Appendix B

Mathematical Induction and the Well-Ordering Principle

Focus Questions

By the end of this investigation, you should be able to give precise and thorough answers to the questions listed below. You may want to keep these questions in mind to focus your thoughts as you complete the investigation.

- What does the Principle of Mathematical Induction say? What do we need to verify in order to prove a statement using the Principle of Mathematical Induction?
- How do the extended and strong forms of induction differ from the Principle of Mathematical Induction? How are all of these different versions of induction similar?
- What does the Well-Ordering Principle say? What do we need to verify in order to prove a statement using the Well-Ordering Principle?
- How are the Principle of Mathematical Induction, the Extended Principle of Mathematical Induction, the Strong Form of Mathematical Induction, and the Well-Ordering Principle all related?

Preview Activity B.1. Suppose you are on a game show called *Let's Make a Great Deal*. You have reached the final round and will be asked one question. If you answer the question correctly, you will win a key to open door number 1. Behind door number 1 is a prize and a key to open door number 2. Behind door number 2 is a prize and a key to open door number 3. Behind door number 3 is a prize and a key to open door number 4, and so on.

(a) How many prizes will you win if you fail to answer the question correctly?

(b) Which prizes will you win if you answer the question correctly?

Introduction

Mathematical induction is an important tool in mathematics. Induction helps us prove that certain types of statements are true for *all* positive integers. This is quite a feat, since there are infinitely

many positive integers! Mathematical induction comes in more than one flavor. There is the basic principle, the extended principle, and the strong (or second, or complete) principle. An equivalent version of the Principle of Mathematical Induction is the Well-Ordering Principle. We will study each of these principles in this investigation.

The Principle of Mathematical Induction

Activity B.1 demonstrated the basic idea behind induction. Just as no prize comes for free (in our game, we needed to answer the question in order to win anything), to verify a statement using induction, we will need to prove something. In other words, we will need to unlock the door that has our first statement behind it. But unlocking the first door is not enough to unlock every other door, unless we are able to establish—as was specified in the rules of our game show—that each door, when opened, contains the key to the next door. If this condition also holds, then once we open the first door—that is, once we prove the first statement—we will be able to open every other door, thus proving our statement for every positive integer.

To illustrate this process in a more concrete way, consider the example in the following activity.

Activity B.2. Let n be a positive integer. Complete Table B.2. What do you notice?

n	$1+2+3+\cdots+n$	$\frac{n(n+1)}{2}$
1		
2		
3		
4		
5		

The calculations in Activity B.2 show that

$$1+2+3+\cdots+n=\frac{n(n+1)}{2} \tag{B.1}$$

for all integers n between 1 and 5. A few more calculations might convince you that equation (B.1) is actually true for many more integers, and perhaps for all positive integers. Although we cannot physically evaluate both sides of equation (B.1) to determine if it is true for every positive integer, we can use mathematical induction to accomplish the same goal.

To return to our game show analogy, think of verifying equation (B.1) as the goal of the game. Each door corresponds to one instance of equation (B.1). The first door corresponds to equation (B.1) with $n=1$, the second door to equation (B.1) with $n=2$, and so on. In general, for each positive integer m, the m^{th} door corresponds to equation (B.1) with $n=m$.

In this context, the question we need to answer to open door number one is whether equation (B.1) is true when $n=1$.

Activity B.3. Is equation (B.1) is true when $n=1$? Why?

Opening the first door is important, but it does not complete the problem of proving equation (B.1) for *all* positive integers. In the game, behind each door was a key to opening the next door. Of course, these keys were a critical part of the game. If one of the doors did not have a key to the next, then we wouldn't necessarily win all of the prizes just by opening the first door. In the same way, to complete our verification of equation (B.1), we will need to show that the first door ($n = 1$) contains the key to the second door ($n = 2$), the second door ($n = 2$) contains the key to the third door ($n = 3$), and so on.

Our calculations in Activity B.2 show that equation (B.1) is true for n from 1 to 5, but they don't demonstrate that each holds the key to the next. In other words, if equation (B.1) is true for $n = 1$, must it also be true when $n = 2$? And if equation (B.1) is true when $n = 2$, must it also be true when $n = 3$? And so on. In a nutshell, what we need to demonstrate is that if equation (B.1) is true for some arbitrary positive integer n, then it must also be true for the integer $n + 1$. This shows that each instance when equation (B.1) is true for a given positive integer n provides the key to proving that the equation is also true for the integer $n + 1$.

As an example, let's show that if equation (B.1) is true for $n = 1$, then it must also be true for $n = 2$. To do so, we will assume equation (B.1) is true when $n = 1$. That is, we will assume that

$$1 = \frac{(1)(2)}{2}. \tag{B.2}$$

Assuming equation (B.2) is true, we need to prove that equation (B.1) is true when $n = 2$, or that

$$1 + 2 = \frac{(2)(3)}{2}.$$

Since we are assuming equation (B.1) to be true when $n = 1$, we can begin with the true statement (B.2). Adding 2 to both sides of equation (B.2) yields

$$\begin{aligned} 1 + 2 &= \frac{(1)(2)}{2} + 2 \\ &= \frac{(1)(2) + 2(2)}{2} \\ &= \frac{(2)(1 + 2)}{2} \\ &= \frac{(2)(3)}{2}, \end{aligned}$$

which shows that equation (B.1) is true when $n = 2$ (assuming that the same equation is true when $n = 1$).

Activity B.4. To complete our proof of equation (B.1) for all positive integers n, we need to verify that whenever equation (B.1) for some arbitrary positive integer n, then it is also true for the integer $n + 1$.

(a) Continue, as above, to show that if equation (B.1) is true for $n = 2$, then it is also true for $n = 3$.

(b) Of course, we cannot continue showing each specific implication in turn, as that would take an infinite amount of time. To be more efficient, we really want to show that if n is any positive integer and equation (B.1) is true for n, then equation (B.1) is also true for $n+1$. To do this, we let n be an arbitrary positive integer and assume that equation (B.1) is true for n. That is, we assume that

$$1 + 2 + 3 + \cdots + n = \frac{(n)(n + 1)}{2}.$$

Use this assumption to show that equation (B.1) is true for $n + 1$.

To summarize, we needed to prove two things to show that equation (B.1) is true for all positive integers n:

(1) Equation (B.1) is true when $n = 1$; and

(2) whenever equation (B.1) is true for a positive integer n, then it is also true for the integer $n + 1$.

Step 1 is equivalent to answering the question in our game show and opening the first door. The prize is that equation (B.1) is true when $n = 1$. Step 2 verifies that each door holds the key to opening the next—that is, if equation (B.1) is true for the integer n, then it is also true for $n + 1$. Completing both steps shows that equation (B.1) is true for every positive integer n.

