 = -1 \)
3. \( \forall x \in \mathbb{C} \, x^2 + 1 > 0 \)
4. \( \exists x \in \mathbb{C} \, x^2 = -1 \)

As before, these statements are (1) True, (2) False, (3) False, and (4) True.

Note that, in a statement with a mix of existential and universal quantifiers, the order of the quantifiers matters! For example, let \( \mathcal{H} \) be the set of all people, and let \( R(x, y) = \text{“} x \text{ loves } y \text{”} \). Think about what each of the following statements means. Do any of them have the same meaning? Are they all true or all false, or a mix of true and false statements?

1. \( \forall x \in \mathcal{H} \, \exists y \in \mathcal{H} \, x \text{ loves } y \)
2. \( \exists y \in \mathcal{H} \, \forall x \in \mathcal{H} \, x \text{ loves } y \)
3. \( \forall y \in \mathcal{H} \, \exists x \in \mathcal{H} \, x \text{ loves } y \)
4. \( \exists x \in \mathcal{H} \, \forall y \in \mathcal{H} \, x \text{ loves } y \)

**Negating a statement with quantifiers**

To negate a quantified statement, consider the following:

\[-(\forall x \, P(x))\]

means that it is not true that for every \( x \) in its universe, the proposition \( P(x) \) holds. That means that there must be some \( x \) for which \( P(x) \) is False. But this is the new statement

\( \exists x \, \neg P(x) \)

Similarly, the statement

\[-(\exists x \, P(x))\]
means that it is not true that there is some $x$ in its universe for which the proposition $P(x)$ holds. That is, there is no element $x$ in the universe for which $P(x)$ is True, or in other words, $P(x)$ is False for every possible $x$ in the universe. This is the new statement

$$\forall x \neg P(x)$$

So we have the following theorem.

**Theorem 3.2.**

- The statement $\neg(\forall x P(x))$ is logically equivalent to the statement $\exists x \neg P(x)$.
- The statement $\neg(\exists x P(x))$ is logically equivalent to the statement $\forall x \neg P(x)$.

**Example.** To negate a statement such as

$$\forall a \in \mathbb{Z} \ \exists n \in \mathbb{N} \ \forall x \in \mathbb{R} \ \text{blah blah blah...}$$

we have the following sequence of statements, each of which is logically equivalent to the one before it by the previous theorem:

$$\neg(\forall a \in \mathbb{Z} \ \exists n \in \mathbb{N} \ \forall x \in \mathbb{R} \ \text{blah blah blah...})$$

$$\exists a \in \mathbb{Z} \ \neg(\exists n \in \mathbb{N} \ \forall x \in \mathbb{R} \ \text{blah blah blah...})$$

$$\exists a \in \mathbb{Z} \ \forall n \in \mathbb{N} \ \neg(\forall x \in \mathbb{R} \ \text{blah blah blah...})$$

$$\exists a \in \mathbb{Z} \ \forall n \in \mathbb{N} \ \exists x \in \mathbb{R} \ \neg(\text{blah blah blah...})$$

Note the idea here: at each step, we are “moving the $\neg$ inside a quantifier”, and each time we do so, we switch the quantifier to the other type: $\forall$ becomes $\exists$, and $\exists$ becomes $\forall$.

**You will use this idea regularly in any setting where you must write proofs.** However, one area of mathematics where this becomes especially crucial is the subject of real analysis. (Real analysis is the name that mathematicians have given to the subject “calculus, but starting from scratch and rigorously proving everything as you go.” You’ll study this in Math 131A, and perhaps also 131B and 131C, if you take those classes in the future.) As an example where you can see this sort of thing immediately rearing its head, recall the formal definition of the limit of a function, which you probably saw in some previous calculus class:
**Definition.** Definition: Let \( a \in \mathbb{R} \), and let \( X \) be a set of real numbers containing an open interval around \( a \), except for possibly \( a \) itself. Let \( f : X \to \mathbb{R} \) be a function. We say that

\[
\lim_{x \to a} f(x) = L
\]

if for all \( \varepsilon > 0 \), there exists \( \delta > 0 \) such that for all \( x \in X \),

\[
|x - a| < \delta \quad \text{implies} \quad |f(x) - L| < \varepsilon.
\]

In this type of definition, it is implied that \( \varepsilon \) and \( \delta \) are real numbers, so we can take the universal set for each of them to be the set of positive real numbers. So let \( \mathbb{R}_+ \) denote the set of all positive real numbers. Then we can rewrite this definition in symbols as follows: \( \lim_{x \to a} f(x) = L \) means

\[
\forall \varepsilon \in \mathbb{R}_+ \exists \delta \in \mathbb{R}_+ \forall x \in X \quad (|x - a| < \delta \implies |f(x) - L| < \varepsilon)
\]

**Exercise 1.** Figure out what it means to say that \( \lim_{x \to a} f(x) \neq L \).

You probably want to start by writing this in symbols, as above. But you should also be able to write it in words, more like in the original definition.

