Mathematical Induction

Notation
$\mathbf{N} := \{1,2,3,\ldots\}$ are called the "natural numbers".

Principle of Mathematical Induction
Suppose S is a set of natural numbers (i.e. $S \subseteq \mathbf{N}$). If:

1) $1 \in S$.
2) $k+1 \in S$ whenever $k \in S$.

Then $S = \mathbf{N}$.

Example
Prove for all $n \in \mathbf{N}$ the following formula holds: $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

Proof:

- Let $S = \left\{ m \in \mathbf{N} \mid 1^2 + \cdots + m^2 = \dfrac{m(m+1)(2m+1)}{6} \right\}$.
- $1 \in S$: $1^2 = 1$ and $\dfrac{1(2)(3)}{6} = 1$.
- Assume $k \in S$. Show $k+1 \in S$.
    - $k \in S \Rightarrow 1^2 + \cdots + k^2 = \dfrac{k(k+1)(2k+1)}{6}$.
    - $$\begin{aligned} 1^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 = (k+1)\frac{k(2k+1)+6(k+1)}{6} \\ &= (k+1)\frac{2k^2+7k+6}{6} = \frac{(k+1)(k+2)(2k+3)}{6} \\ &= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} \end{aligned}$$ So $k+1 \in S$.

Extended Principle of Mathematical Induction
Suppose S is a set of natural numbers (i.e. $S \subseteq \mathbf{N}$). 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 $S = \{ m \in \mathbf{N} \mid m! \geq 3^m \}$. 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 $\mathbf{N}$ other than ϕ has a smallest element.

Theorem
Suppose $S \subseteq \mathbf{N}$. If:
1) $1 \in S$.
2) $k+1 \in S$ whenever $k \in S$.

Then $S = \mathbf{N}$.

Proof:
- Let $T = \{n \in \mathbf{N} \mid n \notin S\}$, i.e., T is the "complement" of S.
- Want to show that $T = \phi$. This is equivalent to $S = \mathbf{N}$.
- Suppose $T \neq \phi$. 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 $a, b \in \mathbf{N}$. Say "a divides b" (write $a \mid b$) if $b = a \cdot c$ for some $c \in \mathbf{N}$.

Definition
$p \in \mathbf{N}$ is <u>prime</u> 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. $S \subseteq \mathbf{N}$). 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 $\left.\begin{array}{r} m = p_1 \cdots p_l \\ m' = q_1 \cdots q_{l'} \end{array}\right\} n = mm' = p_1 \cdots p_l \cdot q_1 \cdots q_{l'}$.

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 $\{p_1, \dots, p_{k+1}\}$ 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 $n \in \mathbf{N}$ 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 $S = \{n \in \mathbf{N} \mid n \neq 1 \text{ and } n \text{ is a product of primes}\}$.
  - $2 \in S$.
  - If $2,3,\dots,n-1 \in s$, 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. $n = mm', m, m' \in \mathbf{N}$ 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 $\{2,3,\dots, p\}$ is the set of all primes.
- Let $M = 2 \cdot 3 \cdot \cdots \cdot p + 1$. Note that 2, 3, …, p don't divide M.
- Now, $M > 1$, so there is some prime number q such that $q \mid M$.
- But $q \neq 2,3,\dots, p$, 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 $M = N - p_1 q_2 \cdots q_l = q_1 q_2 \cdots q_l - p_1 q_2 \cdots q_l = (q_2 \cdots q_l)(p_1 - q_1)$, but also, $M = N - p_1 q_2 \cdots q_l = p_1 p_2 \cdots p_k - p_1 q_2 \cdots q_l = p_1 (p_2 \cdots p_k - q_2 \cdots q_l)$. 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

$48 = 16 \cdot 3 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3 = 3 \cdot 2^4 = 2 \cdot 2 \cdot 3 \cdot 2 \cdot 2$.

Definition

A natural number is called a <u>composite</u> if it is not 1 and it is not a prime number.

SERIES

- $a_1 + a_2 + \cdots, a_i \in \mathbf{R}$ 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) $1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots = 1+\frac{1}{2}+\frac{1}{2^2}+\frac{1}{3^3}+\cdots$ (geometric series) converges. More generally, $1+\frac{1}{r}+\frac{1}{r^2}+\frac{1}{r^3}+\cdots = \frac{1}{1-\left(\frac{1}{r}\right)}, 0 < \frac{1}{r} < 1$. 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 $N \in \mathbf{N}$ be fixed, but arbitrarily.
- Let $F(N) = \#\{1 \le n \le N \mid n \text{ is divisible only by the primes } p_1, \ldots, p_j\}$.

- Now, $N - F(N) = \#\{1 < n < N \mid n \text{ has a prime factor among } p_{j+1}, p_{j+2}, \ldots\}$.
  $N - F(N) \le \frac{N}{p_{j+1}} + \frac{N}{p_{j+2}} + \cdots = N\left(\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \cdots\right) < \frac{N}{2}$. So $N - F(N) < \frac{N}{2} \Leftrightarrow F(N) > \frac{N}{2}$.
- Write $n = s^2 t$, s is the largest perfect square, and t is square free. Note that $s \le \sqrt{N}$ 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 $F(N) \le 2^j \sqrt{N}$.
- So, now $\frac{N}{2} < F(N) \le 2^j \sqrt{N} \Rightarrow \frac{N}{2} < 2^j \sqrt{N} \Rightarrow \sqrt{N} < 2^{j+1}$. But j is fixed, and N arbitrary. Contradiction!

CONGRUENCE AND MODULAR ARITHMETIC

Definition

Let $a, b \in \mathbf{Z}$ be two integers, and let $m \in \mathbf{N}$ be a natural number. If $m \mid a - b$, then we say "a is congruent to b modulo m" and write $a \equiv b \bmod m$.

Examples

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

Example

Suppose $k, m \in \mathbf{N}$. Write $k = qm + r$ (q is the quotient, $0 \le r < m$ is the remainder). Saying $k = qm + r$ is equivalent to saying $k = r \bmod m$.

Application

Is $2^{29} + 3$ divisible by 2?

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

Application

Is $2^{29} + 3$ divisible by 7?

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

Some Rules for Working with Congruence

Let $a,b,c,d \in \mathbf{Z}$, $m,k \in \mathbf{N}$.

1) $a \equiv b \bmod m \Rightarrow a+c \equiv b+c \bmod m$ and $\begin{cases} a \equiv b \bmod m \\ c \equiv d \bmod m \end{cases} \Rightarrow a+c \equiv b+d \bmod m$.
2) $\begin{cases} a \equiv b \bmod m \\ c \equiv d \bmod m \end{cases} \Rightarrow ac \equiv bd \bmod m$.
3) $a \equiv b \bmod m \Rightarrow a^2 \equiv b^2 \bmod m$.
4) $a \equiv b \bmod m \Rightarrow a^k \equiv b^k \bmod m$.

Proof:

1) $a \equiv b \bmod m \Leftrightarrow m \mid a-b \Leftrightarrow m \mid (a+c)-(b+c) \Leftrightarrow a+c \equiv b+c \bmod m$.
2) $\left.\begin{matrix} a \equiv b \bmod m \Leftrightarrow m \mid a-b \Leftrightarrow a-b = qm \Leftrightarrow ac-bc = cqm \\ c \equiv d \bmod m \Leftrightarrow m \mid c-d \Leftrightarrow c-d = qm \Leftrightarrow bc-bd = bq'm \end{matrix}\right\} \Rightarrow ac-bc+bc-bd = cqm+bq'm \Rightarrow$
$ac-bd = m(cq+bq') \Rightarrow m \mid ac-bd \Leftrightarrow ac \equiv bd \bmod m$.

Example

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

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

Theorem

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

Proof: By FTA, $\left.\begin{matrix} a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \\ b = q_1^{\beta_1} \cdots q_l^{\beta_l} \end{matrix}\right\} \Rightarrow ab = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$. Now $p \mid ab$ means $p = p_i$ or $p = q_j$ by FTA. So $p = p_i \Rightarrow p \mid a$ or $p = q_j \Rightarrow p \mid b$.

LAW OF CANCELLATION

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

Examples

1) $3 \cdot 2 = 3 \cdot 0 \bmod 6$, but $2 \not\equiv 0 \bmod 6$. Equivalently, 3 has no inverse modulo 6.
2) $3 \cdot 1 \equiv 3 \cdot 6 \bmod 5$ and $1 \equiv 6 \bmod 5$.

