Definition of Monoid

A monoid is a triple $(A, \otimes, \bar{1})$
1. $\otimes$ **is closed associative binary operator on the set A**
2. $\bar{1}$ **is identity element for** $\oplus$
$\forall \quad a, b, c \in A$
$a \otimes b \otimes c = a \otimes (b \otimes c)$
$a \otimes \bar{1} = \bar{1} \otimes a = a$

fəˈnɛtɪks

Definition of Ring

Let a, b, c $\in \mathbb{R}$
There are addition and multiplication operations and satisfy associative and distributive laws
$a * b * c = a * (b * c)$ *and* $a * (b + c) = a * b + a * c$
There are additive identity **0** and multiplicative identity **1**
$\mathbf{0} + a = a$ and $1 * a = a$
There exists additive inverse $-a$ such that $a + (-a) = 0$

Definition of Ring

let a, b, c $\in \mathbb{R}$
There are two binary operations addition and multiplication and satisfy

Associative Law
$a \times b \times c = a \times (b \times c)$

Distritutive Law
$a \times (b + c) = a \times b + a \times c$

Additive inverse
For all a in $\mathbb{R}$, there exists -a such that
$a + (-a) = 0$

Multiplicative identity
For all a in $\mathbb{R}$, there exist 1 such that
$1a = a$

Group homomorphism(operation preserving)

Given group $(G1, +)$ and $(G2, *)$,for all $a_1, a_2 \in G1$ and $b_1, b_2 \in G2$,
if $\phi(a_1 + a_2) = \phi(b_1) * \phi(b_2)$, then ϕ is group homomorphism

Given $G(\mathbb{R}, +)$ and $(\mathbb{R}, *)$, then $\phi(x) = e^x$ is homomorphism
Let $a_1, b_1 \in \mathbb{R}$ and $a_2, b_2 \in \mathbb{R}$
$\phi(a_1 + b_1) = e^{a_1 + b_1}$ and $\phi(a_2) * \phi(b_2) = e^{a_2} * e^{b_2} = e^{a_2 + b_2}$
$\Rightarrow \phi(a_1 + b_1) = \phi(a_2) * \phi(b_2)$

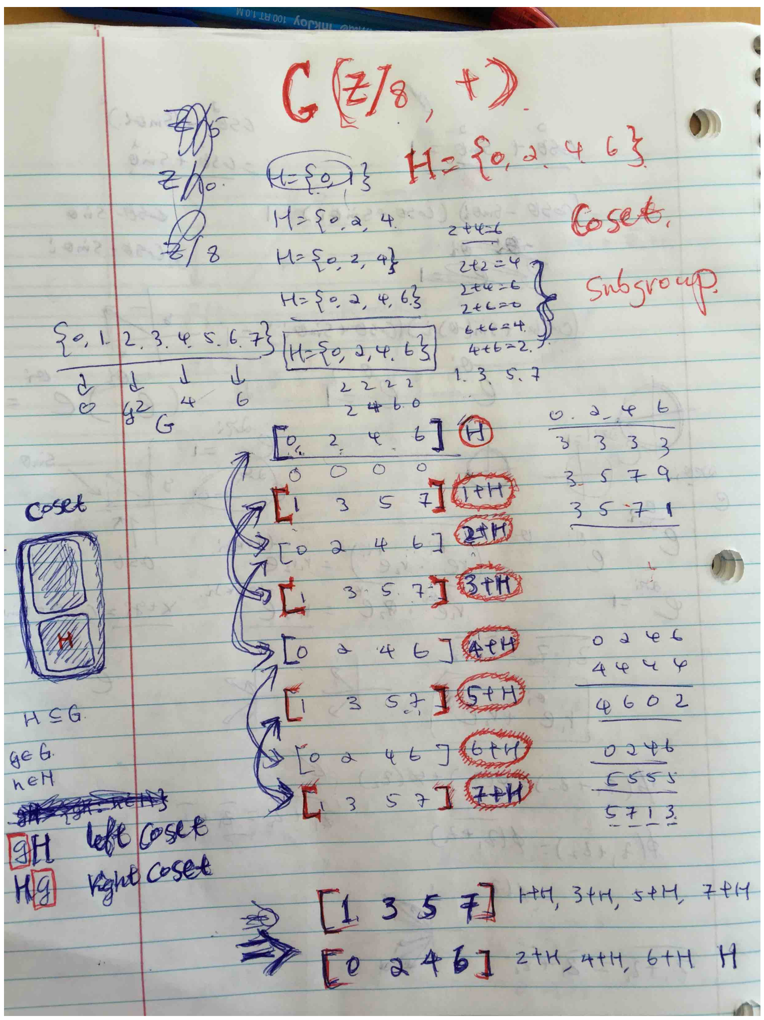
$\Rightarrow \phi(x) = e^x$ is homomorphism for $G(\mathbb{R}, +)$ and $G(\mathbb{R}, *)$

Normal Group

if N is subgroup of G, and if $gH = Hg \quad \forall g \in G$, then H is normal

Coset

if N is subgroup of G, and if $gH = \{gh : \forall g \in G\}$, then gH is left coset of H in G with repsect to g.
Similarly, if $Hg = \{hg : \forall g \in G\}$, then Hg is right coset of H in G with repsect to g.



