

# The Math Less Traveled

(working title)

Chapter 1: Problem-Solving and Proof  
draft version 1  
June 24, 2007

This chapter deals with the general topics of problem-solving and proof. The idea is to give the reader an overview of these topics along with plenty of examples and interesting problems—this is the sort of topic that must be learned by practice, rather than just reading a book or memorizing some rules. Unfortunately, coming up with good problems is difficult, and I still have less than half the number of problems I'd like for this chapter. If you know of or invent any problems that could work well, I would love to include them along with proper attribution.

All content copyright © Brent Yorgey 2007, except where otherwise noted. Permission is granted to make digital or paper copies of this work for personal or educational use. Explicit permission must be obtained in writing for any other use, including copies made or distributed for profit or commercial advantage.



# Chapter 1

## Problem-Solving and Proof

In high school, math tends to work like this:

- (a) You are taught Theorem/Concept/Technique/Thing X.
- (b) You are given way too many homework problems,<sup>1</sup> all of which obviously have to involve Thing X since that's what section of the book you are in.
- (c) If you are a scrupulously honest student, go to (e).
- (d) You copy all the answers from the back of the book, and don't learn much. Go to (f).
- (e) You do all the homework problems yourself, and don't learn much anyway.
- (f) You cram for a test on Thing X.
- (g) You promptly forget everything you ever knew about Thing X after the test.

---

<sup>1</sup>And on the days when you don't get very many homework problems, they all turn out to be those sneaky problems with 17 lettered subparts which might as well be 17 separate problems anyway.

In the real world, on the other hand, math usually works like this:

- (a) Stumble upon/invent a problem.
- (b) Come up with a solution.
- (c) Convince yourself and others that your solution is correct.<sup>2</sup>

Obviously, these are not at all the same. In the real world, no one tells you that you should use Thing X to solve your problem; you have to figure out a way to solve it yourself. And once you do, you can't look up your answer in the 'back of the universe' like you can look up answers in the back of a textbook; instead, you have to demonstrate your solution to other people (and to yourself!) by means of a proof, so they can confirm or refute it.

Does real math sound harder than high school math? That's because it is! . . . But that's not the end of the story.

Suppose I told you to find my aunt Betsy<sup>3</sup> and provided you with detailed directions to her house along with several pictures so you could be sure when you found her. You would probably have little trouble locating Betsy in this scenario: just follow the map, peek in the window, compare to the photos, done! You wouldn't even have to talk to anyone. But suppose I didn't give you a map or pictures, or any other sort of information.<sup>4</sup> You could still find her, but this time your trip would probably require you to do some detective work, meet people, explore, take a few detours and wrong turns along the way, and even (gasp!) talk to Aunt Betsy herself—since otherwise you couldn't be sure it was really her. Of course, one of these scenarios sounds easy, and the other sounds like a fun, challenging, worthwhile opportunity to meet people and appreciate some beautiful scenery along the way. I'll let you decide which.

---

<sup>2</sup>Accomplishing (c) by publishing a totally sweet paper in a prestigious journal of mathematics is optional.

<sup>3</sup>No, I don't *actually* have an aunt named Betsy. Sorry to disappoint any would-be stalkers.

<sup>4</sup>Perhaps I died (under mysterious circumstances, of course) and left nothing but a suitably mysterious note scrawled on a sticky note: "Find Aunt Bets . . ." followed by unintelligible (and mysterious) scribbling.

Dare I suggest that the high school follow-the-map-and-peek-in-the-window method might not be the best way to learn and appreciate mathematics?

## 1.1 Problem-solving techniques

Even if you've bought into the idea that it's worthwhile (and more realistic) to try solving problems without being told how beforehand, it can still be quite intimidating when you're not used to it. It's like someone who grew up in a city suddenly being dropped in the middle of a forest without a map. *Where am I? What do I do now?!*

Of course, there isn't a nice, neat list of steps that one can follow when faced with an unfamiliar problem; that's precisely the point. However, here are a few guidelines and suggestions to help you. Some of them might seem overly simplistic, but these basic approaches go a long way!

### Play!

First, and most importantly, this new approach to problem solving requires a different attitude. Without a clear path to the solution in mind when you start working on a problem (a luxury one rarely gets in reality), just . . . play! Don't expect to figure out the solution immediately. To start, just play around, explore, and gather data; often your explorations may lead you to a key idea that wasn't initially obvious.

*** Some (additional) problems should go here. ***
--

### Try a few examples

This seems obvious, right? Well, it's easy to forget, especially when tackling a problem expressed using fairly abstract language. Trying some examples is often the best way to gain a more intuitive understanding of what the problem involves.

## Look for patterns

If you collect enough examples, sometimes a pattern will jump out at you. Once you notice a pattern, you can try to figure out why that particular pattern occurs.

**Problem 1.1** (\*\*). “I’m thinking of a positive integer  $n$ . When you divide  $n^2$  by 7, you get a remainder of 3.” Am I telling the truth? What could  $n$  be?

**Problem 1.2** (\*\*). Write out all the numbers from 1 to 72 (or as high as you want) in a table with 6 numbers in each row, like this:

1	2	3	4	5	6
7	8	9	10	11	12
13	...				

Circle all the prime numbers. What do you notice? Can you figure out why this happens? ★

## Draw a picture

Drawing a picture doesn’t help with every single problem you might encounter, but it can often give you fresh insight or help you better organize the information you have. Drawing a picture isn’t just for geometry problems!

\*\*\* Some (additional) problems should go here. \*\*\*

## Solve a simpler problem

Sometimes it helps to make a simpler version of a problem you are trying to solve, and solve that instead. With less to worry about you might see the solution more clearly, and the experience and insights gained often translate into a better understanding of the more difficult problem.

## Sleep on it

This is a very important ‘meta-technique’ that is often overlooked. You don’t have to literally go to sleep, but the idea is the same: if you’re really stuck on a problem and aren’t making any progress, put it aside and come back to it later. Work on a different problem, read a book, take a nap, write a short story about a boy and his gorilla, do anything other than work on the problem. A fresh perspective does wonders! It often happens that upon returning to a problem after taking a break, you’ll see something you missed before. Doggedly continuing to work on a problem when stuck can actually be counterproductive; you may just be getting your mind stuck deeper and deeper in a particular rut.

