Chapter 4

Direct Proofs

At last, we are ready to begin learning about writing formal proofs. Just as the previous chapters' material built upon that of the chapters that preceded them, so will this chapter's material build upon that of its predecessors. If you are jumping directly to this chapter and find that some ideas are difficult to follow, please consider returning after you read about logic, quantified expressions, and arguments. A solid foundation in those topics will serve you well as you learn to write proofs.

This chapter focuses on direct proofs, the most common variety. It also explains proof by cases, a technique that is often used in conjunction with direct proofs, but which is also useful with other proof techniques. At the end, we introduce some approaches for showing that a conjecture cannot be proven. If you are looking for indirect (a.k.a. 'contra') proof techniques, see the next chapter . . . but read this one first!

4.1 The Heartbreak of Probarephobia[1]

We have a confession to make. Remember truth tables? Sequences of logical equivalences? Valid arguments using rules of inference? Those are all proofs. You've been soaking your brain in proofs for a few chapters already.[2]

[1] A 1960s ad campaign for Tegrin skin care products introduced the phrase "Heartbreak of Psoriasis" to attract the attention of people with dry, itchy skin.

[2] A 1981 commercial for Palmolive dish-washing liquid featured a woman soaking her fingers in a small bowl of it, in preparation for a manicure, as an illustration of how gentle Palmolive is on your hands. The memorable phrase from Madge the Manicurist was, "You're soaking in it!" We thought about titling this chapter "Direct Proofs: You've Been Soaking in Them!"

There are two reasons we didn't call them proofs. The first is that the kinds of arguments that most people think of as 'proofs' are less constrained, usually more challenging to construct, and often harder to follow than are the examples we've seen so far. The first two of those three justifications come with the territory. You know more now than you did at the start of Chapter 1, and that knowledge allows us to start working with more challenging hypotheses and conclusions.

As for being harder to follow, that's a problem that proof-writers can address by writing their proofs to be readable by a knowledgeable audience. We will try to follow that advice, which means that we will no longer justify every step of every argument. This is necessary to keep the lengths of our proofs manageable, and is standard practice. The content of the proofs will contain justifications for only the less-obvious steps. We will rely on your knowledge of logic, arguments, and the rest of your education to allow you to fill in most of the remaining details.

The second reason for avoiding the word 'proof' until now: Fear. College-bound students are advised to complete a reasonably well-defined sequence of math classes during high school (or the equivalent), but too frequently don't receive a significant introduction to proofs along the way. There are many reasons for this omission, but the consequence is what matters. Students often end up believing that a proof is a mysterious and impossibly difficult construct that isn't important: "If learning to read and write proofs were useful skills, someone would have taught them to us by now!" You're in luck: 'Someone' has already started, and in this chapter 'someone' will continue the job.

In an effort to show that proofs aren't scary (and to entertain the world), writer Ken Keeler of the American animated television show Futurama penned an episode ("The Prisoner of Benda") that included the full text of a proof (Figure 4.1) showing that the effects of Professor Farnsworth's mind-switching machine could be reversed.[3] Keeler, who earned a Ph.D. degree in applied mathematics, wrote the proof specifically for this episode. If a proof can star in a cartoon, you know they don't need to be frightening.

probarephobia

As far as we can tell, no one has bothered to create a word for the fear of proofs. We modestly suggest 'probarephobia, ' from the Latin *probare* (to show to be true, to demonstrate) and the Greek *phobos* (fear). There are words for related fears – for example, 'arithmophobia' is the fear of numbers,

[3] The full text of the proof is available online; one source is http://theinfosphere.org/Futurama_theorem

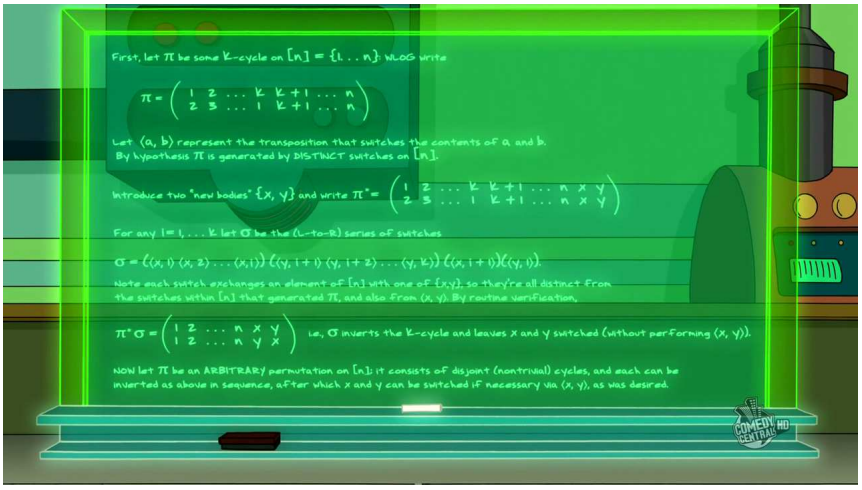

Figure 4.1: Futurama writer Ken Keeler's mind restoration proof from the episode "The Prisoner of Benda." Credit: The Curiosity Company.

and 'phronemophobia' is the fear of thinking.[4] – but until now none for a fear of the content of this chapter[5]

4.2 Proof Preliminaries

Before we write any of these challengingly less-constrained proofs, we have some terminology to introduce and some advice to impart.

4.2.1 Terminology

Proofs come with a handful of associated terms. If you're like most people, you've heard of them, but you're not quite sure how they differ. We start by distinguishing *conjecture* from *theorem*.

Definition 22: Conjecture *conjecture*

[4] Some phobia names contain words related to proofs, but describe very different fears. 'Theo**logic**ophobia' is the fear of theology, while 'a**math**ophobia' is the fear of . . . dust.

[5] Suggested t-shirt and bumper-sticker slogan: Got Probarephobia? Relax; It's a Given.

A statement with an unknown truth value is a *conjecture*.

theorem

Definition 23: Theorem

A *theorem* is a conjecture whose truth has been demonstrated.

Example 76:

The existence of intelligent life elsewhere in the universe is a conjecture.[6] When an extraterrestrial visitor arrives to ask us to stop littering this corner of the galaxy with our space probes and radio waves, it will become a theorem.

disproven conjecture

In this book, we will label as conjectures all statements we are about to try to prove. As soon as we can successfully prove one, from that point forward we'll call it a theorem. If we can disprove it, it's a *disproven conjecture*. If we can do neither, it remains merely a conjecture.

