Learning Notation: Seminar One
Logic and Proof Techniques

Jack (Quan Cheng) Xie

March 6, 2022

1 Mathematical Truth

Discuss: What is truth? How do we determine what is true? Truth in mathematics.

1.1 Statements

Definition 1.1 (Statement)**.** *A* ***statement*** *or* ***claim*** *is an expression that is either* ***true*** *(T) or* ***false*** *(F), but not both. We call T and F* ***truth values****.*

We can use variables to represent a statement. For example:

$$P := 1 + 1 = 2. \tag{1.1}$$
$$Q := \text{There are infinitely many prime numbers.} \tag{1.2}$$
$$R := \sqrt{2} \text{ is rational.} \tag{1.3}$$
$$S := \text{All horses are the same color.} \tag{1.4}$$

For the above statements, P, Q are true while R, S are false.

Not all expressions are statements according to Definition 1.1. For example, the truth values of the following sentences cannot be determined, so they are not mathematical statements.

$$P := \text{Hello world!} \tag{1.5}$$
$$Q := \text{Is } 2 + 2 = 4\text{?} \tag{1.6}$$
$$R := \text{This statement is false.} \tag{1.7}$$
$$S(x) := \text{The integer } x \text{ is even.} \tag{1.8}$$

1.2 Predicates

The truth of a statement can be *predicated* on another variable. For example, consider

$$P(x) := 2x \text{ is even.} \tag{1.9}$$
$$Q(x) := x(x+1) \text{ is odd.} \tag{1.10}$$

We call $P(x)$ and $Q(x)$ **predicates**, and the collection of x the **universe of discourse,** which we describe with set theory.

Definition 1.2 (Set membership)**.** *A* ***set*** *is a collection of objects, which are the set's members. We write $x \in S$ to say that "x is a member of the set S".*

For example, let $S = \{x, y, z\}$ and assume a, b, c, d are all "different" objects (none of them are equal to each other). Then $x \in S = \{x, y, z\}$ is a true statement, and $d \in S = \{x, y, z\}$ is false.

Some good sets to know:

Natural numbers: $\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$.
Integers: $\mathbb{Z} = \{0, -1, 1, -2, 2, ...\}$.
Rationals: $\mathbb{Q} = \{..., -1/3, -2, -1/2, -1, 0, 1, 1/2, 2, 1/3, ...\}$.
Real numbers: $\mathbb{R} = (-\infty, \infty), \quad \pi, e, \sqrt{2} \in \mathbb{R}$.

1.3 Axioms

An **axiom** is a statement that is assumed to be true. An **axiomatic system** uses axioms, definitions, and deductions to derive the truth values of other statements with **proofs**.

A statement is **consistent** in a axiomatic system it does not **contradict** the other axioms or proven statements. To avoid inconsistencies in a axiomatic system, its axioms should be as few and as simple as possible. Though apparently, constructing a consistent system is more difficult than it sounds.[3] See more on Gödel's incompleteness theorem.

1.4 Established truths

Theorems, propositions, lemmas, and **corollaries** are statements that can be **proved** to be true. Terence Tao explains the distinction between them nicely:

> "A **lemma** is an easily proved claim which is helpful for proving other propositions and theorems, but is usually not particularly interesting in its own right. A **proposition** is a statement which is interesting in its own right, while a **theorem** is a more important statement than a proposition which says something definitive on the subject, and often takes more effort to prove than a proposition or lemma. A **corollary** is a quick consequence of a proposition or theorem that was proven recently."[7]

1.5 Conjectures

A **conjecture** is a statement that is believed to be true but is not proven. Goldbach's conjecture and the twin prime conjecture are two famous examples that are very simple to state, though demonstratively not simple to prove.

Conjecture 1 (Goldbach)**.** *Every even number is the sum of two primes.*

Conjecture 2 (Twin prime)**.** *There are infinitely many primes p where $p + 2$ is also prime.*

Other famous conjectures are the Riemann hypothesis, the P versus NP problem and the continuum hypothesis. The first two of these are unsolved Millenium Prize Problems.

2 Predicate Logic

A **logical operator** (or **connective**) is applied to one or more statements to create a new statement. We start with **negation**, which is a **unary** connective that operates on one statement.