## Use a computer

Modern computers are an invaluable tool for exploring mathematics. Unless you live in a cave, you probably have access to a small machine which can perform billions of mathematical calculations every second—which, when you stop to think about it, is really rather remarkable.<sup>5</sup> Such things didn’t exist at all as recently as seventy years ago,<sup>6</sup> and even twenty years ago, most people didn’t have access to one. If the mathematicians of previous centuries could have known about the power and ubiquity of modern computers, they probably would have drooled with envy.<sup>7</sup>

Still, a machine that can do billions of mathematical calculations a second doesn’t help much if you don’t know how to make it do the calculations you want.<sup>8</sup> Here are some tools you can use to help you harness the power of computers for your mathematical exploration.

---

<sup>5</sup>Actually, it’s still rather remarkable even when you’re not stopping to think about it.

<sup>6</sup>This is sort of a lie. Things called computers did exist seventy years ago—but back then the term referred to *people* who were paid to perform mathematical calculations!

<sup>7</sup>It’s probably a good thing they didn’t, since the drool might have gotten all over their manuscripts and we would have had to figure out all that math over again.

<sup>8</sup>It’s like having a huge gorilla who doesn’t listen to you. For extra credit, write a short story (involving math, of course) about a boy with a huge gorilla who doesn’t listen to him.

- (<http://www.wolfram.com/>) is one of my favorites; it's incredibly powerful, elegant, and not too hard to learn how to use. Unfortunately, it's quite expensive; there is, however, a very generous discount for students. If you're a student who is interested in using a computer to play around with math, and you're willing to pay \$150 or so for some top-notch, user-friendly mathematical software, in my opinion is the way to go. (<http://www.maplesoft.com/>) is a competing commercial product with similar features and similar student pricing; although I've never used it myself, I've heard good things about it and you'd probably enjoy it too.
- (<http://maxima.sourceforge.net/>) is a free, open-source software package with features similar to and . It's not as easy to learn as , but it's quite powerful, and the fact that it's free is, of course, a big plus.
- J (<http://jsoftware.com/>) is a free programming language which can be useful for playing around with math. Don't let the "programming language" bit scare you. It essentially acts like a (very advanced) calculator: you type in expressions and it prints out their values. It's fairly easy to get started with, although there's a steep learning curve for some of its more advanced features.
- If you already have some programming experience, there are also more conventional programming languages you can use: Ruby, Python, and Scheme are all well-suited to mathematical experimentation (whereas languages like C, C++, Java, or Visual Basic are not).
- Calculators are computers, too! Although not as fast or powerful as other computing platforms, they have the distinct advantages that (a) they are portable, and (b) you probably already have one and know how to use it.<sup>9</sup>

---

<sup>9</sup>By the way, if you want to learn how to write computer programs, do yourself a favor and *don't* learn on a graphing calculator. It's like learning to drive in a pedal-powered Wienermobile. Try starting with something like Scheme instead (<http://www.htdp.org/2003-09-26/>).

- There are also tons of websites with useful mathematical information. For example:
  - MathWorld (<http://mathworld.wolfram.com>) is essentially a free online mathematical encyclopedia. Regardless of the particular mathematical topic you're interested in, it's a safe bet that MathWorld has way more information on it than you could ever want to know!
  - Although not a website about math in particular, Wikipedia (<http://en.wikipedia.org>) has quite an extensive collection of articles on various mathematical topics; although not as comprehensive as MathWorld, it is often easier to understand and not as terse.
  - If you have a list of integers which you suspect follow a pattern, but you don't know what the pattern is, you can search for it in the Online Encyclopedia of Integer Sequences (<http://www.research.att.com/~njas/sequences/>)—you're likely to find some useful information.
  - There are lots of other useful mathematical websites as well; you can find links to many at <http://www.mathlesstraveled.com>.

**Problem 1.3** (★). What is the 29th prime number? ★

**Problem 1.4** (★★). What is the sum of the first 500 prime numbers?

**Problem 1.5** (★★). Is 18956767008469 prime? How about 4378147351?

**Problem 1.6** (★). What is the primorial of 19? ★

## Practice!

All these techniques are great, but techniques will never be a substitute for good old-fashioned practice. The more problems you solve, the better you'll get at it. Don't believe me? Try it!

**Problem 1.7** (\*\*). If you were to multiply together all the integers from 1 to 100, how many zeros would be at the end of the resulting product?

★

\*\*\* Some (additional) problems should go here. \*\*\*

## 1.2 Proofs and problem-solving

Proofs and problem-solving go together like peanut butter and jelly.<sup>10</sup> Sometimes a proof is simply a description of the logical process used to reach a solution; sometimes a proof is needed to validate a solution reached by a somewhat non-logical process. Problem-solving is about *what* and *how*; proofs are about *why*. Understanding a problem well enough to solve it is the first step; understanding it well enough to prove that your solution is correct (and *why* it is correct) is the next. Problem-solving is exploring a mysterious pyramid to discover its secrets; proof is the triumphant conclusion as you avoid the poison traps and evil mummies by swinging to safety on a vine while carrying the solid gold infinity symbol you found in the pyramid's inner sanctum.<sup>11</sup>

This is all well and good, but what exactly do we mean by *proof*?

## 1.3 What is proof?

The idea of *proof* is central to modern mathematics. Indeed, much of the most elegant and beautiful mathematics is to be found in proofs—which is why it's a real shame that so many people are turned off by the style of proof they met in geometry class.<sup>12</sup> You probably know the kind of proof I'm talking about:

---

<sup>10</sup>Or, um, cheese and crackers if you're allergic to peanuts. If you're allergic to peanuts *and* dairy products, you'll have to come up with your own metaphor.

<sup>11</sup>Wow, you're amazing.

<sup>12</sup>I mean no disrespect to the beautiful subject of geometry, and of course I realize that geometric proofs, and this style of proof in particular, have deep historical roots going all the way back to Euclid in the third century BC. But when most of the high school

Statement	Reason
$\overline{EA} \cong \overline{CO}$	Given
$\triangle EAR \cong \triangle COW$	Corollary to Theorem 10.4.6.2.1.19a, Part VII
$m\angle QRZ < m\angle PRX \cdot GR$	Transitivity of Equalitive Commutation
$\sqrt{19\pi} + 63^\circ \sim \odot P$	Duh

This sort of thing is a proof all right, but concluding that all proofs are boring and tedious after only seeing proofs like this would be like concluding that all food is boring and tedious after only eating bran sticks.<sup>13</sup> If you're like many students I've met, you probably cringed at the title of this chapter. But I hope to convince you not only that proofs can be interesting, but that *you* can do them—since there's nothing quite like an exquisitely elegant proof, or the feeling of accomplishment upon proving something new for yourself.