Let's now formalize the ideas from the previous example. In doing so, we will develop the Principle of Mathematical Induction, which can be used when we have a family of statements, one for each positive integer, that we want to prove. For example, for each positive integer n, let $P(n)$ be the statement that

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^n - 1 \tag{B.3}$$

To prove that $P(n)$ is true for all $n \in \mathbb{N}$, we have seen that we need to prove that:

(1) $P(1)$ is true (we call this the *base case*); and

(2) for every positive integer n, if $P(n)$ is true, then $P(n + 1)$ is also true. (This second step is called the *inductive step*.)

When we prove the inductive step, we assume $P(n)$ is true for some arbitrary positive integer n. This assumption is called the *induction hypothesis* or *inductive hypothesis*. We then show, using this assumption, that $P(n + 1)$ is also true.

Rephrasing this process in a slightly different form leads us to the formal statement of the Principle of Mathematical Induction. Let S be the set of positive integers for which $P(n)$ is true. Proving $P(1)$ is true is the same as showing that 1 is in S. Likewise, showing that $P(n)$ implies $P(n + 1)$ is equivalent to showing that $n + 1 \in S$ whenever $n \in S$. Combining these two observations, we arrive at the following axiom:

Axiom B.5 (Principle of Mathematical Induction)**.** *Let S be a subset of the set of natural numbers $\mathbb{N}$. If*

(i) *S contains 1 and*

(ii) *S contains the positive integer $n + 1$ whenever S contains n,*

then $S = \mathbb{N}$.

In essence, the Principle of Mathematical Induction tells us that if we have a set $S \subseteq \mathbb{N}$ containing 1, and if S contains the integer $n + 1$ whenever S contains n, then S must contain $1 + 1 = 2$. But then S must also contain $2 + 1 = 3$, and $3 + 1 = 4$, and so on. Therefore, S will contain *all* natural numbers. By using the Principle of Mathematical Induction, we can prove infinitely many statements in only two steps.

To illustrate, let's formally apply the Principle of Mathematical Induction to establish equation (B.3). Let

$$S = \{n \in \mathbb{N} : 1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^n - 1\}.$$

To use the Principle of Mathematical Induction, we need to show that $1 \in S$ and that $n+1 \in S$ whenever $n \in S$. First we will show that $1 \in S$ (the base case). Notice that when $n = 1$, we have

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^0 = 1$$

and

$$2^n - 1 = 2^1 - 1 = 2 - 1 = 1.$$

So equation (B.3) is true when $n = 1$, which means that $1 \in S$. For the inductive step, we need to show that $n+1 \in S$ whenever $n \in S$. To do so, we will assume that $n \in S$ for some integer $n \geq 1$ (the inductive hypothesis). In this case, we will assume that

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^n - 1. \tag{B.4}$$

We then need to prove that $n+1 \in S$. So we need to show that

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} + 2^{(n+1)-1} = 2^{n+1} - 1,$$

or, equivalently,

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} + 2^n = 2^{n+1} - 1. \tag{B.5}$$

To prove (B.5), we can substitute from (B.4) in the left hand side of (B.5) to obtain

$$\begin{aligned} 1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} + 2^n &= \left(1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1}\right) + 2^n \\ &= (2^n - 1) + 2^n \\ &= 2(2^n) - 1 \\ &= 2^{n+1} - 1, \end{aligned}$$

which shows that $n+1 \in S$. Therefore, $S = \mathbb{N}$ by the Principle of Mathematical Induction, which means that (B.3) is true for all $n \in \mathbb{N}$.

Activity B.6. Let r be a real number with $r > 1$. Consider the statements

$$1 + r + r^2 + r^3 + \cdots r^{n-1} = \frac{r^n - 1}{r - 1} \tag{B.6}$$

for all $n \geq 1$. (Note that you have probably seen equation (B.6) in a previous class. Do you remember where it comes from?) We will use induction to prove that (B.6) is true for all $n \in \mathbb{N}$.

(a) Identify an appropriate set S on which to apply our induction argument.

(b) What is the base case? Give a precise statement, and then verify your statement.

(c) What is the induction hypothesis? What is the inductive step?

(d) Complete the inductive step to verify that equation (B.6) is true for all $n \in \mathbb{N}$.

The Extended Principle of Mathematical Induction

Preview Activity B.7. Let's now return to our *Let's Make a Great Deal* game. Suppose you fail to correctly answer the question that allows you to open the first door. But suppose also that, after

doing so, the host gives you the opportunity to answer a second question. If you correctly answer question number 2, then you win a key to open door number 2. As before, behind door number 2 is a prize and a key to open door number 3. Behind door number 3 is a prize and a key to open door number 4, and so on.

(a) Which prizes would you win if you answered the second question correctly?

(b) Suppose you fail to answer the second question correctly. The host then gives you an option of answering a third question. If you correctly answer question number 3, then you win a key to open door number 3. Which prizes would you win if you answered the third question correctly?

(c) Suppose you fail to answer the third question correctly. The host then gives you an option of answering a fourth question. If you correctly answer question number 4, then you win a key to open door number 4. Which prizes would you win if you answered the fourth question correctly?

(d) You probably see the pattern by now. Suppose you fail to answer the first $m - 1$ questions correctly for some integer $m \geq 2$. The host then gives you an option of answering an m^{th} question. If you correctly answer question number m, then you win a key to open door number m. Which prizes would you win if you answered the m^{th} question correctly?

(e) Compare this version of the game to the version described in Activity B.1. How are the two versions alike, and how are they different?

The Principle of Mathematical Induction that we stated in the previous section is a method for proving an entire family of statements, one for each positive integer n. There are, however, instances when we need to modify our induction arguments slightly. For example, consider the statement

$$2^n < n!.$$

If we try to prove this statement for all $n \in \mathbb{N}$, we immediately encounter a problem in that the statement is not true for $n = 1$. In fact, the statement is also false for $n = 2$ and $n = 3$. However, the statement does appear to be true for $n \geq 4$. If we want to use the Principle of Mathematical Induction to prove that this statement is true for $n \geq 4$, we will need to somehow translate it to an equivalent statement that is true for *all* positive integers. One way to do this is by re-indexing the statement to say

$$2^{n+3} < (n + 3)!$$

for all positive integers n. Although this would solve the problem, the resulting statement is more complicated, and if we started with a more involved result, re-indexing could potentially make the situation appear more difficult than it really is. This is where the result of Activity B.7 is useful; in fact, proving that $2^n < n!$ for all $n \geq 4$ is analogous to answering the 4^{th} question correctly. The point of Activity B.7 is that it really shouldn't make any difference what our starting point is, as long as we have one. If we can open door number n_0 for some integer n_0, then we will be able to open all doors with numbers higher than n_0 as well—even though we may not be able to open the doors numbered lower than n_0. This is the idea behind the *Extended Principle of Mathematical Induction*.