Now we can define 'proof.'

proof

Definition 24: Proof

A sound argument that demonstrates the truth of a theorem is a *proof*.

Notice that we are insisting on a sound argument, not just a valid one. We can't claim that we've demonstrated that a conjecture is true by beginning with information we're just assuming to be true – we need to start with truth to establish truth.

Our last two definitions are other names for theorems. They are used to describe theorems that are created as parts of, or extensions of, other theorems. We will provide examples of these in section 4.3.

[6] And has only tenuously been accepted to exist here.

Definition 25: Lemma *lemma*

A *lemma* is a theorem created to aid in the construction of another theorem.

Sometimes, while writing a proof, you reach a point where you say to yourself, "Self, I could easily finish this proof if I knew that this statement were true." You start trying to prove that it is, and if you succeed, you will have created a new theorem – a lemma – that you can use to justify a step in your original proof. You can think of a lemma as a 'sub-theorem,' much as you might create a subprogram (e.g., a method or a function) in a programming language for the main program to invoke.

Mathematicians sometimes reserve 'theorem' to describe important results and use 'lemma' for less significant results. In this book, we'll be calling every proven conjecture a theorem, reserving 'lemma' for situations matching our definition.

Definition 26: Corollary *corollary*

A *corollary* is a theorem whose truth follows almost immediately from the truth of another theorem.

The difference between a lemma and a corollary, then, is that lemmas appear in the middle of proofs of other theorems, while corollaries appear immediately after such proofs. They are both usually smaller results (and usually easier to prove) than their associated theorems.

4.2.2 Proof-Writing Advice

Before we cover any proof techniques, we want to try to put you in an appropriate frame of mind. As we've mentioned, many people have a deep-seated fear of proofs. A common manifestation of this fear is a tendency to 'lock up' – to have no idea what to do, or even what to try, to move the argument forward. This is similar to "writer's block," which occurs when an author can't decide what to write next. When you get stuck while writing a proof and aren't sure of the next step, try to remember these pieces of advice.

1. **Not all conjectures can be proven.** Always ask yourself: "Does this conjecture seem to be true?" If you have doubts, start by trying to disprove the conjecture – that is, try to show that the conjecture is false. Techniques for disproof are covered in section 4.4.

2. **Dead-ends are expected.** When writing a proof, it's very common to reason your way to a conclusion that doesn't seem useful for completing the proof. Maybe it isn't useful, or maybe you're just not seeing how it can be useful. If you feel yourself getting frustrated, take a break. If you can, take a walk. During an exam, work on another question and come back to the proof later.

3. **Choose the right tool for the job.** We cover the direct proof technique in this chapter, two more techniques in the next chapter, and a fourth several chapters later. If the technique you chose initially doesn't seem to be a good fit for the conjecture, try another.

4. **"Mind what you have learned. Save you it can."**[7] To Yoda you listen! Any of your education in mathematics, including what you've covered in this book, can be useful in proof-writing. Keep your mind open.

5. **There are multiple ways to say the same thing.** Some of those ways can be more useful than others. For example, we know that $10 \mid x$ is true when x is a multiple of 10. But also, $x \,\%\, 10 = 0$ and the decimal representation of x ends in a zero when x is a multiple of 10.

6. **Practice!** An unfortunate consequence of standardized mathematics curricula and standardized assessment examinations in grade school is that students learn to expect all math problems on a given topic to look the same and to be solved the same way. When they get to college, they are often unprepared to be creative and to embrace flexibility, two characteristics that proof-writing requires. The more conjectures you examine, and the more proofs you write, the more prepared you will be.

4.2.3 Proofs of $p \to q$

Conjectures are written, or can be re-written, as implications. We have some given information (the hypothesis or hypotheses) and the conclusion we hope

[7] Star Wars: Episode V – The Empire Strikes Back, Lucasfilm, 1980. (1980!?!)

to justify. We are also told the circumstances under which the conclusion needs to be true, though sometimes we need to infer them ourselves.

Because we are proving conjectures expressible as implications, it is common to refer to them using the notation $p \to q$. Often, the conjecture needs to be shown to hold over all members of a domain, such as the positive integers. In such "for all" cases, we can use $\forall x(P(x) \to Q(x)), x \in D$ instead of $p \to q$, but as the idea is the same with either notation, most of the time we will stick with the simpler $p \to q$ when we need to use notation.

Methods of Proof

To correctly reason from the hypotheses to the conclusion, we need acceptable proof techniques that can show the truth of conditional statements. Having constructed proofs in the earlier chapters, there must have been at least one underlying technique, and there was:

(a) *Direct proof.* Outside of textbooks, it's safe to say that most proofs are direct proofs. All of the logical equivalence and rule of inference arguments we examined in the previous chapters are direct proofs. We will revisit those, and cover additional structurings of direct proofs, in section 4.3. *direct proof*

The direct proof method is also the foundation for three related proof techniques, the first two of which are covered in the next chapter:

(b) *Proof by Contraposition.* Also known as *proof of the contrapositive*, this technique is a very slight variation of direct proof. It will be covered in Section 5.1. *proof by contraposition*

(c) *Proof by Contradiction* sacrifices the definite conclusion of direct and contraposition proofs to gain a compound hypothesis (a sacrifice which is more useful than it may sound). This method is covered in Section 5.2. *proof by contradiction*

(d) *Proof by Induction*, which, despite the name, has a satisfying, comfort-food core of deduction. Proof by induction is different enough to warrant a chapter of its own. *proof by induction*

Many other proof techniques exist. These can all be considered to be forms of direct proof, but they have separate names to help us keep the variations straight. We won't have a special section for these; instead, we will demonstrate them as we have need of them:

vacuous proof

(e) *Vacuous Proofs* are based on the idea of vacuous truth we defined in Chapter 1. They often appear when we have a definition of a property in the form of an implication and try to apply the definition to a situation in which the antecedent cannot be applied.

trivial proof

(f) *Trival Proofs* are those in which the implication is true because the consequent is true; that is, the truth of the antecedent is irrelevant. For example: *If I am both Batman and Superman, then 2 is even.*

proof by cases

(g) *Proof by Cases* (also known as *proof by exhaustion*[8]) applies when we can show that the conjecture is true for every member of the domain by testing each member individually or by testing partitions of the domain. Proofs by cases often appear within other proof techniques, as we will see.

constructive proof

non-constructive proof

(h) *Constructive Proofs* identify a member of the domain that makes an existential conjecture (that is, one that merely claims a satisfying member exists) true. A related technique is the *non-constructive proof*, which manages to demonstrate that an existential conjecture is true without ever identifying a specific example.

combinatorial proof

(i) *Combinatorial proofs* show the number of ways to count an activity, such as finding the number of subsets of size n of a set of size m. We won't see one of these proofs until the counting chapter.[9]

Additional proof methods exist, but this collection is enough for a discrete mathematics book.

