Summer Research

Joshua J.George

May 3, 2021

(The Blue coloured text are the new weeks additions.)

Contents

1 Introduction

1.1 Fundamental Theorem of Arithmetic

Every integer $n > 1$ can be represented as a product of prime factors in only one way, apart from the order of the factors. That is every nonzero integer x can be written as

$$x = \prod_{i=1}^{n} p_i^{e_i}, \quad p_1 < p_2 < \ldots < p_n \text{ primes}, n \geq 0, e_i > 0$$

1.1.1 Greatest common divisor and Least common multiple

If two positive integers x and y have the factorizations

$$x = \prod_{i=1}^{\infty} p_i^{e_i}, \quad y = \prod_{i=1}^{\infty} p_i^{f_i}$$

Then,

$$\gcd(x, y) := \prod_{i=1}^{\infty} p_i^{g_i} \text{ , where each } g_i = \min\{e_i, f_i\}$$

$$\operatorname{lcm}(x, y) := \prod_{i=1}^{\infty} p_i^{h_i} \text{ ,where each } h_i = \max\{e_i, f_i\}$$

1.1.2 Co-prime

Co-prime or relative prime numbers are those whose gcd is 1.

1.2 Big $\mathcal{O}$-notation, Big Ω-notation

We write

$$f(x) = \mathcal{O}(g(x)) \text{if there exist constant } C > 0 \ni |f(x)| \leq C|g(x)| \quad \text{for all } x$$

Similarly,

$$f(x) = \Omega(g(x)) \text{ if there exist constant } C > 0 \ni |f(x)| \geq C|g(x)| \quad \text{for all } x$$

1.3 Abel Summation

Let $\{a_n\}_n = 1^\infty$ be a sequence of complex numbers and $f(t)$ be a differentiable function for $t \geq 0$. Set $A(x) = \sum_{n \leq x} a_n$. Then

$$\sum_{n \leq x} a_n f(n) = A(x) f(x) - \int_1^x A(t) f'(t) dt$$

Proof: Note: $a_n = A(n) - A(n-1), x \in \mathbb{N}$.

Therefore $\sum\limits_{n \le x}(A(n) - A(n-1))f(n) = \sum\limits_{n \le x} A(n)f(n) - \sum\limits_{n \le x-1} A(n)f(n+1)$

$=$

$$\sum_{n \le x-1} A(n)f(n)+A(x)f(x)-\sum_{n \le x-1} A(n)f(n+1) = A(x)f(x)+\sum_{n \le x-1} A(n)(f(n)-f(n+1))$$

Well:

$$\sum_{n \le x-1} A(n)(f(n) - f(n+1)) = -\int_1^x A(t)f'(t)dt, t \in \{n, n+1\}$$

This proves the claim.

1.4 Homomorphism, Isomorphism and Automorphism

Two groups, $(G, *)$ and $(H, \cdot)$ is a group homomorphism from $(G, *)$ to $(H, \cdot)$ is a function $f : G \to H \ni \forall\, u, v \in G$ it holds that

$$f(u * v) = f(u) \cdot f(v),$$

where the left side is from G and right from H. Here, f preserves group operations
A group homomorphism that is bijective; i.e., injective(preserves distinctness) and surjective is an Isomorphism.(reaches every point in the codomain)
A group homomorphism where the domain and codomain are the same is called a Automorphism.

2 Functions

2.1 Analytic, Multiplicative and Meromorphic functions

Analytic functions: The following are equivalent conditions for a function to be analytic:

(1): If f is differentiable at each point of the domain D then f is called analytic in D; in this case, the derivative function is defined by

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

(2):f can be represented as a power series iff it is analytic.
(3):The Cauchy-Riemann conditions are necessary and sufficient conditions for a function to be analytic at a point. Let $f = u(x,y) + iv(x,y)$, if f satisfies

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \quad \frac{\partial v}{\partial x} = -\frac{\partial u}{\partial y}$$

then f is analytic.

Multiplicative functions:

1) An arithmetical function is a map $f : \mathbb{N} \longrightarrow \mathbb{C}$
2) The function f is called multiplicative if
$f(nm) = f(n)f(m)\ \forall\, n, m \in \mathbb{N}$ where n, m are co-prime.
3) The function f is completely or totally called multiplicative if
$f(nm) = f(n)f(m)\ \forall\, n, m \in \mathbb{N}$ where n,m need not be co-prime

Meromorphic functions:

Complex functions which can be expressed as ratio of two analytic functions are called meromorphic functions.
Facts: Suppose $f(z)$ is a meromorphic function at z_0, $f(z)$ admits an expansion of the form,

$$f(z) = \frac{f_{-R}}{(z-z_0)^R} + \dots \frac{f_{-2}}{(z-z_0)^2} + \frac{f_{-1}}{(z-z_0)^1} + f_0 + \dots f_1(z-z_0) + \dots$$

and is said to have a pole of order R at z_0.The coefficient of f_{-1} is said to be the residue of $f(z)$ at z_0, written as $\mathrm{Re}_{z=z_0} f(z)$. Therefore we can rephrase the defintion of meromorphic function to be, a function $f(z)$ is meromorphic iff it is analytic everywhere except for its isolated singularities ie poles.

2.2 Divisor Function ($\tau(n)$) and Divisor Sum Function ($\sigma(n)$)

$\tau : \mathbb{N} \to \mathbb{N}$, $\tau(n) :=$ number of positive divisors of n. Example $\tau(p) = 2$ for primes p, $\tau(10) = 4$.

$\sigma : \mathbb{N}_1 \to \mathbb{N}_1$, $\sigma(n) :=$ sum of all positive divisors of n.Thus $\sigma(p) = 1 + p$ for primes p, $\sigma(10) = 18$.

2.3 Möbius function ($\mu(n)$)

$\mu : \mathbb{N} \to \mathbb{Z}$. This important function is defined by

$$\mu(n) := \begin{cases} 1, \text{ for } n = 1 \\ 0, \text{ if there exists a prime } p \text{ with } p^2 \mid n \\ (-1)^r, \text{ if } n \text{ is a product of } r \text{ different primes} \end{cases}$$

Examples $\mu(3) = -1, \mu(7) = -1, \mu(8) = \mu(2^3) = 0(2^2|8^2), \mu(6) = 1$
Basic Properties:
The function $\mu(n)$ is multiplicative ie

$$\mu(mn) = \mu(m)\mu(n), \gcd(m, n) = 1$$

Proof :Let $m = p_1p_2 \dots p_s$ where $p_1, p_2, \dots, p_s$ are distinct primes and $n = q_1q_2 \dots q_t$ where $q_1, q_2, \dots, q_t$ are distinct primes. Since $\gcd(m, n) = 1$, then there are no common primes in the prime decomposition between m and n. Thus

$$\mu(m) = (-1)^s, \mu(n) = (-1)^t \text{ and } \mu(mn) = (-1)^{s+t} \text{ by definition of function.}$$

Therefore,

$$\mu(mn) = (-1)^{s+t} = \mu(m)\mu(n)$$

Theorem: If $n \geq 1$ we have

$$\sum_{d|n} \mu(d) = \left[\ 1/n\ \right] = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

where d runs through the positive divisors of n.
Proof: Define $F(n) = \sum_{d|n} \mu(d)$ since $\mu(d)$ is multiplicative it implies $F(n)$ is multiplicative. Also, for $n \geq 1$,let $n = p_1^{e_1}p_2^{e_2} \dots p_k^{e_k}$, where $p_1, p_2, \dots, p_k$ are distinct primes.Now $F(n) = F(p_1^{e_1}p_2^{e_2} \dots p_k^{e_k})$, since F is multiplicative this gives us $F(n) = F(p_1^{e_1})F(p_2^{e_2}) \dots F(p_k^{e_k})$. Now $F(p_i^{e_i}) = \sum_{d|p_i^{e_i}} \mu(d)$. Since d is a divisor of $p_i^{e_i}$ therefore $d \in \{1, p_i, p_i^2 .... p_i^{e_i}\}$. This gives us,$F(p_i^{e_i}) = \sum_{d|p_i^{e_i}} \mu(d) = \mu(1) + \mu(p_i) + \mu(p_i^2) + \dots + \mu(p_i^{e_i}) = 1 + -1 + 0 + 0 + 0 \dots + 0 = 0$.Therefore, $F(p_i^{e_i}) = 0$ for $n \geq 1$.For $n = 1, e_1 = e_2 = \dots e_k = 0$ giving us $F(1) = \sum_{d|1} \mu(d) = \mu(1) = 1$.

2.4 Von-Mangoldt Function ($\Lambda(n)$)

$$\Lambda(n) := \begin{cases} \log(p) & \text{if } n = p^k \text{ for some prime } p \text{ and integer} k \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

Example $\Lambda(1) = 0, \Lambda(8) = \Lambda(2) = \log(2), \Lambda(3) = \log(3)$.

Write $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, taking log on both sides gives us, $\log(n) = e_1 \log(p_1) + e_2 \log(p_2) + \dots e_k \log(p_k)$ (unique factorisation), which is the same as

$$\log(n) = \sum_{d|n} \Lambda(d)$$

.

2.5 Chebyshev Function ($\psi(x)$)

$$\psi(x) := \sum_{n \leq x} \Lambda(n)$$

Chebyshev's result: Let $\psi(x) := \sum_{p \leq x} \log p$ (where p is prime).Then

$$\psi(x) \leq 2n \ln 2$$

Proof: We know,$(1+1)^{2m+1} = \sum_{j=0}^{2m+1} \begin{pmatrix} 2m+1 \\ j \end{pmatrix}$ Let M=$\begin{pmatrix} 2m+1 \\ m \end{pmatrix}$,$2M \leq 2^{2m+1} \implies M \leq 2^{2m} \cdots (1)$.