Ring homomorphism(operation preserving) Let ϕ is a function between two rings R, then ϕ is a *ring* homomorphism if for all $a \in R$ and $b \in R$

$$\phi(a+b) = \phi(a) + \phi(b)$$

$$\phi(ab) = \phi(a)\phi(b)$$

and

$$\phi(1) = 1$$

e.g. $G(\mathbb{N}, +)$ and $G(\mathbb{Z}/\mathbb{Z}_5, +)$

Let $\phi : \mathbb{C} \to \mathbb{C}$ be the map send a complex number to its complex conjugate. Then ϕ is an automorphism of $\mathbb{C}$. ϕ is its own inverse.

$$\begin{aligned}
\phi(z) &= \overline{z} \\
\phi(z_1 + z_2) &= \overline{z_1 + z_2} \\
\overline{z_1 + z_2} &= \overline{z_1} + \overline{z_2} \\
\phi(z_1 z_2) &= \overline{z_1 z_2} \\
\overline{z_1 z_2} &= \overline{z_1} \cdot \overline{z_2} \\
\phi(\phi(z)) &= z
\end{aligned}$$

Let $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ be the map that send $f(x)$ to $f(x+1)$. Then ϕ is an automorphism of $\mathbb{R}[x]$. The inverse map sends $f(x)$ to $f(x-1)$

Ideal

Let R be a ring and let I is additive subgroup of R, then I is called an ideal of R and write $I \triangleleft R$ if $\forall a \in I$ and $\forall r \in R$, and $ar \in I$ and $ra \in I$

Example
$R = (\mathbb{N}, +)$ and $I = (2k, +) \quad k \in \mathbb{N}$

Let I be a kernal of ϕ, then I is an ideal of R
Let $a \in I$ and $r \in R$, then $\phi(ra) = \phi(r)\phi(a)$
I is kernal of $\phi \Rightarrow \phi(a) = 0 \therefore \phi(ra) = 0, \therefore ra \in I$

If $\gcd(a, b) = 1$ **and** $a|bc \quad \Rightarrow a|c$
Proof
$\gcd(a, b) = 1$
$\Rightarrow ma + nb = 1 \quad m, n \in \mathbb{N}$
$\Rightarrow mac + nbc = c$
$a|bc \Rightarrow ak = bc \quad k \in \mathbb{N}$
$\Rightarrow mac + n(ak) = c \quad (ak = bc)$
$\Rightarrow a(mc + nk) = c$

$\Rightarrow a|c$

If $\gcd(a,b)=1 \Rightarrow ma+nb=1 \quad m,n\in\mathbb{N}$
Proof

Prove there is infinite prime

Prove all the eigeivalues $\lambda \geq 0$ **if the matrix is symmetic**

If the determine of matrix $\det A > 0 \iff$ **the matrix is invertable**

Efficient Algorithm to compute Fibonacci Number
Fibonacci Sequence $F_n = F_n + F_{n-1}$ with $F_0 = 0$ $F_1 = 1$
(1) Navier algorithm with recursion in $O(2^n)$
(2) Use Dynamic Algorithm in $O(n)$
(3) Use matrix with repeated squaring to compute Fibonacci Sequence in $O(\log n)$

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}^n = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$$

Show the sum of odd number are square number

1
1 + 3
1 + 3 + 5
1 + 3 + 5 + ... + (2k+1)

$S = \sum_{k=1}^{n}(2k-1)$
$S = \sum_{k=1}^{n} 2k - \sum_{k=1}^{n} 1$
$S = 2(\sum_{k=1}^{n} k) - n$
$S = 2\frac{(1+n)n}{2} - n$
$S = (1+n)n - n$
$S = n^2$

composition function
$g \circ f \circ h$
$g \circ f\colon A \to B$

Find the sum of sequence of squares

$\sum_{k=1}^{n}((k+1)^3 - k^3) = \sum_{k=1}^{n}(k^2+1+2k)(k+1) - k^3$
$\sum_{k=1}^{n}(k^3+k+2k^2+k^2+1+2k) - k^3$
$\sum_{k=1}^{n}(k^3+3k^2+3k+1) - k^3$
$\sum_{k=1}^{n}(3k^2+3k+1)$

