

The Principle of Mathematical Induction

Section 1. Introductory Investigations

In this chapter, we will be making conjectures concerning the positive integers. In order to make our conjectures, we will usually look at a number of examples to see if a specific pattern emerges. We will need a method of proof to verify that our conjectures are correct. Our main tool will be the Principle of Mathematical Induction. Mathematical Induction is one of the defining axioms of the positive integers.

Example 1. Recall that for each positive integer n , $n! = 1 \cdot 2 \cdot 3 \cdots n$. So $n!$ is the product of the first n positive integers. We will attempt to find a formula for $1 \cdot (1!) + 2 \cdot (2!) + \cdots + n \cdot (n!)$ where n is a positive integer. To do this, we will first compute $1!$, $2!$, $3!$, $4!$ and $5!$ and then we will compute the sums $1 \cdot (1!)$, $1 \cdot (1!) + 2 \cdot (2!)$, $1 \cdot (1!) + 2 \cdot (2!) + 3 \cdot (3!)$, $1 \cdot (1!) + 2 \cdot (2!) + 3 \cdot (3!) + 4 \cdot (4!)$ and $1 \cdot (1!) + 2 \cdot (2!) + 3 \cdot (3!) + 4 \cdot (4!) + 5 \cdot (5!)$ to see if we can recognize a pattern. For simplicity of notation, for each positive integer n define S_n by,

$$S_n = 1 \cdot (1!) + 2 \cdot (2!) + \cdots + n \cdot (n!).$$

Let's compile our results in a table.

n	$n!$	S_n
1	1	1
2	2	5
3	6	23
4	24	119
5	120	719

If we compare Columns 2 and 3, we see that each entry in Column 3 is 1 less than the next entry in Column 2. So a reasonable conjecture would be that for each positive integer n , $S_n = (n+1)! - 1$. (The formula $S_n = (n+1)! - 1$ is called a **closed-form formula** for S_n .) Later, we will determine if this formula is correct.

Example 2. Let's see if we can make any conjectures concerning the numbers $n^2 + n + 41$, where n runs over the positive integers. As before, our strategy will be to

begin by computing $n^2 + n + 41$ for several values of n to see if we can detect any interesting common properties.

n	$n^2 + n + 41$
1	43
2	47
3	53
4	61
5	71
6	83

All of the numbers appearing in the second column are primes. (Recall that an integer p is a **prime** if $p > 1$ and the only positive divisors of p are 1 and itself.) So it seems reasonable to conjecture that for all positive integers n , the expression $n^2 + n + 41$ is a prime.

Just recognizing a pattern isn't enough. In fact, one of the conjectures we made above is true and the other one is false. We will discuss both examples further in the next section.

Example 3. We will try to find a general formula for the sum of the first n odd positive integers (where n is a positive integer). To see if we can identify a pattern, we'll first compute the sums $1 + 3$, $1 + 3 + 5$, $1 + 3 + 5 + 7$ and $1 + 3 + 5 + 7 + 9$. Note that the n th odd positive integer is $2n - 1$. Again, let's look at a table.

n	$1 + 3 + \dots + (2n - 1)$
1	1 ($1 = 2 \cdot 1 - 1$)
2	4 ($4 = 1 + 2 \cdot 2 - 1$)
3	9 ($9 = 1 + 2 \cdot 3 - 1$)
4	16
5	25

Can we find a general formula for $1 + 3 + 5 + \dots + (2n - 1)$ where n is a positive integer? When $n = 1$, the above "sum" is 1. In our computations, we found that when $n = 2$, the sum is $4 = 2^2$, when $n = 3$, the sum is $9 = 3^2$, when $n = 4$, the sum is $16 = 4^2$ and when $n = 5$, the sum is $25 = 5^2$. So it seems reasonable to conjecture that for all positive integers n , $1 + 3 + 5 + \dots + (2n - 1) = n^2$.

How would we prove that $1 + 3 + 5 + \dots + (2n - 1) = n^2$ if n is a positive integer? For simplicity of notation, for each positive integer n , define S_n by,

$$S_n = 1 + 3 + 5 + \dots + (2n - 1).$$

So if we put in a few more terms, $S_n = 1 + 3 + 5 + \dots + (2n - 5) + (2n - 3) + (2n - 1)$.

Let's pair up 1 and $(2n - 1)$, 3 and $(2n - 3)$, 5 and $(2n - 5)$, etc. So for example, $S_6 = 1 + 3 + 5 + 7 + 9 + 11$ and we pair 1 and 11, 3 and 9, and 5 and 7. Notice that in each pair, the sum is 12. In the general case, each time we add the two elements in a given pair we get $2n$. How many pairs do we have? That depends upon whether n is even or odd. If n is even, then we have $\frac{n}{2}$ pairs, each of which sum to $2n$. So, when n is even, $S_n = \cancel{n} \cdot \frac{n}{2} \cdot 2n = n^2$.

What happens when n is odd? Do we still have a sum of n^2 ? For example, when $n = 7$, $S_7 = 1 + 3 + 5 + 7 + 9 + 11 + 13$. So we have paired 1 and 13, 3 and 11, and 5 and 9. This time the term in the "middle" of the expression for S_7 has no mate. What is that term and how many remaining pairs do we have? Certainly we can answer those questions for this specific example and in general as well. However, it is more complicated than in the case where n is even. But this line of reasoning gives us a clue as to how to proceed. If we could guarantee that each term had a mate, we could more easily compute the sum. One way of ensuring that every term has a mate is to compute $S_n + S_n$ instead, where we use the fact that

$$\begin{aligned} S_n &= 1 + 3 + 5 + \dots + (2n - 5) + (2n - 3) + (2n - 1) \\ &= (2n - 1) + (2n - 3) + (2n - 5) + \dots + 5 + 3 + 1. \end{aligned}$$

Here is that computation:

$$\begin{aligned} 2S_n &= S_n + S_n \\ &= (1 + 3 + 5 + \dots + (2n - 5) + (2n - 3) + (2n - 1)) \\ &\quad + (1 + 3 + 5 + \dots + (2n - 5) + (2n - 3) + (2n - 1)) \\ &= \begin{array}{cccccccc} 1 & + & 3 & + & 5 & + & \dots & + & (2n - 5) & + & (2n - 3) & + & (2n - 1) \\ \updownarrow & & \updownarrow & & \updownarrow & & & & \updownarrow & & \updownarrow & & \updownarrow \\ + (2n - 1) & + & (2n - 3) & + & (2n - 5) & + & \dots & + & 5 & + & 3 & + & 1 \end{array} \\ &= (1 + (2n - 1)) + (3 + (2n - 3)) + (5 + (2n - 5)) \\ &\quad + \dots + (5 + (2n - 5)) + (3 + (2n - 3)) + (1 + (2n - 1)) \end{aligned}$$

$$\begin{aligned}
 &= (2n) + (2n) + (2n) + \cdots + (2n) + (2n) + (2n) \\
 &= n \cdot (2n) = 2n^2.
 \end{aligned}$$

So $S_n = n^2$.

Note that there are many other ways of proving this result as we shall see in the next section.

Exercise 1. Compute the sums 1 , $1 + 2$, $1 + 2 + 3$, $1 + 2 + 3 + 4$ and $1 + 2 + 3 + 4 + 5$. For each positive integer n , let $S_n = 1 + 2 + \cdots + n$. Can you find a formula that relates S_{n+1} to S_n ? What is the general closed-form formula for the sums S_n ? Prove your result.