Now, $M = \frac{(2m+1)!}{(m)!(m+1)!}$, every prime in the interval $(m+1, 2m+1]$ appears in the numerator. Then

$$\prod_{m+1<p\leq 2m+1} p \mid M \cdots (2)$$

Taking log on both sides and combining (1) and (2), gives us

$$\sum_{m+1 \leq p \leq 2m+1} \log p \leq \log M \leq 2m \ln 2$$

Therefore , $\psi(2m+1) - \psi(m+1) \leq 2m \ln 2$
Now we can proceed with induction, for $m = 1$ we get left hand side, $\log 3 \leq \log 4$ on the right hand side which is true. Now assume the inequality is true $\forall m \geq 1$ upto $m - 1$.
We need to show $\psi(2m+1) - \psi(m+1) < 2(m) \log 2$. Now

$$\psi(2m+1) < \psi(m+1) + 2m \log 2 \implies 2(m+1) \log 2 + 2m \log 2 \implies$$

(By inductive hypothesis)

$$< 2(2m+1) \log 2$$

3 Dirichlet Series

3.1 Dirichlet series introduction

The Dirichlet series is any series of the form

$$\mathfrak{D} := \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

and the riemann zeta function is one case of the dirichlet series. The Riemann zeta function can be expressed as:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Euler claimed:

$$\zeta(s) = \prod_{p} \sum_{k=0}^{\infty} \frac{1}{p^{ks}} = \prod_{p} \frac{1}{1-p^{-s}}, \text{ where p is prime} \ldots (\alpha)$$

Proof:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \ldots$$

Dividing by $\frac{1}{2^s}$ we get,

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \ldots$$

Subtracting the second equation from the first we remove all elements that have a factor of 2 :

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \frac{1}{13^s} + \ldots$$

Repeating for the next term and subtracting in a similar fashion for all primes gives us:

$$\ldots\left(1 - \frac{1}{11^s}\right)\left(1 - \frac{1}{7^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1$$

Dividing both sides by everything but the $\zeta(s)$ we obtain:

$$\zeta(s) = \frac{1}{\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{7^s}\right)\left(1-\frac{1}{11^s}\right)\ldots} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

Claim: The Riemann zeta function converges for $\text{Re}(s) > 1$.

Proof: For $s > 1, s \in \mathbb{R}, \zeta(s)$ converges and this can be checked by the Integral criterion which states that if $f \geq 0$ monotone decreasing on $[a, \infty)$ where

$a \in \mathbb{N}$. Then $\int_a^\infty f(x)dx$ converges if and only if the infinite series $\sum_{n=a}^\infty f(n)$ converges. Taking $f(x) = 1/x^s$,solving this integral gives us $\frac{1}{s-1}$ which converges $(s > 1)$. What about $s \in \mathbb{C}$? if $s = \sigma + it$, we have,$|n^s| = \left|e^{s \ln n}\right| = \left|e^{Re(s)\ln n}\right| = n^\sigma$. Here ,$\left|e^{i \ln n)}\right| = 1$ as $\ln n \in \mathbb{R}, n \in \mathbb{N}$. Consider $\operatorname{Re} s > 1$,

$$\sum_{n=1}^{\infty}\left|\frac{1}{n^s}\right| = \sum_{n=1}^{\infty}\frac{1}{n^\sigma}$$

and since Re $s > 1$, the series on the right converges. Thus $\sum_{n=1}^\infty \frac{1}{n^s}$ converges absolutely in $\operatorname{Re} s > 1$

3.2 Analytic continuation of riemann zeta function

Definition: If $f(s)$ is analytic in a region X and $g(s)$ is analytic in a region Y and $X \subseteq Y$, $f(s) = g(s)$ $\forall s \in X$ we say g is a analytic continuation of f. Therefore applying Abel summation to $\sum_{n \le x} \frac{1}{n^s}$ gives us

$$= \frac{[x]}{x^s} + s\int_1^x \frac{[t]}{t^{s+1}}dt \text{ where } a_n = 1, f(n) = \frac{1}{n^s}$$

Let $x \to \infty$,

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \int_1^\infty \frac{[t]}{t^{s+1}}dt$$

$$= s\int_1^\infty \frac{t - \{t\}}{t^{s+1}}dt, \{t\} = \text{fractional part}$$

$$= \frac{s}{s-1} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}dt$$

, RHS is analytic for $\operatorname{Re}(s) > 0$ except for $s = 1$ where it has a simple pole.

We know the log power series expansions, $\log(1 + x) = \sum_1^\infty \frac{-x^n}{n}$
Also since $\zeta(s)$ is analytic in the region $\operatorname{Re}(s) > 1$,taking log of (α) gives us $\log(\zeta(s)) = -\sum_p \log(1 - \frac{1}{p^s}) = \sum_p \frac{1}{np^{ns}}$ where p is prime,$n \ge 1$.
Differentiating both sides gives us,

$$\frac{\zeta'(s)}{\zeta(s} = -\sum_p \frac{1}{p^{ns}} \implies -\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}$$

Claim:

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s} = s\int_0^\infty e^{-sx}\psi(e^x)dx$$

$$s\int_0^\infty e^{-sx}\psi\left(e^x\right)dx = s\int_0^\infty e^{-sx}\left(\sum_{n \le e^x}\Lambda(n)\right)dx = s\sum_{n=1}^{\infty}\Lambda(n)\int_{\log n}^\infty e^{-sx}dx$$

$$= s\sum_{n=1}^{\infty}\Lambda(n)\left[\frac{-1}{s}e^{-sx}\right]_{\log n}^\infty = \sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}$$

3.3 Dirichlet characters

We say that a function χ from the integers $\mathbb{Z}$ to the complex numbers $\mathbb{C}$ is a Dirichlet character if it has the following properties:

(1)There exists a positive integer k such that $\chi(n) = \chi(n+k)$ for all integers n.
(2)If $\gcd(n,k) > 1$ then $\chi(n) = 0$; if $\gcd(n,k) = 1$then $\chi(n) \neq 0$.
(3)$\chi(mn) = \chi(m)\chi(n)\forall$ integers m and n.

Principle character (χ_0):

$$\chi_0(n) = \begin{cases} 1 & \text{if } (n,k) = 1 \\ 0 & \text{if } (n,k) \neq 1 \end{cases}$$

If $\chi(n)$ is a Dirichlet character $(\bmod k)$, the complex conjugate function $\bar{\chi}(n)$ is also a Dirichlet character $(\bmod k)$;

$$\chi^{\phi(k)}(n) = \chi_0(n)$$

The smallest positive number ν that satisfies the equation $\chi^{\nu}(n) = \chi_0(n)$ is called the order of the Dirichlet character.

Orthogonal relation: (i)For any two Dirichlet charactersχ_1, χ_2 modulo k we have

$$\sum_{n=1}^{k} \chi_1(n)\overline{\chi_2(n)} = \begin{cases} \phi(n) & \text{if } \chi_1 = \chi_2, \\ 0 & \text{otherwise} \end{cases}$$

(ii)For any Dirichlet character χ modulo k we have

$$\sum_{n=1}^{k} \chi(n) = \begin{cases} \phi(k) & \text{if } \chi = \chi_0 \\ 0 & \text{otherwise} \end{cases}$$

where χ_0 is the principal character modulo k. Proof:(i) If $\chi_1 = \chi_2$ then $\bar{\chi}_2(n) = \chi_1(n)^{-1}$ and the sum is equal to $\phi(k)$. Assume that $\chi_1 \neq \chi_2$. Then there is at least one element m such that $\chi_1(m) \neq \chi_2(m)$. Let $F = \sum \chi_1(n)\bar{\chi}_2(n)$. Now, the product mn runs through A when n does, and therefore one has

$$F = \sum \chi_1(mn)\bar{\chi}_2(mn) = \chi_1(m)\bar{\chi}_2(m) \sum \chi_1(n)\bar{\chi}_2(n) = \chi_1(m)\bar{\chi}_2(m)F$$

Therefore $F = 0$, since $\chi_1(m)\bar{\chi}_2(m) = \chi_1(m)\chi_2(m)^{-1} \neq 1$. (ii) if we put consider $\chi = \chi_1\chi_2$ we get the result.

3.4 Dirichlet L-series

Let $\chi : \mathbb{N} \to \mathbb{C}$ be a Dirichlet character. The L -series associated to χ is the Dirichlet series

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

This series converges absolutely for every $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$.

Theorem. Let $\chi : \mathbb{N} \to \mathbb{C}$ and

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

(1) Then we have the euler product representation

$$L(s,\chi) = \prod_{p\text{-prime}} \left(\sum_{k=0}^{\infty} \frac{\chi\left(p^k\right)}{p^{ks}} \right) = \prod_{p\text{-prime}} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi\left(p^2\right)}{p^{2s}} + \frac{\chi\left(p^3\right)}{p^{3s}} + \cdots \right)$$

(2) Since χ is completely multiplicative, (1) is simplified to

$$L(s,\chi)\chi = \prod_{p\text{-prime}} \left(1 - \frac{\chi(p)}{p^s} \right)^{-1}$$

Proof. Since χ is multiplicative, we have for an integer n with prime decomposition $n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$

$$\chi(n) = \chi\left(p_1^{k_1}\right) \chi\left(p_2^{k_2}\right) \ldots \chi\left(p_r^{k_r}\right)$$

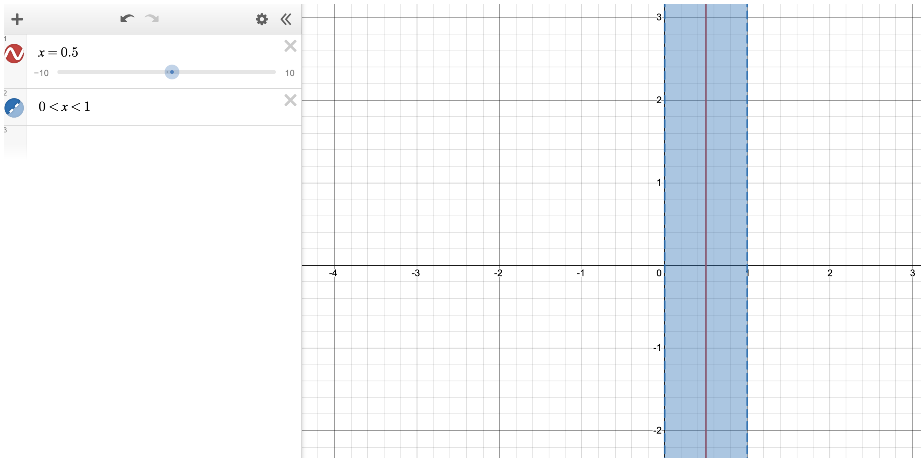
It follows by multiplying the infinite series term by term that (in a similar fashion how Euler claimed (α),

$$\prod_{p-prime} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi\left(p^2\right)}{p^{2s}} + \frac{\chi\left(p^3\right)}{p^{3s}} + \cdots \right) = \sum_{n} \frac{\chi(n)}{n^s}$$

For part (2), since χ is completely multiplicative, $\chi\left(p^k\right) = \chi(p)^k$, hence

$$\sum_{k=0}^{\infty} \frac{\chi\left(p^k\right)}{p^{ks}} = \sum_{k=0}^{\infty} \left(\frac{\chi(p)}{p^s} \right)^k = \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} = \left(\frac{1}{1 - \chi(p)p^s} \right)$$

3.5 Critical Strip, Line and the Riemann Hypothesis



Critical Strip (blue shaded region) and line(red line).