$\sum_{k=1}^{n}((k+1)^3 - k^3) = \sum_{k=1}^{n}(k+1)^3 - \sum_{k=1}^{n} k^3$
$\Rightarrow 2^3 + 3^3 + ... + n^3 + (n+1)^3 - (1 + 2^3 + 3^3 + ... + n^3) = (n+1)^3 - 1$
$\Rightarrow \sum_{k=1}^{n}(k+1)^3 - \sum_{k=1}^{n} k^3 = (n+1)^3 - 1$
$\Rightarrow (n+1)^3 - 1 = \sum_{k=1}^{n}(3k^2+3k+1)$
$\Rightarrow (n+1)^3 - 1 = 3\sum_{k=1}^{n} k^2 + 3\sum_{k=1}^{n} k + n$
$\Rightarrow (n+1)^3 - 1 = 3\sum_{k=}^{n} k^2 + (n+1)n\frac{3}{2} + n$
$\Rightarrow (n+1)^3 - 1 - (n+1)n\frac{3}{2} - n = 3\sum_{k=1}^{n} k^2$
$\Rightarrow (n+1)((n+1)^2 - n\frac{3}{2}) - (n+1) = 3\sum_{k=1}^{n} k^2$
$\Rightarrow (n+1)((n+1)^2 - n\frac{3}{2} - 1) = 3\sum_{k=1}^{n} k^2$
$\Rightarrow (n+1)(n^2 + 1 + 2n - n\frac{3}{2} - 1) = 3\sum_{k=1}^{n} k^2$
$\Rightarrow (n+1)(n^2 + \frac{1}{2}n) = \sum_{k=1}^{n} k^2$
$\Rightarrow \frac{1}{2}(n+1)(2n^2 + n) = \sum_{k=1}^{n} k^2$
$\Rightarrow \frac{1}{6}n(n+1)(2n+1) = \sum_{k=1}^{n} k^2$

Definition of Group

Let a, b, c $\in \mathbb{G}$

There is binary operation * and satisfy

Closure Law

$a * b \in \mathbb{G}$

Associative Law

$a * b * c = a * (b * c)$

Identity

$\exists e \in \mathbb{G}$ such that $e * a = a * e \in \mathbb{G}$

Inverse

If a $\in \mathbb{G}, \exists a^{-1} \in \mathbb{G}$ such that $a * a^{-1} = e$

Definition of Vector Space

Let $\vec{u}, \vec{v}, \vec{w} \in \vec{V}$ and scalars $\alpha, \beta \in \mathbb{F}$

Closure

$\vec{u} + \vec{v}$ and $\in \vec{V}$

Associative Law

$\vec{u} + \vec{v} + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$

Commutative Law

$\vec{u} + \vec{v} = \vec{v} + \vec{u}$

Identity element of addition

$\vec{0} \in \vec{V}$ such that $\vec{0} + \vec{u} = \vec{u}$

Inverse element of addition

$\exists - \vec{u}$ such that $\vec{u} + (-\vec{u}) = \vec{0}$

Identity element of scalar multiplication

$\exists \mathit{1} \in \mathbb{F}$ such that $\mathit{1}\vec{u} = \vec{u}$

Distributivity of scale multiplication with respect to vector addition

$\alpha(\vec{u} + \vec{v}) = \alpha\vec{u} + \alpha\vec{v}$

Distributivity of scale multiplication with respect to field addition

$(\alpha + \beta)\vec{u} = \alpha\vec{u} + \beta\vec{u}$

Definition of Affine Space

An affine space is a set of points that admits free transitive action of a vector space $\vec{V}$ That is, there is a map $X \times \vec{V} \to X : (x, \vec{v}) \mapsto x + \vec{v}$, called translation by a vector $\vec{v}$, such that

1. Addition of vectors corresponds to composition of translation, i.e., for all $x \in X$ and $\vec{u}, \vec{v} \in \vec{V}, (x + \vec{u}) + \vec{v} = x + (\vec{u} + \vec{v})$
2. The zero vector $\vec{0}$ acts as the identity vector, i.e., for all $x \in X, x + \vec{0} = x$
3. The action is transitive, i.e., for all $x, y \in X,$ exists $\vec{v} \in \vec{V}$ such that $y = x + \vec{v}$
4. The dimension of X is the dimension of vector space translations, $\vec{V}$

Or There is unique map
$X \times X \to \vec{V} : (x, y) \mapsto y - x$ such that $y = x + (y - x)$ for all $x, y \in X$ It furthermore satifies