Exercise 2. Compute the sums $1 + 2$, $1 + 2 + 2^2$, $1 + 2 + 2^2 + 2^3$ and $1 + 2 + 2^2 + 2^3 + 2^4$. What is the general closed-form formula for the sum $1 + 2 + \cdots + 2^n$ where n is a positive integer?

Exercise 3. Suppose that the first number a_1 in the sequence $\langle a_n \rangle_{n=1}^{\infty}$ is defined by $a_1 = 1$. The succeeding values are computed as follows:

$$a_2 = \sqrt{3a_1 + 1} = \sqrt{3 \cdot 1 + 1} = \sqrt{4} = 2,$$

$$a_3 = \sqrt{3a_2 + 1} = \sqrt{3 \cdot 2 + 1} = \sqrt{7} \approx 2.65,$$

$$a_4 = \sqrt{3a_3 + 1} = \sqrt{3\sqrt{7} + 1} \approx 2.99, \text{ etc.}$$

So for each positive integer n , we have defined $a_{n+1} = \sqrt{3a_n + 1}$.

a) Are the successive values always increasing, always decreasing, or sometimes increasing and sometimes decreasing? Will the values ever exceed 3? Will they ever exceed 4? What happens in the long run? What conjectures would you make?

b) What happens if you begin with $a_1 = 10$ and still define $a_{n+1} = \sqrt{3a_n + 1}$ for each positive integer n ?

c) Try several other values for a_1 . What conjectures would you make?

Section 2. The Principle of Mathematical Induction

Suppose that for each positive integer n we have a statement p_n such that

(i) p_1 is true

and

(ii) p_{n+1} is true whenever p_n is true.

If we apply (ii) with $n = 1$, then we know that p_2 is true. Now if we apply (ii) this time with $n = 2$, then we may deduce that p_3 is true. How would we deduce that p_{100} is true?

We apply (ii) 98 times to show that p_{99} is true and then apply (ii) one more time to conclude that p_{100} is true. *So if (i) and (ii) are both hold for any positive integer n ,* It seems reasonable to believe that p_n is true for all positive integers n and in fact, that is the assertion of the Principle of Mathematical Induction.

Principle of Mathematical Induction. Suppose that for each positive integer n we have a statement p_n such that

(i) p_1 is true

and

(ii) p_{n+1} is true whenever p_n is true.

Then p_n is true for all positive integers n .

Our strategy for applying the Principle of Mathematical Induction will be to first identify the statement p_n that we wish to prove. We will next prove that p_1 is true and then we will prove that p_{n+1} is true whenever p_n is true. The Principle of Mathematical Induction will then allow us to conclude that p_n is true for all positive integers n .

The proof that p_1 is true is often called the **initial step** or **base step**. The proof that p_{n+1} is true whenever p_n is true is called the **inductive step**. Usually our proof of the inductive step will start off with the assumption that p_n is true, an assumption called the **inductive assumption** or **inductive hypothesis**. We will then use the information provided by that assumption to deduce that p_{n+1} must be true.

We will first use this technique on some of the conjectures we made in Section 1. In several of the problems that follow, we will begin with a discussion to illustrate how one might think through the problem. We will then follow that discussion with a formal explanation or proof.

Example 4. In Example 1 of Section 1, for each positive integer n , we defined S_n by,

$$S_n = 1 \cdot (1!) + 2 \cdot (2!) + \cdots + n \cdot (n!).$$

We then conjectured that $S_n = (n+1)! - 1$ for all n . If we want to prove that conjecture using the Principle of Mathematical Induction, then for each positive integer n , we should let p_n be the statement that $S_n = (n+1)! - 1$. So p_1 is the statement that $1(1!) = 2! - 1$. We will use the fact that $1! = 1$ and $2! = 2$ to prove that p_1 is true.

In the inductive step, we will start by assuming that p_n is true. So we will assume that $S_n = (n+1)! - 1$. We then want to use that information to prove that p_{n+1} is true. In this example, p_{n+1} is the statement that $S_{n+1} = ((n+1)+1)! - 1$ where by definition, $S_{n+1} = 1 \cdot (1!) + 2 \cdot (2!) + \cdots + (n+1) \cdot (n+1)!$.

Proof that $S_n = (n+1)! - 1$ for all positive integers n . For each positive integer n , let p_n be the statement that $S_n = (n+1)! - 1$. Then p_1 is true since $1(1!) = 1 = 2 - 1 = 2! - 1$.

Assume that p_n is true, that is assume that $S_n = (n+1)! - 1$. By definition,

$$S_{n+1} = 1(1!) + 2(2!) + \cdots + (n+1)(n+1)!.$$

So

$$S_{n+1} = (1(1!) + 2(2!) + \cdots + n(n!)) + (n+1)(n+1)!.$$

Recall that by the definition of S_n , $S_n = 1 \cdot (1!) + 2 \cdot (2!) + \cdots + n \cdot (n!)$. So

$$\begin{aligned} S_{n+1} &= (1(1!) + 2(2!) + \cdots + n(n!)) + (n+1)(n+1)! \\ &= S_n + (n+1)(n+1)!. \end{aligned}$$

By our inductive assumption, $S_n = (n+1)! - 1$. Therefore,

$$\begin{aligned}
S_{n+1} &= S_n + (n+1)(n+1)! \\
&= (n+1)! - 1 + (n+1)(n+1)! \\
&= [1 \cdot (n+1)! + (n+1)(n+1)!] - 1 \\
&= [1 + (n+1)](n+1)! - 1 \\
&= (n+2)(n+1)! - 1.
\end{aligned}$$

Now, $(n+1)!$ is the product of the first $n+1$ positive integers. So $(n+2)(n+1)!$ is the product of the first $n+2$ positive integers, that is, $(n+2)(n+1)! = (n+2)!$. Consequently,

$$\begin{aligned}
S_{n+1} &= (n+2)(n+1)! - 1 \\
&= (n+2)! - 1 \\
&= ((n+1)+1)! - 1.
\end{aligned}$$

Therefore p_{n+1} is true whenever p_n is true. So, by the Principle of Mathematical Induction, p_n is true for all positive integers n . Therefore $S_n = (n+1)! - 1$ for all positive integers n .

Example 5. In Section 1 we conjectured that for each positive integer n , $n^2 + n + 41$ is a prime. How would we prove that using the Principle of Mathematical Induction? For each positive integer n , let p_n be the statement that $n^2 + n + 41$ is a prime. In our previous discussion, we already noticed that p_1 is true. Let's consider the inductive step where we assume that p_n is true and prove that p_{n+1} is true. So suppose we know that $n^2 + n + 41$ is a prime. What can we conclude about $(n+1)^2 + (n+1) + 41$? We have that

$$\begin{aligned}
(n+1)^2 + (n+1) + 41 &= n^2 + 2n + 1 + n + 1 + 41 \\
&= (n^2 + n + 41) + (2n + 2).
\end{aligned}$$

The first term, $n^2 + n + 41$, in the above sum is a prime by assumption. But to compute $(n+1)^2 + (n+1) + 41$, we have added the prime $n^2 + n + 41$ to the expression $2n + 2$. Does that allow us to conclude that $(n+1)^2 + (n+1) + 41$ is a prime? It is not clear how to get the desired result from the information that $n^2 + n + 41$ is a prime.

