

# Proof Playground

Severen Redwood

This document serves as my playground for practising the art of writing mathematical proofs. As such, do not expect to find a proof of the Riemann hypothesis here, or indeed anything else that is original. Instead, you will find a range of proofs related to mostly standard undergraduate material that I *hope* are correct.

## Algebra

---

**Theorem 1** (Quadratic Formula). *The solutions of the quadratic equation of the form  $ax^2 + bx + c = 0$  are*

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

*Proof.* Let  $ax^2 + bx + c = 0$ . Complete the square to obtain

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a^2} - \frac{c}{a}.$$

Solve for  $x$  to obtain

$$x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a}.$$

Thus,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

as desired. □

**Theorem 2** (Logarithm of a Product).  $\log_b(xy) = \log_b(x) + \log_b(y)$ .

*Proof.* Let  $x := b^m$  and  $y := b^n$ . From the definition of a logarithm, it follows that  $\log_b(x) = m$  and  $\log_b(y) = n$ .

By substituting  $b^m$  and  $b^n$  for  $x$  and  $y$  in  $\log_b(xy)$ ,

$$\begin{aligned}\log_b(xy) &= \log_b(b^m b^n) \\ &= \log_b(b^{m+n}) \\ &= m + n.\end{aligned}$$

Since  $m = \log_b(x)$  and  $n = \log_b(y)$ , the above can be written as

$$\log_b(xy) = \log_b(x) + \log_b(y),$$

which is the desired identity. □

**Theorem 3** (Logarithm of a Quotient).  $\log_b\left(\frac{x}{y}\right) = \log_b(x) - \log_b(y)$ .

*Proof.* Let  $x := b^m$  and  $y := b^n$ . From the definition of a logarithm, it follows that  $\log_b(x) = m$  and  $\log_b(y) = n$ .

By substituting  $b^m$  and  $b^n$  for  $x$  and  $y$  in  $\log_b(x/y)$ ,

$$\begin{aligned}\log_b\left(\frac{x}{y}\right) &= \log_b\left(\frac{b^m}{b^n}\right) \\ &= \log_b(b^{m-n}) \\ &= m - n.\end{aligned}$$

Since  $m = \log_b(x)$  and  $n = \log_b(y)$ , the above can be written as

$$\log_b\left(\frac{x}{y}\right) = \log_b(x) - \log_b(y),$$

which is the desired identity. □

**Theorem 4** (Logarithm of a Power).  $\log_b(x^y) = y \log_b(x)$ .

*Proof.* Let  $x := b^n$ . From the definition of a logarithm, it follows that  $\log_b(x) = n$ .

By substituting  $b^n$  for  $x$  in  $\log_b(x^y)$ ,

$$\begin{aligned}\log_b(x^y) &= \log_b((b^n)^y) \\ &= \log_b(b^{yn}) \\ &= yn.\end{aligned}$$

Since  $n = \log_b(x)$ , the above can be written as

$$\log_b(x^y) = y \log_b(x),$$

which is the desired identity. □

**Theorem 5** (Change of Base Formula). *Any logarithm can be rewritten in terms of another base with the formula*

$$\log_b(a) = \frac{\log_x(a)}{\log_x(b)}.$$

*Proof.* Let  $c := \log_b(a)$ . From the definition of a logarithm, it follows that  $b^c = a$ . By taking the base- $x$  logarithm of both sides,

$$\log_x(b^c) = \log_x(a).$$

Therefore,

$$\begin{aligned} c \log_x(b) &= \log_x(a) \\ c &= \frac{\log_x(a)}{\log_x(b)}. \end{aligned}$$

Since  $c = \log_b(a)$ , the above can be written as

$$\log_b(a) = \frac{\log_x(a)}{\log_x(b)},$$

which is the change of base formula. □

## Number Theory

---

**Definition 1** (Natural Number). A natural number is a member of the set  $\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, \dots\}$ .

