Mathematical Induction

Notation
\( \mathbb{N} := \{1, 2, 3, \ldots\} \) are called the “natural numbers”.

Principle of Mathematical Induction
Suppose \( S \) is a set of natural numbers (i.e. \( S \subseteq \mathbb{N} \)). If:
1) \( 1 \in S \),
2) \( k + 1 \in S \) whenever \( k \in S \).
Then \( S = \mathbb{N} \).

Example
Prove for all \( n \in \mathbb{N} \) the following formula holds: 
\[
1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.
\]

Proof:
- Let \( S = \left\{ m \in \mathbb{N} | 1^2 + \cdots + m^2 = \frac{m(m+1)(2m+1)}{6} \right\} \).
- \( 1 \in S : 1^2 = 1 \) and \( \frac{1(2)(3)}{6} = 1 \).
- Assume \( k \in S \). Show \( k+1 \in S \).
  - \( k \in S \Rightarrow 1^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6} \).
  - 
    \[
    1^2 + \cdots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2 = \frac{(k+1)(k+1)(2k+1)+6(k+1)}{6}
    \]
  - 
    \[
    = \frac{(k+1)2k^2 + 7k + 6}{6} = \frac{(k+1)(k+2)(2k+3)}{6} \quad \text{So } k+1 \in S.
    \]

Extended Principle of Mathematical Induction
Suppose \( S \) is a set of natural numbers (i.e. \( S \subseteq \mathbb{N} \)). If:
3) \( n_0 \in S \).
4) \( k+1 \in S \) whenever \( k \in S \).
Then \( \{n_0, n_0 + 1, n_0 + 2, \ldots\} \subseteq S \).

Example
Prove for \( n \geq 7 \) that \( n! \geq 3^n \).

Proof:
- Let \( S = \left\{ m \in \mathbb{N} | m! \geq 3^m \right\} \). Let \( n_0 = 7 \).
- \( 7 \in S : 7! = 5040 > 3^7 = 2187 \).
- Assume \( k \in S \). Show \( k + 1 \in S \).
  - \( k \in S \Rightarrow k! \geq 3^k \). Note by assumption \( k \geq 7 \).
• \( k!(k+1) \geq 3^k(k+1) \geq 3^k(8) \geq 3^k(3) = 3^{k+1}. \)

**Well Ordering Principle**
Every subset of \( \mathbb{N} \) other than \( \emptyset \) has a smallest element.

**Theorem**
Suppose \( S \subseteq \mathbb{N} \). If:
1) \( 1 \in S \).
2) \( k+1 \in S \) whenever \( k \in S \).
Then \( S = \mathbb{N} \).

Proof:
- Let \( T = \{ n \in \mathbb{N} \mid n \notin S \} \), i.e., \( T \) is the “complement” of \( S \).
- Want to show that \( T = \emptyset \). This is equivalent to \( S = \mathbb{N} \).
- Suppose \( T \neq \emptyset \). Then (by well ordering principle) \( T \) has a smallest element, call it \( t_1 \in T \).
- So \( t_1 - 1 \notin T \) (\( t_1 \neq 1 \) because \( 1 \in S \)), so \( t_1 - 1 \in S \).
- But by assumption 2, \( (t_1 - 1) + 1 \in S \), so \( t_1 \in S \) and \( t_1 \notin T \). Contradiction.

**Notation**
Let \( a, b \in \mathbb{N} \). Say “\( a \) divides \( b \)” (write \( a \mid b \)) if \( b = a \cdot c \) for some \( c \in \mathbb{N} \).

**Definition**
\( p \in \mathbb{N} \) is prime if the only divisors of \( p \) are 1 and \( p \), and \( p \neq 1 \).

**Extended Principle of Mathematical Induction**
Suppose \( S \) is a set of natural numbers (i.e. \( S \subseteq \mathbb{N} \)). If:
1) \( n_0 \in S \).
2) \( k+1 \in S \) whenever \( n_0, n_0 + 1, \ldots, k \in S \).
Then \( \{ n_0, n_0 + 1, n_0 + 2, \ldots \} \subseteq S \).

• Note: \( 1 < m, m' < n \), so \( m, m' \in S \). It means \( \frac{m = p_1 \cdots p_1}{m' = q_1 \cdots q_1} \) \( n = mm' = p_1 \cdots p_1 \cdot q_1 \cdots q_1 \).

**Example: False Proofs**
“Claim”: In any set of \( n \) people, all of them have the same age.

“Proof”:
- \( n = 1 \). True.
- Assume true for \( k \). Show for \( k + 1 \).
  - Let \( \{ p_1, \ldots, p_{k+1} \} \) be a set of \( k + 1 \) people.
  - Consider \( \{ p_1, \ldots, p_k \} \). They will all have the same age by assumption.
  - Consider \( \{ p_2, \ldots, p_{k+1} \} \). They will all have the same age by assumption.
So the set \( \{p_1, \ldots, p_{k+1}\} \) of \( k+1 \) people all have the same age.

The “proof” was false because if take \( k = 2 \), then \( T_1 = \{p_1\} \) and \( T_2 = \{p_2\} \) have no common element.

**Number Theory**

**Prime Numbers**

**Lemma**

Suppose \( n \in \mathbb{N} \) and \( n \neq 1 \). Then \( n \) is a product of prime numbers.

**Proof:**

- Case 1: \( n \) is prime. Done!
- Case 2: \( n \) is not prime.
  - Let \( S = \{n \in \mathbb{N} \mid n \neq 1 \text{ and } n \text{ is a product of primes}\} \).
  - \( 2 \in S \).
  - If \( 2, 3, \ldots, n-1 \in S \), then \( n \in S \):
    - Since \( n \) is not prime, there is some natural number \( m \neq 1, n \) such that \( m \mid n \), i.e. \( n = mm', m, m' \in \mathbb{N} \) where \( m, m' \neq 1, n \).

**Theorem**

There is no largest prime number.

**Proof:**

- Assume \( p \) is the largest prime number. In particular, this says \( \{2, 3, \ldots, p\} \) is the set of all primes.
- Let \( M = 2 \cdot 3 \cdots p + 1 \). Note that \( 2, 3, \ldots, p \) don’t divide \( M \).
- Now, \( M > 1 \), so there is some prime number \( q \) such that \( q \mid M \).
- But \( q \neq 2, 3, \ldots, p \), so \( q \) is a “new” prime. Contradiction.

**Theorem: Fundamental Theorem of Arithmetic**

Every natural number not equal to 1 is a product of primes, and the primes in the product are unique (including multiplicity) except for the order in which they occur.

**Proof:**

- Suppose there are natural numbers not equal to 1 with 2 distinct factorizations into primes. Then there is the smallest of such number (well-ordering), call it \( N \).
- \( N = p_1 \cdots p_k = q_1 \cdots q_l \). Note that all the \( p_i \)'s are different than the \( q_j \)'s. So in particular, \( p_1 \neq q_1 \) (say \( p_1 < q_1 \)).
- Let \( M = N - p_1q_2 \cdots q_l = q_1q_2 \cdots q_l - p_1q_2 \cdots q_l = (q_2 \cdots q_l)(p_1 - q_1) \), but also, \( M = N - p_1q_2 \cdots q_l = p_1p_2 \cdots p_k - p_1q_2 \cdots q_l = p_1(p_2 \cdots p_k - q_2 \cdots q_l) \). So \( p_1(p_2 \cdots p_k - q_2 \cdots q_l) = (q_2 \cdots q_l)(p_1 - q_1) \). Since \( p_1 \mid p_1(p_2 \cdots p_k - q_2 \cdots q_l) \Rightarrow p_1 \mid (q_2 \cdots q_l)(p_1 - q_1) \Rightarrow p_1 \mid p_1 - q_1 \Rightarrow p_1 \mid q_1 \). Contradiction!
Example

\[ 48 = 16 \cdot 3 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3 = 3 \cdot 2^4 = 2 \cdot 2 \cdot 3 \cdot 2 \cdot 2. \]

Definition

A natural number is called a **composite** if it is not 1 and it is not a prime number.

**SERIES**

- \( a_1 + a_2 + \cdots, a_i \in \mathbb{R} \) is a series.
- We focus on series with \( a_i > 0 \).

**Convergence and Divergence**

Given a series, it can either converge or diverge. For such series, we have the following criteria:

- **Diverge**: If for every number \( M > 0 \), there is some index \( k \) such that \( a_1 + \cdots + a_k > M \).
- **Converge**: If there is a fixed number \( M > 0 \) such that \( a_1 + \cdots + a_k < M \) for all \( k \). Equivalently, if for all \( M > 0 \), there exists \( j \) such that the “\( j \)-tail” \( a_{j+1} + a_{j+2} + \cdots < M \).

**Examples**

1) \( 1 + 2 + 3 + 4 + \cdots \) diverges.

2) \( 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots \) diverges. Note \( 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots = (1) + \left( \frac{1}{2} \right) + \left( \frac{1}{3} + \frac{1}{4} \right) + \left( \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} \right) + \cdots \), and each “grouping” > \( \frac{1}{2} \). So by going \( 2M \) “groupings”, we can guarantee that \( 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots > M \).

3) \( 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots \) (geometric series) converges. More generally,

\[
1 + \frac{1}{r} + \frac{1}{r^2} + \frac{1}{r^3} + \cdots = \frac{1}{1 - \left( \frac{1}{r} \right)}, \quad 0 < \frac{1}{r} < 1.
\]

So the series converges to \( 2 \).

**Theorem**

If \( p_n \) is the \( n \)th prime number, then \( \frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots \) (i.e. \( \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots \)) diverges.

**Proof:**

- Assume the series converge. Then \( \exists j \) such that \( \frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \cdots < \frac{1}{2} \).
- Let \( N \in \mathbb{N} \) be fixed, but arbitrarily.
- Let \( F(N) = \# \{ 1 \leq n \leq N \mid n \text{ is divisible only by the primes } p_1, \ldots, p_j \} \).
Now, \( N - F(N) = \# \{ 1 < n < N \mid n \text{ has a prime factor among } p_{j+1}, p_{j+2}, \ldots \} \).

\[
N - F(N) \leq \frac{N}{p_{j+1}} + \frac{N}{p_{j+2}} + \cdots = \frac{N}{p_{j+1}} + \frac{1}{p_{j+1}} + \cdots < \frac{N}{2}. \quad \text{So } N - F(N) < \frac{N}{2} \iff F(N) > \frac{N}{2}.
\]

- Write \( n = s^2 t \), \( s \) is the largest perfect square, and \( t \) is square free. Note that \( s \leq \sqrt{N} \) and \( t = p_1^{0.1} \cdots p_j^{0.1} \). So there are at most \( \sqrt{N} \) possibilities for \( s \) and at most \( 2^j \) possibilities for \( t \), so there are at most \( 2^j \sqrt{N} \) possibilities for \( n \). So \( F(N) \leq 2^j \sqrt{N} \).
- So, now \( \frac{N}{2} < F(N) \leq 2^j \sqrt{N} \Rightarrow \frac{N}{2} < 2^j \sqrt{N} \Rightarrow \sqrt{N} < 2^{j+1} \). But \( j \) is fixed, and \( N \) arbitrary. Contradiction!

**CONGRUENCE AND MODULAR ARITHMETIC**

**Definition**

Let \( a, b \in \mathbb{Z} \) be two integers, and let \( m \in \mathbb{N} \) be a natural number. If \( m \mid a - b \), then we say “\( a \) is congruent to \( b \) modulo \( m \)” and write \( a \equiv b \mod m \).

**Examples**

1) \( 1 \equiv 13 \mod 12 \).
2) \( 2 \equiv 14 \mod 12 \).
3) \( 3 \equiv 15 \mod 12 \).
4) \( -1 \equiv 11 \mod 12 \).
5) \( 0 \equiv 24 \mod 12 \).