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 $ax \equiv ay \bmod p \Rightarrow x \equiv y \bmod p$.

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

Note

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

Example

$2 \equiv 7 \equiv 12 \equiv 17 \equiv \cdots \bmod 5$. 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 $a^{p-1} \equiv 1 \bmod p$.

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 $a \cdot n \equiv a \cdot m \bmod p, 1 \le n, m \le p-1, n \ne m$. Then $n \equiv m \bmod p$, but $n - m \le p - 1$, so $p - 1 \nmid n - m$. Contradiction!)
  - None of the elements are congruent to 0 modulo p. ($an \equiv 0 \bmod p \Rightarrow n \equiv 0 \bmod p$, but $n \le p - 1 < p$ 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 $a \cdot (a \cdot 2) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p \;\Rightarrow$ $a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p \;\Rightarrow\; a^{p-1} \equiv 1 \bmod p$ 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 $ba \equiv 1 \bmod p$.

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

Example

Let $p = 5$, $a = 3$. If $b3 \equiv 1 \bmod 5$, 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 $(p-1)! \equiv -1 \bmod p$.

Proof:

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

Definition

$n \in \mathbf{N}$ is <u>composite</u> if $n \neq 1$ and n is not prime.

Note

So $\mathbf{N} = \{1\} \cup \{\text{primes}\} \cup \{\text{composites}\}$.

Definition

Let $m, n \in \mathbf{N}$. The greatest common divisor of m and n is the largest $d \in \mathbf{N}$ 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 ϕ

Let $n \in \mathbf{N} \setminus \{1\}$. The Euler function $\phi(n)$ is the number of elements in $\{1,2,\dots,n-1\}$ which are relatively prime to n.

Lemma

$$\left.\begin{array}{l} m \mid ab \\ (m,a) = 1 \end{array}\right\} \Rightarrow m \mid b.$$

Proof: Let $a = {p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k}$, $b = {q_1}^{\beta_1} \cdots {q_l}^{\beta_l}$. $m \mid ab \Rightarrow {p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k} {q_1}^{\beta_1} \cdots {q_l}^{\beta_l} = cm$. 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, $\left.\begin{array}{l} p \mid ab \\ p \nmid a \end{array}\right\} \Rightarrow p \mid b$.

Lemma

$$\left.\begin{array}{r}(a,m)=1\\(b,m)=1\end{array}\right\}\Rightarrow (ab,m)=1\,.$$

Proof: Suppose $(ab,m)\neq 1$. So there exists p such that $p\mid ab$ and $p\mid m$. So $\left.\begin{array}{r}p\mid a\\p\mid m\end{array}\right\}\Rightarrow (a,m)\neq 1$ or $\left.\begin{array}{r}p\mid b\\p\mid m\end{array}\right\}\Rightarrow (b,m)\neq 1$.

Note

$$\left.\begin{array}{r}p\nmid a\\p\nmid b\end{array}\right\}\Rightarrow p\nmid ab\,.$$

Note

$$\left.\begin{array}{r}a\equiv b \bmod m\\(a,m)=1\end{array}\right\}\Rightarrow (b,m)=1\,.$$

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 $\left.\begin{array}{r}p\mid b\\p\mid m\end{array}\right)\Rightarrow p\mid b+km\Rightarrow (b+km,m)\neq 1$. Contradiction!

Proposition

$$\left.\begin{array}{r}ax\equiv ay \bmod m\\(a,m)=1\end{array}\right\}\Rightarrow x\equiv y \bmod m\,.$$

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

Theorem: Euler's Theorem

Let $m\in\mathbf{N}\setminus\{1\}$. If $(a,m)=1$, then $a^{\phi(m)}\equiv 1 \bmod m$.

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 $an_i\equiv an_j \bmod m$, then $n_i\equiv n_j \bmod m$, 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 $(an_1)\cdots(an_{\phi(m)})\equiv n_1\cdots n_{\phi(m)} \bmod m \;\Rightarrow\; a^{\phi(n)}(n_1\cdots n_{\phi(m)})\equiv n_1\cdots n_{\phi(m)} \bmod m \;\Rightarrow\; a^{\phi(n)}\equiv 1 \bmod m$.

PUBLIC KEY CRYPTOGRAPHY

History

Towards RSA public key coding: Ronald Rivest, Adi Shamir, Leonard Adleman.

Fact 1

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

Proof: $N - \phi(N) = \#\{1 \le n \le N \mid (n, N) \ne 1\} = \#\{1 \le n \le N \mid p \mid n \text{ or } q \mid n\} = \#\{1 \le n \le N \mid p \mid n \text{ or } q \mid n\}$. Now, $\#\{1 \le n \le N \mid p \mid n\} = \#\{p, 2p, \ldots (q-1)p, qp\}$ and $\#\{1 \le n \le N \mid p \mid n\} = \#\{q, 2q, \ldots (p-1)q, pq\}$. So $N - \phi(N) = \#\{p, 2p, \ldots (q-1)p, qp\} \cup \#\{q, 2q, \ldots (p-1)q, pq\} = p + q - 1$. Therefore, $N - \phi(N) = p + q - 1 \Rightarrow \phi(N) = N - (p + q - 1) = pq - p - q + 1 = (p-1)(q-1)$.

Example

Let $p = 5$, $q = 3$, $N = pq = 5 \times 3 = 15$.

- $\phi(N) = \phi(15) = \#\{1,2,4,7,8,11,13,14\} = 8$.
- $\phi(N) = \phi(pq) = \phi(15) = \phi(5 \times 3) = 4 \times 2 = 8$.

Fact 2

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

Example

$\gcd(5,7) = 1$. $\left.\begin{array}{l} 7 = 1(5) + (2) \\ 5 = 2(2) + (1) \\ 2 = 2(1) + (0) \end{array}\right\} \Rightarrow 1 = 5 - 2(2) = 5 - 2(7 - 1(5)) = 3(5) - 2(7)$. So let $\begin{array}{l} x = 3 \\ y = -2 \end{array}$.

Lemma

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

Proof:

- $n \equiv 1 \bmod \phi(N) \Leftrightarrow \phi(N) \mid n - 1 \Leftrightarrow n - 1 = k\phi(N) \Leftrightarrow n = k\phi(N) + 1 \Rightarrow M^n = M^{k\phi(N)+1} = M \cdot \left(M^{\phi(N)}\right)^k$.
- We want $M^n \equiv M \bmod N$. It is enough to show $M^n \equiv M \bmod p$ and $M^n \equiv M \bmod q$. We show $M^n \equiv M \bmod p$.
  - Case 1: If $p \mid M$, then $M^n \equiv 0 \equiv M \bmod p$.
  - Case 2: If $p \nmid M$, then $(M, p) = 1$. So by Euler's Theorem, $M^n = M \cdot \left(M^{\phi(N)}\right)^k = M \cdot \left(M^{\phi(p)}\right)^{\phi(q)k} \equiv M \cdot (1)^{\phi(p)k} = M \bmod p$.

Algorithm

Receiver	Sender
Choose p, q large primes. $N = p \cdot q$. $\phi(N) = (p-1)(q-1)$ (fact 1).	N

Choose e relatively prime to p, q. Find d such that $de + k\phi(N) = 1$ (fact 2).	e
	$0 < M < N$, M is the message. $M^e \equiv R \bmod N$. R is the coded message.
R is the encoded message. $R^d \equiv M \bmod N$. M is the decoded message.	

Remarks

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

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 $\gcd(a,b) = d, a, b, d \in \mathbf{N}$, then there exists $x, y \in \mathbf{Z}$ such that $xa + yb = d$.

Proof:

- $\gcd(a,b) = d \ \Rightarrow \ a = q \cdot b + r, 0 \le r < b \ \Rightarrow \ b = q_1 \cdot r + r_1, 0 \le r_1 < r \ \Rightarrow \ r = q_2 \cdot r_1 + r_2, 0 \le r_2 < r_1 \ \Rightarrow \ldots$ $\Rightarrow \ r_{k-1} = q_k \cdot r_k + r_{k+1}, 0 \le r_{k+1} < r_k \ \Rightarrow \ r_k = q_{k+1} \cdot r_{k+1} + 0$ (terminates because $\{r, r_1, \ldots, r_k\}$ is a strictly decreasing sequence).
- Since $d \mid a, b$, so $d \mid a, b \Rightarrow d \mid r, b \Rightarrow d \mid r_1, r \Rightarrow d \mid r_2, r_1 \Rightarrow \cdots \Rightarrow d \mid r_{k+1}, r_k$. So $d \mid r_{k+1}$.
- 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 $\left.\begin{matrix} d \mid r_{k+1} \\ r_{k+1} \mid d \end{matrix}\right\} \Rightarrow r_{k+1} = d$.

