Formal Proof Methodology

Jason Filippou

CMSC250 @ UMCP

06-09-2016
Today’s agenda

- We will talk about how to formally prove mathematical statements.
  - Some connection to inference in propositional and predicate logic.
- More Number Theory definitions will be given as we string along.
Outline

1. Categories of statements to prove

2. Proving Existential statements

3. Proving Universal statements
   - Direct proofs
   - Disproving Universal Statements
   - Indirect proofs

4. Three famous theorems
Categories of statements to prove
Existential statements

- Statements of type:

  $$(\exists x \in D) P(x)$$

  are referred to as **existential statements**.

- They require us to prove a property $P$ for some $x \in D$.

- Two ways that we deal with those questions:
  - **Constructively**: We “construct” or “show” an element of $D$ for which $P$ holds and we’re done (why)?
  - **Non-constructively**: We neither construct nor show such an element, but we prove that it’s a **logical necessity** for such an element to exist!

- Examples:
  - There exists a least prime number.
  - There exists no greatest prime number.
  - $$(\exists a, b) \in \mathbb{R} - \mathbb{Q} : a^b \in \mathbb{Q}$$
Categories of statements to prove

**Universal statements**

- Statements of type:

\[(\forall x \in D)P(x)\]

are referred to as **universal statements**.

- They require of us to prove a property \(P\) for every single \(x \in D\).
  - Most often, \(D\) will be \(\mathbb{Z}\) or \(\mathbb{N}\).

- We can prove such statements **directly** or **indirectly**.

- They constitute the **majority** of statements that we will deal with.

- Examples:
  - \((\forall n \in \mathbb{Z}^{\text{odd}}), \ (\exists k \in \mathbb{Z}) : n = 8k + 1\)
  - \((\forall n \in \mathbb{Z}), \ n^2 \in \mathbb{Z}^{\text{odd}} \Rightarrow n \in \mathbb{Z}^{\text{odd}}\)
  - Every Greek politician is a crook.
Categories of statements to prove

Proving the affirmative or the negative

- Given a mathematical statement $S$, $S$ can be either true or false (law of excluded middle).
- We will call a proof that $S$ is True a proof of the **affirmative**.
- We will call a proof that $S$ is False a proof of the **negative**.
- Recall negated quantifier equivalences:
  \[
  \sim(\exists x)P(x) \equiv (\forall x)\sim P(x) \\
  \sim(\forall x)P(x) \equiv (\exists x)\sim P(x)
  \]
- So, arguing the negative of an existential statement is equivalent to arguing the positive for a universal statement, and vice versa!
Proving Existential statements
Constructive proofs

Theorem (Least prime number)

There exists a least prime number.

Proof: Existence of a least prime number.

By the definition of primality, an integer \( n \) is prime iff \( n \geq 2 \) and its only factors are 1 and itself. 2 satisfies both requirements and because of the definition, no prime \( p \) exists such that \( p < 2 \). End of proof.
Constructive proofs

Let’s all prove the affirmatives of the following statements together:

**Theorem**

There exists an integer \( n \) that can be written in two ways as a sum of two prime numbers.

**Theorem**

Suppose \( r, s \in \mathbb{Z} \). Then, \( \exists k \in \mathbb{Z} : 22r + 18s = 2k \).
Constructive proofs

Let’s all prove the affirmatives of the following statements together:

**Theorem**

There exists an integer $n$ that can be written in two ways as a sum of two prime numbers.

**Theorem**

Suppose $r, s \in \mathbb{Z}$. Then, $\exists k \in \mathbb{Z} : 22r + 18s = 2k$.

**Definition (Perfect squares)**

An integer $n$ is called a **perfect square** iff there exists an integer $k$ such that $n = k^2$.

**Theorem**

There is a perfect square that can be written as a sum of two other perfect squares.
Non-Constructive proofs

Here’s a rather famous example of a non-constructive proof:

Theorem

There exists a pair of irrational numbers $a$ and $b$ such that $a^b$ is a rational number.
Non-Constructive proofs

Here’s a rather famous example of a non-constructive proof:

**Theorem**

There exists a pair of irrational numbers $a$ and $b$ such that $a^b$ is a rational number.

**Proof.**

Let $a = b = \sqrt{2}$. We know that $\sqrt{2}$ is irrational\(^a\), so $a$ and $b$ are both irrational. Is $a^b$ rational? Two cases:

- If yes, the statement is proven.
- If not, then it is irrational by the definition of real numbers.
  