At root, a proof is nothing more than some sort of argument which logically demonstrates the truth of a particular statement.<sup>14</sup> A proof does not need to be written in two columns. In fact, some proofs do not need to be written using words at all.

Figure 1.1 and Figure 1.2 show two particularly beautiful examples of “proofs without words.” You might have to stare at each one a bit before you “get it,” but the effort is well worth it. Anyone who is not moved even a tiny bit by the elegance and beauty of these proofs has something seriously wrong with their sense of wonder!

**Problem 1.8** (★★). Stare at these two proofs until you “get it.” ★

As another example of a particularly beautiful proof, here is Euclid's proof that there is no largest prime number (IX.20 of *The Elements*; see Eu-

---

students I've met shudder at the mention of the word *proof*, it makes me wonder about the wisdom of introducing proofs to middle school students in this way.

<sup>13</sup>Now with 2450% USRDA of bran!

<sup>14</sup>But it's nothing less, either!

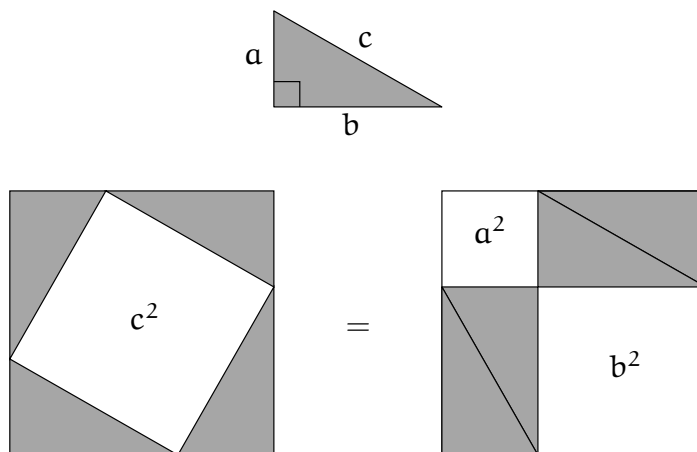


Figure 1.1: Proof of the Pythagorean Theorem:  $a^2 + b^2 = c^2$



Figure 1.2: Proof that the sum of the first  $n$  odd numbers is  $n^2$

clid (1956)).<sup>15</sup> In other words, there are infinitely many primes, since you can keep finding larger and larger ones as long as you want. (Recall that a prime number is a number which is only divisible by itself and 1, such as 2, 3, 5, 7, 11, . . . ; we'll learn much more about prime numbers in Chapter ??.) There are many essentially equivalent ways to present Euler's proof, but I think this is one of the clearest. The basic idea is to show that given any prime number, we can always find another one which is larger.

Let's start by supposing that  $P$  is some prime number. Let's write down a list of all the prime numbers, in order, that are less than or equal to  $P$ :

$$2, 3, 5, \dots, P$$

Now create a new number called  $M$ , by multiplying together all the primes in the list, and adding 1:

$$M = (2 \cdot 3 \cdot 5 \cdots P) + 1.$$

(We could also write this as  $M = P\# + 1$ , as the astute reader will recall from Problem 1.6.) Clearly,  $M$  is bigger than  $P$ . There are two possibilities to consider: first, if  $M$  is prime, then we have succeeded in finding another prime bigger than  $P$ . Now let's consider the other case: if  $M$  is not prime, it must be divisible by some number which *is* prime. Let's call this number  $p_M$ . (Of course, there may be many prime numbers which evenly divide  $M$ ; we'll just look at one of them.) Notice that if you divide  $M$  by 2, you get a remainder of 1, because of the way we defined  $M$ : it is one more than a multiple of 2. By the same reasoning, you get a remainder of 1 when you divide  $M$  by 3, and by 5, and in fact by all the prime numbers up to (and including)  $P$ . In other words, none of the prime numbers in our list evenly divide  $M$ , so  $p_M$  cannot be one of the primes in our list. But our list contains all the prime numbers which are less than or equal to  $P$ , and the inescapable conclusion is that  $p_M$  is a prime number greater than  $P$ . In either case, we have shown that no matter what prime  $P$  you start

---

<sup>15</sup>By the way, *Euclid* is pronounced "YOO-klid". Don't get it confused with *Euler*, which is pronounced "OIL-er". The first is Greek (like *eukaryote* and *eulogy*), while the second is German (like *Deutschland* and *Freud*). Get used to it.

with, you can always find a bigger one—so there must be infinitely many of them, since they can never stop!

**Problem 1.9** (★). As a concrete example (which is a great way of getting a better grasp of a proof like this, regardless of whether you're trying to prove something yourself, or trying to understand a proof someone else has written), try starting with the prime number  $P = 17$ . According to the proof above, what is  $M$  in this case?

**Problem 1.10** (★). According to the proof, we know that the value of  $M$  you found in Problem 1.9 must be either \_\_\_\_\_ or \_\_\_\_\_. Fill in the blanks, and decide which it is.

## 1.4 First lessons in proof-fu

Proving things is an art. The best proofs combine elegance, beauty, and surprise; they are finely crafted works of art which inspire wonder and appreciation. Paul Erdős,<sup>16</sup> one of the twentieth century's most brilliant and prolific mathematicians, was fond of referring to 'The Book,' an imagined collection of the best, most elegant and perfect proofs of all possible mathematical theorems<sup>17</sup> (Hoffman 1998). Erdős's highest praise was reserved for beautiful proofs which were "straight from the book."

Of course, proofs can also inspire the question "How on earth did they think of *that*?!" Being asked to prove something for the first time can be just as bewildering as being asked to solve a problem without being told what techniques to use: there are no steps to follow!

Part of the answer is that experience is the best teacher; the more example proofs you read, and the more proving you do yourself, the better you will become. But if that were all there is to say, this would be the end of the chapter. Fortunately, it isn't.<sup>18</sup> The other part of the answer is that many proofs fall into certain categories; being familiar with common proof types,

<sup>16</sup>Pronounced (approximately) 'air-dish'.

<sup>17</sup>Sort of like the 'Back of the Universe.'

