2. Methods of Proof

2.1. Types of Proofs. Suppose we wish to prove an implication $p \to q$. Here are some strategies we have available to try.

- **Trivial Proof:** If we know q is true then $p \to q$ is true regardless of the truth value of p.
- **Vacuous Proof:** If p is a conjunction of other hypotheses and we know one or more of these hypotheses is false, then p is false and so $p \to q$ is vacuously true regardless of the truth value of q.
- **Direct Proof:** Assume p, and then use the rules of inference, axioms, definitions, and logical equivalences to prove q.
- **Indirect Proof or Proof by Contradiction:** Assume p and $\neg q$ and derive a contradiction $r \wedge \neg r$.
- **Proof by Contrapositive:** (Special case of Proof by Contradiction.)
  Give a direct proof of $\neg q \to \neg p$. Assume $\neg q$ and then use the rules of inference, axioms, definitions, and logical equivalences to prove $\neg p$.(Can be thought of as a proof by contradiction in which you assume p and $\neg q$ and arrive at the contradiction $p \wedge \neg p$.)
- **Proof by Cases:** If the hypothesis p can be separated into cases $p_1 \vee p_2 \vee \cdots \vee p_k$, prove each of the propositions,
  $p_1 \to q$, $p_2 \to q$, $\ldots$, $p_k \to q$, separately.
  (You may use different methods of proof for different cases.)

Discussion

We are now getting to the heart of this course: methods you can use to write proofs. Let's investigate the strategies given above in some detail.

2.2. Trivial Proof/Vacuous Proof.

EXAMPLE 2.2.1. *Prove the statement: If there are 100 students enrolled in this course this semester, then* $6^2 = 36$.

PROOF. The assertion is *trivially* true, since the conclusion is true, independent of the hypothesis (which, may or may not be true depending on the enrollment). □

EXAMPLE 2.2.2. *Prove the statement. If 6 is a prime number, then* $6^2 = 30$.

PROOF. The hypothesis is false, therefore the statement is *vacuously* true (even though the conclusion is also false).

□

Discussion

The first two methods of proof, the "Trivial Proof" and the "Vacuous Proof" are certainly the easiest when they work. Notice that the form of the "Trivial Proof", $q \to (p \to q)$, is, in fact, a tautology. This follows from disjunction introduction, since $p \to q$ is equivalent to $\neg p \vee q$. Likewise, the "Vacuous Proof" is based on the tautology $\neg p \to (p \to q)$.

EXERCISE 2.2.1. *Fill in the reasons for the following proof of the tautology* $\neg p \to (p \to q)$.

$$\begin{aligned}[\neg p \to (p \to q)] &\Leftrightarrow [p \vee (\neg p \vee q)] \\ &\Leftrightarrow [(p \vee \neg p) \vee q] \\ &\Leftrightarrow T \vee q \\ &\Leftrightarrow T\end{aligned}$$

EXERCISE 2.2.2. *Let* $A = \{1, 2, 3\}$ *and* $R = \{(2, 3), (2, 1)\}(\subseteq A \times A)$. *Prove: if* $a, b, c \in A$ *are such that* $(a, b) \in R$ *and* $(b, c) \in R$ *then* $(a, c) \in R$.

Since it is a rare occasion when we are able to get by with one of these two methods of proof, we turn to some we are more likely to need. In most of the following examples the underlying "theorem" may be a fact that is well known to you. The purpose in presenting them, however, is not to surprise you with new mathematical facts, but to get you thinking about the correct way to set up and carry out a mathematical argument, and you should read them carefully with this in mind.

2.3. Direct Proof.

EXAMPLE 2.3.1. *Prove the statement: For all integers* m *and* n, *if* m *and* n *are odd integers, then* $m + n$ *is an even integer.*

PROOF. Assume m and n are arbitrary odd integers. Then m and n can be written in the form

$$m = 2a + 1 \text{ and } n = 2b + 1,$$

where a and b are also integers. Then

$$\begin{aligned} m+n &= (2a+1)+(2b+1) && \text{(substitution)} \\ &= 2a+2b+2 && \text{(associative and commutative laws of addition)} \\ &= 2(a+b+1) && \text{(distributive law)} \end{aligned}$$

Since $m+n$ is twice another integer, namely, $a+b+1$, $m+n$ is an even integer. □

Discussion

The first strategy you should try when attempting to prove any assertion is to give a direct proof. That is, assume the hypotheses that are given and try to argue directly that the conclusion follows. This is often the best approach when the hypotheses can be translated into algebraic expressions (equations or inequalities) that can be manipulated to give other algebraic expressions, which are useful in verifying the conclusion.

