

CHAPTER 3

Proof Techniques

3.1 A Case for Proof

Towards the end of the first chapter we met Bertrand's Postulate, which states that for all $n \geq 2$ there is a prime between n and $2n$. We verified this claim for values of n from $n = 2$ through $n = 10$. One could easily extend this list by hand to values of n in the hundreds or even thousands, or to much higher values with the aid of a computer. In fact, the further one goes, the more plausible the theorem becomes—for instance, there are no less than 135 primes between 1000 and 2000. The list looks like

1009, 1013, 1019, 1021, . . . , 1987, 1993, 1997, 1999.

At this point most of us would happily agree that Bertrand's Postulate is undoubtedly correct. However, we would also concede that we have not really *proved* that Bertrand's Postulate is true; only *convinced* ourselves that it is. Before we consider what constitutes a mathematical proof, we should reflect for a moment on why one should pursue a proof of Bertrand's Postulate at all.

There are a number of answers to this question. One reason that is often forwarded goes along the lines of "You can never be sure." It is true that there are examples of simple, appealing open sentences that are true for a great many



Bernhard Riemann

values of n , only to succumb to an unexpectedly large counterexample—the next Mathematical Outing reveals one such faulty conjecture. Examples such as this illustrate the importance of backing up assertions with proof. Besides, few would debate that a result must be rigorously established before it may attain the honored status of theorem. But to be honest, promising statements that turn out to be false occur relatively infrequently. And even professional mathematicians are willing to accept and implement unproven results when

Mathematical Outing

★ ★ ★



Make a list of the first twenty-four odd primes: 3, 5, 7, . . . , 89, 97. Now go back through the list and circle all the primes that are one less than a multiple of four (such as 3 or 47) and box all the primes that are one more than a multiple of four (such as 5 or 29). Study the distribution of circles and boxes and make three conjectures based on the questions below.

- How many circled primes are there among all the positive integers?
- How do the number of primes of each type compare up to any point?
- How do the number of primes of each type compare in the long run?

Finally, guess which of your conjectures are in fact true.


there is overwhelming evidence in their favor. Perhaps the best known example is the Riemann Hypothesis, which predicts the nature of the solutions to

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots = 0,$$

where $\zeta(s)$ is the Riemann-zeta function. It is not uncommon for a published theorem to include a sentence along the lines of, “We assume that the Riemann Hypothesis is true.” The mathematical community expectantly awaits a proof; the possibility of a disproof is more or less out of the question.

All of this brings us back to the issue of why we bother to prove statements that we already believe to be correct. The more compelling reason is that we, as mathematicians, are even more interested in understanding why numbers (or geometric diagrams, or other mathematical objects) behave in the way that they do than we are in discovering fascinating relationships in the first place. Coming up with an intriguing question or stumbling upon a nice result is exciting, but represents only the initial stage of an investigation. It is in the quest for an explanation that one begins to truly understand the principles governing fascinating mathematical observations, and it is in the careful writing of a proof that one certifies this understanding to oneself (and others). Individuals who are drawn to math often mention that they are attracted to the potential for absolute certainty; to the satisfaction that an irrefutable proof provides.



 The data suggests that there are infinitely many circled primes, that up to any given point there are at least as many circled primes as boxed primes, and that there are approximately “the same number” of each type. The first and the third conjectures are indeed true, although not particularly easy to prove. The second looks good for a very long time, but ultimately falls through. The smallest counterexample occurs for the prime $n = 26861$, at which point the boxed primes outnumber the circled primes for the first time.

3.2 Mathematical Writing

Mastering the craft of writing a good proof takes both practice and guidance. Just as with learning any new language, there is initially a high potential barrier to mathematical writing. One must become accustomed to certain conventions, learn how to use notation correctly, absorb a new vocabulary, master a set of proof techniques, increase ones level of rigor, and more. Nonetheless, this skill is well within the reach of the willing student.

The backbone of any good proof is a complete, watertight argument. Since the mathematical methods for achieving this depend a great deal on the type of problem under consideration, we will relegate the discussion of what constitutes a rigorous proof in each case to the corresponding section covering that topic. But we can at least comment upon how much detail to include with a proof. The general rule of thumb is to provide enough discussion to completely justify each step, but not so much as to obscure the overall thrust of the argument. In this respect excellent proofs resemble poetry, in that they say everything that is necessary in as few words as possible.

There are several ways to achieve brevity in proofs. For starters, effective use of mathematical notation helps to streamline a discussion. Rather than saying

VERSION 1: Let x be an element of one of the sets A_1 or A_2 or A_3 , except that we don't want to have $x = 0$,

it is preferable to write

VERSION 2: Let $x \in (A_1 \cup A_2 \cup A_3) - \{0\}$.

It is possible to go to an extreme with dense notation, but this is not usually an issue when one first begins to write proofs. Where possible, one should build on previous work rather than reproving known results. It is also common for several cases of an argument to be so similar that it becomes redundant to write out all the steps for each. When this occurs, it is acceptable and even desirable to implement phrasing like "In the same manner it follows that..." or "In a similar fashion we have..." Finally, and most importantly, the strategy one employs in proving a statement can have a profound effect on the length and clarity of the proof. It is worth taking the time to look for a clean, elegant approach to a problem. Beautiful mathematics deserves an equally nice presentation.

Beyond mathematical content, it is important to use good style when writing a proof. Thus one should employ proper grammar, punctuate correctly, and so on. In particular, one should write in complete sentences. But there are a number of issues unique to mathematical writing, that curious blend of regular words, logical expressions, and mathematical notation which you have by now become accustomed to reading but which is still very unfamiliar to write. The list below highlights some points to bear in mind when writing a proof.

1. Structure your proof in the form of one or more paragraphs. It is not necessary to restate the assertion to be proved, although it does make the proof more readable. It makes sense to indicate that the claim has yet to be established, for instance by writing "We will prove that $A \cap B \subseteq A \cup B$,"

rather than by simply stating the assertion “For sets A and B we have $A \cap B \subseteq A \cup B$,” as if the result is already known to be true. Regardless, it is helpful to then lead off with a sentence that summarizes the proof strategy, as in “We will show that if $x \in A \cap B$ then $x \in A \cup B$ also.”

2. Take advantage of the abundance of synonyms for common mathematical terms to add flavor to your writing. For instance, the words establish, show, explain, and demonstrate may all be used in place of ‘prove.’ It is also handy to have alternatives for the word ‘therefore.’ Synonyms include thus, hence, it follows that, so, for this reason, and consequently.
3. The ubiquitous use of the pronoun ‘we’ has probably not escaped your notice. It is conventional to use ‘we’ instead of ‘I,’ presumably on the grounds that reading mathematics is intended to be an active rather than a passive activity. In other words, the reader joins the author as the proof unfolds, at least in principle. This same philosophy dictates that we write ‘one’ instead of ‘you’ when the writer wishes to refer to a third person.
4. From a grammatical point of view, a mathematical expression functions as a noun. It can serve as the subject of a sentence, as in “The equation $x^2 + 2x - 2 = 0$ plays an important role in today’s discussion,” or a direct object, as in “We complete the square to solve $x^2 + 2x - 2 = 0$,” or the object of a preposition, as in “Add 3 to both sides of $x^2 + 2x - 2 = 0$.”
5. Avoid beginning a sentence with a mathematical expression. Therefore it is preferable to write “The equation $x^2 + 2x - 2 = 0$ plays. . .” rather than just “ $x^2 + 2x - 2 = 0$ plays. . .” Other examples include “We have $x \in A \cup B$ because we know $x \in A$,” as opposed to “ $x \in A \cup B$ because. . .,” and saying “We know that n is not prime since n is even and $n \geq 4$,” rather than “ n is not prime. . .” There are a variety of other phrases to facilitate this practice, most of which one picks up by reading mathematics.
6. As much as possible one should avoid awkward line breaks that split mathematical expressions across separate lines. Reading “The equation $x^2 + 2x - 2 = 0$ plays an important role. . .” is unnecessarily difficult because the equation is cut in half. This problem occurs primarily when using software such as L^AT_EX to prepare a proof and can usually be remedied by the judicious insertion of a few filler words or a reordering of the sentence.
7. Mathematical definitions, expressions or equations which are particularly important or lengthy should be displayed by centering them on their own line. This practice circumvents the potential for bad line breaks, draws greater attention to the math, and allows more room for writing out bulky formulas. For these reasons we chose to display the expression

$$\bigcap_{r \in J} B_r = \{x \mid -1 < x \leq 0\}$$

in an earlier section, rather than write $\bigcap_{r \in J} B_r = \{x \mid -1 < x \leq 0\}$ in line with the text.

