Proof by Contrapositive

By contrast the next two techniques of proof to be discussed are methods of indirect proof, for in each case, rather than starting with the hypothesis of the given implication, one begins with the negation of its conclusion.

We first discuss the *method of contraposition* or *proof by contrapositive*. This technique establishes the validity of an implication "If P then Q" by showing that its logically equivalent contrapositive "If not-Q then not-P" holds. Thus, to prove that "If P then Q" is valid, one assumes that not-Q holds and derives the conclusion that not-P is valid.

Example 1.3.4 Let n be an integer. Prove: If n^2 is an odd integer, then n is an odd integer.

Proof To prove the statement, we prove the contrapositive: If n is an integer that is not odd, then n^2 is an integer that is not odd.

Suppose n is an integer that is not odd. Then n is even; hence $n = 2k$ for some integer k. Thus $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ is also an even integer. Therefore, n^2 is not odd if n is not odd. ■

Observe that in this example the proof of the contrapositive of the original statement is a direct proof. We take the meaning of the assumption that n is not odd, mix in some simple arithmetic, and conclude that n^2 is not odd. With a more complex statement, it might be necessary to use other pieces of knowledge; such complications, however, need not cloud over the basic structure of the proof by contrapositive.

In spite of the logical equivalence of the statements "If P then Q" and "If not-Q then not-P," the application of a proof by contrapositive must be handled with care. The danger lies in the formation of negations. If P is a complex sentence, then not-P might be difficult to formulate. For example, as we have seen, the negation of a sentence involving universal and existential quantification can be especially challenging. With these words of warning in mind, we move to a related proof technique—proof by contradiction.

Excerpts from Galovich, S. (1989). *Introduction to Mathematical Structures*. San Diego, CA. Harcourt Brace Jovanovich.

Proof by Contradiction

To establish an implication "If P then Q" via the *method of contradiction*, we assume that the statement "If P then Q" is false and attempt to derive a contradiction, namely a statement that is always false no matter what the truth values of its components. Thus we begin with the statement "P and not-Q," and from this statement we deduce a contradiction, usually a statement of the form "R and not-R." Thus we show that the implication $(P \wedge \text{not-}Q) \Rightarrow (R \wedge \text{not-}R)$ is true. Since $R \wedge \text{not-}R$ is false, it follows that $P \wedge \text{not-}Q$ is also false or equivalently "not-(If P then Q)" is false and "If P then Q" is true. In most cases the statement R is either a result established in the course of the proof, a previously derived result, or an assumption made at some point in the proof.

Example 1.3.5 Show that the circle whose equation is $x^2 + y^2 = 2$ and the line with equation $y = x + 4$ do not intersect.

Proof We rewrite the statement as an implication: If C is the circle with equation $x^2 + y^2 = 2$ and L is the line with equation $y = x + 4$, then C and L do not intersect. We give a proof by contradiction. Assume C and L do intersect. Then there exists a point (x_0, y_0) on both C and L. Then $y_0 = x_0 + 4$ and $x_0^2 + y_0^2 = 2$. Therefore, $x_0^2 + (x_0 + 4)^2 = 2$ from which it follows that $x_0^2 + 4x_0 + 7 = 0$ or that $(x_0 + 2)^2 + 3 = 0$. Thus, if (x_0, y_0) lies on the circle $x^2 + y^2 = 2$ and the line $y = x + 4$, then $(x_0 + 2)^2 = -3$. However, for any real number z, $z^2 \geq 0$; hence $z^2 \neq -3$. We have achieved a contradiction, thus confirming that the given circle and line do not intersect. ■

Example 1.3.6 Prove that $\sqrt{2}$ is irrational.

Proof We recall that a number x is rational if there exist integers m and n with $n \neq 0$ such that $x = m/n$. Therefore, to say that $\sqrt{2}$ is irrational is to say that for all integers m and n, $\sqrt{2} \neq m/n$. A direct proof that $\sqrt{2}$ is irrational would evidently require us to begin with an arbitrary pair of integers m and n and to show that $\sqrt{2} \neq m/n$. This task appears to be difficult. Thus a proof by contradiction is worth trying.

Our goal is to show that for all integers m, n with $n \neq 0$, $\sqrt{2} \neq m/n$. We assume that the negation of this statement holds; hence we assume that there exists a pair of integers m and n for which $\sqrt{2} = m/n$. Our aim is to derive a contradiction. If m and n are both even integers, then $m = 2m'$ and $n = 2n'$ where m' and n' are integers and $\sqrt{2} = m/n = 2m'/2n' = m'/n'$. If m' and n' are even, then we repeat this procedure. In fact, we continue to repeat it until we find integers a and b (which are factors of m and n, respectively), *at least one of which is odd*, such that $\sqrt{2} = a/b$.

Squaring both sides and multiplying both sides of the result by b^2 gives $2b^2 = a^2$. Thus a^2 is even; hence a is even. (See Example 1.3.1.) Therefore, $a = 2k$ and $2b^2 = a^2 = (2k)^2 = 4k^2$. By cancellation $b^2 = 2k^2$ from which it follows that b is even.

We conclude that both a and b are even, a contradiction of the fact that at least one of a and b is odd. This completes the proof that $\sqrt{2}$ is irrational. ■

As was mentioned at the start of the argument, trying a direct proof in this case would seem to be futile. On the other hand, by assuming the negation of the desired conclusion (i.e., that $\sqrt{2}$ is rational), we obtain something quite tangible to manipulate: We are given integers m and n such that $\sqrt{2} = m/n$. In general, we should consider a proof by contradiction if negating the conclusion yields a statement that can be manipulated and exploited. For instance, in Example 1.3.5, by assuming that the given curves did intersect, we obtain a point (x_0, y_0) on both curves, and by substituting the numbers x_0 and y_0 in the equations for the curves, we derive a contradiction.

Excerpts from Galovich, S. (1989). *Introduction to Mathematical Structures*. San Diego, CA. Harcourt Brace Jovanovich.

Our next example comes from the theory of numbers, the discipline of mathematics in which the behavior of whole numbers, with respect to the operations of addition and multiplication, is studied. An example of a statement of number theory is the two-hundred-year-old, as-yet-unproved Goldbach conjecture:

> Every even number larger than two is expressible as a sum of two primes.

We illustrate the method of proof by contradiction by proving a truly ancient result, one that goes back to Book 7 of Euclid's *Elements*. Recall that a positive integer $n > 1$ is *prime* if the only positive integer factors of n are 1 and n. For example, the primes less than 25 are 2, 3, 5, 7, 11, 13, 17, 19, and 23. The only even positive integer that is prime is 2. Notice that if n is not prime, then n can be factored as $n = ab$ where a and b are both greater than 1. In other words, nonprimes can be written as a product of two smaller positive integers.

Once prime numbers are defined, several questions concerning primes come to mind. For instance, one can ask: Is every integer greater than 1 divisible by a prime? The next result that is used to prove Theorem 1.3.5 assures us that indeed this is the case.

Lemma 1.3.4 *Let n be any integer greater than 1. Let a be the smallest factor of n that is greater than 1. Then a is prime.*

Proof We take n and a as in the statement of Lemma 1.3.4. We must show that a is prime. We give a proof by contradiction. Suppose a is not prime. Then $a = b \cdot c$ where $b > 1$ and $c > 1$. Since b is a factor of a and a is a factor of n, b is a factor of n. (See Exercise 1.3.3(b).) But b is also greater than 1 and less than a. To summarize, b is a factor of n such that $1 < b < a$. Therefore, a is not the smallest factor of $a > 1$. This contradiction (of the definition of a) means that a is indeed prime. ■