Content of a Complete Proof (As Far As We're Concerned)

Everyone has their own favorite way to write a proof, and there is no single set of proof-writing rules that pleases everyone. Here are the principles to which we will (usually!) adhere for the proofs in this chapter, and in the rest of the book. We reserve the flexibility to ignore them when we need to make a point.

1. Start by writing "Proof (*proof technique*):" at the top of the proof. For example: "Proof (Direct):". This lets the reader know how you have

[8] Magically, at 3 a.m. on a homework due date, every proof technique temporarily shares this name.

[9] You're welcome!

structured your argument, allowing him or her to more easily understand it.

2. State your hypotheses and any other given information. We don't consider this to be a necessity, but is especially helpful (both to you and to the reader) when using a technique other than direct proof. It's also a good way to stave off, if not eliminate, writer's block.

3. Make your proofs comprehensible. You've almost certainly had the experience of trying to read a proof in a textbook, only to mutter, "Wait ... where'd *that* come from?!?" It's possible that you didn't have the knowledge or experience to immediately understand the step, but it's also possible that the author abbreviated the proof for publication and lost too much detail in the process. Proofs should be clear, not cloudy.

4. Justify the less-obvious steps of your argument. Telling the reader that $x + y = y + x$ by commutativity of addition will help few readers, but mentioning that $e^{i\pi} + 1 = 0$ is Euler's Identity will help most anyone who is not a math major.

5. "Declare" your variables. Ever written a program in a language that requires the programmer to declare variables before they are used in statements? One reason for that requirement is to help the language translator correctly convert your statements to a lower-level representation. Similarly, telling the reader of your proof that a variable's value is drawn from a particular domain helps the reader understand your argument.

6. When we wrote our logical equivalence and rules of inference arguments, we used columnar representations. If your proof's clarity would be enhanced by using such a representation, please use it. Proof-writers often prefer to have their proofs look as much like traditional paragraphs of text as possible, but we've already seen that the extra hassle of formatting a few columns can be well worth the trouble.

7. To show that your proof is complete, finish it by writing the word "therefore", a comma, and the original conjecture. We think is this a better way for beginning proof-writers to end a proof than are the traditional endings of "Q.E.D."[10] or a 'tombstone' marker (such as '□' (LaTeX :

[10] Q, E, and D are the first letters of the words in the Latin phrase *quod erat demonstrandum*, which means "this was to be demonstrated." "Quite easily done" is a popular sarcastic alternative.

\Box)), because restating the conjecture helps you remember what you were trying to prove. When you are deep in the middle of an argument, it's easy to forget what you were arguing about in the first place.

4.3 Direct Proofs

As the name suggests, a direct proof is quite straight-forward. To prove a conjecture of the form $p \to q$, we assume that the (often compound) hypothesis (p) is true, and demonstrate that the conclusion (q) must also be true. In short:

To prove $p \to q$: Assume p, show q.

4.3.1 Examples of Direct Proofs

Our first direct proof example is very straight-forward, so that we can focus on the construction of the proof rather than on the difficulty of the argument. We will ease into every new proof technique in the same way.

Example 77:

Problem: Using a direct proof, prove this conjecture: If x and y are odd integers, the product xy is also an odd integer.

Solution: We are told to use a direct proof. This means that we are to assume that the hypothesis is true and show that the truth of the conclusion must follow. Our first task, then, is to identify the hypothesis and the conclusion. In this example, finding them is trivial, because the conjecture is expressed in an if-then form: Our hypothesis is "x and y are odd integers," and our conclusion is "the product xy is an odd integer." The word 'also' doesn't change the conclusion; it can be dropped.

We know from the math review appendix (Section A.8). that each odd integer is one more than twice some integer. That is, we can say $x = 2a+1$ and $y = 2b+1$. Using this form of expression for odds requires the introduction of the new integer variables a and b. In the proof, we'll have to remember to explicitly declare them to be integers.

Now that we have representations for x and y, we can multiply those polynomials to create a representation for xy: $xy = (2a + 1)(2b + 1) =$

$4ab + 2a + 2b + 1$.

Having created such an expression, you might be tempted to say, "OK, but ...so what?" Remember what we are trying to show: That xy is odd. We know that odds have the form $2z + 1$. By factoring a 2 from the first three terms of our xy representation, we can achieve that form: $4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1$. Products and sums of integers are also integers, and so xy is an odd integer because it has the $2z+1$ form.

We could prepend "Proof (Direct):" and append "Therefore, ..." lines to the preceding paragraphs and call it a proof. Such a proof would be unnecessarily wordy, even for us. Instead, we'll condense it into a more compact, though not minimal, version. Here's the result:

Proof (Direct): We may assume that x and y are odd integers. Because they are odd, x and y are each one more than twice some integer. Let those integers be a and b, and let $x = 2a + 1$ and $y = 2b + 1$. Using those representations, $xy = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1$. This expression shows that xy can be represented as one more than twice an integer, demonstrating that xy is an odd integer.

Therefore, if x and y are odd integers, the product xy is also an odd integer.

This proof includes a bit more detail we will use in most proofs in this book – in general, we won't explain everything, but we will explain the key steps. The issue of detail is also addressed in Example 78, below.

The proof in Example 77 needed two new variables to create the representations of x and y, not just one. If we tried to use a single variable, we'd say that $x = 2c + 1$ and $y = 2c + 1$. By transitivity, this means that $x = y$. The conjecture does not require that x and y be the *same* odd integer, meaning that the proof's representations of x and y can't require it, either.

Example 77 demonstrated the level of detail we will use in most proofs in this book. The next example addresses a related concern of students.

Example 78:

Problem: My instructor's exams are really long;[11] I don't have time to write proofs with that much detail! Can I get away with writing just the math?

Solution: Probably not, but of course that depends on your instructor. Here's a shortened version of the proof given in Example 77 that we feel has an acceptable level of detail for a proof on an exam:

Proof (Direct): Let $x = 2a + 1$ and $y = 2b + 1$, $x, y \in \mathbb{Z}^{\text{odd}}$. $xy = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1$. This shows that xy is an odd integer.