Riemann Hypothesis:
For s in the critical strip, $\zeta(s) = 0 \Rightarrow \sigma = \text{Re}(s) = 1/2$

3.6 Gamma Function

The gamma function is defined as:

$$\Gamma(s) = \int_0^\infty x^{s-1} e^{-x} \, \mathrm{d}x$$

3.6.1 Relationship between Gamma and zeta function

Consider the gamma function:

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} dt$$

Subsitute $t = nx$ in the integral to arrive at

$$\frac{\Gamma(s)}{n^s} = \int_0^\infty e^{-nx} x^{s-1} dx$$

which we then sum up to get

$$\Gamma(s)\zeta(s) = \int_0^\infty \frac{x^{s-1}}{e^x - 1} dx$$

3.6.2 Completed Zeta function

The completed zeta function is as follow:

$$\xi(s) = \frac{1}{2} \pi^{-\frac{s}{2}} s(s-1) \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

4 Weiner-Ikehara Theorem (X) and PNT

4.1 Theorem Weiner-Ikehara

Let $A(x)$ be a non-negative, monotonic nondecreasing function of x, defined for $0 \leq x < \infty$. Suppose that

$$f(s) = \int_0^\infty A(x) e^{-xs} dx$$

converges for $\Re(s) > 1$ to the function $f(s)$ and that, for some non-negative number c,

$$f(s) - \frac{c}{s-1}$$

has an extension as a continuous function for $\mathrm{Re}(s) \geq 1$. Then the limit as x goes to infinity of $e^{-x}A(x)$ is equal to c.

4.2 Lemma 1

$a_n \geq 0$. Let $A(x) = \sum_{n \leq x} a_n$.
If $\int_1^\infty \frac{A(x)-x}{x^2} dx < \infty$ then $A(x) \sim x$, an $x \to \infty$.

Proof: Suppose not, ie $\exists\ q \ni A(x_i) \geq qx_i\ \forall\ x_i$
Then

$$\int_{x_i}^{qx_i} \frac{A(t)-t}{t^2} dt \geq \int_{x_i}^{qx_i} \frac{A(x_i)-t}{t^2} dt \geq \int_{x_i}^{qx_i} \frac{q(x_i)-t}{t^2} dt$$

Set $t = x_i u$, this gives us

$$\int_{x_i}^{qx_i} \frac{q(x_i)-t}{t^2} dt = \int_1^q \frac{q-u}{u^2} du = c(q) > 0$$

But, $qx_i \leq \infty \implies \int_{x_i}^{qx_i} \frac{A(t)-t}{t^2} dt \leq \epsilon$, A contradiction.

4.3 Lemma 2

Suppose $a_n \geq 0 \quad A(x) = \sum_n a_n$. If the Dirichlet series $\mathfrak{D} = \sum_{n=1}^\infty \frac{a_n}{n^s}$ converges absolutely for $\mathrm{Re}(s) > 1$, and admits an analytic continuation for $\mathrm{Re}(s) \geq 1$ except for a simple pole at $s = 1$,then $A(x) \sim x$ as $x \to \infty$.

Proof: We have

$$\mathfrak{D} = s \int_1^\infty \frac{A(x)}{s^{x+1}} dx \text{ (from section 3.2)}$$

Now,

$$\mathfrak{D}(s) - \frac{s}{s-1} = s \int_1^\infty \frac{A(x)-x}{x^{s+1}} dx \implies \frac{\mathfrak{D}(s+1)}{(s+1)} - \frac{1}{s} = \int_1^\infty \frac{A(x)-x}{x^{s+2}} dx$$

Let $x = e^t$,

$$\frac{\mathfrak{D}(s+1)}{(s+1)} - \frac{1}{s} = \int_0^\infty \frac{(A(e^t) - e^t)e^t}{e^{t(s+2)}} dt = \int_0^\infty \frac{(A(e^t) - e^t)e^{-st}}{e^{-t}} dt$$

Applying Theorem X, we get the result desired.

4.4 Prime Number Theorem(PNT)

Let $\pi(x)$ =primes $\leq x$ or in other words $\sum_{p\leq x} 1$. This function is called the prime counting function. Example: $\pi(17) = 7$,$\pi(83) = 24$

PNT states that $\pi(x)$ and $x/\ln x$ are asymptotically equivalent ie

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

4.4.1 Proof

The integral $\int_0^\infty e^{-sx}\psi(e^x)\,dx$ converges for $\mathrm{Re}(s) > 1$ and equals $-\frac{\zeta(s)}{s\zeta(s)}$. the function $s \mapsto -\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$ has a continuous extension to $\mathrm{Re}(s) \geq 1$.

Also, $\Lambda \geq 0$, the function $\psi(x) = \sum_{n\leq x} \Lambda(n)$ is non-decreasing.

Now Theorem X gives $\psi(e^x) \sim e^x$ as $x \to \infty$, and therefore $\psi(x) \sim x$. Since we showed $\psi(x) \sim x$, $\psi(x) \sim x \implies \pi(x) \sim x/\ln x$,
because

$$\psi(x) = \sum_{n\leq x} \Lambda(n) = \sum_{p\leq x} \log p \leq \log x \sum_{p\leq x} 1 = \log(x)\pi(x)$$

.Dividing by x on both sides gives us (3) Consider $S(x)/x$,

$$\sum_{x^{1-\epsilon}\leq p\leq x} \ln p \geq \ln(x^{1-\epsilon})(\pi(x) - \pi(x^{1-\epsilon})(\epsilon \in (0,1)$$

Rearraging gives ,

$$\psi(x) + (1-\epsilon)(\ln(x^{1-\epsilon}) \geq \psi(x) + (1-\epsilon)(\ln(x))(\pi(x^{1-\epsilon}) \geq (1 - \epsilon\ln(x)\pi(x)$$

Dividing by x and taking limit gives us, $1 \geq \lim_{x\to\infty}(1-\epsilon)\frac{\pi(x)}{x/\ln x}$(Here $\lim_{x\to\infty} \frac{\psi(x)}{x}$ =1 proved above).Since ϵ was arbitrary $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$.

5 Modular Forms

The modular group, sometimes denoted $\Gamma(1)$, is

$$SL(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}, ad-bc=1 \right\}.$$

The upper half plane is $\mathfrak{h}^2 = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. We can define an action of $\Gamma(1)$ on $\mathfrak{h}^2$ as follows

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{a\tau + b}{c\tau + d}.$$

Lemma: Let $f = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$. Then,$\mathrm{Im}(fz) = \frac{\mathrm{Im}(z)}{|cz+d|^2}$.

Proof. Observe that

$$\begin{aligned} f(z) &= \frac{az+b}{cz+d} \\ &= \frac{(az+b)(d+c\bar{z})}{|cz+d|^2} \\ &= \frac{bd + ac|z|^2 + Re(z)(ad+bc) + i(ad-bc)\,\mathrm{Im}(z)}{|cz+d|^2} \\ &= \frac{bd + ac|z|^2 + \mathrm{Re}(z)(ad+bc) + i\,\mathrm{Im}(z)}{|cz+d|^2} \end{aligned}$$

Hence, $\mathrm{Im}(fz) = \frac{\mathrm{Im}(z)}{|cz+d|^2}$.

Definition: A modular form of weight k for the modular group

$$SL(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}, ad-bc=1 \right\}$$

is a complex-valued function f on the upper half-plane
$\mathfrak{h}^2 = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, satisfying the following three conditions:

1. f is a holomorphic function on $\mathfrak{h}^2$.
2. For any $z \in \mathfrak{h}^2$ and any matrix in $SL(2,\mathbb{Z})$ as above, we have:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

3. As $z \to i\infty$, $f(z)$ is bounded.

Thereom: $SL(2,\mathbb{Z})$ is generated by S and T where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Proof: Observe that $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, $n \in \mathbb{Z}$.

$$T^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}$$

and $S^2 = -I$.

$$S \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \cdots (\alpha)$$

If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$

Case (1):Suppose $c = 0$

$$ad = 1 \Rightarrow a = d = \pm 1 \implies g = \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{cases} T^{b'} \\ \text{or} \\ S^2 T' \end{cases}$$

Case (2): Suppose $c \neq 0$. WLOG, we can suppose $|a| \geq |c|$ (in terms of (α)). By the division algorithm we can wite $a = cq + r \quad 0 \leq r < |c|$

$$T^{-q} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
$$= \begin{pmatrix} a - c_1 & b - qd \\ c & d \end{pmatrix}$$

Repeating this in an iterative procedure which after a finite number of steps leads to case 1.

5.1 Example

Let $s > 2$ be an even integer. Then the Eisenstein series of weight s is a function on $\mathfrak{h}^2$, defined, for $z \in \mathfrak{h}^2$, by

$$G(z,s) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{0,0\}} \frac{1}{(mz+n)^s}$$

5.2 Fundamental domain

Fundamental domain for the upper halfplane $\mathfrak{h}^2$ under the action of $SL(2,\mathbb{Z})$ is a set $\mathscr{F}$ containing the representative of each orbit of $\mathfrak{h}^2$ under $SL(2,\mathbb{Z})$.

Lemma: Fix $z \in \mathfrak{h}^2$. The set $(m,n) \in \mathbb{Z}^2 \setminus (m,n) \neq (0,0)$ such that $|mz+n| \leq 1$ is finite and non empty.

Proof: Let $z = x + iy, |mz + n| \leq 1 \iff (mx + n)^2 + (my)^2 \leq 1 \implies (my)^2 \leq 1 \implies |m| < \frac{1}{\sqrt{y}}$, m is bounded.
Also $|mz + n| \leq \implies -1 \leq mz + n \leq \implies -1 - mx \leq n \leq 1 - mx$,n is bounded. Also, substituting $(m, n) = (0, 1)$ is example of it being non empty.

Claim: Every $\Gamma(1)$ -orbit in $\mathfrak{h}^2$ has a representative in

$$\mathscr{F} = \left\{ z \in \mathfrak{h}^2 : |z| \geq 1, |\operatorname{Re}(z)| \leq \frac{1}{2} \right\}$$

where $\mathscr{F}$ is the fundamental domain for $SL(2, \mathbb{Z})$ acting on $\mathfrak{h}^2$.

Proof: Let $\gamma = \begin{pmatrix} k & l \\ m & n \end{pmatrix} \in SL_2(\mathbb{Z})$.

$$\operatorname{Im}(\gamma z) = \frac{\operatorname{Im}(z)}{|mz + n|^2}$$

As $(m, n) \neq (0, 0)$,we see that $|mz + n|$ attains a minimum as γ varies over $SL(2, \mathbb{Z})$ (using lemma) .Now choose $|mz + n|$ to be minimina l, therefore $\operatorname{Im}(\gamma z)$ is maximal for $\gamma \in SL_2(\mathbb{Z})$
By translation we can ensure $|x| \leq \frac{1}{2}$

Now we claim $\gamma z \geq 1$. Suppose not, ie $\gamma z < 1$. Consider $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ where S acts on γz to yield $S(\gamma z) = \frac{-1}{\gamma z}$, Also

$$\operatorname{Im}(\frac{-1}{\gamma z}) = \frac{\operatorname{Im}(\gamma z)}{|\gamma z|^2}$$

Therefore,

$$\operatorname{Im}(S\gamma z) = \frac{\operatorname{Im}(\gamma z)}{|\gamma z|^2} > \operatorname{Im}(\gamma z) \quad (\gamma z < 1)$$

Contradiction! (as $\operatorname{Im}(\gamma z)$ was assumed to be maximal).