2.1 Negation and truth tables

Definition 2.1 (Negation)**.** *A* ***negation*** $\neg$ *(or $\sim$) is a logical operator on a statement that creates a statement of the opposite truth value.*

For example, for a statement P, its negation is $\neg P$, which we also call "not P". We can also negate the negation, $\neg(\neg P)$. Their truth values can be outlined Table 2.1, which is a **truth table**. A truth table shows all possible truth value combinations of statements or propositional variables.

P	$\neg P$	$\neg(\neg P)$
T	F	T
F	T	F

Table 1: Negation

2.2 Logical equivalence

Definition 2.2 (Logical equivalence)**.** *Two statements are* ***logically equivalent*** *if they have the same values on the truth table. We express an equivalence between two statements P and Q as $P \equiv Q$.*

For example, from Table 2.1 we can see that $P \equiv \neg(\neg P)$ since they have the same truth values.

2.3 Conjunction and disjunction

Definition 2.3 (Conjunction)**.** *For two statements P and Q, we define their* ***conjunction*** *$P \wedge Q$ as a statement that is true if both P and Q are true, and false otherwise.*

Definition 2.4 (Disjunction)**.** *We define their* ***disjunction*** *$P \vee Q$ as a statement that is true if either P is true or Q is true, or both are true.*

We also call $\wedge$ the "and" operator and $\vee$ the "or" operator. The truth table is as follows:

P	Q	$P \wedge Q$	$P \vee Q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

Table 2: Conjunction and disjunction

2.4 De Morgan's laws

Two useful logical equivalences are de Morgan's Laws.

Theorem 1 (De Morgan's laws)**.** *For two statements P and Q,*

$$P \wedge Q \equiv \neg(\neg P \vee \neg Q), \tag{2.1}$$
$$P \vee Q \equiv \neg(\neg P \wedge \neg Q). \tag{2.2}$$

We will prove the first result (2.1) and leave (2.2) as an exercise.

Proof. To proof that two statements are equivalent, we just have to show that they have the same values on the truth table.

(i) P	(ii) Q	(iii) $P \wedge Q$	(iv) $\neg P$	(v) $\neg Q$	(vi) $(\neg P \vee \neg Q)$	(vii) $\neg(\neg P \vee \neg Q)$
T	T	T	F	F	F	T
T	F	F	F	T	T	F
F	T	F	T	F	T	F
F	F	F	T	T	T	F

Table 3: First de Morgan's Law

It can be seen from Table 3 that $p \wedge Q$ in column (iii) and $\neg(\neg P \vee \neg Q)$ in column (vii) have the same truth values for all value combinations of P, Q. Therefore they are logically equivalent by definition. ☐

Exercise 2.1. *Prove the second de Morgan's law* (2.2)*, that $P \vee Q \equiv \neg(\neg P \wedge \neg Q)$.*

2.5 Boolean algebra

For statements $x, y, z,$, the following connective properties can be verified with truth tables:

$$\begin{aligned}
\textbf{Associativity:}\quad & x \wedge (y \wedge z) \equiv (x \wedge y) \wedge z, \quad x \vee (y \vee z) \equiv (x \vee y) \vee z. && (2.3)\\
\textbf{Commutativity:}\quad & x \wedge y \equiv y \wedge x, \quad x \vee y \equiv y \vee x. && (2.4)\\
\textbf{Distributivity:}\quad & x \wedge (y \vee z) \equiv (x \wedge y) \vee (x \wedge z), \quad x \vee (y \wedge z) \equiv (x \vee y) \wedge (x \vee z). && (2.5)\\
\textbf{Identities, annihilators:}\quad & x \wedge T \equiv x, \quad x \wedge F \equiv F, \quad x \vee F \equiv x, \quad x \vee T \equiv T. && (2.6)
\end{aligned}$$

Exercise 2.2. *Show that the distributive properties of $\vee$ and $\wedge$ are true:*

$$x \wedge (y \vee z) \equiv (x \wedge y) \vee (x \wedge z), \quad x \vee (y \wedge z) \equiv (x \vee y) \wedge (x \vee z). \tag{2.7}$$

2.6 Quantifiers

Quantifiers connect a sequence of statements from a predicate with conjunction or disjunctions.