  Examine the number $((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}}$. This number is rational, because 
  
  $((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2 = \frac{2}{1}$. End of proof.

\(^a\)In fact, we will prove that formally down the road.
Proving Universal statements
Direct proofs
Proof by exhaustion

- When my domain $D$ is sufficiently small to explore by hand, I might consider a proof by (domain) exhaustion.
- Example:

**Theorem**

For every even integer between (and including) 4 and 30, $n$ can be written as a sum of two primes.

**Proof.**

\[
\begin{align*}
4 &= 2 + 2 & 6 &= 3 + 3 & 8 &= 3 + 5 & 10 &= 5 + 5^a \\
12 &= 5 + 7 & 14 &= 7 + 7 & 16 &= 13 + 3^b & 18 &= 7 + 11 \\
20 &= 7 + 13 & 22 &= 5 + 17 & 24 &= 5 + 19 & 26 &= 7 + 19 \\
28 &= 11 + 17 & 30 &= 11 + 19
\end{align*}
\]

\[^a\text{Also, } 10 = 3 + 7 \]

\[^b\text{Also, } 16 = 11 + 5 \]
Universal generalization

- Reminder: Rule of **universal generalization**.

**Universal Generalization**

\[ P(A) \text{ for an arbitrarily chosen } A \in D \]
\[ \therefore (\forall x \in D)P(x) \]
Proving Universal statements

Direct proofs

Universal generalization

Reminder: Rule of universal generalization.

Universal Generalization

\[ P(A) \text{ for an arbitrarily chosen } A \in D \]
\[ \therefore (\forall x \in D)P(x) \]

- A: Generic particular (particular element, yet arbitrarily - generically - chosen)
- Needs to be explicitly mentioned.
- Choice of generic particular often perilous.
- Most of our proofs will be of this form.
Example

Theorem (Odd square)

The square of an odd integer is also odd.

Symbolic proof.

Let $a \in \mathbb{Z}$ be a generic particular of $\mathbb{Z}$. Then, by the definition of odd integers, $\exists k \in \mathbb{Z} : a = 2k + 1$. Then,

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2k(2k + 2) + 1 = 2r + 1$$

where $r \in \mathbb{Z}$. 

Question: Is $k$ a generic particular in this proof? What about $r$?
Example

Theorem (Odd square)

The square of an odd integer is also odd.

Symbolic proof.

Let $a \in \mathbb{Z}$ be a generic particular of $\mathbb{Z}$. Then, by the definition of odd integers, $\exists k \in \mathbb{Z} : a = 2k + 1$. Then,

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2k(2k + 2) + 1 = 2r + 1$$

$\{r \in \mathbb{Z}\}$

Question: Is $k$ a generic particular in this proof? What about $r$?
Example

Textual proof.

Let $a$ be a generic particular for the set of integers. Then, by definition of odd integers, we know that there exists an integer $k$ such that $a = 2k + 1$. Then,

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2k(2k + 2) + 1 \quad (1)$$

Let $r = k(2k + 2)$ be an integer. Substituting the value of $r$ into equation 1, we have that $a^2 = 2r + 1$. But this is exactly the definition of an odd integer, and we conclude that $a$ is odd. End of proof.
Let’s prove some universal statements.
Before proving them, make sure you understand what they ask.
Practice

- Let’s prove some universal statements.
- Before proving them, make sure you understand what they ask.

**Theorem**

The sum of any two odd integers is even.

**Theorem**

\((n \in \mathbb{Z}^{\text{odd}}) \Rightarrow (-1)^n = -1\).
Another popular way to prove universal statements is by dividing $D$ into sub-domains and proving the statement for every sub-domain.

Popular divisions: \{\mathbb{Z}^{\text{odd}}, \mathbb{Z}^{\text{even}}\}, \{\mathbb{R}^*, \mathbb{R}^+\}, \{2, \mathbb{P} - \{2\}\}

Example:

**Theorem**

*Any two consecutive integers have opposite parity.*
Proof.

Let $a \in \mathbb{Z}$ be a generic particular. Then, $a + 1$ is its consecutive integer. $a$ will be either odd or even. We distinguish between those two cases:

1. **Assume $a$ is odd.** Therefore, by the definition of odd numbers,
   \[
   \exists k \in \mathbb{Z} : a = 2k + 1 \implies a + 1 = (2k + 1) + 1 \implies a + 1 = 2(k + 2) \implies a + 1 = 2r. \]
   Therefore, $a + 1$ is even.