Note

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

Rational Numbers

Definition

$\mathbf{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbf{Z}; n \ne 0 \right\}$ is the set of rational numbers.

Remark
$\mathbf{R} = \mathbf{Q} \cup \{\text{irrational}\}$.

Definition
$\frac{m}{n} = \frac{m'}{n'}$ if $mn' = m'n$.

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 $2 \mid m^2 \Rightarrow 2 \mid m \Rightarrow m = 2m'$ since 2 prime. So $2n^2 = 2^2 m'^2 \Rightarrow n^2 = 2m'^2 \Rightarrow 2 \mid n^2 \Rightarrow 2 \mid n$. 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 $p \mid m^2 \Rightarrow p \mid m \Rightarrow m = pm'$ since p prime. So $pn^2 = p^2 m'^2 \Rightarrow n^2 = pm'^2 \Rightarrow p \mid n^2 \Rightarrow p \mid n$. 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

$6 \mid m^2 \Leftrightarrow \left\{ \begin{matrix} 2 \mid m^2 \Rightarrow 2 \mid m \\ 3 \mid m^2 \Rightarrow 3 \mid m \end{matrix} \right\} \Leftrightarrow 6 \mid m \Rightarrow m = 2m'$ since 2, 3 prime. So

$6n^2 = 6^2 m'^2 \Rightarrow n^2 = 6m'^2 \Rightarrow 6 \mid n^2 \Rightarrow 6 \mid n$. Contradiction!

Example
Prove $\sqrt[3]{2}$ 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 $2 \mid m^3 \Rightarrow 2 \mid m \Rightarrow m = 2m'$ since 2 prime. So $2n^3 = 2^3 m'^3 \Rightarrow n^2 = 4m'^2 \Rightarrow 2 \mid n^2 \Rightarrow 4 \mid n^2 \Rightarrow 2 \mid n$. Contradiction!

Example

Prove $\sqrt{3}+\sqrt{7}$ is irrational.

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

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

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

Definition

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

Note

Recall from Fundamental Theorem of Arithmetic that for any $n\in\mathbf{N}, n>1$ has a unique (except for order) factorization into primes, i.e. $n=p_1^{\alpha_1}\cdots p_l^{\alpha_l}, \alpha_i\in\mathbf{N}$. So $n=k^2=\left(p_1^{\alpha_1}\cdots p_l^{\alpha_l}\right)^2=p_1^{2\alpha_1}\cdots p_l^{2\alpha_l}$.

Theorem

Let $N\in\mathbf{N}$. 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 $N=p_1^{2\alpha_1}\cdots p_k^{2\alpha_k}, \alpha_i\ge 0\Rightarrow$ $\sqrt{N}=p_1^{\alpha_1}\cdots p_k^{\alpha_k}\in\mathbf{Z}\in\mathbf{Q}$. Contradiction!
- Assume N not perfect square. Suppose $\sqrt{N}$ is rational. Then $\sqrt{N}=\dfrac{m}{n}\Rightarrow$

  $N=\dfrac{m^2}{n^2}=\dfrac{\left(p_1^{\alpha_1}\cdots p_1^{\alpha_k}\right)^2}{\left(p_1^{\beta_1}\cdots p_1^{\beta_k}\right)^2}=,\alpha,\beta\ge 0\Rightarrow N=p_1^{2(\alpha_1-\beta_1)}\cdots p_1^{2(\alpha_k-\beta_k)},\alpha-\beta\ge 0$. This means N is a perfect square. Contradiction!

Example

Prove $\sqrt[3]{4}$ is irrational.

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

$$\begin{cases} n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}\Rightarrow n^3=\left(p_1^{\alpha_1}\cdots p_k^{\alpha_k}\right)^3=p_1^{3\alpha_1}\cdots p_k^{3\alpha_k} \\ m=p_1^{\beta_1}\cdots p_k^{\beta_k}\Rightarrow m^3\left(p_1^{\beta_1}\cdots p_k^{\beta_k}\right)^3=p_1^{3\beta_1}\cdots p_k^{3\beta_k}\end{cases},\alpha,\beta\ge 0\text{, so } 4p_1^{3\alpha_1}\cdots p_k^{3\alpha_k}=p_1^{3\beta_1}\cdots p_k^{3\beta_k}$$

$\Rightarrow 2^{(2+3\alpha)}q=2^{3\beta}q'$. Contradiction because $2^{(2+3\alpha)}q=2^{3\beta}q'\Rightarrow 2+3\alpha=3\beta$, but $3\nmid 2+3\alpha=3\beta$!

Theorem

Let $k,L\in\mathbf{N}$. Then $\sqrt[k]{L}$ is rational iff $\sqrt[k]{L}$ is an integer.

Proof:

- (⇐) is trivial.
- (⇒): $\sqrt[k]{L} = \frac{m}{n} = \frac{p_1^{\alpha_1} \cdots p_n^{\alpha_n}}{p_1^{\beta_1} \cdots p_n^{\beta_n}} = p_1^{(\alpha_1 - \beta_1)} \cdots p_n^{(\alpha_n - \beta_n)} \Rightarrow L = p_1^{k(\alpha_1 - \beta_1)} \cdots p_n^{k(\alpha_n - \beta_n)}$. Now, $L \in \mathbf{N} \Rightarrow k(\alpha_i - \beta_i) \geq 0 \Rightarrow \alpha_i - \beta_i \geq 0 \Rightarrow \sqrt[k]{L} \in \mathbf{N}$.

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
π, e are not algebraic (transcendental).

Real Numbers

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

Definition
For a subset $S \subseteq \mathbf{R}$, $c \in \mathbf{R}$ 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 $S \subseteq \mathbf{R}$ 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) $S = \{x \in \mathbf{R} \mid x < 10\}$. Upper bounds $c = 10, 11, \ldots$; least upper bound is 10.
3) $S = \{x \in \mathbf{R} \mid x^2 < 2\}$. Upper bounds $c = 1.5, 2, \ldots$; least upper bound is $\sqrt{2}$.
4) $S = [3,7] \cup [-1,2] \cup \{111\}$. Upper bounds $c = 111, 112, \ldots$; least upper bound is 111.
5) $S = \mathbf{N}$ has no upper bounds.

The Completeness Property

The basic property that distinguishes **R** from **Q** is that every non-empty subset of **R** which as an upper bound has a least upper bound.

Theorem: Intermediate Value Theorem

Let $f : [a,b] \to \mathbf{R}$ 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 $x = x_0 + \dfrac{\delta}{2}$. 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 $x \in \mathbf{R}$, 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: $\left.\begin{array}{r} a < b \Rightarrow (b-a) \in P \\ k \in P \end{array}\right\} \Rightarrow k(b-a) = (kb - ka) \in P \Rightarrow ka < kb$.
3) $a < b, -k \in P \Rightarrow ka > kb$. Proof: $\left.\begin{array}{r} a < b \Rightarrow (b-a) \in P \\ -k \in P \end{array}\right\} \Rightarrow -k(b-a) = (ka - kb) \in P \Rightarrow ka > kb$.

Example

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

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

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

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

Definition: Real Numbers

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

1) $X \neq \phi$ and $X \neq \mathbf{Q}$.
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 $X = \{q \in \mathbf{Q} \mid q < 3\}$ is a real number.

4) $X \neq \phi$ because $1 \in X$. $X \neq \mathbf{Q}$ because $4 \notin X$.
5) Let $\left.\begin{array}{r} q_1 \in X \Rightarrow q_1 < 3 \\ q_2 < q_1 \end{array}\right\} \Rightarrow q_2 < q_1 < 3$. 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 $\sqrt{2} = \{q \in \mathbf{Q} \mid q^2 < 2\} \cup \{q \in \mathbf{Q} \mid q < 0\}$ is a real number.