Axiom B.8 (Extended Principle of Mathematical Induction)**.** *Let S be a subset of the set of the integers $\mathbb{Z}$. If there is an integer n_0 such that*

(i) *S contains n_0 and*

(ii) *for all $n \geq n_0$, S contains the positive integer $n + 1$ whenever S contains n,*

then S contains every integer greater than or equal to n_0.

When applying the Extended Principle of Mathematical Induction, our base case is when $n = n_0$ instead of $n = 1$, but the inductive step is still the same. Note that our goal in this situation is to show that S contains every integer greater than or equal to n_0, which establishes that our statement is true for all $n \geq n_0$. Doing so doesn't rule out the possibility that S could contain other integers as well, but we are only interested in the integers greater than or equal to n_0.

Activity B.9. To illustrate the Extended Principle of Mathematical Induction, we will continue with our example of proving that $2^n < n!$ for all $n \geq 4$.

(a) State and verify the base case for this inductive proof.

(b) What is the inductive hypothesis in this proof? Give a precise statement, and then complete the inductive step.

(c) What conclusion can you draw from your work in parts (a) and (b)?

Notice that the only difference between the Principle of Mathematical Induction and the Extended Principle of Mathematical Induction is the base case. In fact, letting $n_0 = 1$ in the Extended Principle yields the original Principle of Mathematical Induction. A bit later, we will see that these two forms of induction are actually equivalent.

Before we move one, one additional comment about the format of induction proofs is in order. Generally, when we construct an induction argument, we do not set up the set S as we have done in our previous examples. Instead, if we are trying to prove a family $\{P(n)\}$ of statements, one for each integer greater than or equal to some integer n_0, we simply prove that $P(n_0)$ is true, and then prove that if $P(n)$ is true for some integer $n \geq n_0$, then $P(n+1)$ is also true. In the induction proofs throughout the rest of this appendix (and throughout the remainder of the text), we will follow this simplified format.

The Strong Form of Mathematical Induction

Preview Activity B.10. Let's return once more to our *Let's Make a Great Deal* game. We will keep the rules the same and suppose in addition that behind each door is not only a prize and a key to open the next door, but also keys to open all of the *preceding* doors. Compare and contrast this game to the previous versions of the game we have studied. How is it similar, and how is it different? Do the outcomes of the game change?

The version of the *Let's Make a Great Deal* game from Activity B.10 may seem a bit silly; after all, why do we need all of those extra keys? But let's examine how this version of the game translates to an induction proof. We still need to answer some question (prove some base case n_0) to begin. In our previous inductive steps, we then showed that $n \in S$ implies $n + 1 \in S$—that is, each door contains the key to the next door. In our new version of the game, the idea of having all of the keys to the preceding doors is analogous to assuming not only that $n \in S$, but also that n_0, $n_0 + 1$, $n_0 + 2$, . . ., n are all in S. In other words, we can assume the validity of all of the previous statements, not just the n^{th} statement. To see why this might be useful, consider the statement that

every nonnegative integer n has a binary representation—that is, there exists $r \geq 0$ and integers a_r, a_{r-1}, …, a_1, a_0, all either 0 or 1, such that

$$n = a_r 2^r + a_{r-1} 2^{r-1} + \cdots + a_2 2^2 + a_1 2 + a_0.$$

For our base case ($n = 0$) we have that $0 = 0$, and so we are done (letting $r = 0$ and $a_0 = 0$). For the inductive step, it is a bit complicated to add 1 to n (in binary) to show that $n + 1$ has a binary representation. (We would have to worry about all the possible carries.) However, if $n + 1$ is even, then $k = (n + 1)/2$ is smaller than $n + 1$. If k has a binary representation

$$k = b_s 2^s + b_{s-1} 2^{s-1} + \cdots + b_2 2^2 + b_1 2 + b_0,$$

then

$$n + 1 = 2k = b_s 2^{s+1} + b_{s-1} 2^s + \cdots + b_2 2^3 + b_1 2^2 + b_0 2,$$

and so $n + 1$ has a binary representation. If $n + 1$ is odd, then $k = n/2$ is smaller than $n + 1$. If k has a binary representation

$$k = b_s 2^s + b_{s-1} 2^{s-1} + \cdots + b_2 2^2 + b_1 2 + b_0,$$

then

$$n + 1 = 2k + 1 = b_s 2^{s+1} + b_{s-1} 2^s + \cdots + b_2 2^3 + b_1 2^2 + b_0 2 + 1,$$

and so $n+1$ has a binary representation in this case as well. By assuming that *all* of the nonnegative integers less than or equal to n have binary representations, we can fairly easily prove that $n + 1$ also has a binary representation.

Being able to assume the statement we want to prove for *all* integers less than or equal to n is at times necessary for us to carry out an induction proof. The axiom that allows us to use such a method is called the *Strong Form of Mathematical Induction*.

Axiom B.11 (Strong Form of Mathematical Induction)**.** *Let S be a subset of $\mathbb{Z}$ containing some integer n_0. Suppose that for all $n \geq n_0$, S contains $n + 1$ whenever S contains each integer m with $n_0 \leq m \leq n$. Then S contains all integers greater than or equal to n_0.*

To reiterate, the Strong Form of Mathematical Induction allows us to assume much more in our inductive hypothesis than the previous two versions do. Strong induction is useful in a variety of settings, including proving results involving certain recursively defined sequences like the Fibonacci sequence.

Recall that the Fibonacci sequence is defined by the recurrence relation

$$f_n = f_{n-1} + f_{n-2} \tag{B.7}$$

for all $n \geq 3$, with $f_1 = f_2 = 1$. The recurrence relation (B.7) is very time consuming to use to compute f_n for large values of n. However, it turns out that there is a fascinating formula that gives the n^{th} term of the Fibonacci sequence directly, without using the relation from (B.7).

Let $\varphi = \frac{1+\sqrt{5}}{2}$ and $\overline{\varphi} = \frac{1-\sqrt{5}}{2}$. We will show that

$$f_n = \frac{\varphi^n - \overline{\varphi}^n}{\sqrt{5}}. \tag{B.8}$$

Formula (B.8) is called *Binet's Formula.*[*] The number $\varphi = \frac{1+\sqrt{5}}{2}$ is intimately related to the Fibonacci sequence. This number also occurs often in other areas of mathematics. It was an important

[*] If you wonder where a formula like this comes from, the quantities φ and $\overline{\varphi}$ are eigenvalues for a certain matrix that we can use to generate the Fibonacci sequence. This formula follows in a straightforward manner.

number to the ancient Greek mathematicians who felt that the most aesthetically pleasing rectangles had sides in the ratio of $\varphi : 1$. The Greeks called φ the *golden mean* or *golden ratio*. Formula (B.8) provides a fascinating relationship between the Fibonacci numbers and the golden ratio. It is also surprising (and not at all obvious) that the expression on the right hand side of (B.8) is an integer for each positive integer n.