**Result 1.** *The number  $\sqrt{2}$  is irrational.*

*Proof.* Suppose that  $\sqrt{2}$  is rational, and so it can be expressed as a ratio of two integers. Hence, let  $\sqrt{2} = a/b$ , where  $a$  and  $b$  are coprime. By squaring both sides,

$$2 = \frac{a^2}{b^2} \iff 2b^2 = a^2.$$

Therefore,  $a^2$  is even, and in turn,  $a$  is also even, since squares of odd integers are never even. Hence, there exists some integer  $k$  such that  $a = 2k$ . By substituting this in,

$$2b^2 = (2k)^2 \iff b^2 = 2k^2.$$

Using the same reasoning as with  $a$ , it must be that  $b$  is also even. However, since  $a$  and  $b$  are both even, a contradiction arises. Two even integers cannot be coprime, so  $\sqrt{2}$  cannot be expressed as a ratio of two integers. Thus,  $\sqrt{2}$  is irrational. □

**Theorem 1.** *There are infinitely many prime numbers.*

*Proof.* Suppose there are only finitely many prime numbers. Let  $p_1, p_2, \dots, p_n$  be a list of all primes and let  $m := p_1 p_2 \cdots p_n + 1$ . Note that  $m$  is not divisible by  $p_1$  since dividing  $m$  by  $p_1$  gives a remainder of 1. Similarly,  $m$  is not divisible by any other number in the list. Because  $m$  is larger than 1,  $m$  is either a prime or a product of primes.

If  $m$  is a prime, then we have found a prime not in our list, which contradicts the assumption that it was a list of all prime numbers.

If  $m$  is a product of primes, then it must be divisible by one of the primes in our list. However, we have shown  $m$  is not divisible by any number in the list. Thus the assumption that the list was a list of all prime numbers is again contradicted.

Since the assumption that there are only finitely many prime numbers has led to a contradiction, there must be infinitely many prime numbers.  $\square$

**Result 2.** *If  $p$  and  $q$  are two consecutive primes that are each greater than 2, then  $p + q$  is a product of three integers that are each greater than 1.*

*Proof.* Without loss of generality, assume that  $p < q$ . Note that  $p$  and  $q$  are both odd integers since they are both prime numbers greater than 2. Therefore,  $p + q = 2a$ , for some integer  $a$ . If  $a$  is prime, then  $p < a < q$  since  $a = (p + q)/2$ . However, because  $p$  and  $q$  are consecutive primes,  $a$  cannot also be prime. Hence,  $a$  must be composite, and so the result follows.  $\square$

**Theorem 2.** *The sum of the first  $n$  natural numbers is equal to*

$$\frac{n(n+1)}{2}.$$

*Proof.* We proceed by induction. If  $n = 1$ , then the theorem is clearly true:

$$\sum_{i=1}^1 i = \frac{1(1+1)}{2} = 1.$$

So, the theorem holds for the base case of  $n = 1$ .

For the inductive hypothesis, assume the formula is true for all  $k > 1$ . Hence,

$$\sum_{i=1}^k i = \frac{k(k+1)}{2}.$$

For the inductive step, let  $n = k + 1$ . By the properties of summation,

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^k i + (k+1).$$

By using the inductive hypothesis,

$$\begin{aligned} \sum_{i=1}^k i + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \\ &= \frac{(k+1)((k+1)+1)}{2}. \end{aligned}$$

So, the theorem holds when  $n = k + 1$ .

Since the base case and inductive step have been shown, the theorem holds for all natural numbers by the principle of mathematical induction.  $\square$

**Theorem 3.** *The sum of the squares of the first  $n$  natural numbers is equal to*

$$\frac{n(n+1)(2n+1)}{6}.$$

*Proof.* We proceed by induction. If  $n = 1$ , then the theorem is clearly true:

$$\sum_{i=1}^1 i^2 = \frac{1(1+1)(2 \cdot 1 + 1)}{6} = 1.$$

So, the theorem holds for the base case of  $n = 1$ .

For the inductive hypothesis, assume the formula is true for all  $k > 1$ . Hence,

$$\sum_{i=1}^k i = \frac{k(k+1)(2k+1)}{6}.$$

For the inductive step, let  $n = k + 1$ . By the properties of summation,

$$\sum_{i=1}^{k+1} i^2 = \sum_{i=1}^k i^2 + (k+1)^2.$$

By using the inductive hypothesis,

$$\begin{aligned} \sum_{i=1}^k i^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1) \\ &= \frac{k(k+1)(2k+1) + 6(k+1)}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6} \\ &= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}. \end{aligned}$$

So, the theorem holds when  $n = k + 1$ .

