Proof Examples

Selim Kaan Ozsoy, Middle East Technical University

In this section, we will consider the proof methods we have learned in the previous sections and use them to write some proofs to specific theorems.

Theorem. *For any integer m and for any integer n, if m is even and n is odd, then $mn + n$ is odd.*

Proof. Since it is easy to apply the definitions of odd and even integers to some arbitrary integers, we can consider a direct proof to prove this theorem.
Assume that m is an even integer and n is an odd integer. Then, by the definitions of odd and even integers, respectively, we can write, $n = 2a + 1$ and $m = 2b$ for some $a, b \in \mathbb{Z}$. It follows that $mn + n = n(m + 1) = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1 = 2\mu + 1$ for some $\mu \in \mathbb{Z}$. Therefore, by the definition of odd integers, $mn + n$ is odd. $\square$

Theorem. *Let x and y be integers. If x is even and y is even, then 4 divides $x^2 \cdot y^2$.*

Proof. Similarly, we know the definition of even integers and therefore it is rather convenient to do a direct proof.
Assume that x and y are even integers. Then, by the definition of even integers, we can straightforwardly write $x = 2a$ and $y = 2b$ for some $a, b \in \mathbb{Z}$. It follows from the product of x^2 and y^2 that $x^2 \cdot y^2 = (2a)(2b) = 4ab$. Here, since a and b are integers, the product (ab) is an integer. Then, since we can write $x^2 \cdot y^2 = 4k$ for some $k \in \mathbb{Z}$, setting $k = ab$, we say that 4 divides $x^2 \cdot y^2 = 4k$ by the definition of divisibility of integers. $\square$

Theorem. *If $p_1, p_2, p_3, \ldots, p_r$ are pairwise distinct prime numbers. Then $\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots + \frac{1}{p_r}$ is not an integer.*

Proof. We will provide a proof by contradiction. Let the theorem be expressed by $P \implies Q$, where P is the statement "$p_1, p_2, p_3, \ldots, p_r$ are pairwise distinct prime numbers", and Q is the statement "$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots + \frac{1}{p_r}$ is not an integer". Now, by De Morgan Laws, the negation of the argument is given by $\neg(P \implies Q) \iff \neg(\neg P \vee Q) \iff P \wedge \neg Q$. So, we will assume that $p_1, p_2, p_3, \ldots, p_r$ are pairwise distinct prime numbers AND $\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots + \frac{1}{p_r}$ IS an integer, and so get a contradiction to prove the statement.
Suppose in contradiction that $p_1, p_2, p_3, \ldots, p_r$ are pairwise distinct prime numbers and $\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots + \frac{1}{p_r}$ is an integer. Now, set

$$N = \frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots + \frac{1}{p_r}.$$

It follows from a simple multiplication of N by $p_1, p_2, p_3, \ldots, p_r$

$$(p_1 p_2 p_3 \cdots p_r)(N) = p_2 p_3 \cdots p_r + p_1 p_3 \cdots p_r + \cdots + p_1 p_2 \cdots p_{r-1}.$$

Notice that p_1 divides the left-hand side, and so, due to equality, it must divide the right-hand side. Here, we observe that

$$p_1 p_3 \cdots p_r + \cdots + p_1 p_2 \cdots p_{r-1} = p_1(p_3 \cdots p_r + \cdots p_2 p_3 \cdots p_{r-1}).$$

Therefore, p_1 divides $p_1 p_3 \cdots p_r + \cdots + p_1 p_2 \cdots p_{r-1}$. But then, as p_1 divides the right-hand side, and so p_1 divides $p_2 p_3 \cdots p_r + p_1 p_3 \cdots p_r + \cdots + p_1 p_2 \cdots p_{r-1}$ and as p_1 divides $p_1 p_3 \cdots p_r + \cdots + p_1 p_2 \cdots p_{r-1}$, we also get $p_1 \mid (p_2 p_3 \cdots p_r + p_1 p_3 \cdots p_r + \cdots + p_1 p_2 \cdots p_{r-1}) - (p_1 p_3 \cdots p_r + \cdots + p_1 p_2 \cdots p_{r-1})$, which yields that, finally,

$$p_1 \mid p_2 p_3 \cdots p_r.$$

However, this is impossible, as p_i are pairwise distinct prime numbers, where $i \in [1, r]$. So, this is a contradiction. $\square$