Definition 2.5 (Universal quantifier)**.** *The **universal quantifier** $\forall$ evaluates a conjunction of statements with a predicate $P(x)$ on all elements of x in a set.*

$$\forall x \in \{x_1, x_2, ...\},\ P(x) \ \equiv\ P(x_1) \wedge P(x_2) \wedge ... \tag{2.8}$$

For the above we read, "**For just have to all** x in the set $\{x_1, x_2, ...\}$, $P(x)$ is true." Sometimes we say **"for every"** or **"for any"** instead of "for all"

Definition 2.6 (Existential quantifier)**.** *The **existential quantifier** $\exists$ creates a disjunction of $P(x)$ for all elements of x in a set.*

$$\exists x \in \{x_1, x_2, ...\},\ P(x) \ \equiv\ P(x_1) \vee P(x_2) \vee ... \tag{2.9}$$

For the above we read, "**There exists** a x in the set $\{x_1, x_2, ...\}$ where $P(x)$ is true." Sometimes we say **"there is"** instead of "there exists."

Exercise 2.3. *The set of natural numbers is $\mathbb{R}$. Consider the following statements:*

$$\textit{There exists a real number } a \textit{ where for any real number } x,\ ax = x. \tag{2.10}$$

$$\textit{There exists a real number } b \textit{ where for a any real number } x,\ bx = b. \tag{2.11}$$

Can you rewrite these statements with quantifiers? Are these statements true? If so, what are a and b?

Exercise 2.4. *Consider the following statement:*

$$\forall \epsilon > 0,\ \exists \delta > 0,\ |x - p| < \delta \implies |f(x) - L| < \epsilon. \tag{2.12}$$

*This is called the **epsilon-delta definition** of limit, $\lim_{x \to p} f(x) = L$. Can you restate the definition in words? Can you interpret what it means?*

2.7 Conditional and biconditional statements

Definition 2.7 (Conditional statement)**.** *For two statements P and Q, we can form a new statement*

$$R := \textit{If } P \textit{ (is true), then } Q \textit{ (is true)}, \tag{2.13}$$

where R is a true statement if Q is true under the condition that P is true. We can also say that "P implies Q", or "Q if P", or write $P \implies Q$ (or $P \to Q$).

If $P \implies Q$, we call P the **sufficient condition** for Q, and Q the **necessary condition** for P.

If the reverse implication $Q \implies P$ is true, we can also write $P \impliedby Q$, which we also call the **converse** of $P \implies Q$. Then we can also say that P **only if** Q**.**

Definition 2.8 (Biconditional statement)**.** *For two statements P and Q, if both $P \implies Q$ and $P \impliedby Q$, then we say that **if and only if** P**, then** Q**.** We also call this a biconditional statement, and write it as $P \iff Q$ or $P \longleftrightarrow Q$. A biconditional statement is equivalent to logical equivalence.*

The truth table for conditional and bi-conditional statements is as follows.

P	Q	$P \implies Q$	$P \impliedby Q$	$P \iff Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

The third case where $F \implies T$ is true is called "vacuous truth".

Exercise 2.5. *Show that $P \implies Q$ is logically equivalent to $\neg P \vee (P \wedge Q)$.*

Exercise 2.6. *Express $P \iff Q$ as negations, conjunctions, and disjunctions of P and Q.*

Exercise 2.7. *Which of the following statements are true?*

(a) $x < 3 \implies x \leq 4$

(b) $x < 3 \impliedby x \leq 4$

(c) $x > y \implies x \geq y$

(d) $x > y \impliedby x \geq y$

(e) $[(P \implies Q) \wedge (\neg P)] \implies (Q \equiv T)$

(f) $[(P \implies Q) \wedge (\neg P)] \implies Q$

(g) $[(P \implies Q) \wedge P] \implies Q$

2.8 Tautology

Definition 2.9. *A **tautology** is a statement that is always true.*

Definition 2.10. *A **contradiction** is a statement that is always false.*

For example, $P \vee \neg P$ is a tautology, while $P \wedge \neg P$ is a contradiction.

