Proof Series Episode 1: Writing Proofs (Non-Assessable)

Note(s)

The most important skill in Computer Science is to clearly communicate your ideas. A proof is an argument to convince someone that your statement is correct. This document will outline some common techniques we can use to prove that something is true.

Direct Proof

A direct proof starts with the given information and uses logical steps to arrive at the desired conclusion.

Exercise 1. For any two integers a and b, if a and b are even, then their sum $a + b$ is even.

Answer(s)

Let a and b be arbitrary even integers. By definition of even integers, there exist integers m and n such that:

$$a = 2m \ (1) \text{ and } b = 2n. \ (2)$$

Consider the sum $a + b$:

$$\begin{aligned} a + b &= 2m + 2n && \text{(by (1) and (2))} \\ &= 2(m + n). && \text{(factoring out 2)} \end{aligned}$$

Since m and n are integers, their sum is also an integer. Therefore, $a + b$ can be expressed as 2 multiplied by an integer. By definition, we have $a + b$ is even. □

Proof by Contradiction

Suppose that we want to prove that a statement is true. We can assume the opposite is true and show that it would lead to a contradiction (an outcome that is always false). This would mean that our statement must be true!

Exercise 2. Prove $\sqrt{2}$ is irrational.

Answer(s)

Assume, for the sake of contradiction, that $\sqrt{2}$ is rational. By definition of rational numbers, there exist integers p and $q \neq 0$ where $\gcd(p, q) = 1$, such that:

$$\sqrt{2} = \frac{p}{q}. \tag{1}$$

Squaring both sides of (1):

$$2 = \frac{p^2}{q^2}. \tag{2}$$

Multiplying both sides of (2) by q^2:

$$2q^2 = p^2. \tag{3}$$

Equation (3) implies that p^2 is even. By the lemma that "if p^2 is even, then p is even" (which we assume is proven elsewhere), we can conclude that p is even.

Since p is even, there exists an integer k such that:

$$p = 2k. \tag{4}$$

Substituting (4) into (3):

$$\begin{align} 2q^2 &= (2k)^2 \tag{5}\\ &= 4k^2, \tag{6}\\ q^2 &= 2k^2. \tag{7} \end{align}$$

Equation (7) implies that q^2 is even, and by the same lemma, q is even.

However, we have now shown that both p and q are even, so they have a common divisor of 2. This contradicts our assumption that $\gcd(p, q) = 1$. This contradiction implies that our initial assumption must be false.

Therefore, we proved $\sqrt{2}$ is irrational. □

Proof by Contrapositive

To prove an implication "if P then Q", we can instead prove its contrapositive "if not Q then not P".

Exercise 3. For any integer n, if n^2 is even, then n is even.

Answer(s)

We will prove the contrapositive: if n is odd, then n^2 is odd. Let n be an arbitrary odd integer. By definition of odd integers, there exists an integer k such that:

$$n = 2k + 1. \tag{8}$$

Consider n^2:

$$\begin{align} n^2 &= (2k+1)^2, && \text{(by (8))} \tag{9}\\ &= 4k^2 + 4k + 1, && \text{(expanding the square)} \tag{10}\\ &= 2(2k^2 + 2k) + 1. && \text{(factoring out 2)} \tag{11} \end{align}$$

Let $m = 2k^2 + 2k$. Since k is an integer, m is also an integer. Therefore, we have $n^2 = 2m + 1$, where m is an integer. By definition of odd integers, n^2 is odd.

We have proved that if n is odd, then n^2 is odd. By contraposition, this proves that if n^2 is even, then n is even. □

Exercises

Practice writing formal proofs for the following exercises:

1. Prove that the sum of two odd integers is always even.
2. Prove that if $a \mid b$ and $b \mid c$, then $a \mid c$. (Note: $a \mid b$ means "a divides b")
3. Prove that for any integer n, $n^2 - n$ is always even.
4. Prove by contradiction that there are infinitely many prime numbers.