2. **Assume $a$ is even.** Therefore, by the definition of even numbers,
   \[
   \exists k \in \mathbb{Z} : a = 2k \implies a + 1 = 2k + 1. \]
   Therefore, $a + 1$ is odd.
Critique the following proof segments:

**Proof.**

Let $p, q \in \mathbb{Q}$ be generic particulars. Let also $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{Z}^*$ be generic particulars such that $p = \frac{a}{b}$ and $c = \frac{c}{d}$. ...

**Proof.**

Suppose $m, n$ are generic particulars for the set of odd integers. Then, by definition of odd, $m = 2k + 1$ and $n = 2k + 1$ for some integer $k$. ...

Generic pitfalls in particular proofs

Critique the following proof segments:

Proof.

Let \( p, q \in \mathbb{Q} \) be generic particulars. Let also \( a, c \in \mathbb{Z} \) and \( b, d \in \mathbb{Z}^* \) be generic particulars such that \( p = \frac{a}{b} \) and \( c = \frac{c}{d} \). …

Proof.

Suppose \( m, n \) are generic particulars for the set of odd integers. Then, by definition of odd, \( m = 2k + 1 \) and \( n = 2k + 1 \) for some integer \( k \). …

In the second proof above, which one among \( m \) and \( n \) is truly a generic particular?
Disproving Universal Statements
The counter-example

- Recall: $\neg(\forall x)P(x) \equiv (\exists x)\neg P(x)$
- So an **existential** proof of the negative is required.
  - Most often, this will be a constructive proof.
- The idea works for **all** direct proof methodologies we’ve discussed.
Examples

Theorem

*Every odd number between 3 and 13 inclusive is prime.*
Examples

Theorem

*Every odd number between 3 and 13 inclusive is prime.*

Disproof.

9 is an odd number between 3 and 13 for which

\[(\exists p, q) \in \mathbb{N} \setminus \{1, 9\} : p \cdot q = 9, \text{ since } 9 = 3 \times 3. \text{ Therefore, } 9 \text{ is composite and the statement is false.}\]
Theorem

Every odd number between 3 and 13 inclusive is prime.

Disproof.

9 is an odd number between 3 and 13 for which
(∃p, q) ∈ ℤ − {1, 9} : p · q = 9, since 9 = 3 × 3. Therefore, 9 is composite and the statement is false.

Theorem

(∀n) ∈ ℤ ⇒ (−1)^n = −1.
Examples

Theorem

\textit{Every odd number between 3 and 13 inclusive is prime.}

Disproof.

9 is an odd number between 3 and 13 for which $(\exists p, q) \in \mathbb{N} - \{1, 9\} : p \cdot q = 9$, since $9 = 3 \times 3$. Therefore, 9 is composite and the statement is false.

Theorem

$(\forall n) \in \mathbb{P} \Rightarrow (-1)^n = -1$.

Disproof.

$2 \in \mathbb{P}$, but $(-1)^2 = 1$. Therefore, the statement is false.
Indirect proofs
Proof by contradiction

- Recall the definition of the **law of contradiction** from propositional logic:

  **Law of Contradiction**
  
  \[ \sim p \Rightarrow c \]
  
  \[ \therefore p \]

- Tremendously useful and famous proof mechanism.

- Use when a counter-example isn’t obvious and direct proof has lead nowhere.
Proof by contradiction

- General idea: We want to prove a statement \( p \). If we assume \( \neg p \) and reach a contradiction, then, by the law of contradiction, we can infer \( p \).
- So, for a universal statement \( (\forall x)P(x) \), we assume \( (\neg\forall x)P(x) \equiv (\exists x)\neg P(x) \), and aim towards a contradiction.
- Equivalently for an existential statement.
- Since, when we reach the contradiction, the only additional assumption we’ve made is that \( p \) is false, \( p \) has to be true.
- ***ALWAYS*** mention the discovery of a contradiction clearly within your proof, e.g:
  - “Contradiction, because XYZ.”
  - “Since XYZ, we have reached a contradiction.”
Applications

Theorem

There is no greatest integer.
Applications

Theorem

*There is no greatest integer.*

Proof.

Assume not. Then, \((\exists M \in \mathbb{Z}) : (\forall m \in \mathbb{Z}), M \geq m.\) But the real number \(N = M + 1\) is also an integer, since it’s a sum of two integers. Since \(N > M\), we have reached a contradiction, and we conclude that a greatest integer cannot possibly exist.
Theorem

Prove that the sum of a rational and irrational number is irrational.
Theorem

Prove that the sum of a rational and irrational number is irrational.

Proof.