That doesn't mean that our conjecture is false, only that we do not know how to give a proof of the result using the Principle of Mathematical Induction. Let's stop and reflect on this. Is the conjecture false? Can we find a positive integer n such that $n^2 + n + 41$ can be factored in a nontrivial way? Now, the term 41 can be factored as the

product $1 \cdot 41$. So if we can factor out 41 from each of the other two terms, then we should be able to find a positive integer n such that $n^2 + n + 41$ is not a prime. Can we choose n so that both n^2 and n have the common factor 41? One possible choice for n would be 41 itself. With that value of n we have that

$$\begin{aligned} n^2 + n + 41 &= 41^2 + 41 + 41 \\ &= 41^2 + 41 \cdot 1 + 41 \cdot 1 \\ &= 41(41 + 1 + 1) \\ &= 41 \cdot 43. \end{aligned}$$

Therefore when $n = 41$, $n^2 + n + 41$ is not a prime. So our conjecture *was* indeed false.

Example 6. We've already given a proof that the sum of the first n odd positive integers is n^2 . Let's give a proof of that result using the Principle of Mathematical Induction.

Discussion. Once again, for simplicity of notation, for each positive integer n , let's define

$$S_n = 1 + 3 + 5 + \cdots + (2n - 1).$$

If we want to prove that for each positive integer n , $S_n = n^2$, we should let p_n be the statement that $S_n = n^2$. So the statement that $S_1 = 1^2$ is p_1 . We will use the fact that $1 = 1^2$ to prove that p_1 is true. We will then assume that p_n is true and deduce that p_{n+1} is true. So we will derive the statement that $S_{n+1} = (n+1)^2$ from the assumption that $S_n = n^2$.

Proof that for all positive integers n , $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.
For simplicity of notation, for each positive integer n , define

$$S_n = 1 + 3 + 5 + \cdots + (2n - 1).$$

Let p_n be the statement that $S_n = n^2$. Notice that p_1 is true since $S_1 = 1 = 1^2$. Now assume that p_n is true, that is, assume that $S_n = n^2$. By definition,

$$S_{n+1} = 1 + 3 + 5 + \cdots + (2(n+1) - 1).$$

So

$$\begin{aligned} S_{n+1} &= 1 + 3 + 5 + \cdots + (2n-1) + (2(n+1)-1) \\ &= (1 + 3 + 5 + \cdots + (2n-1)) + (2(n+1)-1). \end{aligned}$$

Recall that $S_n = 1 + 3 + 5 + \cdots + (2n - 1)$. So

$$\begin{aligned} S_{n+1} &= (1 + 3 + 5 + \cdots + (2n-1)) + (2(n+1)-1) \\ &= S_n + (2(n+1)-1). \end{aligned}$$

The inductive assumption gives us that $S_n = n^2$. Consequently

$$\begin{aligned} S_{n+1} &= S_n + (2(n+1)-1) \\ &= n^2 + (2(n+1)-1) \\ &= n^2 + 2n + 1 \\ &= (n+1)^2. \end{aligned}$$

Therefore p_{n+1} is true whenever p_n is true. So, by the Principle of Mathematical Induction, p_n is true for all positive integers n . Therefore $S_n = n^2$ for all positive integers n .

It is certainly the case that the inductive proof we just gave was longer than our original proof of the same conjecture in Section 1. However, our original proof required an idea that was not obvious whereas the second proof was much more routine.

Example 7. Let's look at Exercise 3 from Section 1. Recall that we defined the first number a_1 in the sequence $\langle a_n \rangle_{n=1}^{\infty}$ by $a_1 = 1$. The succeeding values were then computed as follows:

$$a_2 = \sqrt{3a_1 + 1} = \sqrt{3 \cdot 1 + 1} = \sqrt{4} = 2,$$

$$a_3 = \sqrt{3a_2 + 1} = \sqrt{3 \cdot 2 + 1} = \sqrt{7} \approx 2.65,$$

$$a_4 = \sqrt{3a_3 + 1} = \sqrt{3\sqrt{7} + 1} \approx 2.99, \text{ etc.}$$

So for each positive integer n , we had that $a_{n+1} = \sqrt{3a_n + 1}$. Let's conjecture that each value is at most 4 and prove that conjecture using the Principle of Mathematical Induction. So we are going to prove that $a_n \leq 4$ for all positive integers n .

Proof that $a_n \leq 4$ for all positive integers n . For each positive integer n , let p_n be the statement that $a_n \leq 4$. Then p_1 is true since $a_1 = 1 \leq 4$. Assume that p_n is true, that is, assume that $a_n \leq 4$. We will use this assumption to prove that $a_{n+1} \leq 4$. By definition,

$$a_{n+1} = \sqrt{3a_n + 1}.$$

Since $a_n \leq 4$, we have that $\sqrt{3a_n + 1} \leq \sqrt{3 \cdot 4 + 1}$. So

$$\begin{aligned} a_{n+1} &= \sqrt{3a_n + 1} \\ &\leq \sqrt{3 \cdot 4 + 1} \\ &= \sqrt{13} \\ &\leq 4. \end{aligned}$$

Hence p_{n+1} is true whenever p_n is true. So by the Principle of Mathematical Induction, p_n is true for all positive integers n and therefore $a_n \leq 4$ for all positive integers n .

In number theory we are frequently interested in questions concerning divisibility. The Principle of Mathematical Induction is often helpful in such settings. Recall that an integer n is said to **divide** an integer m (or m is said to be a **multiple** of n) if there exists an integer c such that $m = nc$. (Notice that we stated the given property in terms of multiplication, not division! That allows us to consider the case where n and m are both 0.)

Example 8. Prove that for each positive integer n , 3 divides $n^3 + 5n + 6$.

Proof. For each positive integer n , let p_n be the statement that 3 divides $n^3 + 5n + 6$. p_1 is true since $1^3 + 5 \cdot 1 + 6 = 12 = 3 \cdot 4$ and 4 is an integer. Now assume that p_n is true, that is, assume that 3 divides $n^3 + 5n + 6$. So there exists an integer c such that $n^3 + 5n + 6 = 3c$. Let's use this to prove that p_{n+1} is true. Now

$$\begin{aligned} (n+1)^3 + 5(n+1) + 6 &= n^3 + 3n^2 + 3n + 1 + 5n + 5 + 6 \\ &= (n^3 + 5n + 6) + (3n^2 + 3n + 6) \end{aligned}$$

$$\begin{aligned}
 &= 3c + 3(n^2 + n + 2) \\
 &= 3(c + n^2 + n + 2).
 \end{aligned}$$

Since c and n are integers, $c + n^2 + n + 2$ is an integer as well and hence 3 divides $(n+1)^3 + 5(n+1) + 6$. Therefore, p_{n+1} is true whenever p_n is true. Consequently, by the Principle of Mathematical Induction, p_n is true for all positive integers n . So for each positive integer n , 3 divides $n^3 + 5n + 6$.

Remark. In the above proof, notice that we did not simplify the expression $(n+1)^3 + 5(n+1) + 6$. Rather we grouped together the terms n^3 , $5n$ and 6 in order to use the information concerning their sum.

Example 9. Prove that for each positive integer n , 3 divides $4^n - 1$.

Discussion. For each positive integer n , let p_n be the statement that 3 divides $4^n - 1$. Before going to the formal proof, let's look at the inductive step where we assume that p_n is true and try to deduce that p_{n+1} is true. So we will assume that 3 divides $4^n - 1$ and try to prove that 3 divides $4^{n+1} - 1$. The assumption that 3 divides $4^n - 1$ means that there exists an integer c such that $4^n - 1 = 3c$. We want to show that $4^{n+1} - 1 = 3d$ for some integer d . (Why didn't we say that $4^{n+1} - 1 = 3c$ for some integer c ?) Now $4^{n+1} - 1 = 4 \cdot 4^n - 1$. There are several ways to proceed.

