Chapter 3

Proof

3.1 The Nature of Proof

We begin with a philosophical discussion on the nature of proof.

When a person is arrested for a crime and brought to trial, it is assumed that the prosecution has sufficient evidence for proving his guilt. What does this mean? It surely does not mean proved to a logical certainty. No matter how much evidence is presented against him, and no matter how likely his guilt may seem, it is always conceivable that he is innocent nonetheless.

As we have already seen, the same situation is true for science.

This lack of logical certainty is annoying, but the fact remains that decisions must be made and actions taken. If the prosecution presents evidence sufficient to convince twelve unbiased people of the suspect's guilt, we take his guilt to be proven. When scientists find that a theory has passed numerous empirical tests, it is taken as proved. We make do with something less than logical certainty in these contexts because there is no alternative.

Mathematicians, however, do have an alternative. In mathematics we demand logical proof.

All mathematical theorems are ultimately if-then statements. They may not be explicitly stated as such, but they invariably assert that if certain assumptions are granted, then certain consequences follow as a matter of logic.

Recall that an if-then statement is true unless its antecedent is true while its conclusion is false. To prove such a statement I need only show that once the antecedent is assumed to be true, the conclusion is seen to be true as well. In practice there are several ways of accomplishing this task, and that will be the subject of this chapter.

But perhaps there is a nagging doubt. Having had some prior experience with mathematics you are doubtless aware that theorems have a tendency to snowball. Simpler theorems are combined in clever ways to establish more complex theorems. Upon what, exactly, is this pile of theorems based? Surely there comes a time when a proposition is so simple that it can not be proven from anything simpler.

Indeed there does. Unravel the proof of any mathematical theorem and eventually you will find yourself with certain unproved assumptions at its foundation. What good is a logical proof if it is based on things we can not prove? After all, if our theorem is proved on the basis of assumptions that are not proved, why not simply assume the theorem to be true and be done with it?

The unproved assumptions underlying any branch of mathematics are called ***axioms*** or ***postulates***. Since we are stuck with the fact that such unproved statements are necessary, we can at least mitigate the damage by making the assumptions as simple and noncontroversial as possible. And while it is true that axioms are not proved, they are not arbitrary either. Rather, generally speaking, the axioms are chosen in such a way that they effectively describe whatever real-world structure they are intended to model.

For example, when Euclid laid out the assumptions that would underlie his system of geometry, he chose statements that seemed natural given the context in which he was working. He postulated things like “For any two points there is a straight line joining them”, which certainly seems reasonable. I should point out, however, that Euclid did not simply make up a set of axioms out of whole cloth just to see where they would lead. Typically it is only after a particular line of mathematical investigation has proven its worth that mathematicians set about writing down an explicit set of axioms for it. Thus, I suspect Euclid started with a large collection of seemingly plausible theorems, and then set about extracting from them the minimal assumptions upon which they were based. As later scholars pointed out, Euclid’s axioms did not adequately cover all of the assumptions he was making.

As a practical matter, the sorts of axioms that underlie familiar subjects like geometry are simple enough that no difficulty is caused by simply accepting them as true. The effectiveness of mathematics in describing the world is undeniable; I will leave it to the philosophers to explain why.

3.2 Synonyms for Theorem

If you spend some time perusing mathematics books, you will notice that statements to be proved come with a variety of labels. There are three that are especially important.

The most important among these labels is ***theorem***, from a Greek word meaning “to look at” or “study”. The building in which you look at a dramatic performance is called a theater, from the same root. Mathematicians use the word “theorem” to indicate a statement that is not only true, but important and surprising in some way. Of course, assessing the import and surprisal of a mathematical statement is a largely subjective process, so there is no hard and fast rule regarding which mathematical statements earn the theorem label.

A mathematical statement that is true but not especially interesting or surprising is often called a ***proposition***, from Latin words meaning “to put forward.” In this book we will be fairly casual about distinguishing between theorems and propositions.

Finally, a statement that is not so important by itself, but which provides the crucial ingredient in the proof of some more significant result, is called a ***lemma***. “Lemma” comes from a Greek word meaning “to grasp hold of”. The idea is that a lemma is something you grasp hold of as a tool for proving something more significant.