6 Non-Holomorphic Eisenstein series

Definition: Let $z \in \mathfrak{h}^2, \Re(s) > 1$. We define the Eisenstein series.

$$E(z,s) := \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n)=1}} \frac{y^s}{|mz+n|^{2s}}$$

where $\mathfrak{h}^2 = GL(2,\mathbb{R})/(O(2,\mathbb{R})$, and $GL(2,\mathbb{R})$ is the symmetric space and $O(2,\mathbb{R})$ is the rotation space.

6.1 Convergence

$$E(z,s) = E_s(z) = \frac{1}{2} \sum_{gcd(m,n)=1} \frac{y^s}{|mz+n|^{2s}} = \frac{1}{2} y^s \sum_{gcd(m,n)=1} \frac{1}{\left[(mx+n)^2+(my)^2\right]^s}$$

Since E_s is $\Gamma(1)$ -invariant, it suffices to consider z in a fixed compact set X inside the usual fundamental domain

$$\left\{ z = x+iy \in \mathfrak{h}^2 : |z| \geq 1, -\frac{1}{2} \leq x \leq \frac{1}{2} \right\}$$

For such z,

$$(mx+n)^2+(my)^2 = \left(x^2+y^2\right)m^2+2x \cdot mn+n^2 \geq m^2-|mn|+n^2 \geq \frac{1}{2}\left(m^2+n^2\right)$$

Also, the sum over coprime (m,n) is mainly by the sum over all $(m,n) \neq (0,0)$. Thus,

$$\sum_{(m,n) \in \mathbb{Z} \setminus (0,0)} \frac{1}{\left(m^2+n^2\right)^{\operatorname{Re}(s)}}$$

Now for $\operatorname{Re}(s) > 1$, the function $f(m,n) = \frac{1}{m^2+n^2}$ is ≥ 0 and monotone decreasing. Therefore by integral criteria consider the integral

$$\iint_{\mathbb{Z}^2 \setminus (0,0) = D} \frac{dmdn}{(m^2+n^n)^s}$$

Let $m = r\cos\theta$ and $n = r\sin\theta$,
The Jacobian Matrix

$$\begin{aligned} J(r,\theta) = \frac{\partial(m,n)}{\partial(r,\theta)} &= \begin{vmatrix} m_r & m_\theta \\ n_r & n_\theta \end{vmatrix} \\ &= \begin{vmatrix} \cos\theta & -r\sin\theta \\ \sin\theta & r\cos\theta \end{vmatrix} = r. \\ &= r\cos^2\theta + r\sin^2\theta \end{aligned}$$

Therefore $dmdn = rdrd\theta$,

$$\iint_{D'} \frac{J(r,\theta)drd\theta}{r^{2s}} = \iint_{D'} r^{1-2s}drd\theta = \int \frac{r^{2-2s}}{2-2s}d\theta = \frac{\theta \cdot r^{2-2s}}{2-2s}\bigg|_{D'}$$

which converges for all $\mathrm{Re}(s) > 1$ and how r is defined.

6.2 Theorem

The Eisenstein series $E(z,s)$ has the Fourier expansion

$$E(z,s) = y^s + \phi(s)y^{1-s} + \frac{2\pi^s\sqrt{y}}{\Gamma(s)\zeta(2s)}\sum_{n\neq 0}\sigma_{1-2s}(n)|n|^{s-\frac{1}{2}}K_{s-\frac{1}{2}}(2\pi|n|y)e^{2\pi inx}$$

where

$$\phi(s) = \sqrt{\pi}\frac{\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)}\frac{\zeta(2s-1)}{\zeta(2s)}$$

and

$$\sigma_s(n) = \sum_{\substack{d|n \\ d>0}} d^s,$$

and

$$K_s(y) = \frac{1}{2}\int_0^\infty e^{-\frac{1}{2}y\left(u+\frac{1}{u}\right)}u^s\frac{du}{u}.$$

I will show

$$\phi(s) = \sqrt{\pi}\frac{\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)}\frac{\zeta(2s-1)}{\zeta(2s)}$$

Proof: First note that

$$\zeta(2s)E(z,s) = \zeta(2s)y^s + \sum_{c>0}\sum_{d\in\mathbb{Z}}\frac{y^s}{|cz+d|^{2s}}$$

If we let $\delta_{n,0} = \begin{cases} 1 & n=0 \\ 0 & n\neq 0, \end{cases}$ and $d = mc + r$, it follows that

$$\zeta(2s)\int_0^1 E(z,s)e^{-2\pi inx}dx$$

This gives us

$$= \zeta(2s)y^s\delta_{n,0} + \sum_{c=1}^\infty c^{-2s}\sum_{r=1}^{c}\sum_{m\in\mathbb{Z}}\int_0^1 \frac{y^s e^{-2\pi inx}}{\left|z+m+\frac{r}{c}\right|^{2s}}dx$$

Implying,

$$= \zeta(2s)y^s\delta_{n,0} + \sum_{c=1}^\infty c^{-2s}\sum_{r=1}^{c}\sum_{m\in\mathbb{Z}}\int_{m+\frac{r}{c}}^{1+m+\frac{r}{c}} \frac{y^s e^{-2\pi in\left(x-\frac{r}{c}\right)}}{|z|^{2s}}dx$$

$\Longrightarrow$

$$= \zeta(2s) y^s \delta_{n,0} + \sum_{c=1}^{\infty} c^{-2s} \sum_{r=1}^{c} e^{\frac{2\pi i n r}{c}} \int_{-\infty}^{\infty} \frac{y^s e^{-2\pi i n x}}{(x^2+y^2)^s} dx$$

$\therefore$

$$\zeta(2s) \int_0^1 E(z,s) e^{-2\pi i n x} dx = \zeta(2s) y^s \delta_{n,0} + \sigma_{1-2s}(n) y^{1-s} \int_{-\infty}^{\infty} \frac{e^{-2\pi i n x y}}{(x^2+1)^s} dx$$

Dividing both sides by $\zeta(2s)$

$$\int_0^1 E(z,s) e^{-2\pi i n x} dx = y^s \delta_{n,0} + \frac{\sigma_{1-2s}(n) y^{1-s} \int_{-\infty}^{\infty} \frac{e^{-2\pi i n x y}}{(x^2+1)^s} dx}{\zeta(2s)}$$

Now need to show ,

$$\phi(s) = \sqrt{\pi} \frac{\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)} \frac{\zeta(2s-1)}{\zeta(2s)}$$

Part (1) : $\sigma_{1-2s}(0) = \zeta(2s-1)$

Well, $\sigma_{1-2s}(n) = \sigma_s(n) = \sum_{\substack{d|n \\ d>0}} d^s$ therefore ,

$$\sigma_{1-2s}(0) = \sum_{\substack{d|0 \\ d>0}} d^{1-2s}$$

$\Longrightarrow$

$$\sigma_{1-2s}(0) = \sum_{\substack{d|0 \\ d>0}} d^{1-2s} = \sum_{d=1}^{\infty} d^{1-2s} = \sum_{d=1}^{\infty} \frac{1}{d^{2s-1}} = \zeta(2s-1)$$

Part (2) : $\int_{-\infty}^{\infty} \frac{e^{-2\pi i x y}}{(x^2+1)^s} dx = \begin{cases} \sqrt{\pi} \frac{\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)} & \text{if } y = 0 \\ \frac{2\pi^s |y|^{s-\frac{1}{2}}}{\Gamma(s)} K_{s-\frac{1}{2}}(2\pi|y|) & \text{if } y \neq 0 \end{cases}$

Consider the case when $y = 0$,

$$\begin{aligned} \Gamma(s) \int_{-\infty}^{\infty} \frac{e^{-2\pi i x y}}{(x^2+1)^s} dx &= \int_0^{\infty} \int_{-\infty}^{\infty} e^{-u-2\pi i x y} \left(\frac{u}{1+x^2}\right)^s dx \frac{du}{u} \ldots (a) \\ &= \int_0^{\infty} e^{-u} u^s \int_{-\infty}^{\infty} e^{-ux^2} e^{-2\pi i x y} dx \frac{du}{u} \ldots (b) \end{aligned}$$

Here (a) is such by the defintion of $\Gamma(s)$.
Plugging $y = 0$ in (b) gives us,

$$\Gamma(s) \int_{-\infty}^{\infty} \frac{1}{(x^2+1)^s} dx = \int_0^{\infty} e^{-u} u^s \underbrace{\int_{-\infty}^{\infty} e^{-ux^2} .1 dx}_{\text{A}} \frac{du}{u}$$

Consider the gaussian integral,

$$\int_{-\infty}^{\infty} e^{x^2}\,dx$$

Computing the above integral,

$$I^2 = \left(\int_{-\infty}^{\infty} e^{-x^2}\,dx\right)^2 = \int_{-\infty}^{\infty} e^{-x^2}\,dx \int_{-\infty}^{\infty} e^{-y^2}\,dy$$

$\implies$

$$I^2 = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-\left(x^2+y^2\right)}\,dxdy$$

Now let,

$$x = r\cos\theta, \quad y = r\sin\theta$$

therefore

$$r^2 = x^2 + y^2$$

$\implies$

$$I^2 = \int_0^{\infty}\int_0^{2\pi} e^{-r^2}\,rdrd\theta$$

$=$

$$= 2\pi \int_0^{\infty} re^{-r^2}\,dr$$

$=$

$$= 2\pi \int_{-\infty}^{0} \frac{1}{2}e^{s}ds \quad , s = -r^2$$

$=$

$$= \pi \int_{-\infty}^{0} e^{s}ds$$

$=$

$$= \pi\left(e^0 - e^{-\infty}\right)$$

$=$

$$= \pi$$

$=$

$$I = \sqrt{\pi}$$

Taking $x = \frac{m}{\sqrt{u}}$ in the gaussian integral gives us $A = \sqrt{\frac{\pi}{u}}$

Thereofore (b) becomes

$$\Gamma(s)\int_{-\infty}^{\infty} \frac{1}{\left(x^2+1\right)^s}dx = \int_0^{\infty} e^{-u}u^s\sqrt{\frac{\pi}{u}}\frac{du}{u}$$

=

$$\Gamma(s)\int_{-\infty}^{\infty}\frac{1}{(x^2+1)^s}dx=\int_0^{\infty}e^{-u}u^s\sqrt{\frac{\pi}{u}}\frac{du}{u}$$

=

$$\sqrt{\pi}\int_0^{\infty}e^{-u}u^{s-1-\frac{1}{2}}du$$

=

$$\Gamma(s-\frac{1}{2}) \implies \int_{-\infty}^{\infty}\frac{1}{(x^2+1)^s}dx=\frac{\Gamma(s-\frac{1}{2})}{\Gamma(s)}$$

Therefore,

$$\phi(s)=\sqrt{\pi}\frac{\Gamma\left(s-\frac{1}{2}\right)}{\Gamma(s)}\frac{\zeta(2s-1)}{\zeta(2s)}$$

7 Function fields

Let p power of a prime, $\mathbb{F}_p$ finite field .