Method 1. We may solve for 4^n in the equation $4^n - 1 = 3c$ to find that $4^n = 3c + 1$. We may then substitute $4^n = 3c + 1$ in the expression $4 \cdot 4^n - 1$. So

$$\begin{aligned}
 4^{n+1} - 1 &= 4 \cdot 4^n - 1 \\
 &= 4 \cdot (3c + 1) - 1 \\
 &= 12c + 3 \\
 &= 3(4c + 1).
 \end{aligned}$$

Now we could use the fact that $4c + 1$ is an integer (since c is an integer) to deduce that 3 divides $4^{n+1} - 1$.

Method 2. Once again we'll use that $4^{n+1} - 1 = 4 \cdot 4^n - 1$. Then

$$4^{n+1} - 1 = (3 + 1) \cdot 4^n - 1.$$

Now we can use the distributive rule to rewrite $4^{n+1} - 1$ as follows:

$$\begin{aligned}
4^{n+1} - 1 &= 4 \cdot 4^n - 1 \\
&= (1+3) \cdot 4^n - 1 \\
&= 1 \cdot 4^n + 3 \cdot 4^n - 1 \\
&= (4^n - 1) + 3 \cdot 4^n \\
&= 3c + 3 \cdot 4^n \\
&= 3(c + 4^n).
\end{aligned}$$

Since c is an integer and n is a *positive* integer, $c + 4^n$ is an integer as well. (Note that 4^n is not an integer unless we know that n is nonnegative.) So we may then deduce that 3 divides $4^{n+1} - 1$.

Method 3. This time to calculate $4^{n+1} - 1$ we'll subtract 4 and add 4 as follows:

$$\begin{aligned}
4^{n+1} - 1 &= 4 \cdot 4^n - 1 \\
&= 4(4^n - 1) + 4 - 1 \\
&= 4(3c) + 3 \\
&= 3(4c + 1).
\end{aligned}$$

We've looked at three ways of proving that $4^{n+1} - 1$ is divisible by 3 whenever 3 divides $4^n - 1$. We will now proceed with the formal proof. In that proof we will use the first approach we discussed.

Proof that 3 divides $4^n - 1$ for each positive integer n . For each positive integer n , let p_n be the statement that 3 divides $4^n - 1$. p_1 is true since $4^1 - 1 = 3 = 3 \cdot 1$ and 1 is an integer. Assume that p_n is true, that is, assume that 3 divides $4^n - 1$. Then there exists an integer c such that $4^n - 1 = 3c$. So $4^n = 3c + 1$. Then

$$\begin{aligned}
4^{n+1} - 1 &= 4 \cdot 4^n - 1 \\
&= 4 \cdot (3c + 1) - 1 \\
&= 12c + 3 \\
&= 3(4c + 1).
\end{aligned}$$

Since c is an integer, $4c + 1$ is an integer as well and therefore 3 divides $4^{n+1} - 1$. So p_{n+1} is true whenever p_n is true. Consequently, by the Principle of Mathematical Induction, p_n is true for all positive integers n .

Example 10. Prove that for each positive integer n , 6 divides $n^3 - n$.

Discussion. For each positive integer n , let p_n be the statement that 6 divides $n^3 - n$. As in the previous example, let's first look at the inductive step where we assume that p_n is true and try to deduce that p_{n+1} is true. The assumption that p_n is true means that there exists an integer c such that $n^3 - n = 6c$. So

$$\begin{aligned}(n+1)^3 - (n+1) &= (n^3 + 3n^2 + 3n + 1) - (n+1) \\ &= (n^3 - n) + (3n^2 + 3n) \\ &= 6c + (3n^2 + 3n) \\ &= 6\left(c + \frac{n^2+n}{2}\right).\end{aligned}$$

Notice that as in Example 8, we did not combine coefficients to simplify the expression $(n+1)^3 - (n+1)$, but rather grouped the terms n^3 and n to use our information concerning $n^3 - n$. Now we would like to state that $c + \frac{n^2+n}{2}$ is an integer in order to conclude that 6 divides $(n+1)^3 - (n+1)$. But to do that we need to know that $\frac{n^2+n}{2}$ is an integer. $\frac{n^2+n}{2}$ is the quotient of two integers and quotients of integers do not always yield integers. So why is this particular quotient an integer? Well, there are many ways to proceed. One way is to examine two cases, namely the case where n is even and then the case where n is odd. If we can deduce that in each case $\frac{n^2+n}{2}$ is an integer, then we will have that $c + \frac{n^2+n}{2}$ is an integer as well and as a consequence we may then conclude that p_{n+1} is true whenever p_n is true. But since we are studying the Principle of Mathematical Induction, let's try to give an inductive proof of the statement that for each positive integer n , $\frac{n^2+n}{2}$ is an integer. To prove this assertion, we'll prove that $n^2 + n$ is always even, that is, for each positive integer n , $n^2 + n$ is twice an integer.

For each positive integer n , let s_n be the statement that $n^2 + n$ is even. s_1 is true since $1^2 + 1 = 2 = 2 \cdot 1$ and 1 is an integer. Now assume that s_n is true, that is, assume that $n^2 + n$ is even. Then there exists an integer a such that $n^2 + n = 2a$. So

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

Since a and n are integers, $a + n + 1$ is an integer as well and therefore $(n+1)^2 + (n+1)$ is even. So s_{n+1} is true whenever s_n is true. Therefore by the Principle of Mathematical Induction, s_n is true for all positive integers n .

We now have all the pieces we need to write up our formal proof. To make the proof easier to read, we will first prove that $n^2 + n$ is even for all positive integers n . Then we will be able to call on that result when we need it in the proof of the inductive step of our main result.

Proof that 6 divides $n^3 - n$ for all positive integers n . We will first prove that $n^2 + n$ is even whenever n is a positive integer. For each positive integer n , let s_n be the statement that $n^2 + n$ is even. s_1 is true since $1^2 + 1 = 2 = 2 \cdot 1$ and 1 is an integer. Now assume that s_n is true, that is, assume that $n^2 + n$ is even. Then there exists an integer a such that $n^2 + n = 2a$. Thus

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

Since a and n are integers, so is $a + n + 1$ and therefore $(n+1)^2 + (n+1)$ is even. Consequently s_{n+1} is true whenever s_n is true and therefore by the Principle of Mathematical Induction, s_n is true for all positive integers n . So $n^2 + n$ is even whenever n is a positive integer.

Now let's proceed with the proof that 6 divides $n^3 - n$ whenever n is a positive integer. For each positive integer n , let p_n be the statement that 6 divides $n^3 - n$. p_1 is true since $1^3 - 1 = 0 = 6 \cdot 0$ and 0 is an integer. Suppose that p_n is true. Then there exists an integer c such that $n^3 - n = 6c$. So

$$\begin{aligned} (n+1)^3 - (n+1) &= (n^3 + 3n^2 + 3n + 1) - (n+1) \\ &= (n^3 - n) + (3n^2 + 3n) \\ &= 6c + (3n^2 + 3n) \\ &= 6\left(c + \frac{n^2 + n}{2}\right). \end{aligned}$$

By the above, as n is a positive integer, $n^2 + n$ is even and so there exists an integer d such that $n^2 + n = 2d$. Therefore,

$$\begin{aligned}
 (n+1)^3 - (n+1) &= 6\left(c + \frac{n^2+n}{2}\right) \\
 &= 6\left(c + \frac{2d}{2}\right) \\
 &= 6(c+d).
 \end{aligned}$$

Since c and d are integers, so is $c+d$. Therefore 6 divides $(n+1)^3 - (n+1)$. So p_{n+1} is true whenever p_n is true and hence by the Principle of Mathematical Induction, 6 divides $n^3 - n$ for all positive integers n .