Assume not. So, there exists a rational $r$ and an irrational $q$ such that $r + q$ is rational. By the definition of rational numbers, there exist integers $a, b, c, d$, with $b$ and $d$ non-zero, such that $r = \frac{a}{b}$ and $r + q = \frac{c}{d}$. Solving for $q$, we obtain:

$$r + q = \frac{c}{d} \iff \frac{a}{b} + q = \frac{c}{d} \iff q = \frac{a}{b} - \frac{c}{d} \iff q = \frac{ad - bc}{bd}$$

Both $ad - bc$ and $bd$ are integers, because they are linear combinations\(^a\) of integers. Furthermore, $bd \neq 0$ because both $b$ and $d$ are non-zero. But this means that $q$ can be written as a fraction of an integer over a non-zero integer. This contradicts our assumption that $q$ is irrational, which means that the statement is true, and $r + q$ must be irrational.

\(^a\)Sums of products.
To do some more interesting problems with proof by contradiction, let’s introduce some more Number Theory.

Definition (Divisibility)
Let \( n \in \mathbb{Z} \) and \( d \in \mathbb{Z}^* \). Then, we say or denote one of the following:

- \( d \) divides \( n \)
- \( n \) is divided by \( d \)
- \( d \mid n \)
- \( d \) is a divisor (or factor) of \( n \)
- \( n \) is a multiple of \( d \)

iff \( \exists k \in \mathbb{Z} : n = d \cdot k \)
To do some more interesting problems with proof by contradiction, let’s introduce some more Number Theory.

**Definition (Divisibility)**

Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^*$. Then, we say or denote one of the following:

- $d$ divides $n$
- $n$ is divided by $d$
- $d | n$
- $d$ is a divisor (or factor) of $n$
- $n$ is a multiple of $d$

**iff** $\exists k \in \mathbb{Z} : n = d \cdot k$

Some notation: If $a$ does **not** divide $b$, we denote: $a \nmid b$.

**Attention:** $a | b$ is not the same as $a/b$!
Properties of divisibility

- All the following can be proven:

**Theorem (All non-zero integers divide zero)**

$$\forall n \in \mathbb{Z}^*, n|0.$$
Properties of divisibility

- All the following can be proven:

  **Theorem (All non-zero integers divide zero)**
  \[ \forall n \in \mathbb{Z}^*, n \mid 0. \]

- *What about* \( 0 \mid n (\forall n \in \mathbb{Z})? \)
Properties of divisibility

- All the following can be proven:

**Theorem (All non-zero integers divide zero)**
\[ \forall n \in \mathbb{Z}^*, n | 0. \]

- What about \(0 | n(\forall n \in \mathbb{Z})?\)

**Theorem (Transitivity of divisibility)**
\[ (\forall a, b, c \in \mathbb{Z}) a | b \land b | c \Rightarrow a | c \]

- Is divisibility **commutative**?
Prove these!

- Prove the affirmative for all those theorems.

**Theorem**

*For all integers* \(a, b, c\), *if* \(a \not| bc\) *then* \(a \not| b\).

**Theorem**

\[(\forall a, b, c \in \mathbb{Z})(((a|b) \land (a \not| c)) \Rightarrow a \not|(b + c))\]

- Once again, note how different the style of presentation of all of those theorems is.
Here’s two hard ones!

Theorem

*Any integer* \( n > 1 \) *is divisible by a prime number.*

Theorem

*For any integer* \( a \) *and prime* \( p \), \( p | a \) \( \Rightarrow \) \( p \nmid (a + 1) \)

- Prove these at home!
Proving Universal statements

Indirect proofs

LOL WUT (pitfalls with contradictions)

Theorem

*Every integer is rational.*

- We’ve already proven this directly.
- The following is a proof by contradiction of the same fact.

Proof.

Suppose not. Then, every integer is irrational. Since every integer is irrational, so is 0. But we know that we can express 0 as a ratio of integers, e.g.\[ a \quad 0 = \frac{0}{1}. \] By the definition of rational numbers, this means that \( 0 \in \mathbb{Q} \). This contradicts our assumption that every integer is irrational, which means that the statement is true.

\[ a \text{This means “for example”} \]

- What’s going on here?
Proof by contraposition

- A somewhat more rare kind of proof.
- Takes advantage of the equivalence $a \Rightarrow b \equiv \sim b \Rightarrow \sim a$.
- Idea: If you’re having trouble directly proving a universal statement, maybe proving its contrapositive will be easier!
- Example:

**Theorem**

$$(\forall n \in \mathbb{Z}), n^2 \in \mathbb{Z}_{\text{even}} \Rightarrow n \in \mathbb{Z}_{\text{even}}.$$ 

**Proof.**

We can equivalently prove that $(\forall n \in \mathbb{Z}), n \in \mathbb{Z}_{\text{odd}} \Rightarrow n^2 \in \mathbb{Z}_{\text{odd}}$. This was the first universal statement we proved on Thursday (see slide 16). Done.
Proving Universal statements

Indirect proofs

Applications

Prove the following through contraposition:

Theorem

Given two positive real numbers, if their product is greater than 100, then at least one of the numbers is greater than 10.