Analogy between Number and Function fields:

$$\mathbb{Q} \sim \mathbb{F}_p(t)$$

$$\mathbb{Z} \sim \mathbb{F}_p[t]$$

$$p \text{ prime} \sim p(t) \text{ monic irreducible polynomial}$$

$$|n| = \mathbb{Z}/n\mathbb{Z} \quad \sim \quad |f| = \mathbb{F}_p[t]/(f) = p^{\deg f}$$

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \sim \quad \zeta_{\mathbb{F}_p[t]}(s) = \sum_{f \in \mathbb{F}_p[t]} \frac{1}{|f|^s}$$

Equation A:

$$\zeta_{\mathbb{F}_p[t]}(s) = \sum_{f \in \mathbb{F}_p[t]} \frac{1}{|f|^s} = \prod_{p \in \mathbb{F}_p[t]} {}_{\text{irred,monic}} \left(1 - \frac{1}{|p|^s}\right)^{-1}$$

Proof: By the division algorithm $f(t)$ can be expressed a product of irreducible polynomials. Also this factorisation is unique as if

$$f(t) = p_1(t)p_2(t) \cdots p_m(t) \text{ and } f(t) = q_1(t)q_2(t) \cdots q_n(t)$$

with $p_1(t), \ldots, p_m(t)$ and $q_1(t), \ldots, q_n(t)$ all irreducible. We then have

$$q_1(t)q_2(t) \cdots q_n(t) = p_1(t)\left(p_2(t) \cdots p_m(t)\right) \quad (1)$$

Thus

$$p_1(t) \mid q_1(t) \cdots q_n(t)$$

$p_1(t)$ must divide at least one of the $q_i(t)$. By reordering the $q_i(t)$ we can assume without loss of generality that $p_1(t) \mid q_1(t)$. But since $q_1(t)$ is by irreducible,

$$q_1(t) = c_1 p_1(t) \quad , \quad \text{for some } c_1 \in \mathbb{F}_p \quad (2)$$

Substituting (2) into the left hand side of (1) and then dividing both sides by $p_1(t)$ yields

$$c_1 q_2(t) \cdots q_n(t) = p_2(t)\left(p_3(t) \cdots p_m(t)\right)$$

Repeating gives us,

$$c_1 c_2 q_3(t) q_4(t) \cdots q_n(t) = p_3(t)p_4(t) \cdots p_m(t) \quad (3)$$

We can continue in this manner to remove irreducible factors from both sides of (3). This yields us,

$$c_1c_2c_3\cdots = p_{m+1}(t)p_{m+2}(t)\cdots p_n(t)$$

But the left side are constants and right monic polynomials. Contradiction.

Now back to A, Expand the terms on the right into a geometric sum. Since each $f \in \mathbb{F}_p[t]$ has a unique factorisation and can be written uniquely as a product of monic irreducible polynomials. Every monic polynomial f will appear as a product of these geometric sums. Q.E.D

Equation B:

$$\zeta_{\mathbb{F}_p[t]}(s) = \sum_{n=0}^{\infty} \frac{\text{\# of monic polys of deg } n}{p^{ns}} = \frac{1}{1-p^{1-s}}$$

Proof: In the expansion of the left side of equation A, we can reorder the expansion and grouping degree n terms together.
Claim: There are exactly p^n terms of degree n in $\mathbb{F}_p[t]$. Proof: Take the case where $n = 2$ ie quadratic polynomial. The polynomial is of the form $x^2 + bx + c$ and b and c can take values $\{0, 1, 2, \cdots p-1\}$. Therefore all the possible values/combinations of b and c are p^2. Similarly with the other cases.
Now equation B, we can write

$$\zeta_{\mathbb{F}_p[t]}(s) = \sum_{n=0}^{\infty} \sum_{\deg(F)=n} \frac{1}{p^{ns}} = \sum_{n=0}^{\infty} \frac{p^n}{p^{ns}} = \frac{1}{1-p^{1-s}},$$

Q.E.D

Equation C:
The completed zeta function in $\mathbb{F}_p[t]$ is defined as

$$\xi(s) = \frac{1}{1-p^{-s}}\zeta_{\mathbb{F}_p[t]}(s)$$

then

$$\xi(s) = p^{2s-1}\xi(1-s)$$

Proof: Well the left side is just

$$\frac{1}{1-p^{-s}} \cdot \frac{1}{1-p^{1-s}}$$

by def of ξ. The right side after some calculations becomes,

$$p^{2s-1}\frac{1}{1-p^{s-1}} \cdot \frac{1}{1-p^{s}}$$

By multiplying the left side by p^{2s-1} and after some simplifications the LH=RH=

$$\frac{p^{2s-1}}{p^{2s-1} - p^{s-1} - p^s + 1}$$

Q.E.D

7.1 Ideals

Ideals in $\mathbb{F}_p[t]$: Given any polynomial $f(t) \in \mathbb{F}_p[t]$ let
$(f) := \{g(t)f(t) \mid g(t) \in \mathbb{F}_p[t]\}$. The same is analogous in $\mathbb{Z}$ where (n) is multiples of n.

Analogy in $\mathbb{F}_p[t]$,

$$\mathbb{F}_p[t]/(f) := \{\bar{0}, \bar{t}, \cdots \bar{t}^{n-1}\}$$

Where f monic,$|f| = p^{\deg f}$,$\deg f = n$,$\bar{t^i} = t^i + (f)$

Check: $\bar{i}\,\bar{j} = \overline{ij}$and $\bar{i} + \bar{j} = \overline{i+j}$

Proof: Let $i, j \in \mathbb{Z}$ for simplification. It translates to the $\mathbb{F}_p[t]$ case in the same way. Now,

$$\bar{i} = \{i + n \mid i, n \in \mathbb{Z}\} \text{ and } \bar{j} = \{i + n \mid j, n \in \mathbb{Z}\}$$

Therefore,

$$\bar{i} + \bar{j} = i + j + n \bmod n = \overline{i+j}$$

Similarly,

$$\bar{i}\,\bar{j} = ij + in + jn + n^2 \bmod n \equiv ij + n \bmod n = \overline{ij}$$

$\mathbb{F}_p[t]/(f)$ is a ring as all the properties of the ring $\mathbb{F}_p[t]$ just carry over to $\mathbb{F}_p[t]/(f)$ as its operations over the representatives.

Claim:If $f(t)$ is irreducible and monic then $\mathbb{F}_p[t]/(f)$ is a field.

To show this I will first show, if
$\gcd(f, g) = 1$ then there exists $p(t)$ and $q(t)$ such that $f.p + q.g = 1$
Proof:

$$\text{Let } m(t) = \gcd(f, g)$$
$$\text{Then } m(t) \mid f \text{ and } m(t) \mid g \Rightarrow$$
$$m(t)|fp, m(t)|gq \text{ and } m(t)|fp + qg = 1 \Rightarrow m(t)|1 \Rightarrow m(t) = 1$$

Back to the claim,
Proof: It is sufficient to show that any arbitrary element
$(g(t)) + d(t) \in \mathbb{F}_p[t]/(f)$ has an inverse ie $((g(t)) + d(t)).h(t) = 1$
Now consider $d(t) \ni d(t) \notin (g(t))$, therefore $\gcd(g, d) = 1$. By claim,

$$\exists b(t), a(t) \ni g(t)a(t) + d(t)b(t) = 1$$

Rearranging,

$$d(t)b(t) = (-q(t))a(t) + 1 \in (q(t)) + 1.$$

Thus

$$((q(t) + d(t))((q(t)) + b(t)) = (q(t) + d(t)b(t) = (q(t)) + 1$$

Therefore $((q(t) + d(t))$ is invertible . Since $((q(t) + d(t))$ was arbitrary it shows that $\mathbb{F}_p[t]/(f)$ is a field. Q.E.D

7.2 Quadratic reciprocity

Take $f, g \in \mathbb{F}_p[t]$ monic, square free and relatively prime. Then

$$\left(\frac{f}{g}\right) = \left(\frac{g}{f}\right)$$

where (.) is the Legendre symbol defined as

$$\left(\frac{f}{g}\right) = g^{\frac{|f|-1}{2}}\ (\mathrm{mod} f) = \chi_f(g),\ |f| = p^{\deg f}$$

7.2.1 Fermat's Little theorem:

If p is a prime number then $a^p \equiv a(\mathrm{mod} p)$ for all $a \in \mathbb{Z}$.

Proof: We will work over the $\mathbb{Z}/n\mathbb{Z}$ field to make the calculations simpler. If $a = 0$, then we clearly have $a^p \equiv a \mod p$. So we assume that $a \neq 0$. Then $\bar{a} = a + (p) \in (\mathbb{Z}/p\mathbb{Z})$. Let H be a subgroup of $(\mathbb{Z}/p\mathbb{Z})$ generated by $\bar{a}$. Then the order of the subgroup H is the order of the element $\bar{a}$. By Lagrange's Theorem, the order $|H|$ divides the order of the group $(\mathbb{Z}/p\mathbb{Z})$, which is $p - 1$. So we write $p - 1 = |H|m$ for some $m \in \mathbb{Z}$. Therefore, we have

$$\bar{a}^{p-1} = \bar{a}^{|H|m} = \bar{1}^m = \bar{1}$$

Multiplying both sides by a gives us the desired result. Q.E.D

Claim:

$$\left(\frac{f}{g}\right) \equiv g^{\frac{|f|-1}{2}}\ (\mathrm{mod} f)\ = \pm 1,\ \text{when}\ \gcd(f, g) = 1$$

Proof: From the analog of Fermat's Little theorem, we get

$$g^{|f|-1} \equiv 1 \bmod f,\ \text{hence}\ 0 \equiv g^{|f|-1} - 1 = \left(g^{(|f|-1)/2} - 1\right)\left(g^{(|f|-1)/2} + 1\right),$$

and since f is irreducible,monic we conclude that $g^{(|f|-1)/2} \equiv \pm 1 \bmod f$.