Section 3. Statements which are Equivalent to the Principle of Mathematical Induction

In our statement of the Principle of Mathematical Induction, we started with the base case of $n = 1$. But there are times when we would like to start the inductive process at a different integer. For example, suppose we wish to prove that $3^n > 1 + 2^n$ whenever n is a positive integer with $n \geq 2$. (It is certainly *not* true that $3^1 > 1 + 2^1$.) To prove this assertion we may use the following statement which is equivalent to the Principle of Mathematical Induction.

Principle of Mathematical Induction II. Let n_0 be a fixed integer. Suppose that for each integer $n \geq n_0$ we have a statement p_n such that

(i) p_{n_0} is true

and

(ii) p_{n+1} is true whenever p_n is true.

Then p_n is true for all integers $n \geq n_0$.

Suppose that n_0 and p_n satisfy the hypotheses of the Principle of Mathematical Induction II. If we apply (ii) with $n = n_0$, we may conclude that p_{n_0+1} is true. Now if apply (ii) again, this time with $n = n_0 + 1$, we see that p_{n_0+2} is true. Continuing in this manner, we deduce that p_{n_0+3} is true, p_{n_0+4} is true, etc. So it seems reasonable to believe that p_n is true for all integers $n \geq n_0$.

It is possible to give a formal proof that the second version of the Principle of Mathematical Induction follows from the original version of the Principle of Mathematical Induction. To do so, for each positive integer n , let s_n be the statement p_{n_0+n-1} . So s_1 is

the statement p_{n_0+1-1} . In other words, s_1 is the statement p_{n_0} . Similarly, s_2 is the statement p_{n_0+1} , s_3 is the statement p_{n_0+2} , etc. Notice that as n runs through the positive integers, $n_0 + n - 1$ runs through all the integers which are greater than or equal to n_0 . So if we can show that s_n is true for all positive integers n , then p_n will be true for all integers n with $n \geq n_0$. We will leave it as an exercise to prove that, by the first version of the Principle of Mathematical Induction, s_n is true for all positive integers n .

We will use this new version of the Principle of Mathematical Induction in the same way we used the old version.

Example 11. Prove that for all integers n where $n \geq 2$, $3^n > 1 + 2^n$.

Proof. For each integer n with $n \geq 2$, let p_n be the statement that $3^n > 1 + 2^n$. p_2 is true since $3^2 = 9 > 5 = 1 + 2^2$. Assume that p_n is true. So we are assuming that $3^n > 1 + 2^n$. Then

$$\begin{aligned} 3^{n+1} &= 3 \cdot 3^n \\ &> 3 \cdot (1 + 2^n) \\ &= 3 + 3 \cdot 2^n \\ &> 1 + 3 \cdot 2^n \\ &> 1 + 2 \cdot 2^n \\ &= 1 + 2^{n+1}. \end{aligned}$$

So $3^{n+1} > 1 + 2^{n+1}$ and therefore p_{n+1} is true whenever p_n is true. Consequently by the Principle of Mathematical Induction II, p_n is true for all integers n with $n \geq 2$.

Example 12. Prove that each integer which is greater than or equal to 2 is a product of primes.

Discussion. We will use the convention that a prime is a "product" of primes. So for example, 2 is a product of primes. For each positive integer n with $n \geq 2$, let p_n be the statement that n is a product of primes. Let's look at the inductive step. Suppose that p_n is true, that is, suppose that n is a product of primes. Can we deduce that p_{n+1} is true? In other words, can we deduce that $n + 1$ is a product of primes? Well, if $n + 1$ is itself a prime, then by our convention, $n + 1$ is a product of primes. Suppose then that $n + 1$ is not a prime. Then we may factor $n + 1$ and write that $n + 1 = ab$, where a and b are integers with $1 < a < n + 1$ and $1 < b < n + 1$. Hence $2 \leq a \leq n$ and $2 \leq b \leq n$. Now, if we knew that a and b were themselves products of primes, then we would be able to conclude that ab

is a product of primes as well. By convention, 2 is a product of primes and our inductive assumption tells us that n is a product of primes. So if knew that a was either 2 or equal to n and similarly b was either 2 or equal to n , then we would be able to conclude that ab is a product of primes. But we can't guarantee that we are that lucky. All we know is that both a and b are between 2 and n . Fortunately, there is another version of the Principle of Mathematical Induction, called the Principle of Complete Induction, which will allow us to deal with this case.

Principle of Complete Induction. Let n_0 be a fixed integer. Suppose that for each integer $n \geq n_0$ we have a statement p_n such that

(i) p_{n_0} is true

and

(ii) p_{n+1} is true whenever $p_{n_0}, p_{n_0+1}, \dots, p_n$ are true.

Then p_n is true for all integers $n \geq n_0$.

Let's use the Principle of Complete Induction to give a proof that if n is a positive integer and n is greater than or equal to 2, then n is a product of primes. For each positive integer n with $n \geq 2$, let p_n be the statement that n is a product of primes. p_2 is true since 2 is a prime. Suppose that p_2, p_3, \dots, p_n are true, that is, suppose that 2, 3, 4, ..., n are products of primes. So we are assuming that all of the positive integers between 2 and n inclusive are products of primes. If $n + 1$ is a prime, then p_{n+1} is true and so we may assume that $n + 1$ is not a prime. Therefore we may factor $n + 1$ and write that $n + 1 = ab$, where a and b are positive integers with $1 < a < n + 1$ and $1 < b < n + 1$. Hence $2 \leq a \leq n$ and $2 \leq b \leq n$. So by assumption, a and b are products of primes. Therefore ab is a product of primes, that is, $n + 1$ is a product of primes. So p_{n+1} is true whenever p_2, p_3, \dots, p_n are true and consequently p_n is true for all integers n with $n \geq 2$.

The statement that every integer greater than or equal to two is a product of primes is one of the assertions in the Fundamental Theorem of Arithmetic, a theorem which is also known as the Unique Factorization Theorem for Integers. That theorem states that every integer greater than or equal to two can be factored "uniquely" into a product of primes. (Here we need to allow for the possibility of rearranging factors in the factorization of an integer. So for example, although we may factor 6 as $2 \cdot 3$ and also as $3 \cdot 2$, we have used the same primes in both factorizations and have used those primes the same number of

times in both. We will consider those two factorizations of 6 to be the same.) There are other algebraic systems in which factorization does not occur or the factorization is not unique. However there is an analogue of the Fundamental Theorem of Arithmetic for polynomials with real coefficients. A corollary of that theorem is that each polynomial with real coefficients having degree at least one can be factored into a product of linear polynomials and quadratic polynomials where each of the quadratic polynomials has no real root. (Here the **degree of a nonzero polynomial** is the highest power of x which has a nonzero coefficient. If $f(x)$ is a polynomial with real coefficients and c is a real number, then c is said to be a **root of f** if $f(c) = 0$.)