Example 2.3.1 shows a simple direct proof of a very familiar result. We are using the familiar definitions of what it means for an integer to be even or odd: An integer n is *even* if $n = 2k$ for some integer k; an integer n is *odd* if $n = 2k + 1$ for some integer k. Study the *form* of this proof. There are two hypotheses, "m is an odd integer," and "n is an odd integer"; and the conclusion is the statement "$m + n$ is an even integer." This "theorem" is a quantified statement ("for all integers m and n", or "for all odd integers m and n"). In the proof we assumed the hypotheses held for arbitrarily integers m and n, and then we wrote down equations that follow from the definition of what it means for these integers to be odd. Although this looks like a pretty obvious thing to do, at least when you see someone else do it, this step, in which you bring your knowledge to the problem, may seem like a big one to take, and you may find yourself stalling out at this point.

One possible reason this may happen is that you may be trying to do too much at once. The cure for this is to be patient: take small steps, using the appropriate definitions and previously proven facts, and see where they lead. When we wrote down $m = 2a + 1$ and $n = 2b + 1$, we did a number of fairly sophisticated things. First, we used our knowledge (definitions) of what it means for an integer to be odd. Second, in order for this information to be useful, we needed to translate this knowledge into a mathematical expression, or expressions in this case, that are subject to manipulation. And third, in setting up these expressions, we needed to use *appropriate* mathematical notation, so that we did not introduce any subtle or hidden relationships into the picture that are unwarranted by the hypotheses.

A common mistake of this type might arise as follows:

> "Well, m is an odd integer, so I can write $m = 2k + 1$, where k is an integer. Since n is also an odd integer, I can write $n = 2k + 1$, where k is an integer."

Do you see the mistake? By allowing the same letter k to represent what might be different integers, we have inadvertently added another assumption, namely, that $m = n$! Of course, we didn't mean to do this, but, unfortunately, our intentions haven't been carried out, and so our proof breaks down at this point. In order to maintain the "arbitrariness" of m and n, we must allow, at the least, that they be different. We accomplish this by choosing different letters a and b in our representations of m and n as "twice an integer plus one." There is nothing sacred about a and b; we could have used k and ℓ, or x and y, or α and β, or any pair of symbols that have not been appropriated for some other use.

Upon closer scrutiny, this first step now starts to seem like a big one indeed! Especially if we may not be sure just where it will lead. The rest of the proof, however, proceeds fairly routinely. We add m and n and observe that the resulting expression has a factor of 2. We now only have to get past the *recognition problem*: observing that the resulting expression gives us what we were looking for. Since we have expressed $m + n$ as twice another integer, $m + n$ is, by definition, an even integer. By Universal Generalization we may now confidently declare "Q.E.D." (the abbreviation of *quod erat demonstrandum* or "which was to be demonstrated"). Often a box at the end of a proof or the abbrviation "Q.E.D." is used at the end of a proof to indicate it is finished.

EXERCISE 2.3.1. *Give a careful proof of the statement: For all integers m and n, if m is odd and n is even, then $m + n$ is odd.*

2.4. Proof by Contrapositive.

EXAMPLE 2.4.1. *Prove the statement: For all integers m and n, if the product of m and n is even, then m is even or n is even.*

We prove the contrapositive of the statement: If m and n are both odd integers, then mn is odd.

PROOF. Suppose that m and n are arbitrary odd integers. Then $m = 2a + 1$ and $n = 2b + 1$, where a and b are integers. Then

$$\begin{aligned} mn &= (2a+1)(2b+1) && \text{(substitution)} \\ &= 4ab + 2a + 2b + 1 && \text{(associative, commutative, and distributive laws)} \\ &= 2(2ab + a + b) + 1 && \text{(distributive law)} \end{aligned}$$

Since mn is twice an integer (namely, $2ab + a + b$) plus 1, mn is odd. □

Discussion

If a direct proof of an assertion appears problematic, the next most natural strategy to try is a proof of the contrapositive. In Example 2.4.1 we use this method to prove that if the product of two integers, m and n, is even, then m or n is even. This statement has the form $p \to (r \vee s)$. If you take our advice above, you will first try to give a direct proof of this statement: assume mn is even and try to prove m is even or n is even. Next, you would use the definition of "even" to write $mn = 2k$, where k is an integer. You would now like to conclude that m or n has the factor 2. This can, in fact, be proved directly, but it requires more knowledge of number theory than we have available at this point. Thus, we seem to have reached a dead-end with the direct approach, and we decide to try an indirect approach instead.