**Example**

Suppose \( k, m \in \mathbb{N} \). Write \( k = qm + r \) (\( q \) is the quotient, \( 0 \leq r < m \) is the remainder). Saying \( k = qm + r \) is equivalent to saying \( k \equiv r \mod m \).

**Application**

Is \( 2^{29} + 3 \) divisible by 2?

- Equivalent question: Is \( 2^{39} + 3 \equiv 0 \mod 2 \)?
- \( 2 \equiv 0 \mod 2 \Rightarrow 2^{29} \equiv 0 \mod 2 \) and \( 3 \equiv 1 \mod 2 \), so \( 2^{29} + 3 \equiv 1 \mod 2 \).
- Therefore, \( 2^{29} + 3 \) is not divisible by 2.

**Application**

Is \( 2^{29} + 3 \) divisible by 7?

- \( 2^3 \equiv 8 \equiv 1 \mod 7 \Rightarrow (2^3)^9 \equiv 1^9 \equiv 1 \mod 7 \) and \( 2^2 \equiv 4 \equiv 0 \mod 7 \), so \( 2^2 \cdot 2^{27} \equiv 2^{29} \equiv 4 \cdot 4 \mod 7 \Rightarrow 2^{29} + 3 \equiv 4 + 3 \equiv 7 \equiv 0 \mod 7 \).
- Therefore, \( 2^{29} + 3 \) is divisible by 7.

**Some Rules for Working with Congruence**
Let $a, b, c, d \in \mathbb{Z}$, $m, k \in \mathbb{N}$.

1) $a \equiv b \mod m \Rightarrow a + c \equiv b + c \mod m$ and $\begin{cases} a \equiv b \mod m \\ c \equiv d \mod m \end{cases} \Rightarrow a + c \equiv b + d \mod m$.

2) $\begin{cases} a \equiv b \mod m \\ c \equiv d \mod m \end{cases} \Rightarrow ac \equiv bd \mod m$.

3) $a \equiv b \mod m \Rightarrow a^2 \equiv b^2 \mod m$.

4) $a \equiv b \mod m \Rightarrow a^k \equiv b^k \mod m$.

Proof:

1) $a \equiv b \mod m \Leftrightarrow m \mid a - b \Leftrightarrow m \mid (a + c) - (b + c) \Leftrightarrow a + c \equiv b + c \mod m$.

2) $\begin{cases} a \equiv b \mod m \\ c \equiv d \mod m \end{cases} \Rightarrow m \mid a - b \Rightarrow a - b = qm \Rightarrow ac - bc = cqm \Rightarrow ac - bd + bd = cqm + b'qm \Rightarrow ac - bd = m(cq + b') \Rightarrow m \mid ac - bd \Leftrightarrow ac \equiv bd \mod m$.

Example

What is the remainder when $3^{202} + 5^9$ is divided by 8?

- $3^2 \equiv 1 \mod 8 \Rightarrow 3101 \equiv 101 \mod 8 \Rightarrow 3^{202} \equiv 1 \mod 8$.
- $5^2 \equiv 1 \mod 8 \Rightarrow 5^4 \equiv 1 \mod 8 \Rightarrow 5^8 \equiv 1 \mod 8 \Rightarrow 5^9 \equiv 5 \mod 8$.
- So $3^{202} + 5^9 \equiv 1 + 5 \mod 8 \Rightarrow 3^{202} + 5^9 \equiv 6 \mod 8$.
- So the remainder is 6 when $3^{202} + 5^9$ is divided by 8.

Theorem

Suppose $p$ is a prime number and $a, b \in \mathbb{N}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: By FTA, $a = p_1^{a_1} \cdots p_k^{a_k}$, $b = q_1^{\beta_1} \cdots q_l^{\beta_l}$, $ab = p_1^{a_1} \cdots p_k^{a_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$. Now $p \mid ab$ means $p = p_i$ or $p = q_j$ by FTA. So $p = p_i$ or $p = q_j$.

LAW OF CANCELLATION

Does $ax \equiv ay \mod m \Rightarrow x \equiv y \mod m$? Or equivalently, can we find an “inverse”, i.e. a number $b$ such that $ba \equiv 1 \mod m$, for $a$? If so, we can multiply both sides by $b$, then $(ba)x \equiv (ba)y \mod m \Leftrightarrow x \equiv y \mod m$.

Examples

1) $3 \cdot 2 = 3 \cdot 0 \mod 6$, but $2 \not\equiv 0 \mod 6$. Equivalently, 3 has no inverse modulo 6.

2) $3 \cdot 1 \equiv 3 \cdot 6 \mod 5$ and $1 \equiv 6 \mod 5$.

Note: In 1), 3 and 6 are not relatively prime. In 2), 3 and 5 are relatively prime.

Theorem
Let $p$ be a prime, $a$ an integer, and $p \nmid a$. Then $ax \equiv ay \mod p \Rightarrow x \equiv y \mod p$.

Proof: $ax \equiv ay \mod p \Rightarrow p \mid ax - ay \Rightarrow p \mid a(x - y) \Rightarrow p \mid a$ or $p \mid x - y$. But since $p \nmid a$, $p \nmid x - y \Rightarrow x \equiv y \mod p$.

**Note**
Any integer $a$ is congruent to one of $\{0,1,\ldots,m-1\}$ modulo $m$.

**Example**
$2 \equiv 7 \equiv 12 \equiv 17 \equiv \cdots \mod 5$. If $m = 5$, any integer is congruent to one of $\{0,1,2,3,4\}$.

**Example**
If $p \nmid a$, then $a$ is congruent to one of $\{0,1,\ldots,p-1\}$ modulo $p$.

**Theorem: Fermat’s Little Theorem**
Let $p$ be a prime and $a$ an integer such that $p \nmid a$. Then $a^{p-1} \equiv 1 \mod p$.

Proof:
- Let $S = \{a, a \cdot 2, a \cdot 3, \ldots, a \cdot (p-1)\}$. Then note:
  - The elements in $S$ are distinct modulo $p$. (Suppose $a \cdot n \equiv a \cdot m \mod p, 1 \leq n, m \leq p-1, n \neq m$. Then $n \equiv m \mod p$, but $n - m \leq p-1$, so $p-1 \mid n - m$. Contradiction!)
  - None of the elements are congruent to 0 modulo $p$. ($an \equiv 0 \mod p \Rightarrow n \equiv 0 \mod p$, but $n \leq p-1 < p$ so $p \nmid n$.)
- So $S$ contains $p-1$ numbers, no two of which are congruent, and none is congruent to 0 modulo $p$. So in some order, the elements of $S$ are congruent to $S = \{1,2,\ldots,p-1\}$.
- So $a \cdot (a \cdot 2) \cdot (a \cdot 3) \cdot \cdots \cdot (a \cdot (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p \Rightarrow a^{p-1} \equiv 1 \mod p$ by cancellation law (since $1,2,\ldots,p-1 < p \Rightarrow p \nmid 1,2,\ldots,p-1$).

**Corollary**
Let $p$ be a prime, $a$ an integer, and $p \nmid a$. Then “$a$ has an inverse modulo $p$”, i.e. there exists an integer $b$ such that $ba \equiv 1 \mod p$.

Proof: $a^{p-1} \equiv 1 \mod p \Rightarrow a^{p-2}a \equiv 1 \mod p$. So let $b = a^{p-2}$.

**Example**
Let $p = 5$, $a = 3$. If $b3 \equiv 1 \mod 5$, what is $b$? By elimination, $b = 2$ works. By the corollary, $b = 3^3 = 27$ will work also.

**Remark**
3) \( b \) is not unique.
4) \( b \) is unique modulo \( p \).

**Theorem: Wilson’s Theorem**
If \( p \) is a prime, then \((p-1)! \equiv -1 \mod p\).

**Proof:**
- Let \( S = \{2, 3, \ldots, p-2\} \). Then note:
  - None of the elements is divisible by \( p \), so each has an inverse modulo \( p \).
  - All the inverses can be chosen in the set \( S \) (only 1 and \( p-1 \) are their own inverses).
  - None of the elements is its own inverse. (Suppose \( a \in S \) such that \( a \cdot a \equiv 1 \mod p \Rightarrow p \mid a^2 - 1 \Rightarrow p \mid (a+1)(a-1) \), but \( a+1, a-1 < p \) so contradiction.)
- So \( 2 \cdot 3 \cdots (p-2) \equiv 1 \mod p \).
- Now, \((p-1)! = (2 \cdot 3 \cdots (p-2)) \cdot (p-1) \equiv p-1 \equiv -1 \mod p\).

**Definition**
\( n \in \mathbb{N} \) is **composite** if \( n \neq 1 \) and \( n \) is not prime.

**Note**
So \( \mathbb{N} = \{1\} \cup \{\text{primes}\} \cup \{\text{composites}\} \).

**Definition**
Let \( m, n \in \mathbb{N} \). The **greatest common divisor** of \( m \) and \( n \) is the largest \( d \in \mathbb{N} \) such that \( d \mid m \) and \( d \mid n \), write \( \gcd(m,n) \) or \( (m,n) \).
If \((m,n)=1\), then \( m \) and \( n \) are relatively prime.

**Definition: Euler Function \( \phi(n) \)**
Let \( n \in \mathbb{N} \setminus \{1\} \). The Euler function \( \phi(n) \) is the number of elements in \( \{1, 2, \ldots, n-1\} \) which are relatively prime to \( n \).

**Lemma**
\[
\begin{align*}
& m \mid ab \quad (m,a)=1 \\
\Rightarrow & m \mid b.
\end{align*}
\]
**Proof:** Let \( a = p_1^{a_1} \cdots p_k^{a_k}, b = q_1^{\beta_1} \cdots q_l^{\beta_l}. m \mid ab \Rightarrow p_1^{a_1} \cdots p_k^{a_k} \cdot q_1^{\beta_1} \cdots q_l^{\beta_l} = cm \). By FTA, the factors of \( m \) are among the \( p_i \)'s and \( q_i \)'s. But since \((m,a)=1\), the factors of \( m \) are only among the \( q_i \)'s. So \( m \mid b \).

**Note**
For case \( m = p \) a prime, \[
\begin{align*}
p \mid ab & \quad \Rightarrow \quad p \mid b.
\end{align*}
\]
Lemma
\[(a, m)=1 \Rightarrow (ab, m)=1.\]

Proof: Suppose \((ab, m) \neq 1\). So there exists \(p\) such that \(p \mid ab\) and \(p \mid m\). So \(p \mid a\) \(\Rightarrow (a, m) \neq 1\) or \(p \mid b\) \(\Rightarrow (b, m) \neq 1\).

Note
\[p \mid a \quad p \mid b \Rightarrow p \mid ab.\]

Note
\[a \equiv b \mod m \quad (a, m)=1 \Rightarrow (b, m)=1.\]

Why? \(a = b + km\), so \((b + km, m) = 1\). Suppose \((b, m) \neq 1\). Then there exists \(p\) such that \(p \mid b\) and \(p \mid m\). So \(p \mid b\) \(\Rightarrow p \mid b + km \Rightarrow (b + km, m) \neq 1\). Contradiction!

Proposition
\[ax \equiv ay \mod m \quad (a, m)=1 \Rightarrow x \equiv y \mod m.\]

Proof: \(ax \equiv ay \mod m \Leftrightarrow m \mid ax - by = a(x - y)\). But since \((a, m) = 1, m \mid x - y \Leftrightarrow x \equiv y \mod m\).

Theorem: Euler’s Theorem
Let \(m \in \mathbb{N} \setminus \{1\}\). If \((a, m) = 1\), then \(a^{\phi(m)} \equiv 1 \mod m\).

