Zeros of Riemann zeta function

Yuxin Lin

August 2019

Abstract

In this paper we show how some properties of Riemann zeta function lead to the proof of the Prime Number Theorem, the Prime Ideal Theorem, and Chebotarev Density Theorem. We then introduce some results related to Riemann Hypothesis, and Artin's conjecture as a corollary of Generalized Riemann Hypothesis.

Contents

1 Introduction

The Prime number Theorem is a theorem about the distribution of primes. At the first glance primes appear to behave quite wildly. However, the Prime Number Theorem says that the distribution can be described by an asymptotic formula. A more stunning fact is that the proof of the Prime Number Theorem relies heavily on the zero locations of the Riemann zeta function. The fact that Riemann zeta function doesn't have a zero on $\mathrm{Re}(s) = 1$ is the most crucial step in the proof of the Prime Number Theorem. We will also see that an similar property of $L(s,\chi)$ for χ a character on $Gal(K/\mathbb{Q})$ leads to the proof of the Prime Ideal Theorem, a generalization of the Prime Number Theorem to general fields.

The original proof of Chebotarev Density Theorem requires extensive use of Galois theory, and doesn't appear to be similar at all to the Prime Number Theorem. Here we present a classical alternative proof of Chebotarev in which the Chebotarev Density Theorem in abelian field extensions is presented as a simple corollary of the non-zero property of $L(s,\chi)$ on $\mathrm{Re}(s) = 1$, and the Chebotarev Density Theorem for non-abelian field extensions can be obtained as a corollary by considering the non-zero property of the generalized $L(s,\chi)$ series, which is the Artin L series.

From the proof of the Prime Number Theorem and Chebotarev Density Theorem we can guess intuitively that if we have more control of where the zeros of $\zeta(s)$ are, we can obtain a more precise estimation of density of primes. So in the second half of the paper, we will focus on getting more information about the zero location of zeta function. Firstly we extend the $\zeta(s)$ to the entire complex plane and present some results about the zeros of $\zeta(s)$. We also illustrate Riemann's original proof of the functional equation, which gives the symmetricity of the zeros. After getting these fundamental results, we cite the Von Mangoldt's formula of $\psi(x)$, from which we can see that the error bound of $\psi(x)$ depends entirely on the zeros of $\zeta(s)$. Since $\psi(x)$ and $\pi(x)$ differ by very little, to minimize the error bound of $pi(x)$ is equivalent to minimize the terms contributed by the zeros of zeta function. The symmetricity of zeros determines that to least error bound is obtained when all the critical zeros of Riemann zeta function are on $\mathrm{Re}(s) = \frac{1}{2}$, which is the Riemann Hypothesis. Assuming the Riemann Hypothesis and then following almost the same procedure as the proof of asymptotic formula of the Prime number Theorem, we can show that the Riemann Hypothesis gives the desired error bound of the prime counting function. We also have the Generalized Riemann Hypothesis, which is to assume the distribution of zeros of the Dedekind zeta function. At the end we present an

application of the Generalized Riemann Hypothesis. The role of the Generalized Riemann Hypothesis here is to gives more room for the estimation so that the error won't blow up.

The required group theory and Galois theory background is listed in section 2. Section 3 will introduce the Riemann zeta function and prove the Prime Number Theorem, and section 4 will introduce Artin L-functions and prove the Prime Ideal Theorem and the Chebotarev Density Theorem. Section 5 will introduce some results related to the zeros of $\zeta(s)$ and how the Riemann Hypothesis leads to its number theoratical equivalence. Section 6 introduces Artin's Primitive Root conjecture, which can be proven assuming the Generalized Riemann Hypothesis.

2 Background

2.1 Basic representation theory

Definition 2.1. *Let V be a vector space over a field F, and G be a finite group. A representation of G on V is a homomorphism $\rho := G \to GL(V)$. We say that ρ_1, ρ_2 are isomorphic if there exists some matrix M such that $M\rho_1 M^{-1} = \rho_2$.*

We say the dimension of ρ is the dimension of V.

Consider the ring $F[G]$, consists of $\sum_{i=1}^{n} a_i g_i$ with $a_i \in F$ and $g_i \in G$. This ring acts on V by

$$(\sum_{i=1}^{n}(a_i g_i)) \cdot v = \sum_{i=1}^{n} a_i(\rho(g_i)v)$$

So V can be regarded as an $F[G]$ module. So representation of G gives $F[G]$ modules. Conversely if we have a $F[G]$ module V then it's a vector space over F. Every $g \in$ G acts on V as a linear transformation by scalar multiplication, so define $\rho(g)$ to be this transformation in $GL(V)$. ρ is then a representation of G. Therefore, we have the correspondence:

$F[G]$ module V $\Longleftrightarrow \rho : G \longrightarrow GL(V)$

And this turns out to be a bijection. We say that V as a module affords the representation ρ of G.

We make the correspondence in order to state the following definition:

Definition 2.2. *A representation ρ is irreducible if and only if the $F[G]$ module that affords it is irreducible. That is, the only submodules of $F[G]$ are 0 and V.*

In terms of vector space, ρ is irreducible if V doesn't have a G-stable subspace. That is, no subspace V' of V has $gV' \subseteq V \quad \forall g \in G$.

Definition 2.3. *Given a representation $\rho : G \to GL(V)$, the character of ρ is the map $\chi_\rho : G \longrightarrow F$ such that $\chi(g) = Trace(\rho(g))$.*

We say a character χ_ρ is irreducible if ρ is irreducible representation. All representation of G are one dimensional iff G is abelian because $GL(V)$ is no longer commutative when the dimension of $V \geq 2$

Also notice that χ_ρ is the same for isomorphic presentations because trace is a invariant under matrix conjugation. This means that χ_ρ lands in the following category of functions:

Definition 2.4. *A class function is any map $f : G \longrightarrow \mathbb{C}$ such that $f(g^{-1}xg) = f(x)$, $\forall x, g \in G$*

The followings are some facts that we are going to use.

1. $\chi_{\rho_1} = \chi_{\rho_2}$ iff ρ_1 and ρ_2 are isomorphic representations. So the character determines the representation up to isomorphism.

2. For a group G, the number of irreducible characters equal the number of conjugacy classes of G.

3. Irreducible characters span the space of class functions. So every class function on G can be written as linear combination of irreducible characters.

4. (Orthgonality of characters) Define the inner product of two class functions ϕ and ψ on G as:

$$\langle \phi, \psi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}$$

Then let $\chi_1, \chi_2, ...\chi_g$ be the irreducible characters of G. For any class function $f = \sum a_i \chi_i$, $\langle f, \chi_i \rangle = a_i$. In particular, the inner product of two different irreducible characters is zero.

The proof of all the above facts can be found in the section 18.1 and 18.3 of [9].

2.2 One dimensional representation

We just mentioned that G is abelian iff all its irreducible representations are 1-dimensional. In this special case, we can ignore the distinction between the representation and character, and call both of them as the character of G.

Definition 2.5. *A character of a finite abelian group G is a homomorphism $\chi : G \to \mathbb{C}^*$. Let $\widehat{G}$ denote the set of all characters of G*

The followings are facts about abelian groups G we use. The proofs can be found in the chapter 7 of [10].

1. $\widehat{G} \cong G$(non-canonically)
2. (Orthogonality relations of characters)
   (1) For $\chi_1, \chi_2 \in \widehat{G}$, we have

$$\sum_{g \in G} \chi_1^{-1}\chi_2(g) = \begin{cases} |G|, & \text{if } \chi_1 = \chi_2 \\ 0, & \text{if } \chi_1 \neq \chi_2 \end{cases}$$

   (2) For $\sigma, \tau \in G$, we have

$$\sum_{\chi \in \widehat{G}} \chi(\sigma^{-1}\tau) = \begin{cases} |G|, & \text{if } \sigma = \tau \\ 0, & \text{if } \sigma \neq \tau \end{cases}$$

2.3 Induced representation and Frobenius reciprocity

Definition 2.6. *Let H be a subgroup of G. Let ρ be a representation of H on V. Then the representation of G afforded by $F[G] \otimes_{F[H]} V$ by left-multiplication is the induced representation $Ind_H^G \rho$ of ρ.*

When there is no ambiguity about G and H, we will use ρ^* to denote the character induced by ρ

We can actually write down explicit matrix for $\rho^*(g)$. Let $g_1, g_2, ...g_m$ be representatives of left-cosets of H. Then $\rho^*(g)$ can be written as:

$$\begin{bmatrix} \rho(g_1^{-1}gg_1) & \cdots & \rho(g_1^{-1}gg_m) \\ \vdots & \ddots & \vdots \\ \rho(g_m^{-1}gg_1) & \cdots & \rho(g_m^{-1}gg_m) \end{bmatrix}$$

Where $\rho(g_i^{-1}gg_j)$ is the zero matrix whenever $g_i^{-1}gg_j \notin H$. This is obtain by considering the action of g on the basis of $F[G] \otimes_{F[H]} V$.

From this matrix we get the induced character

$$\chi_{\rho^*}(g) = \sum_{g_i^{-1}gg_i \in H} \chi_\rho(g_i^{-1}gg_i) = \frac{1}{|H|} \sum_{x \in G} \chi_\rho(x^{-1}gx)$$

The proof can be found in the section 19.3 of [9]. Now we state an important theorem about restriction and induction of characters.

Theorem 2.7 (Frobenius reciprocity)**.** *Suppose H is a subgroup of G, and let ψ, ϕ be two class functions such that $\psi : G \to \mathbb{C}$ and $\phi : H \to \mathbb{C}$. Then we have*

$$\langle \phi, Res_H^G \psi \rangle_H = \langle \phi^*, \psi \rangle_G$$

where $Res_H^G \psi$ means restricting ψ to H.

The proof can be found in [12]

2.4 The Decomposition and Inertia groups

Let L/K be number field extension. Let $\mathcal{O}_K$ denote the ring of integer of K and $\mathcal{O}_L$ denote the ring of integer of L. For $\mathfrak{p}$ a prime ideal of K, consider the prime decomposition of $\mathfrak{p}\mathcal{O}_L$. say

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{k} \mathcal{P}_i^{e_i}$$

where $\mathcal{P}_i$ are prime ideals of $\mathcal{O}_L$. We define e_i to be $e(\mathcal{P}_i|\mathfrak{p})$.

Definition 2.8. *$\mathfrak{p} \subseteq \mathcal{O}_K$ is called unramified in L if $e(\mathcal{P}_i|\mathfrak{p}) = 1$, $\forall i$. Otherwise $\mathfrak{p}$ is ramified.*

Also, for a prime ideal $\mathcal{P} \in \mathcal{O}_L$, we denote the absolute norm of $\mathcal{P}$ as $||\mathcal{P}||$ $= |\mathcal{O}_L/\mathcal{P}|$. Notice norm of a prime ideal is a power of the rational prime below $\mathcal{P}$. It's a fact that $\mathcal{O}_L/\mathcal{P}_i$ is a field extension of $\mathcal{O}_K/\mathfrak{p}$. We denote the degree of extension of residue fields $[\mathcal{O}_L/\mathcal{P}_i : \mathcal{O}_K/\mathfrak{p}]$ as $f(\mathcal{P}_i|\mathfrak{p})$. It is known that

$$\sum_{i=1}^{k} e(\mathcal{P}_i|\mathfrak{p}) f(\mathcal{P}_i|\mathfrak{p}) = [L : K]$$

Now if L/K is Galois, let G denote $Gal(L/K)$. Then $e(\mathcal{P}_i|\,\mathfrak{p})$ and $f(\mathcal{P}_i|\,\mathfrak{p})$ are all equal since $\mathcal{P}_i = \sigma\mathcal{P}_j$ for some $\sigma \in G$. Then let $e = e(\mathcal{P}_i|\,\mathfrak{p}), f = f(\mathcal{P}_i|\,\mathfrak{p})$. We have $kfe = |G|$. $\mathfrak{p}$ ramifies in $\mathcal{O}_L$ iff $\mathfrak{p} \mid disc(L/K)$, so there are only finitely many ramifying primes in $\mathcal{O}_K$. The proof is found in the chapter 3 of [10]

Definition 2.9. *A prime $\mathfrak{p} \in \mathcal{O}_K$ is defined as splits completely in $\mathcal{O}_L$ iff $e\,(\mathcal{P}_i|\,\mathfrak{p}) = f\,(\mathcal{P}_i|\,\mathfrak{p}) = 1$*

In this paper we always assume L/K is Galois if not specified otherwise.

Definition 2.10. *Define the decomposition group $D\,(\mathcal{P}_i|\,\mathfrak{p})$ of $\mathcal{P}_i$ as*

$$D(\mathcal{P}_i|p) = \{\sigma \in G \mid \sigma\mathcal{P}_i = \mathcal{P}_i \ \ \forall i\}.$$

We can check it is a subgroup of G.

Definition 2.11. *Define the inertia group of $\mathcal{P}_i$ as $E(\mathcal{P}_i|p)$ such that*

$$E\,(\mathcal{P}_i|\,\mathfrak{p}) = \{\tau \in G \mid \tau\alpha \equiv \alpha \bmod \mathcal{P}_i \,\forall \alpha \in \mathcal{O}_L\}$$

We can check that $E(\mathcal{P}_i|p)$ is a subgroup of $D(\mathcal{P}_i|p)$.

Now consider $\mathcal{O}_L/\mathcal{P}_i$. For $\sigma \in D(\mathcal{P}_i|\,\mathfrak{p})$, it can also be regarded as acting on the residue field $\mathcal{O}_L\,/\,\mathcal{P}_i$ by sending $\alpha \bmod \mathcal{P}_i$ to $\sigma(\alpha) \bmod \mathcal{P}_i$. This is well defined because σ fixes $\mathcal{P}_i$. So we have a homomorphism

$$D(\mathcal{P}_i|\,\mathfrak{p}) \longrightarrow \mathrm{Gal}((\mathcal{O}_L/\mathcal{P}_i)/(\mathcal{O}_K/\,\mathfrak{p})).$$

The kernel is $E(\mathcal{P}_i|\,\mathfrak{p})$. It turns out that this map is actually surjective. Thus we have

$$D(\mathcal{P}_i|\,\mathfrak{p})\,/\,E(\mathcal{P}_i|\,\mathfrak{p}) \cong \mathrm{Gal}((\mathcal{O}_L/\mathcal{P}_i)/(\mathcal{O}_K/\,\mathfrak{p})).$$

Also $|\,E(\mathcal{P}_i|\,\mathfrak{p})\,| = e\,(\mathcal{P}_i|\,\mathfrak{p})$, and thus we have

$$|\,D(\mathcal{P}_i|\,\mathfrak{p})\,| = e\,(\mathcal{P}_i|\,\mathfrak{p})\,f\,(\mathcal{P}_i|\,\mathfrak{p})$$

. The proofs of above facts can be found in the chapter 3 of [10]

2.5 Frobenius elements

Recall that $\mathfrak{p}$ is unramified iff $e(\mathcal{P}_i|\,\mathfrak{p}) = 1$. Then $E(\mathcal{P}_i|\,\mathfrak{p})$ is trivial so $D(\mathcal{P}_i|\,\mathfrak{p})$ is isomorphic to the Galois group of residue fields. However, $\mathcal{O}_L/\mathcal{P}_i/\mathcal{O}_K/\,\mathfrak{p}$ is extension of finite fields, so its galois group is cyclic. By basic field theory the generator of $\mathrm{Gal}((\mathcal{O}_L/\mathcal{P}_i)/(\mathcal{O}_K/\,\mathfrak{p}))$ is $\overline{\sigma}$ such that

$$\overline{\sigma}(\overline{\alpha}) = \overline{\alpha}^{||\mathfrak{p}||}$$

where $\overline{\alpha}$ is the reduction of α mod $\mathfrak{p}$. Thus $D(\mathcal{P}_i|\,\mathfrak{p})$ has σ such that $\forall\alpha \in \mathcal{O}_L$, $\sigma\alpha \equiv \alpha^{||\mathfrak{p}||} \bmod \mathcal{P}_i$. This is what we called Frobenius element. We denote Frobenius element of $D(\mathcal{P}_i|\,\mathfrak{p})$ as $[\frac{L/K}{\mathcal{P}_i}]$

We observe some properties of the Frobenius element σ.