Therefore, if x and y are odd integers, the product xy is also an odd integer.

This form is still acceptable because it shows a logical progression from the hypothesis to the conclusion, and includes enough detail for the reader to accept that the conclusion follows from the hypothesis, although the reader is expected to fill in some minor details mentally.

Note that extending the algebra through to the $2(2ab+a+b)+1$ expression is important. If you stop with $4ab+2a+2b+1$, you're not showing that xy has the form of an odd-integer, leaving the reader to wonder if you really know how to complete the proof. Most instructors won't give you the benefit of the doubt on something like this. Be safe; be sure to include enough detail to make it clear that you know what you're doing. The points you save will be your own.

Our next direct proof example requires a little more imagination. It's also rather lengthy, to make a point about how proofs are often constructed.

[11] The author has never heard such a comment from his students. Never happened. Not even once. In unrelated news, rumors of the author's selective hearing and recollection are undoubtedly wild exaggerations.

Example 79:

Problem: Using a direct proof, prove this conjecture: $ac > bd$ when $a > b > 0$, $c \geq d > 0$, where $a, b, c, d \in \mathbb{R}$.

Solution: The first step is to identify the hypothesis and the conclusion. This conjecture uses a "q if p" form, meaning that $ac > bd$ is the conclusion and the rest forms the compound hypothesis.

Next, we need to make sure we understand what the notation is trying to tell us. $a > b > 0$ contains three individual pieces of information: $a > b$, $b > 0$, and, by transitivity of $>$, $a > 0$. Similarly, we are given that $c \geq d$, $d > 0$, and $c > 0$. Pay close attention to the inequalities; all of them are $>$ except for the $\geq$ in $c \geq d$.

We're ready to think about the proof. We need some way to introduce the products ac and bd. It's tempting to say, "Well, just multiply $a > b$ by $c > d$, and we're done!" Unfortunately, that isn't legal; inequalities are boolean expressions, and multiplication doesn't apply to boolean operands. We'll have to create ac and bd another way.

Let's start with $a > b$. We can try to create ac by multiplying the left side by c, producing $ac > b$. But is that true? It may not be, as c could be less than one, which could make ac less than or even equal to b. But we're on the right track: We need to multiply both a and b by c to produce $ac > bc$. This is true because we're multiplying both sides by the same amount, and the direction of the inequality stays the same because $c > 0$.

We can create bd in the same way: Multiplying both sides of $a > b$ by d produces $ad > bd$. Now we have to figure out how to combine $ac > bc$ and $ad > bd$. We can do this with transitivity of $>$ if we knew that $bc > ad$ ... but we don't. We could try to prove that it is true and introduce that result as a lemma in this proof, but before we go to that trouble, let's stop and think: Can we create bd from something other than $a > b$?

Happily, we can. We know that $c \geq d$. Multiplying both sides of it by b produces $bc \geq bd$. We can use the properties of inequalities given in the math review appendix (Appendix A) to combine $ac > bc$ with $bc \geq bd$

and show that the conclusion of $ac > bd$ is true.

Having discovered how to show the truth of the conclusion, we can write up the proof as a tightened version of the above discussion.

Proof (Direct): We are given that $a > b$, and that $c > 0$. Multiplying both sides of $a > b$ by c produces $ac > bc$.

We are also given that $c \geq d$ and $b > 0$. Multiplying both sides of $c \geq d$ by b produces $bc \geq bd$.

By the properties of inequalities, together $ac > bc$ and $bc \geq bd$ tell us that $ac > bd$.

Therefore, $ac > bd$ when $a > b > 0$, $c \geq d > 0$, where $a, b, c, d \in \mathbb{R}$.

Example 79 shows how easily a proof writer can encounter a dead-end in his or her reasoning. Textbook and research paper authors rarely reveal their dead-ends in their final proofs, making it seem that they created the proofs correctly on the first try. As this example has shown, even a short proof can be the result of much 'wasted' work.

Our next example will give us a reason to introduce a lemma. Before that, it will require us to do some reasoning about the meaning of the conjecture.

Example 80:

Problem: Prove that the $\sqrt{x}$ being even is sufficient to show the necessity of x's evenness, given that $x \in \mathbb{R}$.

Solution: Are you tempted to say, "Yeah, I can solve this problem by finding the guy who wrote that and making him put it into English!"? We sympathize. But, Chapter 1 saves us from committing a satisfying but unnecessary act of violence: We know what 'sufficient' and 'neces-

sary' mean when they are used correctly. Here, we are given that $\sqrt{x}$ is even, and we need to show that x is even.

What does '$\sqrt{x}$ is even' give us? We know that only integers can be even, and that the only way for a square root to be an integer is for the argument to be a perfect square.

Let's make this easier to think about by letting $\sqrt{x} = y$. Because we are allowed to assume that $\sqrt{x}$ is even, we can assume that y is even. Now let's consider x. $x = \sqrt{x} \cdot \sqrt{x} = y \cdot y$. If we can show that $y \cdot y$ is even, we will have shown that x is even, and our proof will be complete.

Showing that $y \cdot y$ is even requires a separate proof. Because we will be using the theorem that results from this second proof to complete our original proof, the evenness of $y \cdot y$ will be a lemma to our main proof.

That's all fine, but let's not get ahead of ourselves: Is $y \cdot y$ always even? We are given that y is even, meaning we can represent it as twice some integer (say, twice w). $y \cdot y = 2w \cdot 2w = 4w^2 = 2(2w^2)$. Because we can express $y \cdot y$ as twice an integer, $y \cdot y$ is even. And, because $x = y \cdot y$, x is even, completing the original proof.

Time to write it all up. We will start by proving the lemma (let's call it Lemma 80), but we will toss in a twist to the conjecture to keep it interesting.

Conjecture: The square of any even number is also even.

Proof (Direct): Let y represent any even number. Being even, $y = 2w$, $w \in \mathbb{Z}$. $y^2 = (2w)^2 = 4w^2 = 2(2w^2)$. This shows that y^2 is an even number.

Therefore, the square of any even number is also even.

The 'twist' in the above conjecture is that it isn't in an 'if-then' form. We had to re-write it that way, at least mentally, to know the hypothesis and conclusion: *If y is an even number, then y^2 is also even.* English-to-logic

conversions just don't go away.

There's something else to notice in that proof: We didn't restrict w to being a non-negative integer. First, the conjecture isn't limited, meaning that our proof shouldn't be limited. Second, negative integers are either odd or even, just as the positives (and zero) are. It requires no extra effort to prove the conjecture for all evens, so why not?