Proof:
- Let \(\{n_1, \ldots, n_{\phi(m)}\}\) be the numbers in \(\{1, \ldots, m-1\}\) which are relatively prime to \(m\).
- Let \(S = \{an_1, \ldots, an_{\phi(m)}\}\). Note:
  - The elements of \(S\) are distinct modulo \(m\). (If \(an_i \equiv an_j \mod m\), then \(n_i \equiv n_j \mod m\), but \(n_i, n_j < m\).)
  - All elements in \(S\) are relatively prime to \(m\). (Since \((a, m) = 1\) and \((a, n_i) = 1\), so \((an_i, m) = 1\).)
  - So in some order, the elements of \(S\) are congruent to \(\{n_1, \ldots, n_{\phi(m)}\}\) modulo \(m\).
  - So \((an_1) \cdots (an_{\phi(m)}) \equiv n_1 \cdots n_{\phi(m)} \mod m \Rightarrow a^{\phi(m)}(n_1 \cdots n_{\phi(m)}) \equiv n_1 \cdots n_{\phi(m)} \mod m \Rightarrow a^{\phi(m)} \equiv 1 \mod m\).

Public Key Cryptography
History

Fact 1
Let \( N = p \cdot q \), \( p \) and \( q \) are distinct primes. Then \( \phi(N) = (p-1)(q-1) \).

Proof: \( N - \phi(N) = \# \{ 1 \leq n \leq N \mid (n, N) = 1 \} = \# \{ 1 \leq n \leq N \mid p \mid n \text{ or } q \mid n \} = \# \{ 1 \leq n \leq N \mid p \mid n \} \cdot \# \{ 1 \leq n \leq N \mid q \mid n \} \). Now,
\[
\# \{ 1 \leq n \leq N \mid p \mid n \} = \# \{ p, 2p, \ldots, (q-1)p, pq \}
\]
and
\[
\# \{ 1 \leq n \leq N \mid q \mid n \} = \# \{ q, 2q, \ldots, (p-1)q, pq \}
\]
So \( N - \phi(N) = \# \{ p, 2p, \ldots, (q-1)p, pq \} \cdot \# \{ q, 2q, \ldots, (p-1)q, pq \} = p + q - 1 \). Therefore,
\[
N - \phi(N) = p + q - 1 \Rightarrow \phi(N) = N - (p + q - 1) = pq - p - q + 1 = (p-1)(q-1).
\]

Example
Let \( p = 5 \), \( q = 3 \), \( N = pq = 5 \cdot 3 = 15 \).
\[ \phi(N) = \phi(15) = \# \{ 1, 2, 4, 7, 8, 11, 13, 14 \} = 8 \]
\[ \phi(N) = \phi(pq) = \phi(15) = \phi(5 \cdot 3) = 4 \cdot 2 = 8 \]

Fact 2
If \( \gcd(a, b) = 1 \), \( a, b \in \mathbb{N} \), then there exist \( x, y \in \mathbb{Z} \) such that \( xa + yb = 1 \).

Example
\[
7 = 1(5) + 2 \]
\[
gcd(5, 7) = 1 \Rightarrow 5 = 2(2) + (1) \Rightarrow 1 = 5 - 2(2) = 5 - 2(7 - 1(5)) = 3(5) - 2(7) \Rightarrow \begin{cases} x = 3 \\ y = -2 \end{cases}
\]

Lemma
Let \( N = p \cdot q \), \( p \) and \( q \) are distinct primes. Let \( n, M \in \mathbb{N} \). Then \( n \equiv 1 \mod \phi(N) \Rightarrow M^n \equiv M \mod N \).

Proof:
\[ n \equiv 1 \mod \phi(N) \Leftrightarrow \phi(N) \mid n - 1 \Leftrightarrow n - 1 = k\phi(N) \Leftrightarrow n = k\phi(N) + 1 \Rightarrow M^n = M^{k\phi(N) + 1} = M \cdot (M^{\phi(N)})^k. \]
We want \( M^n \equiv M \mod N \). It is enough to show \( M^n \equiv M \mod p \) and \( M^n \equiv M \mod q \). We show \( M^n \equiv M \mod p \).
\[ \begin{align*}
\text{Case 1: If } & p \mid M \text{, then } M^n \equiv 0 \equiv M \mod p. \\
\text{Case 2: If } & p \nmid M \text{, then } M^n \equiv M. \text{ So by Euler’s Theorem,}
\end{align*} \]
\[
M^n = M \cdot (M^{\phi(N)})^k = M \cdot (M^{\phi(N)})^{\phi(p)k} = M \cdot (1)^{\phi(p)k} = M \mod p.
\]

Algorithm

<table>
<thead>
<tr>
<th></th>
<th>Receiver</th>
<th>Sender</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose ( p, q ) large primes.</td>
<td>( N = p \cdot q ).</td>
<td>( N ).</td>
</tr>
<tr>
<td>( \phi(N) = (p-1)(q-1) ) (fact 1).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Choose \( e \) relatively prime to \( p, q \).
Find \( d \) such that \( de + k\phi(N) = 1 \) (fact 2).

<table>
<thead>
<tr>
<th>( e )</th>
<th>( 0 &lt; M &lt; N ), ( M ) is the message.</th>
<th>( M^e \equiv R \mod N ). ( R ) is the coded message.</th>
</tr>
</thead>
</table>

\(-\)
\( R \) is the encoded message.
\( R^d \equiv M \mod N \).
\( M \) is the decoded message.

### Remarks
1) Why is \( R^d \equiv M \mod N \)? \( R^d \equiv \left(M^e\right)^d = M^{ed} \). Since \( de + k\phi(N) = 1 \Rightarrow de \equiv 1 \mod \phi(N) \), so \( M^{de} \equiv M \mod N \).

2) Why is this secure? To recover \( M \) from \( R \), need to know \( d \) (and \( N \)). To know \( d \), need to know \( \phi(N) \) (and \( e \)). To know \( \phi(N) \), need to know \( N = p \cdot q \) but \( p, q \) are very large, so \( N \) is very large; there is no known effective algorithm to find its factors.

3) If the sender forgets \( M \) but remembers \( R \), the sender can’t recover \( M \)!

### Euclidean Algorithm
If \( \gcd(a,b) = d, a,b,d \in \mathbb{N} \), then there exists \( x, y \in \mathbb{Z} \) such that \( xa + yb = d \).

**Proof:**
- \( \gcd(a,b) = d \) \( \Rightarrow a = q \cdot b + r, 0 \leq r < b \Rightarrow b = q_1 \cdot r + r_1, 0 \leq r_1 < r \Rightarrow r = q_2 \cdot r_1 + r_2, 0 \leq r_2 < r_1 \Rightarrow \ldots \)
  - \( \Rightarrow r_{k-1} = q_k \cdot r_k + r_{k+1}, 0 \leq r_{k+1} < r_k \Rightarrow r_k = q_{k+1} \cdot r_{k+1} + 0 \) (terminates because \( \{r, r_1, \ldots, r_k\} \) is a strictly decreasing sequence).
- Since \( d \mid a, b \), so \( d \mid a, b \Rightarrow d \mid r, b \Rightarrow d \mid r_1, r \Rightarrow d \mid r_2, r_1 \Rightarrow \ldots \Rightarrow d \mid r_k, r_k \). So \( d \mid r_k \).
- Since \( r_{k+1} \mid r_k \), so \( r_{k+1} \mid r_{k-1} \Rightarrow \ldots \Rightarrow r_{k+1} \mid r \Rightarrow r_{k+1} \mid b \Rightarrow r_{k+1} \mid a \). So \( r_{k+1} \mid a, b \Rightarrow r_{k+1} \mid \gcd(a,b) = d \).
- So \( d \mid r_{k+1} \Rightarrow r_{k+1} = d \).

**Note**

Let \( a, b \in \mathbb{N} \), \( (a,b)=1 \). Then \( x_0a + y_0b = 1 \) for some \( x_0, y_0 \in \mathbb{Z} \). Now, \( \begin{cases} x = x_0 + nb \\ y = y_0 - na \end{cases}, n \in \mathbb{Z} \) will produce other solutions because \( xa + by = (x_0 + nb)a + (y_0 - na)b = x_0a + y_0b = 1 \).

### Rational Numbers

**Definition**

\[ \mathbb{Q} = \left\{ \frac{m}{n} \mid m,n \in \mathbb{Z}; n \neq 0 \right\} \] is the set of rational numbers.
Remark
\( \mathbb{R} = \mathbb{Q} \cup \{\text{irrational}\} \).

Definition
\[ \frac{m}{n} = \frac{m'}{n'} \quad \text{if} \quad mn' = m'n. \]

Definition: Addition and Multiplication
1) Addition: \[ \frac{m}{n} + \frac{m'}{n'} = \frac{mn' + n'm}{nn'} \]
2) Multiplication: \[ \frac{m}{n} \cdot \frac{m'}{n'} = \frac{m \cdot m'}{n \cdot n'} \]

Example
Prove \( \sqrt{2} \) is irrational.
Proof: Suppose \( \sqrt{2} \) is rational, i.e. \( \sqrt{2} = \frac{m}{n} \), and assume \((m,n)=1\). Now, \( n\sqrt{2} = m \Rightarrow 2n^2 = m^2 \). So \( 2 | m^2 \Rightarrow 2 | m \Rightarrow m = 2m' \) since 2 prime. So \( 2n^2 = 2 \cdot m^2 \Rightarrow n^2 = 2m^2 \Rightarrow 2 | n^2 \Rightarrow 2 | n \). Contradiction!

Theorem
\( \sqrt{p} \) is irrational for any \( p \) prime.

Proof: Suppose \( \sqrt{p} \) is rational, i.e. \( \sqrt{p} = \frac{m}{n} \), and assume \((m,n)=1\). Now, \( n\sqrt{p} = m \Rightarrow pn^2 = m^2 \). So \( p | m^2 \Rightarrow p | m \Rightarrow m = pm' \) since \( p \) prime. So \( pn^2 = p^2 \cdot m'^2 \Rightarrow n^2 = pm'^2 \Rightarrow p | n^2 \Rightarrow p | n \). Contradiction!

Example
Prove \( \sqrt{6} \) is irrational.
Proof: Suppose \( \sqrt{6} \) is rational, i.e. \( \sqrt{6} = \frac{m}{n} \), and assume \((m,n)=1\). Now, \( n\sqrt{6} = m \Rightarrow 6n^2 = m^2 \). So \( 6 | m^2 \Rightarrow 3 | m^2 \Rightarrow 3 | m \) \( \Rightarrow \) \( 2 | m^2 \Rightarrow 2 | m \Rightarrow m = 2m' \) since 2 and 3 prime. So \( 6n^2 = 2 \cdot m^2 \Rightarrow n^2 = 3m^2 \Rightarrow 6 | n^2 \Rightarrow 6 | n \). Contradiction!

Example
Prove \( \sqrt{2} \) is irrational.
Proof: Suppose \( \sqrt[3]{2} \) is rational, i.e. \( \sqrt[3]{2} = \frac{m}{n} \), and assume \((m,n)=1\). Now, \( n\sqrt[3]{2} = m \Rightarrow 2n^3 = m^3 \). So \( 2 | m^3 \Rightarrow 2 | m \Rightarrow m = 2m' \) since 2 prime. So \( 2n^3 = 2 \cdot m'^3 \Rightarrow n^3 = 4m'^3 \Rightarrow 2 | n^3 \Rightarrow 4 | n^2 \Rightarrow 2 | n \). Contradiction!
Example
Prove $\sqrt{3} + \sqrt{7}$ is irrational.