P	$\neg P$	$P \vee \neg P$	$P \wedge \neg$ P
T	F	T	F
F	T	T	F

Table 4: A tautology and contradiction

Exercise 2.8. *Is each of the following a tautology, contradiction, or neither?*

(a) $(x < 0) \vee (x > 0)$

(b) $(x < 0) \wedge (x > 0)$

(c) $(x < y) \wedge (x \geq y)$

(d) $[(P \implies Q) \wedge (\neg Q)] \implies \neg P$

(e) $[(P \vee Q) \wedge (\neg Q)] \implies \neg P$

(f) $(P \wedge Q) \iff Q$

(g) $Q \iff (P \vee Q)$

Exercise 2.9. *Verify that the following statements are tautologies.*

(a) $P \iff \neg(\neg P)$

(b) $P \vee Q \iff \neg(\neg P \wedge \neg Q)$

(c) $P \wedge Q \iff \neg(\neg P \vee \neg Q)$

(d) $(P \implies Q) \iff (\neg Q \implies \neg P)$

(e) $P \iff (\neg P \implies Q) \wedge (\neg P \implies \neg Q)$

(f) $((A \implies B) \wedge (B \implies C)) \implies (A \implies C)$

(g) $[(A \vee B) \wedge (A \implies C) \vee (B \implies C)] \implies C$

3 Proof Techniques

3.1 Direct proof

The most common type of proof is **direct proof**, where the truth of a statement is derived from direct implications of definitions, axioms, and tautologies.

Definition 3.1 (Odd integer)**.** *An integer x is odd $\iff$ there exists an integer y where $x = 2y + 1$.*

Definition 3.2 (Even integer)**.** *An integer x is even $\iff$ there exists an integer y where $x = 2y$.*

Proposition 3.1. *An integer x is odd, then x^2 is odd.*

Proof. (Direct) We need to show that there exists integers a, b where $x = 2a + 1 \implies x^2 = 2b + 1$

$$\begin{aligned} x = 2a + 1 \implies x^2 &= (2a + 1)^2 && (3.1) \\ &= 4a^2 + 4a + 1 && (3.2) \\ &= 2(2a^2 + a) + 1 && (3.3) \\ &= 2b + 1, \quad b = 2a(a + 1). && (3.4) \end{aligned}$$

Since a is an integer, then $b = 2a(a + 1)$ is an integer by closure of addition and multiplication. □

Theorem 2 (Pythagoras)**.** *For any right triangle with edges abc and hypotenuse c, we have that*

$$a^2 + b^2 = c^2. \tag{3.5}$$

Proof. For any right triangle abc with hypotenuse c, we can rotate four identical such triangles to construct a square of edge lengths $a + b$, where another square of length with edge lengths c is inscribed (see example in Figure 1).

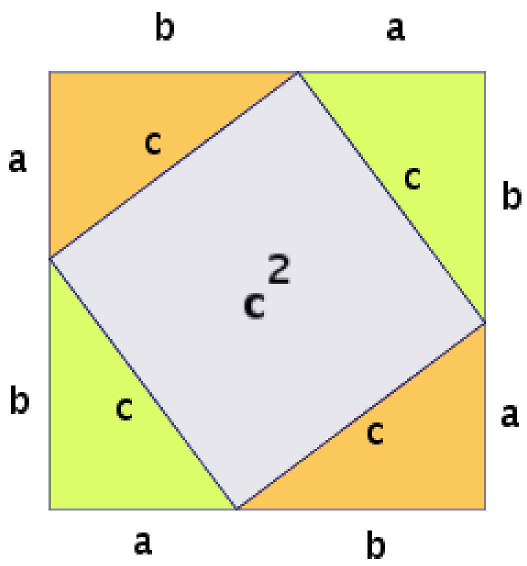

Figure 1: Construction of right triangle

The area of each of each triangle abc is $\frac{1}{2}ab$ (which can also be proved). The area of the larger square is $(a + b)^2$, and the smaller gray square is c^2.

Then we have that from subtracting the area of the large square with the four triangles that

$$c^2 = (a + b)^2 - \left(4\frac{1}{2}ab\right) = (a^2 + 2ab + b^2) - \left(2ab\right) = a^2 + b^2.$$

Then we have that $c^2 = a^2 + b^2$, as required. □

Exercise 3.1. *Prove that if x is an even integer, then xy is even for any integer y.*

Exercise 3.2. *Prove that if x is an odd integer, then x^3 is odd.*

3.2 Proof by cases

Proof by cases or **proof by exhaustion** is another kind of direct proof, where we exhaust all possible cases of the statement.

