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. $\square$

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. $\qquad\square$

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

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. $\qquad\square$

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. $\qquad\square$

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,

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

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

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 6. *There are infinitely many prime numbers.*

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

If n 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 n is a product of primes, then it must be divisible by one of the primes in the list. However, we have shown n is not divisible by any p_n 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. $\qquad\square$

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 7. *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. $\qquad\square$

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. $\qquad\square$

Real Analysis

Definition 3 (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 $x \in D$, if $0 < |x - c| < \delta$, then $|f(x) - L| < \varepsilon$.

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

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

$$|x - 2| < 1 \implies -1 < x - 2 < 1$$
$$\implies 1 < x < 3.$$

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

$$|x - 2| < \delta \implies |x - 2| < \frac{\varepsilon}{5}$$
$$\implies |x + 2||x - 2| < 5 \cdot \frac{\varepsilon}{5}$$
$$\implies |x^2 - 4| < \varepsilon$$
$$\implies |(x^2 + 1) - 5| < \varepsilon. \qquad \square$$

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

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

$$|x - 3| < 1 \implies -1 < x - 3 < 1$$
$$\implies 2 < x < 4.$$

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

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

Result 4. $\lim_{x \to 0} \dfrac{x}{x^2 + 1} = 0$.

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,

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

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

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

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