8. Meaning is clarified by using mathematical terms correctly. For instance, we *solve* the *equation* $x^2 + 2x - 2 = 0$, but we *evaluate* the *expression* $5n + 1$ when $n = 16$. (The difference being that in the former situation there is an $=$ sign, in the latter case there is not.)
9. Finally, a quick word is in order regarding the use of arabic numerals versus words for numbers. In general, one should write out the word for a number when it counts how many of a certain object we have, as in “Three French hens, two turtle doves and a partridge in a pear tree.” However, utilize an arabic numeral when referring to a number as an arithmetic object, such as “Add 3 to both sides of $x^2 + 2x - 2 = 0$.” In some instances either choice is acceptable—we could turn to page five or to p. 31, for example. But numerals are preferred for unwieldy numbers, like “101 Dalmatians.”

We conclude this section by considering how to conclude a proof. Any number of phrases can be used to indicate that the final step has been reached and that the proof is complete. One might write “... as desired,” or “... which was what we wanted,” or simply “This completes the proof.” Traditionally authors will also include a symbol to visually separate the proof from the ensuing discussion. Popular choices include the letters ‘QED’ (from the Latin *quod erat demonstratum*, ‘that which was to be demonstrated’), a filled box ■, or an open box □. But each person has a unique style and should not feel constrained by these options, at least initially. Feel free to use a diamond ♦, a star ★, a circled snowflake ⊗, a boxed plus ⊞, or another symbol of your choosing.



EXERCISES

1. Rewrite the following sentences to address any short-comings in grammar or mathematical style that you notice.
 - a) The sum of 2 3's and 4 5's is twenty-six.
 - b) Let x be a positive real number. x could be ≤ -1 also. $x = 0$ is OK too.
 - c) I recommend using a truth table in order to show that $\neg(P \wedge Q \wedge R) \equiv \neg P \vee \neg Q \vee \neg R$ is a logical equivalence.
 - d) There are 3 kinds of people those who can count or those who cant.
 - e) $A \supseteq B$ can also be written as $B \subseteq A$.
 - f) You should $\sqrt{\quad}$ both sides of $x^2 = 36$ to solve the formula.
 - g) $f(x) = x^2$ and $g(x) = 3x + 4$ means $f(x) = g(x) = x = 4$.
 - h) $A \cup B$ contains more numbers than B as long as B is not a subset of A .
 - i) Did you know that $\sqrt{\frac{6}{1^2} + \frac{6}{2^2} + \frac{6}{3^2} + \frac{6}{4^2} + \dots}$ equals π ?

3.3 Sudoku Interlude

The purpose of this short section is partly to anticipate some of the techniques that will be introduced in subsequent sections, partly to engage in logical thinking, and partly to have fun with a clever puzzle.¹ Your goal is to fill in each square of the 5×5 grid below with one of the digits from 1 to 5 in such a way that each row, each column, and each *pentomino* contains all five digits exactly once. (A pentomino consists of five squares joined along their edges. Five different pentominoes are highlighted in the grid below.) The reader is invited to find the unique answer before reading the partial explanation that comes next.

a	b	c	d	e
f	g	h	i 2	j
k 5	l	m	n	o
p	q	r 3	s	t
u	v 1	w	x	y

We'll do the first few steps together to illustrate the sorts of deductions that one might utilize in order to solve this puzzle. Although not immediately obvious, the square labeled *y* is a promising place to start. Since the pentomino along the right-hand side already contains a 2, we cannot place a 2 in the squares *e*, *j*, *o* nor *t*. But a 2 must appear in the fifth column, so it can only show up in square *y*. We will write $y = 2$ to indicate this fact.

Because a 5 and 1 already appear in the pentomino in the lower left corner, we can only have $w = 2, 3$ or 4. But there is already a 2 in the fifth row and a 3 in the third column, so by process of elimination we must have $w = 4$. Technically

¹The author learned of this sort of miniature Sudoku puzzle from Scott Kim, one of the most creative designers of original puzzles around. Visit www.scottkim.com to enjoy more of his delightful work.

speaking, we are considering five separate cases for square w . Four of them lead to an “illegal” configuration of numbers, so if there is a solution it must involve writing a 4 in square w . Using process of elimination again, we can now easily find that $p = 2$, $u = 3$ and $x = 5$.

The stage is now set to demonstrate yet another strategy for solving Sudoku puzzles (or proving mathematical statements). We will argue that $b \neq 2$ by showing that if we do place a 2 in square b , then we are led to an illegal configuration. So suppose that $b = 2$. Now consider the third column. It must contain a 2, but due to the positions of the four 2’s already placed we can only have $m = 2$. But this results in the middle top pentomino containing two 2’s! Since $b = 2$ leads to trouble, we conclude that $b \neq 2$. We leave the enjoyable task of deducing the contents of the remaining squares to the reader.



EXERCISES

2. Finish solving the Sudoku puzzle that appears in this section.
3. Make a copy of the Sudoku board shown above but do not write any digits into the grid yet. Now find a way to fill in the squares, following the same rules as before, so that squares c , l , i , p and y do not all contain the same digit. (This will ensure that your solution is not equivalent to the previous one.)

WRITING

4. Complete the written solution begun in this section. You may utilize the notation introduced above, and do not need to repeat any steps already presented. You may also assume that your reader is an intelligent human being who is familiar with Sudoku. Your goal is to write as efficient a solution as possible without skipping any steps.
5. The Sudoku puzzle from this section has a unique solution. Explain why at least four squares had to be given as clues in order for the solution to be unique.

FURTHER EXPLORATION

6. Create your own 5×5 pentomino Sudoku puzzle. Convention dictates that your puzzle should have a unique solution. Try to give no more than five clues.


3.4 Indirect Proofs

The majority of the mathematical arguments seen thus far have been **direct proofs**. In this sort of proof each step builds on previous steps or on given facts, in an orderly and logical manner, until the desired conclusion is reached. The techniques used within a direct proof will vary widely from one type of problem to another, but the overall approach is the same: make a sequence of logical deductions starting with the premises, culminating in the result to be proved.

However, at times a direct argument is insufficient or undesirable, particularly when one wishes to prove a negative result; i.e. that something does not occur. To illustrate, consider the following assertion from set theory.

“For arbitrary sets A , B and C , if $A - C \not\subseteq A - B$,
then it follows that $B \not\subseteq C$.” (*)

In this case an attempt at a direct proof becomes overly complicated at best, and flounders at worst. We have a strategy for approaching a statement such as $B \subseteq C$, but how do we deal with $B \not\subseteq C$? More generally, how do we deduce one negative statement from another? In this case the obstacle is not that we are lacking tools for dealing with set theory, but rather that we need a whole new proof technique for handling negative statements.

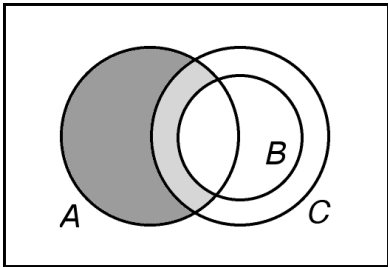
 a) Suppose that $A = \{1, 2, 3, 4, 5, 6\}$ and $C = \{1, 2, 3, 4\}$. Find a set B such that $A - C \not\subseteq A - B$. Is it the case that $B \not\subseteq C$ for your choice of B ?

The key to proving (*) is to utilize **proof by contrapositive**. This approach is motivated and justified by the observation that $P \Rightarrow Q$ is logically equivalent to $\neg Q \Rightarrow \neg P$. (The routine verification of this fact appears as an exercise.)


The implication $\neg Q \Rightarrow \neg P$ is the **contrapositive** of $P \Rightarrow Q$. Since these statements are logically equivalent, to prove that $P \Rightarrow Q$ it suffices to demonstrate that $\neg Q \Rightarrow \neg P$.

Note that if the implication already contains negatives, then it may be clearer to think of the original statement as $\neg P \Rightarrow \neg Q$ and the contrapositive as $Q \Rightarrow P$.

This small logical sleight of hand makes a great deal of difference in our quest to understand (*). That implication has the form $\neg P \Rightarrow \neg Q$, where P is “ $A - C \subseteq A - B$ ” and Q stands for “ $B \subseteq C$.” According to the above discussion, it would be equivalent to prove that $Q \Rightarrow P$; in other words, that $B \subseteq C$ implies $A - C \subseteq A - B$. Now at least we can picture the statement to be proven with a Venn diagram, which is set up so that $B \subseteq C$. The dark gray region represents $A - C$, while the two gray regions together represent $A - B$.



Although this diagram does not constitute a proof, it seems quite plausible now that $A - C \subseteq A - B$. The remainder of the proof is left to the reader.[†]

 b) Formulate the first sentence of a proof that for sets A , B and C , we have $B \subseteq C$ implies $A - C \subseteq A - B$.