1. For all $x, y, z \in X$, z - x = (z - y) + (y - x)
2. For all $x, y, \in X$ and $\vec{u}, \vec{v} \in \vec{V}$, $(y + \vec{v}) - (x + \vec{u}) = (y - x) + (\vec{v} - \vec{u})$
3. For all $x \in X, x - x = \vec{0}$
4. For all $x, y \in X, y - x = -(x - y)$

Affine Space from linear system equation

Consider an $(m \times n)$ linear sytem equations

$\sum_{k=1}^{n} a_{ik} x_k = c_i, (1 \leq i \leq m)$ (1)

where $d = n - rank(M), c_i \neq \vec{0} \in \mathbb{R}^m$

When the system has at least one solution x_p then the full set of solution is a d-dimension affine space $A \subset \mathbb{R}^n$

Since $x_p \in A,$ we can declare point x_p as origin of A and then introduct A coordinates as follows:homogenous system

$\sum_{k=1}^{n} a_{ik} x_k = \vec{0}(1 \leq i \leq m)$

$\Rightarrow dim(Ker(M)) = d$ (Rank Theorem)

(1) has d-linear independent solution $\vec{b_j} \in \mathbb{R}^n$ $(1 \leq j \leq d)$

Affine Space A can be written as

$A = \left\{ x_p + \sum_{j=1}^{d} \alpha_j \vec{b_j} \quad | \quad \alpha_j \in \mathbb{R} \qquad (1 \leq j \leq d) \right\}$

The α_j can be served as coordinates in A, so that A looks as it were a d-dimension coordiate space.

But note that addition(+) in the space refers to the chosen point $x_p,$ and not to the origin of the base vector

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$

Theorem 1

The image of transformation is spanned by the image of the any basis of its domain. For $T:\vec{V}\rightarrow\vec{W}$, if $\beta=\{\vec{b_1},\vec{b_2},...,\vec{b_n}\}$ is a basis of $\vec{V}$, then $T(\beta)=\{T(\vec{b_1}),T(\vec{b_2}),...,T(\vec{b_n})\}$ spans the image of T

Proof

For all $\vec{v}\in\vec{V},\vec{v}=\alpha_1\vec{b_1}+\alpha_2\vec{b_2}+...+\alpha_n\vec{b_n}$
$\Rightarrow T(\vec{v})=T(\alpha_1\vec{b_1}+\alpha_2\vec{b_2}+...+\alpha_n\vec{b_n})$
$\Rightarrow T(\vec{v})=\alpha_1T(\vec{b_1})+\alpha_2T(\vec{b_2})+...+\alpha_nT(\vec{b_n})$
$\Rightarrow\{T(\vec{b_1}),T(\vec{b_2}),...,T(\vec{b_n})\}$ spans the image of T

Rank Theorem

If the domain is finite dimension, then the dimension of domain is the sum of rank and nullity of the transformation
Let $T:\vec{V}\rightarrow\vec{W}$ be a linear transformation ,let n be the dimension of $\vec{V}$,
let k be nullity of T and let k be the rank of T
Show $n=k+r$

Let $\beta=\{\vec{b_1},\vec{b_2},...,\vec{b_k}\}$ be the basis of kernal of T, the basis can be extended to $\gamma=\{\vec{b_1},\vec{b_2},...,\vec{b_k},\vec{b_{k+1}},...,\vec{b_n}\}$
let $\vec{v}\in\vec{V}\Rightarrow\vec{v}=\alpha_1\vec{b_1}+\alpha_2+\vec{b_2}+,...,+\alpha_k\vec{b_k}+\alpha_{k+1}\vec{b}_{k+1}+,...,+\alpha_n\vec{b_n}$
Let $T(\vec{v})=T(\alpha_1\vec{b_1}+\alpha_2+\vec{b_2}+,...,+\alpha_k\vec{b_k}+\alpha_{k+1}\vec{b}_{k+1}+,...,+\alpha_n\vec{b_n})=\vec{0}$
$\Rightarrow\vec{v}=\alpha_1\vec{b_1}+\alpha_2+\vec{b_2}+,...,+\alpha_k\vec{b_k}+\alpha_{k+1}\vec{b}_{k+1}+,...,+\alpha_n\vec{b_n}\in\ker(T)\qquad(1)$
$\because\vec{v}=\sigma_1\vec{b_1}+\sigma_2+\vec{b_2}+,...,+\sigma_k\vec{b_k}\in\ker(T)\qquad(2)$
$(1)-(2)\Rightarrow\vec{0}=(\alpha_1-\sigma_1)\vec{b_1}+(\alpha_2-\sigma_2)\vec{b_2}+,...,+(\alpha_k-\sigma_k)\vec{b_k}+\alpha_{k+1}\vec{b}_{k+1}+,...,+\alpha_n\vec{b_n}$
$\because\vec{b}_1,\vec{b}_2,...,\vec{b}_k,\vec{b}_{k+1},\vec{b}_{k+2},...,\vec{b_n}$ are linearly independent
$\therefore\alpha_{k+1},\alpha_{k+2},...,\alpha_n$ are all zero $\qquad(3)$
$T(\vec{v})=T(\alpha_1\vec{b_1})+T(\alpha_2\vec{b_2})+,...,+T(\alpha_k\vec{b_k})+T(\alpha_{k+1}\vec{b}_{k+1})+,...,+T(\alpha_n\vec{b_n})=\vec{0}$
$T(\vec{v})=\alpha_1T(\vec{b_1})+\alpha_2T(\vec{b_2})+,...,+\alpha_kT(\vec{b_k})+\alpha_{k+1}T(\vec{b}_{k+1})+,...,+\alpha_nT(\vec{b_n})=\vec{0}$
$\because\beta=\{\vec{b_1},\vec{b_2},...,\vec{b_k}\}$ is the basis of kernal of T
$\therefore T(\vec{b_1})=\vec{0},...,T(\vec{b_k})=\vec{0}$
$\therefore T(\vec{v})=\alpha_{k+1}T(\vec{b}_{k+1})+,...,+\alpha_nT(\vec{b_n})=\vec{0}\qquad(4)$
(3) and (4) $\Rightarrow\{T(\vec{b}_{k+1}),T(\vec{b_{k+2}}),...,T(\vec{b_n})\}$ are linearly independent
$\Rightarrow$ dim($\vec{V}$) = nullity(T) + rank(T) or
$\Rightarrow$ dim($\vec{V}$) = dim(ker(T)) + dim(img(T))
$\Rightarrow n=k+r\quad\square$