At last, we can prove the original conjecture, which was: The $\sqrt{x}$ being even is sufficient to show the necessity of x's evenness, given that $x \in \mathbb{R}$.

Proof (Direct): We are given that $\sqrt{x}$ is even. It follows from the definition of evenness that $\sqrt{x}$ is an integer. Let $y = \sqrt{x}$, $y \in \mathbb{Z}$. By the definition of square root, the square of the square root of a real number is the same real number. Thus, $x = (\sqrt{x})^2 = y^2$.

Lemma 80 shows that the square of any even number is also even. By that lemma and the fact that y is even, we know that y^2, and thus x, is even, completing the argument.

Therefore, the $\sqrt{x}$ being even is sufficient to show the necessity of x's evenness, given that $x \in \mathbb{R}$.

If the use of the variable y in both proofs of Example 80 confuses you, feel free to use a completely different set of variables in each proof. We re-used y because we also re-used it in the explanation at the top, to highlight the connection between the original proof and the lemma.

For our final example, we will tie off a loose end. Earlier (in section 4.1) we said that sequences of logical equivalences and rule-of-inference arguments were actually proofs. Let's see how we can re-structure one of those (specifically, Example 66 of Chapter 3) as a proof.

Example 81:

Problem: Assume that if you have a dog and you drop a piece of bread

on the floor, then you won't need to pick up the bread. Further assume that you do have a dog, and you did drop a piece of bread on the floor. Prove that you didn't need to pick up the piece of bread.

Solution: We've already created this argument, so all we have to is write up as we would a proof.

Proof (Direct): By the rule of inference known as Conjunction, we know that the conjunction of "you have a dog" and "you drop a piece of bread on the floor" is true. By applying Modus Ponens to that conjunction and the given implication, we know that you didn't need to pick up the bread.

Therefore, you didn't need to pick up the piece of bread, assuming that if you have a dog and you drop a piece of bread on the floor, then you won't need to pick up the bread; assuming that you do have a dog; and assuming that you did drop a piece of bread on the floor.

The arguments in Chapter 3 required more given information than did our previous direct proof examples, making this proof, especially the 'therefore' line, seem quite wordy. Worse, the proof wasn't especially easy to follow, as the proof's author expected us to 'see' that the rules of inference were applied correctly. That was easy enough for Conjunction, but if you hadn't seen that argument before, would you have been confident that Modus Ponens was used correctly based only on this presentation? Imagine trying to read (or write!) an explanation of an application of a messier rule of inference, such as Resolution.

When writing out an argument in English hinders comprehension more than it helps, use an alternative. Writing arguments in columns, as we did in Chapter refch:arguments, is perfectly acceptable in a proof, too — remember, those arguments are also proofs. We can wrap our original columnar argument in our usual proof trappings and create a hybrid that will be easy to follow.

Proof (Direct): Let d be 'you have a dog,' b be 'you dropped a piece of bread on the floor,' and n be 'you need to pick up that piece of bread.'

(1)		d	[Given]
(2)		b	[Given]
(3)		$d \wedge b$	[1, 2, Conjunction]
(4)		$(d \wedge b) \rightarrow \neg n$	[Given]
(5)	$\therefore$	$\neg n$	[3, 4, Modus Ponens]

Therefore, you didn't need to pick up the piece of bread, assuming that if you have a dog and you drop a piece of bread on the floor, then you won't need to pick up the bread; assuming that you do have a dog; and assuming that you did drop a piece of bread on the floor.

Writing out the 'therefore' line seems even more redundant that it already is, but we did so to stick to our form, and to get the reader's mind back to the English version of the conjecture.

4.3.2 Examples of Direct Proof by Cases

Not infrequently, a conjecture's hypothesis provides so little useful information that it is convenient to create additional information, just so that you have a starting point for your argument. One way to do this is to partition the set upon which the conjecture is constructed, and show that the conjecture holds for each partition. The description of the partitioning can often be all the additional information the argument requires.

Example 82:

Problem: Prove that $n^3 + n + 2 \in \mathbb{Z}^{\text{even}}$, where $n \in \mathbb{Z}$.

Solution: This conjecture doesn't give us much to work with – all we know is that n can be any integer. But what does that tell us that's

helpful? We know that integers are real numbers. We know that integers are rational. We know that the product of two integers is also an integer. We know lots about integers, but nothing that seems useful for this conjecture.

Then again, maybe we do know something of value: We know that every integer is either even or odd. If we can show that n^3+n+2 is even when n is even *and* when n is odd, we will have shown that n^3+n+2 is even for all integers. Sounds like a job for ... proof by cases!

Proof (Direct): Any integer value is either even or odd. We will show that n^3+n+2 is even either way.

Case 1: Let n be even. $n = 2k, k \in \mathbb{Z}$. $n^3+n+2 = (2k)^3+(2k)+2 = 8k^3+2k+2 = 2(4k^3+k+1)$. This demonstrates that n^3+n+2 is even when n is even.

Case 2: Let n be odd. $n = 2j+1, j \in \mathbb{Z}$. $n^3+n+2 = (2j+1)^3+(2j+1)+2 = (8j^3+12j^2+6j+1)+(2j+1)+2 = 8j^3+12j^2+8j+4 = 2(4j^3+6j^2+4j+2)$. This demonstrates that n^3+n+2 is even when n is odd.

Therefore, $n^3+n+2 \in \mathbb{Z}^{\text{even}}$, where $n \in \mathbb{Z}$.

To avoid confusion, we used a different temporary variable in each case. You can make a case[12] that using the same variable for each part is like using 'i' as a loop-control variable in two loops within the same computer program, but we think that keeping the temporary variables unique is a good idea in proofs.

In a proof by cases, each case is a mini-proof, basically a lemma. We could treat them as lemmas, proving them individually as we did with the lemma in Example 80. When the lemmas are as closely related as they are in a proof by cases, it's common practice to prove them all within the original proof.

We left the label on the proof as "Direct" because, even though we proved the conjecture using more than one case, it's still a direct proof: We assumed

[12] Sorry ...

p (n is an integer) and showed q ($n^3 + n + 2$ is even). If you like, you can embellish the label to be "Direct with Cases" or "Direct, Cases." We will just say "Direct" because the reader will be able to see at a glance that such proofs include cases.

Partitioning is a useful tool for understanding large sets. Example 82 made use of the even/odd partitioning of integers. Another way to partition integers: $\{\mathbb{Z}^-, 0, \mathbb{Z}^+\}$.[13] Real numbers can be partitioned into the rationals and the irrationals. Characters in the basic Latin alphabet can be partitioned by case (upper and lower).