Theorem. *Let n be a positive integer. If $n^3 + 2n$ is odd, then n is odd.*

Proof. If we attempt to provide a direct proof, it is required to assume that $n^3 + 2n$ is odd, and then attain the fact that n is odd from this, which is not trivial. So, instead, we wish to assume that n holds a property, and then attain that $n^3 + 2n$ holds a property. Of course, the strategy is proof by contrapositive.
Assume that n is not odd, i.e., n is even. Then, by the definition of even integers, we can write $n = 2k$ for some $k \in \mathbb{Z}$. It follows that $n^3 + 2n = n(n^2 + 2) = (2k)(4k^2 + 2) = 2(4k^3 + 2k) = 2q$ for some $q \in \mathbb{Z}$, setting $q = 4k^3 + 2k$. Therefore, by the definition of even integers, $n^3 + 2n$ is also even. Hence, $n^3 + 2n$ is not odd. $\square$

Theorem. *For every $x \in \mathbb{R}$, if $|x - 3| > 3$, then $x^2 > 6x$.*

Proof. In the theorem, there appears a statement that involves an expression with absolute value. We know that the expression we obtain when we remove the absolute value depends on the sign of the expression inside the absolute value. So, we have to consider two cases. So, we will make a case by case proof.
Let x be a real number. Assume that $|x - 3| > 3$. We split into two cases.
Case I. $(x \geq 3)$
As $x \geq 3$, we have $|x-3| = x-3$, and so, by the initial assumption, $x - 3 > 3 \implies x > 6$. Consider $x^2 - 6x = x(x - 6)$. Now, as $x > 6 > 0$ and $x > 6 \implies x - 6 > 0$, we get $x^2 - 6x > 0$, and so $x^2 > 6x$.
Case II. $(x < 3)$
As $x < 3$, we have $|x - 3| = -(x - 3) = 3 - x$, and so, by the initial assumption, $3 - x > 3 \implies x < 0$. Consider $x^2 - 6x = x(x - 6)$. Now, as $x < 0$ and $x < 0 \implies x - 6 < 0$, we get $x(x - 6) > 0$, and so $x^2 > 6x$. $\square$

Theorem. *Let a, b, c be integers. Let $c \neq 0$. $a \mid b$ if and only if $ac \mid bc$.*

Proof. We are given a theorem involving an if and only if statement. Consequently, in fact, the statement is "If $a \mid b$, then $ac \mid bc$ and if $ac \mid bc$, then $a \mid b$. Therefore, we must prove both sides. Let a, b, c be integers such that $c \neq 0$ and P be the statement $a \mid b$ and Q be the statement $ac \mid bc$.
$(P \implies Q)$:
Assume that $a \mid b$. Then, by the definition of divisibility of integers, there exists some $k \in \mathbb{Z}$ such that $b = k \cdot a$. Now, multiplying both sides by $c \in \mathbb{Z}$, we get $bc = k \cdot (ac)$. Hence, as k is an integer, by the definition of divisibility of integers, $ac \mid bc$.
$(Q \implies P)$:
Assume that $ac \mid bc$. Then, by the definition of divisibility of integers, there exists some $k \in \mathbb{Z}$ such that $bc = k \cdot (ac)$. But then, as c is a nonzero integer, we can divide both sides by c and get $b = k \cdot a$. Hence, by the definition of divisibility of integers, as k is an integer, $a \mid b$. □

Theorem. *The sum of a rational number and an irrational number is irrational.*

Proof. We will provide a proof by contradiction.
Let s be a rational number and k be an irrational number. Assume in contradiction that the sum $s + k$ is rational. Now, by the definition of rational numbers, for some $a, b \in \mathbb{Z} \wedge b \neq 0$, we can write $s = \frac{a}{b}$. Then, we have the sum $s + k = \frac{a}{b}$. Since $s + k$ is rational, similarly, by the definition of rational numbers, for some $c, d \in \mathbb{Z} \wedge d \neq 0$, we can write $s + k = \frac{a}{b} + k = \frac{c}{d}$. But then, we get $k = \frac{c}{d} - \frac{a}{b} = \frac{cb-da}{db}$. Here, we observe that as $a, b, c, d \in \mathbb{Z}$, $(cb - da), (db) \in \mathbb{Z}$ and $(b \neq 0 \wedge d \neq 0) \implies db \neq 0$. Therefore, by the definition of rational numbers, we get k is rational. This contradicts the assumption that k is irrational. □