**Solution.** (Provided by Wei C.)

\[
\lim_{x \to a} f(x) \neq L
\]

means that

\[
\exists \varepsilon \in \mathbb{R}_+ \forall \delta \in \mathbb{R}_+ \exists x \in X \quad (|x - a| < \delta \wedge |f(x) - L| \geq \varepsilon)
\]

\( \square \)

**Exercise 2.** Figure out what it means to say that \( \lim_{x \to a} f(x) \) does not exist.

Again, be able to state this in symbols or in words.
Solution. (Provided by Aidan S.)

\[ \lim_{x \to a} f(x) \] does not exist

means that

\[ \forall L \in \mathbb{R} \quad \exists \varepsilon \in \mathbb{R}_+ \quad \forall \delta \in \mathbb{R}_+ \quad \exists x \in X \quad (|x - a| < \delta \land |f(x) - L| \geq \varepsilon) \]

Exercise 3 (Extra challenge). Let \( f(x) = \cos\left(\frac{\pi}{x}\right) \). See if you can use what you came up with for exercise 2 to prove that

\[ \lim_{x \to 0} f(x) \] does not exist.

(Hints: The only thing you really need to know about this function \( f \) to prove this is that \( f\left(\frac{1}{n}\right) = \pm 1 \) for every whole number \( n \), and more specifically \( f\left(\frac{1}{n}\right) = 1 \) if \( n \) is even, and \( f\left(\frac{1}{n}\right) = -1 \) if \( n \) is odd. Also, to prove a statement of the form

\[ \forall L \in \mathbb{R} \quad P(L) \]

start by just assuming that \( L \) is any arbitrary element of \( \mathbb{R} \). We usually do this by writing simply “Let \( L \in \mathbb{R} \).” Then prove \( P(L) \).)

---

24
4 Intro to proofs: Basic proof techniques (direct, contrapositive, contradiction)

Proving a universally quantified (“for all...”) statement

To prove a statement about all numbers, or all functions, or all bears, the simplest way to start is to choose an arbitrary one of these things (an arbitrary number, any function, any bear). Then if you can deduce some fact about this thing, you will have proved that this fact must be true for all such things. The way we usually do this is simply by saying “Let $x$ be a number”, or “Assume $f$ is a function”, etc. As a silly example:

**Theorem.** All bears are brown.

**Proof.**

Let $b$ be a bear.

[ Insert the real content of the proof here: Use cleverness and ingenuity to deduce things about $b$, concluding with... ]

Therefore $b$ is brown.
Since $b$ was chosen arbitrarily among all bears, and we showed $b$ was brown, we have proved that all bears are brown. □

Proving an if-then statement: direct proof

To prove a logical implication $P \rightarrow Q$, that is, any statement of the form “If $P$ then $Q$”, the direct method is to assume that $P$ (the hypothesis) is true, and use this to deduce that $Q$ (the conclusion) is true. Once again, the simplest way to do this is to just state “Assume $P$”. Here is a real example, that also demonstrates the technique for “for all” statements.

Recall first that an integer $n$ is called even if there exists an integer $k$ such that $n = 2k$, and $n$ is called odd if there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$. As you know, any integer is either even or odd, and cannot be both.

**Theorem 4.1.** For all integers $n$, if $n$ is even then $n^2$ is even.

**Proof.**

Let $n \in \mathbb{Z}$.

[Deal with the “For all...”]
Assume $n$ is even.

[Assume the hypothesis.]
Then there exists $k$ such that $n = 2k$.

25
Therefore $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Therefore $n^2$ is even. [The conclusion!]

We have proved that if $n$ is even, then $n^2$ is even.

Since $n$ was chosen to be an arbitrary integer, this is true for all integers $n$.

---

**Proving an if-then statement: proof by contrapositive**

Another way to prove a statement of the form $P \rightarrow Q$ is to use the contrapositive. Recall that the contrapositive of $P \rightarrow Q$ is the statement $\neg Q \rightarrow \neg P$, and you proved in Theorem 2.1 (1) that these two are always logically equivalent. So proving $\neg Q \rightarrow \neg P$ is equivalent to proving $P \rightarrow Q$. This means that you start by assuming $\neg Q$, and then deduce $\neg P$ from that.

Here is an example. Note the difference between this proof and the previous one.

**Theorem 4.2.** For all integers $n$, if $n^2$ is even then $n$ is even.

**Proof.**

Let $n \in \mathbb{Z}$.
[Deal with the “For all...”]

Assume $n$ is not even. [Assume $\neg Q$.]

Then $n$ must be odd.
Then there exists $k$ such that $n = 2k + 1$.
(Note: We want to show at this point that $n^2$ is not even, hence is odd, which means that we need to show that there exists an integer $l$ such that $n^2 = 2l + 1$.)

Therefore $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$
$= 2(2k^2 + 2k) + 1$.
[So $2k^2 + 2k$ is the $l$.]

Therefore $n^2$ is odd. [Deduced $\neg P$!]