1. σ is unique in $D(\mathcal{P}_i|\,\mathfrak{p})$
2. The order of σ is $f(\mathcal{P}_i|\,\mathfrak{p})$
3. Let $\tau \in G$, then $[\frac{L/K}{\tau\mathcal{P}_i}] = \tau[\frac{L/K}{\mathcal{P}_i}]\tau^{-1}$. Specifically, when G is abelian, $[\frac{L/K}{\mathcal{P}_i}]$ is the same for all $\mathcal{P}_i$ above $\mathfrak{p}$. In this case we use $\psi(p)$ to denote its Frobenius element because it's determined entirely by $\mathfrak{p}$.

This special case gives rise to the following defintion:

Definition 2.12. *Suppose G is abelian Let I^S be all the ideals in $\mathcal{O}_K$ that are coprime to the ramifying primes. Then for the $\mathfrak{p} \in I^S$, $\mathfrak{p}$ is unramified. Then Artin map is the homomorphism ψ:$I^S \longrightarrow G$ such that for a prime $\mathfrak{p}$, $\psi(\mathfrak{p})$ is the corresponding Frobenius element. For $I \in I^S$, $\psi(I)$ is the product of Frobenius element of its prime factor.*

(Notice that if G is non-abelian Artin map is not well defined)

5. Recall that for L/K Galois extension, we say $\mathfrak{p} \subseteq \mathcal{O}_K$ splits completely in $\mathcal{O}_L$ iff $e(\mathcal{P}_i|\,\mathfrak{p}) = f(\mathcal{P}_i|\,\mathfrak{p}) = 1$. Now consider cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. This is an abelian extension and a prime $p \in \mathbb{Q}$ ramifies iff $p|m$. Then for $p \in \mathbb{Q}$, we have $\psi(p)\alpha \equiv \alpha^p \bmod \mathcal{P}_i\ \forall\mathcal{P}_i$. Then by Chinese reminder theorem:

$$\psi(p)\alpha \equiv \alpha^p \bmod p$$

For all $p \nmid m$ But $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$ with the map being

$$k \to (g_k : \zeta_m \to \zeta_m^k)$$

Thus there exists $\sigma \in G$ such that $\sigma\zeta_m = \zeta_m^p$, and there are,

$$\sigma\alpha \equiv \alpha^p \bmod p$$

Thus this σ is the Frobenius element $\psi(p)$.

On the other hand, recall that $f(\mathcal{P}_i|\,\mathfrak{p})$ is the order of $\psi(p)$, so the σ in this case is the identity. So σ should fix ζ_m. This happens iff

$$p \equiv 1 \bmod m$$

which is thus the sufficient and necessary condition for p to split completely in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$.

3 Riemann zeta function and prime number thoerem

3.1 Riemann zeta function

In this section we briefly mention some properties of Riemann zeta function. These proofs can be found in the chapter 7 of [10]

Lemma 3.1. *Consider* $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$. *Series in this form are called the Dirichlet series. If* $\sum_{n \leq t} a_n = O(t^r)$, *then* $f(s)$ *is analytic and convergent for* $Re(s) > r$

Definition 3.2. *The Riemann zeta function is defined as*

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

By the lemma, $\zeta(s)$ converges and is analytic in $\mathrm{Re}(s) > 1$. But this definition does not work $\mathrm{Re}(s) \leq 1$. It turns out that we can find a meromorphic extension of $\zeta(s)$ to $\mathrm{Re}(s) > 0$. i.e., we can find $g(s)$ a meromorphic function that is defined on $\mathrm{Re}(s) > 0$ except for some poles, such that $g(s)$ agrees with $\zeta(s)$ on $\mathrm{Re}(s) \geq 1$. By complex analysis, this means that $g(s)$ and $\zeta(s)$ agree whenever both of them are defined.

Our $g(s)$ is defined as follows. Consider

$$f(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + ...$$

Then the partial sums of the coefficients alter between 0 and 1, so are $\mathcal{O}(t^0)$. Then by the lemma $g(s)$ is convergent on $\mathrm{Re}(s) > 0$. Then let

$$g(s) = \frac{f(s)}{1 - \frac{2}{2^s}}$$

We know that $g(s) = \zeta(s)$ when $\mathrm{Re}(s) > 1$. $\frac{f(s)}{1-\frac{2}{2^s}}$ is analytic on $\mathrm{Re}(s) > 0$ except for when $\frac{2}{2^s} = 1$, where it might have a pole. But it is not necessary since the pole can be cancelled if f(s) is zero.

In order to find where the poles actually are, we construct another expression for $\zeta(s)$.

Let

$$t(s) = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + ...$$

Then the partial sum of the coefficients alter between 0,1,2, so are $\mathcal{O}(t^0)$. So $t(s)$ is also analytic on $\mathrm{Re}(s) > 0$. We can get that $\frac{t(s)}{1-\frac{3}{3^s}} = \zeta(s)$. Thus $\frac{g(s)}{1-\frac{3}{3^s}}$ and $\frac{t(s)}{1-\frac{2}{2^s}}$ are both meromorphic extension of $\zeta(s)$. Since they agree on $\mathrm{Re}(s) > 1$, they agree whenever both of them are defined. Thus the pole of $\frac{t(s)}{1-\frac{3}{3^s}}$ and $\frac{f(s)}{1-\frac{2}{2^s}}$ should also agree.

Now say s is the pole, then we must have $1 - \frac{2}{2^s} = 0$ and $1 - \frac{3}{3^s} = 0$. Thus $(1-s)\log 2 = (1-s)\log 3$. This doesn't happen unless $s = 1$. So the only possible pole of the extension of $\zeta(s)$ is at $s = 1$.

Since $f(1) = \log 2$ is not 0, we have

$$\lim_{s\to 1}(s-1)\frac{f(s)}{1-\frac{2}{2^s}} = \lim_{s\to 1}(s-1)\frac{f(1)}{1-\frac{2}{2^s}} = \lim_{s\to 1}\frac{f(1)}{\frac{2^{1-s}-1}{s-1}}$$

which is 1. Thus $\zeta(s)$ has a simple pole at $s = 1$ with residue 1, and is analytic elsewhere on $\mathrm{Re}(s) > 0$.

3.2 Proof of the Prime Number Theorem

Theorem 3.3 (the Prime Number Theorem)**.** *Let $\pi(x)$ denote the number of primes not exceeding x. Then we have*

$$\pi(x) \sim \frac{x}{\log x}$$

$\pi(x) \sim \frac{x}{\log x}$ here just means that as x approaches infinty, $\frac{\pi(x)}{\frac{x}{\log x}}$ approaches 1. It is quite stunning that the proof of the Prime Number Theorem is based totally on the behavior of $\zeta(s)$ on $\mathrm{Re}(s) \geq 1$.

Consider the product representation of zeta function when $\mathrm{Re}(s) > 1$

$$\zeta(s) = \prod_{p\in\mathbb{Z}}\left(1 - \frac{1}{p^s}\right)^{-1}$$

which is equivalent to the fundamental theorem of arithematic. Taking the logarithm, we have

$$\log\zeta(s) = -\sum_p \log\left(1 - \frac{1}{p^s}\right) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}$$

Differentiating gives

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \sum_{m=1}^{\infty} \frac{\log p}{p^{ms}} = \sum_p \frac{\log p}{p^s} + \sum_p \sum_{m=2}^{\infty} \frac{\log p}{p^{ms}}$$

Since $\log p < p^\sigma$ as $p \to \infty$ $\forall \sigma > 0$, the sum of absolute value of each term is

$$\sum_p \frac{\log p}{|p^s|} = \sum_p \frac{\log p}{p^{\mathrm{Re}(s)}} = \sum_p \frac{\log p}{p^{\frac{\mathrm{Re}(s)-1}{2}}} \cdot \frac{1}{p^{\frac{\mathrm{Re}(s)+1}{2}}}.$$

For $\mathrm{Re}(s) > 1$, $\frac{\mathrm{Re}(s)+1}{2} > 1$, so $\sum_p \frac{\log p}{p^s}$ converges absolutely for $\mathrm{Re}(s) > 1$, and so is analytic there. Similarly we can get $\sum_p \sum_{m=2}^{\infty} \frac{\log p}{p^{ms}}$ converges absolutely for $\mathrm{Re}(s) > \frac{1}{2}$, and thus is analytic on $\mathrm{Re}(s) = 1$. The term $\sum_p \sum_{m=2}^{\infty} \frac{\log p}{p^{ms}}$

converges absolutely for $\mathrm{Re}(s) > \frac{1}{2}$. Thus the asymptotic growth of $-\frac{\zeta'(s)}{\zeta(s)}$ at $\mathrm{Re}(s) = 1$ is the same as $\sum_p \frac{\log p}{p^s}$.

For $\log \zeta(s)$ and its derivative to be defined on $\mathrm{Re}(s) \geq 1$ we need $\zeta(s)$ to be non-zero on $\mathrm{Re}(s) \geq 1$. The non-zero property for $\mathrm{Re}(s) > 1$ is shown by the product representation, so it remains to show that $\zeta(s) \neq 0$ on $\mathrm{Re}(s) = 1$.

Theorem 3.4. *$\zeta(s) \neq 0$ on $Re(s) = 1$*

Proof. For $\mathrm{Re}(s) > 1$ we can use the product representation. We have

$$\log \zeta(s) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}} = \sum_p \sum_{m=1}^{\infty} e^{-ms \log p}$$

Now say $s = \sigma + it$, $\sigma, t \in \mathbb{R}$, we have

$$|\zeta(s)| = \left| \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{m} e^{-\sigma m \log p} (\cos(tm \log p) - i \sin(tm \log p) \right) \right| = \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{m\sigma}} \cos(tm \log p) \right)$$

Now let $1 + it$ be the hypothetical zero, so $t \neq 0$ because $\zeta(s)$ has a pole at 1. Then we have

$$|\zeta(\sigma)|^3 |\zeta(\sigma+it)|^4 |\zeta(\sigma+2it)| = \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{m\sigma}} (3 + 4\cos(tm \log p) + \cos(2tm \log p) \right)$$

But $3 + 4\cos\theta + \cos 2\theta = 2(\cos\theta + 1)^2 \geq 0$ for all θ. So

$$\exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{m\sigma}} (3 + 4\cos tm \log p + \cos 2tm \log p) \right) \geq 1$$

Thus

$$|\zeta(\sigma)(\sigma - 1)|^3 \left| \frac{\zeta(\sigma + it)}{\sigma - 1} \right|^4 |\sigma(2 + it)| \geq \frac{1}{\sigma - 1} \tag{1}$$

Now let σ approach 1 from above. Then $|\zeta(\sigma)(\sigma - 1)|^3$ is a non-zero finite value; $|\zeta(\sigma + 2it)|$ is finite because $\zeta(s)$ is analytic on $\mathrm{Re}(s) \geq 1$ except for $s = 1$; $|\frac{\zeta(\sigma+it)}{\sigma-1}|^4$ is also finite because $\frac{1}{\sigma-1}$ is cancelled by $\zeta(1 + it) = 0$. Thus the left of (1) is finite, while the right of (1) approaches infinity as $\sigma \to 1$. We reach a contradiction.

So $\zeta(s) \neq 0$ on $\mathrm{Re}(s) \geq 1$ □

Since $\zeta(s)$ only has a simple pole at $s = 1$, $\zeta(s)(s-1)$ is analytic everywhere on $\mathrm{Re}(s) \geq 1$ and so is its derivative. We know that

$$(\zeta(s)(s - 1))' = \zeta'(s)(s - 1) + \zeta(s)$$

is finite on $s = 1$. Since $\zeta(s)$ is non-zero on $\mathrm{Re}(s) \geq 1$, we can divide both sides by $\zeta(s)$ and take $s \to 1$, obviously

$$0 = \lim_{s \to 1^+} \frac{\zeta'(s)}{\zeta(s)}(s-1) + 1$$

From here we know that $-\frac{\zeta'(s)}{\zeta(s)}$ has a pole at $s = 1$ with residue 1, and is analytic on the rest of $\mathrm{Re}(s) \geq 1$.

Recall that $\sum_p \frac{\log p}{p^s}$ has the same residue and pole as $-\frac{\zeta'(s)}{\zeta(s)}$ when $s \to 1$. So $\sum_p \frac{\log p}{p^s}$ is analytic on $\mathrm{Re}(s) \geq 1$ except for a simple pole at $s = 1$ with residue 1.

Now let us write $\sum_p \frac{\log p}{p^s}$ as Dirichlet series: let $a(n)$ be the prime indicator function, namely

$$a(n) = \begin{cases} 1, & \text{if n is a prime} \\ 0, & \text{otherwise} \end{cases}$$

Then

$$\sum_p \frac{\log p}{p^s} = \sum_{n=1}^{\infty} \frac{a(n) \log n}{n^s}$$

Notice that $\pi(x) = \sum_{n \leq x} a(n)$, and we want to show that

$$\sum_{n \leq x} a(n) \sim \frac{x}{\log x}$$

We are then able to apply the following theorem:

Theorem 3.5. *Let $f(t)$ be non-negative and non-decreasing piecewise continuous real function on $[1, \infty]$ and $f(t) = \mathcal{O}(t)$. Then the Mellin transform $g(s) = s \int_1^\infty f(x) x^{-s-1} dx$ is analytic for $Re(s) > 1$. Additionally, If $g(s) - \frac{c}{s-1}$ has analytic extension to neighbourhood of $Re(s) = 1$, then as $x \to \infty$, $f(x) \sim cx$*

This theorem is a corollary of Auxiliary Tauberian theorem. The proofs of both can be found at page 10 of [13]. Plugging in the $f(x) = \sum_{n \leq x} a(n) \log n$ into the theorem, we get that $g(s) = \frac{-\zeta'(s)}{\zeta(s)}$. Since $\frac{-\zeta'(s)}{\zeta(s)}$ has only a simple pole at $s = 1$ with residue 1, $\frac{-\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$ has analytic continuation to $\mathrm{Re}(s) \geq 1$. Also it is true that $\sum_{n \leq x} a(n) \log n = \mathcal{O}(x)$, as proved in chapter 4.5 of [17]. Now we have all the conditions required to apply Theorem 3.5. We get

$$\sum_{n \leq x} a(n) \log n \sim x$$

The statement of the Prime Number Theorem is that $\sum_{n \leq x} a(n) \sim \frac{x}{\log x}$, so we want to get rid of $\log n$ in the sum. For this purpose we use the following trick :

Theorem 3.6 (Abel's identity)**.** *Let $a(n)$ to be a function defined on natural numbers. Let $A(x) = \sum_{n \leq x} a(n)$, and let $f(x)$ be a differentiable function, then we have*

$$\sum_{y < n \leq x} a(n) f(n) = A(x) f(x) - A(y) f(y) - \int_y^x A(t) f^{'}(t) dt$$

This is a generalized version of integral by parts if we think of $A(x)$ as the integral of $a(n)$. The proof can be found at page 29 of [2]

Now take $b(n) = a(n)\log n$. Then $\pi(x) = \sum_{n\leq x} a(n) = \sum_{\frac{3}{2}<n\leq x} \frac{b(n)}{\log n}$. Now apply the Abel's identity:

$$\sum_{\frac{3}{2}<n\leq x} \frac{b(n)}{\log n} = \frac{\sum_{n\leq x} b(n)}{\log x} - \int_{\frac{3}{2}}^{x} \frac{\sum_{n\leq t} b(t)}{t(\log t)^2} dt$$

We know that $\sum_{n\leq x} b(n) \sim x$. Using this we can show that

$$\int_{\frac{3}{2}}^{x} \frac{\sum_{n\leq t} b(t)}{t(\log t)^2} dt = o\left(\frac{x}{\log x}\right)$$

The detailed proof can be found in chapter 4.3 of [17]. Then we have

$$\sum_{\frac{3}{2}<n\leq x} \frac{b(n)}{\log n} = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right)$$

Which is the statement of the Prime Number Theorem.