The contrapositive of $p \to (r \vee s)$ is $\neg(r \vee s) \to \neg p$, or, by De Morgan's Law,

$$(\neg r \wedge \neg s) \to \neg p.$$

This translates into the statement

"If m and n are odd, then mn is odd"

(where "not even" translates to "odd"). This is a good illustration of how the symbolic form of a proposition can be helpful in finding the correct statement we wish to prove. In this particular example, the necessity of De Morgan's Law may be more evident in the symbolic form than in the "English version."

Now we give a *direct* proof of the contrapositive: we assume m and n are arbitrary odd integers and deduce mn is odd. This proof is carried out in very much the same way as the direct proof in Example 2.3.1. The main difficulty we encounter with the problem of proving the original assertion is to realize that a direct proof should be abandoned in favor of some other strategy.

Exercise 2.4.1. *The following statement is a special case of the proposition proved in Example 2.4.1. Give a careful proof of this statement without assuming the result in Example 2.4.1.*

For every integer n, if n^2 is even, then n is even.

2.5. Proof by Contradiction.

EXAMPLE 2.5.1. *Prove the statement is true: Let x and y be real numbers. If $5x + 25y = 1723$, then x or y is not an integer.*

PROOF. Assume x and y are real numbers such that $5x+25y = 1723$, and assume that both x and y are integers. By the distributive law,

$$5(x + 5y) = 1723.$$

Since x and y are integers, this implies 1723 is divisible by 5. The integer 1723, however, is clearly not divisible by 5. This contradiction establishes the result. □

Discussion

If we have tried unsuccessfully to find a direct proof of a statement or its contrapositive, we might next try to give a proof by contradiction. In this method of proof we assume the hypotheses are true and the conclusion is false and try to arrive at a contradiction. The validity of proof by contradiction follows from the fact that $\neg(p \wedge \neg q)$ is equivalent to $p \to q$: if we can show that $p \wedge \neg q$ is false, then $\neg(p \wedge \neg q)$ is true, so that the equivalent proposition $p \to q$ is also true.

In Example 2.5.1 we are asked to prove that if $5x + 25y = 1723$, then x is not an integer or y is not an integer. This has the same propositional form as the example in Example 2.4.1:

$$p \to (r \vee s).$$

If we try to give a direct proof of this statement, then we are forced to "prove a negative," which can be difficult. If we try to prove the contrapositive, then knowing that x and y are integers doesn't seem to be helpful in trying to show directly that $5x + 25y \neq 1723$, since we are again trying to prove a negative.

On the other hand, if we assume p and $\neg(r \vee s)$, which is equivalent to $\neg r \wedge \neg s$, then we have two positive statements to work with: $5x+25y = 1723$, and x and y are integers. After a couple of observations we arrive at the contradiction $r \wedge \neg r$, where r is the statement "1723 is divisible by 5." This contradiction establishes the truth of the statement, and we are through.

EXERCISE 2.5.1. *Prove: For all real numbers x and y, if $35x + 14y = 253$, then x is not an integer or y is not an integer.*

Here is another example of a proposition that is best proved by contradiction.

EXAMPLE 2.5.2. *For all positive real numbers a, b, and c, if $ab = c$, then $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$.*

PROOF. Suppose a, b, and c are positive real numbers such that $ab = c$, and suppose $a > \sqrt{c}$ and $b > \sqrt{c}$. (Notice the use of De Morgan's Law again. Also, recall that the symbol $\sqrt{c}$ represents the *positive* square root of c, not $\pm\sqrt{c}$.) By order properties of the real numbers,

$$b > \sqrt{c} \Leftrightarrow ab > a\sqrt{c}, \text{ since } a > 0,$$

and

$$a > \sqrt{c} \Leftrightarrow a\sqrt{c} > \sqrt{c} \cdot \sqrt{c} = c, \text{ since } \sqrt{c} > 0.$$

Thus, $ab > a\sqrt{c} > \sqrt{c} \cdot \sqrt{c} = c$ implies

$$ab > c.$$

But $ab = c$; hence, ab is not greater than c, a contradiction.