3.3 Direct Proof

We have already seen that conditional statements can be proved by assuming the antecedent to be true and showing that the conclusion must be true as well. Since such a proof consists of a series of deductions leading directly from our assumptions in the first line to the desired conclusion in the last, we refer to it as a ***direct proof*** .

Here is an example:

Proposition 1. *If x and y are even integers, then $x + y$ is even as well.*

Proof. Let us suppose that x and y are even integers. Then, by the definition of “even” we know there are integers a and b such that $x = 2a$ and $y = 2b$. It follows that

$$x + y = 2a + 2b = 2(a + b).$$

Thus, $x + y$ is a multiple of two, and is therefore even. $\square$

Let us take a moment to appreciate the form and structure of this proof. We began with a clearly labeled statement of what it is we seek to prove. Having stated the theorem clearly, we skip a line and clearly label the start of the proof. The proof concludes with a small square which is an indication to the reader that the proof is now over. Sometimes, when reading a piece of technical mathematics, you only care about the theorem itself and not its proof. The "end of proof" symbol makes it easier for the reader to skip over the proofs. If you ever find yourself slogging through a math book that does not use end of proof symbols, you will come to appreciate this simple courtesy.

Now examine the proof itself. In the first line we gave a clear statement of our assumptions, namely that we have two even integers. We named those numbers x and y, and made it very clear to our reader what those letters represent. Any time you introduce a variable into your proof, make sure you have clearly stated what that variable represents.

Our assumptions clearly stated and our notation defined, the time has come to construct the proof. I am given one piece of information: that x and y are even. My goal is to draw a conclusion about $x+y$. But what, precisely, does it mean to say x and y are even? It means they can be written as two times some other number. I called those numbers a and b and wrote $x = 2a$ and $y = 2b$. And from here we were able to find our way to the desired result.

From this we learn a critical lesson in writing proofs. As a first step write down the precise definitions of any mathematical jargon included in the statement of the theorem.

Here is another example:

Proposition 2. *The sum of any three consecutive integers is a multiple of three.*

In setting out to prove this we might begin by asking what, exactly, it means to describe a number as a multiple of three? How do we know a multiple of three when we see one? The multiples of three are the numbers $3, 6, 9, 12, \ldots$, and they are united by the fact that each can be written as three times some other number. Therefore, we will need to show that the sum of any three consecutive integers can be written as three times some other number.

Proof. Let x denote the second of the three consecutive integers. Then the number just before x is $x-1$ and the number immediately after x is $x+1$. Then we observe that

$$(x-1)+x+(x+1)=3x,$$

which is evidently a multiple of three. □

In this case we were given three consecutive integers. Thus, once we clearly identified one of the numbers we were able to write the other two in terms of it. The decision to set x equal to the second of the three numbers was a finesse that made our calculation a bit simpler. But suppose we had taken the more natural course of setting x equal to the smallest of the three numbers? In that case our three numbers would have been represented by x, $x+1$ and $x+2$, and their sum would have been $3x+3$. This is also a multiple of three.

And if we had set x equal to the largest of the three? Then we would have had $x-2$, $x-1$ and x, this time with a sum of $3x-3$. No matter how we start, we always end up with a multiple of three.

3.4 Conjectures and Counterexamples

Sometimes mathematicians are confronted with an unproved statement that appears true nonetheless. In such a situation they may assert their belief in the truth of the statement, perhaps in the hope of encouraging other mathematicians to supply the missing proof. Such statements are referred to as ***conjectures***. If a conjecture is subsequently proved to be true, it becomes a theorem. A really deep conjecture might be around for many years before a proof is found. When such a conjecture is proved, it reflects well on the person who first formulated it.

Modern mathematics is chock full of conjectures, many of which are too complicated to describe here. Here is one that is not: It has been observed that there are many pairs of prime numbers whose difference is two. Examples include the pairs 3 and 5, 11 and 13, 29 and 31, and 101 and 103. These pairs are known as ***twin primes***, and it has been conjectured that there are infinitely many such pairs. Nobody knows for certain, however.