We give another equivalent statement of the Prime Number Theorem: Define $Li(x) = \int_2^x \frac{1}{\log t} dt$, then we have:

$$\pi(x) \sim Li(x)$$

$Li(x)$ is a better approximation of $\pi(x)$ than $\frac{x}{\log x}$, but if we just look at the asymptotic formula the two statements are equivalent. From integrating by parts we know that

$$Li(x) = \frac{x}{\log x} - \int_2^x \frac{1}{(\log t)^2}$$

Notice that $\int_2^x \frac{1}{(\log t)^2}$ is small compared to $\frac{x}{\log x}$, so $\frac{Li(x)}{\frac{x}{\log x}}$ goes to 1 as $x \to \infty$. Therefore the two statements of the Prime Number Theorem are equivalent.

4 L-series and Prime Ideal Theorem

4.1 Dedekind zeta function

Now that we have introduced $\zeta(s)$ and its extension to $\mathrm{Re}(s) > 0$, we can consider a generalized version of $\zeta(s)$, the Dedekind zeta function.

Definition 4.1. *Let K be a finite extension of $\mathbb{Q}$. Let j_n denote the number of ideals I of $\mathcal{O}_K$ with $||I||$=n. Then the Dedekind zeta function is defined as*
$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{j_n}{n^s}$.

Equivalently it can also be written as $\zeta_K(s) = \sum_{I\in O_K} \frac{1}{||I||^s}$.

Definition 4.2. *Let $\mathcal{O}_K$ be ring of integer of K. Then we define the class group C to be the group of all the fractional ideals in $\mathcal{O}_K$ quotient out by principal ideals.*

Then we cite a theorem about the distribution of ideals in a number ring. Readers can refer to chapter 6 of [10]

Theorem 4.3. *Let C be a class group in $\mathcal{O}_K$, and let $i_c(t)$ denote the number of ideals in C with norm $\leq t$. Then we have*
$i_c(t) = \kappa t + \mathcal{O}(t^{1-\frac{1}{[K:\mathbb{Q}]}})$, *Where κ is a constant independent of C*

Now let h be the number of ideal classes in K. Then we have

$$\sum_{n\leq t} j_n = h\kappa t + \mathcal{O}(t^{1-\frac{1}{[K:\mathbb{Q}]}})$$

Thus we know that $\sum_{n\leq t} j_n = \mathcal{O}(t)$, which by lemma 3.1 implies $\zeta_K(t)$ is convergent and analytic on $\mathrm{Re}(s) > 1$

Now on $\mathrm{Re}(s) > 1$, by changing the order of summation we have

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{j_n - h\kappa}{n^s} + h\kappa\zeta(s)$$

But $\sum_{n\leq t} j_n - h\kappa = \mathcal{O}(t^{1-\frac{1}{[K:\mathbb{Q}]}})$. By the lemma 3.1 $\sum_{n=1}^{\infty} \frac{j_n - h\kappa}{n^s}$ is convergent and analytic for $\mathrm{Re}(s) \leq 1 - \frac{1}{[K:\mathbb{Q}]}$. We also know that $\zeta(s)$ has extension on $\mathrm{Re}(s) > 0$ except for a simple pole at s=1. So when K different from $\mathbb{Q}$, $\zeta_K(s)$ has meromorphic extension to $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$, analytic except for simple pole at $s = 1$ with residue $h\kappa$.

Similar to $\zeta(s)$ we have product representation for $\zeta_K(s)$ on $\mathrm{Re}(s) > 1$. With the unique factorization of ideals in Dedekind domain, $||I|| = \prod_{\mathfrak{p}_i | I} ||\mathfrak{p}_i||^{e_i}$, where $\mathfrak{p}_i$ denotes prime ideals of $\mathcal{O}_K$. Since norm is multiplicative, when $\mathrm{Re}(s) > 1$, we have

$$\zeta_K(s) = \prod_{\mathfrak{p}\subseteq\mathcal{O}_K} (1 - \frac{1}{||\mathfrak{p}||})^{-1}$$

4.2 L-series

$\mathrm{Gal}(L/K)$ is abelian. We continue to write $G = \mathrm{Gal}(L/K)$, and we let χ to be a character at G.

Let S be set of all ramified prime, so S is finite. Let I^S be group of fractional ideals in $\mathcal{O}_K$ that are coprime to primes in S. Recall we defined the Artin map:

$$\phi : I^S \to G$$

as sending the primes in I^S to the corresponding Frobenius element in G. We denote the image of $\mathfrak{p}$ by $\phi(\mathfrak{p})$. By the multiplicity of ϕ, for ideals $I = \prod_{i=1}^{k} {\mathfrak{p}_i}^{e_i}$, $\phi(I) = \prod_{i=1}^{k} \phi(\mathfrak{p}_i)^{e_i}$. Then $\chi \circ \phi$ is a character on I^S. For $I \notin I^S$, we let $\chi \circ \phi(I) = 0$, thereby extending $\chi \circ \phi$ to all ideals.

Definition 4.4. $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\sum_{||I||=n} \chi\circ\phi(I)}{n^s} = \sum_{I\subseteq\mathcal{O}_K} \frac{\chi\circ\phi(I)}{||I||^s}$

Since $\chi\circ\phi(I)$ is 0 or root of unity, $\sum_{||I||\leq n} \chi\circ\phi(I) \leq \sum_{k=1}^{n} j_k$. Thus $L(s,\chi)$ converges absolutely for $\mathrm{Re}(s) > 1$.

By the multiplicity of $\chi\circ\phi$ has the product representation

$$L(s,\chi) = \prod_{p\subseteq\mathcal{O}_K} (1 - \frac{\chi\circ\phi(\mathfrak{p})}{||\mathfrak{p}||^s})^{-1}$$

Notice that if we take χ as the trivial character χ_0,

$$L(s,\chi) = \prod_{p\subseteq\mathcal{O}_K,\text{unramified}} (1 - \frac{1}{||\mathfrak{p}||^s})^{-1}$$

So $L(s,\chi)g(s) = \zeta_K(s)$, if $g(s) = \prod_{\mathfrak{p}\text{ ramified}}(1-\frac{1}{||\mathfrak{p}||^s})^{-1}$. This is a finite product so it's analytic on $\mathrm{Re}(s) > 0$. So for $1 - \frac{1}{[K:\mathbb{Q}]} < \mathrm{Re}(s) \leq 1$, we can take $\frac{\zeta_K(s)}{g(s)}$ as the memorphic extension of $L(s,\chi_0)$, This extension should have the same asymptotic behavior as $\zeta_K(s)$. It's analytic in the range except for a simple pole at $s = 1$.

In general for $\chi \in \widehat{G}$ we have the following:

Theorem 4.5. *$\sum_{||I||\leq t} \chi\circ\phi(I) = at + \mathcal{O}(t^{1-\frac{1}{[K:\mathbb{Q}]}})$, where a is some non-zero constant if χ is trivial, and zero if χ is non-trivial*

The case when the character is trivial has been proven above. Assuming the theorem is true for non-trivial characters, by Lemma 3.1 we know $L(s,\chi)$ has analytic extension to $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$, except for a simple pole at $s = 1$ when χ is trivial.

Now to prove the theorem, notice that $\chi\circ\phi$ as a character on I^S takes value 1 on kernel of ϕ. So $\chi\circ\phi$ can be regarded as a character on $I^S/\ker\phi$. Then we need to use the Artin reciprocity. Proofs is found in chapter 5.3 of [15]

Theorem 4.6 (Artin reciprocity)**.** *Let L be a finite abelian extension of K, S is the primes ramify in L. Then there exists m such that the primes dividing m are precisely the ramified prims. Then we have*

$$I^S/K_{m,1}Nm_K^L(I) \cong G$$

Here $K_{m,1}$ is the set of principal ideals (a) such that $a \equiv 1 \bmod m$ and a is totally positive. $Nm_K^L(I)$ is the image of ideals in L under the norm map.

Now let ψ be a homomorphism $I^S \to G$ with $K_{m,1}$ included in the kernel. Since $K_{m,1}$ has a finite index in I^s(chapter 5.3 of [15]) ,$I^s/K_{m,1}$ is a finite abelian group, so ψ can be regarded as 1-dimensional character on $I^s/K_{m,1}$. Denote a coset of $K_{m,1}$ in I^S as C. Now consider $\sum_{||I||\leq x} \psi(I) = \sum_C \sum_{||I||\leq x, I\in C} \psi(I)$. Since ψ takes the same value on elements that belong to the same coset of $K_{m,1}$, we can denote the value of ψ on the coset C as $\psi(C)$. The sum is thus $\sum_C \psi(C) \sum_{||I||\leq x, I\in C} 1$

Now consider the inner sum

$$\sum_{||I||\leq x, I\in C} 1$$

Let J be a fixed ideal in C^{-1}. Then for any $I \in C$, there exists a such that $a \equiv 1 \bmod m$ and a totally positive such that $(a) = IJ$. Since a is totally positive we have:

$$||a|| = ||(a)|| = ||I||||J||$$

Thus the inner sum is also

$$\sum_{||a||\leq x||J||, (a)\subseteq J} 1$$

The question is now reduced to counting the number of ideal $(a) \subseteq J$ with some bound on the norm. In page 210 of [16] the author proves that $bx + \mathcal{O}(x^{1-\frac{1}{[K:\mathbb{Q}]}})$, where b is independent of C.

$$\sum_C \psi(C)bx + \mathcal{O}(x^{1-\frac{1}{[K:\mathbb{Q}]}})$$

By the orthogonality relations of characters, $\sum_C \psi(C) = 0$ for non-trivial ψ, and is $cx + \mathcal{O}(x^{1-\frac{1}{[K:\mathbb{Q}]}})$for ψ being trivial, where c is some constant depending on $\mathcal{O}_K$. Since $\chi \circ \phi$ also takes value 1 on $K_{m,1}$, it has this property. Thus we have

$$\sum_{||I||\leq x} \chi \circ \phi(I) = \begin{cases} o(x^{1-\frac{1}{[K:\mathbb{Q}]}}), & \text{if } \chi \circ \phi \text{ is non-trivial} \\ cx + o(x^{1-\frac{1}{[K:\mathbb{Q}]}}), & \text{if } \chi \circ \phi \text{ is trivial} \end{cases}$$

Now we can apply the lemma on $L(s, \chi)$. From the above formula we know that $L(s, \chi)$ is analytic on $\mathrm{Re}(s) \geq 1$ if $\chi \circ \phi$ is trivial, and that $L(s, \chi)$ is analytic on $\mathrm{Re}(s) \geq 1$ except for a simple pole at $s = 1$ if $\chi \circ \phi$ is trivial character.

4.3 Prime Ideal Theorem

We want to prove here the following generalization of the Prime Number Theorem:

Theorem 4.7.

$$\sum_{||\mathfrak{p}||\leq x} \chi \circ \phi(\mathfrak{p}) = \begin{cases} \frac{x}{\log x} + o(\frac{x}{\log x}) & \textit{if } \chi \circ \phi \textit{ is the trivial character} \\ o(\frac{x}{\log x}) & \textit{if otherwise} \end{cases} \tag{2}$$

Similar to the proof of prime number thoery, we need to some properties of $\log L(s, \chi)$ in $\mathrm{Re}(s) \geq 1$. $\log L(s, \chi)$ is analytic and doesn't have zero on $\mathrm{Re}(s) > 1$, and we know that $L(s, \chi)$ is analytic on $\mathrm{Re}(s) = 1$ except for maybe a simple pole at $s = 1$. Now we only need that $L(s, \chi)$ is non-zero on $\mathrm{Re}(s) = 1$ to make $\log L(s, \chi)$ well defined.

Lemma 4.8. *$L(s,\chi) \neq 0$ for any χ*

Proof. The proof is divided into two cases.

Case 1. Suppose $(\chi \circ \phi)^2$ is not a trivial character. Then say that $L(1+it,\chi) = 0$ for $t \neq 0$, and say $s = \sigma + it$. For $\mathrm{Re}(s) > 1$, we can use the product representation of $L(s,\chi)$ and take its logarithm, which is

$$\log L(s,\chi) = \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \sum_{m=1}^{\infty} \frac{\chi \circ \phi(\mathfrak{p}^m)}{m||\mathfrak{p}||^{ms}}$$

Let $\chi \circ \phi(\mathfrak{p}) = e^{ai}$ for $\mathfrak{p}$ unramified. Thus

$$L(s,\chi) = \exp\left(\sum_{\mathfrak{p} \subseteq \mathcal{O}_K, \mathfrak{p} \text{ unramified}} \sum_{m=1}^{\infty} e^{mi(a - t\log||\mathfrak{p}||)} \frac{1}{m\,\mathfrak{p}^{m\sigma}} \right)$$

Take the absolute value, we have

$$|\,L(s,\chi)\,| = \exp\left(\sum_{\mathfrak{p} \text{ unramified } \in \mathcal{O}_K} \sum_{m=1}^{\infty} \cos(m(a - t\log||\mathfrak{p}||)) \frac{1}{m\mathfrak{p}^{m\sigma}} \right)$$

Then

$$|L(s,\chi_0)|^3 |L(\sigma+it,\chi)|^4 |L(\sigma+2it,\chi^2)|$$

$$= \exp \sum_{\mathfrak{p} \text{ unramified } \subseteq \mathcal{O}_K} \sum_{m=1}^{\infty} \frac{1}{m\mathfrak{p}^{m\sigma}} (3 + 4\cos m(a - t\log||\mathfrak{p}||) + \cos 2m(a - t\log||\mathfrak{p}||))$$

Also, $L(\sigma+2it,\chi^2)$ isn't a pole, since $L(s,\chi)$ only has a pole when $s=1$ and $\chi = \chi_0$. The rest is exactly the same as in the Prime number theorem. We can derive a contradiction. $\square$

Case 2. Now suppose $\chi \circ \phi^2$ is trivial character. If the hypothetical zero of $L(s,\chi)$ is not $s=1$, say it's $s = 1+it$. then $|L(1+2it,\chi_0)|$ is finite because $L(s,\chi)$ has a pole only when $s=1$ and $\chi = \chi_0$. Then the above proof still works out.

Now we only need to consider the case when the hypothetical zero of $L(s,\chi)$ is $s=1$. This is impossible for $\chi \circ \phi$ being trivial character, so we only need to consider the case when $\chi \circ \phi$ is non-trivial.

By extending the Dirichlet series product, we find

$$\zeta_K(s)\, L(s,\chi) = \sum_{I} \frac{\sum_{d|I} \chi \circ \phi(d)}{||I||^s} \tag{3}$$

when the series is convergent. Now let $a_n = \sum_{||I||=n} \sum_{d|I} \chi \circ \phi(d)$, and write (3) as a Dirichlet series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$.