Since the base case and inductive step have been shown, the theorem holds for all natural numbers by the principle of mathematical induction.  $\square$

## Set Theory

---

**Definition 1** (Ordered Pair). The ordered pair of two elements  $a$  and  $b$  is the set

$$(a, b) := \{\{a\}, \{a, b\}\}.$$

**Definition 2** (Cartesian Product). The Cartesian product of two sets  $A$  and  $B$  is the set

$$A \times B := \{ (a, b) : a \in A, b \in B \}.$$

**Theorem 1.** For any sets  $A$ ,  $B$ , and  $C$ , the following hold:

$$(a) (A \cup B) \times C = (A \times C) \cup (B \times C)$$

$$(b) (A \cap B) \times C = (A \times C) \cap (B \times C)$$

$$(c) A \times (B \cup C) = (A \times B) \cup (A \times C)$$

$$(d) A \times (B \cap C) = (A \times B) \cap (A \times C).$$

*Proof of A.* Let  $(u, v) \in (A \cup B) \times C$ . Therefore,  $u \in A \cup B$  and  $v \in C$ . This means that  $u \in A$  or  $u \in B$ . If  $u \in A$ , then  $(u, v) \in A \times C$ . If  $u \in B$ , then  $(u, v) \in B \times C$ . Either way,  $(u, v) \in (A \times C) \cup (B \times C)$ . Hence,

$$(A \cup B) \times C \subseteq (A \times C) \cup (B \times C).$$

Now, let  $z := (x, y) \in (A \times C) \cup (B \times C)$ . Either  $z \in A \times C$  or  $z \in B \times C$ . In the first case,  $x \in A$  and  $y \in C$ . In the second,  $x \in B$  and  $y \in C$ , so  $z = (x, y) \in (A \cup B) \times C$ . This implies that

$$(A \times C) \cup (B \times C) \subseteq (A \cup B) \times C.$$

Putting the two parts together completes the proof.  $\square$

*Proof of B.* Let  $(u, v) \in (A \cap B) \times C$ . Therefore,  $u \in A \cap B$  and  $v \in C$ . This means that  $u \in A$  and  $u \in B$ . Thus,  $(u, v) \in A \times C$  and  $(u, v) \in B \times C$ , and consequently,  $(u, v) \in (A \times C) \cap (B \times C)$ . Hence,

$$(A \cap B) \times C \subseteq (A \times C) \cap (B \times C).$$

Now, let  $z := (x, y) \in (A \times C) \cap (B \times C)$ . Therefore,  $z \in A \times C$  and  $z \in B \times C$ . So,  $x \in A$  and  $x \in B$ , and likewise,  $y \in C$ . Thus,  $z = (x, y) \in (A \cap B) \times C$ . This implies that

$$(A \times C) \cap (B \times C) \subseteq (A \cap B) \times C.$$

Putting the two parts together completes the proof.  $\square$

## Real Analysis

---

**Definition 1** (Limit). Let  $f$  be a real-valued function defined on a subset  $D$  of the real numbers. Let  $c$  be a limit point of  $D$  and let  $L$  be a real number. We say that

$$\lim_{x \rightarrow c} f(x) = L$$

if for every  $\varepsilon > 0$ , there exists a  $\delta > 0$  such that, for all  $x \in D$ ,

$$0 < |x - c| < \delta \implies |f(x) - L| < \varepsilon.$$

**Definition 2** (Partition of an Interval). A partition of a closed interval  $[a, b]$  is a set of points  $P = \{x_0, x_1, \dots, x_n\}$  satisfying the condition that  $a = x_0 < x_1 < \dots < x_{n-1} < x_n = b$ .

**Definition 3** (Norm of a Partition). The norm (or mesh) of a partition  $P = \{x_0, x_1, \dots, x_n\}$  is the length of the longest subinterval of  $P$  and is denoted by  $\|P\| = \max \{x_i - x_{i-1}\}_{i=1}^n$ .

**Definition 4** (Riemann Sum). Let  $f$  be a function defined on a closed interval  $I$ , and let  $P = \{x_0, x_1, \dots, x_n\}$  be a partition of  $I$ . A Riemann sum of  $f$  over  $I$  with partition  $P$  is defined as

$$\sum_{i=1}^n f(x_i^*) \Delta x_i,$$

where  $\Delta x_i = x_i - x_{i-1}$  and  $x_i^* \in [x_{i-1}, x_i]$ .

**Definition 5** (Definite Integral). Let  $f$  be a function defined on a closed interval  $I$ , and let  $J$  be a real number. We say that

$$\int_a^b f(x) dx = J,$$

and that  $J$  is the limit of the Riemann sums  $\sum_{i=1}^n f(x_i^*) \Delta x_i$  if the following condition is satisfied:

Given any  $\varepsilon > 0$ , there is a corresponding  $\delta > 0$  such that, for every partition  $P = \{x_0, x_1, \dots, x_n\}$  of  $I$  with  $\|P\| < \delta$  and any sample point  $x_i^* \in [x_{i-1}, x_i]$ , we have that

$$\left| \sum_{i=1}^n f(x_i^*) \Delta x_i - J \right| < \varepsilon.$$

**Result 1.**  $\lim_{x \rightarrow 2} (x^2 + 1) = 5$ .

*Proof.* Suppose  $\varepsilon > 0$ . Let  $\delta := \min(1, \varepsilon/5)$  and  $x \in \mathbb{R}$  such that  $0 < |x - 2| < \delta$ .