Another example involves ***perfect*** numbers. By this we mean a number that is equal to the sum of its proper divisors (meaning we do not count the number itself as one of its divisors). Examples are 6, which is equal to $1+2+3$ and 28 which is equal to $1+2+4+7+14$. Every perfect number known to date is even. Are there any odd perfect numbers? The conjecture is that there are not any. Resolving this question one way or another will assure you of a nice career in mathematics.

Let us suppose that the conjecture is false, and that someone produces a number x that is both odd and a perfect number. The number x would then be a ***counterexample*** to the conjecture. By this we mean it is an example that shows that particular conjecture is false. If someone asserts that all crows are black, then a single non-black crow will serve as a counterexample.

As another example, suppose I believe that if x, y and z are three distinct prime numbers then their sum is odd. For supporting evidence I point out that this is often the case. For example, $3+5+7=15$ which is odd and $11+17+23=51$ which is also odd. In fact, I could produce many more cases for which my conjecture is true. But then someone comes along and points out that $2+3+5=10$. Since 2, 3 and 5 are all primes and their sum is even, I have produced a counterexample to my conjecture.

So my conjecture was false. What do I do now? Let us look more closely at our counterexample. It involved the prime 2, and this is a strange prime indeed. It is the only prime number that is even. To exclude the possibility of invoking this particular prime, suppose I revise my conjecture to state, "If x, y and z are distinct, odd primes, then their sum is odd." Now the conjecture is true, as can be seen by observing that the sum of any three odd numbers must be odd.

Though a counterexample disproves a proposed conjecture, it can still help point us in the right direction.

3.5 Conditionals Revisited

Before proceeding with our examination of different methods of proof, we pause to give some further thought to the nature of conditional statements.

The statement $P \rightarrow Q$ asserts that if proposition P is true, then proposition Q must be true as well. There are three other if-then statements related to this assertion, each bearing a different name:

1. The statement $Q \rightarrow P$ is called the ***converse*** of $P \rightarrow Q$.

2. The statement $\neg P \rightarrow \neg Q$ is called the ***inverse*** of $P \rightarrow Q$.

3. The statement $\neg Q \rightarrow \neg P$ is called the ***contrapositive*** of $P \rightarrow Q$.

In the converse we reverse the roles of P and Q, in the inverse we negate both of them, and in the contrapositive we both switch and negate them. If you prefer, the inverse could be described as the contrapositive of the converse. For that matter, the contrapositive is the inverse of the converse.

The converse of the statement "If Spot is a healthy dog then Spot has four legs" is the statement "If Spot has four legs then Spot is a healthy dog." As we saw in chapter two, the converse is false in this case, since Spot could be a cat. On the other hand, the original statement is true. From this we conclude that an if-then and its converse are not logically equivalent.

The inverse of our sentence is "If Spot is not a healthy dog then Spot does not have four legs." Like the converse before it, this statement is clearly false. Consequently, a statement and its inverse are logically distinct.

The contrapositive of our statement is "If Spot does not have four legs then Spot is not a healthy dog." This statement is true. In fact a conditional and its contrapositive are logically equivalent. Recall that this means the statement

$$(P \rightarrow Q) \leftrightarrow (\neg Q \rightarrow \neg P)$$

is a tautology. This is easily shown by constructing its truth table.

It follows that to prove the statement $P \rightarrow Q$ it is sufficient to prove the statement $\neg Q \rightarrow \neg P$. Thus, to prove the statement "All crows are black," it is sufficient to prove that "All non-black things are not crows." An amusing approach to the problem, if not very practical.

3.6 Proof by Contrapositive

Actually, it often happens that while $P \rightarrow Q$ is the statement we are interested in, its contrapositive $\neg Q \rightarrow \neg P$ is easier to prove. Here is an example:

Theorem 1. *Let x be a positive integer. If x^2 is even, then x is even.*

Proof. Assume x is a positive integer. We will prove the contrapositive, namely "If x is not even, then x^2 is not even." Of course, this is equivalent to saying that if x is odd then so is x^2.