Since

$$\sum_{d|I} \chi \circ \phi(d) = \prod_{\mathfrak{p}\,|I} (1 + \chi \circ \phi(\mathfrak{p}) + \chi \circ \phi(\mathfrak{p}^2) + ... + \chi \circ \phi(\mathfrak{p}^{e_{\mathcal{P}}}))$$

This sum is positive if $\chi \circ \phi(\mathfrak{p}) = 1$, and when $\chi \circ \phi(\mathfrak{p}) = -1$ then the sum is 1 for $e_{\mathfrak{p}}$ being odd and is 0 when $e_{\mathfrak{p}}$ being even. Thus $a(n) \geq 0$. For I being a square, we have $\sum_{d|I} \chi \circ \phi(d) \geq 1$. Thus we have the below inequality:

$$\sum_{I} \frac{\sum_{d|I} \chi \circ \phi(d)}{||I||^s} \geq \sum_{J} \frac{1}{||J||^{2\sigma}} \tag{4}$$

Here we assume the fact that $\zeta_K(s)$ and $L(s, \chi)$ has meromorphic extension to the entire complex plane, analytic everywhere except for a simple pole at $s = 1$ for $\zeta_K(s)$ (page 7 of [18]). Then $\zeta_K(s)\, L(s, \chi)$ should be analytic everywhere as the pole of $\zeta_K(s)$ at $s = 1$ is cancelled by the hypothetical zero of $L(s, \chi)$ at $s = 1$. Here we cite a theorem of Dirichlet series from page 213 of [16]:

Theorem 4.9. *The Dirichlet series $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ with $a_n \geq 0$ has a half plane $Re(s) > a$ as its domain of convergence. If a is finite, then $f(s)$ is non-regular (has a pole) at $s = a$*

To apply the theorem take $f(s) = \zeta_K(s)\, L(s, \chi)$ and so $f(s)$ is the series $\sum_I \frac{\sum_{d|I} \chi \circ \phi(d)}{||I||^s}$ when both are convergent. Knowing that $f(s)$ converges everywhere, we want to show that$\sum_I \frac{\sum_{d|I} \chi \circ \phi(d)}{||I||^s}$ also converges everywhere. If it doesn't, then there exists σ_0 such that $\sum_I \frac{\sum_{d|I} \chi \circ \phi(d)}{||I||^s}$ converges to the right of σ_0 and to the left. Then theorem 4.9 says that $f(s)$ can't be extended to the neighbourhood of σ_0, which is not true because we just showed that $f(s)$ is analytic on the entire complex plane. So $\sum_I \frac{\sum_{d|I} \chi \circ \phi(d)}{||I||^s}$ should be convergent everywhere.

Now take $\sigma \to \frac{1}{2}$ in equation 4. The left is convergent, while the right diverges. So we derive a contradiction, which means $L(s, \chi)$ can't have an zero at $s = 1$.

Combining with case 1 we show that $L(s, \chi)$ is non-zero on $\mathrm{Re}(s) = 1$. Then if $\chi \circ \phi$ is non-trivial, $L(s, \chi)$ is non-zero and analytic on $\mathrm{Re}(s) \geq 1$, thus $L(s, \chi)$ is also analytic in this region, and so is $-\frac{L'(s,\chi)}{L(s,\chi)}$. If $\chi \circ \phi$ is the trivial character, similar to in the proof of the Prime Number Thoerem, we can prove that $-\frac{L'(s,\chi)}{L(s,\chi)}$ has a simple pole at $s = 1$ with residue 1

Now for $\mathrm{Re}(s) > 1$, use the product representation of $L(s, \chi)$ and differentiate its logarithm, we obtain

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{\log ||\mathfrak{p}||\, \chi \circ \phi(\mathfrak{p})}{||\mathfrak{p}||^s} + \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \sum_{m=2}^{\infty} \frac{\log ||\mathfrak{p}||\, \chi \circ \phi(\mathfrak{p})}{||\mathfrak{p}||^s}$$

Since there are only at most $[K:\mathbb{Q}]$ of $\mathfrak{p}$ above a rational prime p, and that $||\mathfrak{p}|| \geq p$, we know that

$$\sum_{m=2}^{\infty} \frac{\log ||\mathfrak{p}||\, \chi \circ \phi(\mathfrak{p})}{||\mathfrak{p}||^s} \leq \mathcal{O}(\sum_{\mathfrak{p}} \sum_{m=2}^{\infty} \frac{1}{p^{m\sigma}})$$

Since $\sum_{\mathfrak{p}} \sum_{m=2}^{\infty} \frac{1}{\mathfrak{p}^{m\sigma}}$ is analytic on $\mathrm{Re}(s)=1$, $-\frac{L(s,\chi)'}{L(s,\chi)}$ has the same pole and same residue as $\sum_{\mathfrak{p}\subseteq\mathcal{O}_K} \frac{\log ||\mathfrak{p}||\, \chi \circ \phi(\mathfrak{p})}{||\mathfrak{p}||^s}$ when $s \to 1$. Now we write $\sum_{\mathfrak{p}\subseteq\mathcal{O}_K} \frac{\log ||\mathfrak{p}||\, \chi \circ \phi(\mathfrak{p})}{||\mathfrak{p}||^s}$ as a Dirichlet series, namely

$$\sum_{n=1}^{\infty} \frac{\sum_{||\mathfrak{p}||=n} \log ||\mathfrak{p}||\, \chi \circ \phi(\mathfrak{p})}{n^s}$$

This allows us the apply the following Wiener-Ikehara theorem.

Theorem 4.10 (Wiener-Ikehara)**.** *Consider two Dirichlet series*

$$f(s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s}, \quad a_m \geq 0$$

And

$$g(s) = \sum_{m=1}^{\infty} \frac{b_m}{m^s}$$

such that both are absolutely convergent for Re$(s) > 1$. Also $f(s)$ is analytic on Re$(s) = 1$ except for a simple pole at $s = 1$ with residue 1, and $g(s)$ is analytic on Re$(s) = 1$, having either a simple pole at s=1 with residue η or being analytic at $s = 1$ (in which case we can take η as 0). Then if $\exists$ c such that $|b_m| \leq c|a_m|$, we have

$$\lim_{x\to\infty} \frac{\sum_{m\leq x} b_m}{x} = \eta$$

i.e.,$\sum_{m\leq x} b_m \sim \eta x$

Apply the Wiener-Ikehara theorem: let $f(s)$ be $\sum_{n=1}^{\infty} \frac{a(n)\log n}{n^s}$ where $a(n)$ is 1 if n is a prime and 0 otherwise. $f(s)$ is analytic on $\mathrm{Re}(s) \geq 1$ except for a simple pole at $s = 1$ with residue 1. Let $g(s)$ be $\sum_{n=1}^{\infty} \frac{\sum_{||\mathfrak{p}||=n} \log ||\mathfrak{p}||\, \chi \circ \phi(\mathfrak{p})}{n^s}$. We showed above that $g(s)$ is analytic on $\mathrm{Re}(s) \geq 1$ except for possibly a simple pole at $s = 1$ with residue η ($\eta = 1$ if $\chi \circ \phi$ is trivial character and 0 otherwise).

Also the coefficient of $\frac{1}{n^s}$ is at most $\sum_{||\mathfrak{p}||=n} \log ||\mathfrak{p}|| \leq [K:\mathbb{Q}]n$. Thus

$$\left| \sum_{||\mathfrak{p}||=n} \log ||\mathfrak{p}||\, \chi \circ \phi(\mathfrak{p}) \right| \leq [K:\mathbb{Q}]a(n)\log n$$

Apply Wiener-Ikehara theorem, we get that

$$\sum_{||\mathfrak{p}||\leq x} \chi \circ \phi(\mathfrak{p}) \log \mathfrak{p} \sim \eta x$$

Now let $a(n) = \sum_{||\mathfrak{p}||=n} \chi \circ \phi(\mathfrak{p}), b(n) = \sum_{||\mathfrak{p}||=n} \chi \circ \phi(\mathfrak{p}) \log \mathfrak{p}$. Doing the same partial summation as we did in the Prime number theorem proof, we get that

$$\sum_{||\mathfrak{p}||\leq x} \chi \circ \phi(\mathfrak{p}) = \begin{cases} \frac{x}{\log x} + o(\frac{x}{\log x}) & \text{if } \chi \circ \phi \text{ is the trivial character} \\ o(\frac{x}{\log x}) & \text{if otherwise} \end{cases} \tag{5}$$

(5) is the generalized version of prime number thoerem in number field extension. However, we can get more than the Prime Number Theorem from (5): we can derive Chebotarev density theorem for L/K abelian.

4.4 Chebotarev Density theorem as a corollary

Corollary 4.10.1 (Chebotarev density theorem)**.** *For $G = Gal(L/K)$ abelian, take $a \in G$. Then we have*

$$\frac{\#\{\mathfrak{p} : ||\mathfrak{p}|| \leq x, \phi(\mathfrak{p}) = a\}}{\#\{\mathfrak{p} : ||\mathfrak{p}|| \leq x\}} \to \frac{1}{|G|} \quad \textit{as } x \to \infty$$

Proof. Since G is finite abelian, it admits only 1-dimensional characters χ, and $\chi \circ \phi$ is trivial iff χ is the trivial character χ_0. Then consider

$$\sum_{||\mathfrak{p}||\leq x} \sum_{\chi \in \widehat{G}} \chi(a^{-1}\phi(\mathfrak{p})) \tag{6}$$

By orthogonality relations of characters, we know that $\sum_{\chi \in \widehat{G}} \chi(a^{-1}\phi(\mathfrak{p}))$ is 0 if $\phi(\mathfrak{p}) \neq a$ and is $|G|$ if $\phi(\mathfrak{p}) = a$. Thus (6) is $|G| \cdot \#\{\mathfrak{p} : ||\mathfrak{p}|| \leq x, \phi(\mathfrak{p}) = a\}$

However, (6) is also

$$\chi_0(a^{-1}) \sum_{||\mathfrak{p}||\leq x} \chi_0\phi(\mathfrak{p}) + \sum_{\chi \text{ non-trivial}} \chi(a^{-1}) \sum_{||\mathfrak{p}||\leq x} \chi\phi(\mathfrak{p}) \tag{7}$$

By (5), we know that (7) is $\frac{x}{\log x} + o(\frac{x}{\log x})$. Then equates two expressions of (6), we get that

$$\frac{\#\{\mathfrak{p} : ||\mathfrak{p}|| \leq x, \phi(\mathfrak{p}) = a\}}{\#\{\mathfrak{p} : ||\mathfrak{p}|| \leq x\}} = \frac{\frac{1}{|G|}(\frac{x}{\log x}) + o(\frac{x}{\log x})}{\frac{x}{\log x} + o(\frac{x}{\log x})} \to \frac{1}{|G|}$$

as $x \to \infty$ □

So we prove the Chebotarev density theorem for abelian extension.

4.5 Prime Ideal Theorem and Chebotarev for the non-abelian case

When L/K is not an abelian extension, $\mathrm{Gal}(L/K)$ doesn't admit only 1-dimensional characters. So we need to generalize L-series associated to characters of G.

Definition 4.11 (Artin L-series)**.** *For $G = Gal(L/K)$ not abelian, let ρ be an irreducible representation of G. Take $\mathcal{P}$ an unramified prime in $\mathcal{O}_L$, and let $\mathfrak{p}$ be the prime below it in $\mathcal{O}_K$. Recall that $[\frac{L/K}{\mathcal{P}}]\alpha \equiv \alpha^{||\mathfrak{p}||} \bmod \mathcal{P}$. Then $L(s, \rho, L/K)$ is defined as*

$$L(s, \rho, L/K) = \prod_{\mathfrak{p}\ unramified\ in\ \mathcal{O}_L} \frac{1}{det(\mathbb{I} - \rho[\frac{L/K}{\mathcal{P}}]) \cdot \frac{1}{||\mathfrak{p}||^s}}$$

Since determinant is an invariant under conjugation and different $\mathcal{P}$ above the same $\mathfrak{p}$ are conjugates of each other, the series is independent of the chose of $\mathcal{P}$.

Notice that $[\frac{L/K}{\mathcal{P}}]$ is diagonalizable since it has finite order in G. Also the eigenvalues satisfy the polynomial $x^f - 1 = 0$, so they are roots of unity. Recall that the character of ρ is the trace of its matrix denoted as χ_ρ

Now assume some nice properties of $L(s, \rho, L/K)$ that we will prove later on : $L(s, \rho, L/K)$ is analytic and non-zero on $\mathrm{Re}(s) \geq 1$. Then we will know that $\frac{-L'(s,\rho,L/K)}{L(s,\rho,L/K)}$ is analytic on $\mathrm{Re}(s) \geq 1$. But $\frac{-L'(s,\rho,L/K)}{L(s,\rho,L/K)}$ is also the derivative of $-\log L(s, \rho, L/K)$. So

$$\frac{-L'(s, \rho, L/K)}{L(s, \rho, L/K)} = \sum_{\mathfrak{p}\text{ unramified in }\mathcal{O}_L} \sum_{m=1}^{\infty} \frac{\log ||\mathfrak{p}|| \chi_\rho([\frac{L/K}{\mathcal{P}}]^m)}{||\mathfrak{p}||^{ms}}$$

If the dimension of ρ is n, then

$$\left| \sum_{\mathfrak{p}\text{ unramified in }\mathcal{O}_L} \sum_{m=2}^{\infty} \frac{\log ||\mathfrak{p}|| \chi_\rho([\frac{L/K}{\mathcal{P}}]^m)}{||\mathfrak{p}||^{ms}} \right| \leq n \sum_{\mathfrak{p}\text{ unramified in }\mathcal{O}_L} \sum_{m=2}^{\infty} \frac{\log ||\mathfrak{p}||}{||\mathfrak{p}||^{ms}}$$

which we proved to be convergent for $\mathrm{Re}(s) > \frac{1}{2}$ Thus $\frac{-L'(s,\rho,L/K)}{L(s,\rho,L/K)}$ has the same pole and residue on $\mathrm{Re}(s) = 1$ as $\sum_{\mathfrak{p}\text{ unramified in }\mathcal{O}_L} \frac{\log ||\mathfrak{p}|| \chi_\rho([\frac{L/K}{\mathcal{P}}])}{||\mathfrak{p}||^s}$. Then by exactly the same proof as in the abelian case we can show that

$$\sum_{||\mathfrak{p}|| \leq x} \chi_\rho([\frac{L/K}{\mathcal{P}}]) = \begin{cases} \frac{x}{\log x} + o(\frac{x}{\log x}) & \text{if } \chi_\rho \text{ is the trivial character} \\ o(\frac{x}{\log x}) & \text{if otherwise} \end{cases}$$

This proves the Prime Ideal Theorem for the non-abelian case.

Corollary 4.11.1 (Chebotarev Density theorem for non-abelian case)**.** *Let C be an arbitrary conjugacy class in $G = Gal(L/K)$, then we have*

$$\frac{\#\{\mathfrak{p} : ||\mathfrak{p}|| \leq x, [\frac{L/K}{\mathcal{P}}] \in C\}}{\#\{\mathfrak{p} : ||\mathfrak{p}|| \leq x\}} \to \frac{|C|}{|G|} \quad as\ x \to \infty$$

Proof. Let f be a class function on G that takes 1 on elements in C and 0 otherwise. Since the irreducible characters span the space of class function, we

can write f as a linear combination of irreducible characters. Say $\chi_1, ...\chi_g$ are the irreducible characters of G, then say

$$f = \sum_{i=1}^{g} a_i \chi_i$$

Also $\sum_{\mu \in G} f(\mu) = |C|$. But we also have

$$\sum_{\mu \in G} f(\mu) = \sum_{i=1}^{g} a_i \sum_{\mu \in G} \chi_i(\mu) = a_0 |G|$$

where a_0 is the coefficient of trivial character. Thus $a_0 = \frac{|C|}{|G|}$

The number of $\mathfrak{p} \subseteq \mathcal{O}_K, ||\mathcal{P}|| \leq x$ that maps to C is $\sum_{||\mathfrak{p}|| \leq x} f([\frac{L/K}{\mathcal{P}}])$, then we have

$$\sum_{||\mathfrak{p}|| \leq x} f([\frac{L/K}{\mathcal{P}}]) = \sum_{||\mathfrak{p}|| \leq x} \sum_{i=1}^{g} a_i \chi_i([\frac{L/K}{\mathcal{P}}]) = \frac{|C|}{|G|} \frac{x}{\log x} + o(\frac{x}{\log x})$$

and we have

$$\frac{\#\{\mathfrak{p} : ||\mathfrak{p}|| \leq x, [\frac{L/K}{\mathcal{P}}] \in C\}}{\#\{\mathfrak{p} : ||\mathfrak{p}|| \leq x\}} \to \frac{|C|}{|G|} \quad \text{as } x \to \infty$$

□

Now our task becomes to ensure that $L(s, \rho, L/K)$ has the nice properties we mentioned. We do this by reducing $L(s, \rho, L/K)$ into product of $L(s, \chi)$'s, in which χ are abelian characters.