To further illustrate how one might phrase a proof by contrapositive, let us examine the relatively simple assertion that if $C \not\subseteq A \cup B$ then $C \not\subseteq A$. We will prove the contrapositive of this statement; i.e. we will show that if $C \subseteq A$ then $C \subseteq A \cup B$. We focus on the conclusion of this if-then statement: we must

Mathematical Outing

★ ★ ★



Irrational numbers can behave in unexpected ways. Suppose that α and β are irrational numbers. Which of the following numbers *must* also be irrational, according to your intuition? As much as possible, give specific counterexamples in the remaining cases; in other words, find irrationals α and β such that the given expression is clearly rational.

$$7\alpha, \quad \beta - 4, \quad \alpha + \beta, \quad \alpha^2, \quad \sqrt{\beta}, \quad \alpha\beta.$$

An intriguing fact, which is far from obvious, is that it is possible for α^β to be a rational number. The clever idea is to take $\alpha = \sqrt{2}^{\sqrt{2}}$ and $\beta = \sqrt{2}$. There are two options to consider. First suppose that α is irrational. What is the value of α^β ? How does this prove the claim? On the other hand, why would it also be fine if α turned out to be rational?

show that $C \subseteq A \cup B$, which is a set inclusion. So take any element $x \in C$; since $C \subseteq A$ we deduce that $x \in A$ also. Since $x \in A$ we know that $x \in A \cup B$ by definition of union. Because $x \in C$ implies $x \in A \cup B$, we conclude that $C \subseteq A \cup B$, as desired.

The second indirect proof technique that we consider is often invoked when dealing with irrational numbers. Recall that a real number r is a rational number if it can be written in the form $r = \frac{m}{n}$ for integers m and n with $n \neq 0$. Thus $\frac{1}{3}$, $-7\frac{2}{5}$, 5 and 0 are all rational numbers. A real number that is not equal to the ratio of two integers is called irrational. In the language of set theory, the irrationals are the set $\mathbb{R} - \mathbb{Q}$. With varying amounts of effort one can prove that the numbers $\sqrt{7}$, π and e^2 are all irrational, among many others.



c) Decide whether or not $\log_7 14$ and $\log_8 16$ are irrational.

Our intuition suggests that if α is an irrational number, then 3α must be also. We employ the following strategy to establish this result.

To prove an implication $P \Rightarrow Q$ using **proof by contradiction**, assume that the result (Q) to be proved is in fact false, then combine this assumption with given information (P) and any other useful true statements to arrive at a deduction which contradicts a known fact.

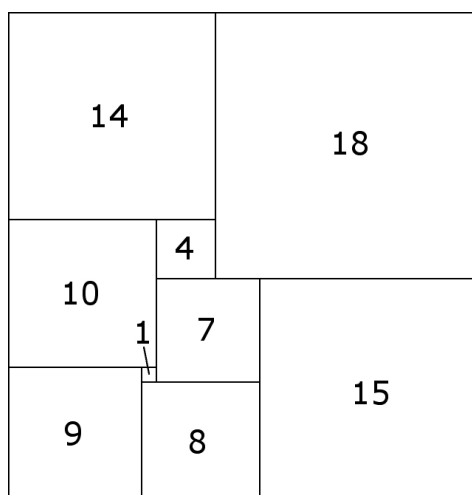
The point is that since the result to be proved can't be false, it must be true. As we shall see, this approach is particularly effective when attempting to prove a negative statement; that is, trying to show that some situation cannot occur. This technique may also be employed to prove a stand-alone statement Q ; just show that $\neg Q$ leads to a deduction that contradicts standard known facts.

To see this technique in action, let us prove that if α is irrational, then 3α is also irrational. (Note that we wish to prove a negative statement—that 3α *cannot* be written as a fraction.) Suppose to the contrary that 3α is in fact a rational. Then we can write $3\alpha = \frac{m}{n}$ for integers m and n . Dividing through by 3 gives $\alpha = \frac{m}{3n}$. (We know to perform this step because we want to work our way back to α algebraically, because we already know something about α .) Since $\alpha = \frac{m}{3n}$ we see that α can be written as a ratio of integers, contradicting the fact that α is irrational. Therefore our assumption that 3α is rational cannot be true, so we conclude that 3α is irrational, as claimed.†



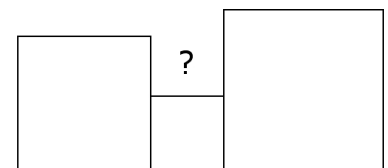
d) It is the case that if β is irrational then $\sqrt{\beta}$ is also irrational. Write the first two sentences of a proof by contradiction of this fact.

Proof by contradiction is a powerful tool, applicable to a wide range of problems. To appreciate its versatility, consider the following curious arrangement of squares discovered in 1925 by a secondary school teacher in Poland named Zbigniew Moron.



Such an arrangement is known as a *perfect square dissection*; it illustrates how to dissect a 32×33 rectangle into nine squares, each of which has a different side length. (It was long thought impossible to obtain a perfect square dissection of a square, until R. Sprague found a way to do so in 1939 using 55 squares.) Our purpose here is to explain why the smallest square of any perfect square dissection must always be situated somewhere in the middle of the arrangement.

Although it is not immediately obvious that we should do so, we employ proof by contradiction. Thus assume to the contrary that the smallest square is *not* located in the middle of the arrangement; that is, it rests against one of the edges. Now consider the squares immediately adjacent to the smallest square on either side. Because they are larger, their sides extend beyond that of the smallest square, as shown in the figure at right.



(The same is true if the smallest square happens to be situated in the corner.)

There must be another square to help fill the space above the smallest square. But now we reach our contradiction: the other squares are all larger, and so it is impossible to fit one into the space indicated by the ‘?’. This contradiction forces us to reject the possibility that the smallest square rests against an edge. Therefore we conclude that the smallest square must appear in the middle of the configuration of squares, as claimed.



- a) One possibility is $B = \{3, 5\}$, since in this case $A - C = \{5, 6\}$ while $A - B = \{1, 2, 4, 6\}$, and clearly the former set is not a subset of the latter set. As expected, $B \not\subseteq C$.
- b) “To prove $A - C \subseteq A - B$ we must show that for any $x \in A - C$ we have $x \in A - B$.”
- c) We calculate $\log_7 14 \approx 1.356207187108$ and $\log_8 16 \approx 1.333333333333$, so $\log_7 14$ appears to be irrational, while $\log_8 16$ seems to equal $\frac{4}{3}$.
- d) “Assume to the contrary that $\sqrt{\beta}$ is rational. Then we may write $\sqrt{\beta} = \frac{m}{n}$ for integers m and n .”
- ☞ The numbers 7α , $\beta - 4$, and $\sqrt{\beta}$ must also be irrational. However, if we choose $\alpha = 3 + \sqrt{2}$ and $\beta = 3 - \sqrt{2}$, then $\alpha + \beta = 6$, which is rational. Similarly, taking $\alpha = \sqrt{7}$ gives $\alpha^2 = 7$, a rational. Finally, letting $\alpha = \pi$ and $\beta = \frac{1}{\pi}$ we find $\alpha\beta = 1$.

We compute $\alpha^\beta = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2$, using standard laws of exponents. Hence α^β is rational, as desired. If α happens to be rational, then we would conclude that $\sqrt{2}^{\sqrt{2}}$ is rational, so either way we discover that it is possible for an irrational raised to an irrational power to be rational.

EXERCISES

7. Validate the technique of proof by contrapositive by showing that $P \Rightarrow Q$ is logically equivalent to $\neg Q \Rightarrow \neg P$.
8. State the contrapositive of each of the following implications. Then decide whether you would prefer to prove the original statement or the contrapositive. (You do *not* actually need to prove these statements.)
- Let m and n be positive integers. Prove that if m^3 is not divisible by n^3 , then m is not divisible by n .
 - Show that for a real number x , if $x > 1$ then $3^x > 3x$.
 - For finite sets A and B , prove that if $A \not\subseteq B$ then $|A| \geq 1$.
 - If all the sides of a triangle have different lengths, then all of its angles have different sizes.
9. How would a proof by contradiction of the following statements begin? Write at least the first sentence. Include more sentences where possible.
- The number $\sqrt{7}$ is irrational.
 - There are infinitely many primes.
 - If five sisters split up 2000 grams of chocolate, then at least one of the sisters receives 400 or more grams of chocolate.
 - Given four non-collinear points in the plane, there exist three points which form an angle measuring 90° or more.

