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.

Contents

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

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

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

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. $\square$

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. $\square$

2 Number Theory

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

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. $\square$

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. □

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. □

Theorem 2. $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.

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. □

Theorem 3. $1+4+9+\cdots+n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

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. □

3 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. □

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. □

4 Real Analysis

4.1 Limits

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

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

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

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

Result 1. $\lim\limits_{x \to 2} (x^2 + 1) = 5.$

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. $\lim\limits_{x \to 3} (x^2 + 6) = 15.$

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,

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

□

Result 3. $\lim_{x \to 0} \dfrac{x}{x^2+1} = 0.$

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,

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

□

Result 4. $\lim_{x \to 5^+} \dfrac{1}{x-5} = \infty.$

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

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

□

4.2 Sequences and Series

Definition 1 (Sequence)**.** A sequence is a function $f : X \to Y$, where $X \subseteq \mathbb{N}$.

It is customary to denote a sequence by a letter such as "a". Then, for each $n \in X$, $f(n)$ is denoted by a_n, and f itself is denoted by $(a_n)_{n \in X}$.

Definition 2 (Convergent Sequence)**.** A sequence (a_n) converges to the limit L if, for every $\varepsilon > 0$, there exists an N such that, for all n,

$$n > N \implies |a_n - L| < \varepsilon.$$

If this condition is met, we write $\lim_{x\to\infty} a_n = L$, or simply $a_n \to L$. Otherwise, we say that (a_n) diverges.

Theorem 1 (Squeeze Theorem)**.** *Let (a_n), (b_n), and (c_n) be sequences of real numbers. If $b_n \leqslant a_n \leqslant c_n$ for all $n > N$, and $\lim_{n\to\infty} b_n = \lim_{n\to\infty} c_n = L$, then $\lim_{n\to\infty} a_n = L$.*

Proof. Let $\varepsilon > 0$ be given. By hypothesis, there exists an N_1 such that $|b_n - L| < \varepsilon$ for all $n > N_1$, and an N_2 such that $|c_n - L| < \varepsilon$ for all $n > N_2$. Hence, let $N' := \max\{N, N_1, N_2\}$. If $n > N'$, then

$$\begin{aligned} b_n - L \leqslant a_n - L \leqslant c_n - L &\implies -\varepsilon < a_n - L < \varepsilon \\ &= |a_n - L| < \varepsilon. \end{aligned}$$

Since the choice of ε is arbitrary, $\lim_{n\to\infty} a_n = L$. □

Theorem 2. *Let (a_n) be a sequence of real numbers. If $\lim_{n\to\infty} a_n = L$, and f is a function that is continuous at L and defined for all a_n, then $\lim_{n\to\infty} f(a_n) = f(L)$.*

Proof. Let $\varepsilon > 0$ be given. Since f is continuous at L, there exists a $\delta > 0$ such that, for all x in the domain of f,

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

Likewise, since $\lim_{n\to\infty} a_n = L$, there exists an N such that $|a_n - L| < \delta$ for all $n > N$. Hence, when $x = a_n$,

$$n > N \implies |f(a_n) - f(L)| < \varepsilon.$$

Since the choice of ε is arbitrary, $\lim_{n\to\infty} f(a_n) = f(L)$. □

4.3 Differentiation

Definition 1 (Derivative)**.** The derivative of a function f with respect to a variable x is the function f' whose value at x is

$$f'(x) = \lim_{h\to 0} \frac{f(x+h) - f(x)}{h},$$

provided that the limit exists.

Theorem 1. *If f is a differentiable function, then*

$$(kf(x))' = kf'(x),$$

for some constant k.

Proof. From the definition of a derivative,

$$\begin{aligned}(kf(x))' &= \lim_{h\to 0} \frac{kf(x+h) - kf(x)}{h} \\ &= \lim_{h\to 0} \frac{k(f(x+h) - f(x))}{h}.\end{aligned}$$

By the properties of limits,

$$\begin{aligned}\lim_{h\to 0} \frac{k(f(x+h) - f(x))}{h} &= k \lim_{h\to 0} \frac{f(x+h) - f(x)}{h} \\ &= kf'(x),\end{aligned}$$

as desired. □

Theorem 2. *If f and g are differentiable functions, then*

$$(f(x) + g(x))' = f'(x) + g'(x).$$

Proof. From the definition of the derivative,

$$
\begin{aligned}
(f(x)+g(x))' &= \lim_{h\to 0} \frac{(f(x+h)+g(x+h))-(f(x)+g(x))}{h} \\
&= \lim_{h\to 0} \left(\frac{f(x+h)-f(x)}{h} + \frac{g(x+h)-g(x)}{h} \right).
\end{aligned}
$$

By the properties of limits,

$$
\begin{aligned}
\lim_{h\to 0} \left(\frac{f(x+h)-f(x)}{h} + \frac{g(x+h)-g(x)}{h} \right) &= \lim_{h\to 0} \frac{f(x+h)-f(x)}{h} + \lim_{h\to 0} \frac{g(x+h)-g(x)}{h} \\
&= f'(x)+g'(x),
\end{aligned}
$$

as desired. □

4.4 Integration

Definition 1 (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 $a = x_0 < x_1 < \cdots < x_{n-1} < x_n = b$.

Definition 2 (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 3 (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 4 (Definite Integral). Let f be a function defined on a closed interval I, and let J be a real number. We say that

$$\int_a^b f(x)\,\mathrm{d}x = J,$$

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 $\varepsilon > 0$ 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

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

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

$$\int_a^b kf(x)\,\mathrm{d}x = k\int_a^b f(x)\,\mathrm{d}x,$$

for some constant k.

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

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

By the properties of limits and summation,

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

as desired. □