<sup>18</sup>As your inimitable powers of induction indubitably inclined you to infer.

and the sorts of statements they are useful for proving, goes a long way towards getting that black belt in proof-fu.

Where to begin? Let's start with what we know: we'll look at each type of statement we studied in Chapter ??, and discuss some of the proof techniques relevant to each.

## Implications

Suppose you are asked to prove the implication  $A \implies B$ . The simplest way is with a *direct proof*: begin by assuming that  $A$  is true, and see if this leads you to logically conclude that  $B$  is true as well. You might also consider proving the contrapositive,  $\neg B \implies \neg A$ ; that is, assume that  $B$  is false, and show this logically leads to the conclusion that  $A$  is also false. Since we know that an implication and its contrapositive are logically equivalent (Problem ??), you can choose whichever approach is easier. Here's an example:

*Theorem.* If  $k$  is an even integer,  $k^2$  is also even.

*Proof.* Suppose  $k$  is an even integer. That means  $k$  is divisible by 2, so we can write  $k = 2r$  for some other integer  $r$ . Then  $k^2 = (2r)^2 = 4r^2 = 2 \cdot (2r^2)$ , which is even, since it is twice an integer.  $\square$

Perhaps all this *assuming* and *supposing* bothers you. "How can we *assume* that  $A$  is true if we haven't proved it?" you may wonder. Keep in mind that we're not trying to prove  $A$ , we're trying to prove  $A \implies B$ ; there's a big difference!  $A \implies B$  says nothing at all about what happens when  $A$  is false, so it's perfectly fine for our proof to ignore this possibility. In the example above, by saying "suppose  $k$  is an even number," we're not saying that  $k$  is *always* an even number.<sup>19</sup> We're only saying that in this particular proof, we're ignoring the cases when it isn't.

By the way, did you notice that little empty square ( $\square$ ) at the end of the proof? Sometimes you'll also see a filled square ( $\blacksquare$ ) or the letters QED,

---

<sup>19</sup>Which would be sort of ridiculous.

which stand for the Latin phrase *quod erat demonstrandum* (that which was to be demonstrated). It's customary to place one of these symbols at the end of a proof, to indicate that the proof is complete.<sup>20</sup>

**Problem 1.11** (★). What about the cases when  $k$  is not even? Can we conclude from the above theorem and proof that whenever  $k$  is not even,  $k^2$  is not even either? ★

**Problem 1.12** (★). Can we conclude from the above theorem that whenever  $k^2$  is not even, neither is  $k$ ?

To *disprove* an implication is easy: since  $A \implies B$  means that  $B$  should be true whenever  $A$  is true, all you need to do is find a counterexample (that is, a particular case where  $A$  is true but  $B$  is false). For example, if someone states “if it is cloudy, then it is raining,” all you need to do to prove them wrong (once you have finished laughing at them) is wait until a particular time when it *is* cloudy but *not* raining.<sup>21</sup>

**Problem 1.13** (★). Prove or disprove: if  $n$  is an odd number greater than 1,  $n$  is prime.

**Problem 1.14** (★★). Prove or disprove: if  $\triangle ABC$  is a triangle where the measures of angles  $A$  and  $B$  sum to  $170^\circ$ ,  $\triangle ABC$  is obtuse.

**Problem 1.15** (★★). Prove or disprove: if  $k$  is an odd integer, so is  $k^2$ . ★

**Problem 1.16** (★★). Let  $k$  be an integer. Prove or disprove: if  $k$  is not divisible by 3, then  $k^2 - 1$  is. ★

## Logical equivalence

If you are asked to prove the logical equivalence  $A \iff B$ , you really have to prove two things: that  $A$  implies  $B$ , and that  $B$  implies  $A$ . Often you will see  $(\implies)$  and  $(\impliedby)$  at the beginning of the two sections of an ‘if and only if’ proof, so the reader knows which part of the proof to expect

<sup>20</sup>Think of it as the mathematical equivalent of writing “BOOYAH!” at the end of your proof.

<sup>21</sup>Laughing at them some more is optional.

when. Sometimes you will also see the word *Conversely* . . . to mark the transition from the first half to the second.

\*\*\* Some (additional) problems should go here. \*\*\*

## AND

Proving a statement of the form  $A \wedge B$  is very simple (assuming that you know how to prove  $A$  and  $B$  separately). In fact, if you know how to prove  $A$  and  $B$  separately, then . . . well . . . you're done!

## OR

If you want to prove a statement of the form  $A \vee B$ , here's what to do: assume  $A$  to be false, and show this implies the truth of  $B$ . In other words, you should prove  $\neg A \implies B$ . Why does this work? If  $A$  is true,  $A \vee B$  will be true no matter what  $B$  is, so we show that  $B$  must be true whenever  $A$  is not (since otherwise  $A \vee B$  would be false). To look at it from a more formal perspective, using the tools you learned in Chapter ??, it should not be too hard to show that

$$(A \vee B) \iff (\neg A \implies B).$$

Of course, since  $A \vee B$  is the same as  $B \vee A$ , this works equally well the other way around: you can prove  $A \vee B$  by showing that  $\neg B \implies A$ . Just choose whichever seems easier.

**Problem 1.17** (\*\*). Show that  $(A \vee B) \iff (\neg A \implies B)$ .

## The existential quantifier

What if you want to prove that something *exists*? There are two basic approaches: give an example, or show that it doesn't make sense for it *not* to exist.

The first approach, generally known as a *proof by construction*, is quite simple: if you're asked to prove that a certain thing exists, just give an example, and show that your example fits the bill.

**Problem 1.18** (★). Prove that there exists a prime number which can be written as a difference of two squares.

**Problem 1.19** (★). Prove that there exist integers  $n$  and  $k$  for which  $213 = n^k - k$ .

A *proof by contradiction* is the second approach to proving a statement with an existential quantifier; it's actually quite common, and is useful for more than just existence proofs. The basic idea is simple: begin by assuming the *negation* of the statement you want to prove, and show this leads to a contradiction. In other words, instead of directly showing that  $S$  is true, a proof by contradiction shows that  $S$  can't be false—which amounts to the same thing from a logical point of view, but sometimes the more roundabout method is easier.

★★★ Some (additional) problems should go here. ★★★

## The universal quantifier

One way to prove a statement with a universal quantifier is with a proof by contradiction. If you are trying to show that all  $X$ 's have property  $Y$ , you can show that if there *were* an  $X$  that did *not* have property  $Y$ , it would lead to a contradiction.