10. For each statement determine which type of proof is most likely to succeed: a direct proof, a proof by contrapositive, or a proof by contradiction.
- Prove that there do not exist $a, b, c \in \mathbb{N}$ such that $a^3 + b^3 = c^3$.
 - For sets A and B , prove that if $A \cup B \neq \emptyset$ then either $A \neq \emptyset$ or $B \neq \emptyset$.
 - For $x, y \in \mathbb{R}$, prove that if $x + y = 7$ and $xy = 10$, then $x^2 + y^2 = 29$.
 - If $2^n - 1$ is not divisible by 7, then n is not a multiple of 3.
 - For sets A, B and C show that $\mathcal{P}(A) \cup \mathcal{P}(B) \cup \mathcal{P}(C) \subseteq \mathcal{P}(A \cup B \cup C)$.
 - If x and y are positive real numbers then $\frac{x}{x+2y} \geq \frac{1}{3}$ or $\frac{y}{y+2x} \geq \frac{1}{3}$.

WRITING

- For sets A and B prove that if $A \times B = \emptyset$ then either $A = \emptyset$ or $B = \emptyset$.
- For sets A, B and C demonstrate that if $A \not\subseteq B \cup C$ then $A - B \not\subseteq C$.
- Let A, B and C be sets such that $A \subseteq B \cap C$. Prove that $\overline{B \cup C} \subseteq \bar{A}$.
- Explain why stating that $B \not\subseteq C$ is equivalent to saying that there exists an element x such that $x \in B$ but $x \notin C$. Use this idea to find a direct proof of (*).
- Let x be a real number. Prove that if $x^3 + 5x = 40$ then $x < 3$. (Do not use a calculator to solve for x ; rather, find a “pencil-and-paper” proof.)
- Prove that for real numbers x and y , if $x \neq y$ then $\frac{x}{2x-1} \neq \frac{y}{2y-1}$.
- Prove that if $x, y \in \mathbb{R}$ are positive then $\frac{x}{x+2y} \geq \frac{1}{3}$ or $\frac{y}{y+2x} \geq \frac{1}{3}$.
- Let β be an irrational number. Use proof by contradiction to prove that $\beta - 4$ is also irrational.
- Let β be an irrational number. Employ proof by contrapositive to prove that $\sqrt{\beta}$ is also irrational.
- Prove that there is no positive rational number that is smaller than all other positive rational numbers.
- Let A, B and C be finite nonempty sets such that $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(C)$. Prove that either $A = C$ or $B = C$.

FURTHER EXPLORATION

- Now that we have alluded to the fact that there exists a perfect square dissection of a square, it is natural to wonder whether or not there exists a perfect cube dissection of a cube. In other words, is it possible to begin with an $m \times m \times m$ cube, for some $m \in \mathbb{N}$, and dissect it into a finite collection of smaller cubes whose side lengths are distinct positive integers? Surprisingly, the answer is no! The proof relies on the ideas presented in this section. Once you understand the argument, adapt it to decide whether or not there exist perfect cube dissections of $l \times m \times n$ rectangular boxes.

3.5 Biconditional, Vacuous and Trivial Proofs

In this section we consider three more types of proof. The first is quite important, while the next two do not crop up very often. We begin with proofs of biconditional statements, written as $P \iff Q$ in logical notation. Recall that these statements may be phrased as “ P if and only if Q ” or “ P is necessary and sufficient for Q ” or “ P is equivalent to Q .” Earlier we established the logical equivalence of $P \iff Q$ and $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$, which gives us the following proof strategy.

To prove that two statements P and Q are equivalent, one must prove that each statement implies the other. Thus to prove a result of the form “ P if and only if Q ,” one should show that $P \Rightarrow Q$ and that $Q \Rightarrow P$, utilizing whichever proof techniques are most applicable in each case.

C_{RE}C_K^{EPT} a) Suppose that P , Q and R are statements such that $P \iff Q$ and $Q \iff R$. What can be said about statements P and R ?

To illustrate the structure of a biconditional proof we will show that for sets A and B we have $A \cup B = B$ if and only if $A \subseteq B$.

Step one: We first show that $A \cup B = B$ implies $A \subseteq B$. We need to prove a set inclusion (namely, that $A \subseteq B$), so our strategy will be to prove that if $x \in A$ then $x \in B$. So suppose that $x \in A$. Then clearly $x \in A \cup B$ by definition of union. Since $A \cup B = B$, it follows that $x \in B$, which was what we wanted.

Step two: We prove the converse, which states that $A \subseteq B$ implies $A \cup B = B$. This time we must prove a set equality (namely, that $A \cup B = B$), so we must argue that if $x \in A \cup B$ then $x \in B$ and vice-versa. So suppose that $x \in A \cup B$; then either $x \in A$ or $x \in B$. In the former case, we deduce that $x \in B$ since $A \subseteq B$. Hence $x \in B$ in either case, as desired. It remains to show that if $x \in B$ then $x \in A \cup B$, but this is clear by definition of union. Hence $A \cup B = B$ as claimed, which completes the entire proof.[†]

Since the main challenge in constructing this argument is keeping track of where we are in the proof, we also present the overall flow of the proof in outline form in Figure 3.1, to help clarify its logical structure.

Biconditional statements provide the appropriate language when we wish to characterize a certain class of mathematical objects.

A property is said to **characterize** a certain class of objects if the set of objects possessing the property is exactly the specified class of objects. To prove a characterization one must show that an object has the property if and only if it is a member of the designated class of objects.

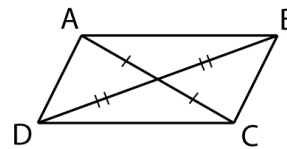
- | | |
|--|---|
| I. $A \cup B = B \Rightarrow A \subseteq B$
A. Proof that $A \subseteq B$
B. Suppose $x \in A$
C. Deduce $x \in A \cup B$
D. Use $A \cup B = B$
E. Conclude $x \in B$ | II. $A \subseteq B \Rightarrow A \cup B = B$
A. Proof that $A \cup B = B$
B. If $x \in A \cup B$ then $x \in B$ <ol style="list-style-type: none"> 1. Suppose $x \in A \cup B$ 2. Case one: $x \in A$ <ol style="list-style-type: none"> a. Use $A \subseteq B$ b. Deduce $x \in B$ 3. Case two: $x \in B$ 4. Either way $x \in B$ C. If $x \in B$ then $x \in A \cup B$ <ol style="list-style-type: none"> 1. Clear by defn of union |
|--|---|

Figure 3.1: Proof that $A \cup B = B \iff A \subseteq B$

For instance, the class of objects might be a certain set of numbers, such as primes, or a particular set of geometric figures, such as parallelograms. Although the concept of characterization might seem to be abstract, it is actually a very familiar idea. Thus taxonomists characterize birds as the set of animals having feathers. To arrive at this characterization, a taxonomist mentally reviews the collection of all birds and searches for a property or feature which every bird possesses but which no other animal shares. The property of having feathers is a suitable choice, since an animal has feathers if and only if it is a bird.

CONCEPT b) Give two different reasons why the property of being able to fly is not a valid means of characterizing animals that are birds.

Most students have also encountered the concept of characterization in their high school geometry course. A standard exercise involves showing that the class of quadrilaterals known as parallelograms may be characterized by the condition that each diagonal bisects the other. To prove that this condition does in fact characterize parallelograms one must show that if $ABCD$ is a parallelogram then diagonals \overline{AC} and \overline{BD} bisect one another, and conversely that if diagonals \overline{AC} and \overline{BD} bisect one another then $ABCD$ is a parallelogram.



CONCEPT c) What class of quadrilaterals is characterized by the property that the diagonals bisect one another and are also perpendicular?

In the same manner, Wilson's Theorem provides a characterization of primes. We have seen (although not proved) that an integer $n \geq 2$ is a prime if and only if $(n-1)! + 1$ is a multiple of n . Hence primes are characterized by the property that n divides evenly into $(n-1)! + 1$. (By the way, this is not an especially practical characterization of primes. There are far more efficient means of testing whether a number such as 2011 is prime than to compute $2010! + 1$.) To prove

Wilson's Theorem it turns out to be more convenient to prove that if n is prime then $(n - 1)! + 1$ is a multiple of n , while if n is not prime then $(n - 1)! + 1$ is not a multiple of n . This suggests the following alternate strategy to proving biconditional statements, whose validity we will confirm in the exercises.

To prove that the biconditional statement $P \iff Q$ holds, it suffices to prove both $P \Rightarrow Q$ and $\neg P \Rightarrow \neg Q$.

We will now dramatically change gears by considering two very different types of proofs. To illustrate them, consider the somewhat fanciful claims

- 1) *If pigs can fly then I can run a six-minute mile.*
- 2) *If I'm on time for class then the pope is Catholic.*

QUICK d) To review, what is the only way an implication can fail to be true? In light of this, which of the above statements are true, and why?