Proposition 3.2. *For any $y \geq 0$, we have that $|x| \leq y \implies (-y \leq x) \vee (x \leq y)$ (or alternatively, $-y \leq x \leq y$).*

Proof. The absolute function can be defined as

$$|x| = \begin{cases} x, & x \geq 0, \\ -x, & x \leq 0. \end{cases} \tag{3.6}$$

We can show that the implication is true when $x \leq 0$ and when $x \geq 0$, which exhausts all cases of $|x| \leq y$.

Case 1: If $x \leq 0$, then

$$|x| \leq y \implies -x \leq y \implies x \geq -y, \tag{3.7}$$

which is the first necessary statement in the disjunction.

Case 2: If $x \geq 0$, then

$$|x| \leq y \implies x \leq y, \tag{3.8}$$

which is the second necessary statement in the disjunction.

Then we have that

$$\begin{aligned} |x| \leq y \wedge [(x \leq 0) \vee (x \geq 0)] &\implies (-y \leq x) \vee (x \leq y) && (3.9) \\ \iff \quad |x| \leq y &\implies (-y \leq x) \vee (x \leq y), && (3.10) \end{aligned}$$

since $(x \leq 0) \vee (x \geq 0)$ is a tautology.

□

Exercise 3.3. *Prove that $|x| \geq y \implies (x \leq -y) \vee (x \geq y)$.*

Exercise 3.4. *Prove that if x, y are either both even or both odd, then $x + y$ is even.*

Exercise 3.5. *Prove that if x, y are not both even or both odd, then $x + y$ is odd.*

3.3 Proof by contrapositive

We can also prove statements with **indirect proofs**, which do not show the truth of the statement from only direct implications. The first type of indirect proof we will look at is **contrapositive proof**.

A conditional statement $P \implies Q$ is logically equivalent to the **contrapositive statement**, $\neg Q \implies \neg P$ (which can be verified with a truth table). Therefore we can prove the original conditional statement by proving the contrapositive instead.

Let's look at the same example as before, but using contrapositive proof.

Proposition 3.3. *For an integer x, if $x^2 - 6x + 5$ is even, then x is odd.*

Proof. (Contrapositive) We need to show the **contrapositive** is true, that

$$x \text{ is not odd} \implies x^2 - 6x + 5 \text{ is not even}. \tag{3.11}$$

If x is not odd then it is even, then there is an integer a where

$$\begin{aligned} x = 2a \implies x^2 - 6x + 5 &= (2a)^2 - 6(2a) + 5 && (3.12) \\ &= 4a^2 - 12a + 5 && (3.13) \\ &= a(4a - 12) + 5 && (3.14) \end{aligned}$$

We can show that $a(4a-12)+5$ is odd since

$$\begin{aligned}
& 4a && \text{is even by product of an even integer} && (3.15)\\
\implies & 4a-12 && \text{is even by sum of two even integers} && (3.16)\\
\implies & a(4a-12) && \text{is even by product of an even integer} && (3.17)\\
\implies & a(4a-12)+5 && \text{is odd by sum of two opposite parities} && (3.18)
\end{aligned}$$

See exercise 3.1 for (3.15) and (3.17), exercise 3.4 for (3.16), and exercise 3.5 for (3.18). Then we have that

$$x = 2a \text{ is even} \implies x^2 - 6x + 5 = a(4a-12)+5 \text{ is odd}, \tag{3.19}$$

which is the contrapositive of the original proposition. □

Definition 3.3 (Informal). *The derivative of a function $f(x)$ at x can be approximated as*

$$f'(x) \simeq \frac{f(x+dx)-f(x)}{dx} \simeq \frac{f(x)-f(x-dx)}{dx}, \; dx > 0. \tag{3.20}$$

Assume these approximations hold as equalities for an (infinitesimally) small $dx > 0$.

Proposition 3.4 (FOC). *Let $f(x)$ be differentiable. If $f(x^*)$ is the maximum of $f(x)$, then $f'(x^*) = 0$.*

Proof. (Contrapositive) We can informally prove the contrapositive of the proposition, which is that

$$f'(x^*) = \frac{f(x^*+dx)-f(x^*)}{dx} = \frac{f(x^*)-f(x^*-dx)}{dx} \neq 0 \implies f(x^*) \text{ is not the maximum.} \tag{3.21}$$

There are two cases where $f'(x^*) \neq 0$, which are $f'(x^*) > 0$ and $f'(x^*) < 0$.