Consider truth tables. Each row of a truth table represents a unique assignment of truth values to variables. That is, a truth table is a partitioning of the possible assignments in which each assignment is a partition of cardinality one. Looked at another way, a truth table is a proof by cases.

Example 83:

Problem: Prove that $(p \vee q) \vee \overline{p}$ is a tautology.

Solution: We used a truth table to demonstrate this in Chapter 1. We could re-write the truth table in English to have each case be its own short paragraph, or we could just wrap the trappings of a proof around the truth table.

[13] That's right – zero is neither positive nor negative. Some numeric representations, such as the IEEE 754 floating-point standard, do distinguish between $+0$ and -0 because doing so is sometimes scientifically useful.

Proof (Direct): There are four possible assignments of boolean values to the variables p and q. The following table shows the evaluation of $(p \vee q) \vee \overline{p}$ on all four:

	p	q	$p \vee q$	$\overline{p}$	$(p \vee q) \vee \overline{p}$
(Case 1:)	T	T	T	F	T
(Case 2:)	T	F	T	F	T
(Case 3:)	F	T	T	T	T
(Case 4:)	F	F	F	T	T

No matter how true and false are assigned to the variables, the expression evaluates to true.

Therefore, $(p \vee q) \vee \overline{p}$ is a tautology.

We added the "*(Case 1:)*," "*(Case 2:)*," etc., just to highlight how cases are used in a truth table. In general, labeling the rows of a truth table in that fashion is not necessary.

As we've seen multiple times, most recently in Example 83, it's entirely possible for a conjecture to have multiple variables. If we can partition the domain of one variable (as we did in Example 82), we can certainly do it for more than one. However, there is a cost: The number of cases that need to be considered increases, making it more likely that one of them is considered more than once, or worse, overlooked entirely.

Example 84:

Problem: Prove that if gh is odd, then g and h are both odd.

Solution: You should recognize the situation: We aren't given a hypothesis with much useful information (and we only know how to write direct proofs), so we need to manufacture additional information.

This conjecture deals with odd numbers, making us think that partitioning g and h into evens and odds might be a good approach to try. Because we have two variables and two partitions for each, there are at

most four cases to consider: Both g and h are even, both are odd, g is even and h is odd, and g is odd and h is even. However, multiplication is commutative, meaning that the last two cases are logically identical – both represent the product of an even with an odd – leaving us with only three cases to consider. Of those, only the ones with gh being odd interest us, given the conjecture's hypothesis.

Proof (Direct): Both g and h can be odd or even. We need to consider three cases: Both g and h are even, both are odd, or one is even and the other is odd.

Case 1: Let both g and h be even. $g = 2a$ and $h = 2b$, where $a, b \in \mathbb{Z}$. $gh = (2a)(2b) = 4ab = 2(2ab)$, showing that, in this case, gh is even. As the conjecture's hypothesis is that gh is odd, this case is irrelevant to the proof and can be ignored.

Case 2: Let both g and h be odd. $g = 2c+1$ and $h = 2d+1$, where $c, d \in \mathbb{Z}$. $gh = (2c+1)(2d+1) = 4cd+2c+2d+1 = 2(2cd+c+d)+1$, showing that gh is odd and thus fits our conjecture. For this case, the conjecture holds (that is, when gh is odd, g and h are odd).

Case 3: One of the variables is even and the other is odd. WLOG, let g be even and h be odd. $g = 2e$ and $h = 2f + 1$, where $e, f \in \mathbb{Z}$. $gh = (2e)(2f + 1) = 4ef + 2e = 2(2ef + e)$, showing that gh is even. As with Case 1, this case can be ignored.

Of the three possible ways to assign odd and even integers to g and h, only one fits the conjecture's hypothesis. In that case, the conclusion is true.

Therefore, if gh is odd, then g and h are both odd.

---

wlog

'*WLOG*' is an acronym[14] for the phrase "without loss of generality," a common way to tell the reader that an arbitrary choice can be made without violating the logic of the argument. In this proof, one of the variables needed to be even and the other odd. It makes no difference to the argument which is which, so we picked one of the two possibilities

and used 'WLOG' to let the reader know that our specific choice didn't matter to the proof.

The proof in Example 84 got the job done, but it seems wasteful. We had to consider three cases to discover that only one of them mattered. This observation might cause you to think, "Maybe there's an easier way to prove this ..." There is, but we have yet to cover it. Don't worry; we will, in Example 95 of Chapter 5.

4.3.3 Detecting Poor Proofs

Seeing nothing but correct proofs can leave the impression that all proofs are correct. Not true, of course. The history of mathematics includes many examples of proposed proofs that turned out to be invalid arguments when they were examined closely[15] [16] .

Here are three examples of poor proofs. Each demonstrates a common mistake made in proof development. Hopefully, having seen these, you will be less likely to make similar mistakes when writing your own proofs.

Example 85:

Problem: Prove that if $5n + 4$ is even, then n is even, $n \in \mathbb{Z}$.

'Solution': Consider this attempt at a direct proof:

'Proof' (Direct): Assume that $n \in \mathbb{Z}^{\text{even}}$. $n = 2k$, $k \in \mathbb{Z}$. $5n + 4 = 5(2k) + 4 = 10k + 4 = 2(5k + 2)$, which matches the given information that $5n + 4$ is even.

Therefore, if $5n + 4$ is even, then n is even.

---

[14] A point of pedantry: 'WLOG' is more accurately an *initialism*, but *acronym* is also acceptable. Be aware that, if you start using 'initialism' in everyday communication, you'll never make it as a politician. You should probably avoid 'pedantry,' too.

[15] Wikipedia has a list: http://en.wikipedia.org/wiki/List_of_incomplete_proofs

[16] Wikipedia is conveniently ignoring the reality that approximately 99.995% of poor proofs were written by students on homework assignments or exams and discovered to be invalid by incredulous teachers who used to have full heads of thick, lustrous hair.

The reasoning behind this proof is perfect, except for one huge problem: **It starts by assuming that the conclusion is true!** Proofs exist to demonstrate the truth of conclusions, not to accept them as being true. The conjecture that this proof proves is the converse of the given conjecture. That is: *If n is even, then $5n + 4$ is even.* As we learned in Chapter 1, $p \to q \not\equiv q \to p$. The truth of the converse says nothing about the true of the original.

