Revision: Theorem Proofs

Nouman M Durrani

Outline for Direct Proof

Proposition If P, then Q.
Proof. Suppose P.
$\vdots$
Therefore Q. ■

Proposition If x is odd, then x^2 is odd.
Proof. Suppose x is odd.
Therefore x^2 is odd. ■

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.
Then $x = 2a+1$ for some $a \in \mathbb{Z}$, by definition of an odd number.

Therefore x^2 is odd. ■

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.
Then $x = 2a+1$ for some $a \in \mathbb{Z}$, by definition of an odd number.

Thus $x^2 = 2b+1$ for an integer b.
Therefore x^2 is odd, *by definition of an odd number.* ■

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.
Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.
Thus $x^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$.
So $x^2 = 2b + 1$ *where* b *is the integer* $b = 2a^2 + 2a$.
Thus $x^2 = 2b + 1$ for an integer b.
Therefore x^2 is odd, by definition of an odd number. ■

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd. Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number. Thus $x^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$, so $x^2 = 2b + 1$ where $b = 2a^2 + 2a \in \mathbb{Z}$. Therefore x^2 is odd, by definition of an odd number. ■

(10 points) Let $m, n \in \mathbb{Z}$. Prove that if mn is odd, then $m + n$ is even.

Proof. Suppose mn is odd. Since the product of an even number with any other integer is even, it must be the case that both m and n are odd. Thus $m = 2k + 1$ and $n = 2j + 1$ for some $k, j \in \mathbb{Z}$. It follows that $m + n = 2k + 1 + 2j + 1 = 2(k + j + 1)$ and since $k + j + 1 \in \mathbb{Z}$, we have that $m + n$ is even. $\square$

Proposition Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.

Therefore $a \mid c$. ■

Proposition Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.
By Definition 4.4, we know $a \mid b$ means there is an integer d with $b = ad$.
Likewise, $b \mid c$ means there is an integer e for which $c = be$.
Thus $c = be = (ad)e = a(de)$, *so* $c = ax$ *for the integer* $x = de$.
Therefore $a \mid c$. ■

Proposition If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof. Suppose x is an even integer.
Then $x = 2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.
So $x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 = 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1$.
Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in \mathbb{Z}$.
Consequently $x^2 - 6x + 5$ is odd, by definition of an odd number. ■

Proposition Let x and y be positive numbers. If $x \le y$, then $\sqrt{x} \le \sqrt{y}$.

Proof. Suppose $x \le y$. Subtracting y from both sides gives $x - y \le 0$.
This can be written as $\sqrt{x}^2 - \sqrt{y}^2 \le 0$.
Factor this to get $(\sqrt{x} - \sqrt{y})(\sqrt{x} + \sqrt{y}) \le 0$.
Dividing both sides by the positive number $\sqrt{x} + \sqrt{y}$ produces $\sqrt{x} - \sqrt{y} \le 0$.
Adding $\sqrt{y}$ to both sides gives $\sqrt{x} \le \sqrt{y}$. ■

Proposition If x and y are positive real numbers, then $2\sqrt{xy} \leq x + y$.

Proof. Suppose x and y are positive real numbers.
Then $0 \leq (x-y)^2$, that is, $0 \leq x^2 - 2xy + y^2$.
Adding $4xy$ to both sides gives $4xy \leq x^2 + 2xy + y^2$.
Factoring yields $4xy \leq (x+y)^2$.
Previously we proved that such an inequality still holds after taking the square root of both sides; doing so produces $2\sqrt{xy} \leq x + y$. ■

LEMMA (Needed in the following example $\cdots$) For $x \in \mathbb{R}$, $x \neq 0, 1$:

$$\sum_{k=0}^{n} x^k \;=\; \frac{1 - x^{n+1}}{1 - x} \,, \qquad \forall n \geq 0 \,, \qquad (\; \textit{Geometric sum} \;) \,.$$

PROOF (a *"constructive proof"*) :

Let

$$S_n \;=\; \sum_{k=0}^{n} x^k \,.$$

Then

$$S_n \;=\; 1 + x + x^2 + \cdots + x^{n-1} + x^n \,,$$

$$x \cdot S_n \;=\; x + x^2 + \cdots + x^{n-1} + x^n + x^{n+1} \,,$$

so that

$$S_n - x \cdot S_n \;=\; (1 - x) \cdot S_n \;=\; 1 - x^{n+1} \,,$$

from which the formula follows. **QED !**

Proving the contrapositive.

It is easy to see (by Truth Table) that

$$p \rightarrow q \quad \Longleftrightarrow \quad \neg q \ \rightarrow \ \neg p \ .$$

EXAMPLE :

The statement

$$\text{"}n^2 \text{ even} \ \Rightarrow \ n \text{ even"},$$

proved earlier is equivalent to

$$\text{"}\neg(n \text{ even}) \Rightarrow \neg(n^2 \text{ even})\text{"},$$

i.e., it is equivalent to

$$n \text{ odd} \ \Rightarrow \ n^2 \text{ odd} \ .$$

PROPOSITION : Let $n \in \mathbb{Z}^+$, with $n \geq 2$.

If the sum of the divisors of n is equal to $n+1$ then n is prime.

PROOF : We prove the contrapositive :

If n is *not* prime then the sum of the divisors can *not* equal $n+1$.

So suppose that n is not prime.

Then n has divisors

$$1,\ n,\ \text{and } m, \quad \text{for some } m \in \mathbb{Z}^+,\ m \neq 1,\ m \neq n\ ,$$

and possibly more.

Thus the sum of the divisors is greater than $n+1$. **QED !**

Quod Erat Demonstrandum which **means** "that which was to be demonstrated“, the proof is complete

This equivalence justifies the following :

If we must prove

$$P \Rightarrow Q \ ,$$

then we may equivalently prove the *contrapositive*

$$\neg Q \Rightarrow \neg P \ .$$

(Proving the contrapositive is *sometimes easier* .)