Proof: Suppose $\sqrt{3} + \sqrt{7}$ is rational, i.e. $\sqrt{3} + \sqrt{7} = \frac{m}{n}$, and assume $(m, n) = 1$. Now,

$$\sqrt{3} = \frac{m}{n} - \sqrt{7} \Rightarrow 3 = \left(\frac{m}{n} - \sqrt{7}\right)^2 = \frac{m^2}{n^2} - 2\sqrt{7} \frac{m}{n} + 7 \Rightarrow 3 - \frac{m^2}{n^2} = -2\sqrt{7} \frac{m}{n} \Rightarrow \sqrt{7} = \frac{3n^2 - m^2 - 7n^2}{-2mn} \in \mathbb{Q}.$$ 

But $\sqrt{7}$ is irrational since 7 prime. Contradiction!

Definition
An integer of the form $k^2$ (for some $k \in \mathbb{Z}$) is called a “perfect square”.

Note
Recall from Fundamental Theorem of Arithmetic that for any $n \in \mathbb{N}, n > 1$ has a unique (except for order) factorization into primes, i.e. $n = p_1^{a_1} \cdots p_k^{a_k}, a_i \in \mathbb{N}$. So $n = k^2 = \left(p_1^{a_1} \cdots p_k^{a_k}\right)^2 = p_1^{2a_1} \cdots p_k^{2a_k}$.

Theorem
Let $N \in \mathbb{N}$. Then $\sqrt{N}$ is irrational if and only if $N$ is not perfect square.

Proof:
- Assume $\sqrt{N}$ is rational. Suppose $N$ is perfect square. Then $N = p_1^{2a_1} \cdots p_k^{2a_k}, a_i \geq 0 \Rightarrow \sqrt{N} = p_1^{a_1} \cdots p_k^{a_k} \in \mathbb{Z} \subseteq \mathbb{Q}$. Contradiction!
- Assume $N$ not perfect square. Suppose $\sqrt{N}$ is rational. Then $\sqrt{N} = \frac{m}{n} \Rightarrow N = \frac{m^2}{n^2} = \left(\frac{p_1^{a_1} \cdots p_k^{a_k}}{p_1^{b_1} \cdots p_k^{b_k}}\right)^2 = \alpha, \beta \geq 0 \Rightarrow N = p_1^{2(\alpha_1 - \beta_1)} \cdots p_k^{2(\alpha_k - \beta_k)}, \alpha - \beta \geq 0$. This means $N$ is a perfect square. Contradiction!

Example
Prove $\sqrt{4}$ is irrational.

Proof: Suppose $\sqrt{4} = \frac{m}{n}$ where $(m, n) = 1$. Then $4n^3 = m^3$. Now,

$$\left\{ \begin{array}{l}
 n = p_1^{a_1} \cdots p_k^{a_k} \Rightarrow n^3 = \left(p_1^{a_1} \cdots p_k^{a_k}\right)^3 = p_1^{3a_1} \cdots p_k^{3a_k}, \alpha, \beta \geq 0, \text{ so } 4p_1^{3a_1} \cdots p_k^{3a_k} = p_1^{3\beta_1} \cdots p_k^{3\beta_k} \\
 m = p_1^{\beta_1} \cdots p_k^{\beta_k} \Rightarrow m^3 = \left(p_1^{\beta_1} \cdots p_k^{\beta_k}\right)^3 = p_1^{3\beta_1} \cdots p_k^{3\beta_k}
\end{array} \right.$$

$\Rightarrow 2^{(2 + 3\alpha)} q = 2^{3\beta} q'$. Contradiction because $2^{(2 + 3\alpha)} q = 2^{3\beta} q' \Rightarrow 2 + 3\alpha = 3\beta$, but $3 \not| 2 + 3\alpha = 3\beta$!

Theorem
Let $k, L \in \mathbb{N}$. Then $\sqrt{k}$ is rational iff $\sqrt{L}$ is an integer.
Proof:
  a. \((\Leftarrow)\) is trivial.
  b. \((\Rightarrow)\): 
      \[
      \sqrt[k]{L} = \frac{m}{n} = \frac{p_1^{a_1} \cdots p_n^{a_n}}{p_1^{b_1} \cdots p_n^{b_n}} = p_1^{k(a_1-b_1)} \cdots p_n^{k(a_n-b_n)} \Rightarrow L = p_1^{k(a_1-b_1)} \cdots p_n^{k(a_n-b_n)}. \]
      Now,
      \[
      L \in \mathbb{N} \Rightarrow k(a_i - \beta_i) \geq 0 \Rightarrow a_i - \beta_i \geq 0 \Rightarrow \sqrt[k]{L} \in \mathbb{N}.
      \]

**ALGEBRAIC NUMBERS**

**Definition**
A real number is called algebraic if there exists a polynomial with integer coefficients that has this number as a root (not allowing the zero polynomial).

**Example**
1) \(\sqrt{2}\) is algebraic: \(p(x) = x^2 - 2\).
2) Any rational number \(\frac{m}{n}\) is algebraic: \(p(x) = nx - m\).

**Example**
\(\pi, e\) are not algebraic (transcendental).

**REAL NUMBERS**

**Motivation**
Suppose we assume that the real numbers \(\mathbb{R}\) exist. How would we prove that \(\sqrt{2}\) exists? That is, is there \(x_0 \in \mathbb{R}\) such that \(x_0^2 = 2\)?

**Definition**
For a subset \(S \subseteq \mathbb{R}\), \(c \in \mathbb{R}\) is an upper bound of \(S\) if for all \(x \in S\), \(x \leq c\).

**Remark**
There are many upper bounds for a given set.

**Definition**
A least upper bound for a subset \(S \subseteq \mathbb{R}\) is:
- An upper bound \(c\).
- Such that for any other upper bound \(c'\), we have \(c \leq c'\).

**Example**
1) \(S = \{1, 2, 3, 4, 5\}\). Upper bounds \(c = 6, 6.1, 10^{10}, \ldots\); least upper bound is 5.
2) \( S = \{ x \in \mathbb{R} \mid x < 10 \} \). Upper bounds \( c = 10, 11, \ldots \); least upper bound is 10.

3) \( S = \{ x \in \mathbb{R} \mid x^2 < 2 \} \). Upper bounds \( c = 1.5, 2, \ldots \); least upper bound is \( \sqrt{2} \).

4) \( S = [3, 7] \cup [-1, 2] \cup \{ 11 \} \). Upper bounds \( c = 11, 11.2, \ldots \); least upper bound is 11.

5) \( S = \mathbb{N} \) has no upper bounds.

The Completeness Property
The basic property that distinguishes \( \mathbb{R} \) from \( \mathbb{Q} \) is that every non-empty subset of \( \mathbb{R} \) which has an upper bound has a least upper bound.

Theorem: Intermediate Value Theorem
Let \( f : [a, b] \to \mathbb{R} \) be a continuous function such that \( f(a) < 0 \) and \( f(b) > 0 \). Then there exists \( x_0 \in (a, b) \) where \( f(x_0) = 0 \).

Proof:
Let \( S = \{ x \in [a, b] \mid f(t) < 0, \forall t \in [a, x] \} \). Note:
- \( S \) is not empty since \( a \in S \).
- \( S \) has an upper bound \( b \).

So \( S \) has a least upper bound \( x_0 \). Want to show \( f(x_0) = 0 \).
- If \( f(x_0) > 0 \), then there exists \( \delta > 0 \) such that for all \( x \in (x_0 - \delta, x_0 + \delta) \), \( f(x) > 0 \) since \( f \) is continuous. So \( x_0 - \delta \) is an upper bound because otherwise there exists \( x \in S, x_0 - \delta < x \) such that \( f(x) < 0 \). So \( x_0 \) is not the least upper bound.
- If \( f(x_0) < 0 \), then there exists \( \delta > 0 \) such that for all \( x \in (x_0 - \delta, x_0 + \delta) \), \( f(x) < 0 \) since \( f \) is continuous. Let \( x = x_0 + \frac{\delta}{2} \). Then \( f(x) < 0 \), i.e. \( x \in S \). So \( x_0 \) is not an upper bound.

So \( f(x_0) = 0 \).

Definition: Order
Assume we have the real numbers. \( a < b \) if \( b - a \in P \), where \( P = \{ \text{positive numbers} \} \).

Note
The set \( P \) has the following properties:
1) Closed under addition and multiplication.
2) For each \( x \in \mathbb{R} \), exactly one of the following holds: \( x \in P \), \(-x \in P \), or \( x = 0 \).

Claim
1) \( a < b \Rightarrow -a > -b \).

2) \( a < b, k \in P \Rightarrow ka < kb \). Proof: \( a < b \Rightarrow (b-a) \in P \)
\[
\Rightarrow k(b-a) = (kb-ka) \in P \Rightarrow ka < kb .
\]

3) \( a < b, -k \in P \Rightarrow ka > kb \). Proof: \( a < b \Rightarrow (b-a) \in P \)
\[
\Rightarrow -k(b-a) = (ka-kb) \in P \Rightarrow ka > kb .
\]

Example
There exists irrational numbers $x$ and $y$ such that $x^y$ is rational.

Consider \( \left( \sqrt[3]{2} \right)^{\sqrt[3]{2}} = \sqrt[3]{2}^2 = 3 \).

If $\sqrt[3]{2}$ is rational, then let $x = \sqrt[3]{2}$ and $y = \sqrt{2}$.
If $\sqrt[3]{2}$ is irrational, then let $x = \sqrt[3]{\sqrt{2}}$ and $y = \sqrt{2}$.

**Definition: Real Numbers**

A real number $X$ is a subset of $\mathbb{Q}$ (the rational numbers) such that:

1) $X \neq \emptyset$ and $X \neq \mathbb{Q}$.
2) If $q_1 \in X$, then $q_2 \in X$ for all $q_2 < q_1$.
3) $X$ has no largest element.

**Example**

Show that $X = \{q \in \mathbb{Q} \mid q < 3\}$ is a real number.

4) $X \neq \emptyset$ because $1 \in X$. $X \neq \mathbb{Q}$ because $4 \notin X$.
5) Let $q_1 \in X \Rightarrow q_1 < 3 \Rightarrow q_2 < q_1$. So $q_2 \in X$.

6) Suppose $q \in X$ is the largest element. Then $q < 3$. By the property of the rational numbers, there always exists a rational number between any two rational numbers. So there exists $q'$ such that $q < q' < 3$. So $X$ has no largest element.

**Example**

Show that $\sqrt{2} = \{q \in \mathbb{Q} \mid q^2 < 2\} \cup \{q \notin \mathbb{Q} \mid q < 0\}$ is a real number.

1) $\sqrt{2} \neq \emptyset$ because $0 \in \sqrt{2}$. $\sqrt{2} \neq \mathbb{Q}$ because $3 \notin \sqrt{2}$.
2) Let $q_1 \in \sqrt{2}$ and $q_2 < q_1$. If $q_2 < 0$, then $q_2 \in \sqrt{2}$. If $q_2 > 0$, then $q_2 < q_1 \Rightarrow q_2^2 < q_1^2 < 2$. So $q_2 < q_1 \Rightarrow q_2 \in \sqrt{2}$.

3) Suppose $q \in \sqrt{2}$ is the largest element. Let $q' = q + \frac{1}{n}$. Then $q'^2 = \left( q + \frac{1}{n} \right)^2 = q^2 + 2q + \frac{1}{n^2} < q^2 + \frac{2q}{n}$, so $q'^2 < q^2 + \frac{2q}{n} < 2 \Rightarrow n > \frac{2q}{\sqrt{2} - q^2}$. So we can find $n$ large enough such that $q' = q + \frac{1}{n} \in \sqrt{2}$. So $\sqrt{2}$ has no largest element.