Affine plane

Affine plane is a set, whose elements are called points, and a set of subset, called lines, satifying the following three axioms:

1. Given two distinct points P and Q, there is one and only one containing both P and Q.
2. Given a line l, and a point P not in l, there is one and only one line m which is parallel to l and which passes through P.

3. There exists three non-collinear points.

A coordinate system in an affine space $(\mathbf{X}, \mathbf{V})$ consists of a point $\mathbf{O} \in \mathbf{X}$ is called origin, and basis $\vec{v_1}, ..., \vec{v_n}$ for $\vec{V}$ Any point $\mathbf{x} \in \mathbf{X}$ can be written as

$\mathbf{x} - \mathbf{O} = \mathbf{x} - \mathbf{O}$
$\Rightarrow \mathbf{x} = \mathbf{O} + (\mathbf{x} - \mathbf{O}) = \mathbf{O} + \sum_{k=1}^{n} x_k \vec{v_k}$
where the numbers $x_1, ..., x_n$ are the coordinates for vector $\mathbf{x} - \mathbf{O}$ with respect to the basis $\vec{v_1}, ...\vec{v_n}$. They are now also called the coordinates for $\mathbf{x}$ with respect to the coordinate system $\mathbf{O}, \vec{v_1}, ..., \vec{v_n}$

Projective plane
A projective plane $\mathbb{S}$ is a set, whose elements are called points, and a set of subset, called lines, satifying the following four axioms.
1. Two distinct points meets P, Q of S lie on one and only one line.
2. Any two lines meet in at least one point.
3. There exist three non-colinear points
4. Every line contains at least three points.

Manifold
An subset $\mathbf{S}$ of $\mathbb{R}^m$ is called a manifold of dimension of d if every point p of $\mathbf{S}$ has a neighbourhood in $\mathbf{S}$ which is homeomorphic to an open set of $\mathbb{R}^d$

Homeomorphrism
Let S be a subset of $\mathbb{R}^m$ and sp be the subset of $\mathbb{R}^n$. A map $f : \mathbb{R}^m \mapsto \mathbb{R}^n$ is called homeomorphism if f is continuous and bijective and f^{-1} is continuous

Definition Open and Close Sets
1. $\mathbf{S}$ is said to be open set if every point of $\mathbf{S}$ is an interior of $\mathbf{S}$
2. $\mathbf{S}$ is said to be closed set if $\mathbb{R} \setminus \mathbf{S}$ is open

Proposition
1. $\mathbf{S}$ is open if there exists $\delta > 0$ such that $(s - \delta, s + \delta) \subseteq \mathbf{S}$
2. $\mathbf{S}$ is open if any $s \in \mathbf{S}$ there exists a neighbourhood of s included in $\mathbf{S}$