For this purpose we need some properties.

1. $L(s, \rho_1 + \rho_2, L/K) = L(s, \rho_1, L/K) L(s, \rho_2, L/K)$. This comes from the linearity of $\log L(s, \rho_1 + \rho_2, L/K)$

2. Let ρ be representation of $\mathrm{Gal}(L/F)$ with character χ_ρ, and ρ^* is the representation of $\mathrm{Gal}(L/K)$ induced by ρ with character χ_{ρ^*}. Then

$$L(s, \rho^*, L/K) = L(s, \rho, L/F)/g(s, \rho)$$

for $g(s, \rho)$ being non-zero regular function. This is true also for F/K not Galois.

Proof. Take $g(s, \rho)$ to be $\prod_{\mathfrak{p} \in S} \frac{1}{\det(\mathbb{I} - \rho^*[\frac{F/K}{\mathcal{P}_F}] \cdot \frac{1}{||\mathfrak{p}||^s})}$, where S denotes the set of $\mathfrak{p} \in \mathcal{O}_K$ such that $\mathfrak{p}$ is unramified in $\mathcal{O}_F$ and ramified in $\mathcal{O}_L$, and $\mathcal{P}_F = \mathcal{P} \cap F$. Then it is sufficient to examine $\mathfrak{p}$ unramified in L and the primes in F, L that is above $\mathfrak{p}$.

Say $\mathfrak{p} = q_1 q_2 .....q_r$ in F. Let $f_i = f(q_i | \mathfrak{p})$, the inertia degree of q_i over $\mathfrak{p}$. We still denote the subgroup fixing F as H. Fix a prime $\mathcal{P} \in \mathcal{O}_L$ above $\mathfrak{p}$ and let

$\tau_i \in G$ such that $\tau_i \mathcal{P} \cap F = q_i$. Denote $[\frac{L/K}{\mathcal{P}}]$ as μ. We have the decomposition of G into cosets of H given by

$$G = \bigcup_{i=1}^{r} \bigcup_{x_i=1}^{f_i} H\tau_i\mu^{x_i}$$

This can be checked by checking that $H\tau_i\mu^{x_i} \cap H\tau_j\mu^{x_j} = \emptyset$.

Now

$$\chi_{\rho^*}(\mu^n) = \sum_{i=1}^{r} \sum_{x_i=0}^{f_i-1} \chi_\rho(\tau_i\mu^n\tau_i^{-1})$$

where $\chi_\rho(\tau_i\mu^n\tau_i^{-1}) = 0$ if $\tau_i\mu^n\tau_i^{-1}$ is not in H, because μ^{x_i} and μ^{-x_i} cancel in the middle. So it is also

$$\sum_{i=1}^{r} f_i\, \chi_\rho((\tau_i\mu\tau_i^{-1})^n)$$

Notice that $(\tau_i\mu\tau_i^{-1})^n = [\frac{L/K}{\tau_i\mathcal{P}}]^n$. It is in H iff it acts trivially in F. But $[\frac{L/K}{\tau_i\mathcal{P}}]^n|_F = [\frac{F/K}{q_i}]^n$, which is trivial iff the order of $[\frac{F/K}{q_i}]$ divides n iff $f_i|n$

Thus each factor of $\log L(s, \rho^*, L/K)$ associated to $\mathfrak{p}$ is

$$\sum_{n=1}^{\infty} \frac{1}{n||\mathfrak{p}||^{ns}}\, \chi_{\rho^*}([\frac{L/K}{\mathcal{P}}]^n)$$

$$= \sum_{i=1}^{r} f_i \sum_{n=1}^{\infty} \frac{1}{n||\mathfrak{p}||^{ns}}\, \chi_\rho((\tau_i\mu\tau_i^{-1})^n)$$

But $\chi_\rho((\tau_i\mu\tau_i^{-1})^n) = 0$ unless $f_i|n$. So it is summing over n that are multiples of f_i. Now take $n = f_i t$, t running through all the positive integers. Then the sum is

$$\sum_{i=1}^{r} \sum_{t=1}^{\infty} \frac{f_i}{f_i t||\mathfrak{p}||^{ts}}\, \chi_\rho(((\tau_i\mu\tau_i^{-1})^{f_i})^t)$$

But $||\mathfrak{p}||^{f_i} = ||q_i||$, so $(\tau_i\mu\tau_i^{-1})^{fi} = [\frac{L/K}{\tau_i\mathcal{P}}]^{f_i} = [\frac{F/K}{q_i}]$. Thus the sum is

$$\sum_{i=1}^{r} \sum_{t=1}^{\infty} \frac{1}{t||q_i||^{ts}}\, \chi_\rho\left(\left(\left[\frac{F/K}{q_i}\right]\right)^t\right)$$

This is the factor of $\log L(s, \rho, F/K)$ corresponds to q_i that are above $\mathfrak{p}$. So the proof is complete. □

We know L-series do not change under induction. We state a lemma that will be proven later.

Lemma 4.12. *Let ρ be an irreducible representation of G. Then χ_ρ is a rational linear combination of characters induced from the cyclic subgroups of G. Moreover, if ρ is non-trivial character, then it is a rational linear combination of characters induced from the non-trivial characters of cyclic subgroups of G.*

To be precise, let a denote the number of cyclic subgroups of G, and let i denote the ith cyclic subgroup. Let n_i denotes the cardinality of the ith cyclic subgroup H_i. For a fixed cyclic subgroup H_i, let ζ_{ij} be the irreducible (thus 1-dimensional) characters of H_i where j runs through 0 to $n_i - 1$, and ζ_{i0} is the trivial character. Then we have

$$\chi_\rho = \sum u_{ij}\zeta_{ij}^*$$

Where u_{ij} are rationals. When ρ is non-trivial representation on G, we can have $u_{i0} = 0, \forall i$.

If we assume the lemma, we have

$$L(s, \rho, L/K) = \prod_{ij} L(s, \zeta_{ij}, L/\Omega_i)^{u_{ij}}$$

where Ω_i is the fixed field of H_i. Moreoever ζ_{ij} are all non-trivial. Since the cyclic group is abelian, we can apply what we proved in the abelian case: $L(s, \zeta_{ij}, L/\Omega_i)$ is analytic and non-zero on $\mathrm{Re}(s) \geq 1$, so we can take rational power of it in $\mathrm{Re}(s) \geq 1$ and it is still analytic and non-zero, so the product $\prod_{ij} L(s, \zeta_{ij}, L/\Omega_i)^{a_{ij}}$ is also non-zero and analytic here. Thus we prove the nice properties of $L(s, \rho, L/K)$ required.

Now the only thing left is to show the lemma.

Proof. Recall the Frobenius reciprocity we discussed in the background section:

Suppose H is a subgroup of G, and let ψ, ϕ be two class functions. Then we have

$$\langle \phi, Res_H^G \psi \rangle_H = \langle \phi^*, \psi \rangle_G$$

Let ψ_k run through the irreducible characters of G, $0 \leq k \leq g-1$, and ψ_0 denote the trivial character. Since the induced character ${\zeta_{ij}}^*$ is a class function, we can have

$${\zeta_{ij}}^* = \sum_k r_{jik}\psi_k$$

where r_{jik} are rationals. We also know the inner product $\langle {\zeta_{ij}}^*, \psi_k \rangle_G = r_{jik}$.By Frobenius reciprocity we have

$$\langle \zeta_{ij}, Res_H^G \psi_k \rangle_H = \langle {\zeta_{ij}}^*, \psi_k \rangle_G = r_{jik}$$

Now restricting ψ_k to H_i is a character on H_i. So we have

$$\psi_k(\tau) = \sum_j b_{jik}\, \zeta_{ij}(\tau)$$

for $\tau \in H_i$. So $b_{jik} = \langle Res_H^G \psi_k, \zeta_{ij} \rangle_H = r_{jik}$. Now we have a system of equations

$${\zeta_{ij}}^* = \sum_k r_{jik}\, \psi_k$$

Now if we collect these coefficients into a matrix, and let M be the matrix below:

$$\begin{bmatrix} r_{110} & \cdots & r_{11g} \\ r_{210} & \cdots & r_{21g} \\ \vdots & \ddots & \vdots \\ r_{n_1 10} & \cdots & r_{n_1 1g} \\ \vdots & \ddots & \vdots \\ r_{n_a a0} & \cdots & r_{n_a ag} \end{bmatrix}$$

Then we have

$$\begin{bmatrix} \zeta_{11}^* \\ \vdots \\ \zeta_{1n_1}^* \\ \zeta_{21}^* \\ \vdots \\ \zeta_{2n_2}^* \\ \vdots \\ \zeta_{a1}^* \\ \vdots \\ \zeta_{an_a}^* \end{bmatrix} = M \begin{bmatrix} \psi_0 \\ \vdots \\ \psi_g \end{bmatrix}$$

We wish to show that M has a left inverse, say M^*. Then

$$M^* \begin{bmatrix} \zeta_{11}^* \\ \vdots \\ \zeta_{an_a}^* \end{bmatrix} = \begin{bmatrix} \psi_0 \\ \vdots \\ \psi_g \end{bmatrix}$$

which exists if the rank of $M = \#$ columns of M. Suppose that rank of $M < g$, then the columns of M are linearly dependent. There exists $c_0, ...c_{g-1}$ not all zero such that

$$c_0 r_{ji0} + ... + c_{g-1} r_{jig-1} = 0$$

for all j, i.

Now fix H_i and for any $\tau \in H_i$

$$\sum_{k=0}^{g-1} c_k \, \psi_k(\tau) = \sum_{k=0}^{g-1} c_k \sum_{j=0}^{n_i-1} r_{jik} \, \zeta_{ij}(\tau) = \sum_{j=0}^{n_i-1} \zeta_{ij}(\tau) \sum_{k=0}^{g-1} c_k r_{jik} = 0$$

Since each element in G generates a cyclic group, each element is in some cyclic group H_i. Thus for all $\tau \in G$, $\sum_{k=0}^{g-1} c_k \, \psi_k(\tau) = 0$. Thus $\sum_{k=0}^{g-1} c_k \, \psi_k = 0$. Then $\psi_0, ...\psi_{g-1}$ are not linearly independent. But irreducible characters of G are linearly independent, so we derive a contradiction. Thus the rank of M is g, which shows that each ψ_k can be expressed as a rational combination of ${\zeta_{ij}}^*$.

We have shown that $\psi_k = \sum_{i=1}^{a} \sum_{j=0}^{n_i-1} u_{ij} \, {\zeta_{ij}}^*$. We are going to show that if ψ_k is non-trivial then $u_{i0} = 0$.

Proof. Fix H_i. By definition of induced character, we have that $\forall g \in G$

$$\sum_{j=0}^{n_i-1} {\zeta_{ij}}^*(g) = \sum_{t\in G, tgt^{-1}\in H_i} \sum_{j=0}^{n_i-1} \zeta_{ij}(tgt^{-1}) \frac{1}{|H_i|}$$

Since ζ_{ij} runs through all characters of H_i, by the orthogonality relations of characters we know that

$$\sum_{j=0}^{n_i-1} \zeta_{ij}(tgt^{-1}) = \begin{cases} 0, & \text{if } tgt^{-1} \neq 1 \\ |H_i|, & \text{if } tgt^{-1} = 1 \end{cases}$$

But $tgt^{-1} = 1$ iff $g = 1$. Let's denote $\sum_{j=0}^{n_i-1} \zeta_{ij}(tgt^{-1})$ as $T_i(g)$. Then we know that $T_i(g) = 0$ for $g \neq 1$, and is $|G|$ when $g = 1$. Thus we know that

$$\zeta_{i0}^* = (-\sum_{j=1}^{n_i-1} {\zeta_{ij}}^*) + T_i$$

Now consider ψ_k non-trivial character of G. We have that

$$\psi_k = \sum_{i=1}^{a} \sum_{j=0}^{n_i-1} u_{ij}\, {\zeta_{ij}}^*$$

$$= \sum_{i=1}^{a} u_{i0} T_i + \sum_{i=1}^{a} \sum_{j=1}^{n_i-1} (u_{ij} - u_{i0})\, {\zeta_{ij}}^*$$

Now take the inner product with the trivial character ψ_0. We know that

$$\langle \psi_k, \psi_0 \rangle_G = \sum_{i=1}^{a} u_{i0} \langle T_i, \psi_0 \rangle_G + \sum_{i=1}^{a} \sum_{j=1}^{n_i-1} (u_{ij} - u_{i0}) \langle {\zeta_{ij}}^*, \psi_0 \rangle_G$$

But it is also 0. By Frobenius reciprocity, $\langle {\zeta_{ij}}^*, \psi_0 \rangle_G = 0$. So we have that

$$\langle \psi_k, \psi_0 \rangle_G = \sum_{i=1}^{a} u_{i0} \langle T_i, \psi_0 \rangle_G$$

$$= \sum_{i=1}^{a} u_{i0} T_i(1) = 0$$

We already know that $\psi_k - \sum_{i=1}^{a} \sum_{j=1}^{n_i-1} u_{ij}\, {\zeta_{ij}}^* = \sum_{i=1}^{a} u_{i0} T_i$. But $\sum_{i=1}^{a} u_{i0} T_i$ takes 0 on $g \neq 1$ ($T_i(g) = 0$ for each i) and also takes 0 on $g = 1$. Therefore $\sum_{i=1}^{a} u_{i0} T_i$ is identically zero. So we have $\psi_k = \sum_{i=1}^{a} \sum_{j=1}^{n_i-1} (u_{ij} - u_{i0})\, {\zeta_{ij}}^*$. This shows that ψ_k is a linear combination of characters introduced from non-trivial characters of cyclic subgroups of G, and we are done. □

□

5 Properties of Riemann zeta function and Riemann Hypothesis

The proof of the Prime Number Theorem reveals that the non-zero property of zeta function on $\mathrm{Re}(s) = 1$ gives the asymptotic formula for $\pi(x)$. The celebrated Riemann Hypothesis assumes a more precise distribution of zero of $\zeta(s)$: the non-trivial zeros are all on $\mathrm{Re}(s) = \frac{1}{2}$. And this is expected to give a better error bound to the Prime Number Theorem. The equivalent statement, or say a well-known consequence of Riemann Hypothesis is that, (Assuming Riemann Hypothesis),

$$\pi(x) = Li(x) + \mathcal{O}(\sqrt{x}\log x)$$

For the statement of Riemann Hypothesis to even make sense, we need to first define Riemann zeta function on the entire complex plane.

5.1 Gamma function and some of its properties

Let's start by defining Gamma function, a component in the functional equation and in meromorphic extension fo $\zeta(s)$.