Case 1. If $f'(x^*) > 0$, then there is a small $dx > 0$ where

$$\begin{aligned}
f'(x^*) = \frac{f(x^*+dx)-f(x^*)}{dx} > 0 &\implies = \frac{f(x^*+dx)}{dx} > \frac{f(x^*)}{dx} && (3.22)\\
&\implies f(x^*+dx) > f(x^*), && (3.23)
\end{aligned}$$

which means $f(x^*)$ is not the maximum.

Case 2. If $f'(x^*) < 0$, then there is a small $dx > 0$ where

$$\begin{aligned}
f'(x^*) = \frac{f(x^*)-f(x^*-dx)}{dx} < 0 &\implies = \frac{f(x^*)}{dx} < \frac{f(x^*-dx)}{dx} && (3.24)\\
&\implies f(x^*) < f(x^*+dx), && (3.25)
\end{aligned}$$

which also means $f(x^*)$ is not the maximum.

In both cases $f'(x^*) > 0$ and $f'(x^*) < 0$, we see that $f(x^*)$ is not a maximum. Therefore $f'(x^*) \neq 0$ always implies $f(x^*)$ is not the maximum, which is the contrapositive as required. □

Exercise 3.6. *Prove that for a differentiable function $f(x)$, if $f(x^*)$ is the minimum, then $f'(x^*) = 0$.*

Exercise 3.7. *Prove that for any real numbers x and y, if $y^3 + yx^2 \leq x^3 + xy^2$, then $y \leq x$.*

3.4 Proof by contradiction

Another indirect proof method to show P is true is to show that there is a contradiction from assuming $\neg P$ is true.

This is valid since the statement $P \iff (\neg P \implies Q) \wedge (\neg P \implies \neg Q)$ is a tautology, which says that if P is true, then assuming $\neg P$ is true causes a contradiction from its implications.

Proposition 3.5. *If x^2 is even, then x is even.*

Note that the negation of a conditional statement $P \implies Q$ is $P \wedge \neg Q$:

$$\begin{aligned}
\neg[P \implies Q] &\equiv \neg[\neg P \vee (P \wedge Q)] && \text{by definition of implication} && (3.26)\\
&\equiv P \wedge \neg(P \wedge Q) && \text{by de Morgan's law} && (3.27)\\
&\equiv P \wedge (\neg P \vee \neg Q) && \text{by de Morgan's law} && (3.28)\\
&\equiv (P \wedge \neg P) \vee (P \wedge \neg Q) && \text{by distributivity} && (3.29)\\
&\equiv F \vee (P \wedge \neg Q) && \text{by contradiction} && (3.30)\\
&\equiv P \wedge \neg Q && \text{by annihilation} && (3.31)
\end{aligned}$$

Proof. (Contradiction) For the sake of contradiction, suppose x^2 is even and x is not even. Then x is odd, and there exists some number a where $x = 2a + 1$. Then

$$\begin{aligned}
x = 2a + 1 \implies x^2 &= (2a + 1)^2 && (3.32)\\
&= 4a^2 + 4a + 1 && (3.33)\\
&= 2b + 1, \; b = 2a(a + 1). && (3.34)
\end{aligned}$$

Then x^2 is odd, which contradicts the assumption that x^2 is even. □

Definition 3.4 (Rationality)**.** *A number q is **rational** if it can be expressed as a quotient of two integers without common denominators.*

$$q \in \mathbb{Q} \iff \exists\, m, n \in \mathbb{Z}, \; q = \frac{m}{n}. \tag{3.35}$$

*If $q \in \mathbb{R}$ and q is not rational, then it is **irrational**.*

Proposition 3.6. *The number $\sqrt{2}$ is irrational.*

Proof. (Contradiction) For sake of contradiction, suppose that $\sqrt{2}$ is rational. Then there exists $p, q \in \mathbb{Z}$ with no common factors where $\sqrt{2} = \frac{p}{q}$. Then we have that

$$\begin{aligned}
\sqrt{2} = \frac{p}{q} &\implies 2 = \frac{p^2}{q^2}\\
&\implies p^2 = 2p^2.
\end{aligned}$$