Since we are assuming x is odd, we can find an integer a such that $x = 2a + 1$. Then

$$x^2 = (2a+1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1.$$

This shows that x^2 is one more than a multiple of two, which implies that it is odd. The proof is complete. □

Proving the statement directly would require starting with a perfect square and drawing a conclusion about its square root. This is possible, but far trickier than the method we employed above. So why did we not just say "If x is odd then x^2 is odd," in the first place? We presented the theorem in the form we did because this is precisely the way we will use it in the next section.

3.7 Proof by Contradiction

A **contradiction** is a statement that is never true. Equivalently, a contradiction is the negation of a tautology.

Let us suppose that some statement of the form $P \wedge \neg Q$ is a contradiction. This implies that if P is true, then $\neg Q$ must be false. If $\neg Q$ and P were simultaneously true, then the conjunction $P \wedge \neg Q$ would be true as well, you see. Since $\neg Q$ is false, we know that Q is true.

As a consequence we see that if $P \wedge \neg Q$ is a contradiction, then assuming P to be true implies that Q is true as well. In other words, the conditional statement $P \to Q$ must be true. Now reverse the situation. If we want to prove that the statement $P \to Q$ is true, we can do that by showing that $P \wedge \neg Q$ is a contradiction.

This technique is appropriately known as ***proof by contradiction***, and it is one of the most useful proof techniques in mathematics. In carrying out such a proof, you begin by assuming the statement to be proved is false. You then show this leads to a logical contradiction. By the law of the excluded middle, this tells us that our statement is true.

We will now consider two of the most famous proofs by contradiction in all of mathematics. Both of them were first proved by Euclid over two millenia ago. I, for one, find it comforting that they are still true today. The great British mathematician Godfrey Hardy, when seeking two prime examples of mathematical beauty, chose these two theorems. Let me suggest that if you can look at these proofs and see nothing clever or interesting about them, then mathematics may not be the subject for you.

Theorem 2. *If x is a number satisfying $x^2 = 2$, then x is irrational.*

Of course, this is just a fancy way of saying that $\sqrt{2}$ is irrational. I have phrased it the way that I have to make explicit the fact that this is an if-then statement.

Carrying out a proof by contradiction requires that I begin by assuming my theorem is false. Since an if-then statement is false only when the antecedent is true and the conclusion is false, I will assume that $x^2 = 2$ and that x is rational. Let us see where this leads.

Proof. Let us suppose that x is a rational number satisfying $x^2 = 2$. Since x is rational, I can find integers p and q such that $x = \frac{p}{q}$. Since every fraction can be put into lowest terms, I can assume that p and q do not have a common factor.

Since we are assuming that $x^2 = 2$, we know that $\dfrac{p^2}{q^2} = 2$. This implies that $p^2 = 2q^2$. Since p^2 is equal to two times another integer, we see that p^2 is even. By the theorem that we proved in the previous section, we know this implies that p is even as well.

Since p is even we know there is some integer, call it a, such that $p = 2a$. It follows that

$$p^2 = (2a)^2 = 4a^2.$$

But since we also know that $p^2 = 2q^2$ we have that $2q^2 = 4a^2$. Dividing both sides by two leaves us with $q^2 = 2a^2$. This implies that q^2 is even, and consequently that q is even as well.

Therefore, p and q are both even, which implies that each is a multiple of two. But this contradicts our assumption that p and q did not have any common factors. Since our assumption that x is rational has led to a contradiction, we conclude that x must be irrational. □

Before moving on to our second example, let me remind you of a famous result called the Fundamental Theorem of Arithmetic:

Theorem 3. *Every positive integer greater than one is either prime or can be written as the product of prime numbers. This factorization is unique up to the order of the factors.*

For example, the number $60 = (2^2)(3)(5)$, where two, three and five are all prime. When we say the factorization is unique up to the order of the factors, we mean that the factorization $(2^2)(3)(5)$ should be considered identical to the factorization $(3)(2^2)(5)$, for example. Once that is understood, there is only one way to write any particular integer as the product of prime numbers.

We will not stop to prove this now.

Theorem 4. *There are infinitely many prime numbers*

Proof. We will prove this by contradiction. Let us suppose the theorem is false. Then there are only finitely many prime numbers. That means we could write down a list containing all of the prime numbers. Assume there are exactly k prime numbers. We will denote the k primes by $p_1, p_2, \ldots, p_k$.