We have proved that if $n$ is not even, then $n^2$ is not even.

Now by contrapositive, if $n^2$ is even, then $n$ is even.

Since $n$ was chosen to be an arbitrary integer, this is true for all integers $n$. 

\[\square\]
Proof by contradiction

Finally, another common proof technique, that may seem similar to proof by contrapositive but is not quite the same, is proof by contradiction. Suppose you are trying to prove some conclusion \( Q \). To construct a proof by contradiction, start by assuming that \( Q \) is false. (That is, assume \( \neg Q \).) Then use this to deduce a contradiction: a statement that is obviously false, or that directly contradicts something you’ve already proved. If assuming \( Q \) is false leads to a contradiction, then certainly \( Q \) must be true.

Here is a classic example of a proof by contradiction, which uses the previously proved theorem as a small step along the way. Note the distinction between this type of proof and a proof by contrapositive: here we assume \( \neg Q \) just as before, but the conclusion we arrive at is not the negation of some hypothesis \( P \). Rather, the conclusion we come to is a statement that contradicts something we’ve already concluded within the proof.

**Theorem 4.3.** \( \sqrt{2} \) is not a rational number.

**Proof.**
Assume that \( \sqrt{2} \) is a rational number. [Assume \( \neg Q \).]
Then there exist integers \( a \) and \( b \), with \( b \neq 0 \), for which \( \sqrt{2} = \frac{a}{b} \). Furthermore, if \( a \) and \( b \) had any common factor, we could divide both by that common factor to get a fraction in lowest terms. Therefore, we may assume without loss of generality that \( a \) and \( b \) have no common factor.
Squaring both sides gives \( 2 = \frac{a^2}{b^2} \), so \( a^2 = 2b^2 \).
This means that \( a^2 \) is even.
By Theorem 4.2, \( a \) must be even.
So there exists \( k \in \mathbb{Z} \) such that \( a = 2k \).
Then \( a^2 = 2b^2 \) becomes \( 4k^2 = 2b^2 \).
Dividing by 2 yields \( b^2 = 2k^2 \), which means that \( b^2 \) is even.
Therefore by Theorem 4.2 again, \( b \) is even.
But now \( a \) and \( b \) are both even, meaning they have a common factor of 2. This contradicts the assumption we made earlier that \( a \) and \( b \) have no common factor. [Contradiction!]
Therefore our assumption that \( \sqrt{2} \) is rational must have been false.

---

\(^4\)Actually, there are some mathematicians who do not accept this premise. So-called “constructivist” or “intuitionist” logic disallows proof by contradiction. At the most basic level, this comes from rejecting a logical concept known as the Law of the Excluded Middle. However, most working mathematicians are perfectly okay with proofs by contradiction.
So $\sqrt{2}$ is not a rational number.
5 Divisibility

It is finally time for us to start doing a little bit of number theory! We begin with one of the most basic concepts that can be defined in the natural numbers.

Definition 5.1. Let $a$ and $b$ be integers. We say $b$ divides $a$ if there exists $k \in \mathbb{Z}$ such that $a = bk$. We write $b$ divides $a$ as

$$b \mid a.$$  

Remark.
1. The notation $b \mid a$ is very unfortunate, because this notation is perfectly symmetric looking, but the relationship that it describes is not at all symmetric! For example, it is true that $5 \mid 20$ (that is, 5 divides 20), but it is not true that $20 \mid 5$ (that is, 20 does not divide 5). Since the symbol $|$ is symmetric, it might be hard to remember at first which way it’s supposed to go.
2. When $b$ divides $a$, we can also say that $b$ is a divisor of $a$, or $b$ is a factor of $a$, or that $a$ is a multiple of $b$. These all mean the same thing.
3. If $b$ does not divide $a$, we can write $b \nmid a$.

Examples.
1. $4 \mid 12$, since $12 = 4 \cdot 3$.
2. For any integer $n$, $(n + 1) \mid (n^2 - 1)$, because $n^2 - 1 = (n + 1) \cdot (n - 1)$, and if $n$ is an integer, $n - 1$ will be an integer as well.

For now, we collect a few basic theorems about divisibility.

Theorem 5.2. Let $a,b,c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid (a + b)$.

Proof. (By Shehan F.)
Suppose $c \mid a$ and $c \mid b$.
Then, $\exists k \in \mathbb{Z}$ and $\exists l \in \mathbb{Z}$

$$a = ck \quad \text{and} \quad b = cl$$

Thus, $a + b = ck + cl = (k + l)c$.
Therefore, $c \mid (a + b)$.  

Theorem 5.3. Let $a, b, c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid (a - b)$.

Proof. (By Laetitia W.)
Suppose $c \mid a$ and $c \mid b$.
$c \mid a$ means $xc = a$ for some $x \in \mathbb{Z}$.
$c \mid b$ means $yc = a$ for some $y \in \mathbb{Z}$.
Subbing in values for $a$ and $b$:

$$a - b = xc - yc$$
$$a - b = c(x - y)$$

Therefore, $c \mid (a - b)$. □

Theorem 5.4. Let $a, b, c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid ab$.