1) $\sqrt{2} \neq \phi$ because $0 \in \sqrt{2}$. $\sqrt{2} \neq \mathbf{Q}$ 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 $q'^2 = \left(q + \frac{1}{n}\right)^2 = q^2 + \frac{2q}{n} + \frac{1}{n^2} < q^2 + \frac{2q}{n}$, so $q'^2 < q^2 + \frac{2q}{n} < 2 \Rightarrow n > \frac{2q}{2 - q^2}$. 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

R-world	**Q**-world
3	$3 := \{q \in \mathbf{Q} \mid q < 3\}$
$\frac{m}{n}$	$\frac{m}{n} := \left\{q \in \mathbf{Q} \mid q < \frac{m}{n}\right\}$
$\sqrt{2}$	$\sqrt{2} := \{q \in \mathbf{Q} \mid q < 0, q^2 < 2\}$
$\sqrt[3]{2}$	$\sqrt[3]{2} := \{q \in \mathbf{Q} \mid q^3 < 2\}$

Definition: Addition
Let X, Y be real numbers. $X+Y=\{p+q \mid p\in X, q\in Y\}$.

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

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

Definition
A real number X is "positive" if $0\subset X$.

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

Definition: Negative of a Number
For a real number X, define $-X := \{-q\in \mathbf{Q} \mid q\notin X\} \setminus \text{largest element (if it exists)}$.

Example
If $X=\{q\in \mathbf{Q} \mid q<2\}$, then $-X=\{-q\in \mathbf{Q} \mid q\ge 2\}=\{q\in \mathbf{Q} \mid q<-2\}$.

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

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

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

Definition
$1 := \{q\in \mathbf{Q} \mid q<1\}$.

Theorem
$1 \cdot X = X, \forall X \in \mathbf{R}$.

Definition
If $X > 0$, define $\frac{1}{X} = \left\{ q \in \mathbf{Q} \mid q \le 0 \text{, or } q = \frac{1}{q'}, q' \in \mathbf{Q} \setminus X \right\} \setminus \{\text{largest element}\}$.

If $X < 0$, define $\frac{1}{X} = -\frac{1}{|X|}$.

Completeness Property of the Reals
Every subset of **R** (other than ϕ) which has an upper bound has a least upper bound.

Complex Numbers

Examples
1) $3x + 2$ has no solution in **Z**, but there exists a solution in **Q**.
2) $x^2 - 2 = 0$ has no solution in **Q**, but there exists a solution in **R**.
3) $x^2 + 1 = 0$ has no solution in **R**, but there exists a solution in **C**.

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

Notation
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 $\mathbf{R} \subset \mathbf{C}$? $a \in \mathbf{R}$ is $a + i0 \in \mathbf{C}$.
- For $b \in \mathbf{R}$, $0 + ib \in \mathbf{C}$ is (pure) imaginary.

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

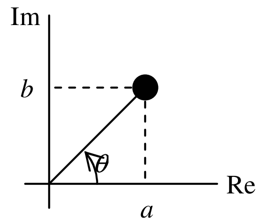
Examples

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

2) $(a+ib)\left(\overline{a+ib}\right)=(a+ib)(a-ib)=\left(a^2+b^2\right)+i(ab-ab)=a^2+b^2=|a+ib|^2$.

3) $\dfrac{1}{a+ib}=\dfrac{1}{a+ib}\dfrac{a-ib}{a-ib}=\dfrac{a-ib}{a^2+b^2}=\dfrac{a}{a^2+b^2}+i\dfrac{-b}{a^2+b^2}=\dfrac{\overline{a+ib}}{a^2+b^2}$, $a+ib\neq 0$.

Notation



$\theta :=$ argument of $a+ib$.

$$r\cos\theta+ir\sin\theta \Leftrightarrow a+ib \Leftrightarrow \begin{cases} r=\sqrt{a^2+b^2}, r>0 \\ \theta=\arctan\left(\frac{b}{a}\right)\end{cases}.$$

DeMoivre Formula

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

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

$z_0=1\left[\cos\left(\dfrac{\pi}{3}\right)+i\sin\left(\dfrac{\pi}{3}\right)\right]=\dfrac{1}{2}+i\dfrac{\sqrt{3}}{2}$, $z_1=1[\cos(\pi)+i\sin(\pi)]=-1$,

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

Triangle Inequality

$|z_1+z_2|\leq|z_1|+|z_2|, \forall z_1,z_2\in\mathbf{C}$.

FUNDAMENTAL THEOREM OF ALGEBRA

Definition: Closed Curve

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

Definition: Winding Number

If ϕ 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 2π.

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.
$p(z)=a_n z^n+\cdots+a_1 z+a_0$, where $a_i\in\mathbf{C}$, $a_n\neq 0$ (so n 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 $r\in\mathbf{C}$, i.e. $p(r)=0$.

1) $z-r$ divides this polynomial. So $p(z)=(z-r)q(z), \deg(q)<\deg(p)$.
2) $p(z)=a(z-r_1)\cdots(z-r_n), a, r_1,\ldots,r_n\in\mathbf{C}$, or $p(z)=a(z-r_1)^{k_1}\cdots(z-r_l)^{k_l}$.

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 $n\in\mathbf{N}$ 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

$\{\text{blue}, \text{green}, \text{red}\}$ 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

$\mathbf{N}=\{1,2,3,\ldots\}$, $\mathbf{Q}=\text{rationals}$, $\mathbf{R}=\text{reals}$ are infinite sets.

Definition
Two sets *S* and *T* have the same cardinality if there exists a bijection (one-to-one and onto) $f : S \to T$, 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 $f : S \to T; s_i \to t_i$).

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

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

NOTIONS OF CARDINALITY

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

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

Theorem
The set $[0,1] := \{x \in \mathbf{R} \mid 0 \le x \le 1\}$ 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:

$$\begin{aligned} s_1 &= 0.a_{11}a_{12}a_{13}\ldots \\ s_2 &= 0.a_{21}a_{22}a_{23}\ldots \\ s_3 &= 0.a_{31}a_{32}a_{33}\ldots \\ &\vdots \end{aligned}.$$

Make a number $x = 0.x_1x_2x_3$ as follows: $x_i = \begin{cases} 5, a_{ii} \ne 5 \\ 6, a_{ii} = 5 \end{cases}$. This is a real number between 0 and 1.
Now, *x* is not in the list because: $x \ne s_1$ since $x_1 \ne a_{11}$, $x \ne s_2$ since $x_2 \ne a_{22}$, and so on.

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

Definition
$|S| < |T|$ if $|S| \le |T|$ and $|S| \ne |T|$.

Claim
$|\mathbf{N}| < |[0,1]|$.
Proof:
We showed $|\mathbf{N}| \ne |[0,1]|$, so it is enough to show $|\mathbf{N}| \le |[0,1]|$. Let $S = \mathbf{N}$ and $T = [0,1]$. Let $T_0 = \left\{1, \frac{1}{2}, \frac{1}{3}, \cdots\right\}$.
$|T_0| = |S|$ because $f : S \to T_0, f(n) = \frac{1}{n}$.

Theorem: Schroeder-Bernstein-Cantor Theorem
If $|S| \le |T|$ and $|S| \ge |T|$, 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 $\left|\bigcup_{i=1}^{\infty} S_i\right| = c$.
Proof: $S_1 \subset \bigcup_{i=1}^{\infty} S_i \Rightarrow c = |S_1| \le \left|\bigcup_{i=1}^{\infty} S_i\right|$. Note that $\bigcup_{i=1}^{\infty} S_i = \underbrace{S_1}_{S_1'} \cup \underbrace{(S_2 \setminus S_1)}_{S_2'} \cup \underbrace{(S_3 \setminus (S_1 \cup S_2))}_{S_3'} \cup \cdots$ is the union of disjoint sets. Now, take $f : \bigcup_{i=1}^{\infty} S_i \xrightarrow{\text{1-1}} \mathbf{R}$, where $S_1' \xrightarrow{\text{1-1}} (0,1)$ (since $|S_1| = c$), $S_2' \xrightarrow{\text{1-1}} (1,2)$ (since $|S_2| = c$), etc; then $\left|\bigcup_{i=1}^{\infty} S_i\right| \le |\mathbf{R}| = c$. So, by S-C-B, $\left|\bigcup_{i=1}^{\infty} S_i\right| = c$.

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

Example

Let *S* be the set of all sets of real numbers (ex: $S=\{\{0\},\{1\},\ldots,\{1,2\}\ldots[0,1],[34]\cup[110,11^{11}],\ldots\}$). Then $|S|>c$.

Proof:

Want: $c<|S|$. Take $f:\mathbf{R}\xrightarrow{\text{1-1}}S;x\mapsto\{x\}$, so $|\mathbf{R}|=c<|S|$.