The other primary method of proving a universal quantifier is with a *proof by induction*. The basic idea of an induction proof is like knocking over a chain of dominoes—once you set up the dominoes, all you have to do is knock over the first one, and they all go! Of course, in real life it takes a lot of time and effort to set up each individual domino, but in a proof by induction we get to set up all the 'dominoes' at once.

Here's how it works. Suppose we have a statement  $P(n)$  involving the number  $n$ , and we're trying to prove the universally quantified statement " $P(n)$ , for all integers  $n \geq 1$ ." First, we show that for any integer  $k \geq 1$ ,

$P(k) \implies P(k+1)$ —that is, *if*  $P(k)$  is true (called the *inductive hypothesis*, sometimes abbreviated as ind. hyp., i. h., or IH in proofs), then  $P(k+1)$  must be true also. This is called the *inductive step*, and it's like setting up the dominoes; we're showing that the  $k$ th domino will always knock over the  $(k+1)$ st domino. The second step is to show that  $P(1)$  is actually true. This is called the *base case*, and it's like knocking over the first domino—which causes all the dominoes to fall! If  $P(1)$  is true, then  $P(2)$  must be true; but that means  $P(3)$  must be true also, which in turn means  $P(4)$  must be true, which means . . . and so on, forever!

Two comments before we proceed to a real example: first of all, the order in which we perform these two steps doesn't really matter (unlike with real-life dominoes). In practice, it's often easier to do the base case first, and it's also a good check: if the base case doesn't work, there's no use wasting your energy trying to prove the (usually more difficult) inductive step! Secondly, the base case isn't always to prove  $P(1)$ ; the base case should use whatever value of  $n$  is the 'first' that needs to be proven. That is, if you are asked to prove  $Q(n)$  for all  $n \geq 17$ , your base case should be  $Q(17)$ .

Let's do a real example to show how this works. We'll prove our favorite example statement,<sup>22</sup> that the sum of the first  $n$  odd numbers is always  $n^2$ . If we let  $P(n)$  represent the statement " $1 + 3 + 5 + \dots + (2n - 1) = n^2$ " (it shouldn't be too hard to convince yourself that the  $n$ th odd number is, in fact,  $2n - 1$ ), then we wish to prove the statement " $P(n)$ , for all integers  $n \geq 1$ ." This is a prime candidate for a proof by induction. Let's do the proof together.

First, the base case. Since we're asked to prove  $P(n)$  whenever  $n \geq 1$ , we need to check  $P(1)$ .

**Problem 1.20** ( $\star$ ). What statement does  $P(1)$  represent? Is it true?

Now for the inductive step. We want to show that if  $k$  is any integer greater than or equal to 1, assuming the truth of  $P(k)$  leads us to conclude that  $P(k+1)$  must be true as well.

---

<sup>22</sup>Well, it's mine, at least.

**Problem 1.21** (★). What statement is represented by  $P(k)$ ? What about  $P(k + 1)$ ?

**Problem 1.22** (★★). Prove the inductive step by *assuming* the truth of  $P(k)$  and showing that  $P(k + 1)$  must be true as well. ★

**Problem 1.23** (★). Conclude that  $P(n)$  is true for all  $n \geq 1$ . Rejoice.

**Problem 1.24** (★★). Recall DeMorgan's laws from Chapter ??:

$$\neg(A \wedge B) \iff \neg A \vee \neg B \quad (??)$$

$$\neg(A \vee B) \iff \neg A \wedge \neg B \quad (??)$$

Prove an extended version of equation (??): ★

$$\neg(A_1 \wedge A_2 \wedge \dots \wedge A_n) \iff \neg A_1 \vee \neg A_2 \vee \dots \vee \neg A_n, \quad \text{when } n \geq 2.$$

## 1.5 Fallacious proof 'techniques'

If you're looking for ways to *fail* at proving things and have real mathematicians laugh at you, this is the section for you! Of course, if for some reason you'd rather not have mathematicians laugh at you, you could also try avoiding these proof 'techniques'.

### Proof by evidence

One fairly obvious type of fallacious proof is a *proof by evidence*. This is the kind of proof you find in a courtroom, since it is impossible to prove *with mathematical certainty* that yes, Mr. Jones purchased an illegal spacemonkey from a spacemonkey smuggler on the night of February 29, 1946.<sup>23</sup> In a court, all you have to go on is evidence. But evidence, even lots of it, isn't good enough for mathematical proof. And while you're thinking about that, here's a neat math tidbit for you: did you know that all numbers are less than one million? Really, it's true. I mean, look, 2 is

<sup>23</sup>(For example.)

less than one million, 3 is less than one million, and so are 5, 19, 124397, and on and on . . . I have tried a *lot* of numbers—really, like, hundreds of thousands—and every single one of them is less than one million. QED!

OK, that's a silly example, but you get the point. As another example, consider the Goldbach Conjecture, which we met last chapter. It's been checked up to some ridiculously large number, but that's not the same as a proof. In fact, it's nowhere even close.<sup>24</sup>

## Circular proof

A *circular proof* occurs when you assume that statement *S* is true in order to prove statement *S*! “Well, since grass is green, it isn't not green; therefore, grass is green!” It sounds dumb and obvious when worded like that, but it can be subtle.

## Proof by hand-waving

A proof by hand-waving is what you do when you can't explain something that you 'know' is true, so you sort of wave your hands around while muttering something like, “it's obvious to *smart* people.” While intuition does often play a central role in the process of mathematical discovery, when it comes to proof it's not enough to say that something “just seems true”; the problem, of course, is that it might not be. Here's another way to think about it: if someone points to any particular place in your proof and says, “I don't understand this step. Can you explain it to me?” you'd better be able to. If you can't, you're probably guilty of hand-waving.<sup>25</sup>

---

<sup>24</sup>For one thing, that 'ridiculously large' number is actually rather small, relative to ridiculously, *stupendously* large numbers (see section ??).

<sup>25</sup>Which is certainly not to say you need to write out every step in excruciating detail—only that you should be able to supply the detail if asked.

## 1.6 More problems

Here's a collection of problems you can use to hone your problem-solving and proving skills.