Proof. (By Lucas M.)
Suppose $c \mid a$ and $c \mid b$.
$c \mid a \leftrightarrow \exists k \in \mathbb{Z} \ a = ck$, $c \mid b \leftrightarrow \exists n \in \mathbb{Z} \ b = cn$
Multiplying the equations, $ab = c^2 nk = c(cn k)$
\[ \exists k \in \mathbb{Z} \ x = cn k \]
\[ ab = cx \rightarrow c \mid ab \] □

Remark. Can you come up with a simpler version of Theorem 5.4? It should be a “stronger” theorem. Why? What do I mean by “stronger” here?

Solution. (By Aidan S.)
You don’t need to assume both $c \mid a$ and $c \mid b$. Just assuming one or the other is enough:

Theorem. Let $a, b, c$ be integers. If $c \mid a$, then $c \mid ab$.

Proof. Assume $c \mid a$. So $\exists k \in \mathbb{Z}$ s.t. $a = kc$.
So $ab = kcb = (kb)c$. Since $kb \in \mathbb{Z}$, we have $c \mid ab$. □

This is a “stronger” theorem because we are not assuming as many things, but we reach the same conclusion as before.

Another way of saying this is that we have “weakened the hypothesis”. When you can state a theorem with a weaker hypothesis (i.e. not assuming as many things) but the same conclusion, you have stated a stronger theorem. □
Theorem 5.5. Let $a$, $b$, and $c$ be integers. If $c \mid a$ and $c \mid b$, then $c \mid (ax+by)$ for any $x, y \in \mathbb{Z}$.

Proof. (By Maddie Y.)
Assume $c \mid a$ and $c \mid b$.
$\exists k \in \mathbb{Z}$ s.t. $a = ck$.
$\exists m \in \mathbb{Z}$ s.t. $b = cm$.
Let $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$.
$ax + by = ckx + cmy$ by substitution.
$ax + by = (kx + my)c$
$kx + my \in \mathbb{Z}$
So $c \mid (ax + by)$.
Since $x$ and $y$ were chosen arbitrarily from $\mathbb{Z}$, we have shown that for all $x, y \in \mathbb{Z}$, $c \mid (ax + by)$. \hfill $\Box$

Theorem 5.6. Let $a, b \in \mathbb{N}$. If $b \mid a$ then $b \leq a$.

Proof. (By Mien T., Christine D.)
Assume that $b \mid a$ is true.
$b$ divides $a$ iff there exists some integer $k$ such that $a = bk$.
$b = \frac{a}{k} = k \cdot \frac{1}{k} \cdot a$
$\therefore k \in \mathbb{N}$ \therefore $k \geq 1$ \therefore $\frac{1}{k} \leq 1$ \therefore $\frac{1}{k} - 1 \leq 0$
$b - a = \frac{1}{k} \cdot a - a = \left(\frac{1}{k} - 1\right) a \leq 0$ (since $a \geq 0$)
$b - a \leq 0$
$b \leq a$ \hfill $\Box$

Theorem 5.7. Let $a$ and $b$ be natural numbers. If $b \mid a$ and $a \mid b$ then $a = b$.

Proof. (By Samanda H.)
Assume that $b \mid a$ and $a \mid b$.
Since $b \mid a$, $b \leq a$.
Since $a \mid b$, $a \leq b$.
Therefore $a = b$. \hfill $\Box$

Having now defined divisors, we can proceed to define what is perhaps the most important concept in all of number theory:
Definition 5.8. An integer $n > 1$ is called a prime number if the only natural numbers that divide $n$ are 1 and $n$.

Prime numbers are a theme that will come up over and over again in this course. But for now, just knowing the definition will suffice.
6 The Division-with-Remainder Theorem

Theorem 6.1 (The Division-with-Remainder Theorem\textsuperscript{5}). Let \( a \) and \( b \) be integers, with \( b > 0 \). Then there exist unique integers \( q \) and \( r \) such that

\[ a = bq + r \quad \text{and} \quad 0 \leq r < b. \]

Remark. We will prove this theorem soon, but first, notice that the idea of the theorem is something you probably learned many years ago: you are trying to divide \( a \) by \( b \). The number \( q \) that you get is called the quotient, and the number \( r \) is called the remainder. For example, consider dividing 52 by 15. In elementary school, you might have said something like

\[ 52 \div 15 = 3 \text{ with remainder 7}. \]

What this means, and exactly what the theorem concludes, is that

\[ 52 = 15 \cdot 3 + 7, \]

which is easy to verify. Furthermore, to see that 7 is the correct remainder, note that \( 0 \leq 7 < 15 \).

Examples.

- \( a = 22, b = 5 \):
  \[ 22 = 5 \cdot 4 + 2 \]

- \( a = 9374, b = 38 \):
  \[ 9374 = 38 \cdot 246 + 26 \]

- \( a = -26, b = 6 \):
  \[ -26 = 6 \cdot (-5) + 4 \]
  Note that in this example, we didn’t use \( q = -4 \) and \( r = -2 \), which would also give the correct calculation \( (-26 = 6 \cdot (-4) + -2) \), because the theorem requires the remainder \( r \) to be nonnegative.