Want: $c\neq S$. Suppose $c=|\mathbf{R}|=|S|$, so there exists $g:\mathbf{R}\xrightarrow{\text{bijection}}S$. Note that in particular *g* is onto and $g(x)$ is a set of real numbers. Let $T:=\{x\in\mathbf{R}\mid x\notin g(x)\}\subset S$. Claim: There is no $y\in\mathbf{R}$ such that $g(y)=T$. Suppose there is $y\in\mathbf{R}$ 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 **R**), then let *S* be the set of all subsets of S_0. We can show that $|S_0|<|S|$.

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

Theorem

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

Proof: Let $f:\mathbf{N}\to\{0,1\}$ be a characteristic function. For a subset $S\subseteq\mathbf{N}$ 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 **N**.

Define $\varphi:T\to[0,1], f\mapsto 0.f(1)f(2)\cdots$. φ 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 $|T|\le[0,1]=c$.

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 $[0,1]=c\le|T|$.

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

ENUMERATION PRINCIPLE

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

Example

Prove **Q** is countable.

$S=\mathbf{Q}^+\cup\{+,-\}$ is countable. So $\mathbf{Q}\setminus\{0\}$ is countable, so **Q** is countable.

Example

Prove $\mathbf{Q}^n = \{(q_1, \ldots, q_n) \mid q_i \in \mathbf{Q}\}$ is countable.

Note: $\mathbf{Q}^n \subseteq S$ a finite sequence of elements of **Q**, so $\left|\mathbf{Q}^n\right| \le |S| = \aleph_0$.

Now let S^i be the set of sequences of length *i* of elements of a countable set. Since $|S| = \aleph_0 \Rightarrow |S \times S| = \left|S^2\right| = \aleph_0 \Rightarrow \cdots \Rightarrow |S \times \cdots \times S| = \left|S^n\right| = \aleph_0$, so $\bigcup_{i=1}^{\infty} S^i$ 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 $|S| \ge \aleph_0$, 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 $S = (S \setminus S_0) \dot{\cup} S_0 = (S \setminus S_0 \dot{\cup} S_1) \dot{\cup} S_0 \dot{\cup} S_1$. Let $f : S_0 \cup S_1 \to S_1$ be any 1-1 function.

Define $\varphi : S \to S \setminus S_0, \varphi(s) = \begin{cases} s, s \in S \setminus (S_0 \cup S_1) \\ f(s), s \in S_0 \cup S_1 \end{cases}$. φ 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. $S = (S \setminus S_0) \dot{\cup} S_0$.
Let $T = S \setminus \{s_1\}$ a proper subset of *S*.
Let $f : S \to T, f(s) = \begin{cases} s, s \in S \setminus S_0 \\ s_{k+1}, s = s_k \in S_0, k = 1, 2, \ldots \end{cases}$ 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 coefficient that has it as a root.
Notation: $\mathbf{A} := \{\text{algebraic numbers}\}$.

Theorem
A is countable.

Proof: Let $\begin{cases} \mathbf{A}_1 := \{x \in \mathbf{R} \mid p(x) = 0,\ p \text{ is polynomial of degree 1 with integer coefficients}\} \\ \mathbf{A}_2 := \{x \in \mathbf{R} \mid p(x) = 0,\ p \text{ is polynomial of degree 2 with integer coefficients}\} \\ \quad \vdots \end{cases}$. Note that

$\begin{cases} \mathbf{A}_1 \leftrightarrow \mathbf{Z} \times \mathbf{Z} \\ \mathbf{A}_2 \leftrightarrow \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \\ \quad \vdots \end{cases}$, so each $\mathbf{A}_k$ is countable. Thus $\mathbf{A} = \bigcup_{k \geq 1} \mathbf{A}_k$ is countable.

Corollary

$\left|\{\text{non-algebraic numbers}\}\right| = c$.

ARITHMETIC WITH CARDINAL NUMBERS

Cardinal numbers: $\{1, 2, \ldots, \aleph_0, c, 2^c, \ldots\}$.

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

Definition: Multiplication

$c_1 \times c_2 := |S_1 \times S_2|$.

Example

1) $\aleph_0 \times \aleph_0 = ?$. Let $\aleph_0 = |\mathbf{N}|$, then $\aleph_0 \times \aleph_0 = |\mathbf{N} \times \mathbf{N}| = \aleph_0$.
2) $\aleph_0 \times c = ?$. Let $\aleph_0 = |\mathbf{N}|$ and $c = |\mathbf{R}|$. Then $\left.\begin{matrix} \aleph_0 \times c = |\mathbf{N} \times \mathbf{R}| \leq |\mathbf{R} \times \mathbf{R}| = c \\ \aleph_0 \times c = |\mathbf{N} \times \mathbf{R}| \geq |1 \times \mathbf{R}| = c \end{matrix}\right\} \Rightarrow \aleph_0 \times c = c$.

Definition: Exponential

$X^A := \left|\{f \mid f : A \to X\}\right|$.

Example

$2^{\aleph_0} = ?$. Let $2 = \left|\{0,1\}\right|$ and $\aleph_0 = |\mathbf{N}|$, then $2^{\aleph_0} = \left|\{f \mid f : \mathbf{N} \to \{0,1\}\}\right| = |P(\mathbf{N})| = c$.

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 **R** which contains 0 and 1, and which is closed under the four basic arithmetic operations is called a number field.

Examples

1) **Q**, **R** are number fields.
2) $\mathbf{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ is a number field. It is closed under multiplication since $(a + b\sqrt{2})(a' + b'\sqrt{2}) = \underbrace{(aa' + bb')}_{\in \mathbf{Q}} + \underbrace{(ab' + a'b)}_{\in \mathbf{Q}}\sqrt{2}$. It is closed under multiplicative inverse since

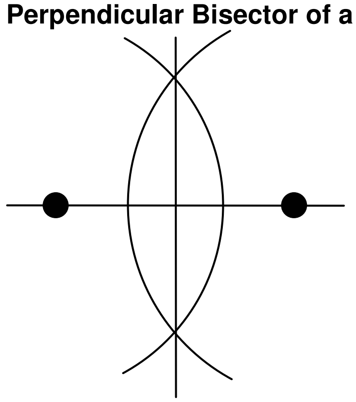
$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 + 2b^2} = \underbrace{\left(\frac{a}{a^2 + 2b^2}\right)}_{\in \mathbf{Q}} - \underbrace{\left(\frac{b}{a^2 + 2b^2}\right)}_{\in \mathbf{Q}}\sqrt{2}.$$

Remark

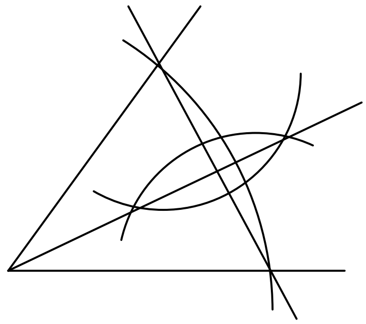
- **Q** is the smallest number field.
- **R** is the largest number field.

CONSTRUCTION YOU CAN MAKE WITH STRAIGHTEDGE AND COMPASS

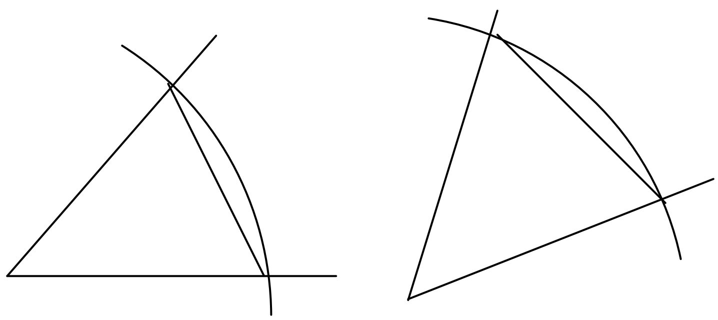
Perpendicular Bisector of a Line Segment