To prove formula (B.8), we will use mathematical induction. Note that since f_1 and f_2 are defined independent of the recursion relation, it will be necessary to verify our statement in both the $n = 1$ and $n = 2$ cases. First we will make a few observations. Note that the golden ratio φ and its conjugate $\overline{\varphi}$ are the solutions (check this!) to the quadratic equation

$$x^2 = x + 1.$$

In addition,

$$\varphi + \overline{\varphi} = 1 \qquad \text{and} \qquad \varphi - \overline{\varphi} = \sqrt{5}.$$

Therefore,

$$\varphi^{n+1} = \varphi^2\varphi^{n-1} = (\varphi + 1)\varphi^{n-1} = \varphi^n + \varphi^{n-1}.$$

Similarly,

$$\overline{\varphi}^{n+1} = \overline{\varphi}^2\overline{\varphi}^{n-1} = (\overline{\varphi} + 1)\overline{\varphi}^{n-1} = \overline{\varphi}^n + \overline{\varphi}^{n-1}.$$

We will use these last two identities in our proof of Binet's Formula. We will proceed by mathematical induction on n. When $n = 1$, we have

$$\frac{1}{\sqrt{5}}(\varphi + \overline{\varphi}) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = \frac{\sqrt{5}}{\sqrt{5}} = 1 = f_1.$$

So equation (B.8) is true when $n = 1$. When $n = 2$, we have

$$\begin{aligned}
\frac{1}{\sqrt{5}}(\varphi^2 + \overline{\varphi}^2) &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right] \\
&= \frac{1}{\sqrt{5}}\left(\frac{1}{4}(1 + 2\sqrt{5} + 5) - \frac{1}{4}(1 - 2\sqrt{5} + 5)\right) \\
&= \frac{\sqrt{5}}{\sqrt{5}} \\
&= 1 \\
&= f_1.
\end{aligned}$$

So equation (B.8) is true when $n = 2$.

Since each term in the Fibonacci sequence depends on the preceding two terms, we will need to use the Strong Form of Mathematical Induction in our proof. Therefore, assume equation (B.8) is true for all positive integers m less than a given $n \geq 2$. We must show that

$$f_{n+1} = \frac{\varphi^{n+1} - \overline{\varphi}^{n+1}}{\sqrt{5}}.$$

This follows by observing that

$$\begin{aligned}\frac{\varphi^{n+1}-\overline{\varphi}^{n+1}}{\sqrt{5}} &= \frac{1}{\sqrt{5}}\left[\left(\varphi^n+\varphi^{n-1}\right)-\left(\overline{\varphi}^n+\overline{\varphi}^{n-1}\right)\right]\\ &= \frac{1}{\sqrt{5}}\left[\left(\varphi^n-\overline{\varphi}^n\right)+\left(\varphi^{n-1}-\overline{\varphi}^{n-1}\right)\right]\\ &= f_n+f_{n-1}\\ &= f_{n+1}.\end{aligned}$$

Thus, by induction, Binet's Formula is true for all $n \in \mathbb{N}$.

Note that, with Binet's Formula, we can easily compute f_n for very large values of n. For example, f_{500} is equal to

$$\begin{aligned}&139423224561697880139724382870407283950070256587697 3\\ &072641089629483255716228632906915576588762225212941 25.\end{aligned}$$

The Well-Ordering Principle

Preview Activity B.12.

(a) Which of the following sets contains a smallest element? Explain.

(i) $A = \{1, 2, 3, 4\}$

(ii) $B = \{n \in \mathbb{N} \mid n > 4\}$

(iii) $C = \{x \in \mathbb{Z} \mid x > 4\}$

(iv) $D = \{x \in \mathbb{Z} \mid x < 4\}$

(b) Do you believe the following statement is true or false?

Every nonempty subset of $\mathbb{N}$ has a least element.

No proof is required if you believe the statement is true, but if you believe it is false, you should be able to give a counterexample.

(c) Do you believe the following statement is true or false?

Every nonempty subset of $\mathbb{Z}$ has a least element.

No proof is required if you believe the statement is true, but if you believe it is false, you should be able to give a counterexample.

(d) Let's return to our *Let's Make a Great Deal* game. Suppose a friend of yours has won the game. Is it possible to determine which question your friend answered correctly to win? Explain.

We will begin our discussion of the Well-Ordering Principle with the following familiar proof that $\sqrt{2}$ is not a rational number:

> Assume to the contrary that $\sqrt{2} = \frac{m}{n}$ for some positive integers m and $n \neq 0$ so that $\frac{m}{n}$ is in reduced form (that is, the greatest common divisor of m and n is 1). Then $n\sqrt{2} = m$, and so $2n^2 = m^2$. Thus, the prime 2 divides m^2 and so 2 also divides m. This means that $m = 2k$ for some integer k. Then $4k^2 = m^2 = 2n^2$, and so $2k^2 = n^2$. From this we see that 2 divides n, contradicting the fact that m and n have no common factors greater than 1. We can therefore conclude that $\sqrt{2}$ is not a rational number.

All of the results that we used in this proof—including those that you may not have seen before—are verified in our investigations, with one exception. This exception illustrates how easy it is to take certain mathematical results for granted. The exception in the proof is that we can always find a rational number *in reduced form* that is equal to $\frac{m}{n}$. How do we know we can do this? Recall that the rational numbers $\frac{a}{b}$ and $\frac{c}{d}$ are equal if $ad = bc$. To show that we can find a rational number in reduced form that is equal to $\frac{m}{n}$, we might consider all rational numbers $\frac{a}{b}$ that are equal to $\frac{m}{n}$ and prove that there is one so that the greatest common divisor (or gcd) of a and b is 1. In other words, let

$$S = \left\{ \gcd(a, b) : \frac{a}{b} = \frac{m}{n} \right\}$$

be the set of all greatest common divisors of the numerators and denominators of fractions that are equal to $\frac{m}{n}$. Certainly S is not empty, since $\gcd(m, n)$ is in S. Also, since $\gcd(x, y) \geq 1$ for any integers x and y, not both 0, it follows that the integers in S are all greater than or equal to 1. We need to actually show that 1 is in S. If 1 is in S, then 1 will have to be the smallest element in S.