Definition 5.1. $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt$ *for* $Re(s) > 0$

First notice that this is a well definied function. Say $\mathrm{Re}(s) = \varepsilon > 0$, then

$$|\Gamma(s)| = \left|\int_0^\infty e^{-t}t^{s-1}\right| dt \leq \int_0^\infty e^{-t}t^{\varepsilon-1}dt = \int_1^\infty e^{-t}t^{\varepsilon-1}dt + \int_0^1 e^{-t}t^{\varepsilon-1}dt$$

$\int_1^\infty e^{-t}t^{\varepsilon-1}dt$ always converges, and $\int_0^1 e^{-t}t^{\varepsilon-1}dt = \mathcal{O}(\int_0^1 t^{\varepsilon-1})$, which converges when $\varepsilon > 0$. Thus the integral converges absolutely when $\mathrm{Re}(s) > 0$

As $s \to 0$, $\int_0^1 e^{-t}t^{\varepsilon-1}dt$ goes to infinity. So as for $\mathrm{Re}(s) \leq 0$, we need other definition of $\Gamma(s)$

Below are two ways to extend the function. Each of them gives some property of $\Gamma(s)$.

1. Extension by "integrating by parts"

For $\mathrm{Re}(s) > 0$, $\int_0^\infty e^{-t}t^s dt$. By integrating by parts, we have

$$\frac{\Gamma(s+1)}{s} = \Gamma(s)$$

For $-1 < \mathrm{Re}(s) \leq 0$, $\frac{\Gamma(s+1)}{s} = \Gamma(s), s \neq 0$ is well defined and analytic. For $s = 0$,$\Gamma(s+1) = \Gamma(1) = 1$, so $\frac{\Gamma(s+1)}{s} = \Gamma(s)$ will have simple pole at $s = 0$. Thus for $-1 < \mathrm{Re}(s) \leq 0$, we can define $\Gamma(s)$ as $\frac{\Gamma(s+1)}{s}$. We obtain a meromorphic extension of $\Gamma(s)$ to $\mathrm{Re}(s) > -1$. But now we can extend it to $-2 < \mathrm{Re}(s) \leq -1$ in a similar way. Repeating the same process we can define Γ on the entire complex plane:

$$\Gamma(s) = \begin{cases} \int_0^\infty e^{-t}t^{s-1}dt, & \mathrm{Re}(s) > 0 \\ \frac{\Gamma(s+k+1)}{z(z+1)\ldots(z+k)}, & -k-1 < \mathrm{Re}(s) \leq -k, k \in \mathbb{Z}^+ \cup \{0\} \end{cases}$$

From the above formula we can find out that the poles of $\Gamma(s)$ are 0 and all the negative integers, but we can't get accurate information about zeros. Here the product represetation of $\Gamma(s)$ will tell us clearly that $\Gamma(s)$ is no-where 0.

Since

$$\lim_{n\to\infty}(1-\frac{t}{n})^n \to e^{-t}$$

and the convergence is uniform, we can plug it into the integral representation of $\Gamma(s)$ and we get

$$\Gamma(s) = \lim_{n\to\infty}\int_0^n t^{s-1}(1-\frac{t}{n})^n dt$$

By integrating by parts, this is

$$\lim_{n\to\infty}\frac{1}{n^n}\cdot\frac{n}{s}\int_0^n t^s(n-t)^{n-1}dt$$

Repeating the same process, we can get the expression of $\Gamma(s)$:

$$\lim_{n\to\infty}\frac{1}{n^n}\cdot\frac{n}{s}\cdot\frac{n-1}{s+1}\cdot.....\cdot\frac{1}{s+n-1}\cdot\int_0^n t^{s+n-1}dt$$

$$=\lim_{n\to\infty}\frac{1}{n^n}\cdot\frac{n}{s}\cdot.....\cdot\frac{1}{s+n-1}\cdot\frac{n}{s+n}$$

$$=\lim_{n\to\infty}\frac{n^s}{s}\cdot\frac{1}{s+1}\cdot\frac{2}{s+2}.....\frac{n}{s+n}$$

This product converges for $\mathrm{Re}(s) > 0$. Now insert a "convergenve factor" to make this product converge everywhere.

Lemma 5.2.

$$\lim_{n\to\infty}\sum_{k=1}^{n}\frac{1}{k}-\log n \quad \textit{exists}$$

Proof. Write $\log n$ as

$$(\log 2-\log 1)+(\log 3-\log 2)+.....+(\log n-\log n-1)$$

So when n is finite , the sum is

$$\sum_{k=1}^{n-1}\frac{1}{k}-\log\frac{k+1}{k}+\frac{1}{n}$$

Use the Taylor expansion of $\log(1+\frac{1}{k})$

$$\log(1+\frac{1}{k})=\frac{1}{k}-\frac{1}{2k^2}+\frac{1}{3k^3}-\frac{1}{4k^4}+.....$$

Thus we have

$$\frac{1}{k}-\log(1+\frac{1}{k})=\frac{1}{2k^2}-\frac{1}{3k^3}+\frac{1}{4k^4}+.....$$

Which is less than $\frac{1}{2k^2}$

Thus

$$\sum_{k=1}^{n-1} \frac{1}{k} - \log \frac{k+1}{k} + \frac{1}{n} \leq \sum_{k=1}^{n-1} \frac{1}{2k^2} + \frac{1}{n}$$

Take the limit as $n \to \infty$,$\sum_{k=1}^{n-1} \frac{1}{2k^2} + \frac{1}{n}$ converges. Also $\frac{1}{k} - \log \frac{k+1}{k} \geq 0$. Thus the limit exists. We denote the limit as γ, the Euler constant. $\square$

Now go back to $\Gamma(s)$. From the product representation of $\Gamma(s)$ we know that

$$\frac{1}{\Gamma(s)} = \lim_{n\to\infty} sn^{-s} \prod_{k=1}^{n} (1 + \frac{s}{k})$$

$$= \lim_{n\to\infty} s \cdot e^{s(\sum_{n=1}^{\infty} \frac{1}{n} - \log n)} \prod_{k=1}^{n} (1 + \frac{s}{k}) e^{-\frac{s}{k}}$$

$$= se^{s\gamma} \prod_{k=1}^{\infty} (1 + \frac{s}{k}) e^{-\frac{s}{k}}$$

Which converges everywhere. Thus we can take

$$\frac{1}{se^{s\gamma} \prod_{k=1}^{\infty} (1 + \frac{s}{k}) e^{-\frac{s}{k}}}$$

as the meromorphic extension of $\Gamma(s)$ to the entire complex plane. This product representation shows that $\Gamma(s)$ is non-where 0.

5.2 Analytic continuation of $\zeta(s)$

Now we are in a good position to define the analytic continuation of $\zeta(s)$ to the entire complex plane.

When $\mathrm{Re}(s) > 0$,

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

Since the integral converges absolutely. Then

$$\lim_{n\to\infty} \sum_{k=1}^{n} \int_0^\infty e^{-kt} t^{s-1} dt = \lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{k^s} \int_0^\infty e^{-t} t^{s-1} dt = \Gamma(s)\zeta(s)$$

But on the other hand we also have

$$\lim_{n\to\infty} \sum_{k=1}^{n} \int_0^\infty e^{-kt} t^{s-1} dt = \int_0^\infty \sum_{k=1}^{n} e^{-kt} t^{s-1} dt = \int_0^\infty \frac{t^{s-1}}{e^t - 1} dt$$

Thus we have for $\mathrm{Re}(s) > 1$

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

For $\mathrm{Re}(s) \leq 0$ consider

$$\int_0^\infty \frac{t^{s-1}}{e^t - 1} dt = \int_1^\infty \frac{t^{s-1}}{e^t - 1} dt + \int_0^1 \frac{t^{s-1}}{e^t - 1} dt$$

The integral on $[1, \infty)$ certainly converges. For $\int_0^1 \frac{t^{s-1}}{e^t-1} dt$, consider the Laurent expansion

$$\frac{1}{e^t - 1} = \frac{1}{t} + A_0 + A_1 t + A_2 t^2 + ...$$

Where A_i are constant. The expression converges at $t = 1$. Apply Laurent expansion we get

$$\int_0^1 \frac{t^{s-1}}{e^t - 1} dt = \frac{1}{s-1} + \frac{A_0}{s} + \frac{A_1}{s+1} + ...$$

Which is analytic except for possible simple poles at $s = 1, 0, -1, -2, ...$ Now we can take

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

As the meromorphic extension of $\zeta(s)$ to the entire complex plane. Also $\frac{1}{\Gamma(s)}$ has simple zeros at $s = 0, -1, -2, ...$, which cancel out the possible simple poles of $\int_0^1 \frac{t^{s-1}}{e^t-1} dt$ except for at $s = 1$. So the the meromorphic extension of $\zeta(s)$ to the entire complex plane is analytic everywhere except for a simple pole at $s = 1$.

5.3 Trivial zeros of $\zeta(s)$

Now that we have analytic extension of $\zeta(s)$, it's time to consider its zeros. Consider the Laurent Expansion

$$\frac{1}{e^t - 1} = \frac{1}{t} + A_0 + A_1 t + A_2 t^2 + ...$$

$$\frac{1}{e^{-t} - 1} = -\frac{1}{t} + A_0 - A_1 t + A_2 t^2 - .....$$

Summing up the two equations we get

$$-1 = 2A_0 + 2A_2 t^2 + 2A_4 t^4 + ...$$

This forces A_{2k} to be 0 for k positive integers. Now plug $s = -2k \quad (k \geq 1)$ into expression of $\zeta(s)$, we have

$$\zeta(s) = \frac{1}{\Gamma(-2k)} \left(\frac{1}{-2k-1} + \frac{A_0}{-2k} + \frac{A_1}{-2k+1} + ... + \int_1^\infty \frac{t^{s-1}}{e^t - 1} dt \right)$$

The pole at $\frac{A_{2k}}{-2k+2k}$ is cancelled by $A_{2k} = 0$ and $\frac{1}{\Gamma(-2k)} = 0$. Thus $\zeta(-2k) = 0$.Thus even negative integers are zeros of $\zeta(s)$. It turns out that they are the only zeros on the region $\mathrm{Re}(s) \geq 1$ and $\mathrm{Re}(s) \leq 0$, and we are going to show this by deriving a functional equation that $\zeta(s)$ satisfies.

5.4 The functional equation of $\zeta(s)$ and the proof from Riemann's original paper

Consider

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

$\phi(s)$ is analytic everywhere since the pole of $\zeta(s)$ is cancelled by $(s-1)$ and the pole of $\Gamma(\frac{1}{2}s)$ is cancelled by the trivial zeros of $\zeta(s)$ and s.

Theorem 5.3. *$\phi(s)$ satisfies the functional equation*

$$\phi(s) = \phi(1-s)$$

Let's see what happens if the functional equation is true. Say

$$\frac{1}{2}s(s-1)\pi^{-\frac{1}{2}s}\Gamma(\frac{1}{2}s)\zeta(s) = \frac{1}{2}s(s-1)\pi^{-\frac{1}{2}(1-s)}\Gamma(\frac{1-s}{2})\zeta(1-s) \tag{8}$$

When $\mathrm{Re}(s) \leq 0$, $\mathrm{Re}(1-s) \geq 1$. So $\zeta(1-s)$ and $\Gamma(\frac{1-s}{2})$ are non-zero. s is cancelled by the pole of $\zeta(1-s)$ at $s = 0$. Thus the left of equation (8) is zero-free, and so should be the right. That means that for $\mathrm{Re}(s) \leq 0$, the zero of $\zeta(s)$ can only appears at the pole of $\Gamma(\frac{1}{2}s)$. Also $\zeta(s) \neq 0$ for $s = 0$ because the simple pole of $\Gamma(\frac{1}{2}s)$ there is cancelled by s. This means the zeros of $\zeta(s)$ on $\mathrm{Re}(s) \leq 0$ are exactly the negative even integers $s = -2, -4, ...$

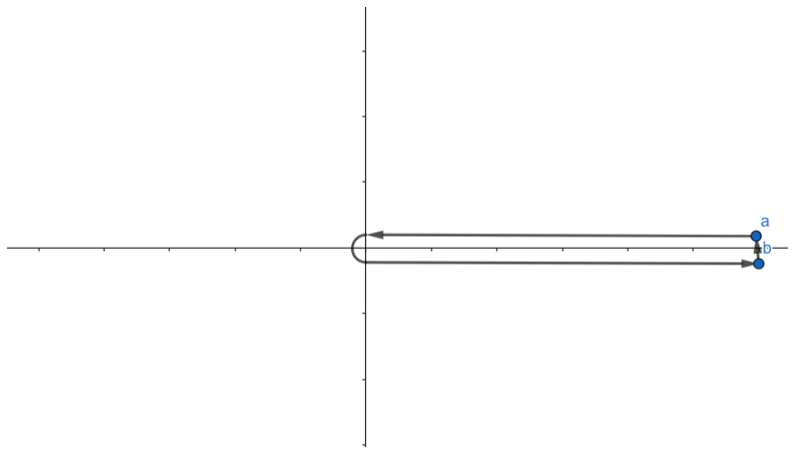
Moreoever, for $0 < \mathrm{Re}(s) < 1$, s is a zero of $\zeta(s)$ iff it's a zero of $\zeta(1-s)$ because other factors in $\phi(s)$ and $\phi(1-s)$ are analytic and non-zero. Thus the zeros of $\zeta(s)$ in $0 < \mathrm{Re}(s) < 1$ is symmetric of $s = \frac{1}{2}$.

Riemann proved the functional equation of $\zeta(s)$ in the first page of [3], which is illustrated as below. The basic idea is to consider

$$\int_{\infty}^{\infty} \frac{(-x)^{s-1}}{e^x - 1} dx \tag{9}$$

for $s < 0$ and compute the integral on two contours.

The first way is to take a contour starting from a point a that is above x on real line by distance ε; then go all the way to 0, and then go to point b that is below x by distance ε, and eventually go back to a. We denote this contour as P_1. Equation 9 is the integral on this contour when $M \to \infty$ and $\varepsilon \to 0$.



Since

$$a = xe^{\varepsilon\, i}\ ,\ b = x^{-\,\varepsilon\, i}$$

we have

$$-a = xe^{\pi+\varepsilon\, i}\ ,\ -b = xe^{\pi-\varepsilon\, i}$$

So

$$(-a)^{s-1} = e^{(s-1)\log x+(s-1)(\pi+\varepsilon)i}$$

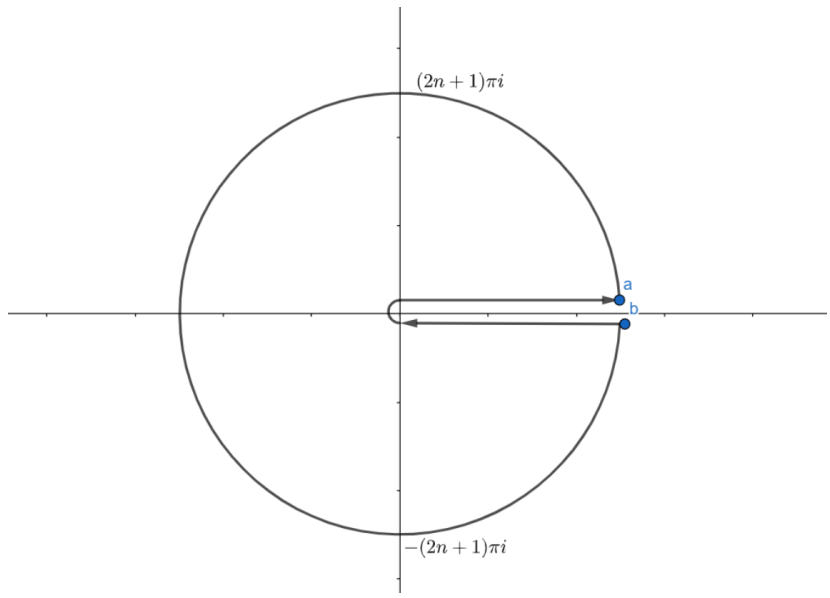
Here we take the angle of $\log x$ to be between πi and $-\pi i$, so the $\log x$ is continous on positive real axis and has discontinuity on negative real axis. P_1 on the positive half plane so the logarithm function is continous. The integral along P_1 is

$$\lim_{x\to\infty,\varepsilon\to 0}\int_0^x \frac{(-a)^{s-1}}{e^a-1}da + \int_x^0 \frac{(-b)^{s-1}}{e^b-1}db$$

When we take the limit, e^a-1, e^b-1 will be very closed to e^x-1, So the integral will be

$$\begin{aligned}
&\lim_{x\to\infty,\varepsilon\to 0}\int_0^\infty \frac{(-a)^{s-1}-(-b)^{s-1}}{e^x-1}dx \\
&= \frac{x^{s-1}(e^{(s-1)\pi i}-e^{-(s-1)\pi i})}{e^x-1}dx \\
&= (e^{-\pi si}-e^{\pi si})\int_0^\infty \frac{x^{s-1}}{e^x-1}dx \\
&= -2i\sin\pi s\zeta(s)\,\Gamma(s) \qquad (10)
\end{aligned}$$

Another way to evaluate the integral $\int_\infty^\infty \frac{(-x)^{s-1}}{e^x-1}dx$ is to consider the contour that starts from a little bit above $(2n+1)\pi$ and goes counterclockwise along the circle with radius $(2n+1)\pi$ and center as origin until a little bit below $(2n+1)\pi$. Then goes left all the way to the origin, goes above the positive real axis and back to where we start. We denote this path as P_2.