7.3 L-series

For f monic and square-free, define the L -series:

$$L(s,\chi_f) = \prod_{p(t)\text{monic,irred}} \left(1 - \frac{\chi_f(p)}{|p|^s}\right)^{-1}$$
$$= \sum_{g\text{ monic},g(t)\neq 0} \frac{\chi_f(g)}{|g|^s}$$

Completed L -series by

$$L^*(s,\chi_f) = \begin{cases} \frac{1}{1-p^{-s}} L(s,\chi_f) & \text{if deg } f \text{ even} \\ L(s,\chi_f) & \text{if deg } f \text{ odd.} \end{cases}$$

Functional equation:

$$L^*(s,\chi_f) = \begin{cases} p^{2s-1}|f|^{1/2-s} L^*(1-s,\chi_f) & \text{if deg } f \text{ even} \\ p^{2s-1}(p|f|)^{1/2-s} L^*(1-s,\chi_f) & \text{if deg } f \text{ odd.} \end{cases}$$

Proposition: Let χ be a non-trivial Dirichlet character modulo f. Then, $L(s,\chi_f)$ is a polynomial in p^{-s} of degree at most $\deg(f) - 1$.

Proof. Define

$$A(n,\chi_f) = \sum_{\deg(g)=n} \chi(g)$$

f monic It is clear from the definition of $L(s,\chi)$ that

$$L(s,\chi_f) = \sum_{n=0}^{\infty} A(n,\chi)p^{-ns}.$$

if we can show that $A(n,\chi) = 0$ for all $n \geq \deg(f)$ then the result will holds. Let's assume that $n \geq \deg(m)$. If $\deg(g) = n$, we can write $g = hf + r$ where r is a polynomial of degree less than $\deg(f)$ or $r = 0$. Here, h is a polynomial of degree$= n - \deg(f) \geq 0$. All monic polynomials of degree $n \geq \deg(f)$ can be uniquely written in this fashion. Since χ is periodic modulo f and since h can be chosen in $p^{n-\deg(f)}$ ways, we have

$$A(n,\chi_f) = p^{n-\deg(f)} \sum_r \chi(r) = 0$$

by the orthogonality relation since $\chi \neq \chi_o$, and the sum is over all r with $\deg(r) < \deg(f)$.

7.3.1 Proof of functional equation

Consider $\deg f$ to be odd.

Therefore,

$$L^*(s,\chi_f) = \prod_{j=1}^{\deg f-1}\left(1-\frac{\pi_j}{p^s}\right)$$

$=$

$$(-\frac{\pi_{\deg f-1}}{p^s})^{\deg f-1}\prod_{j=1}^{\deg f-1}\left(1-\frac{1}{\frac{\pi_j}{p^s}}\right)$$

$=$

$$(-1)^{\deg f+1-2}(\frac{\pi_{\deg f-1}}{p^s})^{\deg f+1-2}L^*(1-s,\chi_f)$$

$=$

$$p|f|^{\frac{1}{2}-s}(\frac{p^{2s}}{p})L^*(1-s,\chi_f)$$

(as $|\pi| = p^{\frac{1}{2}}$ and $(-1)^{\deg f+1-2} = 1$ since $\deg f = 2m \pm 1 \implies -1^{2m\pm 2} = 1$

Consider $\deg f$ to be even.

$$L(s,\chi_f) = (1-p^{-s})L^*(s,\chi_f) = (1-p^{-s})\prod_{j=1}^{\deg f-2}\left(1-\frac{\pi_j}{p^s}\right)$$

$=$

$$(1-p^{-s})(-\frac{\pi_{\deg f-2}}{p^s})^{\deg f-2}\prod_{j=1}^{\deg f-2}\left(1-\frac{1}{\frac{\pi_j}{p^s}}\right)$$

$=$

$$(1-p^{-s})(-1)^{\deg -2}(\frac{\pi_{\deg f-2}}{p^s})^{\deg f-2}L^*(1-s,\chi_f)$$

$=$

$$(1-p^{-s})|f|^{\frac{1}{2}-s}(\frac{p^{2s}}{p})L^*(1-s,\chi_f)$$

Q.E.D

8 Multiple dirichlet series

Define an additive character on K_∞. First let e_0 be a nontrivial additive character on $\mathbb{F}_p$. Use this to define a character $e_\star$ of $\mathbb{F}_q$ by $e_\star(a) = e_0\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\, a\right)$. Let ω be the global differential dx/x^2. Finally define the character e of K_∞ by $e(y) = e_\star\left(\mathrm{Res}_\infty(\omega y)\right)$ for $y \in K_\infty$. Note that

$$\{y \in K : e \mid y\mathcal{O} = 1\} = \mathcal{O}$$

Fix an embedding ϵ from the the n^{th} roots of unity of $\mathbb{F}_q$ to $\mathbb{C}^\times$. For $r, c \in \mathcal{O}$ we define the Gauss sum

$$g(r, \epsilon, c) = \sum_y \epsilon\left(\left(\frac{y}{c}\right)\right) e\left(\frac{ry}{c}\right).$$

For $x, y \in K_\infty$ we write $x \sim y$ if $x/y \in K_\infty^{\times n}$.
Define the Dirichlet series

$$\psi(r, \epsilon, \eta, s) = \left(1 - q^{n-ns}\right)^{-1} \sum_{\substack{c \in \mathcal{O}\ m \\ c \sim^{\eta n}_{\eta}}} g(r, \epsilon, c)|c|^{-s}$$

where the sum is over all nonzero monic polynomials $c \sim \eta$ and $|c|$ is $q^{\deg c}$. The η we will use are of the form $\pi_\infty^{-i}, 0 \le i < n$.

A Basic Topology

A.1 Heine-Borel Theorem

A.1.1 Set of Measure Zero

A subset $N \subseteq \mathbb{R}$ is called a set of measure zero, if for very $\varepsilon > 0$ there are (at most) countably infinitely many open intervals $I_1, I_2, \ldots$ such that $N \subseteq I_1 \cup I_2 \cup \ldots$, and such that $|I_1| + |I_2| + \cdots = \sum_{k=1}^{\infty} |I_k| < \varepsilon$

Here for any interval I of the form $(a, b), [a, b], (a, b], [a, b)$ we put $|I| = b - a$.

Lemma.
1. Subsets of a zero set are zero sets.
2. Any finite or countable union of zero sets is again a zero set.

Proof. 1.Any open cover of a set of of measure zero is also an open cover of any subset.
2 .The case of a finite union is covered by the case of a countably infinite union. Let Z_k ($k \in \mathbb{N}$) be a countably infinite collection of sets of measure zero, and let $\varepsilon > 0$. Then for each k, Z_k may be covered by a countably infinite union of open intervals $I_{k\ell}$ such that

$$\sum_{\ell=1}^{\infty} |I_{k\ell}| < \frac{\varepsilon}{2^k}$$

Let $Z = \bigcup_{k=1}^{\infty} Z_k$. Then $Z \subseteq \bigcup_{k=1}^{\infty} \cup_{\ell=1}^{\infty} I_{k\ell} = \{x \in \mathbb{R} \mid \exists k, \ell : x \in I_{k,\ell}\}$.
By the Cauchy Double Series Theorem $\sum_{k,\ell=1}^{\infty} |I_{k\ell}| = \sum_{k=1}^{\infty} \sum_{\ell=1}^{\infty} |I_{k\ell}| \implies$
Now $\sum_{k=1}^{\infty} \sum_{\ell=1}^{\infty} |I_{k\ell}| \leq \sum_{k=1}^{\infty} \frac{\varepsilon}{2^k} = \varepsilon \left(\frac{1}{1 - \frac{1}{2}} - 1 \right) = \varepsilon$. But, $\sum_{\ell=1}^{\infty} |I_{1\ell}| < \frac{\varepsilon}{2}$.
Thus, Z is a set of measure zero.

A.1.2 Open cover

If $S \subseteq \mathbb{R}$ is any subset, an open cover or open covering of S is a family $\{U_i\}_{i \in I}$ of open sets $U_i \subseteq \mathbb{R}$ such that $S \subseteq \bigcup_{i \in I} U_i = \{x \in \mathbb{R} \mid \exists i : x \in U_i\}$

A.1.3 Compact set

A subset $K \subseteq \mathbb{R}$ is called compact, if every open covering has a finite subcover, ie,

$$K \subseteq \bigcup_{i \in I} U_i$$

then there are $i_1, i_2, \ldots, i_n \in I$ such that

$$K \subseteq U_{i_1} \cup U_{i_2} \cup \ldots \cup U_{i_n}$$

A.1.4 Theorem Heine-Borel

A subset K of $\mathbb{R}$ is compact if and only if K is bounded and closed.

A.2 Topological space

Let $X \neq \emptyset$. A topology on X is a collection of open subsets of X which satisfy the following-
(1) $X, \emptyset$ are open.
(2) The union of any family of open sets is open.
(3) The finite intersection of any collection of open sets is open.

Suppose, $\tau = \{$ all open subsets of X$\}$. Then a topological space is a pair (X, τ).

A.3 Manifolds

A subset $S \subseteq \mathbb{R}$ is called open if for every $x \in s$, there is $\varepsilon > 0$ such that $(x - \varepsilon, x + \varepsilon) \subseteq U$. A subset $S \subseteq \mathbb{R}$ is closed, if for every convergent sequence $a_n \in S$ we have $\lim a_n \in S$.

A.3.1 Homeomorphism

A continuous map $\phi : X \to Y$ is a homeomorphism if its bijective and ϕ^{-1} exists. Homeomorphism is a continuous function between topological spaces that has a continuous inverse function.

A.3.2 Covering space

A covering space of X is a topological space C together with a continuous surjective map:$p : C \to X \ni \forall\, x \in X \;\exists$ an open neighborhood U of $x \ni p^{-1}(U)$ is a union of disjoint open sets in C, each of which is mapped homeomorphically onto U by p.

A.3.3 Haussdorffness

A space X is Hausdorff if
$\forall\, x, y \in X \ni x \neq y \;\exists\, U, V \subseteq X$ open $\;\ni x \in U, y \in V$ and $U \cap V = \emptyset$

Lemma: A compact subset $K \subseteq X$ of a Hausdorff space X is closed.

Proof: Pick $y \in X \backslash K$. Each $x \in K$ gives us $x \in U$ and $y \in V \ni U \cap V = \emptyset$ As K is compact, $\exists$ finite set $\{x_i\}_{i \in I} \subseteq K \ni K = \bigcup_{i \in I} U_i$ Then $\bigcap_{i \in I} V_i$ is open & disjoint from $K \Rightarrow K$ closed as each y is contained in an open set disjoint from K

A.3.4 Second countable

Let S be a set.S is countable if and only if there exists a bijection between S and a subset of $\mathbb{N}$. A countable basis for a topology X is a basis for X which is a countable set. X is called second countable if it has a countable basis.

A.3.5 Atlases

A chart is a pair of an open set and a homeomorphism (U, ϕ) that maps elements locally around a point say x of an open set in a manifold to $\mathbb{R}^n$.
An atlas for a topological space is a collection of charts on a topological space X which covers X. If the co-domain of each chart is the $n - dim$ euclidean space (basic coordinate system) then X is said to be a $n - dim$ manifold.