Theorem

For all integers \( m \) and \( n \), if \( m + n \) is even, then either \( m \) and \( n \) are both even or \( m \) and \( n \) are both odd.
Floor & Ceiling

- Number Theory deals with integers (whole numbers).
- Sometimes, however, we have to deal with non-integers (rationals, irrationals).
- Two functions from $\mathbb{R}$ to $\mathbb{Z}$ are $\text{floor} : \lfloor \rfloor$ and $\text{ceiling} : \lceil \rceil$. 
Floor & Ceiling

Definition (Floor and Ceiling)

Let $r$ be a real number. Then:

- The *ceiling* of $r$, denoted $\lceil r \rceil$ is the smallest integer $n$ such that $n \geq r$.
- The *floor* of $r$, denoted $\lfloor r \rfloor$ is the largest integer $n$ such that $n \leq r$.

Corollary 1

$\forall n \in \mathbb{Z}, \lfloor n \rfloor = \lceil n \rceil = n$

Corollary 2

$\forall x \in \mathbb{R}, \lfloor x \rfloor = \lceil x \rceil$ if $n < x < n+1$
Floor & Ceiling

Definition (Floor and Ceiling)
Let $r$ be a real number. Then:

- The *ceiling* of $r$, denoted $\lceil r \rceil$ is the smallest integer $n$ such that $n \geq r$.
- The *floor* of $r$, denoted $\lfloor r \rfloor$ is the largest integer $n$ such that $n \leq r$.

Corollary 1
$$\forall n \in \mathbb{Z}, \lfloor n \rfloor = \lceil n \rceil = n$$

What's the value of $\lfloor n + \frac{1}{2} \rfloor$?

What about $\lceil n + \frac{99}{100} \rceil$?
Floor & Ceiling

Definition (Floor and Ceiling)

Let $r$ be a real number. Then:

- The *ceiling* of $r$, denoted $\lceil r \rceil$ is the smallest integer $n$ such that $n \geq r$.
- The *floor* of $r$, denoted $\lfloor r \rfloor$ is the largest integer $n$ such that $n \leq r$.

Corollary 1

$$\forall n \in \mathbb{Z}, \lfloor n \rfloor = \lceil n \rceil = n$$

Corollary 2

$$\forall x \in \mathbb{R}, n = \lfloor x \rfloor \iff n - 1 < x \leq n \text{ and}$$
$$\forall x \in \mathbb{R}, n = \lceil x \rceil \iff n \leq x < n + 1$$
Floor & Ceiling

Definition (Floor and Ceiling)

Let $r$ be a real number. Then:

- The ceiling of $r$, denoted $\lceil r \rceil$ is the smallest integer $n$ such that $n \geq r$.
- The floor of $r$, denoted $\lfloor r \rfloor$ is the largest integer $n$ such that $n \leq r$.

Corollary 1

$\forall n \in \mathbb{Z}, \lfloor n \rfloor = \lceil n \rceil = n$

Corollary 2

$\forall x \in \mathbb{R}, n = \lfloor x \rfloor \iff n - 1 < x \leq n$ and
$\forall x \in \mathbb{R}, n = \lceil x \rceil \iff n \leq x < n + 1$

- What’s the value of $\lfloor n + 1/2 \rfloor$?
- What about $\lfloor n + \frac{99}{100} \rfloor$?
Proving Universal statements

Indirect proofs

Proofs with Floor / Ceiling

Prove the truth or falsehood of these conjectures. Read them carefully!

Conjecture 1

$$(\forall x, y \in \mathbb{R}), \lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$$

Conjecture 2

$$(\forall x \in \mathbb{R}, y \in \mathbb{Z}), \lfloor x + y \rfloor = \lfloor x \rfloor + y$$

Conjecture 3

For any integer $n$,

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{otherwise} \end{cases}$$
Three famous theorems
In this section, we will present three famous theorems:

1. **Unique factorization theorem.**
2. $\sqrt{2}$ is **irrational.**
3. There are infinitely many primes.