We also denote the contour going counterclockwise of the circle as C. Then

$$P_2 = C - P_1$$

Also notice that $\frac{(-x)^{s-1}}{e^x-1}$ is analytic along P_2 because the poles only appear at $2n\pi i$, which is not on P_2

Now as $n \to \infty$, the integral of $\frac{(-x)^{s-1}}{e^x-1}$ along C tends to 0. We show this by $M - L$ estimation.

First find a upper bound for $|\frac{1}{e^x-1}|$. This is the same as finding a lower bound for $|e^x - 1|$. Since $e^x - 1$ is continuous, $\exists\, \varepsilon$ such that if $|y - (2n+1)\pi i| < \varepsilon$, then we have $|(e^y - 1) - (-1 - 1)| < \frac{1}{4}$, which means $\frac{7}{4} < |e^y - 1| < \frac{9}{4}$. Now take a circle C_1 with center at $(2n+1)\pi$ and radius ε. On C_1, $|\frac{1}{e^y-1}|$ is bounded from above. So as the circle C_2 with radius ε and center $-(2n+1)\pi i$. Now say C_1, C_2 intersect the big circle at points with x-coordinate t. So for $-t < \mathrm{Re}(x) < t$, $\frac{1}{e^x-1}$ is bounded from above.

For $t \leq \mathrm{Re}(x) < (2n+1)\pi$ and $-(2n+1)\pi < \mathrm{Re}(x) \leq -t$, $|\frac{1}{e^x-1}|$ is bounded above by $\frac{1}{e^t-1}$. Thus on the entire circle, $|\frac{1}{e^x-1}|$ is bounded from above, say, by c.

The upperbound for $|(-x)^{s-1}|$ is $((2n+1)\pi)^{s-1}$

Thus by $M - L$ estimation, we have

$$\int_C \frac{(-x)^{s-1}}{e^x - 1} dx \leq (4n+2)\pi^2((2n+1)\pi)^{s-1}c$$

But $\mathrm{Re}(s) < 0$ by our assumption, so the exponent is negative. Since the integral of an entire function doesn't depend on its path, we can take $n \to \infty$, then $(4n+2)\pi^2((2n+1)\pi)^{s-1}C \to 0$. Thus the integral in 8 can only be 0.

Therefore

$$-\int_{P_1} \frac{(-x)^{s-1}}{e^x-1}dx = \int_{P_2} \frac{(-x)^{s-1}}{e^x-1}dx$$

On the other hand, by residue theorem,

$$\int_{P_2} \frac{(-x)^{s-1}}{e^x-1} = 2\pi i(\sum \text{residues}) \tag{11}$$

The poles inside P_2 are at $s = 0, \pm 2\pi i, \pm 4\pi i, ... \pm 2n\pi i$ for radius being $(2n+1)\pi$. For a pole at $2k\pi i$, the residue is:

$$\lim_{x\to 2k\pi i} \frac{(-x)^{s-1}(x-2k\pi i)}{e^x - e^{2k\pi i}} = \lim_{x\to 2k\pi i} \frac{(-2k\pi i)^{s-1}}{\frac{e^x - e^{2k\pi i}}{x-2k\pi i}} = (-2k\pi i)^{s-1}$$

Plug this into equation (11) , we have

$$\int_{\infty}^{\infty} \frac{(-x)^{s-1}}{e^x-1}dx = -2\pi i \sum_{n=1}^{\infty}[(-2n\pi i)^{s-1} + (2n\pi i)^{s-1}]$$

$$= -2\pi i \cdot 2^{s-1}(i^{s-1} + (-i)^{s-1}) \cdot \sum_{n=1}^{\infty} \frac{1}{n^{1-s}}$$

Equate the two expression for $\int_{\infty}^{\infty} \frac{(-x)^{s-1}}{e^x-1}dx$, we get that

$$\sin \pi s \zeta(s)\,\Gamma(s) = (2\pi)^s \zeta(1-s) \sin \frac{\pi s}{2} \tag{12}$$

Here we cite two functional equations of $\Gamma(s)$ from page 250 of [17]:

$$\Gamma(\frac{1+s}{2})\,\Gamma(\frac{1-s}{2}) = \frac{\pi}{\cos\frac{\pi s}{2}}$$

$$\Gamma(\frac{s}{2})\,\Gamma(s+\frac{1}{2}) = \sqrt{2\pi}2^{\frac{1}{2}-s}\,\Gamma(s)$$

Both of the above equations can be derived from the product presentation of $\Gamma(s)$. Plug

$$\Gamma(s) = \frac{\Gamma(\frac{s}{2}\pi)}{\sqrt{2\pi}2^{\frac{1}{2}-s}\cos\frac{\pi s}{2}\,\Gamma(\frac{1-s}{2})}$$

into equation (12) and do some algebraic manipulation, we will eventually get

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

Thus $\phi(s) = \frac{1}{2}s(s-1)\pi^{-\frac{s}{2}}\zeta(s)\,\Gamma(\frac{s}{2})$ will have the property that $\phi(s) = \phi(1-s)$ for $\mathrm{Re}(s) < 0$. But both $\phi(s)$ and $\phi(1-s)$ are analytic on the entire complex plane. So if they agree on $\mathrm{Re}(s) < 0$, they will agree on the entire complex plane. Thus we finish the proof for the functional equation for $\zeta(s)$

We have some other facts about the zeros of $\zeta(s)$. $\zeta(s)$ has infinitely many zeros in the critical strip, and the number of zeros of $\zeta(s)$ in the rectangle $0 < \mathrm{Re}(s) < 1, 0 < Im(s) < T$, denoted as $N(T)$, is approximately $\frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi}$. Readers can refer to page 19 of [6] for detailed proof.

5.5 Riemann's Hypothesis and the error of the Prime Number Theorem

We mentioned earlier an equivalent statement of Riemann's Hypothesis: All zeros of $\zeta(s)$ in critical strip are on $\mathrm{Re}(s) = \frac{1}{2}$ iff $\pi(x) = Li(x) + \mathcal{O}(\sqrt{x}\log x)$. Let's see why the equivalence should be true.

Recall our proof for asymptotic formula for prime number theorem. We were largely dealing with $\psi(x)$ and we didn't get into $\pi(x)$ until the very last moment. Let's follow the same procedure here. For the sake of convenience let us define one more arithematic function besides $\psi(x), \Lambda(x)$.

Definition 5.4. *We define $\theta(x)$ such that*

$$\theta(x) = \sum_{p \leq x} \log p$$

Notice that by definition of $\psi(x), \theta(x)$,

$$\psi(x) = \theta(x) + \theta(x^{\frac{1}{2}}) + \theta(x^{\frac{1}{3}}) + ... + \theta(x^{\frac{1}{m}})$$

Where $x^{\frac{1}{m}} \geq 2$ and $x^{\frac{1}{m+1}} < 2$. But

$$\psi(x) - \theta(x) \leq m\theta(x^{\frac{1}{2}}) \leq \frac{\log x}{\log 2}\theta(x^{\frac{1}{2}})$$

Also we cite the fact that $\theta(x) = \mathcal{O}(x)$ from page 83 of ([17]). So we know that

$$\psi(x) - \theta(x) = \mathcal{O}(\sqrt{x}\log x)$$

This difference is way smaller than $\frac{x}{\log x}$. We can see in the following sketch of proof that this error is always smaller than $\psi(x) - x$, so we if we can get the error bound for $\psi(x) - x$, we can get it for $\theta(x) - x$.

The reason we use $\psi(x)$ is that we actually have a very precise formula for $\psi(x)$ which gives us insight of how the location of zero can determine the error bound of the Prime Number Theorem. This is the Von-Mangoldt's formula:

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} + \sum_{n=1}^{\infty} \frac{x^{-2n}}{2n} - \frac{\zeta(0)'}{\zeta(0)} \quad (x > 1) \tag{13}$$

Where ρ is the zero of $\zeta(s)$ inside critical strip. This formula can be derived by evaluating the integral $\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} -\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}dx$ in two ways, one way gives $\psi(x)$ and the other way gives the right of equation (13). The detailed proof of this formula is in chapter 3 of [6].

As we can see, $\psi(x) - x$ consists of a constant, $-\sum_{\rho}\frac{x^{\rho}}{\rho}$ where ρ is the zeros in the critical strip, and $-\sum_{\rho}\frac{x^{\rho}}{\rho}$ when ρ is the trivial zeros.

Notice that $-\sum_{\rho \text{ trivial zeros}}\frac{x^{\rho}}{\rho}$ behaves even nicer than the constant as it will get smaller when $x \to \infty$. So it contributes nothing to the error $\psi(x) -$

x (That's why we say these zeros are trivial). Therefore, the error term is dominated by $\sum_\rho \frac{x^\rho}{\rho}$ because they gets infinite as $x \to \infty$. We can see from here that $\zeta(s)$ being non-zero on $\mathrm{Re}(s) = 1$ is crucial to the proof of $\psi(x) \sim x$: If $\zeta(s)$ has a zero on $\mathrm{Re}(s) = 1$ then $\sum_\rho \frac{x^\rho}{\rho}$ would no longer be a minor term compare to x, and the asymptotic formula is no longer true.

Now say we want to minimize the error of approximating $\pi(x)$ by $Li(x)$, which is $|\pi(x) - Li(x)|$. Since we derive $\pi(x)$ from $\psi(x)$ we would hope to minimize $\psi(x) - x$, which is to minimize $\sum_\rho \frac{x^\rho}{\rho}$. Since the real part of ρ determines how x^ρ grows, we may hope that $\mathrm{Re}(\rho)$ to very closed to 0. However, we proved in the functional equation that zeros appear in pairs: if ρ is a zero in the critical strip then $1 - \rho$ will also be a zero. So if $\mathrm{Re}(\rho)$ is far from $\frac{1}{2}$, either ρ or $1 - \rho$ would have big real part. Therefore, the best hope for us is that all the zeros of $\zeta(s)$ has real part being $\frac{1}{2}$, and this is why we care about Riemann Hypothesis: It gives the smallest error bound for $\psi(x) - x$ and thus $\pi(x) - Li(x)$.

To go from here, if we assume that Riemann Hypothesis is true, then we can bound $\psi(x)$ by

$$\int_{x-1}^{x} \psi(t)dt \leq \psi(x) \leq \int_{x}^{x+1} \psi(t)dt$$

Then plug in Mangold's formula and that $\rho = \frac{1}{2} + it$. We can ignore$-\frac{\zeta(0)'}{\zeta(0)} + \sum_{n=1}^{\infty} \frac{x^{-2n}}{2n}$.

Now we need to use the fact that the vertical density of zeros is less than $2\log T$. i.e., for large enough T, the number of zeros ρ for $T \leq Im(\rho) \leq T + 1$ is less than $2\log T$, and the proof is given in page 71 of [6]. This ensure that there won't be too many zeros anyway, so when we sum up the terms $\frac{x^\rho}{\rho}$ it is dominant by $\sqrt{x}$. Eventually we can get the following bound:

$$x - C\sqrt{x}\log x^2 \leq \int_{x-1}^{x} \psi(t)dt \leq \psi(x) \leq \int_{x}^{x+1} \psi(t)dt \leq x + C\sqrt{x}\log x^2$$

Where the $\sqrt{x}$ comes from estimating $|(x+1)^\rho - x^\rho|$ and $\log x^2$ comes from summing up the term $|\frac{1}{\rho(\rho+1)}|$, where we need the vertical density of zeros. Now we have that

$$\psi(x) = x + \mathcal{O}(\sqrt{x}\log x^2)$$

The error term here is less than $\psi(x) - \theta(x)$, so we also have that

$$\theta(x) = x + \mathcal{O}(\sqrt{x}\log x^2)$$

To go from $\theta(x)$ to $\pi(x)$, Notice that

$$\pi(x) = \sum_{2 \leq n \leq x} \frac{\theta(n) - \theta(n-1)}{\log n}$$

And $Li(x) = \int_2^x \frac{1}{\log t} dt$. The upper Riemann sum $Li^*(x)$ is

$$\int_2^3 \frac{1}{\log 2} + \int_3^4 \frac{1}{\log 3} + \ldots\ldots + \int_{[x]-1}^{[x]} \frac{1}{\log[x]-1} + \int_{[x]}^{x} \frac{1}{\log[x]} = \sum_{n=2}^{[x]-1} \frac{1}{\log n} + \frac{x - [x]}{\log[x]}$$

Then we have

$$\pi(x) - Li^*(x) = \sum_{n=2}^{[x]} \frac{\theta(n) - \theta(n-1) - 1}{\log n} + \mathcal{O}(1)$$

Apply Abel's identity:

$$\sum_{n=2}^{[x]} \frac{\theta(n) - \theta(n-1) - 1}{\log n} + \mathcal{O}(1) = \frac{\theta(x) - x}{\log x} + \int_2^{[x]} \frac{\theta(t) - t}{t \log t^2} + \mathcal{O}(1)$$

Then plug in $\theta(x) - x = \mathcal{O}(\sqrt{x} \log x)$, we can get that

$$|\pi(x) - Li^*(x)| \leq C\sqrt{x} \log x$$

Similarly, let $Li_*(x)$ denote the lower Riemann sum of $Li(x)$, we can get $|\pi(x) - Li_*(x)| \leq C\sqrt{x} \log x$. Thus we get

$$|\pi(x) - Li(x)| \leq \mathcal{O}(\sqrt{x} \log x)$$

So assuming the Riemann Hypothesis, we get the intended bound.

6 Artin's conjecture on primitive roots

Recall that

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{j_n}{n^s} = \sum_{I \in \mathcal{O}_K} \frac{1}{||I||}$$

Where j_n is the number of I such that $||I|| = n$. This is a natural extension of Riemann zeta function which shares lots of asymptotic behavior with $\zeta(s)$. It turns out that $\zeta_K(s)$ also has meromorphic extension to the entire complex plane and also satisfies a functional equation. The proof involves use of higher dimensional Gamma function. Readers can refer to page 7 of [18] for detailed proof. It should be not surprising that $\zeta_K(s)$ has its own version of Riemann Hypothesis. This is the Generalized Riemann Hypothesis:

Let ρ be zeros of $\zeta_K(s)$ such that $0 < \mathrm{Re}(\rho) < 1$, then $\mathrm{Re}(\rho) = \frac{1}{2}$.