Since p is an integer, then p must be divisible by 2, thus $p = 2m$ for some $m \in \mathbb{Z}$. Then we have that

$$\begin{aligned}
2q^2 = p^2, p = 2m &\implies 2q^2 = 4m^2\\
&\implies q^2 = 2m^2.
\end{aligned}$$

Since q is also an integer, it must also be divisible by 2. Then both p and q are divisible by two, which contradicts the statement that they have no common factors. □

Definition 3.5. *A prime number p is a natural number that is only divisible by one and itself. That is, for any other number n, the remainder from $p \div n$ is not 0.*

This definition implies that if a number $\hat{p}$ is **not divisible by any prime**, then $\hat{p}$ is a prime.

Theorem 3. *(Euclid) There are infinitely many prime numbers.*

Proof. (contradiction Suppose for the sake of contradiction that there are finitely many primes. In other words, we can exhaustively list the n many finite primes in ascending order:

$$p_1,\ p_2,\ p_3,\ p_4, ...,\ p_n = 2,\ 3,\ 5,\ 7, ...,\ p_n, \tag{3.36}$$

where p_n is the largest prime number.

Let p^* be the one plus the product of all finite primes:

$$p^* = 1 + \prod_{i=0}^{n} p_i = 1 + (p_1 \times p_2 \times ... \times p_n). \tag{3.37}$$

The number p^* is not divisible by any of other other primes since $p^* \div p_i$ always has remainder 1, which is not 0. Since p^* is not divisible by any prime, then p^* must be a prime. But p^* is not included in the list of primes $p_1, p_2, ..., p_n$, since $p^* > p_n$, the largest prime.

Thus there cannot be such a finite list, as you can always construct a number not divisible by any prime like above, which by definition makes it a prime not included in the list of primes—a contradiction. $\square$

Exercise 3.8. *For any natural number n, $n+1$ is a natural number, and $n+1 \neq 0$. Prove that there are infinitely many natural numbers.*

Exercise 3.9. *Prove that $\sqrt{3}$ is irrational.*

Exercise 3.10. *Prove that $\sqrt[3]{2}$ is irrational.*

Exercise 3.11. *For $n \in \mathbb{N},\ n > 1$, show that if p is prime, then $\sqrt[n]{p}$ is irrational.*

3.5 Proof by induction

The last proof method we will look at is **induction**, which has to do with statements predicated on a natural number, $P(n),\ n \geq b,\ n \in \mathbb{N}$.

Induction proofs involve two steps:

(a) Proof of the **base case**, that $P(b)$ is true.

(b) Proof of the **inductive step,** that $P(k) \implies P(k+1)$.

Since $P(b)$ is true, and $P(k) \implies P(k+1)$, then $P(b) \implies P(b+1) \implies ... \implies P(n-1) \implies P(n)$.

Then we have

$$P(b) \wedge [P(b) \implies P(n)] \implies P(n). \tag{3.38}$$

Proposition 3.7. *For all natural numbers $n \geq 1$, we have that*

$$1 + 2 + 3 + ... + n = \sum_{m=1}^{n} m = \frac{n(n+1)}{2} \tag{3.39}$$

Proof. We will prove this with mathematical induction.

Base case: For $n = \sum_{m=1}^{n} m = 1$, we have that

$$\frac{n(n+1)}{2} = \frac{1(1+1)}{2} = 1. \tag{3.40}$$

Inductive step: We want to show that

$$\sum_{m=1}^{k} m = \frac{k(k+1)}{2} \implies \sum_{m=1}^{k+1} m = \frac{(k+1)(k+2)}{2}. \tag{3.41}$$

We have that

$$\sum_{m=1}^{k} m = \frac{k(k+1)}{2} \implies \sum_{m=1}^{k+1} m = [1+2+...+k]+(k+1) = \left[\sum_{m=1}^{k} m\right] + (k+1) \tag{3.42}$$

$$= \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)+2(k+1)}{2} \tag{3.43}$$

$$= \frac{(k+1)(k+2)}{2}. \tag{3.44}$$

Then it follows by induction that $1+2+3+...+n = \frac{n(n+1)}{2}$. □

Definition 3.6 (Fibonacci)**.** *The Fibonacci sequence* $\{F_n\}_1^\infty$ *follows* $F_1 = 1,\ F_2 = 2,$ *and for* $n > 2$*,*

$$F_n = F_{n-2} + F_{n-1} \tag{3.45}$$

Proposition 3.8. *The Fibonacci sequence obeys*

$$F_{n+1}^2 - F_n^2 - F_{n+1} \cdot F_n = (-1)^n \tag{3.46}$$

Proof. We will prove this with mathematical induction.