One means of ascertaining that a statement of the form "For all n we have $P \Rightarrow Q$ " is true would be to make a list of the truth values of P and Q for each value of n and then to search for an instance in which P is true but Q is false. Such a list is shown at right for the statement "For all positive integers n , if n is a power of 2 then $8n - 7$ is a perfect square." (So P represents " n is a power of 2" and Q stands for " $8n - 7$ is a perfect square.") It becomes apparent when we reach $n = 8$ that this statement is not true for all n .

n	P	Q	$P \Rightarrow Q$
1	T	T	T
2	T	T	T
3	F	F	T
4	T	T	T
5	F	F	T
6	F	F	T
7	F	T	T
8	T	F	F

However, suppose that in the process of investigating an implication $P \Rightarrow Q$ we were to discover that statement P is always false. Then clearly we would never encounter an instance in which P was true but Q was false.

If the premise P of an implication $P \Rightarrow Q$ is always false then we say that the implication is vacuously true, and by showing that P is always false we provide a **vacuous proof** of the statement.

The word 'vacuous' literally means 'void' or 'empty.' Once we have determined that P is always false there is nothing left to prove; the conclusion Q is irrelevant. For this reason the first statement above is vacuously true.

We encountered a vacuously true statement when we first began studying subsets. At that point there was some debate over whether or not the empty set should count as a subset of a given set A . According to the definition, to prove that $\emptyset \subseteq A$ we must show that if $x \in \emptyset$, then $x \in A$. But the premise of this implication is always false (there are no elements in the empty set), therefore the statement is vacuously true.

Let's consider the seemingly remarkable claim that for $n \in \mathbb{N}$ it is the case that $3n + 4$ is a perfect square whenever $n^2 + 5n + 6$ is a prime. This fact seems astonishing, until we begin to try a few values of n and discover that $n^2 + 5n + 6$ seems to always factor. This observation affords the following explanation. We will prove that the statement is vacuously true by showing that $n^2 + 5n + 6$ is never prime. Observe that this expression factors as $(n + 2)(n + 3)$. Since each factor is 3 or more for $n \in \mathbb{N}$, their product cannot be a prime. Hence the statement is vacuously true.[†]

There is another situation in which an implication $P \Rightarrow Q$ is automatically true; namely, when statement Q is always true. Again, it is clear that we could never encounter an instance in which P was true but Q was false. For this reason the second statement above is true, since the pope is definitely Catholic.

If the conclusion Q of an implication $P \Rightarrow Q$ is always true then we say that the implication is trivially true, and by showing that Q is always true we provide a **trivial proof** of the statement.

This sort of situation is even more rare than a vacuously true statement. The name also has the potential to misleading: when someone refers to a proof as 'trivial' they are usually referring to how easy it was to find rather than to its logical structure. We mention trivial proofs here for sake of completeness. A template for writing out a trivial proof may be found in the reference section at the end of this chapter.



- a) It follows that $P \iff R$; statements P and R are equivalent.
- b) There are birds that don't fly (such as ostriches or penguins) and non-birds that do fly (such as bats or bumblebees).
- c) A quadrilateral possesses this property if and only if it is a rhombus.
- d) An implication $P \Rightarrow Q$ fails only if the premise P is true while the conclusion Q is false. Hence both statements are true, since the premise of the first statement is false while the conclusion of the second statement is true.

EXERCISES

23. An alternate strategy for proving a biconditional statement $P \iff Q$ is to prove that $P \Rightarrow Q$ and that $\neg P \Rightarrow \neg Q$. Explain why this approach is valid.
24. Determine whether each biconditional statement given below is true or false. Briefly justify your answers.
- a) An integer a is divisible by 12 if and only if a^3 is divisible by 12.
 - b) Let $\triangle ABC$ be a triangle. We have $\overline{AB} \cong \overline{AC}$ exactly when $\angle B \cong \angle C$.
 - c) For nonempty sets A and B , having $A \subseteq B$ is a necessary and sufficient condition to ensure that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
 - d) Let x and y be nonzero real numbers. Then $x < y$ iff $1/x > 1/y$.

25. Give a succinct description of those integers m which are characterized by the property that $m^2 - 1$ is a multiple of 8.
26. Which numbers are characterized by the property that their decimal expansions either terminate or eventually begin repeating?
27. Write down the two implications which must be proven in order to demonstrate that linear functions $f(x)$ are characterized by the condition that they satisfy $f(x - a) + f(x + a) = 2f(x)$ for all $a, x \in \mathbb{R}$.
28. Determine a property that characterizes the set of points in the plane situated on one of the lines $y = x$ or $y = -x$.
29. Each of the following statements is either vacuously true or trivially true. Determine which category each assertion belongs to.
- For all $n \in \mathbb{N}$, if $n^2 + n + 1$ is a prime then $n^2 + 2n + 1$ is a perfect square.
 - For all $n \in \mathbb{N}$, if $4n + 5$ is even then $6n + 7$ is a perfect cube.
 - Let x be a real number. If $2^x = 0$ then $3^x = 0$ also.
 - For real numbers x and y , if $|x + 1| > |y - 2|$ then $|x + y + 1| > -2$.
 - If B is the midpoint of \overline{AC} and C is the midpoint of \overline{AB} then $BC = 4$.
 - If points A, B and C satisfy $(AB)(BC) = (AC)^2$ then $AB + BC \geq AC$.
 - For finite sets A and B , if $|A| < |B|$, then it follows that $A \subseteq A \cup B$.
 - For finite sets A and B , if $|A \times B| < |B \times A|$ then $|\mathcal{P}(A)| < |\mathcal{P}(B)|$.

WRITING

30. Let A and B be sets. Outline the logical structure of a proof that $A \subseteq B$ if and only if $A \cap B = A$, as done earlier in this section.
31. Let A and B be sets. Prove that $A \subseteq B$ if and only if $A \cap B = A$. (It will help to complete the previous exercise first.)
32. Given circles \mathcal{C}_1 and \mathcal{C}_2 , prove that the circumference of \mathcal{C}_1 is twice the circumference of \mathcal{C}_2 exactly when the area of \mathcal{C}_1 is quadruple the area of \mathcal{C}_2 .
33. Let x and y be nonzero real numbers. Prove that $\frac{2}{x} + \frac{3}{y} = 1$ is equivalent to $(x - 2)(y - 3) = 6$.
34. Show that a positive integer a is even if and only if a^2 ends with one of the digits 0, 4 or 6.
35. Prove that for a given nonempty set B , subsets of B are characterized by the condition that they are disjoint from \overline{B} .
36. Demonstrate that the real numbers in the interval $[-1, 1]$ are characterized by the condition that their squares are at least as close to 0 as they are.
37. Write a short, complete proof of each statement below.
- For all $n \in \mathbb{N}$, if $n^2 + n + 1$ is a prime then $n^2 + 2n + 1$ is a perfect square.
 - For real numbers x and y , if $|x + 1| > |y - 2|$ then $|x + y + 1| > -2$.
 - If B is the midpoint of \overline{AC} and C is the midpoint of \overline{AB} then $BC = 4$.
 - For finite sets A and B , if $|A \times B| < |B \times A|$ then $|\mathcal{P}(A)| < |\mathcal{P}(B)|$.

3.6 Conjecture and Disproof

Searching for and discovering interesting results is one of the most exciting aspects of studying mathematics. The exact process by which this occurs can be difficult to pin down, though. Noticing patterns or unexpected connections is something of an art, as is the closely related skill of asking productive questions. At the risk of over-simplifying, we could say that successful mathematicians combine diligent exploration of new ideas with well-developed intuition in order to formulate appealing new results.

To gain some sense of how this process unfolds, let us focus our attention on a sequence of numbers that ought to contain some interesting mathematics: the perfect squares. The square numbers from 0^2 up to 20^2 are listed below.

0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121,
144, 169, 196, 225, 256, 289, 324, 361, 400

Using what we already know about square numbers as a launching pad, we now search for patterns and ask ourselves questions, motivated by the conviction that there are nice relationships among the square numbers waiting to be found.



a) What facts concerning square numbers are you familiar with? What patterns do you notice among the numbers in the above list? What questions could you ask about the perfect squares?

For instance, we might already be aware that it is possible to add two squares and obtain a third square, as in $64 + 225 = 289$. Thus we might ask ourselves whether the sum of two squares can be equal to the sum of *two* other squares.

Of the many possible directions that this discussion could take us, we choose to pursue the idea of doubling squares. Experimentation suggests that multiplying a positive square by 2 never yields another square. This conjecture turns out to be true; however, in some cases one can come exceedingly close! For example we find that $2(25) = 50 = 49 + 1$ and, even more impressively, that $2(144) = 288 = 289 - 1$. The first five instances in which twice a square differs from another perfect square by only one are listed below. We organize our findings in a table to aid in our search for conjectures.