This proves our assumption $a > \sqrt{c}$ and $b > \sqrt{c}$ cannot be true when a, b, and c are positive real numbers such that $ab = c$. Therefore $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$. □

EXERCISE 2.5.2. *Consider the statement: For all nonnegative real numbers a, b, and c, if $a^2 + b^2 = c^2$, then $a + b \geq c$.*

(a) Give a proof by contradiction.
(b) Give a direct proof. [Hint: The extra idea needed for a direct proof should emerge naturally from a proof by contradiction.]

Let's step back and compare direct proof, proof by contrapositive, and proof by contradiction.

EXERCISE 2.5.3. *Fill in the blanks.*

If we are proving the implication $p \to q$ we assume...

(1) p for a direct proof.
(2) _____ for a proof by contrapositive
(3) _____ for a proof by contradiction.

We are then allowed to use the truth of the assumption in 1, 2, or 3 in the proof.

After the initial assumption, we prove $p \to q$ by showing

(4) q must follow from the assumptions for a direct proof.
(5) _____ must follow the assumptions for a proof by contrapositive.
(6) _____ must follow the assumptions for a proof by contradiction.

2.6. Proof by Cases.

EXAMPLE 2.6.1. *If x is a real number such that $\dfrac{x^2-1}{x+2} > 0$, then either $x > 1$ or $-2 < x < -1$.*

PROOF. Assume x is a real number for which the inequality

$$\frac{x^2-1}{x+2} > 0$$

holds. Factor the numerator of the fraction to get the inequality

$$\frac{(x+1)(x-1)}{x+2} > 0.$$

For this combination of $x+1, x-1$, and $x+2$ to be positive, either all are positive or two are negative and the other is positive. This gives four cases to consider:

Case 1. $x+1 > 0, x-1 > 0$, and $x+2 > 0$. In this case $x > -1, x > 1$, and $x > -2$, which implies $x > 1$.
Case 2. $x+1 > 0, x-1 < 0$, and $x+2 < 0$. In this case $x > -1, x < 1$, and $x < -2$, and there is no x satisfying all three inequalities simultaneously.
Case 3. $x+1 < 0, x-1 > 0$, and $x+2 < 0$. In this case $x < -1, x > 1$, and $x < -2$, and there is no x satisfying all three inequalities simultaneously.
Case 4. $x+1 < 0, x-1 < 0$, and $x+2 > 0$. In this case $x < -1, x < 1$, and $x > -2$, which implies that $-2 < x < -1$.

Thus, either $x > 1$ (Case 1) or $-2 < x < -1$ (Case 4). □

Discussion

Sometimes the hypothesis of a statement can be broken down into simpler cases that may be investigated separately. The validity of a *proof by cases* rests on the equivalence

$$[(p_1 \vee \cdots \vee p_n) \to q] \Leftrightarrow [(p_1 \to q) \vee \cdots \vee (p_n \to q)].$$

In Example 2.6.1 this method is used to verify the "solution" to the inequality,
$\dfrac{x^2-1}{x+2} > 0.$

EXERCISE 2.6.1. *Prove: For every real number x, $\sqrt{x^2} = |x|$. [Hint: Recall as above that $\sqrt{x^2}$ represents the positive square root of x^2, and look at two cases: $x \geq 0$ and $x < 0$.]*

A proof by cases can tend to be a little tedious. Here is an extreme example of such a proof.

EXAMPLE 2.6.2. *Prove that if n is a natural number less than 41, then n^2-n+41 is a prime number.*

PROOF. Recall that a prime number is an integer greater than 1 that is only divisible by itself and 1. It would be nice if there was some general line of argument that would work, but, unfortunately, there doesn't seem to be an obvious one. As a result, the proof must be broken down into 41 cases corresponding to $n = 0, 1, 2, ..., 40$. In each case we examine the integer $n^2 - n + 41$ to see if it is prime. For example, we can observe:

$n = 0$: $0^2 - 0 + 41 = 41$ is prime.

$n = 1$: $1^2 - 1 + 41 = 41$ is prime.

$n = 2$: $2^2 - 2 + 41 = 43$ is prime.

$n = 3$: $3^2 - 3 + 41 = 47$ is prime.

$n = 4$: $4^2 - 4 + 41 = 53$ is prime.