We conclude this section with another principle which is equivalent to the original version of the Principle of Mathematical Induction.

Well Ordering Principle. If S is any nonempty subset of the set of positive integers, then S has a smallest element.

What does it mean for S to have a smallest element? We need to be careful here. We do not want to assert the existence of an element s_0 in S such that $s_0 < s$ for all s in S . Indeed, that condition would be violated if we were to substitute s_0 for s in the inequality $s_0 < s$. So to say that S has a smallest element means that there exists an element s_0 in S such that $s_0 \leq s$ for all s in S .

We will not give the proof that the Well Ordering Principle is equivalent to the Principle of Mathematical Induction.

Let's use the Well Ordering Principle and a proof by contradiction to justify that each positive integer n greater than or equal to two is a product of primes. Suppose the given statement is false. Then there must exist a positive integer n_0 such that $n_0 \geq 2$ but n_0 is not a product of primes. Define the set S by,

$$S = \{n: n \text{ is a positive integer, } n \geq 2 \text{ and } n \text{ is not a product of primes}\}.$$

Since n_0 is an element of S , S is nonempty. By definition, S is a subset of the positive integers. So by the Well Ordering Principle, S has a smallest element. Let's denote that element by m . Then m is a positive integer, $m \geq 2$ and m is not a product of primes. So we may factor m and write $m = ab$ where a and b are integers with $1 < a < m$ and

$1 < b < m$. Since a and b are less than m and m is the smallest element of S , then a and b are not elements of S . So as both a and b are at least two, a and b must each be a product of primes. Therefore as $m = ab$, m must also be a product of primes, a contradiction. So our original assertion must be true, that is, each positive integer greater than or equal to two is a product of primes.

When discussing the Principle of Mathematical Induction, we noticed that we didn't need to start with the base case $n = 1$. Can the same be said for the Well Ordering Principle? For example, can we assert that if S is any nonempty subset of the set of nonnegative integers, then S has a smallest element? The answer is *yes*. There are two cases to consider. First of all, if S contains the integer 0, then 0 is the smallest element of S . What happens if S does not contain 0? Then S is a nonempty subset of the set of positive integers and so by the Well Ordering Principle, we know that S has a smallest element. We will use this fact in Section 4 in the proof of the Division Algorithm.

Exercise 4. Suppose that S is a nonempty subset of the set $\{n: n \text{ is an integer and } n \geq -1\}$. Prove that S has a smallest element.

How far "down" can we continue this argument? For example, is it true that every nonempty subset of the set of integers has a smallest element? Some subsets of the set of integers do have a smallest element. For example the set of positive integers has a smallest element, namely the number 1. But the set of integers themselves contains no smallest element. So the answer to the question "Is it true that every nonempty subset of the set of integers has a smallest element?" is *no*.

Exercise 5. Suppose that I is a nonempty subset of the set of all integers. Determine when I has the property that for all nonempty subsets S of I , S has a smallest element.

Section 4. The Division Algorithm (Note- we may end up deleting this section and including the Division Algorithm in the chapter concerning properties of the integers.)

Division Algorithm for Integers. Suppose that a and b are integers with $b \neq 0$. Then there exist integers q and r with

$$(i) \ a = bq + r$$

and

$$(ii) 0 \leq r < |b|.$$

Remarks.

1. The integers q and r above are unique. However, since we will not use that fact below, we have not added that property to the statement of the Division Algorithm for Integers.

2. There is an analogue of the Division Algorithm which applies to polynomials. One version of it states that if $f(x)$ and $g(x)$ are polynomials with real coefficients such that $g(x)$ is not the zero polynomial, then there are real polynomials $q(x)$ and $r(x)$ such that

$$f(x) = g(x)q(x) + r(x)$$

and $r(x)$ is the zero polynomial or the degree of $r(x)$ is less than the degree of $g(x)$.

3. In the proof of the Division Algorithm for Integers, if q and r exist having the desired properties, then we must have that $r = a - bq$ and $r \geq 0$. So in order to find an appropriate choice for r , it is natural to consider the set S where S is defined as follows:

$$S = \{a - bq: q \text{ is an integer and } a - bq \geq 0\}.$$

By definition, to find the elements of S , we compute the expressions $a - bq$ where q ranges over all of the integers and we put such an expression in S if it is nonnegative. For example, let $a = 31$ and let $b = 6$. When q is a negative integer, the expression $31 - 6q$ is an element of S since $31 - 6q \geq 31 - 6(-1) = 37 \geq 0$. When q ranges over the nonnegative integers, the only elements of S are $31 - 6(0) = 31$, $31 - 6(1) = 25$, $31 - 6(2) = 19$, $31 - 6(3) = 13$, $31 - 6(4) = 7$, and $31 - 6(5) = 1$ since we have required that $31 - 6q$ is nonnegative. In the Division Algorithm, since we need that $r \geq 0$ and that $r < 6$, the only appropriate choice for r in this example is $r = 1$. Notice that this value is in fact the smallest of all the elements of S . We will use that observation to give us an idea as to how to prove the Division Algorithm for Integers.

Proof of the Division Algorithm for Integers. First assume that $b > 0$. Define S as follows:

$$S = \{a - bq: q \text{ is an integer and } a - bq \geq 0\}.$$

Notice that whenever q is an integer, $a - bq$ is also an integer. So S is a subset of the set of nonnegative integers. We would like to apply our extended version of the Well Ordering Principle to S and in order to do so, we need to know that S is nonempty. If $a \geq 0$, then $a - b \cdot 0$ is in S . If $a < 0$ then $a - ba = (1 - b)a \geq 0$ since $1 - b \leq 0$ and $a < 0$. So in this case, $a - ba$ is in S . Therefore, in any case, S is nonempty. So S contains a smallest element that we will denote by r . Since r is an element of S , $r = a - bq$ for some integer q . Also as r is in S , $r \geq 0$. So we have that $a = bq + r$ where q and r are integers with $r \geq 0$. Therefore, in order to complete the proof of the Division Algorithm when $b > 0$, we must show that $r < b$.

We will assume that $r \geq b$ and show that assumption leads to an impossibility. If $r \geq b$, then $r - b \geq 0$. But $r - b = (a - bq) - b = a - b(q + 1)$. Since q is an integer, so is $q + 1$ and hence $r - b$ is of the form a minus b times some integer. Moreover as $r - b \geq 0$, $r - b$ is an element of S by the definition of S . So $r - b$ must be greater than or equal to the smallest element of S , that is, $r - b \geq r$. But since $b > 0$, $r - b < r$. So $r - b < r$ and $r - b \geq r$, which is impossible. Therefore, we must have that $r < b$. Consequently the Division Algorithm holds when $b > 0$.

Suppose then that $b < 0$. Then $-b > 0$ and so by the above, we may apply the Division Algorithm to the integers a and $-b$ to deduce that there exist integers q and r such that $a = (-b)q + r$ and $0 \leq r < -b = |b|$. Then $-q$ and r are integers satisfying $a = b(-q) + r$ and $0 \leq r < |b|$. This completes the proof of the Division Algorithm.