Now define the number N as follows:

$$N = p_1 p_2 p_3 \ldots p_k + 1.$$

In other words, multiply all of the prime numbers together, add one, and call the resulting number N.

The number N is larger than any number on our list of primes. If N were prime, it would be a prime number that is not on our list, which is a contradiction. Consequently, we must have that N is not prime.

The fundamental theorem of arithmetic then tells us that there must be some prime number that divides N. Since the list $p_1, p_2, \ldots, p_k$ contains all the prime numbers there are, it follows that N is divisible by one of these primes. But N actually leaves a remainder of one when divided by any of the primes on the list. This is a contradiction.

It follows that there must be infinitely many prime numbers, and the proof is complete. □

3.8 Proof by Cases

Consider the following theorem:

Proposition 3. *In any collection of three consecutive odd numbers there is at least one multiple of three.*

Proof. Let x denote the smallest of the three odd numbers. Then x leaves a remainder of either 0, 1 or 2 when divided by three. We will consider each case separately.

Case One: Suppose x leaves a remainder of 0 when divided by three. This is equivalent to saying that x is a multiple of three and we are done.

Case Two: Suppose x leaves a remainder of 1 when divided by three. Then there is some integer a such that $x = 3a + 1$, because that is what it means to leave a remainder of one when divided by three. In this case, the next odd number after x is

$$x + 2 = (3a + 1) + 2 = 3a + 3 = 3(a + 1).$$

This shows that the second of our three numbers is a multiple of three and again we are done.

Case Three: Suppose x leaves a remainder of 2 when divided by three. Then there is some integer b such that $x = 3b + 2$. The next odd number after x is $x + 2$ and the next one after that is $x + 4$. Then we have that

$$x + 4 = (3a + 2) + 4 = 3a + 6 = 3(a + 2).$$

This shows that the third of our three numbers is a multiple of three.

Since these three cases exhaust all the possibilities, and in each case we find that we have at least one multiple of three, the proof is complete. □

The difficulty in proving this theorem lies in the fact that we have so little information with which to work. We are given three consecutive odd numbers and must draw some conclusion regarding the remainders they leave when divided by three. An unpromising state of affairs, to be sure.

But then we notice that every integer falls into exactly one of three categories according to the remainder it leaves upon division by three. After arbitrarily setting x to be the smallest of the three numbers, we considered each case individually. In each case we discovered there must be some multiple of three among our consecutive odd numbers.

This is known as a proof by cases, and it is a surprisingly useful method of attack. You may find that hard to believe. After all, it seems you are replacing the need for one proof with the need for many proofs, one for each case. What have we gained by adding this extra complication?

Well, it often happens when constructing a proof that you have too little information to work with. By breaking up all the possibilities into separate cases, we gain a little more leverage over the problem. By this I mean that in each case we are given an added assumption, an extra piece of information, to work with. In this case by considering different cases I was able to obtain an algebraic expression for each of my numbers. This was just the tool I needed to deduce there was some multiple of three among them.

Sadly, we really must mention a common error made in constructing proofs by cases. In delineating your cases, careful thought is required to ensure that every possible case really has been considered. Omitting even one possibility is the difference between proving your theorem, and proving nothing.

Let us close this section with one further example:

Proposition 4. *Every perfect square leaves a remainder of zero or one when divided by four.*

Proof. Let $2k$ be an arbitrary even number. If we square it we get $4k^2$, which is a multiple of four. Consequently, it leaves a remainder of zero when divided by four.

Now let $2\ell + 1$ be an arbitrary odd number. This time squaring it gives us: $4\ell^2 + 4\ell + 1 = 4(\ell^2 + \ell) + 1$. This number leaves a remainder of one when divided by four.

Let x be a perfect square. Then the positive square root of x is either even or odd. If it is even, then x must be multiple of four. If it is odd, then x must leave a remainder of one when divided by four. Since this exhausts all the possibilities, the proof is complete. □

3.9 Existence Proofs

Many mathematical theorems merely assert that something exists, a number having certain given properties for example, and we need methods for proving such statements. We consider two such methods in this section.