$2m^2 = n^2 \pm 1$	m	n
$2(1) = 1 + 1$	1	1
$2(4) = 9 - 1$	2	3
$2(25) = 49 + 1$	5	7
$2(144) = 289 - 1$	12	17
$2(81) = 1681 + 1$	29	41

At this point several nice patterns begin to emerge. For instance, the sum of the m and n values in any particular row gives the m value for the next row.

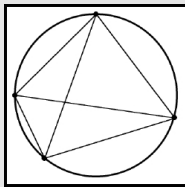


b) Make at least three other conjectures regarding the numbers appearing above. Use the patterns you notice to predict the next two rows of the table, then confirm that they do in fact work.

Mathematical Outing

★ ★ ★

The investigation described here illustrates a classic example of the process of making and testing a conjecture. To experience it for yourself, conduct the following experiment. Draw a circle, then plot n irregularly spaced points around its circumference. Next connect every pair of points with a line segment. For a given value of n , what is the largest number of regions created within the circle? For instance, using $n = 4$ points we can create eight regions, as illustrated at left.



- a) Determine the maximum number of regions created by $n = 2, 3, 4$ and 5 points.
- b) Make a conjecture based on your findings and predict the number of regions for $n = 6$ or $n = 7$.
- c) Confirm or refute your conjecture by actually counting the regions for $n = 6$ and $n = 7$.

Observe that what has turned into an interesting investigation began with a fertile topic (perfect squares), germinated since we asked a good question (what happens if we double squares), and bore fruit in part due to a well-organized table. These conditions often accompany the discovery of nice results.

Intriguing, accessible conjectures usually attract enough attention that they are proven within a relatively short length of time. Occasionally such conjectures persist for many years before sufficiently powerful techniques or an exceptionally ingenious approach finally permits a proof. The most famous example concerns a generalization of our observation above that it is possible for two squares to sum to a third square. In algebraic terms, we have observed that there exist positive integers a , b and c such that $a^2 + b^2 = c^2$. One might ask whether the same is possible for higher powers—can we have $a^3 + b^3 = c^3$ or $a^4 + b^4 = c^4$, for example? In 1637 Fermat conjectured that there are no solutions involving higher powers and managed to prove that this is the case for fourth powers. Over a century later Euler supplied a proof for perfect cubes. However, it was not until the 1990's that Wiles and other mathematicians were finally able to establish “Fermat’s Last Theorem” in full generality.



Pierre de Fermat

Once one has formulated and tested a promising conjecture, the next step is usually to find a proof. However, it is not unusual for conjectures to turn out to be false, in which case one supplies a disproof instead.

To **disprove** a claim, write the negation of the conjectured statement and then prove that this negation is true.

Typically the (false) statement involves a universal quantifier; in other words, it asserts that “For all \dots , if we have \dots then \dots .” In this case the negation reads “There exists \dots for which we have \dots but not \dots .” Therefore a disproof amounts to finding a **counterexample**: a particular mathematical object satisfying the premise but not the conclusion of the implication.

We have already seen several promising conjectures succumb to counterexamples. We present one more in order to carefully apply the above principles. Consider the claim that “For all $n \in \mathbb{N}$, if n is prime then $6n + 1$ is also prime.” To disprove this assertion we first state the negation, “There exists an $n \in \mathbb{N}$ such that n is prime but $6n + 1$ is not prime.” Thus to find a counterexample we check each prime value for n in turn to see whether or not $6n + 1$ is prime. With a bit of patience we find that the smallest counterexample is $n = 19$, since $6n + 1 = 115$ is not prime.[†]



c) Describe what conditions a counterexample must satisfy in order to disprove the claim that “Given any four points in the plane, there exists a circle through three of the points containing the fourth point in its interior.”


By the way, it would be inappropriate to begin a disproof with the sentence, “We will show that this proof is false.” The proof should be sound; it’s the *claim* that is false. We also mention that the best response to a conjecture that doesn’t pan out would be to modify the conjecture and continue exploring, rather than to shelve the idea. There is hardly ever such a thing as a mathematical dead end. As we have seen, finding a counterexample often amounts to proving that there exists some number (or formula, or diagram) satisfying certain conditions. This task is an important enough mathematical activity that we will devote an entire section to it, coming up next.



a) Common answers might include the fact that subtracting each square from the next gives the sequence of odd numbers, or the fact that squares may only end in the digits 0, 1, 4, 5, 6 or 9. Questions about squares are virtually limitless. We might ask how many square numbers are also Fibonacci numbers, or if there is a perfect square involving only the digits 3 and 4, or whether there is a function which crosses the x -axis precisely at the square numbers, to mention but a few possibilities.

b) For starters, it appears that the $+1$ ’s and -1 ’s alternate down the first column. Furthermore, the sum of two consecutive m values seems to always give the adjacent n value. Finally, the sum of an m value and twice the next m value gives another n value. (The same pattern holds for n values as well.) The next two rows of the table are $m = 70$, $n = 99$ and $m = 169$, $n = 239$.

c) We must find four points in the plane such that the circle through any three of them does not contain the fourth in its interior. This can be accomplished by taking the points at the vertices of a square, for example.

 a) The number of regions formed by $n = 2, 3, 4$ and 5 points is $2, 4, 8$ and 16 regions, respectively. At this point it seems abundantly clear that the answers are given by powers of 2. More precisely, n points seem to yield 2^{n-1} regions, so there will be 32 regions for $n = 6$ points and 64 regions for $n = 7$ points. To our dismay, a carefully diagram reveals that this is not the case! In fact we can obtain at most 31 regions when $n = 6$ and at most 57 regions when $n = 7$.

EXERCISES

38. Find three pairs of positive integers m and n such that $3m^2 = n^2 \pm 1$. Thus tripling a square can produce a number that is very close to another perfect square. (The first three values of m are less than 20.)

39. Based on the values found in the previous question, make three conjectures regarding pairs of numbers (m, n) for which $3m^2 = n^2 \pm 1$, and predict the next two pairs of integers that satisfy this equation.

40. Choose any three positive real numbers x , y and z and compute the values of $x + y + z$ and $3\sqrt[3]{xyz}$. Repeat this process for three other triples. How do the two values compare in each case? Make a conjecture based on your results.

41. One of the most famous open conjectures is known as the $3x + 1$ problem. Beginning with any positive integer, divide by 2 if it is even or triple and add 1 if it is odd. Repeatedly apply this rule to obtain a sequence of numbers. The conjecture states that regardless of the initial number the sequence will eventually reach the number 1. For instance, starting with 17 gives

$$17 \rightarrow 52 \rightarrow 26 \rightarrow 13 \rightarrow 40 \rightarrow 20 \rightarrow 10 \rightarrow 5 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1.$$

Confirm the $3x + 1$ problem for all values of n from 10 to 20. (Observe that the above sequence already takes care of 10, 13, 16, 17 and 20.)

42. Which positive integers can be written as the difference of two squares? Make a list of all such numbers from 1 to 20. For instance we have

$$1 = 1^2 - 0^2, \quad 3 = 2^2 - 1^2, \quad 4 = 2^2 - 0^2, \quad \text{and} \quad 5 = 3^2 - 2^2.$$

Make a conjecture about which positive integers (such as 2) are left off this list.

43. Draw a triangle ABC and plot the midpoints L , M and N of sides \overline{BC} , \overline{AC} and \overline{AB} . Next draw segments \overline{AL} and \overline{BM} , crossing at point G . How does length AG compare to GL ? What about BG and GM ? Now draw segment \overline{CN} . What seems to occur? Make two conjectures based on your observations.

WRITING

44. Disprove the assertion that “For positive integers m , if $m + 1$ and $5m + 1$ are both perfect squares, then $m = 3$.”

45. Show that the following assertion is false: for every quadrilateral $ABCD$, if $m\angle A > m\angle B$ then $BD > AC$.

46. Find a disproof of the statement, “For real numbers x and y , if $x^2 + 3x = y^2 + 3y$ then it follows that $x = y$.”

47. A classmate claims that there exists a perfect square with two or more digits that immediately follows a prime. Show that he is mistaken.

48. Disprove the claim that there exist four points in the plane all of which are the same distance from one another.

FURTHER EXPLORATION

49. Goldbach's conjecture states that every even number from 4 onwards can be written as the sum of two primes. Goldbach's conjecture is almost certainly true. However, it is possible to concoct similar sorts of conjectures that seem quite plausible but which fail for a surprisingly large counterexample. For instance, consider the claim that every odd number from 3 onwards can be written as the sum of a prime and twice a square.² Thus $3 = 3 + 2(0^2)$, $15 = 13 + 2(1^2)$ and $35 = 17 + 2(3^2)$. Write a computer program to disprove this claim. (The smallest counterexample lies between 1000 and 10000.) Then create similar conjectures of your own.