6.1 Interlude: Proofs by Mathematical Induction

To prove the Division-with-Remainder Theorem, we will need to employ a new type of proof, which we will now explore. Suppose we want to prove a statement of the form

\[ \text{For all } n \in \mathbb{N}, \quad P(n). \quad (4) \]

\textsuperscript{5}This theorem is also known as The Division Algorithm, even though it’s not an algorithm. The concept is also sometimes called Euclidean Division, although Euclid had nothing to do with it, and may not have even known this theorem.
where $P(n)$ is some propositional function that says something about natural numbers $n$. Sometimes, the easiest way to prove such a statement is to use a sort of iterative proof: first verify that $P(n)$ is true for $n = 1$; then prove that for any $n \in \mathbb{N}$, if $P(n)$ is true, then $P(n + 1)$ is true. (In symbols, this latter step is to prove that $\forall n \in \mathbb{N} \quad P(n) \rightarrow P(n + 1)$.) This will then mean that we can make the following series of deductions:

- $P(1)$ is true.
- We proved that if $P(1)$ is true, then $P(2)$ is true. Therefore $P(2)$ is true.
- We proved that if $P(2)$ is true, then $P(3)$ is true. Therefore $P(3)$ is true.
- We proved that if $P(3)$ is true, then $P(4)$ is true. Therefore $P(4)$ is true.
- We proved that if $P(4)$ is true, then $P(5)$ is true. Therefore $P(5)$ is true.
- Etc.

Since we could continue this process forever and would eventually reach any $n$, $P(n)$ must be true for all natural numbers $n$.

The reasoning that we have just described is called a proof by mathematical induction (though this is often shortened to just “proof by induction”). Note that this type of proof can only be applied to a statement that has the form (4). In particular, it can only be used to prove that something is true for all natural numbers. This basic process can be modified slightly, for example to start at $n = 0$ (and thus prove that a statement is true for all nonnegative integers), or to start at, say, $n = 3$ (and thus prove that a statement is true for all integers $\geq 3$). You could also use induction to prove that a statement is true for all integers, but you would essentially have to do two separate proofs: one going in the upward direction (prove that $P(n) \rightarrow P(n + 1)$ for all $n \geq 0$), and one in the downward direction (prove that $P(n) \rightarrow P(n - 1)$ for all $n \leq 0$). Usually, the latter is not necessary, so induction proofs are generally only employed for proofs involving the natural numbers (or nonnegative integers). In particular, proof by induction cannot be used to prove statements about all real numbers, or all complex numbers, etc.
Here is the basic structure that every proof by mathematical induction must follow, with standard names given to certain parts of the proof:

Proof.

**Base case:** [Prove that \( P(1) \) is true.]

**Induction step:** Let \( n \in \mathbb{N} \). Assume that \( P(n) \) is true. (This is called the induction hypothesis.)

[Now prove that \( P(n + 1) \) is true. The crucial thing will be to somehow use the induction hypothesis, that \( P(n) \) is true, to prove this. So you will need to somehow take the new statement \( P(n + 1) \) and “relate it back” to the statement \( P(n) \), then use the fact that \( P(n) \) is true to “go forward” and prove that \( P(n + 1) \) is true. This sort of back and forth is characteristic of all induction proofs.]

We have now proved that, for all \( n \in \mathbb{N} \), \( P(n) \rightarrow P(n + 1) \).

Therefore, by mathematical induction, \( P(n) \) is true for all \( n \in \mathbb{N} \). \( \square \)

It is highly recommended that whenever you write an induction proof, you start by stating and proving the base case, then clearly state your induction hypothesis (starting with “Assume...”). Then prove the statement is true for \( n + 1 \), and conclude that “by induction, the statement is true for all \( n \)”.

As a fairly simple first example, we will prove the following:

**Theorem.** For all \( n \in \mathbb{N} \),

\[
1^2 + 2^2 + \cdots + n^2 = \frac{n(n + 1)(2n + 1)}{6}.
\]  

(5)

Proof.

**Base case:** \( (n = 1) \) When \( n = 1 \), the sum on the left hand side of (5) is just \( 1^2 \), which evaluates to 1. And the expression on the right hand side of (5) is \( \frac{1 \cdot 2 \cdot 3}{6} \), which also evaluates to 1. So when \( n = 1 \), equation (5) is true.