One especially effective method is to produce the desired object for your readers. For example:

Proposition 5. *There exists a number that can be written as the sum of two cubes in two different ways.*

Proof. Consider the number 91. It is a simple computation to show that

$$91 = (4^3) + (3^3) = (6^3) + (-5)^3.$$

We see that 91 is a number that can be written as the sum of two cubes in two different ways and the proof is complete. □

Please notice that nothing in the statement of this theorem required me to restrict my attention to positive cubes. In proving theorems it is crucial that you do not impose unnecessary restrictions on yourself. As it happens, this theorem would remain true even if I had restricted my attention to positive cubes. Give careful consideration to the number 1729 if you do not believe me.

There are other cases where it is not possible to produce the desired object. Often, however, it is still possible to prove that the object exists, as we see in the next example. Let me remind you that a basic rule for manipulating exponents states that

$$(a^b)^c = a^{bc}.$$

Proposition 6. *There exist irrational numbers x and y with the property that x^y is a rational number.*

Proof. We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. If this number is rational, then set $x = y = \sqrt{2}$. In this case x and y are both irrational, but x^y is rational.

Now suppose that $\sqrt{2}^{\sqrt{2}}$ is irrational. In this case set $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We now carry out the following computation:

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2.$$

Since this is rational, we have found the numbers we seek. □

Notice that we effectively used a proof by cases here. We do not know which case actually occurs, but we can obtain our desired result regardless.

3.10 Proofs and Tautologies

How do the various proof techniques we have considered so far relate to the ideas introduced in the previous chapter?

Ultimately, all proofs are based on tautologies. In a direct proof we seek to prove the statement $P \to R$ by assuming P to be true and constructing a chain of deductions that ultimately conclude with R. The logical basis for this is that the statement

$$[(P \to Q) \land (Q \to R)] \to (P \to R)$$

is a tautology, as can be seen by constructing a truth table. In plain English, this proposition says, "If P implies Q, and Q implies R, then P implies R."

In a proof by contradiction we prove $P \to Q$ by showing that $P \land \neg Q$ is a contradiction. This works because

$$(P \to Q) \leftrightarrow \neg(P \land \neg Q)$$

is a tautology.

Finally, a proof by cases is based on the fact that

$$[(P \lor Q) \to R] \leftrightarrow [(P \to R) \land (Q \to R)]$$

is a tautology. Here, P and Q are the cases and R is the statement we seek to prove. On the right-hand side we are saying that each of the cases P and Q independently imply R. Therefore, as long as we know that at least one of the cases must hold true, we can be sure that R is true as well.

On the other hand, there are many statements that seem like tautologies, but in fact are not. Arguments based on such statements will not be valid. One such example is the statement

$$[(P \to Q) \land Q] \to P.$$

This proposition is asserting that if we know that Q is true, and we also know that P implies Q, then we conclude that P is true as well. This statement is false when P is false and Q is true, so it is not a tautology. This is known as ***the fallacy of affirming the conclusion***. If I say "If it rains, then I will go to the movies," and later you find out that I did go to the movies, you would be wrong to conclude that it rained. It is possible that I went to the movies for some reason other than the rain.

A related error is ***the fallacy of denying the antecedent*** which looks like this:

$$[(P \to Q) \land \neg P] \to \neg Q.$$

This proposition asserts that if we know P is false, and we also know P implies Q, then we can conclude that Q is false as well. This statement will be false whenever Q is true and P is false, so it is not a tautology. Again, the error is easy to spot in a concrete example. Using the same example as before, you would be wrong to conclude that just because it did not rain I did not, nevertheless, go to the movies.

3.11 Problem Solving Skills

3.11.1 How Do You Construct a Proof?

When confronted with a mathematical conjecture, you have only your own experience and ingenuity to guide you in finding a proof. Sadly, there is no procedure to carry out that will tell you which method of proof to use, or how to begin your logical journey from "what you know" to "what you want". There are, however, certain guidelines and rules of thumb that can come to your aid.

The first step in almost any proof is to translate the given information into precise mathematical statements. For example, in proving that the sum of two even numbers is always even, we began by writing down $x = 2a$ and $y = 2b$. Why did we do this? Well, the fact that we are given two even integers is not so useful by itself. There is nothing there to manipulate; nothing there that suggests what to do next. But once we have $x = 2a$ and $y = 2b$, it was the most natural thing in the world to add them together to get $2a + 2b$.