First one due to C.F Gauss, the other ones due to Euclid of Alexandria.

You need not remember their proofs, but you **need remember what they state!**
Unique Factorization Theorem

- Also referred to as the **Fundamental Theorem of Arithmetic**.

**Theorem (Fundamental Theorem of Arithmetic)**

*For all integers $n > 1$, there exist:*
Unique Factorization Theorem

- Also referred to as the **Fundamental Theorem of Arithmetic**.

**Theorem (Fundamental Theorem of Arithmetic)**

*For all integers* \( n > 1 \), *there exist*:

- \( k \in \mathbb{N}^+ \)
Unique Factorization Theorem

- Also referred to as the **Fundamental Theorem of Arithmetic**.

**Theorem (Fundamental Theorem of Arithmetic)**

*For all integers* $n > 1$, *there exist*:

- $k \in \mathbb{N}^+$
- $p_1, p_2, \ldots p_k \in \mathbb{P}$
Unique Factorization Theorem

- Also referred to as the **Fundamental Theorem of Arithmetic.**

**Theorem (Fundamental Theorem of Arithmetic)**

*For all integers $n > 1$, there exist:*

- $k \in \mathbb{N}^+$
- $p_1, p_2, \ldots p_k \in \mathbb{P}$
- $e_1, e_2, \ldots e_k \in \mathbb{N}^+$
Unique Factorization Theorem

- Also referred to as the **Fundamental Theorem of Arithmetic**.

**Theorem (Fundamental Theorem of Arithmetic)**

*For all integers* $n > 1$, *there exist:*

- $k \in \mathbb{N}^+$
- $p_1, p_2, \ldots, p_k \in \mathbb{P}$
- $e_1, e_2, \ldots, e_k \in \mathbb{N}^+$

*such that:*

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$
Unique Factorization Theorem

- Also referred to as the **Fundamental Theorem of Arithmetic**.

**Theorem (Fundamental Theorem of Arithmetic)**

*For all integers* $n > 1$, *there exist:*

- $k \in \mathbb{N}^+$
- $p_1, p_2, \ldots p_k \in \mathbb{P}$
- $e_1, e_2, \ldots e_k \in \mathbb{N}^+$

*such that:*

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$

*Additionally, this representation is *unique*: any other prime factorization is identical to this one up to re-ordering of the factors!*

Jason Filippou (CMSC250 @ UMCP)
Three famous theorems

Unique Factorization Theorem

- Also referred to as the **Fundamental Theorem of Arithmetic**.

**Theorem (Fundamental Theorem of Arithmetic)**

*For all integers* $n > 1$, *there exist:*

- $k \in \mathbb{N}^+$
- $p_1, p_2, \ldots p_k \in \mathbb{P}$
- $e_1, e_2, \ldots e_k \in \mathbb{N}^+$

such that:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots \cdot p_k^{e_k}$$

Additionally, this representation is **unique**: any other prime factorization is identical to this one up to re-ordering of the factors!

- Examples: $2 = 2^1$, $3 = 3^1$, $4 = 2^2$, $10 = 2^1 \cdot 5^1$, $20 = 2^2 \cdot 5^1$, $162 = 2^1 \cdot 3^3$, $999 = 3^3 \cdot 37$, $1000 = 2^3 \cdot 5^3$, $1001 = 7 \cdot 11 \cdot 13$
$\sqrt{2}$ is irrational

**Theorem ($\sqrt{2}$ is irrational)**

The number $\sqrt{2}$ is irrational.
Proof (by contradiction).

Suppose not. Therefore, \( \sqrt{2} \in \mathbb{Q} \Rightarrow \exists a, b \in \mathbb{Z}, b \neq 0, \) such that

\[
\sqrt{2} = \frac{a}{b}
\]  (1)
\[ \sqrt{2} \text{ is irrational} \]

**Proof (by contradiction).**

Suppose not. Therefore, \( \sqrt{2} \in \mathbb{Q} \Rightarrow \exists a, b \in \mathbb{Z}, b \neq 0 \), such that

\[
\sqrt{2} = \frac{a}{b} \tag{1}
\]

Without loss of generality, we can assume that \( a \) and \( b \) have no common factors.

By (1), we deduce that \( b^2 \) is also even and, by the same theorem, that \( b \) is even.

So, both \( a \) and \( b \) are even.

But this means that they have common factors.