**Problem 1.25** (\*\*). The *double factorial* of a positive integer  $n$ , written  $n!!$ , is defined as the product of every other number from  $n$  down to 1 (or 2). For example,  $7!! = 7 \cdot 5 \cdot 3 \cdot 1 = 105$ , and  $8!! = 8 \cdot 6 \cdot 4 \cdot 2 = 384$ . (Note that the name and notation for 'double factorial' is slightly<sup>26</sup> misleading: one might think it means to take the factorial of the factorial, for example,  $(3!)! = 6! = 24$ . But it doesn't. Although you're free to make up your own name for that if you want.)

Write down an equation expressing the relationship between  $(2n)!!$  and  $n!$  for any positive integer  $n$ .

**Problem 1.26** (\*\*). Are there any integers greater than 9 which are equal to the sum of their digits?

**Problem 1.27** (\*\*\*) . Are there any integers greater than 9 which are equal to the product of their digits?

**Problem 1.28** (\*\*). The following definition of *Euclid numbers*<sup>27</sup> is inspired by Euclid's proof:

$$e_n = e_1 e_2 \dots e_{n-1} + 1.$$

That is, to get each Euclid number, multiply all the previous Euclid numbers together, then add 1. Of course, it's not immediately clear from this definition what  $e_1$  should be; we'll choose  $e_1 = 2$ . Then

$$e_2 = e_1 + 1 = 2 + 1 = 3$$

$$e_3 = e_1 e_2 + 1 = 2 \cdot 3 + 1 = 7$$

$$e_4 = e_1 e_2 e_3 + 1 = \dots$$

<sup>26</sup>By which I mean 'very'.

<sup>27</sup>This definition follows Graham, Knuth, and Patashnik (1994). Elsewhere,  $e_n$  is defined to be one more than the product of the first  $n$  primes, so that the first few Euclid numbers are 3, 7, 31, 211, and so on. (See, for example, <http://mathworld/EuclidNumber.html>.) The latter definition is actually more closely related to Euclid's proof, but the former is (for our purposes) more interesting.

. . . and so on.

- (a) Find  $e_4$ ,  $e_5$ , and  $e_6$ .
- (b) Are all Euclid numbers prime? Why or why not?
- (c) Are all Euclid numbers (other than  $e_1$ ) odd? Why or why not?

**Problem 1.29** (\*\*\*). Prove that  $e_n = e_{n-1}^2 - e_{n-1} + 1$  whenever  $n > 1$ . ★

**Problem 1.30** (\*\*). Prove or disprove: every prime number other than 2 can be written as a difference of two squares.

**Problem 1.31** (\*\*\*). Prove that if  $m$  and  $n$  are integers such that  $n^2 + 1 = 2m$ , then  $m$  can be written as the sum of two squares. ★

**Problem 1.32** (\*\*). Consider the following function:

$$f(0) = 2^0$$

$$f(1) = 2^0 + 2^1$$

$$f(2) = 2^0 + 2^1 + 2^2$$

⋮

$$f(n) = 2^0 + 2^1 + 2^2 + \cdots + 2^n = \sum_{k=0}^n 2^k$$

Find and prove a simpler definition for  $f(n)$ . ★

**Problem 1.33** (\*\*\*). What's wrong with each of the following 'proofs'? ★

- (a) Here's a proof by induction that all horses are the same color. Consider a group of  $n$  horses. For the base case ( $n = 1$ ), all the horses in a group consisting of just one horse have the same color (that is, any horse has the same color as itself). For the inductive step, suppose that in any group of  $k$  horses, all the horses have the same color. Now consider a group of  $k + 1$  horses. If we remove one of the horses, by the inductive hypothesis all the remaining ones must have the same color, call this color  $C$ . If we now put the one horse back and remove a different horse, all the remaining horses must again have the same color, but this color must be  $C$  because of the overlap between the groups of horses. So in fact all

of the  $k + 1$  horses have the same color. Therefore, by induction, all the horses in a group of any size must all have the same color; in particular, we can choose the group of all the horses in the world to show that all horses have the same color.

\*\*\* Some (additional) problems should go here. \*\*\*

## Hints for Chapter 1

1.2 If you're not sure which numbers are prime, you could just do a Google search for "list of prime numbers" or something similar, although there *are* quick ways to determine primality in your head for numbers under 100—more on this in Chapter ??.

1.3 You probably don't even need a special program for this one—just use Google!

1.6 Don't know what 'primorial' means? Don't worry, that's the point! Try looking it up.

1.7 This really amounts to counting how many factors of 10 are in the product. Since  $10 = 2 \cdot 5$ , you'll have to count the factors of 2 and 5 separately.

1.8 (a) Why are the white areas labeled  $a^2$ ,  $b^2$ , and  $c^2$ ? How does the picture show that  $c^2 = a^2 + b^2$ ? (b) Which part of the picture represents a "sum of odd numbers"? Which part represents  $n^2$ ? What's with the grey shaded blocks?

1.11 Re-read section ??.

1.15 Any odd number can be written in the form  $2r + 1$ , where  $r$  is an integer.

1.16 Use a proof by cases: if  $k$  is not divisible by 3, then it can be written as either  $3s + 1$  or  $3s + 2$  for some integer  $s$ .

1.22 We want to show something about the sum  $1 + 3 + 5 + \dots + (2k + 1)$ . Can you use the inductive hypothesis to simplify this sum?

1.24 Use induction on  $n$ , and note that  $A_1 \wedge \dots \wedge A_{n-1} \wedge A_n$  can be written as  $(A_1 \wedge \dots \wedge A_{n-1}) \wedge A_n$ , since  $\wedge$  is associative (Problem ??).

1.29 Write out the definition of  $e_n$ . Can you find a way to simplify it by substituting an expression involving  $e_{n-1}$ ?

1.31 Begin by trying some examples and looking for patterns: make a list of values for  $m$  and  $n$  that satisfy  $n^2 + 1 = 2m$ , and see if you can express  $m$  as a sum of two squares in each case.

1.32  $f(n) = 2^{n+1} - 1$ ; use a proof by induction.

1.33 (a) Are you sure that the inductive step works in *all* cases?

# Bibliography

- Euclid (1956). *The Thirteen Books of The Elements*. Trans. and comm., with an introd., by Sir Thomas L. Heath. 2nd ed. Vol. 2. New York: Dover.
- Graham, Ronald L., Donald E. Knuth, and Oren Patashnik (1994). *Concrete Mathematics: A Foundation for Computer Science*. 2nd ed. Addison-Wesley.
- Hoffman, Paul (1998). *The Man Who Loved Only Numbers*. Hyperion.