Another example came in our proof of the irrationality of the square root of two. In this case we might reason that the only alternative to being irrational is being rational. Furthermore, rational numbers are precisely the ones that can be written in the form $\frac{p}{q}$, where p and q are integers. And once I have an algebraic expression like $\sqrt{2} = \frac{p}{q}$, certain common manipulations suggest themselves.

How natural that seems to you will depend on how comfortable you are thinking precisely about mathematical terminology. The connection between "even" and "can be written as two times some other integer" needs to be automatic. Similarly with the connection between "sum" and "the result of adding two numbers", or "rational" and "can be written as $\frac{p}{q}$ where p and q are integers." Thinking about mathematical terminology with this level of precision is something that comes with practice.

The table below shows some especially common bits of terminology and how to translate them into useful algebraic expressions. Throughout the table, k, p and q denote arbitrary positive integers:

Mathematical Terminology	**Algebraic Expression**
x is an even number	$x = 2k$
x is an odd number	$x = 2k + 1$
x is a multiple of three	$x = 3k$
x is a multiple of n	$x = nk$
x is a rational number	$x = \frac{p}{q}$
x leaves a remainder of 2 when divided by 3	$x = 3k + 2$
x leaves a remainder of p when divided by q	$x = kq + p$
x divides y	$y = kx$
x is the sum or difference of two squares	$x = p^2 + q^2$ or $x = p^2 - q^2$
x is the average of p and q	$x = \frac{p+q}{2}$

There are also certain algebraic manipulations that frequently turn out to be useful. For example, when confronted with an equation that involves fractions, it is usually a good idea to clear the denominators. Also, square root signs can be eliminated by squaring both sides of an equation. We saw both of these techniques at work when we proved the irrationality of the square root of two. There we started with the equation $\sqrt{2} = \frac{p}{q}$ and quickly rewrote it as $2p^2 = q^2$. First we squared both sides to get rid of the radical, then we cleared denominators by multiplying both sides of the equation by q^2.

Here's another example of these techniques at work:

Proposition 7. *Let a and b be positive real numbers. Then*

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Furthermore, equality holds if and only if $a = b$.

The expression on the left is no doubt familiar to you. It is the ***average*** or ***arithmetic mean*** of the two numbers. The expression on the right is called the ***harmonic mean*** of the two numbers.

Notice that nothing in the first part of the proposition said that a and b had to be two different numbers. We said only that they were positive. This is another good lesson in avoiding unwarranted assumptions.

There is something else you should notice about the structure of this proposition. We are asserting that a certain inequality is always true, namely that the arithmetic mean of two numbers is not smaller than the harmonic mean. But we are also leaving open the possibility that the two quantities are equal. In such a situation a mathematician finds it natural to wonder what conditions need to be satisfied in order for equality to hold. Apparently, this happens only when $a = b$. It is easy to see that if we assume that $a = b$ then the two expressions really are equal. So we are asserting that it is only in the obvious case that the two expressions are equal.

Proof. Let a and b be two positive real numbers. The inequality

$$\frac{a+b}{2} \geq \sqrt{ab}$$

is equivalent to the inequality

$$(a+b)^2 \geq 4ab.$$

By this we mean that the first inequality is true if and only if the second one is true. The second inequality is equivalent to

$$a^2 + 2ab + b^2 \geq 4ab.$$

We can manipulate this to get

$$a^2 - 2ab + b^2 \geq 0.$$

The expression on the left hand side is equal to $(a-b)^2$. Since perfect squares are always positive, we see this inequality is true. It follows that the original inequality is true as well.

Furthermore, the only time the expression $(a-b)^2$ is equal to zero is when $a = b$. This establishes the second part of the proposition. □

To prove this proposition we used a combination of straightforward algebra, and the realization that perfect squares are always nonnegative. Many other propositions can be solved in a similar manner.

3.11.2 Writing Proofs

Figuring out the ideas that go into a given proof is only half the battle. The other half is writing your ideas down in a way that will make sense to another mathematician. There are two key things to keep in mind in that regard: precision and efficiency.