As n increases, it becomes increasingly more time-consuming to show that n^2-n+41 is, indeed, prime. For example, when $n = 40$, $40^2 - 40 + 41 = 1601$. The simplest way to show that 1601 is prime is to show that every prime number $\leq \sqrt{1601}$ fails to be a divisor of 1601. There are 12 such numbers to try, and you might as well check them on your calculator. Alternatively, you could write a computer program or use a symbolic program such as Maple or Mathematica that has a routine to test a number for primality. □

2.7. Existence Proofs. An **existence proof** is a proof of a statement of the form $\exists x P(x)$. Existence proofs generally fall into one of the following two types:

Constructive Proof: Establish $P(c)$ for some c in the universe of discourse.

Nonconstructive Proof: Assume no c exists that makes $P(c)$ true and derive a contradiction. In other words, use a proof by contradiction.

2.8. Constructive Proof.

EXAMPLE 2.8.1. *Prove the statement: There exists a triple (a, b, c) of positive integers such that $a^2 + b^2 = c^2$.*

PROOF. Choose $a = 3$, $b = 4$ and $c = 5$. □

Discussion

In a constructive proof one finds an explicit example in the universe of discourse for which the statement is true.

Here is another example.

EXAMPLE 2.8.2. *Prove: If $f(x) = x^3 + x - 5$, then there exists a positive real number c such that $f'(c) = 7$.*

PROOF. Calculate the derivative of f: $f'(x) = 3x^2 + 1$. Then we want to find a positive number c such that $f'(c) = 3c^2 + 1 = 7$. Solving for c:

$$\begin{aligned} 3c^2 &= 6 \\ c^2 &= 2 \\ c &= \pm\sqrt{2} \end{aligned}$$

Then $c = \sqrt{2}$ is a positive real number and $f'(\sqrt{2}) = 3(\sqrt{2})^2 + 1 = 7$. □

2.9. Nonconstructive Proof.

EXAMPLE 2.9.1. **Pigeon Hole Principle:** *If $n + 1$ objects (pigeons) are distributed into n boxes (pigeon holes), then some box must contain at least 2 of the objects.*

PROOF. Assume $n + 1$ objects (pigeons) are distributed into n boxes. Suppose the boxes are labeled
$B_1, B_2, ..., B_n$, and assume that no box contains more than 1 object. Let k_i denote the number of objects placed in B_i. Then $k_i \leq 1$ for $i = 1, ..., n$, and so

$$k_1 + k_2 + \cdots + k_n \leq \underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}} \leq n.$$

But this contradicts the fact that $k_1 + k_2 + \cdots + k_n = n + 1$, the total number of objects we started with. □

Discussion

Sometimes, constructing an example may be difficult, if not impossible, due to the nature of the problem. If you suspect this is the case, you should try a proof by contradiction: Assume there is no such example and show that this leads to a contradiction. If you are successful, you have established existence, but you have not exhibited a specific example. After you have studied the proof of the basic pigeon hole principal in Example 2.9.1, try your hand at the following variations.

EXERCISE 2.9.1. *Prove: If $2n+1$ objects are distributed into n boxes, then some box must contain at least 3 of the objects.*

EXERCISE 2.9.2. *Fill in the blank in the following statement and then give a proof.*

Suppose k is a positive integer. If $kn+1$ objects are distributed into n boxes, then some box must contain at least _____of the objects.

EXERCISE 2.9.3. *Suppose that 88 chairs are arranged in a rectangular array of 8 rows and 11 columns, and suppose 50 students are seated in this array (1 student per chair).*

(a) Prove that some row must have at least 7 students.
(b) Prove that some column must have at most 4 students.

2.10. Nonexistence Proofs. Suppose we wish to establish the truth of the statement $\neg\exists x P(x)$, which is equivalent to $\forall x \neg P(x)$. One way is to assume there is a member, c, of the universe of discourse for which $P(c)$ is true, and try to arrive at a contradiction.

EXAMPLE 2.10.1. *Prove there does not exist an integer k such that $4k+3$ is a perfect square.*

PROOF. Proof by Contradiction: Assume there is an integer k such that $4k+3$ is a perfect square. That is, $4k+3=m^2$, where m is an integer. Since the square of an even integer is even and $4k+3$ is odd, m must be odd. Then $m=2a+1$ for some integer a. Thus,

$$\begin{aligned}
4k+3 &= m^2\\
4k+3 &= (2a+1)^2\\
4k+3 &= 4a^2+4a+1\\
4k+3 &= 4(a^2+a)+1\\
3-1 &= 4(a^2+a)-4k\\
2 &= 4(a^2+a-k)\\
1 &= 2(a^2+a-k)
\end{aligned}$$

But this contradicts the fact that 1 is an odd integer. □

Discussion

In order to show some property is false for every member of the universe of discourse it is almost always best to try to use a proof by contradiction. Example 2.10.1 illustrates a property of the integers that can be easily proved in this way.