**Induction step:** Let \( n \in \mathbb{N} \). Assume that

\[
1^2 + 2^2 + \cdots + n^2 = \frac{n(n + 1)(2n + 1)}{6}.
\]  

(induction hypothesis)

We now want to prove that equation (5) is true for \( n + 1 \). That is, we want to prove that

\[
1^2 + 2^2 + \cdots + (n + 1)^2 = \frac{(n + 1)((n + 1) + 1)(2(n + 1) + 1)}{6}.
\]  

(6)
Substituting the induction hypothesis into the left hand side of (6), then simplifying, we get

\[
(1^2 + 2^2 + \cdots + n^2) + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2
\]

\[
= \frac{n(n+1)(2n+1)}{6} + \frac{6(n+1)^2}{6}
\]

\[
= \frac{(n+1)(n(2n+1) + 6(n+1))}{6}
\]

\[
= \frac{(n+1)(2n^2 + 7n + 6)}{6}
\]

\[
= \frac{(n+1)(n+2)(2n+3)}{6}
\]

The right hand side of (6) easily simplifies to the same thing as the last line above, so we have proved that equation (6) is true.

We have now proved that, for all \( n \in \mathbb{N} \), equation (5) implies equation (6). That is the induction step.

Therefore, by induction, equation (5) is true for all \( n \in \mathbb{N} \).

\[
\square
\]

### 6.2 Weak Induction and Strong Induction

Sometimes, when writing a proof by induction, it is not enough to just use the \( n \) case of a statement to prove the \( n+1 \) case. Rather, you may need to use the \( n-1 \) and the \( n \) cases to prove the \( n+1 \) case. Or you may need to use any or all of the cases that came before \( n+1 \) to prove the \( n+1 \) case. Doing this is completely valid, but just requires a different (stronger) induction hypothesis. Therefore, this type of proof is often referred to as a proof by strong induction. Here is a sketch of the general structure of a strong induction proof. Contrast this with the sketch of an induction proof given in the previous section.

**Proof.**

**Base case(s):** [Prove that \( P(1) \) is true, and possibly additional cases: \( P(2), P(3), \text{ etc.} \)]

**Induction step:** Let \( n \in \mathbb{N} \). Assume that for all natural numbers \( k \leq n \), \( P(k) \) is true. (This is the strong induction hypothesis.)

[Now prove that \( P(n+1) \) is true. The crucial thing will be to somehow...]

36
use the induction hypothesis, that $P(k)$ is true for all $k \leq n$, to prove this. Just as before, you will need to somehow take the new statement $P(n+1)$ and “relate it back” to previous cases. But in this case, you can relate it to any statement $P(k)$ for any $k \leq n$. Use the fact that one (or many, or all) of these are true to “go forward” and prove that $P(n+1)$ is true.}

We have now proved that, for all $n \in \mathbb{N}$, if $\forall k \leq n \ P(k)$, then $P(n+1)$. Therefore, by mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

Note that the key difference in the way the proof is set up is the induction hypothesis. In a regular induction proof, the induction hypothesis is simply

Assume that $P(n)$ is true.

In a strong induction proof, the induction hypothesis is

Assume that for all $k \leq n$, $P(k)$ is true.

The fact that you are assuming more here, that is, that this is a stronger hypothesis, is why this is called “strong mathematical induction”. In light of this, the type of induction proof we described in the previous section is sometimes called “weak induction”.

It is worth noting, however, that there is nothing that is actually stronger about strong induction than about weak induction. They are actually logically equivalent, in the sense that it is possible to use regular (weak) induction to prove that strong induction is valid. Or, to put that another way, any proof by strong induction could be rewritten to use weak induction. But in many cases, it would be much more complicated, so the use of strong induction is more convenient.

As a real example of a proof by strong induction, we will use this technique to prove the existence part of the Division-with-Remainder Theorem.

### 6.3 Proof of the Division-with-Remainder Theorem

Before we finally get to the proof of this theorem, we should also discuss how to prove a uniqueness statement in general, as this is a common ingredient in many mathematical theorems. Suppose we want to prove a theorem that says, “There exists a unique $n \in \mathbb{N}$ for which ….” Very often, the proof of such a statement will be broken into two distinct parts: one proof that
there is such a number \( n \) (existence), and another proof that there is only one such \( n \) (uniqueness). For the uniqueness part, the standard way to set up the proof is to assume that \( n_1 \) and \( n_2 \) are numbers that each satisfy the statement. Then prove that \( n_1 = n_2 \). This will prove that there is only one number that satisfies the statement.

Note that I didn’t just say to “assume that \( n_1 \) and \( n_2 \) are different numbers that each satisfy the statement”. Rather, I just gave these two variables different names; they turn out in the proof to be equal. It is possible to do this instead as a proof by contradiction: assume that \( n_1 \) and \( n_2 \) both satisfy the statement, and that \( n_1 \neq n_2 \), then deduce a contradiction from this. However, usually this is unnecessary. Indeed, usually the contradiction that you’ll arrive at will be that \( n_1 = n_2 \), so that a direct proof would have been simpler!

**Proof of Theorem 6.1.**

(Existence) Let \( b \) be a natural number, which we will assume is fixed throughout this part of the proof. We will use strong induction (on the variable \( a \)) to prove that for all nonnegative integers \( a \), there exist \( q, r \in \mathbb{Z} \) such that \( a = bq + r \) and \( 0 \leq r < b \).