By precision we mean that your thoughts must be expressed in an entirely unambiguous way. For example, let's revisit our proposition about the sum of two even numbers always being even. Consider the following attempt at a proof:

Proof. An even number is a number with a two in it. If you add together two numbers, each of which has a two in it, then their sum must have a two in it as well. This shows that the sum is even and the proof is complete. □

The person who wrote this evidently had the right idea. The trouble is that the phrase "has a two in it" does not actually mean anything. It captures in an intuitive sort of way what it means to be even, but it is too imprecise to be useful to someone reading this proof. Furthermore, there is nothing in this proof to justify the assertion that the sum under consideration really does "have a two in it", whatever that means.

The way we actually proved it went like this:

Proof. Suppose that x and y are even. Then there are integers a and b such that $x = 2a$ and $y = 2b$. It follows that $x+y = 2a+2b = 2(a+b)$. This shows that the sum of x and y is a multiple of two, and therefore it is even. □

There is nothing left to the imagination there. We have made explicit the intuitive notion that even numbers "have a two in them", and we have also shown algebraically that the sum of the two numbers really is even.

This brings us to efficiency. In writing up a proof, it is important that you have no wasted words. Every sentence either needs to move the proof forward in some way, or it needs to provide some comment that will help your reader follow your reasoning. Generally, your sentences should be short. A good rule of thumb is "One thought, one sentence." If you find that you have an excessive number of commas in one of your sentences, you should probably break it up into several pieces.

I think you will find that if you remember the importance of precision and efficiency, you will find it a lot easier to get the hang of writing proofs. You just need to have the courage to pursue a line of investigation without knowing where it will lead, and the confidence that your mathematical skills are up to the task.

3.12 Problems

Prove each of the following statements. Recall that if x is a real number, then $|x|$ is equal to x if x is positive and is equal to $-x$ if x is negative. The quantity $|x|$ is called the ***absolute value*** of x.

1. The sum of an even number and an odd number is odd.

2. The product of two odd numbers is again odd.

3. If x and y are integers and xy is odd, then $x + y$ is even.

4. Every even perfect square is a multiple of four.

5. Every even nth power is a multiple of 2^n.

6. The sum of two multiples of five is another multiple of five. The product of two multiples of five is a multiple of twenty-five.

7. Every perfect cube is either a multiple of nine, one more than a multiple of nine, or one less than a multiple of nine.

8. If n baseball teams play $2n - 1$ games, then there is at least one team that played more than one game.

9. Two distinct straight lines are either parallel or intersect at one point. (Hint: Remember that a nonvertical straight line has an equation of the form $y = mx + b$.)

10. If x is a positive real number, then $x + \frac{1}{x} \geq 2$.

11. If x and y are positive real numbers, then $\sqrt{x + y} \leq \sqrt{x} + \sqrt{y}$.

12. If a, b and c are integers such that a divides b and b divides c, then a divides c. (Hint: Recall that the precise definition of "divides" is, "x divides y if there is some integer k such that $xk = y$.

13. If x is a perfect square then x has an odd number of divisors. (For example, 9 is a perfect square. Its divisors are 1, 3 and 9 for a total of three, which is odd. The divisors of 16 are 1, 2, 4, 8 and 16, for a total of five, which is again odd.

14. If x and y are real numbers such that $x > 5$ and $y > 3$, then the area of the rectangle with corners (x, y), $(x, -y)$, $(-x, y)$, and $(-x, -y)$ is greater than 60. (Hint: Plot these four points on a set of coordinate axes).

15. The $\sqrt{3}$ is irrational.

16. The $\sqrt[3]{3}$ is irrational.

17. If p is prime, then $\sqrt{p}$ is irrational.

18. If a, b and c are odd integers, then $ax^2 + bx + c = 0$ has no rational solutions. (Hint: Proceed by contradiction. Suppose that $\frac{p}{q}$ were a rational solution, in lowest terms, to this equation. Do some algebra to get rid of the denominators. Then determine whether p or q are even or odd.)

19. If x and y are real numbers, then $|xy| = |x||y|$.

20. If x and y are real numbers, then $|x + y| \leq |x| + |y|$. Under what conditions will equality hold?