Terminology
$\mathcal{M}$ Set (ZFC) book
$\mathcal{Q}$ topology =: set of open set
$(\mathcal{M}, \mathcal{Q})$ toplogy space
$\mathcal{U} \in \mathcal{Q} \iff$ all $\mathcal{U} \subseteq \mathcal{M}$ and open set
$\mathcal{M} \setminus \mathcal{A} \iff$ all $\mathcal{A} \subseteq \mathcal{M}$ closed set
open $\not\Longrightarrow$ closed
open $\not\Longleftarrow$ closed

Definition of Inner Product Positivity
$\langle \vec{v}, \vec{v} \rangle \geq 0$

$\langle \vec{v}, \vec{v} \rangle = \vec{0} \iff \vec{v} = \vec{0}$

Bilinearity
$\langle c_1\vec{v_1} + c_2\vec{v_2}, \vec{v_3} \rangle = c_1\langle \vec{v_1}, \vec{v_3} \rangle + c_2\langle \vec{v_2}, \vec{v_3} \rangle$

Conjugate Symmetic
$\langle \vec{v_1}, \vec{v_2} \rangle = \overline{\langle \vec{v_2}, \vec{v_1} \rangle}$
Proof Cauchy-Schwarz Inequality by picture
$|a \cdot b| \leq \|a\|\|b\|$

Calculate the Excel Sheet Row number algorithm Latex Environment has different mode
Math mode
Text mode
Command mode

Elliptic Curve and Group Structure Conic Curve
$\begin{bmatrix} x & y & z \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \end{bmatrix}$
$ax^2 + ey^2 + iz^2 + (b+d)xy + (c+g)xz + (f+h)yz = 0$

$(x, y, z) = (x/z, y/z, 1)(z \neq 0)$

$$\begin{array}{lcl} ax^2 + ey^2 + (b+d)xy + (c+g)x + (f+h)y + i & = & 0 \\ ax + by + c & = & 0 \end{array}$$

sub (1) into (2) $\Rightarrow ax^2 + bx + c = 0$
$\Rightarrow x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$

Exponential backoff algorithm

$\frac{1}{N+1} \sum_{i=1}^{k} i$
For example, the expected backoff time for the third collision, one could calculate the maximum backoff time, N
$N = 2^c - 1 (c = 3)$ $N = 7$
Calculate the mean of backoff time for the third collision(c=3)
$\mathbf{E(c)} = \frac{1}{N+1} \sum_{i=0}^{N} i$
$\mathbf{E(c)} = \frac{1}{N+1} \sum_{i=0}^{N} \Rightarrow \frac{1}{N+1} \frac{N(N+1)}{2} = \frac{N}{2}$
$\mathbf{E(3)} = \frac{1}{7+1} \sum_{i=0}^{N} i = \frac{1}{8}(0+1+2+3+4+5+6+7) = \frac{28}{8}$
$\mathbf{E(3)} = 3.5$

Prove Square root of two is irrational $\sqrt{2} \notin \mathbb{Q}$
Assume $\sqrt{2} \in \mathbb{Q}$
let $n = min\{n \in \mathbb{N} \mid n * \sqrt{2} \in \mathbb{N}\}$
$\Rightarrow n * (\sqrt{2} - 1) * \sqrt{2} \in \mathbb{Q}$
$\because \sqrt{2} - 1 < 1$
$\Rightarrow n * (\sqrt{2} - 1) * \sqrt{2} < n * \sqrt{2}$
$\Rightarrow n * (\sqrt{2} - 1) < n$ such as $n * (\sqrt{2} - 1) * \sqrt{2} \in \mathbb{N}$
$\Rightarrow$ This contracts our assumption $\square$

Prove Square root of 2 is irrational [Geometric proof]

Assume $\sqrt{2} \in \mathbb{Q}$

$\Rightarrow \frac{a}{b} = \sqrt{2} \quad a, b \in \mathbb{N}$ and $\gcd(a, b) = 1, a > b$

given a right issoseles triangle

$AB = AC = AE, \quad FE$ tangles to arc at point E

$\Rightarrow AF = EF$

Let $AB = AC = 1$

$\Rightarrow BC = \sqrt{2}$

$\Rightarrow FB = 1 - EB = 1 - (\sqrt{2} - 1) = 2 - \sqrt{2}$

$\because \frac{AC}{CB} = \frac{EB}{FB} = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}-1}{2-\sqrt{2}}$

$\therefore \frac{1}{\sqrt{2}} = \frac{1}{\frac{a}{b}} = \frac{\sqrt{2}-1}{2-\sqrt{2}} = \frac{\frac{a}{b}-1}{2-\frac{a}{b}}$

$\therefore \frac{b}{a} = \frac{\frac{a-b}{b}}{\frac{2b-a}{b}} = \frac{a-b}{2b-a}$