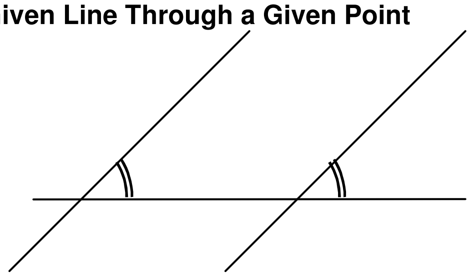
Bisect an Angle



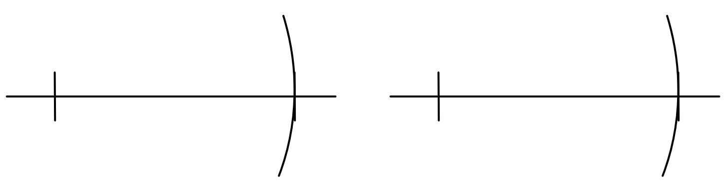
Copy Angles



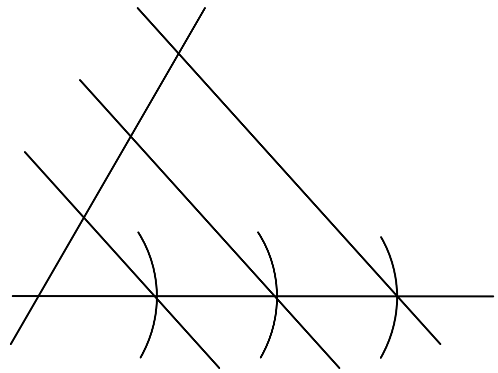
Draw a Parallel Line To a Given Line Through a Given Point



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

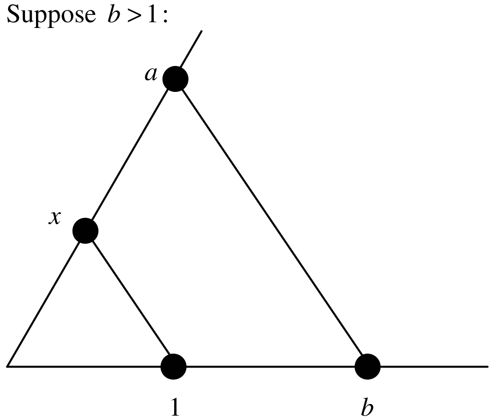
The set of numbers that can be marked on a line using straightedge and compass is called constructible numbers.

Notation: $C := \text{set of constructible numbers}$.

Note

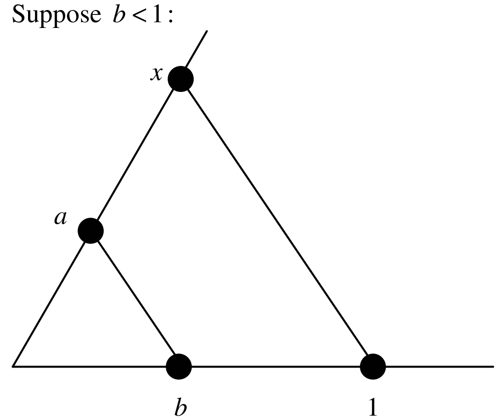
1) If $a, b \in C$, then $a + b \in C$.
2) If $a \in C$, then $-a \in C$.
3) If $a, b \in C$ and $a, b > 0$, then $\frac{a}{b} \in C$. Note in particular, $\frac{1}{a} \in C$

Suppose $b > 1$:



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

Suppose $b < 1$:



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

4) If $a, b \in C$ and $a, b > 0$, then $ab \in C$ (since $ab = \frac{a}{\frac{1}{b}} \in C$).

These prove the following theorem.

Theorem
C is closed under the four basic arithmetic operations.

Corollary
C is a number field.

Note
Recall that $\mathbf{Q}\left(\sqrt{2}\right)$ 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.

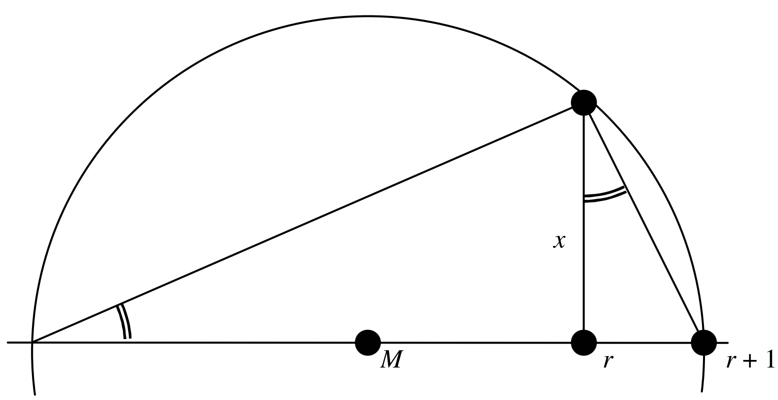
Theorem
$F\left(\sqrt{r}\right)$ is a number field.

Example
$\underbrace{\mathbf{Q}}_{F_0} \subseteq \underbrace{\mathbf{Q}\left(\sqrt{2}\right)}_{F_1} \subseteq \underbrace{\mathbf{Q}\left(\sqrt{2}\right)\left(\sqrt{3}\right)}_{F_2} \subseteq \underbrace{\mathbf{Q}\left(\sqrt{2}\right)\left(\sqrt{3}\right)\left(\sqrt{5}\right)}_{F_3} \subseteq \cdots$.

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: $F_0 \subseteq \underbrace{F_0\left(\sqrt{r_1}\right)}_{F_1} \subseteq \underbrace{F_1\left(\sqrt{r_2}\right)}_{F_2} \subseteq \underbrace{F_2\left(\sqrt{r_3}\right)}_{F_3} \subseteq \cdots \subseteq \underbrace{F_{n-1}\left(\sqrt{r_n}\right)}_{F_n}$.

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

Proof:



$\frac{1}{x} = \frac{x}{r} \Rightarrow r = x^2 \Rightarrow x = \sqrt{r}$.

Corollary

If $\mathbf{Q} \subset F_1 \subset F_2 \subset \cdots \subset F_k$ is any tower, then $F_j \subset C$.

Surds

Definition: Surd

A surd is a number that is in some F_k where F_k is in some tower starting at **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 **Q** such that $a,b,c,d \in F$.

Now the equation of the line joining (a,b) and (c,d) is $\frac{y-b}{x-a} = \frac{d-b}{c-a}$ or $y = \underbrace{\left(\frac{d-b}{c-a}\right)}_{\alpha} x + \underbrace{\left(b - a\frac{d-b}{c-a}\right)}_{\beta}$. 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 $(x-a)^2 + (y-b)^2 = r^2 \Leftrightarrow x^2 + y^2 + \underbrace{(-2a)}_{\alpha} x + \underbrace{(-2b)}_{\beta} y + \underbrace{\left(a^2 + b^2 - r^2\right)}_{\gamma} = 0$. Since there is some extension *F* such that $a,b,r \in F$, so $\alpha, \beta, \gamma \in F$.

Now, at the intersection $\begin{cases} y^2 + x^2 + \alpha x + \beta y + \gamma = 0 \\ y = \alpha' x + \beta' \end{cases} \Rightarrow (\alpha' x + \beta')^2 + x^2 + \alpha x + (\alpha' x + \beta') y + \gamma = 0 \Rightarrow$

$\underbrace{(\alpha'^2 + 1)}_{A} x^2 + \underbrace{(2\alpha'\beta' + \alpha + \alpha'\beta)}_{B} x + \underbrace{(\beta'^2 + \beta\beta' + \gamma)}_{C} = 0$, so

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

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 θ (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, $\cos(60°) = \frac{1}{2} \Leftrightarrow 4\cos^3(20°) - 3\cos(20°) = \frac{1}{2} \Leftrightarrow$

$8\cos^3(20°) - 6\cos(20°) - 1 = 0 \Leftrightarrow (2\cos(20°))^3 - 3(2\cos(20°)) - 1 = 0$, 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.

<u>Proof</u>: A rational root $r = \frac{a}{b}$ must be such that $a \mid 1$ and $b \mid 1$, so $r = \pm 1$. But ± 1 are not roots!

Theorem

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

<u>Proof</u>: 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 $(x - r_1)(x - r_2)(x - r_3) = x^3 + \underbrace{(r_1 + r_2 + r_3)}_{\in \mathbf{Q}} x^2 + \cdots$, i.e. the sum of all three roots of a cubic is a rational number.

4) Let $a+b\sqrt{r} \in F(\sqrt{r}) := \{a+b\sqrt{r} \mid a,b,r \in F, \sqrt{r} \notin F\}$. Define the conjugate of $a+b\sqrt{r}$ as $\overline{a+b\sqrt{r}} = a-b\sqrt{r}$.
5) $\overline{(a+b\sqrt{r})+(c+d\sqrt{r})} = \overline{a+b\sqrt{r}} + \overline{c+d\sqrt{r}}$.
6) $\overline{(a+b\sqrt{r})\cdot(c+d\sqrt{r})} = \left(\overline{a+b\sqrt{r}}\right)\cdot\left(\overline{c+d\sqrt{r}}\right)$.
7) $\overline{(a+b\sqrt{r})^k} = \left(\overline{a+b\sqrt{r}}\right)^k$.