**Comparison**

<table>
<thead>
<tr>
<th>R-world</th>
<th>Q-world</th>
</tr>
</thead>
<tbody>
<tr>
<td>$3$</td>
<td>$3 := {q \in \mathbb{Q} \mid q &lt; 3}$</td>
</tr>
<tr>
<td>$\frac{m}{n}$</td>
<td>$\frac{m}{n} := {q \in \mathbb{Q} \mid q &lt; \frac{m}{n}}$</td>
</tr>
<tr>
<td>$\sqrt{2}$</td>
<td>$\sqrt{2} := {q \in \mathbb{Q} \mid q^2 &lt; 2}$</td>
</tr>
<tr>
<td>$\sqrt[3]{2}$</td>
<td>$\sqrt[3]{2} := {q \in \mathbb{Q} \mid q^3 &lt; 2}$</td>
</tr>
</tbody>
</table>
**Definition: Addition**
Let $X, Y$ be real numbers. $X + Y = \{ p + q \mid p \in X, q \in Y \}.$

**Definition: Zero**
$0 = \{ q \in \mathbb{Q} \mid q < 0 \}.$

**Theorem**
$0 + X = X$ for all real number $X$.

**Definition**
A real number $X$ is “positive” if $0 \in X$.

**Definition: Multiplication of Positive Real Numbers**
Suppose $X$ and $Y$ are two positive real numbers. Then $X \cdot Y := \left\{ r \in \mathbb{Q} \mid r \leq 0 \text{ or } r < p \cdot q \text{ where } \begin{cases} 0 < p \in X \\ 0 < q \in Y \end{cases} \right\}.$

**Definition: Negative of a Number**
For a real number $X$, define $-X := \{ -q \in \mathbb{Q} \mid q \not\in X \} \setminus \text{largest element (if it exists)}$.

**Example**
If $X = \{ q \in \mathbb{Q} \mid q < 2 \}$, then $-X = \{ -q \in \mathbb{Q} \mid q \geq 2 \} = \{ q \in \mathbb{Q} \mid q < -2 \}$.

**Theorem**
For every $X \in \mathbb{R}$, we have $X + (-X) = 0$.

**Definition: Absolute Value**
$|X| := \begin{cases} X \text{ if } X \geq 0 \\ -X \text{ if } X < 0 \end{cases}$

**Definition: Multiplication**
$X \cdot Y := \begin{cases} |X| \cdot |Y|, \text{ if } X \geq 0 \text{ and } Y \geq 0, \text{ or } X < 0 \text{ and } Y < 0 \\ -|X| \cdot |Y|, \text{ if } X \geq 0 \text{ and } Y < 0, \text{ or } X < 0 \text{ and } Y \geq 0 \end{cases}$

**Definition**
$1 := \{ q \in \mathbb{Q} \mid q < 1 \}.$
Theorem
\[ 1 \cdot X = X, \forall X \in \mathbb{R}. \]

Definition
If \( X > 0 \), define \( \frac{1}{X} = \left\{ q \in \mathbb{Q} \mid q \leq 0, \text{ or } q = \frac{1}{q}, q' \in \mathbb{Q} \setminus X \right\} \setminus \{\text{largest element}\}. \)
If \( X < 0 \), define \( \frac{1}{X} = \frac{1}{|X|}. \)

Completeness Property of the Reals
Every subset of \( \mathbb{R} \) (other than \( \emptyset \)) which has an upper bound has a least upper bound.

**COMPLEX NUMBERS**

Examples
1) \( 3x + 2 \) has no solution in \( \mathbb{Z} \), but there exists a solution in \( \mathbb{Q} \).
2) \( x^2 - 2 = 0 \) has no solution in \( \mathbb{Q} \), but there exists a solution in \( \mathbb{R} \).
3) \( x^2 + 1 = 0 \) has no solution in \( \mathbb{R} \), but there exists a solution in \( \mathbb{C} \).

Definition
A complex number \( z = a + ib \), where \( a, b \in \mathbb{R} \), \( i^2 = -1 \).

Notation
\( \mathbb{C} \) is the set of all complex numbers.

Definition: Addition and Multiplication
Addition: \( (a + ib) + (a' + ib') = (a + a') + i(b + b') \).
Multiplication: \( (a + ib) \cdot (a' + ib') = (aa' - bb') + i(ba' + ab') \).

Notes
- Why is \( \mathbb{R} \subset \mathbb{C} \) ? \( a \in \mathbb{R} \) is \( a + i0 \in \mathbb{C} \).
- For \( b \in \mathbb{R} \), \( 0 + ib \in \mathbb{C} \) is (pure) imaginary.

Notation
1) \( \text{Re}(a + ib) := a \), \( \text{Im}(a + ib) := b \).
2) \( |a + ib| = \sqrt{a^2 + b^2} \) is the modulus of \( a + ib \).
3) \( a + ib := a + i(-b) = a - ib \) is the conjugate of \( a + ib \).
Examples

1) \(- (a + ib) = -a + i(-b)\). Check: \((a + ib) + (-a + i(-b)) = 0 + i0 = 0\).

2) \((a + ib)(\frac{1}{a + ib}) = (a + ib)(a - ib) = (a^2 + b^2) + i(ab - ab) = a^2 + b^2 = |a + ib|^2\).

3) \(\frac{1}{a + ib} = \frac{1}{a + ib} \cdot \frac{a - ib}{a^2 + b^2} = \frac{a - ib}{a^2 - b^2 + i(-b) + a + ib} = \frac{a - ib}{a^2 + b^2}, a + ib \neq 0\).

Notation

\[\theta = \text{argument of } a + ib.\]

DeMoivre Formula

\[r(\cos \theta + i \sin \theta)^n = r^n [\cos(n\theta) + i \sin(n\theta)] \forall n \in \mathbb{N}.\]

Example

\[(1+i)^8 = \left[\sqrt{2} \left(\cos \left(\frac{\pi}{4}\right) + i \sin \left(\frac{\pi}{4}\right) \right)\right]^8 = \left(\sqrt{2}\right)^8 \left(\cos \left(\frac{8\pi}{4}\right) + i \sin \left(\frac{8\pi}{4}\right) \right) = 16(\cos(2\pi) + i \sin(2\pi)) = 16.\]

Example

Find the solution to \(z^3 = -1\).

Let \(z = r[\cos \theta + i \sin \theta]\). \(z^3 = -1 \Rightarrow r^3[\cos(3\theta) + i \sin(3\theta)] = \cos(\pi) + i \sin(\pi) \Rightarrow \begin{cases} r = 1 \\ \theta = \frac{\pi + 2k}{3} \pi \end{cases}\). So,

\[z_0 = 1 \left[\cos \left(\frac{\pi}{3}\right) + i \sin \left(\frac{\pi}{3}\right) \right] = \frac{1}{2} + i \frac{\sqrt{3}}{2},
\]

\[z_1 = 1[\cos(\pi) + i \sin(\pi)] = -1,
\]

\[z_2 = 1 \left[\cos \left(\frac{5\pi}{3}\right) + i \sin \left(\frac{5\pi}{3}\right) \right] = -\frac{1}{2} + i \frac{\sqrt{3}}{2}.
\]

Triangle Inequality

\[|z_1 + z_2| \leq |z_1| + |z_2| \forall z_1, z_2 \in \mathbb{C}.\]

Fundamental Theorem of Algebra

Definition: Closed Curve
A closed curve in the plane is a continuous function from $[0, 2\pi]$ into $\mathbb{C}$ such that its values at 0 and $2\pi$ are the same.

**Definition: Winding Number**

If $\phi$ is a closed curve in the plane that doesn’t go through $(0, 0)$, the its winding number about $(0, 0)$ is the total number of times a vector from $(0, 0)$ to the point $\phi(t)$ winds around $(0, 0)$ as $t$ goes from 0 to $2\pi$.

**Lemma**

If $L(t)$ and $M(t)$ are two closed curves (not passing through $(0, 0)$), and $|L(t) - M(t)| < |L(t)|, \forall t$, then $L$ and $M$ have the same winding number.

**Theorem: Fundamental Theorem of Algebra**

Every polynomial with complex coefficients (other than a constant polynomial) has a complex root.

$$p(z) = a_n z^n + \cdots + a_1 z + a_0, \text{ where } a_i \in \mathbb{C}, \ a_n \neq 0 \text{ (so } n \text{ is the degree of the polynomial)}. $$

**Theorem: Factor Theorem**

If $p(z)$ is a polynomial with complex coefficients, then by FTA it must have a root $r \in \mathbb{C}$, i.e. $p(r) = 0$.

1) $z - r$ divides this polynomial. So $p(z) = (z - r)q(z), \ deg(q) < \ deg(p)$.

2) $p(z) = a(z - r_1) \cdots (z - r_n), a, r_1, \ldots, r_n \in \mathbb{C}$, or $p(z) = a(z - r_1)^{k_1} \cdots (z - r_n)^{k_n}$.

**Cardinality**

**Motivation**

How to compare sizes of sets? Especially sizes of infinite sets?

**Definition: Finite Set**

A (non-empty) set $S$ is finite if there exists some $n \in \mathbb{N}$ such that the elements of $S$ can be paired with the elements of $\{1, 2, \ldots, n\}$.

Equivalently, if can label the elements of $S$ as $s_1, \ldots, s_n$, then say $S$ is finite, of cardinality (“size”) $n$.

**Example**

$\{\text{blue, green, red}\}$ is finite with cardinality 3. blue $\leftrightarrow 1$, green $\leftrightarrow 2$, red $\leftrightarrow 3$.

**Definition: Infinite Set**

An infinite set is a set which is not finite.

**Examples**

$\mathbb{N} = \{1, 2, 3, \ldots\}$, $\mathbb{Q}$ = rationals, $\mathbb{R}$ = reals are infinite sets.
Definition
Two sets $S$ and $T$ have the same cardinality if there exists a bijection (one-to-one and onto) $f : S \rightarrow T$, i.e. can pair elements of $S$ with elements of $T$.
Notation: $|S| = |T|$.

Note
For finite sets, if $S$ and $T$ both have $n$ elements, then they have the same cardinality (take $f : S \rightarrow T; s_i \rightarrow t_i$).

Example
Let $S = \mathbb{N} = \{1, 2, \ldots \}$ and $T = \{2, 4, \ldots \}$. Then $|S| = |T|$.
Why? Take $f : S \rightarrow T; n \rightarrow 2n$. $f$ is 1-1 because $f(n) = f(m) \Rightarrow 2n = 2m \Rightarrow n = m$. $f$ is onto because for all $m \in T$, $m = 2l$, $l \in \mathbb{N}$, so take $n = l$.

Example
Let $S = \mathbb{N} = \{1, 2, \ldots \} \supset T = \{2, 3, \ldots \}$. Then $|S| = |T|$.

NOTIONS OF CARDINALITY

Definition: Countable
If $|\mathbb{N}| = |T|$, then say $T$ is countably infinite (“countable”).
Notation: $|\mathbb{N}| = \aleph_0$.

Example
$S = \mathbb{Q}^+$ the set of positive rationals is countable, i.e. they can be enumerated. So $|\mathbb{Q}^+| = |\mathbb{N}| = \aleph_0$.

Theorem
The set $[0,1] := \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$ is not countable (i.e. uncountable).
Notation: Say $[0,1]$ has the cardinality of the “continuum”. Write $|[0,1]| = c$.

Proof:
Suppose we have a list of all real numbers between 0 and 1:
$s_1 = 0.a_{11}a_{12}a_{13} \ldots$
$s_2 = 0.a_{21}a_{22}a_{23} \ldots$
$s_3 = 0.a_{31}a_{32}a_{33} \ldots$
$\vdots$

Make a number $x = 0.x_1x_2x_3 \ldots$ as follows: $x_i = \begin{cases} 5, & a_{ii} \neq 5 \\ 6, & a_{ii} = 5 \end{cases}$. This is a real number between 0 and 1.