$\because \sqrt{2} < \sqrt{4} = 2 \therefore a < 2b$

$\Rightarrow a - b < b$

$\because 2a > 2b$

$\Rightarrow 2b - a < a$

That contracts our assumption $\gcd(a, b) = 1$

$\Rightarrow \frac{a}{b} \notin \mathbb{Q}$

Geometric proof: square root of two is irrational
Given an isosceles right triangle from above and let $\gcd(a,b)=1,$ from Pythagorean theorem
$\Rightarrow a^2 = b^2 + b^2$
$\Rightarrow \sqrt{2} = \frac{a}{b}$

singular point on affine plane curve
If $p \in (x,y)$ and $\frac{df}{dx}, \frac{df}{dy}$ are undefined on $p \in (x,y),$ then $p \in (x,y)$ is singular point

Eisenstein series

$L = [w_1, w_2] \in \mathbb{C}, G(L) = \sum_{w \in L \setminus \{0,0\}} \frac{1}{w^k}$
Let lattices $L = [1, \tau]$ and parametrized by τ in the upper half plane $\mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$
$G(L) = G([1,\tau]) = G(\tau) = \sum'_{m,n \in \mathbb{Z}} \frac{1}{(m+n\tau)^k}$

Show $G_k(\tau+1) = G_k(\tau)$

$G_k(\tau+1) = \sum'_{m,n \in \mathbb{Z}} \frac{1}{(m+n(\tau+1))^k} = \sum'_{m,n \in \mathbb{Z}} \frac{1}{(m+n+n\tau)^k} = \sum'_{m',n \in \mathbb{Z}} \frac{1}{(m'+n\tau)^k}$
$\Rightarrow G_k(\tau+1) = G_k(\tau)$

Show $G_k(\tau) = \tau^{-k} G_k(\dfrac{-1}{\tau})$

$\tau^{-k} G_k(\frac{-1}{\tau}) = \tau^{-k} \sum'_{(m,n \in \mathbb{Z})} \frac{1}{(m+\frac{n}{\tau})^k}$
$\tau^{-k} \sum'_{m,n \in \mathbb{Z}} \frac{1}{(m+\frac{n}{\tau})^k} = \tau^{-k} \sum'_{m,n \in \mathbb{Z}} \frac{1}{(\frac{m\tau}{\tau}+\frac{n}{\tau})^k} = \sum'_{m,n \in \mathbb{Z}} (\tau^{-k}\tau^{k})(m\tau+n)^{-k})$
$\Rightarrow G_k(\tau) = \tau^{-k} G_k(\frac{-1}{\tau})$

Show $G_k(\tau) = 0$ if $k = (2j+1) \quad j \in \mathbb{Z}$

For each $\omega = (m+n\tau) \in L,$ there exists $-\omega = -(m+n\tau) \in L$
$\because \omega^{-(2J+1)} + (-1)^{-(2J+1)} \omega^{-(2j+1)} = 0$
$\therefore \sum'_{m,n \in \mathbb{Z}} (m+n\tau)^{-k} = 0 \quad$ for all $k \in (2j+1)$

Show for any lattices L, the sum $\displaystyle\sum'_{\omega \in L} \frac{1}{\omega^k}$ converges absoluately for all $k > 2$

Proof:

$$\text{Show } \frac{1}{(1-x)^2} = \sum_{n=0}^{\infty}(n+1)x^n \quad |x|<1$$

Proof: For all $|x|<1$, power series expansion

$$(\frac{1}{1-x}) = (\sum_{n=0}^{\infty} x^n)$$

Differentiate both sides

$$\begin{aligned}
(\frac{1}{1-x})' &= (\sum_{n=0}^{\infty} x^n)' \\
(\frac{1}{1-x})' &= (1-x)^{-2} \\
\sum_{n=1}^{\infty} nx^{n-1} &= \sum_{i=0}^{\infty}(i+1)x^i \quad (n-1=i) \\
\frac{1}{(1-x)^2} &= \sum_{n=0}^{\infty}(n+1)x^n \qquad \text{sub } (i=n)
\end{aligned} \tag{1}$$

Weierstrass function $\wp$-function of lattice L is defined by

$\wp(z) = \wp(z;L) = \frac{1}{z^2} + \sum'_{w\in L}\left[\frac{1}{(z-\omega)^2} + \frac{1}{\omega^2}\right]$