A.3.6 Topological manifold

A topological manifold is a topological space that is Hausdorff and every point possess an open neighbourhood homeomorphic to $\mathbb{R}^n$.(locally similar to $\mathbb{R}^n$- we can map a point of the manifold onto the $\mathbb{R}^n$ plane)

B Groups

B.1 Sub groups

A Subgroup is a subset which is also a group. H is a subgroup of G denoted by $H \leq G$. Two standard subgroups of G are G and the trivial group = {e} where e is the identity element.

B.1.1 Cosets

For a subgroup H and some a in $G \setminus H$, we define the left coset $aH = \{ah : h \in H\}$ and the right coset $Ha = \{ha : h \in H\}$.

If G is partitioned into k cosets (where each coset has same size denoted by $|H|$) we say the index of G is k. Therefore, $|H| \cdot k = |G|$, which is Langrange's theorem. Claim (1):if $aH = \{ah : h \in H\}$ then $aH \cap bH = \emptyset \vee aH = bH$.

Proof: Suppose $ah_1 = bh_2 \implies ah = bh_2h_1^{-1}h \in H$ where h arbitrary element in H. The right side belongs to H as closed under multiplication (H subgroup).
Thereofore ,

$$\forall ah \in aH : ah \in bH$$

giving us

$$aH \subseteq bH$$

Similarly with the other implication. Also $|aH| = |H|$ as consider two elements $ah_1 = ah_2$ multiplying by a^{-1} yields the required result.

B.1.2 Langrange's theorem

Lagrange's Theorem: If $H \leq G$, then $|H|$ divides $|G|$.

Proof: The case where subsets are {e} and G are trivial. Now suppose G is a finite group with $|G| = n$ Case : $H < G$ and $H \neq \{e\}$ Construction: Pick $a_1 \in G$ not in H. Now consider $a_1H = \{a_1 \cdot h \; \forall \; h \in H\}$(left coset) $\ni H \bigcap a_1H = \emptyset$. Claim (2): H and a_1H have no element in common Assume there is an element in H and a_1H: This means $a_1 \cdot h_i = h_j$ for some h_i and h_j in H

$$\begin{aligned}
a_1 \cdot h_i &= h_j \\
(a_1 \cdot h_i) \cdot h_i^{-1} &= h_j \cdot h_i^{-1} \\
a_1 \cdot \left(h_i \cdot h_i^{-1}\right) &= h_j \cdot h_i^{-1} \\
a_1 \cdot e &= h_j \cdot h_i^{-1} \\
a_1 &= h_j \cdot h_i^{-1} \in H \Longrightarrow a_1 \in H
\end{aligned}$$

Contradiction! Similarly, consider $a_2H = \{a_2 \cdot h \; \forall \; h \in H\}$(left coset) $\ni H \bigcap a_1H \bigcap a_2H = \emptyset$. Repeat the process till G is divided into k such non-overlapping left cosets. Each coset has size $|H|$(by claim). Number of cosets $= k$ times size of each coset $|H| = |G|$ ie n. Therefore, $|H|$ divides $|G|$.

B.2 Orbits, representatives

Let $X = G$-set,
Definition: For $x \in X$, the G-orbit of $x \in X$ is $\quad G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X$

Orbit Decomposition
Theorem: Let $X = G$-set. Then X is partitioned into G-orbits. The set of G-orbits is denoted X/G.

Proof: Suffice show $x \sim g.x$ for $x \in X, g \in G$ defines an equivalence relation.
(1)$x \sim 1 \cdot x = x$
(2)$x \sim g \cdot x$ and $g \cdot x \sim g^{-1} \cdot (g \cdot x) = \left(g^{-1}g\right) \cdot x = 1 \cdot x = x$
(3)$x \sim g \cdot x, g \cdot x \sim h(g \cdot x)$ and $x \sim (h \cdot g) \cdot x = h \cdot (g \cdot x)$

A representative of an equivalence class is any element of X which belongs to that equivalence class. A complete set of representatives R is a list of elements of X such that you have a representative for each class. That is to say that any element of X will be equivalent to exactly one element of R.

B.3 Lie Groups

A differentiable manifold is a Hausdorff and second countable topological space X, together with a maximal differentiable atlas on X.

Let G be a topological group, with a differentiable manifold structure. If The group operation $* : G \times G \to G$ and the inverse operation $*^{-1} : G \to G$ are differentiable maps. G is a Lie Group

B.4 Symplectic groups

A compact (topological) group is a topological group whose topology is compact. A topological space X is said to be disconnected if it is the union of two disjoint non-empty open sets. Otherwise, X is said to be connected.

$Sp(2n, R)$-The symplectic group over the field of real numbers non-compact, connected, simple Lie group.

$Sp(2n, C)$-The symplectic group over the field of complex numbers is a non-compact, simply connected, simple Lie group.

B.5 Metaplectic groups

B.5.1 Cover group

A covering group of a topological group G is a covering space C of H such that C is a topological group and the covering map $p : C \to G$ is a continuous group homomorphism.

B.5.2 Double cover group

A topological double cover in which G has index 2 in C.

$Mp(2n)$**-The metaplectic group is a double cover of the symplectic group** $Sp(2n)$**.**

C Function field theory

C.1 Theory

C.1.1 Algebraic function field

If K is a subfield of L then we can view L as a field extension over K.We define $[L : K]$ = degree of extension :=$\dim_k L$. If the extension if a finite extension then for all elements in L each element can be represented as a K-basis of L.($\gamma = \sum_{i=0}^{n} a_i\beta_i, \beta_i \in K$)

Now suppose $\alpha \in L$, we say L is algebraic over K if $\exists f(x) \in K[x] \ni f(\alpha) = 0, f$ non trivial polynomial.Also, $\exists! p(x) \in K[x]$ monic irreducible polynomial in $K[x]$ s.t $p(\alpha) = 0 \Rightarrow p(x)$ is called the minimal poly of α.

L is called an **algebraic extension** over K if $\gamma \in L$ is algebraic over K.

$x \in L$ is transcendental over K if $\exists$ no polynomial $f(x) \in K[x] \ni f(x) = 0$

An algebraic function field over K is a field extension s.t. $\exists x \in L$ which is transcendental over K and $[L : K(x)] < \infty$

C.1.2 Discrete Valuation ring

Let F/K be a function field, a valuation ring θ of F/K is a subring of F such that:
(1)$K \subsetneq \theta \subsetneq F$.
(2)$\forall\alpha \in F, \alpha \in \theta \vee \alpha^{-1} \in F \vee$ both $z \in \theta^{\times}$is a unit.

Note: If θ is a valuation ring then $P := \theta \setminus \theta^{\times}$ is the unique maximal ideal.

A PID with unique max ideal is a discrete valuation ring.
Every element $t \in P \ni P = t\theta$ is called prime element for P.

C.1.3 Maximal Idea, PID

For an ideal P of a ring R it is maximal if the following equivalent conditions hold:
- There exists no other proper ideal J of R so that $P \subsetneq J$.
- For any ideal J with $P \subseteq J$, either $J = P$ or $J = R$.
-The quotient ring R/P is a simple ring.(a ring whose ideals are itself and zero)

Principal ideal is an ideal I in a ring$R$ that is generated by a single element a of R through multiplication by every element of R. An integral domain is a nonzero commutative ring in which the product of any two nonzero elements is nonzero. A PID or a principal ideal domain is an integral domain in which every ideal is principal.

C.2 Riemann Roch Theorem

C.2.1 Divisors

Consider the alg. extension of K over $F_p(x)$. Let P be the unique maximal ideal. Let K be a function field, and let $\mathcal{D}_K$ be the group of divisors of K, which is the free commutative group generated by the primes.A divisor is a finite sum

$$D = \sum_P a(P)P$$

where P are primes of K. A divisor D is said to be effective if $a(P) = \text{ord}_P(D) \geq 0$ for all P. We denote this by $D \geq 0$.
Let $a \in K^*$ (group of diviors of degree 0). The divisor of $a, (a)$,is defined to be $\sum_P$ ord $_P(a)P$ (coefficients- ord $_P(D)$). The degree of a divisor is defined as $\deg(D) = \sum_P a(P) \deg P$.The map $a \to (a)$ is a homomorphism from K^* to $\mathcal{D}_K$. The image of this map is called the group of principal divisors. Let

$$(a)_o = \sum_P \text{ord}_{ord_P(a)>0}(a)P \text{ and } (a)_\infty = - \sum_{ord_P(a)<0} \text{ord}_P(a)P.$$

The divisor $(a)_o$ is called the divisor of zeros of a and the divisor $(a)_\infty$ is called the divisor of poles of a. Also $(a) = (a)_o - (a)_\infty$.

C.2.2 Theorem

Definition. Let D be a divisor. Define $L(D) = \{x \in K \mid (x) + D \geq 0\} \cup \{0\}$. The dimension of $L(D)$ over F is denoted by $l(D)$. The number $l(D)$ is sometimes referred to as the dimension of D.them as ord $_P(D)$.Two divisors, D_1 and D_2, are said to be linearly equivalent, $D_1 \sim D_2$ if their difference is principal, i.e., $D_1 - D_2 = (a)$ for some $a \in K^*$.The divisor class group is the group of divisors modulo linear equivalence

Lemma If $\deg(D) \leq 0$ then $l(D) = 0$ unless $D \sim 0$ in which case $l(D) = 1$.
Proof. If $\deg(D) < 0$ and $x \in L(D)$, then $\deg((x) + D)$ is both < 0 and ≥ 0 which is a contradiction. If $\deg(D) = 0$ and $L(D)$ is not empty, let $x \in L(D)$. Then $(x) + D \geq 0$ and has degree zero, so it must be the zero divisor. Thus, $D \sim 0$. Conversely, if $D \sim 0$, then $l(D) = l(0) = 1$ since $L(0) = F$ because $x \in L(0)$ implies x has no poles.

Genus: The genus of the function field K is the integer g defined by

$$1 - g = \min_D(l(D) - \deg(D)),$$

where the minimum is taken over all divisors $D \in \text{Div}(C)$.
Theorem (Riemann-Roch) There is an integer $g \geq 0$ and a $\text{Div}(C)$ such that for $C \in \text{Div}(C)$ and $D \in \mathcal{D}_K$ we have

$$l(D) = \deg(D) - g + 1 + l(C - D)$$

Remarks: if we set $D = 0$ we get $l(C) = g$, if we set $C = 0$ we get $\deg(C) = 2g - 2$ and lastly If $\deg(D) \geq 2g - 2$, then $l(D) = \deg(D) - g + 1$.

Let h_k be the number of divisor classes of degree 0. For any divisor D, the number of effective divisors in $\mathrm{Div}(D)$ is $\frac{p^{l(D)}-1}{p-1}$ By remarks and theorem we get,if $\deg D = n > 2g - 2$, then $b_n = h_k \frac{p^{n-g+1}-1}{p-1}$.