Now, $x$ is not in the list because: $x \neq s_1 \text{ since } x_1 \neq a_{11}$, $x \neq s_2 \text{ since } x_2 \neq a_{22}$, and so on.
Definition

$|S| \leq |T|$ if there exists $T_0 \subseteq T$ such that $|T_0| = |S|$.

Definition

$|S| < |T|$ if $|S| \leq |T|$ and $|S| \neq |T|$.

Claim

$|\mathbb{N}| < [0,1]$.

Proof:

We showed $|\mathbb{N}| \neq [0,1]$, so it is enough to show $|\mathbb{N}| \leq [0,1]$. Let $S = \mathbb{N}$ and $T = [0,1]$. Let $T_0 = \left\{1, \frac{1}{2}, \frac{1}{3}, \ldots\right\}$.

$|T_0| = |S|$ because $f : S \to T_0$, $f(n) = \frac{1}{n}$.

Theorem: Schroeder-Bernstein-Cantor Theorem

If $|S| \leq |T|$ and $|S| \geq |T|$, then $|S| = |T|$.

Theorem

If $a < b$ and $c < d$, then $[a,b] = [c,d]$.

Proof: Take $f : [a,b] \to [c,d]$, $x \to (x-a)\frac{d-c}{b-a} + c$. $f$ is 1-1 and onto.

Theorem

If $|S_i| = c$, $i = 1,2,3,\ldots$, then $\bigcup_{i=1}^{\infty} S_i = c$.

Proof: $S_1 \subseteq \bigcup_{i=1}^{\infty} S_i \Rightarrow c = |S_1| \leq \bigcup_{i=1}^{\infty} S_i$. Note that $\bigcup_{i=1}^{\infty} S_i = S_1 \cup (S_2 \setminus S_1) \cup (S_3 \setminus (S_1 \cup S_2)) \cup \cdots$ is the union of disjoint sets. Now, take $f : \bigcup_{i=1}^{\infty} S_i \overset{1:1}{\longrightarrow} \mathbb{R}$, where $S_1 \overset{1:1}{\longrightarrow} (0,1)$ (since $|S_1| = c$), $S_2 \overset{1:1}{\longrightarrow} (1,2)$ (since $|S_2| = c$), etc; then $\bigcup_{i=1}^{\infty} S_i \leq |\mathbb{R}| = c$. So, by S-C-B, $\bigcup_{i=1}^{\infty} S_i = c$.

Example

$|\mathbb{R}^2| = c$ because $\mathbb{R}^2$ can be divided into unit squares $S_i$, and then $|\mathbb{R}^2| = \bigcup_{i=1}^{\infty} S_i = c$. 

Page 22 of 39
Example
Let $S$ be the set of all sets of real numbers (ex: $S = \{\emptyset, \{1\}, \{1,2\}, \ldots, [0,1], [0,10,11], \ldots \}$). Then $|S| > c$.

Proof:
Want: $c < |S|$. Take $f : \mathbb{R} \to S; x \mapsto \{x\}$, so $|\mathbb{R}| = c < |S|$.

Want: $c \neq S$. Suppose $c = |\mathbb{R}| = |S|$, so there exists $g : \mathbb{R} \mapsto S$. Note that in particular $g$ is onto and $g(x)$ is a set of real numbers. Let $T := \{x \in \mathbb{R} | x \notin g(x)\} \subseteq S$. Claim: There is no $y \in \mathbb{R}$ such that $g(y) = T$.

Suppose there is $y \in \mathbb{R}$ such that $g(y) = T$. If $y \in g(y)$, then $y \in T \Rightarrow y \notin g(y)$ a contradiction; if $y \notin g(y)$, then $y \in T \Rightarrow y \in g(y)$ a contradiction. So this contradicts "$g$ is onto".

Notation
$|S| = 2^c$.

Remark
If $S_0$ is any set (not necessarily of $\mathbb{R}$), then let $S$ be the set of all subsets of $S_0$. We can show that $|S_0| < |S|$.

So $c < 2^c < 2^{2^c} < 2^{2^{2^c}} < \ldots$!

Theorem
The set of all subsets of $\mathbb{N}$ has cardinality $c$, i.e. $2^{\aleph_0} = c$.

Proof: Let $f : \mathbb{N} \to [0,1]$ be a characteristic function. For a subset $S \subseteq \mathbb{N}$ define its characteristic function $f_S(n) = \begin{cases} 1, & n \in S \\ 0, & n \notin S \end{cases}$. Let $T$ be the set of all characteristic function of $\mathbb{N}$.

Define $\varphi : T \to [0,1], f \mapsto 0.f(1)f(2)\cdots$. $\varphi$ is 1-1 because $\varphi(f) = \varphi(f') \Rightarrow 0.f(1)f(2)\cdots = 0.f'(1)f'(2)\cdots \Rightarrow f(1) = f'(1), f(2) = f'(2), \ldots \Rightarrow f = f'$. So $|T| \leq [0,1] = c$.

Now, for each $x \in [0,1]$ write it as $0.x_1x_2\cdots$ in binary (so $x_i = 0, 1$). Given $x \in [0,1]$ define a characteristic function $g_x(n) = x_n$. Define $\psi : [0,1] \to T, x \mapsto g_x$, which is 1-1. So $[0,1] = c \leq |T|$.

So $2^{\aleph_0} = c$.

**Enumeration Principle**

Any set in bijection with finite sequences of elements of a countable set is countable.

Example
Prove $\mathbb{Q}$ is countable.

$S = \mathbb{Q}^+ \cup \{+, -\}$ is countable. So $\mathbb{Q} \setminus \{0\}$ is countable, so $\mathbb{Q}$ is countable.
Prove \( \mathbb{Q}^n = \{(q_1, \ldots, q_n) | q_i \in \mathbb{Q}\} \) is countable.

Note: \( \mathbb{Q}^n \subseteq S \) a finite sequence of elements of \( \mathbb{Q} \), so \( |\mathbb{Q}^n| \leq |S| = \aleph_0 \).

Now let \( S^i \) be the set of sequences of length \( i \) of elements of a countable set. Since \( |S| = \aleph_0 \Rightarrow |S \times S| = |S|^2 = \aleph_0 \Rightarrow \cdots \Rightarrow |S \times \cdots \times S| = |S|^n = \aleph_0 \), so \( \bigcup_{i=1}^n S^i \) is countable.

**Lemma**
If \( S \) is infinite, then \( S \) contains a countably infinite set.

**Proof:** \( \exists s_1 \in S \), \( \exists s_2 \in S \setminus \{s_1\} \), \( \exists s_3 \in S \setminus \{s_1, s_2\} \), etc.

**Corollary**
If \( S \) is infinite, then \( |S| \geq \aleph_0 \), i.e. \( \aleph_0 \) is the smallest infinite cardinal.

**Theorem**
If \( S \) is uncountable and \( S_0 \) is a countable subset of \( S \), then \( |S \setminus S_0| = |S| \).

**Proof:** \( S \setminus S_0 \) is uncountable (otherwise \( (S \setminus S_0) \cup S_0 = S \) is countable). So there exists \( S_1 \subset S \setminus S_0 \) countable. Now \( S = (S \setminus S_0) \cup S_0 = (S \setminus S_0 \cup S_1) \cup S_0 \cup S_1 \). Let \( f : S_0 \cup S_1 \rightarrow S_1 \) be any 1-1 function.

Define \( \varphi : S \rightarrow S \setminus S_0 \), \( \varphi(s) = \begin{cases} s, & s \in S \setminus (S_0 \cup S_1) \\ f(s), & s \in S_0 \cup S_1 \end{cases} \). \( \varphi \) is 1-1 and onto. So \( |S \setminus S_0| = |S| \).

**Theorem**
\( S \) is infinite iff it has a proper subset \( S_0 \) such that \( S_0 \) has the same cardinality as \( S \).

**Proof:** If \( S \) is infinite, the by lemma there exists \( S_0 \subseteq S \) countably infinite. \( S = (S \setminus S_0) \cup S_0 \).

Let \( T = S \setminus \{s_1\} \) a proper subset of \( S \).

Let \( f : S \rightarrow T \), \( f(s) = \begin{cases} s, & s \in S \setminus S_0 \\ s_k \in S_0, k = 1, 2, \ldots \end{cases} \) is 1-1 and onto. So \( |T| = |S| \).

**ALGEBRAIC NUMBERS**

**Definition: Algebraic Number**
A real number is algebraic if there exists a (non-zero) polynomial with integer coefficients that has it as a root.

Notation: \( \mathbb{A} := \{\text{algebraic numbers}\} \).

**Theorem**
\( \mathbb{A} \) is countable.
Proof: Let \( A_1 := \{ x \in \mathbb{R} | p(x) = 0, p \) is polynomial of degree 1 with integer coefficients \}\). Note that:

\[
\begin{align*}
& A_1 \leftrightarrow \mathbb{Z} \times \mathbb{Z} \\
& A_2 \leftrightarrow \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}, \text{ so each } A_k \text{ is countable. Thus } A = \bigcup_{k \geq 1} A_k \text{ is countable.}
\end{align*}
\]

Corollary
\[ [\text{non-algebraic numbers}] = c. \]

ARITHMETIC WITH CARDINAL NUMBERS

Cardinal numbers: \( \{ 1, 2, \ldots, \aleph_0, 2^\aleph_0, \ldots \} \).

Definition: Addition
Let \( c_1 \) and \( c_2 \) be cardinal numbers, where \( c_1 = |S_1| \), \( c_2 = |S_2| \); assume \( S_1 \) and \( S_2 \) are disjoint.
\[ c_1 + c_2 := |S_1 \cup S_2|. \]

Example
1) \( \aleph_0 + \aleph_0 = ? \). Let \( \aleph_0 = \left| \left\{ n \in \mathbb{N} \right\} \right| \) and \( \aleph_0 = \left| \left\{ n + 1 | n \in \mathbb{N} \right\} \right| = |\mathbb{N}| = \aleph_0 \).
2) \( \aleph_0 + c = ? \). Let \( \aleph_0 = |\mathbb{Q}| \) and \( c = |\mathbb{R} \setminus \mathbb{Q}| \), then \( \aleph_0 + c = |\mathbb{R}| = c \).

Definition: Multiplication
\[ c_1 \times c_2 := |S_1 \times S_2|. \]

Example
1) \( \aleph_0 \times \aleph_0 = ? \). Let \( \aleph_0 = |\mathbb{N}| \), then \( \aleph_0 \times \aleph_0 = |\mathbb{N} \times \mathbb{N}| = \aleph_0 \).
2) \( \aleph_0 \times c = ? \). Let \( \aleph_0 = |\mathbb{N}| \) and \( c = |\mathbb{R}| \). Then \( \aleph_0 \times c = |\mathbb{N} \times \mathbb{R}| \leq |\mathbb{R} \times \mathbb{R}| = c \) \( \Rightarrow \aleph_0 \times c = c \).

Definition: Exponential
\[ X^A := \left| \left\{ f : f : A \to X \right\} \right|. \]

Example
\( 2^{\aleph_0} = ? \). Let \( 2 = |\{0, 1\}| \) and \( \aleph_0 = |\mathbb{N}| \), then \( 2^{\aleph_0} = \left| \left\{ f : f : \mathbb{N} \to \{0, 1\} \right\} \right| = |P(\mathbb{N})| = c \).
Classical Geometry

**NUMBER FIELDS**

**Examples: Closed Sets**

1) The set of rational numbers is closed under the four basic operations of arithmetic: +, −, ×, ÷.

2) The set of integer is not closed under division: \( 1 \div 2 = \frac{1}{2} \) is not an integer.