This is where our conclusion from Activity B.12 is helpful. If we assume that every nonempty subset of $\mathbb{N}$ contains a smallest integer, then S must contain a smallest integer d. Now all we have to do is show that $d = 1$. This is because if $d = 1$, then there must be a fraction $\frac{a}{b}$ equal to $\frac{m}{n}$ with $\gcd(a, b) = 1$. Since $d \in S$, there exists a rational number $\frac{a}{b}$ that is equal to $\frac{m}{n}$ with $\gcd(a, b) = d$. Now d divides both a and b, so let $da' = a$ and $db' = b$ for some positive integers a' and b'. Since $d = \gcd(a, b)$, it follows that $\gcd(a', b') = 1$. But

$$\frac{m}{n} = \frac{a}{b} = \frac{a'd}{b'd} = \frac{a'}{b'},$$

and so $\gcd(a', b')$ is in S. However, this can happen only if $d = 1$, and so 1 is the smallest element in S, and there is a fraction in reduced form that is equal to $\frac{m}{n}$.

The key to our proof that every rational number is equal to a rational number in reduced form was the assumption that the set S contained a smallest element. Based on Activity B.12, this seems like a reasonable assumption to make. The principle that allows us to make it is called the *Well-Ordering Principle*.

To thoroughly understand the Well-Ordering Principle, we first need to discuss well-ordered sets. But to talk about well-ordered sets, we need to understand ordered sets in general. This leads us to the idea of binary relations.

A *binary relation* on a set (or *relation* for short) is simply a way to compare elements in the set. For example, consider the set consisting of the citizens of the state of Michigan. We might say that one person is related to another if the two have at least one parent in common. Note that some people in this set are related and others are not. This observation illustrates the fact that a relation on a set does not need to compare *every* pair of elements in the set.

As a smaller example, let $S = \{1, 2, 3, 4\}$, and say that a and b are related in S if a divides b. In this case we have that 1 is related to 2, 3, and 4, while 2 is related only to 4. To clearly identify related pairs of elements in S, we might list all of the related elements as ordered pairs. For this relation, the resulting pairs are $(1, 2)$, $(1, 3)$, $(1, 4)$, and $(2, 4)$. The general definition of a relation on a set follows this example.

Definition B.13. A **relation** on a set S is a subset R of the Cartesian product $S \times S$. In other words, a relation on S is a set of ordered pairs, where both coordinates of each pair are elements of S.

For example, the subset $R = \{(a, a) : a \in \mathbb{Z}\}$ of $\mathbb{Z} \times \mathbb{Z}$ is the relation we call *equals*. If R is a relation on a set S, we usually suppress the set notation and write $a \sim b$, read "a is related to b," if $(a, b) \in R$. In this case, we often refer to $\sim$ as the relation instead of the set R. Sometimes we use familiar symbols for special relations. For example, we write $a = b$ if (a, b) is in the set $R = \{(a, a) : a \in \mathbb{Z}\}$.

There are several properties that relations may satisfy. For example:

- A relation $\sim$ on a set S is *reflexive* if $a \sim a$ for all $a \in S$.
- A relation $\sim$ on a set S is *symmetric* if whenever $a \sim b$ (for any a, $b \in S$), we also have $b \sim a$.
- A relation $\sim$ on a set S is *transitive* if whenever $a \sim b$ and $b \sim c$ (for any a, b, $c \in S$), we also have $a \sim c$.
- A relation $\sim$ on a set S is *antisymmetric* if whenever $a \sim b$ and $b \sim a$ (for any a, $b \in S$), then $a = b$.

Activity B.14. Determine whether each of the given relations on $\mathbb{Z}$ is reflexive, symmetric, transitive, and/or antisymmetric. Give reasons to support your answers.

(a) $R = \{(a, b) : a > b\}$

(b) $R = \{(a, b) : a^2 = b^2\}$

(c) $R = \{(a, b) : ab \geq 0\}$

(d) $R = \{(a, b) : a$ and b leave the same remainder when divided by $3\}$

Some relations, like the relation $\leq$ on $\mathbb{R}$, give us a way of organizing the elements in the sets on which they are defined in a specified way (e.g., on the number line). The next definition formalizes this idea.

Definition B.15. A set S is a **partially ordered set** (or **poset**) if there is a relation, which we will denote by $\leq$, on S such that for all $x, y, z \in S$:

(i) $x \leq x$ ($\leq$ is a reflexive relation);

(ii) if $x \leq y$ and $y \leq x$, then $x = y$ ($\leq$ is an antisymmetric relation); and

(iii) if $x \leq y$ and $y \leq z$, then $x \leq z$ ($\leq$ is a transitive relation).

A partially ordered set S is **totally ordered** if it also satisfies

(iv) either $x \leq y$, $y \leq x$, or $x = y$ ($\leq$ satisfies the trichotomy property).

What makes a partially ordered set totally ordered is that *any* two elements are related somehow, which is not necessary in a partially ordered set. An example of a partially ordered set that is not totally ordered is the set of positive integers, where a is related to b if a divides b. Examples of totally ordered sets are $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, using the standard "less than or equal to" relation ($\leq$).

The Well-Ordering Principle tells us that any subset of $\mathbb{Z}$ that is bounded below contains a smallest element. To make this all precise, we need to explain what we mean by a smallest element in a set and also what bounded below means. These definitions should not be surprising.

Definition B.16. Let S be a totally ordered set, and let A be a subset of S.

- An element $m \in S$ is a **lower bound** for A if $m \leq a$ for all $a \in A$. The set A is **bounded below** if A has a lower bound in S.
- An element $a \in A$ is a **least** or **smallest** element in A if $a \leq a'$ for all $a' \in A$.

It is important to note the difference between a lower bound and a smallest element. The integer -2 is a lower bound for $\mathbb{N}$, but is not a smallest element in $\mathbb{N}$ since it is not an element of $\mathbb{N}$. Every smallest element in a set is also a lower bound for the set. However, not every set is bounded below or contains a least element. For example, the set of even integers is not bounded below. In addition, a set can be bounded below but not contain a least element. For example, the open interval $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$ is bounded below by 0 but does does not have a smallest element (since there is no smallest positive real number).

We have one more step before stating the Well-Ordering Principle.

Definition B.17. A totally ordered set S is **well-ordered** if every nonempty subset A of S contains a least element.

We can now formally state the Well-Ordering Principle.