The lesson: **Never assume that the conclusion is true.**

A poorly constructed proof doesn't tell us much about the conjecture. Unfortunately, even attempting a direct proof with the correct hypothesis can lead to a bad proof, as the next example shows.

Example 86:

Problem: Prove that if $5n + 4$ is even, then n is even, $n \in \mathbb{Z}$.

'Solution': Having learned the lesson of Example 85, we try again:

'Proof' (Direct): Assume that $5n + 4$ is even. $5n + 4 = 2k$, $k \in \mathbb{Z}$. Solving for n, we find that $n = \frac{2k-4}{5}$, which is . . . ummmm, wow, not even always an integer, so it can't always be even . . . can it?

Maybe the Deity of Partial Credit will smile upon me if I write . . .

Therefore, if $5n + 4$ is even, then n is even.

Indeed, $\frac{2k-4}{5}$ isn't always an integer. We started the proof correctly, and still couldn't prove it. That means that the conjecture is false . . . right? Not necessarily. The problem with this proof is that it doesn't make use of a key piece of given information: n is an integer. This conjecture is true; it can be proven with a direct proof that uses a little more creativity, such as was used in Example 84.

The lesson: **Heed the advice in Section 4.2.2.**

By the way: The Deity of Partial Credit might give you some partial credit for remembering to supply the proper conclusion to the proof, but that doesn't mean the proof itself will be worth much. The Deity of Partial Credit, kind as she/he/it may be, still has standards.

Our last example of a poor proof is a variation on a classic.

Example 87:

Problem: Lots of people have trouble writing their sevens and their twos clearly enough to make them distinct. This isn't really a problem at all, because, as the following proof shows, $7 = 2$! Be as sloppy as you like!

'Proof' (Direct): Seven times two is fourteen, and let's make it negative to show negative numbers a little love.

$$\begin{array}{rcll} -14 & = & -14 & \text{[Any integer equals itself]} \\ 49-63 & = & 4-18 & \text{[Strange expressions for } -14\text{]} \\ 49-63+\frac{81}{4} & = & 4-18+\frac{81}{4} & \text{[Add } \frac{81}{4} \text{ to each side]} \\ (7-\frac{9}{2})^2 & = & (2-\frac{9}{2})^2 & \text{[Factoring (reverse FOIL)]} \\ 7-\frac{9}{2} & = & 2-\frac{9}{2} & \text{[Take square root of both sides]} \\ 7 & = & 2 & \text{[Add } \frac{9}{2} \text{ to both sides]} \end{array}$$

Therefore, $7 = 2$.

Does seven really equal two? Is the number line not to be believed? Is reasoned society doomed to collapse?

Solution: No, no, and probably.[17] There's something wrong with this proof, the same problem that many other 'proofs' of impossible conclusions share: The square root step. In this 'proof,' it is claimed that $\sqrt{(2-\frac{9}{2})^2} = 2-\frac{9}{2}$. What most people forget about square roots is that $\sqrt{x^2} = \pm x = |x|$. That is, $x \cdot x = -x \cdot -x = x^2$. This proof quietly drops that plus-minus sign ($\pm$, LaTeX: `\pm`), a hidden step that breaks the validity of the argument. If you were to finish the argument correctly, you'd get a very boring, but correct, conclusion:

$$\begin{array}{rcll} (7-\frac{9}{2})^2 & = & (2-\frac{9}{2})^2 & \text{[From the above 'proof']} \\ |\,7-\frac{9}{2}\,| & = & |\,2-\frac{9}{2}\,| & \text{[Correct square roots]} \\ |\,\frac{5}{2}\,| & = & |\,-\frac{5}{2}\,| & \\ \frac{5}{2} & = & \frac{5}{2} & \text{[No surprise there]} \end{array}$$

The lesson: **Check each step of proposed proofs carefully.**

Square roots, logarithms, and division by zero are common sources of logical errors in 'proofs.' Whenever you see someone claim that they can prove that $0 = 1$, $1 = 2$, $1 = -1$, or the like, check the proof for a step involving one of those constructs. Chances are, that's where you will find the logical error.

4.4 Disproving Conjectures

When a conjecture 'smells' false, or despite your best efforts you can't create its proof, you should spend some time trying to demonstrate that it is false. Such demonstrations are known as *disproofs*. Disproofs do prove that conjectures are false, but you won't often see a disproof written up as a formal proof.[18]

disproof

4.4.1 Find a Counter-Example

By far the most common way to show that a conjecture is false is to find a *counter-example*, a specific assignment of legal values to variables that demonstrates that the conjecture is false. Sometimes a counter-example is easy to find (they are often found at the low and high ends of domains), but often a remarkable amount of searching is required.

counter-example

Example 88:

Problem: Prove or disprove: 2^n is even for all $n \in \mathbb{Z}^*$.

[17] Hopefully, with the power of well-written proofs, we can delay that collapse for a while longer. Everyone listens to reason . . . don't they?

[18] Actually, you rarely see disproofs at all. Although studying failures can be very educational, who wants to become famous for creating a failure? Some disproven conjectures have lingered as cautionary examples. Wikipedia has a small collection: http://en.wikipedia.org/wiki/Category:Disproved_conjectures.

Solution: If you start by listing 2, 4, 8, 16, 32, etc., you will soon conclude that the conjecture must be true, because each number is double the previous, and the first is even. But look at the domain more carefully: $\mathbb{Z}^*$ includes zero, and $2^0 = 1$, which certainly isn't even. Thus, the counter-example 2^0 shows that the conjecture is not true.

To write this as an answer on a homework or exam, something like this would be fine:

Disproof (Counter-Example): Let $n = 0$. $n \in \mathbb{Z}^*$, but $2^0 = 1$ is not even. The conjecture is not true.

That's right – no fancy argument, just a clear statement of an example from the desired domain that 'breaks' the conjecture.

Example 89:

Problem: Prove or disprove this conjecture:[19] If $2^k \equiv 2 \pmod{k}$, then k is prime, $k \geq 2$, $k \in \mathbb{Z}$.

Solution: At first glance, this conjecture seems to be based on too many coincidences to be true – the mod keeps increasing by one but the congruences keep occurring. If you start looking for a counter-example, you might find yourself believing in coincidences, because it does seem that only when $2^k \equiv 2 \pmod{k}$ is k prime: $2^2 \equiv 2 \pmod{2}$, $2^3 \equiv 2 \pmod{3}$, $2^4 \not\equiv 2 \pmod{4}$, $2^5 \equiv 2 \pmod{5}$, $2^6 \not\equiv 2 \pmod{6}$, $2^7 \equiv 2 \pmod{7}$, etc.