3.7 Existence

As we have just seen, to show that an assertion is false one usually hunts for a counterexample consisting of numbers, a diagram, or some other mathematical object satisfying certain conditions. Thus to disprove the claim "For all positive real numbers x and y it is the case that $\frac{1}{2}(x + y) > \sqrt{xy}$," we need only find a single pair of real numbers x and y for which $\frac{1}{2}(x + y) \leq \sqrt{xy}$.



a) Find positive real numbers for which $\frac{1}{2}(x + y) \leq \sqrt{xy}$.

Being naturally curious folk, mathematicians are also prone to search for objects with certain properties for the sheer pleasure of discovering whether or not they exist. For example, do there exist integers a , b and c such that $a + b + c = 3$ and $a^3 + b^3 + c^3 = 3$ other than the obvious solution $a = b = c = 1$? Or given two rectangles in the plane, does there necessarily exist a line that simultaneously cuts the areas of both of them in half? The answers to both these questions turns out to be yes, as you will discover in the exercises.

On the surface a question about existence seems more approachable than a proof. After all, one need only come up with a single object satisfying certain properties, as opposed to proving that an assertion is true for all values of the variables. While it is true that a solution to an existence question has a very different flavor than the proofs we have seen in previous sections, they are not necessarily easier to find. For example, Euler made a conjecture centuries ago that implies that it is not possible for the sum of three perfect fourth powers to equal another perfect fourth power. It was not until 1986 (well into the computer age) that Noam Elkies found a counterexample to this claim:

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$


The smallest possible counterexample still involves five and six digit numbers.

There are two standard methods for settling an existence question. The most obvious way is to exhibit a certain number or other mathematical object and show that it has the desired properties. This was the technique employed


²Our thanks to Tom Kilkelly for sharing this entertaining conjecture.

by Elkies, although there was certainly a good deal of insight and deeper mathematics going on behind the scenes. However, it is also possible to argue that something exists even though a precise description is never provided.

To provide a **constructive solution** to an existence problem, carefully describe the sought after mathematical object and demonstrate that it has the desired properties. It is also acceptable to give an **existence proof** by arguing that an object must exist without ever explicitly describing it.

 b) It is undeniably the fact that there exist two individuals in Los Angeles having the same number of hairs on their head. Which type of proof of this fact is more appropriate, a constructive solution or an existence proof?

To illustrate both approaches, let us prove that there exists a number with the property that adding 287 to this number gives a total of 1000. The most obvious solution would be to point out that 713 has the desired property, since $713 + 287 = 1000$. Believe it or not, one can also convincingly argue for the existence of such a number without actually identifying it! Consider the sums $1 + 287$, $2 + 287$, $3 + 287$, and so on. The results, of course, are 288, 289, 290 and on up. Eventually we must hit 1000, even if it is not clear at precisely what point we arrive. Hence the number we are seeking does indeed exist.

 c) Give both an existence proof and a constructive solution showing that there exists a real number satisfying $4x + 4^x = 14$.

Depending on the problem at hand, there are a variety of strategies for obtaining a constructive solution. When searching for a positive integer with certain properties it is often possible to perform a computer search which tests each positive integer in turn for the desired property. This was the approach taken by the author to find the counterexample $n = 26861$ mentioned earlier in this chapter. In geometry problems, a constructive solution generally consists of a step-by-step sequence of geometric operations that yields the sought after point, line, or circle. An existence problem involving numbers might have as its solution an algebraic expression.

To understand what is meant by the latter remark, suppose that we wish to prove that there exists a rational number between any two other rational numbers. Letting $r < s$ be the two given fractions, we claim that the number $\frac{1}{2}(r + s)$ satisfies the statement of the problem. To begin, this quantity is clearly also a rational number: if we write $r = a/b$ and $s = c/d$ for integers a, b, c, d then $\frac{1}{2}(r + s) = (ad + bc)/2bd$, a ratio of integers. And since $\frac{1}{2}(r + s)$ is the average of r and s it lies midway between them. More precisely, we have $r < \frac{1}{2}(r + s)$ since this inequality is equivalent to $\frac{1}{2}r < \frac{1}{2}s$, which reduces to $r < s$, a given fact. In the same way we find that $\frac{1}{2}(r + s) < s$ as well, establishing that $\frac{1}{2}(r + s)$ does lie between r and s .

Solutions to harder existence questions might require a bit of ingenuity to construct. For instance, consider the unexpectedly long list of integers 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, all of which are *not* prime. (We have to wait until 524, 525, . . . , 540 to reach a longer string of non-primes.) It is natural to wonder whether there are arbitrarily long strings of consecutive composite numbers; say, one thousand composites in a row. The answer is yes, and the construction of such a sequence is both simple and delightfully clever. Consider the numbers

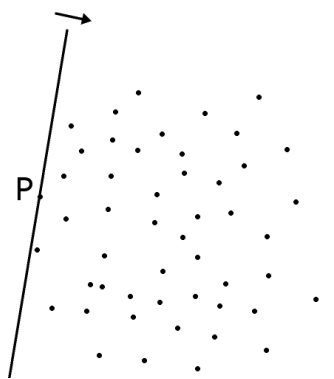
$$1001! + 2, 1001! + 3, 1001! + 4, \dots, 1001! + 1001,$$

where $1001! = (1001)(1000)(999) \cdots (2)(1)$ as usual. The first number is clearly even, the second number is divisible by 3, and so on, all the way to the final number, which is a multiple of 1001. Voilà, one thousand consecutive numbers, none of which are prime.[†]



d) Do there exist one thousand consecutive numbers, none of which are perfect squares?

To illustrate an existence proof in another context, we shall convince ourselves that given 101 points in the plane, no three of which lie on the same line, there exists a line through one of the points that neatly divides the remaining points in half, with fifty points on either side. To see why this must always be the case, imagine drawing a line through one of the points (call it P) on the “edge” of the set, so that all the remaining points are to one side of the line. Now steadily rotate the line 180° clockwise, keeping track along the way of how many points the line has crossed. As the line rotates it must cross the other points one at a time, since no three points lie on a single line. Furthermore, after 180° the line will have passed all 100 points. Hence at some point it will have just passed 50 points; this position of the line solves the problem.



- a) Choosing $x = y = 5$ results in $\frac{1}{2}(x + y) = 5 = \sqrt{xy}$. This is the best we can do; it is not possible to obtain $\frac{1}{2}(x + y) < \sqrt{xy}$.
- b) An existence proof probably springs to mind first. Since every human has less than 200,000 hairs on their head and there are well more than this number of individuals in Los Angeles, it is not possible for everyone to have a different number of hairs on their head. However, a constructive solution is also feasible; just find two completely bald men.
- c) Clearly the quantity $4x + 4^x$ grows steadily as x increases. At $x = 1$ we obtain 8, while $x = 2$ gives 24, so at some point in between we must have $4x + 4^x = 14$. (Technically, we are invoking the Intermediate Value Theorem.) However, it is also possible to exhibit a solution. Taking $x = 1.5$ we find that $4(1.5) + 4^{1.5} = 6 + 8 = 14$.
- d) There are indeed one thousand consecutive nonsquare numbers. For instance, take the 2000 numbers between 1000^2 and 1001^2 .

EXERCISES

50. Show that there are numbers x and y such that $x + y = \pi$ and $x - y = \sqrt{2}$.
51. Disprove the claim that for all positive real numbers x and y it is the case that $x + 2y < \sqrt{8xy}$.
52. Prove that there exist three consecutive integers, one of which is divisible by 3^2 , one of which is divisible by 5^2 , and one of which is divisible by 7^2 .
53. Demonstrate that there exist three integers a , b and c other than the obvious choice $a = b = c = 1$ such that $a + b + c = 3$ and $a^3 + b^3 + c^3 = 3$. (HINT: the solution only involves one-digit numbers, one of which is negative.)
54. Explain why there is a real number x satisfying $8^x + 9x = 10$. Give both an existence proof and a constructive solution.
55. Given a circle in the plane, what must be true of a line that cuts the circle's area in half? Based on your answer, explain how to construct a line that simultaneously cuts the area of two different circles each in half.
56. Use the ideas developed in the previous exercise to show that given any two rectangles in the plane, there exists a line that simultaneously cuts the area of each rectangle in half. In what situations will such a line not be unique?