Contradiction. Therefore, \( \sqrt{2} \not\in \mathbb{Q} \).
## $\sqrt{2}$ is irrational

**Proof (by contradiction).**

Suppose not. Therefore, $\sqrt{2} \in \mathbb{Q} \Rightarrow \exists a, b \in \mathbb{Z}, b \neq 0$, such that

$$\sqrt{2} = \frac{a}{b} \quad (1)$$

**Without loss of generality,** we can assume that $a$ and $b$ have no common factors. Squaring both sides of (1), we obtain:

$$a^2 = 2b^2 \quad (2)$$
Proof (by contradiction).

Suppose not. Therefore, \( \sqrt{2} \in \mathbb{Q} \Rightarrow \exists a, b \in \mathbb{Z}, \ b \neq 0, \) such that

\[
\sqrt{2} = \frac{a}{b}
\]  

(1)

Without loss of generality, we can assume that \( a \) and \( b \) have no common factors. Squaring both sides of (1), we obtain:

\[
a^2 = 2b^2
\]  

(2)

From (2) and the definition of even numbers, we deduce that \( a^2 \) is even.
Three famous theorems

$\sqrt{2}$ is irrational

Proof (by contradiction).

Suppose not. Therefore, $\sqrt{2} \in \mathbb{Q} \Rightarrow \exists a, b \in \mathbb{Z}, b \neq 0$, such that

$$\sqrt{2} = \frac{a}{b} \quad (1)$$

Without loss of generality, we can assume that $a$ and $b$ have no common factors. Squaring both sides of (1), we obtain:

$$a^2 = 2b^2 \quad (2)$$

From (2) and the definition of even numbers, we deduce that $a^2$ is even. From a known theorem, we have that $a$ is also even, therefore, $\exists m \in \mathbb{Z}$:

$$a = 2m \overset{(2)}{\Rightarrow} 4m^2 = 2b^2 \Rightarrow b^2 = 2m^2 \quad (3)$$
Three famous theorems

\( \sqrt{2} \) is irrational

**Proof (by contradiction).**

Suppose not. Therefore, \( \sqrt{2} \in \mathbb{Q} \Rightarrow \exists a, b \in \mathbb{Z}, b \neq 0 \), such that

\[
\sqrt{2} = \frac{a}{b}
\]

(1)

**Without loss of generality,** we can assume that \( a \) and \( b \) have no common factors. Squaring both sides of (1), we obtain:

\[
a^2 = 2b^2
\]

(2)

From (2) and the definition of even numbers, we deduce that \( a^2 \) is even. **From a known theorem,** we have that \( a \) is also even, therefore, \( \exists m \in \mathbb{Z} : \)

\[
a = 2m \Rightarrow 4m^2 = 2b^2 \Rightarrow b^2 = 2m^2
\]

(3)

By (3), we deduce that \( b^2 \) is also even and, by the same theorem, that \( b \) is even.
Proof (by contradiction).

Suppose not. Therefore, $\sqrt{2} \in \mathbb{Q} \Rightarrow \exists a, b \in \mathbb{Z}, b \neq 0$, such that 

$$\sqrt{2} = \frac{a}{b} \quad (1)$$

**Without loss of generality**, we can assume that $a$ and $b$ have no common factors. Squaring both sides of (1), we obtain:

$$a^2 = 2b^2 \quad (2)$$

From (2) and the definition of even numbers, we deduce that $a^2$ is even. **From a known theorem**, we have that $a$ is also even, therefore, $\exists m \in \mathbb{Z}$:

$$a = 2m \quad (2) \quad 4m^2 = 2b^2 \Rightarrow b^2 = 2m^2 \quad (3)$$

By (3), we deduce that $b^2$ is also even and, by the same theorem, that $b$ is even. So, both $a$ and $b$ are even.
\[ \sqrt{2} \] is irrational

Proof (by contradiction).

Suppose not. Therefore, \( \sqrt{2} \in \mathbb{Q} \Rightarrow \exists a, b \in \mathbb{Z}, b \neq 0, \) such that

\[ \sqrt{2} = \frac{a}{b} \quad (1) \]

**Without loss of generality**, we can assume that \( a \) and \( b \) have no common factors. Squaring both sides of (1), we obtain:

\[ a^2 = 2b^2 \quad (2) \]

From (2) and the definition of even numbers, we deduce that \( a^2 \) is even. **From a known theorem**, we have that \( a \) is also even, therefore, \( \exists m \in \mathbb{Z} : \)

\[ a = 2m \Rightarrow 4m^2 = 2b^2 \Rightarrow b^2 = 2m^2 \quad (3) \]

By (3), we deduce that \( b^2 \) is also even and, by the same theorem, that \( b \) is even. So, both \( a \) and \( b \) are even. But this means that they have common factors. Contradiction. Therefore, \( \sqrt{2} \notin \mathbb{Q} \). \( \square \)
Infinitude of primes

Theorem (Infinitude of primes)

There are infinitely many prime numbers.