The conjecture is false, but it takes quite a bit more snooping to discover a counter-example: $2^{341} \equiv 2 \pmod{341}$. 341 looks like it might be prime, but it isn't: $341 = 11 \cdot 31$. You'd definitely want to use a computer to verify this counter-example: 2^{341} is over 100 decimal digits long!

[19] This is half of a biimplication conjecture, known as the Chinese Hypothesis, that never really existed. It appears to have originated as a mis-translation of a math text, rather than as a serious conjecture. The other half (if k is prime, then $2^k \equiv 2 \pmod{k}$) is an instance of Fermat's Little Theorem (not to be confused with Fermat's Last Theorem), and is true.

4.4.2 Prove the Negation

The second way to show that a conjecture is false is to prove that its negation is true. Frequently, this is similar to finding a counter-example, but the two approaches are not the same.

Imagine that you're asked to prove a conjecture of the form $p \to q$. You try and try, but can't do it, and so begin to suspect that it isn't true. You spend time looking for a counter-example, but can't find one. Instead, you try to prove the negation $(\neg(p \to q))$ is true, which would show that $p \to q$ is false. $\neg(p \to q) \equiv p \wedge \neg q$, meaning that you have to show that $p \wedge \neg q$ is true. As there's no hypothesis, a direct proof would give you nothing with which to work, and, unless you've read ahead, direct proof is the only technique you know. Even with those other techniques, proving $\neg(p \to q)$ probably won't be easy.

All is not lost – proving $\neg(p \to q)$ may still be a reasonable option if you think about what $p \to q$ represents. Back at the start of section 4.2.3 we mentioned that in this chapter the $p \to q$ notation was a stand-in for the more complete $\forall x(P(x) \to Q(x)), x \in D$ quantified predicate notation. In the following example, that quantified notation will be very helpful.

Example 90:

Problem: Disprove the conjecture of Example 88 (2^n is even for all $n \in \mathbb{Z}^*$) again, this time without using a counter-example.

Solution: Let $E(n) : 2^n$ is even, $n \in \mathbb{Z}^*$, and note that our conjecture does not have an explicit hypothesis. That is, the conjecture can be expressed as $\forall n\ (\mathbf{T} \to E(n))$, with the same domain. $\mathbf{T} \to E(n) \equiv E(n)$ (by the Law of the True Antecedent), allowing us to represent the conjecture as $\forall n\ E(n)$.

To verify that $\forall n\ E(n)$ is false without using a counter-example, we need to prove that its negation $(\neg\, \forall n\, E(n))$ is true. By Generalized De Morgan's Laws, $\neg\, \forall n\ E(n) \equiv \exists n\ \neg E(n)$. In conversational English: There's a non-negative integer that makes 2^n odd.

To prove an existential conjecture, we just need to find one member of the domain that makes the conjecture true. We already know the member: $n = 0$. All that remains is to write this up more compactly.

Disproof (Proof of the Negation): The conjecture can be expressed as $\forall n\ E(n)$, $n \in \mathbb{Z}^*$, where $E(n)$ represents '2^n is even.' Its negation is $\exists n\ \neg E(n)$ (by Generalized De Morgan's). This negated conjecture is true, as the following proof shows:

Proof (Direct): Consider $E(0)$. $0 \in \mathbb{Z}^*$ and $2^0 = 1$. Therefore, $\exists n\ \neg E(n)$ is true.

Because it is possible for 2^n to be odd, the claim that 2^n is even for all $n \in \mathbb{Z}^*$ is false.

Please note that $n = 0$ is not a counter-example, because we aren't 'countering' the original conjecture with it. Rather, $n = 0$ proves the negation of the conjecture. Because the conjecture's negation is an existential statement, all we needed was an example to prove it. The proof of the negation disproves the conjecture.

By the way, our little proof of the truth of $\exists n\ \neg E(n)$ is a simple example of a constructive proof (see section 4.2.3).

Having seen Example 90, it's not hard to imagine this prove-the-negation approach working on existential conjectures that we suspect are false. Imagine you're asked to show that $\exists x A(x)$ is true. All you need is one example, but try as you might, you can't find one. Suspecting that the conjecture is false, you look to prove its negation. By Generalized De Morgan's Laws, $\neg\exists x A(x) \equiv \forall x\, \neg A(x)$. The negation is universally quantified, just as are most of the conjectures we usually need to prove, meaning that a common proof technique (such as direct proof) might be just what we need.

Example 91:

Problem: Prove or disprove: There exists an odd multiple of four.

Solution: This conjecture is clearly false, but let's pretend that it's more of a challenge.

Because this is an existential conjecture, to prove it we only need one example of an odd multiple of four to show that that conjecture is true. Enumeration of multiples of four $(\ldots -8, -4, 0, 4, 8, \ldots)$ doesn't help us find one, making us think that the conjecture may be false.

To show that the conjecture is false, we can either find a counter-example or prove the conjecture's negation. Finding a counter-example for an existential conjecture isn't easy, so we'll try to prove the negation. Let $O(x)$: x is an odd multiple of four.[20] In logic notation, our conjecture is $\exists x\ O(x)$, where $x \in \mathbb{Z}$. We can express its negation as a universal quantification: $\neg\exists x\ O(x) \equiv \forall x \neg O(x)$. In English: If x is a multiple of four, it's even. We can prove that easily.

Because the negation of the original conjecture is true, the conjecture must be false. The following write-up is more terse than was that of Example 90.

Disproof (Proof of the Negation): The given conjecture (an odd multiple of four exists) is false because its negation (all multiples of four are even) is true, as the following argument shows:

Proof (Direct): Let x be a multiple of four. $x = 4k$, $k \in \mathbb{Z}$. $x = 4k = 2(2k)$. Therefore, all multiples of four are even.

Disproofs, even those containing proofs, don't usually include much explanation.

These disproof techniques are independent of proof techniques. We placed the disproof section in this chapter because it makes sense to discuss disproofs soon after proofs are introduced, not because they can only be used with conjectures you first tried to prove with a direct proof.

[20] If you said to yourself, "Hey, that predicate should be expressed as multiple predicates!", you get an imaginary gold star. If you said that aloud in a public place, try to act like you don't care what other people think. To keep this example short(er), we're cheating on the predicate. Writing it out as multiple predicates, performing the negation, and rewriting the result in English should produce the result given above. But why take our word for it?