# Solutions

## Chapter 1

1.1 For values of  $n$  from 0 to 6,  $n^2$  gives remainders of 0, 1, 4, 2, 2, 4 and 1 when divided by 7, respectively. For higher values of  $n$  this pattern simply repeats. So, there aren't any perfect squares with a remainder of 3 (or 5, or 6) when divided by 7. I was lying.

1.2 All the primes other than 2 and 3 fall in the first and fifth columns—put another way, all primes greater than 3 seem to be of the form  $6k \pm 1$  (that is, one greater or less than a multiple of 6). This is because all the numbers in the second, fourth and sixth columns are divisible by 2 (and hence not prime), and all the numbers in the third column are divisible by 3.

1.3 The 29th prime is 109. You could find this in many ways; for example, you could type `p: 28` in J,<sup>1</sup> or `Prime[29]` in Mathematica, or you could do a Google search for “list of primes” (or something similar) and come up with a website such as <http://primes.utm.edu/lists/small/10000.txt>.

1.4 The first 500 prime numbers add up to 824,693, which could be calculated by, for example, `+/ p: i.500` (J) or `Sum[Prime[i],{i,500}]` (Mathematica).

1.5 18956767008469 is not prime; it is equal to  $1260829 \times 15035161$ . On the other hand, 4378147351 is prime.

Using J:

---

<sup>1</sup>The first prime is `p: 0`.

```

q: 18956767008469
1260829 15035161
q: 4378147351
4378147351

```

Using Mathematica:

```

In[1] := PrimeQ[18956767008469]
Out[1]= False

```

```

In[2] := FactorInteger[18956767008469]
Out[2]= {{1260829, 1}, {15035161, 1}}

```

```

In[3] := PrimeQ[4378147351]
Out[3]= True

```

**1.6** As you can find by searching MathWorld or Wikipedia, the *primorial* of  $n$  (denoted  $n\#$ ) is the product of all the prime numbers less than or equal to  $n$  (the analogy with *factorial*—the product of *all* the numbers less than or equal to  $n$ —should be clear). Therefore,

$$19\# = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 9699690.$$

**1.7** It's actually enough just to count the factors of 5: there will be many more factors of 2 in the product than factors of 5, so every factor of 5 will always have a factor of 2 to pair with in order to yield a factor of 10. For example, the product of all the integers from 1 to 10 has two zeros at the end:

$$\begin{aligned}
10! &= 1 \cdot 2 \cdot 3 \cdot (2^2) \cdot 5 \cdot (2 \cdot 3) \cdot 7 \cdot (2^3) \cdot (3^2) \cdot (2 \cdot 5) \\
&= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \\
&= (10^2) \cdot 2^6 \cdot 3^4 \cdot 7 \\
&= 3628800
\end{aligned}$$

So, how do we count the factors of 5 in  $100!$ , the product of all the integers from 1 to 100? Well, every fifth number (5, 10, 15 . . . ) contributes a factor



1.10 Because of the way you constructed  $M$ , it must either be prime, or divisible by some prime which is greater than 17. In this case,  $M$  isn't prime; it can be factored as the product of three primes,  $M = 19 \cdot 97 \cdot 277$ . (All three of which, of course, are greater than 17.)

1.11 Although it may seem 'obvious,' we certainly can't conclude this from the given theorem. The statement in question—that  $k^2$  is not even whenever  $k$  is not even—is the inverse of the given theorem, and the truth of an implication tells us nothing about the truth of its inverse.

1.12 Yes, we can—this is the contrapositive of the theorem.

1.13 This implication is false; it can be disproved simply by finding a counterexample. For example, 9 is odd and greater than 1, but it is not prime.

1.14 This is not true; for example, we could have  $m\angle A = 85^\circ$ ,  $m\angle B = 85^\circ$ , and  $m\angle C = 10^\circ$ : a triangle with  $m\angle A + m\angle B = 170^\circ$  which is nonetheless acute.

1.15 This is true. Suppose  $k$  is an odd number. Then  $k$  can be written in the form  $2r + 1$  for some integer  $r$ . So  $k^2 = (2r + 1)^2 = 4r^2 + 4r + 1 = 2(2r^2 + 2r) + 1$  which is odd, since it is one more than twice an integer.

1.16 Let  $k$  be an integer which is not divisible by 3. There are two cases to consider:  $k$  could give a remainder of 1 or 2 when divided by 3. In the first case, say  $k = 3s + 1$ . Then  $k^2 - 1 = (3s + 1)^2 - 1 = 9s^2 + 6s + 1 - 1 = 9s^2 + 6s = 3(3s^2 + 2s)$ . In the other case, suppose  $k = 3s + 2$ ; then  $k^2 - 1 = (3s + 2)^2 - 1 = 9s^2 + 12s + 4 - 1 = 3(3s^2 + 4s + 1)$ . In either case,  $k^2 - 1$  is divisible by 3. Therefore  $k^2 - 1$  is divisible by 3 whenever  $k$  is not.

1.17 One method is to make a truth tables to show that these expressions are logically equivalent. Another approach is to simplify  $(\neg A \implies B)$  using Problem ??:

$$\begin{aligned} \neg A \implies B &\iff \neg(\neg A) \vee B && \text{(by Problem ??)} \\ &\iff A \vee B. && \text{(by (??))} \end{aligned}$$

1.18 Since you are only asked to prove that such a prime number *exists*,

all you need to do is give an example. There are many possible examples; one is  $3 = 2^2 - 1^2$ .

1.19  $213 = 6^3 - 3$ .

1.20  $P(1)$  represents the statement " $1 = 1^2$ ", which is obviously true.

1.21  $P(k)$  represents the statement " $1 + 3 + 5 + \dots + (2k - 1) = k^2$ ," and  $P(k + 1)$  the statement " $1 + 3 + 5 + \dots + (2k + 1) = (k + 1)^2$ ."

1.22 Assume  $P(k)$  is true, that is,  $1 + 3 + 5 + \dots + (2k - 1) = k^2$ . We can therefore substitute  $k^2$  into the sum  $1 + 3 + 5 + \dots + (2k + 1)$ , as follows:  $1 + 3 + 5 + \dots + (2k - 1) + (2k + 1) = k^2 + 2k - 1 = (k + 1)^2$ , and we have shown that  $1 + \dots + (2k + 1) = (k + 1)^2$ , as desired.