Proof (by contradiction). Suppose not. Then, the set of primes is finite, so we can enumerate them in finite time in ascending order:

\[ p_1, p_2, \ldots, p_n \]

Consider the integer:

\[ N = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1. \]

Clearly, \( N > 1 \), since the smallest prime \( p_1 = 2 \).

Therefore, by a known theorem, \( N \) is divisible by a prime. Let \( p_i \in \{1, 2, \ldots, n\} \) be this prime, then \( p_i \mid N \). Clearly, \( p_i \mid p_1 \cdot p_2 \cdot \cdots \cdot p_n \), by construction of this product.

By a known theorem, \( p_i \nmid (p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1) = N \). Contradiction.

Therefore, the set of primes cannot be finite.
Theorem (Infinitude of primes)

There are infinitely many prime numbers.

Proof (by contradiction).

Suppose not. Then, the set of primes is finite, so we can enumerate them in finite time in ascending order: $p_1, p_2, \ldots, p_n$.
Three famous theorems

Infinitude of primes

Theorem (Infinitude of primes)

There are infinitely many prime numbers.

Proof (by contradiction).

Suppose not. Then, the set of primes is finite, so we can enumerate them in finite time in ascending order: $p_1, p_2, \ldots, p_n$

Consider the integer: $N = p_1 \cdot p_2 \cdots \cdot p_n + 1$. 

Clearly, $N > 1$, since the smallest prime $p_1 = 2$. Therefore, by a known theorem, $N$ is divisible by a prime. Let $p_i, i \in \{1, 2, \ldots, n\}$ be this prime, then $p_i | N$. Clearly, $p_i | p_1 \cdot p_2 \cdots \cdot p_n$, by construction of this product. By a known theorem, $p_i \nmid (p_1 \cdot p_2 \cdots \cdot p_n + 1) = N$. Contradiction.

Therefore, the set of primes cannot be finite.
Infinitude of primes

**Theorem (Infinitude of primes)**

*There are infinitely many prime numbers.*

**Proof (by contradiction).**

Suppose not. Then, the set of primes is finite, so we can enumerate them in finite time in ascending order: $p_1, p_2, \ldots, p_n$

Consider the integer: $N = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$. Clearly, $N > 1$, since the smallest prime $p_1 = 2$. 
Infinitude of primes

Theorem (Infinitude of primes)

There are infinitely many prime numbers.

Proof (by contradiction).

Suppose not. Then, the set of primes is finite, so we can enumerate them in finite time in ascending order: \( p_1, p_2, \ldots, p_n \)

Consider the integer: \( N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \). Clearly, \( N > 1 \), since the smallest prime \( p_1 = 2 \). Therefore, by a known theorem, \( N \) is divisible by a prime.
Theorem (Infinitude of primes)

There are infinitely many prime numbers.

Proof (by contradiction).

Suppose not. Then, the set of primes is finite, so we can enumerate them in finite time in ascending order: $p_1, p_2, \ldots, p_n$

Consider the integer: $N = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$. Clearly, $N > 1$, since the smallest prime $p_1 = 2$. Therefore, by a known theorem, $N$ is divisible by a prime.

Let $p_i, i \in \{1, 2, \ldots, n\}$ be this prime, then $p_i | N$. Clearly, $p_i | p_1 \cdot p_2 \cdot \cdots \cdot p_n$, by construction of this product.
Infinitude of primes

**Theorem (Infinitude of primes)**

*There are infinitely many prime numbers.*

**Proof (by contradiction).**

Suppose not. Then, the set of primes is finite, so we can enumerate them in finite time in ascending order: $p_1, p_2, \ldots, p_n$

Consider the integer: $N = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$. Clearly, $N > 1$, since the smallest prime $p_1 = 2$. Therefore, **by a known theorem**, $N$ is divisible by a prime.

Let $p_i, i \in \{1, 2, \ldots, n\}$ be this prime, then $p_i | N$. Clearly, $p_i | p_1 \cdot p_2 \cdot \cdots \cdot p_n$, by construction of this product.

**By a known theorem**, $p_i \nmid (p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1) = N$. Contradiction.

Therefore, the set of primes cannot be finite.