(12 points) Let n be a natural number. Prove that either n is prime or n is a perfect square or n divides $(n-1)!$.

Proof. Suppose that n is neither prime nor a perfect square. Since n is not prime, we may factor n as $n = ab$ where $1 < a < n$ and $1 < b < n$. Also, since n is not a perfect square we know that $a \neq b$. Without loss of generality, we will assume $a > b$. Thus

$$\begin{aligned}
(n-1)! &= (n-1)(n-2)\ldots a \ldots b \ldots 2 \cdot 1 \\
&= [(n-1)(n-2)\ldots(a+1)(a-1)\ldots(b+1)(b-1)\ldots 2 \cdot 1](ab) \\
&= [(n-1)(n-2)\ldots(a+1)(a-1)\ldots(b+1)(b-1)\ldots 2 \cdot 1]\, n
\end{aligned}$$

so that $n \mid (n-1)!$. $\square$

(14 points) Prove that $\sqrt[3]{4}$ is irrational.

You may use the following statement without proving it: For all integers a, if a^3 is even then a is even.

Proof: Suppose to the contrary that $\sqrt[3]{4}$ is rational, so that we can write it as a fraction $\frac{a}{b}$, written where a and b are both positive and have no common factor. Then, cubing both sides of $\sqrt[3]{4} = \frac{a}{b}$, we get $4 = \frac{a^3}{b^3}$, so that $4b^3 = a^3$. Thus, a^3 is even, and so a is also even, and we can write $a = 2r$ for some integer r. We have $4b^3 = (2r)^3$, so that $b^3 = 2r^3$. Therefore, b^3 is even, and hence b is even also.

But this shows that a and b are both even and have the common factor 2, contrary to assumption. This is a contradiction; therefore, $\sqrt[3]{4}$ is irrational.

PROPOSITION : Let $n \in \mathbb{Z}^+$, with $n \geq 2$.

$$\forall a, b \in \mathbb{Z}^+ \ (\ n|a \ \vee \ n|b \ \vee \ n \not| ab \ ) \qquad \Rightarrow \qquad n \text{ is prime} .$$

PROOF : The contrapositive is

If n is not prime then $\exists a, b \ (\ n \not| a \ \wedge \ n \not| b \ \wedge \ n|ab \ )$.

Here the contrapositive is *easier to understand* and quite *easy to prove* :

Note that if n is not prime then

$$n \ = \ a \ b \ ,$$

for certain integers a and b, both greater than 1 and less than n.

Clearly $n \not| a$, $n \not| b$, and $n|ab$. **QED !**

Proof by contradiction.

To prove a statement $P \Rightarrow Q$ *by contradiction* :

- assume $P = T$ and $Q = F$,

- show that these assumptions lead to an impossible conclusion (a "contradiction").

(We have already seen some proofs by contradiction.)

PROPOSITION :

If a prime number is the sum of two prime numbers

then one of these equals 2.

PROOF :

Let p_1, p_2, and p be prime numbers, with $p_1 + p_2 = p$.

Suppose that neither p_1 nor p_2 is equal to 2.

Then both p_1 and p_2 must be odd (and greater than 2) .

Hence $p = p_1 + p_2$ is even, and greater than 2.

This contradicts that p is prime. **QED !**

(13 points) Suppose that the product of three positive real numbers x, y, and z is at least 70. Prove that at least one of x, y, and z is greater than 4.

We argue by contradiction. Suppose that x, y, and z are all positive integers which are less than or equal to 4. Then,

$$x \cdot y \cdot z \leq 4 \cdot 4 \cdot 4 = 64,$$

so that $xyz < 64$. However, this contradicts the assumption that $xyz \geq 70$. Therefore, at least one of x, y, and z is greater than 4.

PROPOSITION : $\sqrt{2}$ is irrational, *i.e.*, if $m, n \in \mathbb{Z}^+$ then $\frac{m}{n} \neq \sqrt{2}$.

PROOF : Suppose $m, n \in \mathbb{Z}^+$ and $\frac{m}{n} = \sqrt{2}$.

We may assume m and n are *relatively prime* (cancel common factors).

$$
\begin{array}{llll}
\text{Then } m = \sqrt{2}\, n & \Rightarrow & m^2 = 2n^2 & * \\
& \Rightarrow & m^2 \text{ even} & \\
& \Rightarrow & m \text{ even} & \text{(proved earlier)} \\
& \Rightarrow & \exists k \in \mathbb{Z}^+ (m = 2k) & \\
& \Rightarrow & 2n^2 = m^2 = (2k)^2 = 4k^2 & \text{(using * above)} \\
& \Rightarrow & n^2 = 2k^2 & \\
& \Rightarrow & n^2 \text{ even} & \\
& \Rightarrow & n \text{ even} &
\end{array}
$$

Thus both n and m are even and therefore both are divisible by two.

This contradicts that they are relatively prime. **QED !**

NOTATION : The "$\Rightarrow$" means that the immediately following statement is implied by the preceding statement(s).

The sum of the squares of any two rational numbers is a rational number.

PROOF : Suppose x and y are rational numbers :

$$x = \frac{p_1}{q_1} \qquad \text{and} \qquad y = \frac{p_2}{q_2} .$$

where p_1, q_1 and p_2, q_2 are positive integers.

Then

$$\begin{aligned} x^2 + y^2 &= \frac{p_1^2}{q_1^2} + \frac{p_2^2}{q_2^2} \\ &= \frac{p_1^2 q_2^2 + p_2^2 q_1^2}{q_1^2 q_2^2} . \end{aligned}$$

which is rational.