WRITING

57. Demonstrate that there exist two positive integers which differ by ten whose sum is one million. Give both an existence proof and a constructive solution.
58. Ten children at a party collect a total of 74 pieces of candy from a piñata. Prove that there exists some child who received at least eight pieces of candy.
59. Show that there exist 1000 consecutive positive integers, each having two or more digits, such that the first number is not even, the next is not a multiple of 3, the third is not a multiple of 4, and so on.
60. Prove that there exists a real number r with $0 < r < 1$ having the property that every possible finite string of digits appears at some place within its decimal expansion. (For example, the string '314159' should occur if we look far enough out in the decimal expansion for r .)
61. Given 102 points in the plane, no three of which lie on the same line, prove that there exists a line passing through two of the points which divides the remaining points in half, with fifty points on each side of the line.
62. Show that for every $n \in \mathbb{N}$, a unique number in the list $n + 1, n + 2, \dots, 2n$ is a power of 2. (Recall that the powers of 2 are 1, 2, 4, 8, 16, ...)
63. We are given one-hundred points in the plane so that no three are situated along the same line. Fifty of the points are colored red, while the remaining fifty are colored blue. Prove that there exists a line dividing each set of points in half, with twenty-five red points and twenty-five blue points on either side.

3.8 Reference

We give a summary of the various types of proofs that have been presented, along with a sample paragraph to illustrate how to phrase such a proof.

* *Direct Proof* This is the most common type of argument. Each step in such an argument follows directly from previous steps or from the hypotheses until the desired conclusion is reached. Along the way the proof may appeal to definitions or other relevant known facts to move from one step to the next.

* *Proof by Contrapositive* This technique is most advantageous when both the conclusion and hypothesis claim that something does not occur; i.e., are negative statements. The first task is to carefully state the contrapositive of the implication $P \Rightarrow Q$, which is written as “If not Q then not P .” Then prove the contrapositive statement instead, using whatever method works best. *Note that it is not valid to write the contrapositive as “not P and not Q .”*

Begin the proof by saying “We prove the contrapositive, which states that [write contrapositive]. This is true because [proof of contrapositive].”

* *Proof by Contradiction* This technique is also effective when attempting to prove that something does *not* occur, such as as an implication of the form $P \Rightarrow Q$ where Q is a negative statement. The idea is to assume the negative of the conclusion and then argue to a contradiction. In other words, show that assuming both P and $\neg Q$ leads to an impossible or absurd situation.

Begin the proof by saying “Suppose to the contrary that [state negative of conclusion here]. Then [main argument leading to absurd statement], which is a contradiction. Hence our assumption is false, which means that [original conclusion] must be true.”

* *Biconditional Proofs* Here one wishes to prove a statement of the form “Under certain conditions, $P \iff Q$.” This is usually signified by the phrase “ P if and only if Q ” or “ P is necessary and sufficient for Q .” To prove a biconditional, show that each statement implies the other, using any helpful proof techniques. Present these arguments in separate paragraphs.

The first paragraph might begin “We first prove that $P \Rightarrow Q$. [Proof of implication]” An abbreviated form looks like “ (\implies) [Proof of implication]”

The second paragraph could read “Conversely, $Q \Rightarrow P$ because [proof of implication]” which can be shortened to “ (\impliedby) [Proof of implication]”

Alternatively, one can prove a biconditional $P \iff Q$ by showing that $P \Rightarrow Q$ and also $\neg P \Rightarrow \neg Q$. One would again prove each implication separately.

* *Characterization* To show that a property characterizes a certain class of objects, show that an object satisfies has the property if and only if it is a member of the designated class of objects.

One could write “To begin, suppose that [x is an object in the class of objects]. [Proof that x has the property.] On the other hand, suppose that [x has the property]. [Proof that x is a member of the class of objects.] This shows that [property] characterizes [class of objects].”

* *Vacuous Proof* If while digesting the statement to be proven it comes to light that the premise is never true, one can employ a vacuous proof. (This typically only occurs when dealing with empty sets, special cases of general results, or artificially concocted textbook problems.)

A proof would look like “We will show that the statement is vacuously true. Observe that [premise] is never true because [include reasons here]. This completes the proof.”

* *Trivial Proof* If while digesting the statement to be proven it comes to light that the conclusion is always true irregardless of the premise, one can employ a trivial proof. (In actual practice this sort of proof rarely comes up.)

A proof would look like “We will show that the statement is trivially true. Observe that [conclusion] is always true because [include reasons here]. This completes the proof.”

* *Disproving an Assertion* A disproof would involve stating and then proving the negation of the assertion. Mathematical claims usually take the form of a universally quantified implication; i.e. a statement of the form “For all values of the variables, $P \Rightarrow Q$.” In this situation to supply a disproof it suffices to find a single counterexample: find an instance in which P is true but Q is false. This is essentially an instance of an existence argument.

* *Existence* The most common way to demonstrate that a mathematical object having certain properties does indeed exist is to construct an object and then show that it satisfies the stated conditions. At times it may also be possible to convincingly argue for the existence of the object without actually giving an explicit example of such an object.

SAMPLE PROOFS

The following proofs provide concise explanations for results discussed within this chapter. They are meant to serve as an illustration for how proofs of similar statements could be phrased. The boldface numbers indicate the section containing each result; the location of that result within the section is marked by a dagger (†).



3.4 Prove for any sets A , B and C that if $A - C \subseteq A - B$ then $B \subseteq C$.

Proof We will prove the contrapositive of the given implication, which states that if $B \subseteq C$ then $A - C \subseteq A - B$. To conclude that $A - C \subseteq A - B$ we must show that if $x \in A - C$ then $x \in A - B$. So suppose that $x \in A - C$. This means that $x \in A$ but $x \notin C$. However, we are given that $B \subseteq C$. Because $x \notin C$, we may deduce that $x \notin B$ either. We now have $x \in A$ but $x \notin B$, which means that $x \in A - B$, as desired. Finally, since the contrapositive is logically equivalent to the original statement, we are done.



3.4 Demonstrate that if α is irrational then 3α is also irrational.

Proof Suppose to the contrary that 3α is rational. This would mean that we could write $3\alpha = \frac{m}{n}$ for integers m and n . Dividing by 3 yields $\alpha = \frac{m}{3n}$. But this contradicts the fact that we are told that α is irrational, since we could write α as the ratio $\frac{m}{3n}$ of the integers m and $3n$. Since supposing that 3α is rational leads to a contradiction, we conclude that 3α is irrational, as claimed.



3.5 Prove that for sets A and B we have $A \cup B = B$ if and only if $A \subseteq B$.

Proof We first explain why $A \cup B = B$ implies $A \subseteq B$. To deduce that $A \subseteq B$ we will show that if $x \in A$ then $x \in B$. So suppose that $x \in A$. Then clearly $x \in A \cup B$ by definition of union. Since $A \cup B = B$, it follows that $x \in B$.

We next prove the converse, which states that $A \subseteq B$ implies $A \cup B = B$. To conclude that $A \cup B = B$ we will argue that if $x \in A \cup B$ then $x \in B$ and vice-versa. So suppose that $x \in A \cup B$; then either $x \in A$ or $x \in B$. In the former case, we deduce that $x \in B$ since $A \subseteq B$. Hence $x \in B$ in either case, as desired. It remains to show that if $x \in B$ then $x \in A \cup B$, but this is clear by definition of union. Hence $A \cup B = B$ as claimed, which completes the proof.



3.5 Show that $3n + 4$ is a perfect square whenever $n^2 + 5n + 6$ is a prime.

Proof Observe that the expression $n^2 + 5n + 6$ factors as $(n + 2)(n + 3)$. Since each factor is 3 or more for $n \in \mathbb{N}$, their product cannot be a prime. Hence the premise is always false, meaning that the statement is vacuously true.



3.6 Prove or disprove the claim that for all $n \in \mathbb{N}$, if n is prime then $6n + 1$ is also prime.

Disproof We will disprove the statement by showing that its negative is true; namely, that there exists an $n \in \mathbb{N}$ such that n is prime but $6n + 1$ is not prime. One such value of n is $n = 19$, since 19 is prime but $6(19) + 1 = 115$ is not. This counterexample provides the disproof.



3.7 Demonstrate that there exist one thousand consecutive positive integers, none of which are prime.

Proof We claim that the numbers

$$1001! + 2, 1001! + 3, 1001! + 4, \dots, 1001! + 1001$$

satisfy the statement of the problem. Here $1001! = (1001)(1000)(999) \cdots (2)(1)$ as usual. Clearly $1001!$ is a multiple of 2, hence so is $1001! + 2$. Since this number is divisible by 2 it is not prime. In the same manner, for each k in the range $2 \leq k \leq 1001$ we find that $1001!$ is a multiple of k , hence so is $1001! + k$, which means that this number is not prime. In summary, our list contains one thousand consecutive integers, none of which are prime, so we are done.