**Definition: Number Field**

A subset of \( \mathbb{R} \) which contains 0 and 1, and which is closed under the four basic arithmetic operations is called a number field.

**Examples**

1) \( \mathbb{Q}, \mathbb{R} \) are number fields.

2) \( \mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \) is a number field. It is closed under multiplication since

\[
(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + bb') + (ab' + a'b)\sqrt{2}.
\]

It is closed under multiplicative inverse since

\[
\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 + 2b^2} = \frac{a}{a^2 + 2b^2} - \frac{b}{a^2 + 2b^2} \sqrt{2}.
\]

**Remark**

- \( \mathbb{Q} \) is the smallest number field.
- \( \mathbb{R} \) is the largest number field.

**CONSTRUCTION YOU CAN MAKE WITH STRAIGHTEDGE AND COMPASS**

**Perpendicular Bisector of a Line Segment**

\[\text{\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{perpendicular_bisector.png}
\caption{Perpendicular Bisector of a Line Segment}
\end{figure}}\]
Bisect an Angle

Copy Angles

Draw a Parallel Line To a Given Line Through a Given Point

Copy Lengths

Trisect a Given Line Segment
CONSTRUCTIBLE NUMBERS

Start with a line and two points marked 0 and 1. Using straightedge and compass, can mark any natural number on the line by copying lengths.

Definition: Constructible Numbers
The set of numbers that can be marked on a line using straightedge and compass is called constructible numbers.
Notation: $C :=$ set of constructible numbers.

Note
1) If $a, b \in C$, then $a + b \in C$.
2) If $a \in C$, then $-a \in C$.
3) If $a, b \in C$ and $a, b > 0$, then $\frac{a}{b} \in C$. Note in particular, $\frac{1}{a} \in C$.

Suppose $b > 1$:

Suppose $b < 1$:

$x = \frac{1}{a} \Rightarrow x = \frac{a}{b}$.

$x = \frac{b}{1} \Rightarrow x = \frac{a}{b}$.

4) If $a, b \in C$ and $a, b > 0$, then $ab \in C$ (since $ab = \frac{a}{b} \in C$).

These prove the following theorem.
**Theorem**

$C$ is closed under the four basic arithmetic operations.

**Corollary**

$C$ is a number field.

**Note**

Recall that $\mathbb{Q} \left( \sqrt{2} \right)$ is a number field. More generally, if $F$ is any number field and $r \in F$ is such that $r > 0$ but $\sqrt{r} \notin F$, then define $F \left( \sqrt{r} \right) := \left\{ a + b\sqrt{r} \mid a, b \in F \right\}$ is a “bigger” number field.

**Theorem**

$F \left( \sqrt{r} \right)$ is a number field.

**Example**

$\mathbb{Q} \subseteq \mathbb{Q} \left( \sqrt{2} \right) \subseteq \mathbb{Q} \left( \sqrt{2} \right) \left( \sqrt{3} \right) \subseteq \mathbb{Q} \left( \sqrt{2} \right) \left( \sqrt{3} \right) \left( \sqrt{5} \right) \subseteq \cdots$.

**Definition: Tower of Number Fields**

A tower of number fields is a finite collection of number fields such that each is obtained from previous one by adjoining a square root: $F_0 \subseteq F_0 \left( \sqrt{r} \right) \subseteq F_1 \left( \sqrt{r} \right) \subseteq F_2 \left( \sqrt{r} \right) \subseteq \cdots \subseteq F_{n-1} \left( \sqrt{r} \right)$.

**Theorem**

If $r \in C$ and $r > 0$, then $\sqrt{r} \in C$.

**Proof:**

$$1 \frac{x}{r} \Rightarrow r = x^2 \Rightarrow x = \sqrt{r}.$$
If $\mathbb{Q} \subset E_1 \subset E_2 \subset \cdots \subset E_k$ is any tower, then $E_j \subset C$.

**SURDS**

**Definition: Surd**

A surd is a number that is in some $E_k$ where $E_k$ is in some tower starting at $\mathbb{Q}$.

Notation $S := \text{set of surds}$.

**Corollary**

$S \subseteq C$.

**Note**

Can construct a point $(a, b)$ in the plane iff the numbers $a$ and $b$ are construtable.

**Remark**

To prove $C \subseteq S$, we show that if you start with points whose coordinates are in $S$, then any construction produces points whose coordinates are also in $S$.

**Constructions Operations**

1) Join two constructed points by a line.
2) Make a circle with centre at a constructible point with constructible radius.
3) Take points of intersection of above.

**Corollary**

If a point is constructed as the intersection of two lines, both of which are determined by points with coefficients in $S$, then the point has coefficients in $S$.

**Proof:** Suppose $(a, b)$ and $(c, d)$ have $a, b, c, d \in S$. Then there exists an extension $F$ (the end of a tower) of $\mathbb{Q}$ such that $a, b, c, d \in F$.

Now the equation of the line joining $(a, b)$ and $(c, d)$ is

$$\frac{y-b}{x-a} = \frac{d-b}{c-a} \quad \text{or} \quad y = \left(\frac{d-b}{c-a}\right)x + \frac{b-d}{c-a}.$$  

Note $\alpha, \beta \in F$.

**Corollary**

If a point is constructed as the intersection of a line and a circle, both of which are determined by points with coefficients in $S$, then the point has coefficients in $S$.

**Proof:** A circle with centre $(a, b)$ and radius $r$, where $a, b, r \in S$, has equation

$$(x-a)^2 + (y-b)^2 = r^2 \iff x^2 + y^2 + \left(-2a\right)x + \left(-2b\right)y + \left(a^2 + b^2 - r^2\right) = 0.$$  

Since there is some extension $F$ such that $a, b, r \in F$, so $\alpha, \beta, \gamma \in F$. 
Now, at the intersection
\[ \begin{align*}
\begin{cases}
y^2 + x^2 + \alpha x + \beta y + \gamma &= 0 \\
y &= \alpha' x + \beta'
\end{cases} \Rightarrow (\alpha' x + \beta')^2 + x^2 + \alpha + (\alpha' x + \beta')y + \gamma &= 0
\end{align*} \]

\[
\left(\frac{\alpha'^2 + 1}{A}\right)x^2 + \left(\frac{2\alpha'\beta' + \alpha + \alpha'\beta}{B}\right)x + \left[\frac{(\beta'^2 + \beta\beta')}{C}\right] = 0, \text{ so}
\]

\[
x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A} = \frac{-B}{2A} \pm \frac{1}{2A} \sqrt{B^2 - 4AC} \in F\left(\sqrt{B^2 - 4AC}\right) \subseteq S.
\]

**Corollary**

\[ C \subseteq S. \]

**CANNOT TRISECT A 60° ANGLE**

**Facts**

1) Can construct a 60° angle.
2) If we could trisect a 60° angle, then we could construct a 20° angle.
3) If an angle \( \theta \) (acute) is constructible, then \( \cos \theta \) is constructible.

So, to show one cannot trisect a 60° angle, it is enough to show that \( \cos(20°) \notin C \). Since \( C = S \), it is enough to show \( \cos(20°) \notin S \).

**Note**

\[ \cos(3A) = 4 \cos^3 A - 3 \cos A. \] So, \( \cos(60°) = \frac{1}{2} \Leftrightarrow 4 \cos^3(20°) - 3 \cos(20°) = \frac{1}{2} \Leftrightarrow \]

\[ 8 \cos^3(20°) - 6 \cos(20°) - 1 = 0 \Leftrightarrow \left(2 \cos(20°)\right)^3 - 3(2 \cos(20°)) - 1 = 0, \] which means \( 2 \cos 20° \) is a solution to \( x^3 - 3x - 1 = 0 \).

**Facts**

1) If a cubic equation with rational coefficient has a solution which is a constructible number, then it has a rational solution.
2) \( x^3 - 3x - 1 = 0 \) has no rational root.

**Proof:** A rational root \( r = \frac{a}{b} \) must be such that \( a \mid 1 \) and \( b \mid 1 \), so \( r = \pm 1 \). But \( \pm 1 \) are not roots!

**Theorem**

If a cubic equation with rational coefficient has a constructible root, then it must have a rational root.

**Proof:** Note the following facts:
1) It suffices to consider cubics with leading coefficient 1.
2) Any cubic with leading coefficient 1 looks like \( (x - r_1) \cdots (x - r_n) \), where \( r_1, \ldots, r_n \) are (perhaps complex) roots.
3) Notice that \( (x - r_1)(x - r_2)(x - r_3) = x^3 + \left(\frac{r_1 + r_2 + r_3}{Q}\right)x^2 + \cdots \), i.e. the sum of all three roots of a cubic is a rational number.
4) Let \( a + b\sqrt{r} \in F\left(\sqrt{r}\right) = \left\{ a + b\sqrt{r} \mid a, b \in F, \sqrt{r} \notin F \right\} \). Define the conjugate of \( a + b\sqrt{r} \) as \( \overline{a + b\sqrt{r}} = a - b\sqrt{r} \).

5) \( (a + b\sqrt{r}) + (c + d\sqrt{r}) = a + b\sqrt{r} + c + d\sqrt{r} \).

6) \( (a + b\sqrt{r}) \cdot (c + d\sqrt{r}) = \left( a + b\sqrt{r} \right) \cdot \left( c + d\sqrt{r} \right) \).

7) \( \left( a + b\sqrt{r} \right)^k = \left( a + b\sqrt{r} \right)^k \).

Let \( x_0 \) be the constructible root, so \( x_0 \) is a surd. So there exists some tower \( Q \subset F_0 \subset \cdots \subset F_k, F_{i+1} = F_i \left( \sqrt[n]{r_i} \right) \) such that \( x_0 \in F_k \). So \( x_0 = a_0 + b_0 \sqrt[k]{r_{k-1}}, a_0, b_0, r_{k-1} \in F_{k-1} \). Assume we choose a shortest tower containing \( x_0 \) (i.e. \( b_0 \neq 0 \); or if \( x_0 \in Q \) then we’re done).

By proposition, \( x_0 = a_0 - b_0 \sqrt[k]{r_{k-1}} \) is also a root. Let \( s \) be the third root. Now

\[
x_0 + \bar{x}_0 + s = q \in Q \Rightarrow 2a_0 + s = q \Rightarrow s = \frac{q - 2a_0}{e Q} \in F_{k-1} \cdot \text{By repeating this argument, we can conclude that} \quad s \in Q.
\]

**Proposition**

Suppose \( p \) is a polynomial with rational coefficients. If \( p(a + b\sqrt{r}) = 0 \), then \( p(a - b\sqrt{r}) = 0 \).

**Proof:** Notice \( p(x) = a_k x^k + \cdots + a_0 = a_k x^k + \cdots + a_0 = a_k (x)^k + \cdots + a_0 = a_k x^k + \cdots + a_0 \). So

\[
p(a + b\sqrt{r}) = 0 \Rightarrow p(a + b\sqrt{r}) = 0 \Rightarrow p(a + b\sqrt{r}) = 0.
\]

**Lemma**

If \( x_0 \) is a root of a polynomial with coefficients in \( F\left(\sqrt{r}\right) \), when \( x_0 \) is a root of a polynomial with coefficients in \( F \) (of twice degree).

**Proof:** \( \alpha_{e F} x_o + \cdots + \alpha_0 = 0, \alpha_i \in F\left(\sqrt{r}\right), \alpha_i = a_i + b_i \sqrt{r}, a_i, b_i, r \in F \Rightarrow \Rightarrow \)

\[
(a_k + b_k \sqrt{r})x_o^k + \cdots + a_0 + b_0 \sqrt{r} = 0 \Rightarrow (a_k + b_k \sqrt{r})x_o^k + \cdots + a_0 + b_0 \sqrt{r} = 0 \Rightarrow
\]

\[
a_k x_o^k + \cdots + a_0 = -\sqrt{r} \left( b_k x_o^k + \cdots + b_0 \right) \Rightarrow \left( a_k x_o^k + \cdots + a_0 \right)^2 - r \left( b_k x_o^k + \cdots + b_0 \right)^2 = 0 \Rightarrow
\]

\[
\left( a_k^2 - rb_k^2 \right) x_o^{2k} + \cdots + \left( a_0^2 - rb_0^2 \right) = 0.
\]

**Theorem**

Every constructible number is algebraic.