Since  $|x - 2| < \delta$ , it follows that

$$\begin{aligned} |x - 2| < 1 &\implies -1 < x - 2 < 1 \\ &\implies 1 < x < 3. \end{aligned}$$

In particular, this means that  $|x + 2| < 5$ . Likewise, it follows that  $|x - 2| < \varepsilon/5$ .

Hence,

$$\begin{aligned} |x - 2| < \delta &\implies |x - 2| < \frac{\varepsilon}{5} \\ &\implies |x + 2||x - 2| < 5 \cdot \frac{\varepsilon}{5} \\ &\implies |x^2 - 4| < \varepsilon \\ &\implies |(x^2 + 1) - 5| < \varepsilon. \end{aligned}$$

□

**Result 2.**  $\lim_{x \rightarrow 3} (x^2 + 6) = 15$ .

*Proof.* Suppose  $\varepsilon > 0$ . Let  $\delta := \min(1, \varepsilon/7)$  and  $x \in \mathbb{R}$  such that  $0 < |x - 3| < \delta$ .  
 Since  $|x - 3| < \delta$ , it follows that

$$\begin{aligned} |x - 3| < 1 &\implies -1 < x - 3 < 1 \\ &\implies 2 < x < 4. \end{aligned}$$

In particular, this means that  $|x + 3| < 7$ . Likewise, it follows that  $|x - 3| < \varepsilon/7$ .  
 Hence,

$$\begin{aligned} |x - 3| < \delta &\implies |x - 3| < \frac{\varepsilon}{7} \\ &\implies |x + 3||x - 3| < 7 \cdot \frac{\varepsilon}{7} \\ &\implies |x^2 - 9| < \varepsilon \\ &\implies |(x^2 + 6) - 15| < \varepsilon. \end{aligned} \quad \square$$

**Result 3.**  $\lim_{x \rightarrow 0} \frac{x}{x^2 + 1} = 0$ .

*Proof.* Suppose  $\varepsilon > 0$ . Let  $\delta := \min(1, 2\varepsilon)$  and  $x \in \mathbb{R}$  such that  $0 < |x| < \delta$ .  
 Since  $|x| < \delta$ , it follows that  $|x| < 1$ , and thus  $|x^2 + 1| < 2$ . Likewise, it follows that  $|x| < 2\varepsilon$ .  
 Hence,

$$\begin{aligned} |x| < 2\varepsilon &\implies \frac{|x|}{|x^2 + 1|} < \frac{2\varepsilon}{2} \\ &\implies \frac{|x|}{|x^2 + 1|} < \varepsilon \\ &\implies \left| \frac{x}{x^2 + 1} \right| < \varepsilon. \end{aligned} \quad \square$$

**Result 4.**  $\lim_{x \rightarrow 5^+} \frac{1}{x - 5} = \infty$ .

*Proof.* Suppose  $M > 0$ . Let  $\delta := 1/M$  and  $x \in \mathbb{R}$  such that  $0 < x - 5 < \delta$ .  
 Since  $x - 5 < \delta$ , it follows that

$$x - 5 < \frac{1}{M} \implies \frac{1}{x - 5} > M. \quad \square$$

**Theorem 1** (Constant Multiple of Definite Integrals). *If  $f$  is a integrable function, then*

$$\int_a^b kf(x) \, dx = k \int_a^b f(x) \, dx,$$

*for some constant  $k$ .*



*Proof.* From the definition of a definite integral, we have that

$$\int_a^b kf(x) \, dx = \lim_{\|P\| \rightarrow 0} \sum_{i=1}^n kf(x_i^*)\Delta x_i.$$

By the properties of limits and summation,

$$\begin{aligned} \lim_{\|P\| \rightarrow 0} \sum_{i=1}^n kf(x_i^*)\Delta x_i &= k \lim_{\|P\| \rightarrow 0} \sum_{i=1}^n f(x_i^*)\Delta x_i \\ &= k \int_a^b f(x) \, dx, \end{aligned}$$

as desired. □