**Base cases:** Suppose \( a \in \mathbb{Z} \), and \( 0 \leq a < b \). (That is, we have \( b \) different base cases: \( a = 0 \), \( a = 1 \), \( a = 2 \), \ldots, \( a = b - 1 \).) Let \( q = 0 \) and \( r = a \). Then \( a = bq + r \) and \( 0 \leq r < b \).

**Induction step:** Let \( a \) be an integer, greater than or equal to \( b - 1 \) (the last of our base cases). Assume the following (our strong induction hypothesis):

For all \( k \in \mathbb{Z} \) with \( 0 \leq k \leq a \), there exist \( q, r \in \mathbb{Z} \) such that \( k = bq + r \) and \( 0 \leq r < b \).

We now want to prove the existence of such a \( q \) and \( r \) for \( a + 1 \). To do this, let \( a' = a + 1 - b \). Since \( b > 0 \) and \( a \geq b - 1 \), we have \( 0 \leq a' \leq a \), and therefore our induction hypothesis applies to \( a' \). So there exist \( q', r' \in \mathbb{Z} \) such that

\[
a' = bq' + r' \quad \text{and} \quad 0 \leq r' < b.
\]

Therefore

\[
a + 1 = a' + b = bq' + r' + b = b(q' + 1) + r'.
\]
Letting $q = q' + 1$ and $r = r'$, we have

$$a + 1 = bq + r \quad \text{and} \quad 0 \leq r < b.$$  

Therefore, by induction, we have that for all integers $a \geq 0$, there exist $q, r \in \mathbb{Z}$ such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$  

The proof above works for all integers $a \geq 0$, but we still need to prove that this is true for negative integers $a$. But rather than doing another induction proof, let’s use what we have just proved. So let $a \in \mathbb{Z}$, and assume $a < 0$. Let $a' = -a$, so that $a' > 0$. Then, applying what we proved above, there exist $q', r' \in \mathbb{Z}$ such that

$$a' = bq' + r' \quad \text{and} \quad 0 \leq r' < b.$$  

If $r' = 0$, then we can let $q = -q'$ and $r = 0$, and we have

$$a = -a' = -(bq') = b(-q') = bq = bq + r,$$

as required. On the other hand, if $r' > 0$, then

$$a = -a' = -(bq' + r') = b(-q') - r' = b(-q' - 1) + (b - r'),$$

so we can let $q = -q' - 1$ and $r = b - r'$, and we have the desired result.

(Uniqueness) (By Wei C., Aidan S.)

Assume there exist $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ such that

$$a = bq_1 + r_1 \quad \text{with} \quad 0 \leq r_1 < b \quad \text{and} \quad a = bq_2 + r_2 \quad \text{with} \quad 0 \leq r_2 < b.$$  

Then $q_1b + r_1 = q_2b + r_2$.

So $b(q_1 - q_2) = r_2 - r_1$, and thus $b \mid (r_2 - r_1)$.

Negating the inequality $0 \leq r_1 < b$ gives $-b < -r_1 \leq 0$. Adding this to the inequality $0 \leq r_2 < b$ then gives

$$-b < r_2 - r_1 < b$$

The only integer in this range that is a multiple of $b$ is 0, so therefore $r_2 - r_1 = 0$, and thus $r_1 = r_2$.

But now $b(q_1 - q_2) = 0$, so since $b > 0$, we can divide this equation by $b$ to get $q_1 - q_2 = 0$, and therefore $q_1 = q_2$. 

\[\square\]
Theorem 6.2. Let \( a, b \in \mathbb{Z} \) with \( b > 0 \). Assume that \( q \) and \( r \) are integers such that \( a = b \cdot q + r \) and \( 0 \leq r < b \), as given by the Division-with-Remainder Theorem. Then

(a) \( b \mid a \) if and only if \( r = 0 \).

(b) If \( c \mid a \) and \( c \mid b \), then \( c \mid r \).

(c) If \( c \mid b \) and \( c \mid r \), then \( c \mid a \).

Proof. (a) (By Christine D.)

\[ (\to) \text{ Suppose } b \mid a. \]

By definition, \( \exists k \in \mathbb{Z} \) such that \( a = kb \).

\[ a = kb \text{ and } a = bq + r \]

\[ r = b(k - q) \text{ and } k - q \in \mathbb{Z}, \text{ so } b \mid r. \]

But \( 0 \leq r < b \).

The only multiple of \( b \) in this range is 0, \( r = 0 \).

\[ \therefore \text{ } b \mid a \rightarrow r = 0 \]

\[ (\leftarrow) \text{ Suppose } r = 0. \]

Then \( a = bq \). Since \( q \in \mathbb{Z}, b \mid a. \)

\[ \therefore \text{ } r = 0 \rightarrow b \mid a \]

Note: While this proof is perfectly correct, and nicely written, a shorter/easier way to do the \((\rightarrow)\) direction would have been to apply the uniqueness part of the Division-with-Remainder Theorem, right after stating that \( a = bk + 0 \) and \( a = bq + r \), to immediately conclude that \( r = 0 \). Instead, the three lines before the conclusion are re-proving that theorem in this special case. Let this be a reminder! It will often save some time/effort/writing to apply a previous theorem, rather than re-proving it.