Holomorphic

A function $f(z)$ defined on some open neibourhood of a point $z_0 \in \mathbb{C}$ is said to be holomorphic at z_0 if the complex derivative

$$f'(z_0) = \lim_{h\to 0}\frac{f(z_0+h)-f(z_0)}{h}$$

exists. We said f is holomorphic on an open set Ω if it is holomorphic at every $z_0 \in \Omega$ and we said f is holomorphic in a closed set $\mathbf{C}$ if it is holomorphic on some open set Ω containing $\mathbf{C}$. Functions are holomorphic on all of $\mathbb{C}$ are said to be *entire*

$$\begin{aligned}
&\text{Show } f(z) = z^2 \text{ is holomorphic} \\
&f'(z) = \lim_{h\to 0}\frac{(z+h)^2 - z^2}{h} \\
&f'(z) = \lim_{h\to 0}\frac{z^2+2hz+h^2-z^2}{h} \\
&f'(z) = \lim_{h\to 0}\frac{2hz+h^2}{h} \\
&f'(z) = \lim_{h\to 0} 2z+h \\
&f'(z) = 2z
\end{aligned}$$

Differential
A function $f(x)$ is differential on $x_0 \in \mathbb{R}$ if

$$f'(x_0) = \lim_{h \to 0} \frac{f(x_0 + h) - f(x_0)}{h}$$

exists

Show $f(x) = x^2$ is differentiable for all $x \in \mathbb{R}$

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$
$$f'(x) = \lim_{h \to 0} \frac{x^2 + h^2 + 2xh - x^2}{h}$$
$$f'(x) = \lim_{h \to 0} \frac{h^2 + 2xh}{h}$$
$$f'(x) = \lim_{h \to 0} h + 2x$$
$$f'(x) = 2x \quad \text{for all } x \in \mathbb{R}$$

Elliptic Curve

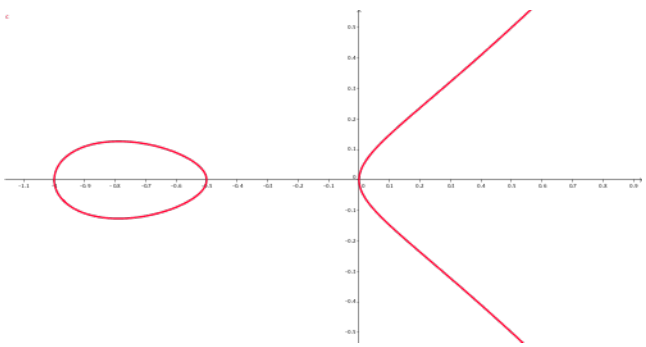
Find the formula for

$$s(n) = \sum_{k=1}^{n} k^2$$

$$s(n) = \frac{(2n+1)(n+1)n}{2 \times 3}$$

Let $y^2 = S(n)$ and $x = n$

$$y^2 = \frac{1}{6}x(x+1)(2x+1)$$



$(x, y) = (0, 0), (-1, 0), (-\frac{1}{2}, 0)$ are on the curve

$$y^2 = x^3 + bx^2 + cx + d$$

$\because (x + \frac{b}{3})^3 = x^3 + 3x^2\frac{b}{3} + 3x(\frac{b}{3})^2 + (\frac{b}{3})^3$
$y^2 = (x + \frac{b}{3})^3 - 3x(\frac{b}{3})^2 - (\frac{b}{3})^3 + cx + d$
$y^2 = (x + \frac{b}{3})^3 - [3(\frac{b}{3})^2 - c]x + d$
let x + $\frac{b}{3} = x'$
$y^2 = x'^3 - [3(\frac{b}{3})^2 - c][x' - \frac{b}{3}] + d$
$y^2 = x'^3 - [3(\frac{b}{3})^2 - c]x' + 3(\frac{b}{3})^3 - \frac{b}{3}c + d$
$y^2 = x'^3 + [c - 3(\frac{b}{3})^2]x' + 3(\frac{b}{3})^3 - \frac{b}{3}c + d$

For any lattice $L,$ the sum of $\displaystyle\sum_{\omega_k \in L}^{\prime\infty} \frac{1}{\omega_k}$ is converges absoluately for all $k > 2$

Definition of topology

Let $\mathcal{M}$ be a set. A topology $\mathcal{Q}$ is a subset $\mathcal{Q} \subseteq \mathcal{P}(\mathcal{M})$
Satisfy
1.$\varnothing \subseteq \mathcal{Q}, \mathcal{M} \subseteq \mathcal{Q}$
2.$\mathcal{U} \subseteq \mathcal{Q}, \mathcal{V} \subseteq \mathcal{Q} \implies \mathcal{U} \cap \mathcal{V} \in \mathcal{Q}$
3.$\mathcal{U} \in \mathcal{Q} \implies \bigcup_{\alpha \in \mathcal{A}} \mathcal{U}_\alpha \in \mathcal{Q}$

Topological Space

a topological space is pair (X, τ) where X is a set and τ is subset of X satifying certain axioms. τ is called topology
1. $\emptyset$ and space X are both in τ
2. the union of any collection of set in τ is contained in τ
3. the intersection of any finitly many sets in τ is contained in τ