Let x_0 be the constructible root, so x_0 is a surd. So there exists some tower $\mathbf{Q} \subset F_0 \subset \cdots \subset F_k, F_{i+1} = F_i\left(\sqrt{r_i}\right)$ such that $x_0 \in F_k$. So $x_0 = a_0 + b_0\sqrt{r_{k-1}}, a_0, b_0, r_{k-1} \in F_{k-1}$. Assume we choose a shortest tower containing x_0 (i.e. $b_0 \neq 0$; or if $x_0 \in \mathbf{Q}$ then we're done).
By proposition, $\overline{x_0} = a_0 - b_0\sqrt{r_{k-1}}$ is also a root. Let *s* be the third root. Now $x_0 + \overline{x_0} + s = q \in \mathbf{Q} \Rightarrow 2a_0 + s = q \Rightarrow s = \underbrace{q}_{\substack{\in \mathbf{Q} \\ \in F_{k-1}}} - \underbrace{2a_0}_{\in F_{k-1}} \in F_{k-1}$. By repeating this argument, we can conclude that $s \in \mathbf{Q}$.

Proposition

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

<u>Proof</u>: Notice $\overline{p(x)} = \overline{a_k x^k + \cdots + a_0} = \overline{a_k x^k} + \cdots + \overline{a_0} = \overline{a_k}\left(\overline{x^k}\right) + \cdots + \overline{a_0} = a_k \overline{x}^k + \cdots + a_0$. So $p(a+b\sqrt{r}) = 0 \Rightarrow \overline{p(a+b\sqrt{r})} = \overline{0} = 0 \Rightarrow p\left(\overline{a+b\sqrt{r}}\right) = 0$.

Lemma

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

<u>Proof</u>: $\underbrace{\alpha_k}_{\in F(\sqrt{r})} x_o^k + \cdots + \alpha_0 = 0, \alpha_i \in F(\sqrt{r}), \alpha_i = a_i + b_i\sqrt{r}, a_i b_i, r \in F \Rightarrow$
$(a_k + b_k\sqrt{r})x_o^k + \cdots + (a_0 + b_0\sqrt{r}) = 0 \Rightarrow (a_k + b_k\sqrt{r})x_o^k + \cdots + (a_0 + b_0\sqrt{r}) = 0 \Rightarrow$
$a_k x_o^k + \cdots + a_0 = -\sqrt{r}(b_k x_o^k + \cdots + b_0) \Rightarrow (a_k x_o^k + \cdots + a_0)^2 - r(b_k x_o^k + \cdots + b_0)^2 = 0 \Rightarrow$
$\underbrace{(a_k^2 - rb_k^2)}_{\in F} x_0^{2k} + \cdots + \underbrace{(a_0^2 - rb_0^2)}_{\in F} = 0$.

Theorem

Every constructible number is algebraic.
<u>Proof</u>: Suppose x_0 is constructible, so $x_0 \in F_k$. Now $p(x) = x - x_0$ has coefficients in $F_k = F_{k-1}(\sqrt{r})$. Now apply the lemma until the coefficients are in $\mathbf{Q}$, and multiply it by the common denominator.

Example

A 50° angle is not constructible.

Note that a 90° is constructible. Suppose 50° is constructible, then 40° is constructible. By bisecting, 20° 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, $\left(x^3-5\right)' = 3x^2 > 0, \forall x \in \mathbf{R}$, there is one real root. But $\sqrt[3]{5}$ is real, but not rational. Contradiction.

Example

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

Note that $\mathbf{Q} \subset \mathbf{Q}\left(\sqrt{5}\right) \subset \underbrace{\mathbf{Q}\left(\sqrt{5}\right)\left(\sqrt{3}\right)}_{\text{contains } \sqrt{5}+\sqrt{3}} \subset \mathbf{Q}\left(\sqrt{5}\right)\left(\sqrt{3}\right)\left(\sqrt{\sqrt{5}+\sqrt{3}}\right)$.

Corollary

Cannot trisect 60°.

Proof: Assume can trisect 60°. Since 60° is constructible, this implies 20° is constructible. Contradiction.

REGULAR POLYGONS

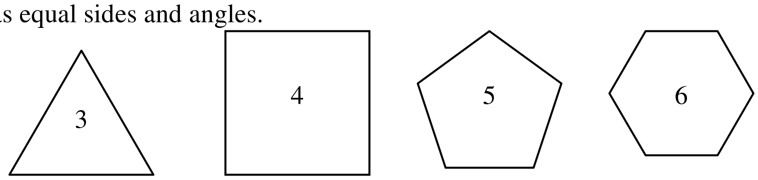
Example: Duplication of the Cube

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 $\frac{m}{n}$ s 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

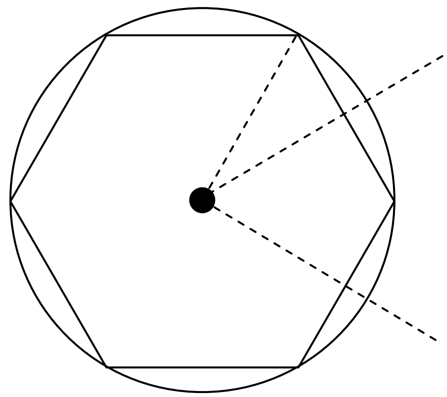
Regular polygon has equal sides and angles.



Fact

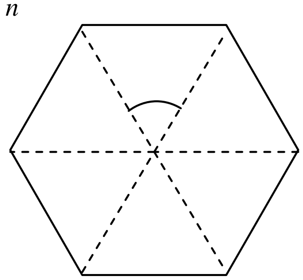
Every regular polygon can be inscribed in a circle.

Proof: Find the centre and radius of the circle as follows:



Definition: Central Angle

The central angle of a regular n-gon is $\dfrac{360°}{n}$.



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

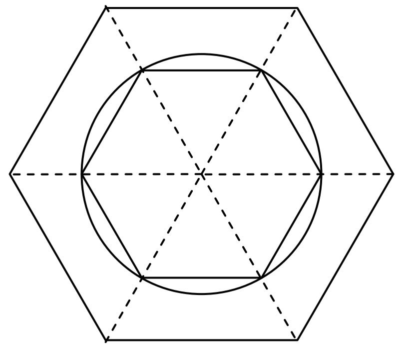
Corollary
A regular 18-gon is not constructible.

Proof: The central angle is $\dfrac{360°}{18} = 20°$.

Corollary
A regular 9-gon is not constructible.

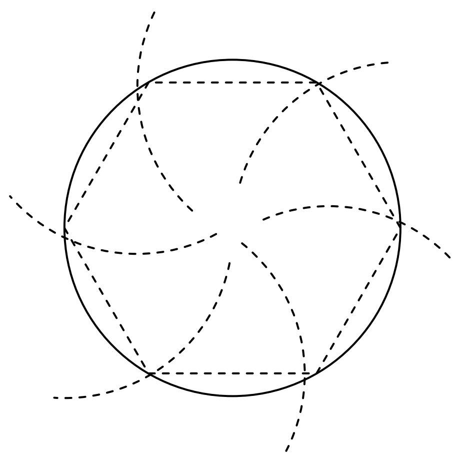
Corollary
Regular 9, 18, 36, 72,…-gons are not constructible.

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.



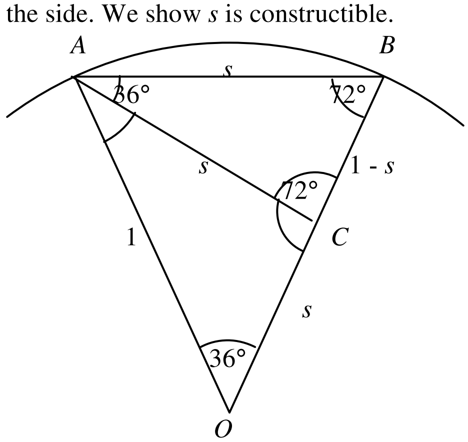
Lemma
A regular n-gon is constructible if and only if the length of an edge of the regular n-gon inscribed in a circul of radius 1 is constructible.

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.