(b) (By Sandy K.)

Suppose \( c \mid a \), and \( c \mid b \), then \( a = ck \) for some \( k \in \mathbb{Z} \), and \( b = cn \) for some \( n \in \mathbb{Z} \). If \( a = bq + r \), then \( r = a - bq \). Through substitution, \( r = ck - cnq \) and by the distributive property, \( r = c(k - qn) \). Therefore \( c \mid r \).

(c) (By Lucas M.)

Suppose \( c \mid b \) and \( c \mid r \).
\[ c \mid b, \text{ so } \exists m \in \mathbb{Z} \quad b = cm \]
\[ c \mid r, \text{ so } \exists n \in \mathbb{Z} \quad r = cn \]
Substitute:
\[
\begin{align*}
a &= cmq + cn \\
&= c(mq + n)
\end{align*}
\]
Since \( mq + n \in \mathbb{Z} \), \( \therefore c \mid a \).

**Exercise 1.** With the same hypotheses as the above theorem, is it true that if \( c \mid a \) and \( c \mid r \), then \( c \mid b \)? Prove or give a counterexample.

**Solution.** (By Aidan S.)
No. Here’s a counterexample: \( a = 30, b = 7 \). Then \( q = 4 \) and \( r = 2 \):
\[
30 = 7 \cdot 4 + 2
\]
Now, \( 2 \mid 30 \) and \( 2 \mid 2 \), but \( 2 \nmid 7 \).
7 Greatest common divisors and the Euclidean Algorithm

Definition 7.1. Let \( a \) and \( b \) be integers, not both 0. The greatest common divisor of \( a \) and \( b \) is a positive integer \( d \) satisfying the following two properties:

(i) \( d \mid a \) and \( d \mid b \)

(ii) For all \( c \in \mathbb{Z} \), if \( c \mid a \) and \( c \mid b \), then \( c \leq d \)

We write \( \gcd(a, b) \) for the greatest common divisor of \( a \) and \( b \).

Remark. Although in this class, we will write \( \gcd(a, b) \) for the greatest common divisor of \( a \) and \( b \), in many number theory textbooks and papers, the standard way of writing the greatest common divisor of \( a \) and \( b \) is the (rather ambiguous) notation \( (a, b) \).

Examples.

• \( \gcd(75, 45) = 15 \)
• \( \gcd(84, 34) = 2 \)
• \( \gcd(-60, 24) = 12 \)
• \( \gcd(-35, -57) = 1 \)

Exercise 1. For any natural number \( n \), what is \( \gcd(n, 0) \)? Prove your answer.

Solution. (By Josef C.)

Any \( d \in \mathbb{N} \) divides 0, so \( \gcd(n, 0) \) is equal to the greatest divisor of \( n \), which is \( n \) itself. So \( \gcd(n, 0) = n \).

Theorem 7.2. Let \( a, b \in \mathbb{N} \), and let \( g = \gcd(a, b) \). Assume that \( q \) and \( r \) are integers such that \( a = b \cdot q + r \) and \( 0 \leq r < b \), as given by the Division-with-Remainder Theorem. Then
(a) $g \mid b$ and $g \mid r$

(b) Any common factor of $b$ and $r$ is less than or equal to $g$.
Therefore $\gcd(b, r) = g$.

Proof. (a) (By Mien T.)

Since $g$ is a common factor of $a$ and $b$, we can conclude that $g \mid b$.

$$a = bq + r, \quad \text{so}$$
$$r = a - bq$$

Since $g = \gcd(a, b)$, $g \mid a$ and $g \mid b$. So $\exists k \in \mathbb{Z}$ such that $a = gk$ and $\exists l \in \mathbb{Z}$ such that $b = gl$. Now

$$r = gk - glq$$
$$r = g(k - ql)$$

Since $l, q, k \in \mathbb{Z}$, $k - ql \in \mathbb{Z}$. So $g \mid r$.

Remark: Note that most of this proof is a repeat of Theorem 6.2 (c). So, while this is a very well written proof, a shorter way to do this would have been to just apply that theorem. Once again, it would save some time/effort/writing to apply a previous theorem, rather than re-proving it.

(b) To be completed by you!

Definition 7.3. Let $a$ and $b$ be integers, not both 0. We say that $a$ is relatively prime to $b$, or $a$ is coprime to $b$, if $\gcd(a, b) = 1$.

This terminology makes sense, because if $\gcd(a, b) = 1$, then that means that the only positive integer that divides both $a$ and $b$ is 1, and so in particular there is no prime number that divides both $a$ and $b$. It especially makes sense if you know that every natural number can be factored into primes, in one and only one way (a fact that we’ll prove soon). So saying two integers are relatively prime means that they have none of their prime factors in common.