The notation q and r is used in the statement of the Division Algorithm for Integers since in many computations q is the integral part of the quotient of a by b and r is the integral part of the remainder of that quotient, that is, q and r satisfy the equation $\frac{a}{b} = q + \frac{r}{b}$. So for example, if we want to solve for q and r when $a = 50$ and $b = 3$, we can compute $\frac{50}{3}$ and write that $\frac{50}{3} = 16 + \frac{2}{3}$. So let's define q to be 16 and r to be 2. Since

$$a = 50 = 3 \cdot 16 + 2 \text{ and } 0 \leq 2 < 3,$$

those are appropriate choices for q and r . But if we take a to be -50 and b to be 3 and compute $\frac{-50}{3}$, we obtain that $\frac{-50}{3} = -16 + \frac{-2}{3}$. So although $-50 = 3(-16) + (-2)$, -2 is not an appropriate choice for r since -2 does not satisfy the inequality $0 \leq r < 3$. So how should we modify this? Well, if we decrease -16 by 1 in the equation $-50 = 3(-16) + (-2)$, then in order to maintain the equality, we must increase -2 by 3. Therefore we may write that

$$-50 = 3(-17) + 1.$$

Here -17 and 1 are appropriate choices for q and r respectively since 1 satisfies the inequality $0 \leq 1 < 3$.

Recall that an integer a is said to be **even** if $a = 2n$ for some integer n . How should we define the term "**odd**?" Some authors define an integer a to be odd if a is not even and others define a to be odd if there exists an integer m such that $a = 2m + 1$. There are several questions that come to mind. First of all, although it is clear that every integer is either even or not even, can every integer be written in the form twice an integer or twice an integer plus one? Secondly, is it true that the two definitions of odd are the same? We'll apply the Division Algorithm for Integers in the case where $b = 2$ to answer those questions. By the Division Algorithm, if a is any integer, then there exist integers q and r such that $a = 2q + r$ and $0 \leq r < |2| = 2$. So r must be either 0 or 1 here and therefore we may write a in the form $2q + 0$ or $2q + 1$ for some integer q . Consequently we may use the Division Algorithm to answer the first question in the affirmative. Suppose now that a is not even. Then we know that a is not of the form $2q + 0$ and so a must be of the form $2q + 1$ where q is some integer. Conversely, if a is of the form $2q + 1$ for some integer q , then a cannot be even. Indeed, if a is even, we may write that $a = 2n$ for some integer n . Then we have that $2q + 1 = a = 2n$ where q and n are integers. From the equation $2q + 1 = 2n$, we may deduce that $1 = 2(n - q)$ and so $n - q = \frac{1}{2}$. But since n and q are integers, this is impossible. So if a is of the form $2q + 1$ where q is an integer, then a is not even. Consequently, the two definitions of odd are equivalent.

There are many examples of problems and proofs when dealing with the integers where it is helpful to divide the problem into two cases, one where the given integer is of the form $2n$ for some integer n and secondly where the given integer is of the form $2n + 1$ for some integer n . As we saw above, the fact that every integer falls into one of these two categories is a consequence of the Division Algorithm for Integers where $b = 2$. But there are many problems where those cases do not aid us in our investigation, where it is more useful to apply the Division Algorithm for other values of b . For example, one proof that $\sqrt{3}$ is irrational uses the fact that if a is any integer, then a is of the form $3q$ or $3q + 1$ or $3q + 2$ for some integer q . The fact that a can be written in one of those three forms follows from the Division Algorithm where $b = 3$. Similarly, in a given problem it may be useful to note that every integer is of the form $15q$ or $15q + 1$ or $15q + 2$ or, ..., or $15q + 14$ for some integer q , a consequence of the Division Algorithm for Integers with $b = 15$.

Problems

In the following exercises, \mathbf{N} denotes the set of positive integers.

I. Proofs and Counterexamples

1. Prove each of the following:

- a) 3 divides $10^{n+1} + 10^n + 1$ for all n in \mathbf{N} .
 b) Define a_n for all positive integers n as follows:

$$a_1 = 1$$

and

$$a_{n+1} = \sqrt{a_n + 1} \text{ for all } n \text{ in } \mathbf{N}.$$

Prove that $a_n < a_{n+1}$ for all positive integers n .

- c) 5 divides $6^{n+1} - 1$ for all n in \mathbf{N} .
 d) 8 divides $5^n + 2 \cdot 3^{n-1} + 1$ for all n in \mathbf{N} .
 e) For each n in \mathbf{N} and for each positive real number x , $\ln(x^n) = n \ln(x)$. (Here, for each n in \mathbf{N} , let p_n be the statement that $\ln(x^n) = n \ln(x)$ for all positive real numbers x . In the inductive step, you may use the property that for all positive real numbers x and y , $\ln(xy) = \ln(x) + \ln(y)$.)
 f) $\frac{d}{dx}(x^n) = (n)x^{n-1}$ for all n in \mathbf{N} . (You may use the product rule for derivatives in the inductive step.)
 g) There exists a positive integer n such that $2n > n^2$.
 h) $3 + 6 + 12 + \cdots + 3 \cdot 2^{n-1} = 3(2^n - 1)$ for all n in \mathbf{N} .
 i) $2^1 \cdot 2^3 \cdot 2^5 \cdots 2^{2n-1} = 2^{n^2}$ for all n in \mathbf{N} .
 j) $2 + 2^n \leq 2 \cdot 2^n$ for all n in \mathbf{N} .
 k) $(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta$ for all n in \mathbf{N} and for all real numbers θ . (Remember that $i^2 = -1$. In this problem, let p_n be the statement that $(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta$ for all real numbers θ .)
 l) $(xy)^n = x^n y^n$ for all n in \mathbf{N} and for all real numbers x and y .
 m) For each positive integer n where $n \geq 3$, the sum of the interior angles of any convex polygon having precisely n sides is $(n - 2)180^\circ$.

n) If n is a positive integer with $n \geq 2$ and if P_1, P_2, \dots, P_n are n distinct points in the plane, then the total number of line segments having endpoints in the set

$$\{P_1, P_2, \dots, P_n\} \text{ is } \frac{n^2 - n}{2}.$$

o) $1^3 + 2^3 + \dots + n^3 = (1 + 2 + \dots + n)^2$ for all n in \mathbf{N} .

p) We will define a sequence $\langle F_n \rangle_{n=0}^{\infty}$ of nonnegative integers as follows:

$$F_0 = 0, F_1 = 1 \text{ and for each integer } n \text{ with } n \geq 2, \text{ let } F_n = F_{n-1} + F_{n-2}.$$

So $F_2 = F_1 + F_0 = 1$, $F_3 = F_2 + F_1 = 2$, $F_4 = F_3 + F_2 = 3$, $F_5 = F_4 + F_3 = 5$,

$F_6 = F_5 + F_4 = 8$, etc. (The integers F_n are called the **Fibonacci numbers**.)

Let m denote a fixed nonnegative integer. Use the Principle of Complete Induction to prove that for each nonnegative integer n , $F_{m+n} = F_n F_{m+1} + F_{n-1} F_m$. Then prove that F_m divides F_{2m} whenever m is a nonnegative integer.

2. Prove or give a counterexample for each of the following:

a) $2^n \geq 2 + n$ for all positive integers n with $n \geq 2$.

b) 3 divides $n^2 - 3n + 2$ for all n in \mathbf{N} .

c) $3^n \geq 2^n + n$ for all n in \mathbf{N} .

II. The Division Algorithm

1. Find integers q and r where $a = bq + r$ and $0 \leq r < |b|$ in each of the following:

a) $a = 100, b = 6$.

b) $a = 100, b = -6$.

c) $a = -100, b = 6$.

d) $a = -100, b = -6$.