Axiom B.18 (The Well-Ordering Principle)**.** *Every nonempty subset of $\mathbb{Z}$ that is bounded below is well-ordered.*

The Well-Ordering Principle is often stated within the specific context of the natural numbers, where it implies that every nonempty subset of $\mathbb{N}$ contains a smallest element. Our version is somewhat more general and is equivalent to the following:

Axiom B.19 (The Well-Ordering Principle)**.** *Every nonempty subset of $\mathbb{Z}$ that is bounded below contains a smallest element.*

Note that, in general, a set can have a smallest element without being well-ordered. Consider, for example, the set $\mathbb{R}^*$ of all nonnegative real numbers. Note that $\mathbb{R}^*$ has a smallest element—namely, 0—but is not well-ordered, since it contains a nonempty subset (the positive reals, for example) that does not have a smallest element. The equivalence of the two forms of the Well-Ordering Principle, as we have stated them, stems from the fact that both are universally quantified—that is, both refer to *every* nonempty subset of $\mathbb{Z}$ that is bounded below. The first is really saying that if S is a nonempty subset of $\mathbb{Z}$ that is bounded below, then every nonempty subset of S contains a smallest element. But a nonempty subset of S is still a nonempty subset of $\mathbb{Z}$ that is bounded below. For this reason, the second version of the Well-Ordering Principle is equivalent to the first.

As an example of the use of the Well-Ordering Principle, we will prove the following theorem, which we also proved in Investigation 1 as part of the Fundamental Theorem of Arithmetic. (See page 10.)

Theorem. *Every integer greater than 1 is either prime or can be factored into a product of primes.*

Proof. To use the Well-Ordering Principle, we need to define a nonempty subset of $\mathbb{Z}$ that is bounded below. To do so, we will proceed by contradiction and assume that there is an integer greater than 1 that is not prime and cannot be written as a product of primes. Let

$$S = \{n \in \mathbb{N} : n \text{ is not prime and cannot be written as a product of primes}\}.$$

Then S is nonempty by hypothesis and is bounded below (by 1). The Well-Ordering Principle tells

us that S contains a smallest element m. By definition, m is not prime, so there exist integers a and b with $1 < a, b < m$ such that $m = ab$. Since m is the smallest element in S, it follows that a and b are not in S. Thus, a and b are either prime or can be written as a product of primes. Therefore, there exist positive integers r and s and primes $p_1, p_2, \ldots, p_r$ and $q_1, q_2, \ldots, q_s$ such that

$$a = p_1 p_2 \cdots p_r \quad \text{and} \quad b = q_1 q_2 \cdots q_s.$$

But then

$$m = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

is a product of primes, which is a contradiction, since we assumed that m could not be written as a product of primes. We can therefore conclude that every integer greater than 1 is either prime or can be factored into a product of primes. ■

You may want to compare the above proof to the proof of the Fundamental Theorem of Arithmetic from Investigation 1, which used induction instead of the Well-Ordering Principle. It is no coincidence that both methods can be used to establish similar results. In fact, as we will see in the next section, the Well-Ordering Principle and all three different forms of the Principle of Mathematical Induction are logically equivalent.

It is also important to note that we have labeled both the principles of mathematical induction and the Well-Ordering Principle as axioms and not theorems. That is because we cannot prove any one of these principles (although, as noted above, we can prove that they are equivalent to each other), but they seem evident enough that we will assume them to be true.

The Equivalence of the Well-Ordering Principle and the Principles of Mathematical Induction

In this section, we will prove that the principles of mathematical induction and the Well-Ordering Principle are equivalent. That is, any one of these principles implies any of the others. It is important to note that Theorem B.20 does not prove any of these principles, but says that if we assume one of them to be valid, then all of the others are valid as well.

Theorem B.20. *The following are equivalent:*

(i) *The Principle of Mathematical Induction*

(ii) *The Extended Principle of Mathematical Induction*

(iii) *The Strong Form of Mathematical Induction*

(iv) *The Well-Ordering Principle.*

A word on the proof of Theorem B.20: To prove this string of equivalences, we will show that (i) implies (ii), (ii) implies (iii), (iii) implies (iv), and then (iv) implies (i). This will demonstrate that any one of the four statements implies any of the others, as can be seen by following an appropriate string of implications. (For example, to see that (iii) implies (ii), we can simply note that (iii) implies (iv), (iv) implies (i), and (i) implies (ii).) Also, the proofs of each equivalence are subtle in that both the hypotheses and conclusions are complicated statements. Because of this, we will have to be

very careful about our assumptions in each case. We will begin by showing that the Principle of Mathematical Induction implies the Extended Principle of Mathematical Induction. The steps to complete this proof are outlined in the next activity.

Activity B.21. To prove that the Principle of Mathematical Induction implies the Extended Principle of Mathematical Induction, we will assume that the Principle of Mathematical Induction is true. This means that any subset S of $\mathbb{N}$ that contains 1 and has the property that $n+1 \in S$ whenever $n \in S$ must be equal to $\mathbb{N}$.

We need to prove that the Extended Principle of Mathematical Induction is true. So we will assume that n_0 is an integer and T is a subset of $\mathbb{Z}$ such that $n_0 \in T$ and $n+1 \in T$ whenever $n \geq n_0$ and $n \in T$. We need to prove that $\{n \in \mathbb{Z} \mid n \geq n_0\} \subseteq T$.

In order to use the Principle of Mathematical Induction, we need to construct some subset of $\mathbb{N}$ that is related to T but contains 1 as its smallest element. To do so, we can shift or re-index the elements of T so that n_0 corresponds to 1. In particular, we will define S to be the set

$$S = \{k - n_0 + 1 \in \mathbb{N} \mid k \in T\}.$$

(a) Use the assumption that $n_0 \in T$ to prove that $1 \in S$.

(b) We now need to prove that if $n \geq 1$ is in S, then $n+1 \in S$. Let $n \geq 1$ be in S. There is a corresponding element k in T. Write down a formula for k in terms of n and n_0. Explain your reasoning.

(c) Based on our assumptions about T, what integer besides k must also be in T?

(d) Now use the result of part (c) to conclude that $n+1 \in S$.

This proves that S contains 1 and that $n+1 \in S$ whenever $n \in S$. Therefore, by the Principle of Mathematical Induction, $S = \mathbb{N}$. We will now use this fact to prove that $\{n \in \mathbb{Z} \mid n \geq n_0\} \subseteq T$.

By assumption, $n_0 \in T$. So we need to prove that if $x \in \mathbb{Z}$ with $x > n_0$, then $x \in T$. To this end, assume that $x \in \mathbb{Z}$ and $x > n_0$.

(e) Prove that $x - n_0 \in \mathbb{N}$ and therefore $x - n_0 \in S$.

(f) Show that part (e) implies that $x - 1 \in T$. Then explain how we can conclude that $x \in T$.

(g) Explain why we have now completed the proof that the Extended Principle of Mathematical Induction is implied by the Principle of Mathematical Induction.