Base case: For $n = 1$, we have that $(-1)^n = (-1)^1 = -1$, and

$$F_{n+1}^2 - F_n^2 - (F_{n+1} \cdot F_n) = F_2^2 - F_1^2 - (F_{n+1} \cdot F_n) = 1 - 1 - (1 \cdot 1) = -1. \tag{3.47}$$

Inductive step: We want to show that

$$F_{k+1}^2 - F_k^2 - (F_{k+1}F_k) = (-1)^k \implies F_{k+2}^2 - F_{k+1}^2 - (F_{k+2}F_{k+1}) = (-1)^{k+1}. \tag{3.48}$$

If $F_{k+1}^2 - F_k^2 - F_{k+1}F_k = (-1)^k$, then

$$F_{k+2}^2 - F_{k+1}^2 - (F_{k+2} \cdot F_{k+1}) = (F_{k+1} + F_k)^2 - F_{k+1}^2 - ([F_{k+1} + F_k]F_{k+1}) \tag{3.49}$$

$$= (F_{k+1}^2 + 2F_k \cdot F_{k+1} + F_k^2) - F_{k+1}^2 - (F_{k+1}^2 + F_k \cdot F_{k+1}) \tag{3.50}$$

$$= F_k \cdot F_{k+1} + F_k^2 - F_{k+1}^2 \tag{3.51}$$

$$= (-1)(F_{k+1}^2 - F_k^2 - F_k \cdot F_{k+1}) \tag{3.52}$$

$$= (-1)(-1)^n = (-1)^{n+1}. \tag{3.53}$$

Then the induction proof is complete. □

Exercise 3.12. *Show by induction that for any* $n \geq 1$ *and any* $x \in \mathbb{R}$*,*

$$\sum_{m=0}^{n} x = nx. \tag{3.54}$$

Exercise 3.13. *Show that for any* $r \neq 1$*,*

$$\sum_{m=0}^{n} r^m = \frac{1 - r^{n+1}}{1 - r}. \tag{3.55}$$

Exercise 3.14. *Show that for any* $n \geq 1$ *and any* $x \in \mathbb{R}$*,*

$$\sum_{m=0}^{n} m^2 = \frac{n(n-1)(2n-1)}{6}. \tag{3.56}$$

Exercise 3.15. *Prove the binomial theorem, that for any natural* $n \geq 0$*,*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k, \quad \binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{3.57}$$

References

- ▷ Hardy, G.H., (1950). *A Mathematician's Apology*. Cambridge University Press. http://www.arvindguptatoys.com/arvindgupta/mathsapology-hardy.pdf
- ▷ Hammack, Richard, (2018). *Book of Proof, third edition*. Richard Hammack. https://www.people.vcu.edu/~rhammack/BookOfProof/
- ▷ Rayo, Agustin, (2020). *About this class*, lecture. Paradox and Infinity. MIT Open Learning Library. https://openlearninglibrary.mit.edu/courses/course-v1:MITx+24.118x+2T2020/course
- ▷ Leighton, Tom, & Dijk, Marten. (2010, Fall) *Lecture 1*. 6.042J Mathematics for Computer Science. Massachusetts Institute of Technology: MIT OpenCourseWare. https://youtu.be/L3LMbpZIKhQ
- ▷ Statements and Logical Operators. (2021, September 5). Grand Valley State University. https://math.libretexts.org/@go/page/7039
- ▷ Tao, Terence. (2003). *Week 1*, lecture notes. Honors Analysis Math131AH. University of California, Los Angeles. https://www.math.ucla.edu/~tao/resource/general/131ah.1.03w/
- ▷ Tao, Terence. (2016). *Analysis I, third edition*. Springer Singapore.