**Proof:** Suppose \( x_0 \) is constructible, so \( x_0 \in F_k \). Now \( p(x) = x - x_0 \) has coefficients in \( F_k = F_k \left( \sqrt{r} \right) \). Now apply the lemma until the coefficients are in \( Q \), and multiply it by the common denominator.

**Example**

A 50\(^\circ\) angle is not constructible.
Note that a $90^\circ$ is constructible. Suppose $50^\circ$ is constructible, then $40^\circ$ is constructible. By bisecting, $20^\circ$ is constructible. Contradiction.

**Example**

$\sqrt[3]{5}$ is not constructible.

Suppose $\sqrt[3]{5}$ is constructible. Since $\sqrt[3]{5}$ is a root of $x^3 - 5$, so $x^3 - 5$ has a rational root. Now, $(x^3 - 5)' = 3x^2 > 0, \forall x \in \mathbb{R}$, there is one real root. But $\sqrt[3]{5}$ is real, but not rational. Contradiction.

**Example**

$\sqrt{5} + \sqrt{3}$ is constructible.

Note that $\mathbb{Q} \subset \mathbb{Q} \left( \frac{\sqrt{5}}{\sqrt{3}} \right) \subset \mathbb{Q} \left( \frac{\sqrt{5}}{\sqrt{3}} \right) \left( \sqrt{5} + \sqrt{3} \right)$.

**Corollary**

Cannot trisect $60^\circ$.

**Proof:** Assume can trisect $60^\circ$. Since $60^\circ$ is constructible, this implies $20^\circ$ is constructible. Contradiction.

**REGULAR POLYGONS**

**Example: Duplication of the Cube**

Given a cube of volume 1 (edges are 1), can you construct a cube of volume 2? Volume of cube is $x^3$, where $x$ is the length of the edge. Does $x^3 - 2 = 0$ have a constructible solution? If $x^3 - 2$ has a constructible root, then it has a rational root, but $x^3 - 2$ has no rational root. (Suppose $\frac{m}{n}$ is a root, then $\left( \frac{m}{n} \right)^3 = 2 \Rightarrow m^3 = 2n^3$. If $p \mid m \Rightarrow p^3 \mid m^3 \Rightarrow p^3 \mid 2n^3 \Rightarrow p \mid n \Rightarrow m = \pm 1$; if $p \mid n \Rightarrow p^3 \mid n^3 \Rightarrow p \mid m \Rightarrow n = \pm 1$. So $\frac{m}{n} = \pm 1$. Contradiction! So no rational solution.)

**Definition: Regular Polygon**

Regular polygon has equal sides and angles.

![Regular Polygons](image)

**Fact**

Every regular polygon can be inscribed in a circle.

**Proof:** Find the centre and radius of the circle as follows:
Definition: Central Angle
The central angle of a regular \( n \)-gon is \( \frac{360^\circ}{n} \).

Note
A regular polygon is constructible if and only if the central angle is constructible.

Corollary
A regular 18-gon is not constructible.
Proof: The central angle is \( \frac{360^\circ}{18} = 20^\circ \).

Corollary
A regular 9-gon is not constructible.

Corollary
Regular 9, 18, 36, 72,...-gons are not constructible.

Fact
If a regular \( n \)-gon is constructible, then the regular \( n \)-gon can be constructed such that it is inscribed in a circle of radius 1.
Lemma
A regular \( n \)-gon is constructible if and only if the length of an edge of the regular \( n \)-gon inscribed in a circle of radius 1 is constructible.

Proof (\( \Leftarrow \)):

Corollary
A regular 10-gon is constructible.

Proof: Suppose we have a 10-gon inside the unit circle (don’t know if it is constructible) Let \( s \) be the length of the side. We show \( s \) is constructible.

Since \( \triangle OAB \sim \triangle ABC \Rightarrow \frac{s}{1} = 1 - s \), so

\[ s^2 = 1 - s \Rightarrow s^2 + s - 1 = 0 \Rightarrow s = \frac{-1 \pm \sqrt{1+4}}{2} \]. But since \( s > 0 \), so \( s = \frac{\sqrt{5} - 1}{2} \in Q(\sqrt{5}) \) which is constructible.
Corollary
A regular 5, 10, 20,…-gon is constructible.

Corollary
A 7-gon is not constructible.

Proof:
Let \( z \in \mathbb{C} \). We know \( z^7 = 1 \), \( |z| = 1 \), \( z \neq 1 \).

\[
\begin{align*}
    z^7 - 1 &= 0 \\
    (z-1)(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) &= 0 \\
    z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 &= 0 \\
    z^3 + z^2 + z + 1 + \frac{1}{z} + \frac{1}{z^2} + \frac{1}{z^3} &= 0 \\
    (z + \frac{1}{z})^3 + (z + \frac{1}{z})^2 - 2(z + \frac{1}{z}) + 1 &= 0
\end{align*}
\]

Now, let \( x_0 = z + \frac{1}{z} \). Then \( x_0 = 2 \text{Re}(z) \) (because \( |z| = 1 \Rightarrow \text{Re}z = 1 \Rightarrow z = \frac{1}{z} \), so \( x_0 = z + \frac{1}{z} = 2 \text{Re}(z) \)).

So \( x_0 = 2 \text{Re}(z) \) satisfies \( x^3 + x^2 - 2x - 1 = 0 \). To show \( z \) is not constructible, it’s enough to show \( x_0 \) is not constructible. Now if \( x_0 \) is constructible, then \( x^3 + x^2 - 2x - 1 \) has a rational root, but it doesn’t.

**TRISECTING ANGLES**

**Remark**
36° is constructible since a 10-gon is constructible.

**Recall**
We proved that every constructible number is algebraic.

**Corollary**
An angle cannot be constructed (with straightedge and compass) if \( \cos \theta \) is transcendental.

**Proof** \( \theta \) constructible \( \iff \) \( \cos \theta \) constructible \( \iff \) \( \cos \theta \) algebraic.

**Example**
Suppose \( \cos \frac{\theta}{3} \) is transcendental. Then we know \( \frac{\theta}{3} \) is not constructible.

**Note**
Given an angle \( \theta \) (don’t know if \( \theta \) is constructible or not), can \( \theta \) be trisected?
Theorem
If \( \cos \theta \) is transcendental, then \( \theta \) is not trisectible.

Proof:
Given angle \( \theta \), can construct from it the number \( c := \cos \theta \).
Let \( F_0 = \left\{ \frac{p(c)}{q(c)} \mid p, q \text{ polynomials with rational coefficients such that } q(c) \neq 0 \right\} \). Note \( F_0 = \mathbb{Q}(c) \) is the smallest number field containing \( \mathbb{Q} \) and \( c \).
Using straightedge and compass, can construct towers starting with \( F_0 : F_0 \subset F_0 \left( \sqrt[n]{c} \right) \subset \cdots \).
Assume \( \frac{\theta}{3} \) is constructible from \( \theta \). Then \( \frac{\theta}{3} \) is in such a tower. So \( 4x^3 - 3x = c \) has a solution in such a tower \( (F_0 \subset F_0 \left( \sqrt[n]{c} \right) \subset \cdots) \), and thus \( 4x^3 - 3x = c \) has a solution in \( F_0 = \mathbb{Q}(c) \).
We need to show \( 4x^3 - 3x = c \) has no solution in \( F_0 = \mathbb{Q}(c) \). Suppose there is a solution in \( F_0 = \mathbb{Q}(c) \), i.e.
\[
4 \left( \frac{p(c)}{q(c)} \right)^3 - 3 \left( \frac{p(c)}{q(c)} \right)^3 = c \Rightarrow 4(p(c))^3 - 3(p(c))(q(c))^2 - c(q(c))^3 = 0 ,
\]
which is a polynomial in \( c \) with rational coefficient. Now, not all coefficients are 0 because \( c := \cos \theta \) is transcendental and:
- Case 1: \( \deg(p) < \deg(q) \). The highest appearing power of \( c \) comes from \( -c(q(c))^3 \neq 0 \).
- Case 2: \( \deg(p) > \deg(q) \). The highest appearing power of \( c \) comes from \( 4(p(c))^3 \neq 0 \).
- Case 3: \( \deg(p) = \deg(q) \). The highest appearing power of \( c \) comes from \( -c(q(c))^3 \neq 0 \).
Therefore, \( 4(p(c))^3 - 3(p(c))(q(c))^2 - c(q(c))^3 \neq 0 \). Contradiction.

Example
Any angle can be trisected with compass and ruler. Given \( \theta \)

\[
\begin{align*}
p & = \theta \quad \text{Claim: } x = \frac{\theta}{3} . \\
\pi - 2x & = \pi - y \Rightarrow 2x = \pi - y \\
\pi & = 2(\pi - y) + z \\
\pi - \gamma & = \pi - \theta \\
\gamma & = \pi - \theta .
\end{align*}
\]

Proof:
\[
\begin{align*}
y = \pi - 2x & \Rightarrow \pi - y = 2x \\
\pi & = 4x + z \Rightarrow z = \pi - 4x .
\end{align*}
\]
Also, \( \gamma = \pi - \pi - \theta \). So \( 4x = x + \theta \Rightarrow x = \frac{\theta}{3} .
\]

REGULAR POLYHEDRONS

Definition: Polyhedron
A polyhedron is a solid, all of whose faces are polygons.

Definition: Regular Polyhedron
A regular polyhedron (platonic solid) is a polyhedron all of whose faces are regular polygons with the same number of sides as each other, and all of whose vertices lie on the same number of faces.

**Examples**

![Polyhedra Diagram]

**Theorem**
There are only 5 regular polyhedrons.

**Proof**: Let \( n \) be the number of sides of a face, and \( k \) be the number of faces on which a vertex lies. Note that \( n, k \geq 3 \).

Note that for a regular \( n \)-gon,
\[
\begin{align*}
2\theta &= 2\pi \\
2x + \theta &= \pi
\end{align*}
\]

So
\[
2x = \pi - \theta = \frac{n\theta}{2} - \theta = \theta \left( \frac{n-2}{2} \right) = \frac{(n-2)\pi}{n}.
\]
Now, $k$ faces meet at a vertex means $k(2\pi) < 2\pi \Rightarrow \frac{k(n-2)}{n} < 2 \Rightarrow k - \frac{2k}{n} < 2$. Since

$$n \geq 3 \Rightarrow \frac{1}{n} \leq \frac{2}{3} \Rightarrow \frac{n}{2k} \geq \frac{k-2}{3} = \frac{k}{3}.$$ Thus $k - \frac{2k}{n} \geq \frac{k}{3} < 2 \Rightarrow k < 6 \Rightarrow k = 3, 4, 5$.

If $k = 3$, then $3 - \frac{2(3)}{n} < 2 \Rightarrow n < 6 \Rightarrow n = 3, 4, 5$. If $n = 3$, tetrahedron; if $n = 4$, cube; if $n = 5$, dodecahedron.

If $k = 4$, then $4 - \frac{2(4)}{n} < 2 \Rightarrow n < 4 \Rightarrow n = 3$. This is the octahedron.

If $k = 5$, then $5 - \frac{2(5)}{n} < 2 \Rightarrow n < \frac{10}{3} \Rightarrow n = 3$. This is the icosahedron.