We will now consider the other implications in Theorem B.20.

Proof of Theorem B.20. (ii) $\rightarrow$ (iii): We will assume that the Extended Principle of Mathematical Induction is true. We will then prove that the Strong Form of Mathematical Induction must also be true.

To prove the Strong Form, we let n_0 be an integer and assume T is a subset of $\mathbb{Z}$ such that

(1) $n_0 \in T$, and

(2) for every $n \in \mathbb{Z}$ with $n \geq n_0$, if $\{n_0, n_0+1, \ldots, n\} \subseteq T$, then $(n+1) \in T$.

We then need to prove that T contains all integers greater than or equal to n_0—or, equivalently, that

$$\{x \in \mathbb{Z} \mid x \geq n_0\} \subseteq T.$$

We will use the Extended Principle of Mathematical Induction to prove the following statement:

For each natural number k with $k \geq n_0$, $\{n_0, n_0 + 1, \ldots, k\} \subseteq T$.

Since we have assumed that $n_0 \in T$, we know that $\{n_0\} \subseteq T$. Hence the base case ($k = n_0$) is true.

For the inductive step, let $k \in \mathbb{N}$ with $k \geq n_0$, and assume that

$$\{n_0, n_0 + 1, \ldots, k\} \subseteq T.$$

By what we assumed about the set T, we can conclude that $k + 1 \in T$, and therefore

$$\{n_0, n_0 + 1, \ldots, k, k + 1\} \subseteq T.$$

This proves that if $\{n_0, n_0 + 1, \ldots, k\} \subseteq T$, then $\{n_0, n_0 + 1, \ldots, k, k + 1\} \subseteq T$ is true; hence, the inductive step has been established. By the Extended Principle of Mathematical Induction, we can conclude that for each natural number k with $k \geq n_0$, $\{n_0, n_0 + 1, \ldots, k\} \subseteq T$. This proves that T contains all integers greater than or equal to n_0, which is what we needed to prove to show that the Strong Form of Mathematical Induction is true.

We have therefore shown that if the Extended Principle of Mathematical Induction is true, then the Strong Form of Mathematical Induction is also true.

(iii) $\rightarrow$ (iv): We will now show that the Strong Form of Mathematical Induction implies the Well-Ordering Principle. We will assume the Strong Form of Mathematical Induction. That is, whenever we have a subset U of $\mathbb{Z}$ such that

- $n_0 \in U$ for some integer n_0; and
- whenever $k \in U$ for all $n_0 \leq k \leq n$, then $n + 1 \in U$,

then U contains the set of all integers greater than or equal to n_0. To prove the Well-Ordering Principle, we must show that any nonempty subset of $\mathbb{Z}$ that is bounded below contains a smallest element. We will proceed by contradiction and assume there is a nonempty subset T of $\mathbb{Z}$ that is bounded below and does not contain a least element. Let m be a lower bound for T. If $m \in T$, then T contains a smallest element, namely m. So m cannot be an element of T. Let S be the set of all strict lower bounds for T—that is,

$$S = \{n \in \mathbb{Z} : n < t \text{ for all } t \in T\}.$$

Since m is a lower bound for T and $m \notin T$ it follows that $m < t$ for all $t \in T$. So $m \in S$. Suppose $n \geq m$ so that m, $m + 1$, $m + 2$, …, n are all in S. We will show $n + 1 \in S$. Since $n \in S$ we must have $n < t$ for all $t \in T$. This, however, implies that

$$n + 1 \leq t \tag{B.9}$$

for all $t \in T$. If $n + 1 = t$ for some $t \in T$, then $n + 1$ must be the smallest element in T, which cannot happen. Therefore,

$$n + 1 \neq t \tag{B.10}$$

for all $t \in T$. Combining (B.9) and (B.10) shows $n + 1 < t$ for all $t \in T$, and so $n + 1 \in S$. By the Strong Form of Mathematical Induction, we can then conclude that S contains all integers greater than or equal to m. It follows that every integer is a strict lower bound for T, and so $T = \emptyset$, a contradiction. Therefore, no such set T exists, which means that every nonempty subset of $\mathbb{Z}$ that is bounded below contains a smallest element. We have therefore shown that the Strong Form of Mathematical Induction implies the Well-Ordering Principle.

(iv) $\rightarrow$ (i): This is left to the reader in Activity B.22.

■

Concluding Activities

Activity B.22. Complete the proof of Theorem B.20 by proving that the Well-Ordering Principle implies the Principle of Mathematical Induction. (Hint: If S is a subset of $\mathbb{N}$ that contains 1 and also contains $n + 1$ whenever S contains n, consider the set T of all natural numbers that are not in S.)

Exercises

(1) In calculus, we often use the fact that $\frac{d}{dx}x^n = nx^{n-1}$ for every positive integer n, but we usually don't provide a rigorous proof of this result. Use induction to verify this derivative formula. Assume the product rule if you need it.

(2) Prove that

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for every positive integer n.

(3) In the mid 20th century, the mathematician George Pólya suggested the apparent paradox that all girls have eyes of the same color.[†] His induction argument to verify this statement is as follows:

> For $n = 1$ the statement is obviously (or "vacuously") true. It remains to pass from n to $n + 1$. For the sake of concreteness, I shall pass from 3 to 4 and leave the general case for you.
>
> Let me introduce you to any four girls, Ann, Berthe, Carol, and Dorothy, or A, B, C, and D, for short. Allegedly ($n = 3$) the eyes of A, B, and C are of the same color. Consequently, the eyes of all four girls A, B, C, and D, must be of the same color; for the sake of full clarity, you may look at the diagram:
>
> $$\overbrace{A + \underbrace{B + C}} + D.$$

[†]This appears in Pólya's 1954 work *Induction and Analogy in Mathematics*, volume 1 of *Mathematics and Plausible Reasoning*, Princeton University Press.

This proves the point for $n+1=4$, and the passage from 4 to 5, for example, is, obviously, not more difficult.

A quick glance into the eyes of several girls will show that not all girls have the same eye color, so there must be a flaw in the argument. Find and explain the flaw.

(4) Consider the conjecture

$$1+2+3+4+\cdots+n=\frac{1}{2}\left(n+\frac{1}{2}\right)^2. \tag{B.11}$$

(a) Assume (B.11) is true for some positive integer n. That is, assume

$$1+2+3+4+\cdots+n=\frac{1}{2}\left(n+\frac{1}{2}\right)^2.$$

Show that (B.11) is true for the integer $n+1$.

(b) For which integers n is (B.11) a true statement? Explain. What does this exercise tell us about the importance of establishing a base case in an induction proof?