1.23 Huzzah!

1.24 The base case,  $n = 2$ , is just equation (??), which we already know to be true. For the inductive step, suppose that  $\neg(A_1 \wedge \dots \wedge A_k) \iff \neg A_1 \vee \dots \vee \neg A_k$  for some  $k \geq 2$ . Then

$$\begin{aligned} \neg(A_1 \wedge \dots \wedge A_{k+1}) &\iff \neg((A_1 \wedge \dots \wedge A_k) \wedge A_{k+1}) \\ &\iff \neg(A_1 \wedge \dots \wedge A_k) \vee \neg A_{k+1} && \text{(??)} \\ &\iff (\neg A_1 \vee \dots \vee \neg A_k) \vee \neg A_{k+1} && \text{(IH)} \\ &\iff \neg A_1 \vee \dots \vee \neg A_{k+1}. \end{aligned}$$

1.25  $(2n)!! = 2^n \cdot n!$ , since  $2^n \cdot n! = 2^n \cdot n \cdot (n - 1) \cdot (n - 2) \dots 2 \cdot 1 = 2n \cdot (2n - 2) \cdot (2n - 4) \dots 4 \cdot 2 = (2n)!!$ . For example,  $8!! = 384 = 16 \cdot 24 = 2^4 \cdot 4!$ .

1.26 No. Here's why: because we use a base-10 number system, any number is actually equal to its last digit, plus 10 times the second-to-last digit, plus 100 times the third-to-last digit . . . and so on. Symbolically,  $d_n d_{n-1} \dots d_1 d_0 = 10^n d_n + 10^{n-1} d_{n-1} + \dots + 10 d_1 + d_0$ . The only way for this to be equal to  $d_n + d_{n-1} + \dots + d_1 + d_0$  (the sum of the digits) is if all the digits other than  $d_0$  are equal to zero.

1.27 As of this writing, I'm pretty sure the answer is 'no', although I'm actually unsure how to prove it. Any solutions or partial solutions I receive will be credited appropriately!

**1.28** (a)  $e_4 = 2 \cdot 3 \cdot 7 + 1 = 43$ ;  $e_5 = 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807$ ;  $e_6 = 2 \cdot 3 \cdot 7 \cdot 43 \cdot 1807 + 1 = 3263443$ . (b) No; although  $e_1$  through  $e_4$  are all prime,  $e_5 = 13 \cdot 139$  is not. (c) Every Euclid number other than  $e_1$  is indeed odd. Every Euclid number from  $e_2$  onward is equal to  $e_1 \cdot Q + 1$ , where  $Q$  is some product of other Euclid numbers; it doesn't really matter, since  $e_1 = 2$ , and  $2Q + 1$  is odd no matter what  $Q$  is.

**1.29** Note that  $e_{n-1} - 1 = e_1 \cdots e_{n-2}$ , so we can substitute  $(e_{n-1} - 1)$  into the definition of  $e_n$ , like this:

$$e_n = e_1 \cdots e_{n-2} e_{n-1} + 1 = (e_{n-1} - 1) e_{n-1} + 1 = e_{n-1}^2 - e_{n-1} + 1.$$

**1.30** In fact, a stronger statement is true: every positive odd number can be written as a difference of two squares. Given an odd number  $2n + 1$ , it can be expressed as the difference between  $n^2$  and  $(n + 1)^2$ :

$$(n + 1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1.$$

For example, since 19 can be written as  $2 \cdot 9 + 1$ , it follows that  $19 = 10^2 - 9^2$ , as you can check for yourself. Since all prime numbers other than 2 are odd, it follows that all prime numbers other than 2 can be expressed in this way.

**1.31** First, if  $n^2 + 1 = 2m$ , then  $n$  has to be odd; so there is some integer  $s$  for which  $n = 2s + 1$  (all odd numbers can be written in such a form). Then I claim that  $m = s^2 + (s + 1)^2$ :

$$\begin{aligned} m &= \frac{n^2 + 1}{2} \\ &= \frac{(2s + 1)^2 + 1}{2} \\ &= \frac{4s^2 + 4s + 2}{2} \\ &= 2s^2 + 2s + 1 \end{aligned}$$

and also

$$\begin{aligned} s^2 + (s + 1)^2 &= s^2 + (s^2 + 2s + 1) \\ &= 2s^2 + 2s + 1 \end{aligned}$$

So  $m = 2s^2 + 2s + 1 = s^2 + (s + 1)^2$ , as claimed. For example, if  $n = 7$ , then  $m = 25$  and  $s = 3$ , and 25 is indeed equal to  $3^2 + 4^2$ .

Of course, this is a very nice solution which completely obscures the *method* of solution. This is quite common in mathematical writing, actually, which in my opinion is quite a shame. Someone solving a problem will spend a lot of time trying things, playing around, hitting dead ends and starting over, until they finally hit a solution; when they write about it, however, they leave out all the trials and dead ends and mental processes that led them there. This is great as far as elegance and conciseness go, but fairly useless in learning how to solve similar problems yourself.

**1.32**  $f(n) = 2^{n+1} - 1$ .

*Proof.* The base case is true:  $f(0) = 2^0 = 1 = 2^{0+1} - 1$ . For the inductive step, suppose that  $f(k) = 2^{k+1} - 1$  for some  $k \geq 0$ . Then we want to show that  $f(k + 1) = 2^{k+2} - 1$ . Using the inductive hypothesis, this is not too difficult:

$$\begin{aligned} f(k + 1) &= 2^0 + 2^1 + 2^2 + \cdots + 2^k + 2^{k+1} \\ &= f(k) + 2^{k+1} \\ &= (2^{k+1} - 1) + 2^{k+1} \\ &= 2 \cdot 2^{k+1} - 1 \\ &= 2^{k+2} - 1. \quad \square \end{aligned}$$

**1.33** (a) The inductive step does not work when  $k = 2$ , since with only two horses, removing one and then the other does not produce any “overlap” between the two groups which remain. In other words, the fact that every horse has the same color as itself (which is true) does *not* mean that any two horses have the same color (which is obviously false). The first domino doesn’t knock over the second. Interestingly, if it *were* true that *any two* horses have the same color, then this proof would indeed show that all horses are the same color.<sup>3</sup>

<sup>3</sup>For philosophy homework, write a 1,000-word essay on the topic: *If all horses were the same color, what color would they be?*