2. a) Prove that if a is any integer, then there exists an integer q such that

$$a = 5q, a = 5q + 1, a = 5q + 2, a = 5q + 3 \text{ or } a = 5q + 4.$$

b) Prove that if a is any integer, then there exists an integer q such that

$$a = 5q - 2, a = 5q - 1, a = 5q, a = 5q + 1 \text{ or } a = 5q + 2.$$

(Hint: What happens if a is of the form $5q + 3$ or $5q + 4$ for some integer q ?)

3. Let $f(x)$ and $g(x)$ be polynomials with real coefficients. $f(x)$ is said to **divide** $g(x)$ if

there exists a polynomial $t(x)$ with real coefficients such that $g(x) = f(x)t(x)$.

Use the Division Algorithm for Polynomials to prove the following theorem:

Factor Theorem. Let $f(x)$ be a polynomial with real coefficients and let c be a real number. Then c is a root of f if and only if $x - c$ divides $f(x)$.

4. Consider the function $f(x) = \frac{x^2 - 3x + 5}{x - 2}$. We want to examine the behavior of f for large values of x . Use the Division Algorithm for Polynomials to show that $y = x - 1$ is an asymptote of f .

III. Incorrect Arguments

In each of the following, the given "proof" is incorrect. Find all the errors in the proof.

Determine if the "claim" is correct or incorrect and justify your answer.

1. **Claim:** All the positive integers are equal.

Proof. For each positive integer n , let p_n be the statement that the positive integers between 1 and n inclusive are equal, that is, p_n is the statement that $1 = 2 = \dots = n$. So p_1 is the statement that the positive integers between 1 and 1 inclusive are equal, that is, p_1 is the statement that $1 = 1$. Clearly p_1 is true. Now assume that p_n is true. So we are assuming that $1 = 2 = \dots = n$. In order to show that p_{n+1} is true, we need to show that $1 = 2 = \dots = n = n + 1$. Since we have already assumed that $1 = 2 = \dots = n$, we only need to show that $n = n + 1$. From $1 = 2 = \dots = n$, we have that $1 = 2 = \dots = n - 1 = n$. So $n - 1 = n$ and therefore, $(n - 1) + 1 = n + 1$. Consequently $n = n + 1$ and so $1 = 2 = \dots = n = n + 1$. Hence p_{n+1} is true whenever p_n is true and so by the Principle of Mathematical Induction, p_n is true for all positive integers n .

Now we will apply the above result to prove the claim. Suppose that m and n are positive integers. We know that either $m \leq n$ or $n \leq m$. In the first case since p_n is true, then m and n are equal. In the second case since p_m is true, then $n = m$ as well. This completes the proof of the claim.

2. **Claim:** All horses are colored the same.

Proof. For each positive integer n , let p_n be the statement that all the horses in any given collection having precisely n horses are all colored the same. If we take any collection containing only one horse, then clearly all the horses in that given collection are colored the same. So p_1 is certainly true. Now assume that p_n is true, that is, assume that whenever we are given a collection containing precisely n horses, all the horses in that collection are colored the same. Now take a collection containing precisely $n + 1$ horses. Let's label the horses as $H\#1, H\#2, \dots, H\#n$ and $H\#(n + 1)$. If we remove $H\#1$ from the collection, then we are left with the n horses, $H\#2, H\#3, \dots, H\#(n + 1)$. By hypothesis, all of the horses in that collection are colored the same. So if we can show that $H\#1$ is colored the same as those horses, we will show that all horses in our original collection of $n + 1$ horses are colored the same. We will in fact show that $H\#1$ is colored the same as $H\#2$. Since we know that $H\#2$ is colored the same as $H\#3, H\#4, \dots$, then that will yield that $H\#1$ is colored the same as the rest. To show that $H\#1$ and $H\#2$ are colored the same, let's take our original collection of horses, $H\#1, H\#2, \dots, H\#(n + 1)$ and this time let's remove $H\#(n + 1)$. We now have a collection of n horses and so we know by our inductive assumption that all the horses in this collection are colored the same. In particular, $H\#1$ and $H\#2$ are colored the same. So p_{n+1} is true whenever p_n is true and therefore by the Principle of Mathematical Induction, p_n is true for all positive integers n .

Now we will apply the above result to prove our claim. There are only finitely many horses in the world. Let n denote that number. Then as p_n is true, in any given collection containing precisely n horses, all the horses in that collection are colored the same. Let's use as our collection the collection of all horses in the world. We then have that all the horses in that collection are colored the same.

3. **Claim:** $n^2 + n$ is odd for all positive integers n .

Proof. 1 is odd and so the assertion holds when $n = 1$. Assume that $n^2 + n$ is odd. Then there exists an integer m such that $n^2 + n = 2m + 1$. So

$$\begin{aligned}
 (n+1)^2 + (n+1) &= (n^2 + 2n + 1) + (n+1) \\
 &= (n^2 + n) + (2n + 2) \\
 &= (2m + 1) + (2n + 2) \\
 &= 2(m + n + 1) + 1.
 \end{aligned}$$

Since m and n are integers, so is $m + n + 1$. Consequently $(n+1)^2 + (n+1)$ is odd whenever $n^2 + n$ is odd. Therefore by the Principle of Mathematical Induction, $n^2 + n$ is odd for all positive integers n .

IV. Investigations

1. In Exercise 1 in Section 1, we defined S_n for each positive integer n , by

$$S_n = 1 + 2 + \cdots + n.$$

- Find a formula that relates S_{n+1} to S_n .
- Find a closed-form formula for S_n . (Hint: The "pairing" technique we used in Example 3 of Section 1 might be helpful here.)
- Use the Principle of Mathematical Induction to prove that your formula in part **b** is correct.

2. For each positive integer n , let $S_n = 1 + 2 + 2^2 + \cdots + 2^n$.

- Find a formula that relates S_{n+1} to S_n .
- Find a closed-form formula for S_n .
- Use the Principle of Mathematical Induction to prove that your formula in part **b** is correct.

3. For each integer n where $n \geq 2$, let $B_n = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) \cdots \left(1 - \frac{1}{n}\right)$.

- Calculate B_2 , B_3 , and B_4 .
- Find a closed-form formula for B_n .
- Prove your conjecture from part **b** using the second version of the Principle of Mathematical Induction.

4. For each positive integer n , let p_n be the statement $2^n > n^2$.

a) For which positive integers is p_n true?

b) Prove your result in part a using the Principle of Mathematical Induction II.

5. In Exercise 3 of Section 1, we defined a sequence $\langle a_n \rangle_{n=1}^{\infty}$ of real numbers as follows:

Let $a_1 = 1$ and for each positive integer n , we defined $a_{n+1} = \sqrt{3a_n + 1}$.

In Example 7, we proved that $a_n \leq 4$ for all n . Let's conjecture that $a_n \leq 3$ for all n . Try to give a proof of that conjecture using the Principle of Mathematical Induction. Where does that proof break down? Is the conjecture true? Justify your answer.

6. For each positive integer n , let $a_{n+1} = (a_n)^{\frac{1}{2}}$.

a) Define a_1 to be 8. Are the successive values always increasing, always decreasing, or sometimes increasing and sometimes decreasing? What happens in the long run?

b) What happens if you begin with $a_1 = \frac{1}{8}$?

c) Try several other values for a_1 . What conjectures would you make?

d) Find a formula that relates a_n to a_1 . Prove that your formula is correct using the Principle of Mathematical Induction.

e) Use your formula from part d to determine what happens to a_n in the long run. (You should expect that the behavior of a_n will depend upon the initial value for a_1 .)