(5) (a) Experiment and conjecture a simple closed form for the sum

$$s_n=\frac{1}{1\times 3}+\frac{1}{3\times 5}+\frac{1}{5\times 7}+\cdots+\frac{1}{(2n-1)(2n+1)}$$

that is valid for every positive integer n.

(b) Use induction to prove your formula from part (a). Be explicit about which version of induction you are using.

(6) Experiment and conjecture a simple closed form for

$$\left(1-\frac{1}{4}\right)\left(1-\frac{1}{9}\right)\left(1-\frac{1}{16}\right)\cdots\left(1-\frac{1}{n^2}\right)$$

that is valid for every positive integer $n\geq 2$. Prove your conjecture.

(7) (a) Let $a_1=5$, $a_2=7$ and $a_n=3a_{n-1}-2a_{n-2}$ for $n\geq 3$. Experiment and conjecture a simple closed form for a_n that is valid for every positive integer n. (Hint: Compare a_n to 2^n.)

(b) Use induction to prove your formula from part (a). Be explicit about which version of induction you are using.

(8) Recall that the Fibonacci numbers f_n are defined by $f_1=1$, $f_2=1$, and $f_n=f_{n-1}+f_{n-2}$ for all $n\geq 3$. Show that every fifth Fibonacci number is divisible by 5. (In fact, something stronger is true: for any prime p, every p^{th} Fibonacci number is divisible by p.)

(9) Prove that for every positive integer n,

$$1(1!)+2(2!)+3(3!)+\cdots+n(n!)=(n+1)!-1. \tag{B.12}$$

(10) Prove that for every $n\in\mathbb{N}$, the number of subsets of a set with n elements in 2^n.

(11) Is the following statement true or false?

For all $n \in \mathbb{N}$, $(1 + 2 + 3 + \cdots + n)^2 = 1^3 + 2^3 + 3^3 + \cdots n^3$

If the statement is true, prove it. If it is false, find a counterexample.

(12) For which positive integers is $n!$ less than n^n? Prove your assertion.

(13) In this exercise, we will compare exponential functions to factorials. Let $a \geq 2$ be a positive integer.

(a) Show that if $a^n < n!$ for some positive integer n, then $a^{n+1} < (n+1)!$.

(b) To show that $a^n < n!$ for all n larger than some fixed integer, it remains to demonstrate that $a^n < n!$ for some positive integer n. This is a challenging problem. It is conjectured that, for $a > 3$, the sequence

$$s(a) = \text{round}\left(ae - \left(\frac{1}{2}\right)\log(2a\pi) - \frac{1}{a}\right)$$

gives the smallest positive integer n so that $a^n < n!$.[‡] (The function *round* means to round to the nearest integer.) Verify this formula for $a = 4$, $a = 5$, and $a = 6$.

(14) **Round Robin Tournaments.** Consider a tournament involving m players in which each player plays every other player just once and there are no ties. A *cycle* in the tournament is a set $\{P_1, P_2, \ldots, P_n\}$ of players so that player P_1 beats player P_2, player P_2 beats player P_3, and so on, and player P_n beats player P_1. Show that if there is a cycle in the tournament, then there is a cycle consisting of exactly three players.

(15) In this investigation, we proved that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

for every positive integer n. Then, in Exercise (2), you were asked to show that

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for every positive integer n. Mathematical induction is a useful tool for verifying such formulas, but how do we actually find the formulas in the first place? In this exercise, we will consider ways to answer this question.

(a) Let's next determine a formula for the sum of cubes. Our starting place is the expansion of $(x-1)^4$. Note that

$$(x-1)^4 = x^4 - 4x^3 + 6x^2 - 4x + 1.$$

Then

$$x^4 - (x-1)^4 = 4x^3 - 6x^2 + 4x - 1.$$

Next, we will calculate each side of the previous equation as x ranges from 1 to n:

$$\begin{array}{rcccccccc}
n^4 - (n-1)^4 & = & 4n^3 & - & 6n^2 & + & 4n & - & 1 \\
(n-1)^4 - (n-2)^4 & = & 4(n-1)^3 & - & 6(n-1)^2 & + & 4(n-1) & - & 1 \\
(n-2)^4 - (n-3)^4 & = & 4(n-2)^3 & - & 6(n-2)^2 & + & 4(n-2) & - & 1 \\
\vdots & & & & \vdots & & & & \\
4^4 - 3^4 & = & 4(4)^3 & - & 6(4)^2 & + & 4(4) & - & 1 \\
3^4 - 2^4 & = & 4(3)^3 & - & 6(3)^2 & + & 4(3) & - & 1 \\
2^4 - 1^4 & = & 4(2)^3 & - & 6(2)^2 & + & 4(2) & - & 1 \\
1^4 - 0^4 & = & 4(1)^3 & - & 6(1)^2 & + & 4(1) & - & 1
\end{array}$$

[‡]By Benoit Cloitre; see sequence A086824 in the On-Line Encyclopedia of Integer Sequences (`https://oeis.org/`).

Now we can add the entries on each side to find a formula for

$$1^3 + 2^3 + \cdots + n^3.$$

Complete this process, and then prove your formula by induction.

(b) Repeat the process from part (a) to find a formula for

$$1^4 + 2^4 + \cdots + n^4.$$

Then prove your formula.

(16) **The Towers of Hanoi.** In an ancient city in India, so the legend goes, monks in a temple have to move a pile of 64 sacred disks from one location to another. The disks are fragile; only one can be carried at a time. A disk may not be placed on top of a smaller, less valuable disk. In addition, there is only one other location in the temple (besides the original and destination locations) sacred enough that a pile of disks can be placed there.

So the monks begin moving disks back and forth, between the original pile, the pile at the new location, and the intermediate location, always keeping the piles in order (largest on the bottom, smallest on the top). The legend is that, before the monks make the final move to complete the pile in the new location, the temple will turn to dust and the world will end.

Generalize this problem to show that if there were n disks to move, it would take a total of $2^n - 1$ moves to complete the transfer from one location to another. Should we be worried about the world coming to an end?

(17) The usual total ordering given by $\leq$ on $\mathbb{Z}$ behaves nicely with respect to addition. Show that there is *no* total ordering of $\mathbb{Z}_n$ that behaves nicely with respect to addition in $\mathbb{Z}_n$. That is, show that there is no total ordering on $\mathbb{Z}_n$ such that, for all $[a]$, $[b]$, $[c] \in \mathbb{Z}_n$, if $[a] \leq [b]$, then $([a] + [c]) \leq ([b] + [c])$. (Hint: If there is such an ordering with $[0] \leq [1]$, use transitivity to show that $[0] \leq [n-1]$, and explain why this leads to a contradiction. Then think about what similar argument needs to be made to complete the proof.)