EXERCISE 2.10.1. *Prove: There does not exist a positive real number a such that* $a + \frac{1}{a} < 2$.

2.11. The Halting Problem.

EXAMPLE 2.11.1. **The Halting Problem:** *There does not exist a program which will always determine if an arbitrary program P halts. We say the Halting Problem is undecidable. Note that this is not the same as determining if a specific program or finite set of programs halts. This is decidable.*

PROOF. We simplify the proof by only considering input-free programs (which may call other procedures). Assume there is a program called Halt which will determine if any input-free program P halts.

Halt(P) prints "yes" and halts if P halts. Halt(P) prints "no" and halts otherwise.

Now we construct a new procedure.

```
procedure Absurd
if  Halt(Absurd) = "yes" then
      while true do print "ha"
```

Notice that the procedure Absurd is input-free. Now we consider two cases.

Case 1 If Absurd halts then we execute the loop which prints unending gales of laughter, and thus the procedure does not halt – a contradiction.

Case 2 If Absurd does not halt then we will exit the program, and halt. Again, this is a contradiction.

Now the only assumption we made was that a program exists which determines if any program will halt. Thus this assumption must be false. There is no such program.

□

2.12. Counterexample. Counterexample to $\forall x P(x)$: We may disprove a statement of the form $\forall x P(x)$ by finding a counterexample. That is, use the equivalence $\neg\forall x P(x) \Leftrightarrow \exists x \neg P(x)$, and find a c in the universe of discourse for which $P(x)$ is false.

Discussion

From Example 2.6.1 one might be led to think that $n^2 - n + 41$ is a prime number for every natural number n. After all, it worked for the first 41 natural numbers. (Or so, you were led to believe. Did you finish the remaining 35 cases?) Showing that a predicate $P(x)$ is true for a few, perhaps many millions of x's in its universe of discourse, however, does not constitute a *proof* of $\forall x P(x)$, unless you were able to exhaust all possibilities. This, of course, is not possible if the universe of discourse is an infinite set, such as the set of natural numbers or the set of real numbers. Since the negation of $\forall x P(x)$ is $\neg \forall x P(x) \Leftrightarrow \exists x \neg P(x)$, it only takes *one* x for which $P(x)$ is false, a *counterexample*, to disprove $\forall x P(x)$. The assertion "for every natural number n, $n^2 - n + 41$ is prime" is, in fact, false.

EXERCISE 2.12.1. *Find a counterexample to the statement: For every natural number n, $n^2 - n + 41$ is prime.*

2.13. Biconditional. In order to establish the truth of the statement $p \leftrightarrow q$, use the fact that $(p \leftrightarrow q)$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$, and prove both implications using any of the previous methods.

Discussion

We conclude this module with a discussion on proving a biconditional or "if and only if" statement. As pointed out above, a proof of a biconditional requires two proofs: the proof of an implication *and* a proof of its converse. Our example below is very similar to theorems we have proved earlier. The point here is that the two implications may be proved independently of each other, and the decision on the best strategy to use should be made for each one separately.

EXAMPLE 2.13.1. *Prove: For any integer n, n is odd if and only if n^2 is odd.*

In order to prove this statement, we must prove two implications:

(a) If n is odd, then n^2 is odd.
(b) If n^2 is odd, then n is odd.

PROOF OF (a): We give a direct proof of this statement. Assume n is an odd integer. Then $n = 2a + 1$ for some integer a. Then $n^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$, which is twice an integer plus 1. Thus, n^2 is odd. □

PROOF OF (b): We give a proof of the contrapositive of this statement: "If n is even (not odd), then n^2 is even (not odd). Assume n is an even integer. Then $n = 2a$ for some integer a. Then $n^2 = (2a)^2 = 4a^2 = 2(2a^2)$, which is an even integer.

□

EXERCISE 2.13.1. *Prove the following statements are equivalent.*

(1) $n - 5$ *is odd.*
(2) $3n + 2$ *is even.*
(3) $n^2 - 1$ *is odd.*

Hint: Prove the following implications:

(1) 1→2
(2) 2→1
(3) 1→3
(4) 3→1