C.3 Zeta function

The zeta function of $K, \zeta_K(s)$, is defined by

$$\zeta_K(s) = \sum_{\substack{D \in \mathcal{D}_K \\ D \geq 0}} |D|^{-s} = \prod_{P \in \mathcal{S}_K} \left(1 - |P|^{-s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{b_n}{q^{ns}}$$

where the sum runs over all divisors $D \in \mathcal{D}_K$, and the product over all primes $P \in \mathcal{S}_K$(set of all primes). (if $K = F_p(x)$ this is the completed zeta function)

By the definition of the completed zeta function and L-function :

$$L^*(s, \chi_D) := \frac{\zeta_K(s)}{\zeta_k(s)} = \left(1 - p^{-s}\right)^{-\lambda} L(s, \chi_D)$$

where

$$\lambda = \begin{cases} 1 & \deg D \text{ even} \\ 0 & \deg D \text{ odd} \end{cases}$$

C.3.1 Theorem

Let K be a function field over $\mathbb{F}_p$ of genus g. Then

$$\zeta_K(s) = \frac{P_K(p^{-s})}{(1 - p^{-s})(1 - p^{1-s})}$$

where $P_K(p^{-s})$ is a polynomial of degree $2g$.
Proof: Let b_n be the number of effective divisors of degree n in $\mathcal{D}_K$. Assume that for $n > 2g - 2$, we have

$$b_n = h_K \frac{p^{n-g+1} - 1}{p - 1}$$

Therefore $\zeta_K(s)$ becomes,

$$\zeta_K(s) = \sum_{n=0}^{2g} b_n p^{-sn} + \frac{h_K}{p-1} \left(\frac{p^g}{1 - p^{1-s}} - \frac{1}{1 - p^{-s}} \right) p^{-s(2g-1)}$$

by some manipulation we get,

$$\zeta_K(s) = \frac{P_K(p^{-s})}{(1 - p^{-s})(1 - p^{1-s})}$$

Q.E.D

C.3.2 Reimann Hypothesis for Function fields

Let K be a function field over $\mathbb{F}_p$. Then, all the roots of $\zeta_K(s)$ lie on the line $\mathrm{Re}(s) = 1/2$. Equivalently, the inverse roots of $P_K(p^{-s})$ have absolute value $\sqrt{p}$

Thus, the Riemann hypothesis for $\zeta_K(s) = Z_K\left(q^{-s}\right)$ translates into the statement that the inverse roots of $P_K\left(q^{-s}\right)$ have absolute value $\sqrt{p}$ writing

$$P_K(p^{-s}) = \prod_{j=1}^{\deg P_K} \left(1 - \frac{\pi_j}{p^s}\right)$$

as $\zeta_K(s) = 0 \Longleftrightarrow P_K\left(p^{-s}\right) = 0 \Longleftrightarrow p^{-s} = \pi_j^{-1},\ j = 1, \ldots, \deg P_K$

Then, if $\mathrm{Re}(s) = 1/2$, we have

$$\pi_j(K)^{-1} = p^{-1/2} p^{-i\,\mathrm{Im}(s)} \Longleftrightarrow |\pi_j|\, p^{1/2}, \quad j = 1, \ldots, \deg P_K$$

Remark: if $K = F_p(X)$,

$$\zeta_K(s) = \frac{P_K\left(p^{-s}\right)}{\left(1 - p^{-s}\right)\left(1 - p^{1-s}\right)}$$

=

$$\frac{\zeta_K(s)}{\zeta_k(s)} = \frac{P_K\left(p^{-s}\right)}{\left(1 - p^{-s}\right)}$$

and let $L(s, \chi) = P_K\left(p^{-s}\right)$.

D Multiple Dirichlet Series Theory

D.1 Additive characters of Finite fields

Let e_o be the additive character on $\mathbb{F}_p$ given by $e_o(j(\bmod p)) = \exp(2\pi i j/p)$.
We use this to define an additive character $e_\star$ on $\mathbb{F}_q$ by
$e_\star(x) = e_o\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)\right)$ (here $q = p^s$ (prime power))
By definition, each $\star \in \mathbb{F}_q$ induces the additive character $e_\star : \mathbb{F}_q \to \mathbb{C}^\times$ with

$$e_\star(x) = \exp\left(\frac{2\pi i \cdot \mathrm{Tr}_{q/p}(\star x)}{p}\right)$$

where $\mathrm{Tr}_{q/p}(x) = \sum_{i=0}^{s-1} x^{p^i}$ denotes the trace of F_q on F_p.

D.2 Terminology

Let $\mu_n = \{a \in \mathbb{F}_q : a^n = 1\}$ and let $\chi : \mathbb{F}_q^\times \to \mu_n$ be the character $a \mapsto a^{\frac{q-1}{n}}$. Let K be the rational function field $\mathbb{F}_q(t)$ with polynomial ring $\mathcal{O} = \mathbb{F}_q[t]$. We let $K_\infty = \mathbb{F}_q((t))$ denote the field of Laurent series in t^{-1} (the completion of K at the infinite place) Let deg denote the degree of an element of $\mathcal{O}$. We shall write π_∞ for t^{-1} when we consider the latter as an element of K_∞. Also, let $\mathcal{O}_{\text{mon}}$ denote the set of monic polynomials in $\mathcal{O}$. For $x, y \in \mathcal{O}$ relatively prime, $\left(\frac{x}{y}\right)$ denotes the n^{th} order power residue symbol. We have the reciprocity law

$$\left(\frac{x}{y}\right) = \left(\frac{y}{x}\right)$$

for x, y monic.

D.3 Differentials Rings

D.3.1 Places

A place of a number tield K is an equivalence class of absolute values on K.An absolute value is a notion to measure the size of elements x in K. Two absolute are considered equivalent if they give rise to the same notion of smallness. The equivalence relation between absolute values $|\cdot|_0 \sim |\cdot|_1$ is given by some $\lambda \in \mathbb{R}_{>0}$ such that $|\cdot|_0 = |\cdot|_1^\lambda$ meaning we take the value of the norm $|\cdot|_1$ to the λ -th power.

D.3.2 Global rings

A derivation is a map d of a ring R into itself and satisfies the relation $d(a \cdot b) = ad(b) + bd(a)$. Let K be a number field (of finite degree over $\mathbb{Q}$) and let $\mathbb{P}_K$ be the set of primes or finite places of K, respectively. Then every $p \in \mathbb{P}_K$ defines a nonarchimedean valuation $|\cdot|_p$ on K with valuation ring $\mathcal{O}_\mathfrak{p}$, valuation ideal $\mathcal{P}_\mathrm{p}$ (or p for short) and with residue field $\mathcal{K}_\mathrm{p} := \mathcal{O}_\mathrm{p}/\mathrm{p}$. In the case $\mathbb{S}_K \subseteq \mathbb{P}_K$ is a finite subset of places we use the notation $\mathbb{P}'_K := \mathbb{P}_K \backslash \mathbb{S}_K$ and $\mathcal{O}'_K$ is called a global ring.

$$\mathcal{O}'_K := \mathcal{O}_{\mathbb{S}_K} := \bigcap_{\mathrm{p} \in \mathbb{P}'_K} \mathcal{O}_{\mathrm{p}} \subseteq K$$

Now let F/K be a function field of one variable and $t \in F$ transcendental over K. Then $F/K(t)$ is a finite extension. By extending the derivation $\partial_t := \frac{d}{dt}$ from $K(t)$ to F, the field F becomes a differential field (F, ∂_F). Moreover, every place $p \in \mathbb{P}_K$ can be uniquely extended to a place $\mathfrak{P}$ or a valuation $|\cdot|_{\mathfrak{q}}$ of $K(t)$, respectively, by assuming

$$\left| \sum_{i=0}^{n} a_i t^i \right|_{\mathfrak{P}} = \max \left\{ |a_i|_{\mathrm{p}} \mid i = 0, \ldots, n \right\}$$

(GauB extension). The set of places $\mathfrak{P}_F$ of F lying over any such GauB extension $\mathfrak{P}$ of $p \in \mathbb{P}_K$ is denoted by

$$\mathbb{P}_F := \mathbb{P}_{t,F} := \left\{ \mathfrak{P}_F \, | \mathfrak{P}_F|_{K(t)} = \mathfrak{P} \text{ GauB place over } \mathfrak{p} \in \mathbb{P}_K \right\}$$

and is called the set of t -extensions of $\mathbb{P}_K$. (this set is referred to as the set of t -functional primes of F/K.) Likewise we use the notation

$$\mathbb{S}_F := \{ \mathfrak{P}_F \in \mathbb{P}_F \, | \mathfrak{P}_F|_K = \mathfrak{p} \in \mathbb{S}_K \}$$

and $\mathbb{P}'_F := \mathbb{P}_F \backslash \mathbb{S}_F$. Then the intersection

$$\mathcal{O}'_F := \mathcal{O}_{S_F} := \bigcap_{\mathfrak{P}_p \in \mathbb{P}_F} \mathcal{O}_{\mathfrak{P}_F} \subseteq F$$

Throughout this note a subring $\mathcal{O}'_F$ of F with nontrivial derivation $\partial_F|_{\mathcal{O}'_F}$ is called a global differential ring (global D-ring) if $\partial_F(\mathcal{O}'_F) \subseteq \mathcal{O}'_F$ and $\partial_F(\mathfrak{P}_F) \subseteq \mathfrak{P}_F$ for all $\mathfrak{P}_F \in \mathbb{P}'_F$

D.4 Global Differentials

D.4.1 Riemann Surface

Given two charts, $(U_1, \varphi_1), (U_2, \varphi_2)$, on a n-dimensional topological manifold, such that: $U_1 \cap U_2 \neq \emptyset$, we get transition maps:
$\varphi_1 \circ \varphi_2^{-1} : \varphi_2(U_1 \cap U_2) \to \varphi_1(U_1 \cap U_2)$, and
$\varphi_2 \circ \varphi_1^{-1} : \varphi_1(U_1 \cap U_2) \to \varphi_2(U_1 \cap U_2)$ Two charts, as above, are called compatible if the transition maps, as above, are homeomorphisms. If $U_1 \cap U_2 = \emptyset$, then they are compatible.

A collection of charts that are pairwise compatible and cover X (topological space) gives rise to a Riemann Surface.

D.4.2 Local parameter

A complex variable t defined as a continuous function $t_{p_0} = \phi_{p_0}(p)$ of a point p on a Riemann surface X, defined everywhere in some neighbourhood $V(p_0)$ of a point $p_0 \in X$ and realizing a homeomorphic mapping of $V(p_0)$ onto the disc $D(p_0) = \{t \in \mathbf{C} : |t| < r(p_0)\}$, where $\phi_{p_0}(p_0) = 0$.