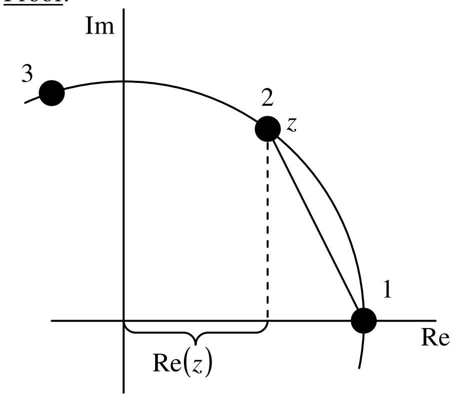


Since $OAB \sim ABC \Rightarrow \frac{s}{1} = \frac{1-s}{s}$, so $s^2 = 1 - s \Rightarrow s^2 + s - 1 = 0 \Rightarrow s = \frac{-1 \pm \sqrt{1+4}}{2}$. But since $s > 0$, so $s = \frac{\sqrt{5}-1}{2} \in \mathbf{Q}\left(\sqrt{5}\right)$ which is constructible.

Corollary
A regular 5, 10, 20,…-gon is constructible.

Corollary
A 7-gon is not constructible.

Proof:



Let $z \in \mathbf{C}$. We know $z^7 = 1$, $|z| = 1$, $z \neq 1$.

$z^7 - 1 = 0$

$(z-1)(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) = 0$

$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$

$z^3 + z^2 + z + 1 + \frac{1}{z} + \frac{1}{z^2} + \frac{1}{z^3} = 0$

$\left(z + \frac{1}{z}\right)^3 + \left(z + \frac{1}{z}\right)^2 - 2\left(z + \frac{1}{z}\right) + 1 = 0$

Now, let $x_0 = z + \frac{1}{z}$. Then $x_0 = 2\operatorname{Re}(z)$ (because $|z| = 1 \Rightarrow z\bar{z} = 1 \Rightarrow \bar{z} = \frac{1}{z}$, so $x_0 = z + \bar{z} = 2\operatorname{Re}(z)$).
So $x_0 = 2\operatorname{Re}(z)$ 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: θ constructible $\Leftrightarrow$ $\cos\theta$ constructible $\Rightarrow$ $\cos\theta$ algebraic.

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

Note
Given an angle θ (don't know if θ is constructible or not), can θ be trisected?

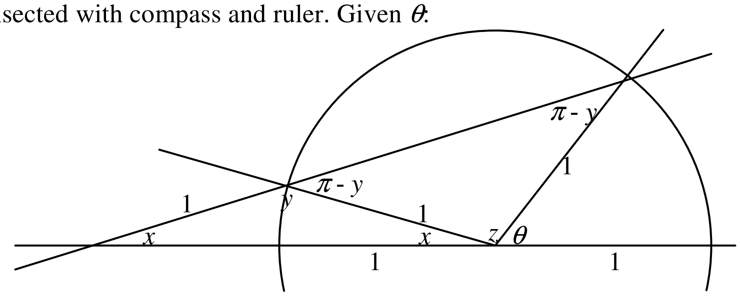
Theorem
If $\cos\theta$ is transcendental, then θ is not trisectible.

Proof:
Given angle θ, 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 $F_0 = \mathbf{Q}(c)$ is the smallest number field containing $\mathbf{Q}$ and c.
Using straightedge and compass, can construct towers starting with F_0: $F_0 \subset F_0\left(\sqrt{r_o}\right) \subset \cdots$.
Assume $\frac{\theta}{3}$ is constructible from θ. Then $\frac{\theta}{3}$ is in such a tower. So $4x^3 - 3x = c$ has a solution in such a tower ($F_0 \subset F_0\left(\sqrt{r_o}\right) \subset \cdots$), and thus $4x^3 - 3x = c$ has a solution in $F_0 = \mathbf{Q}(c)$.
We need to show $4x^3 - 3x = c$ has no solution in $F_0 = \mathbf{Q}(c)$. Suppose there is a solution in $F_0 = \mathbf{Q}(c)$, i.e. $4\left(\frac{p(c)}{q(c)}\right)^3 - 3\left(\frac{p(c)}{q(c)}\right) = c \Rightarrow 4(p(c))^3 - 3(p(c))(q(c))^2 - c(q(c))^3 = 0$, 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 θ:



Claim: $x = \frac{\theta}{3}$.

Proof: $\left.\begin{array}{l} y = \pi - 2x \Rightarrow \pi - y = 2x \\ \pi = 2(\pi - y) + z \end{array}\right\} \Rightarrow \pi = 4x + z \Rightarrow z = \pi - 4x$. Also, $z = \pi - x - \theta$, so $4x = x + \theta \Rightarrow x = \frac{\theta}{3}$.

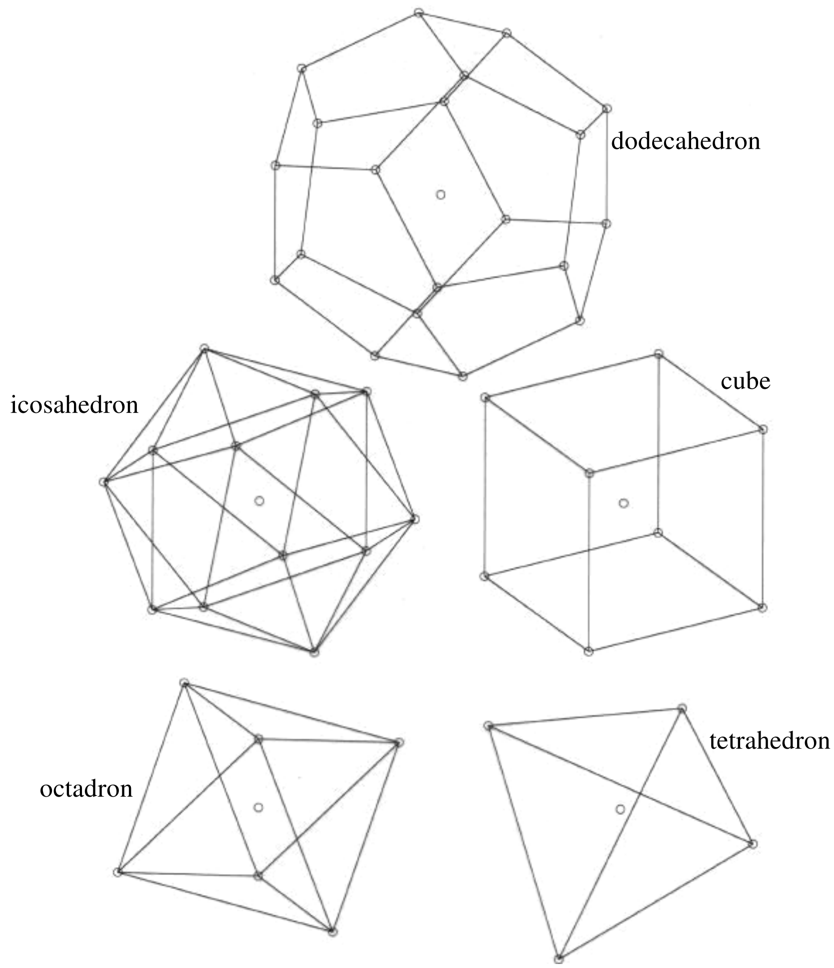
Regular Polyhedrons

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 same number of sides as each other, and all of whose vertices lie on the same number of faces.

Examples



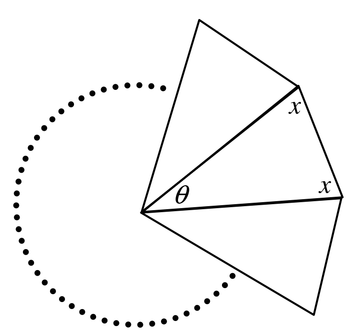
Theorem

There are only 5 regular polyhedrons.

<u>Proof</u>: 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,

$\begin{cases} n\theta = 2\pi \\ 2x + \theta = \pi \end{cases}$. So $2x = \pi - \theta = \dfrac{n\theta}{2} - \theta = \theta\left(\dfrac{n-2}{2}\right) = \dfrac{(n-2)\pi}{n}$.



Now, k faces meet at a vertex means $k(2x) < 2\pi \Rightarrow \frac{k(n-2)}{n} < 2 \Rightarrow k - \frac{2k}{n} < 2$. Since $n \geq 3 \Rightarrow \frac{1}{n} \leq \frac{1}{3} \Rightarrow -\frac{1}{n} \geq -\frac{1}{3}$, so $k - \frac{2k}{n} \geq k - \frac{2k}{3} = \frac{k}{3}$. Thus $\frac{k}{3} < 2 \Rightarrow k < 6 \Rightarrow k = 3,4,5$.

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.