6.1 Artin's conjecture on primitive roots

Here we will present a corollary of generalized Riemann Hypothesis: Artin's conjecture on primitive roots

Definition 6.1. *We say that a is a primitive root* $\bmod p$ *if the order of a* $\bmod p$ *is $p-1$. i.e., $a^{\frac{p-1}{q}}$ is not congruent to* $1 \bmod p$ *for any prime $q|p-1$.*

Then the Artin's conjecture on primitive roots is stated as follow:

For any $a \in \mathbb{Z}$ such that $a \neq 0, \pm 1$ or any perfect square, there exists infinitely many primes p such that a is a primitive root mod p. What's more,

fix a, denote $N_a(x)$ as the number of primes $p \leq x$ such that a is a primitive root mod p, then we have the following asymptotic formula:

$$N_a(x) \sim A(a)\frac{x}{\log x}$$

In which A(a) is a non-zero constant depending on a.

Artin's primitive root conjecture was proven by Hooley in 1967 assuming the generalized Riemann Hypothesis and the proof is contained in [7]. In fact he gets an error bound for $N_a(x)$:

$$N_a(x) = A(a)\frac{x}{\log x} + \mathcal{O}(\frac{x \log\log x}{\log x^2})$$

And he gave an expression for $A(a)$. I will present intuition and a sketch of how the proof uses generalized Riemann's Hypothesis, but the computational details will be omitted. Here we define some notations that are going to be used in the proof:

$R(q,p)$ denotes the event that "$p \equiv 1 \bmod q$ and $a^{\frac{p-1}{q}} \equiv 1 \bmod p$". Notice that a is a primitive root mod p iff $R(p,q)$ doesn't happen for any prime q.

$P_a(x,k)$ (k is square free) denotes the number of $p \leq x$ such that $R(p,q)$ holds for any prime $q|k$.

Lemma 6.2. *If k_1, k_2 are co-prime and square-free, then p is counted by $P_a(x, k_1k_2)$ iff p is counted by $P_a(x,k_1)$ and $P_a(x,k_2)$*

Proof.

$$p \text{ is counted by } P_a(x,k_1) \text{ iff } \forall q|k_1 \quad \begin{cases} p \equiv 1 \bmod q \\ a^{\frac{p-1}{q}} \equiv 1 \bmod p \end{cases}$$

And by Bezout's lemma, for two primes q_1, q_2 that are co-prime, we have

$$a^{\frac{p-1}{q_1}} \equiv 1 \bmod p \text{ and } a^{\frac{p-1}{q_2}} \equiv 1 \bmod p \text{ iff } a^{\frac{p-1}{q_1q_2}} \equiv 1 \bmod p$$

By Chinese Reminder theorem, for two primes q_1, q_2 that are co-prime, we have

$$p \equiv 1 \bmod q_1 \text{ and } p \equiv 1 \bmod q_2 \text{ iff } p \equiv 1 \bmod q_1q_2$$

Since k_1 is square free, each of its prime factor is co-prime to others, so we have

$$a^{\frac{p-1}{k_1}} \equiv 1 \bmod p \text{ and } p \equiv 1 \bmod k_1$$

Same for k_2. But now k_1, k_2 is co-prime. So by the same reasoning, p is counted by $P_a(x,k_1)$ and $P_a(x,k_2)$ iff

$$a^{\frac{p-1}{k_1k_2}} \equiv 1 \bmod p \text{ and } p \equiv 1 \bmod k_1k_2$$

Which is true iff p is counted in $P_a(x,k_1k_2)$ □

Since by definition,

$N_a(x) =$ the number of $p \leq x$ - the number of $p \leq x$ such that $R(p,q)$ holds for some q

Then by inclusion-exclusion principle, the number of $p \leq x$ that satisfies $R(p,q)$ for some prime q is:

$$\sum_i P_a(x,q_i) - \sum_{i,j} P_a(x,q_iq_j) + \sum_{i,j,k} P_a(x,q_iq_jq_k) + ... = -\sum_{k=2}^{\infty} P_a(x,k)\mu(k)$$

And we can think of $P_a(x,1)$ as the number of all the primes $p \leq x$. Then we have

$$N_a(x) = \sum_{k=1}^{\infty} P_a(x,k)\mu(k)$$

So we have expression of $N_a(x)$ in terms of $P_a(x,k)$. But what exactly is $P_a(x,k)$? It turns out that $P_a(x,k)$ can be categorized in terms of algebraic extension.

6.2 Categorizing $P_a(x,k)$ by algebraic number theory

First if a is an hth power (h must be odd because a is not a square), we take $k_1 = \frac{k}{(h,k)}$. We do this essentially because we want $x^{k_1} - a$ to be irreducible.

Now

p counted by $P_a(x,k)$ iff for all $q|k$ $\begin{cases} p \equiv 1 \bmod q \\ a^{\frac{p-1}{q}} \equiv 1 \bmod p \text{ i.e., } a \text{ is a } q\text{th power mod } p \end{cases}$

But if $q|h$, then a is automatically a qth power. So essentially we only need to ensure that

$$p \equiv 1 \bmod k \text{ and } a^{\frac{p-1}{k_1}} \equiv 1 \bmod p$$

Now consider $\mathbb{Q}(\zeta^m)/\mathbb{Q}$ and $Gal\,\mathbb{Q}(\zeta^m)/\mathbb{Q} = G$. We have shown that $p \equiv 1 \bmod k$ iff p splits completely in $\mathbb{Q}(\zeta^m)/\mathbb{Q}$

$a^{\frac{p-1}{k_1}} \equiv 1 \bmod p$ iff a is a k_1th power iff $u^{k_1} - a$ has a solution in $\mathbb{F}_p^*$. From basic number theory we know that $u^{k_1} - a$ has a solution iff it has k_1 solutions, which happens iff $u^{k_1} - a$ splits into linear factor in $\mathbb{F}_p^*$.

Here we cite a lemma from algebriac number theory which is proven in [10]

Lemma 6.3. *Let α to be an algebraic integer and $f(x)$ is the minimal polynomial of α. For $p \nmid [\mathbb{Q}(\alpha) : \mathbb{Q}]$, if*

$$f(x) = \prod_{i=1}^{k} g_i(x)^{e_i} \bmod p$$

Then

$$p = \prod_{i=1}^{k} {q_i}^{e_i}$$

in $\mathbb{Q}(\alpha)$, and the degree of $g_i(\alpha) = f(q_i|p)$

We want to apply this lemma to $\mathbb{Q}(a^{\frac{1}{k_1}})/\mathbb{Q}$. But we need to make sure that $u^{k_1} - a$ is irreducible. Suppose it is not, then say $[\mathbb{Q}(a^{\frac{1}{k_1}}) : \mathbb{Q}] = m \;\; m|k_1$. Then let q be a prime factor of $\frac{k_1}{m}$. Since $q|k_1$, $a^{\frac{1}{q}} \in \mathbb{Q}(a^{\frac{1}{k_1}})$. so $\mathbb{Q}(a^{\frac{1}{q}})/\mathbb{Q}$ is a subextension of $\mathbb{Q}(a^{\frac{1}{k_1}})/\mathbb{Q}$ with degree q. so $q|m$. But this is impossible because k_1 is squarefree, so we reach a contradiction, so $u^{k_1} - a$ is irreducible. And by our assumption $p \nmid k_1$. Then the lemma says that $u^{k_1} - a$ splits completely in $\mathbb{F}_p$ iff p splits completely in $\mathbb{Q}(a^{\frac{1}{k_1}})$.

Now we finally establish the equivalence: p is counted by $P_a(x,k)$ iff p splits completely in $\mathbb{Q}(\zeta^k)$ and in $\mathbb{Q}(a^{\frac{1}{k_1}})$. But p splits in two fields iff it splits in the composite field (proven in chapter 4 of [10]). So We have

$$p \text{ is counted by } P_a(x,k) \leftrightarrow p \text{ splits completely in } Q(\zeta^k, a^{\frac{1}{k_1}})$$

6.3 Where the Generalized Riemann Hypothesis gets into place

Now we know that $P_a(x,k)$ counts the number of primes $\leq x$ that splits completely in $Q(\zeta^k, a^{\frac{1}{k_1}})$. But p splits completely iff it's mapped to the identity of the Galois group. Let $n_k = [\mathbb{Q}(\zeta^k, a^{\frac{1}{k_1}}) : \mathbb{Q}]$. Chebotarev Density theorem tells us that such primes has density $\frac{1}{n_k}$. Then $P_a(x,k)$ should be $\frac{1}{n_k}\frac{x}{\log x}$. Plug these into the expression of $N_a(x)$, we will get that

$$N_a(x) = \sum_{k=1}^{\infty} \frac{\mu(k)}{n_k} \frac{x}{\log x} + \text{error}$$

We will calculate the $\sum_{k=1}^{\infty} \frac{\mu(k)}{n_k}$ later, and this is indeed the expression for $A(a)$ in Hooley's proof.

The problem with this intuition is that the error of Chebotarev Density theorem is too big to be directly plugged into the expression. We need some kind of bound to the error such that after our algebraic manipulation the error can still stay as an error term. And that's where the Generalized Riemann Hypothesis comes in: it can lead to a more precise bound for the Prime Number Theorem (and thus Chebotarev Density theorem), such that there is more "room" for approximation. Assuming Generalized Riemann Hypothesis, Hooley essentially derived the Prime Ideal Theorem and effective form of Chebotarev Density theorem. However, if we then plug in the effective form of Chebotarev, we still couldn't get then error to be small enough. The reason is that we don't have much control on the sign of $\mu(k)$, so during the approximation we have to think it as 1, and that causes the error to blow up.

What Hooley did in his proof is to decompose $N_a(x)$ into four parts. He chooses each part carefully that when he applies the corollary of generalized Riemann Hypothesis, the error of each one won't blow up. Eventually he shows that $\sum_{k=1}^{\infty} \frac{\mu(k)}{n_k}$ is actually the density.

To better illustrates his method, we need to define more notations and make some observations on them.

$N_a(x, y)$ denotes the number of primes $p \leq x$ such that $R(p, q)$ is not true for any $q \leq y$.

$M_a(x, y_1, y_2)$ denote the number of prime $p \leq x$ such that $R(p, q)$ holds for some prime q that $y_1 < q \leq y_2$

Below are some observations:

1. $N_a(x) = N_a(x, x-1)$. Because for any q that satisfies $R(p, q)$ should have $q|p$ so $q \leq p - 1 \leq x - 1$

2. $N_a(x) \leq N_a(x, y)$ for any y. That's because $N_a(x) =$ the number of all primes $\leq x$ - the number of p that satisfies $R(p, q)$ for some q, while $N_a(x, y) =$ the number of all primes $\leq x$ - the number of p that satisfies $R(p, q)$ for $q \leq y$. So the part being subtracted in $N_a(x, y)$ is a subset of the part being subtracted in $N_a(x)$

3. $N_a(x) \geq N_a(x, y) - M_a(x, y, x-1)$. That's because in the right handside of the inequality we subtract for twice the primes p that satisfies $R(p, q)$ for some $q \leq y$ and for some q that $y < q \leq x - 1$

4. $M_a(x, t_1, t_3) \leq M_a(x, t_1, t_2) + M_a(x, t_2, t_3)$ because the right handside of the inequality over counts the primes that satisfies $R(p, q)$ for some $t_1 < q \leq t_2$ and some q that $t_2 < q \leq t_3$. We can think of this as the traingular inequality

Use these observatons we can get that

$$N_a(x) = N_a(x, t_1) + \mathcal{O}(M_a(x, t_1, t_2)) + \mathcal{O}(M_a(x, t_2, t_3)) + \mathcal{O}(M_a(x, t_3, x-1))$$

Where $t_1 = \frac{1}{6}\log x$, $t_2 = \frac{\sqrt{x}}{\log x^2}$, $t_3 = \sqrt{x}\log x$

It turns out that $\mathcal{O}(M_a(x, t_2, t_3))$ and $\mathcal{O}(M_a(x, t_3, x-1))$ can be approximated without assuming Generalized Riemann hypothesis. These two give $\mathcal{O}(\frac{x \log\log x}{\log x^2})$, and the computational details can be found in [7].

The Generalized Riemann Hypothesis is required for the approximation of $N_a(x, t_1)$ and $\mathcal{O}(M_a(x, t_1, t_2))$. The idea of deriving the Prime Ideal Theorem from Generalized Riemann Hypothesis is similar to how we derive the Prime Number Theorem with error bound from Riemann Hypothesis except that it's much more tedious([7]). Let $\pi(x, k)$ denotes the number of prime ideals $\mathcal{P}$ in $\mathbb{Q}(\zeta^k, a^{\frac{1}{k_1}})$ such that $||\mathcal{P}|| \leq x$, then assuming generalized Riemann Hypothesis we have the following error bound for Prime Ideal Theorem:

$$\pi(x, k) = Li(x) + \mathcal{O}(n_k\sqrt{x}\log kx)$$

But if we consider seperately the primes that splits completely, use $\omega(x, k)$ denotes the number of prime ideals $\mathcal{P}$ such that $||\mathcal{P}|| \leq x$ and that the prime $p \in \mathbb{Q}$ below it splits completely in $\mathbb{Q}(\zeta^k, a^{\frac{1}{k_1}})$(and thus $||\mathcal{P}|| = p$). Use $\omega(x, k)'$ to denote the number of $\mathcal{P}$ with norm not exceeding x and p belows it ramifies in $\mathbb{Q}(\zeta^k, a^{\frac{1}{k_1}})$ (This happens iff $p|n_k$). Use $\omega(x, k)''$ to denote the number $\mathcal{P}$ that is unramified but also not splits completely. Then we have

$$\pi(x, k) = \omega(x, k) + \omega(x, k)' + \omega(x, k)''$$

For $\mathcal{P}$ counted by $\omega(x,k)$, there are n_k of $\mathcal{P}$ that is above a p that splits completely, and the number of $p \leq x$ that splits completely is counted by $P_a(x,k)$. So we have

$$\omega(x,k) = n_k\, P_a(x,k)$$

Notice that each $p \in \mathbb{Q}$ can have at most n_k numbers of primes above it in $\mathbb{Q}(\zeta^k, a^{\frac{1}{k_1}})$, and $||\mathcal{P}|| \geq p$ for $p \in \mathbb{Q}$ below $\mathcal{P}$. Also recall that p ramifies iff

p divides the discriminant of $\mathbb{Q}(\zeta^k, a^{\frac{1}{k_1}}) \,/\, \mathbb{Q}$, which is equivalent to $p|ak$ in our case. So

$$\omega(x,k)' \leq n_k(\text{number of prime divisor of } ak) \leq n_k \frac{\log ak}{\log 2}$$

For p unramified but doesn't split completely, $||\mathcal{P}|| \geq p^2$. Thus

$$\omega(x,k)'' \leq n_k \sum_{p \leq \sqrt{x}} \leq n_k \sqrt{x}$$

So now we have

$$\pi(x,k) = n_k\, P_a(x,k) + n_k \mathcal{O}(\sqrt{x})$$

Now express $P_a(x,k)$ in terms of $\pi(x,k)$ and then plug in $\pi(x,k) = Li(x) + \mathcal{O}(n_k\sqrt{x}\log kx)$, we will get

$$P_a(x,k) = \frac{1}{n_k} Li(x) + \mathcal{O}(\sqrt{x}\log kx)$$

This is essentially the effective form of Chebotarev density theorem.

Now back to $N_a(x,t_1)$ and $\mathcal{O}(M_a(x,t_1,t_2))$.

Let $k = \prod_{p \leq t_1}$, k square free. Similar to how we get the formula for $N_a(x)$, we have

$$N_a(x,t_1) = \sum_{d|k} \mu(d)\, P_a(x,d) = \sum_{d|k} \frac{\mu(d)}{n_d} Li(x) + \mathcal{O}(\sum_{d|k} \mu(d)\sqrt{x}\log dx)$$

Now we can see why t_1 is chosen to be $\frac{1}{6}\log x$. $k = \prod_{p \leq t_1} p = e^{\theta(t_i)} \leq e^{2t_1} = x^{\frac{1}{3}}$. So for $d|k$, $d \leq x^{\frac{1}{3}}$, which means the number of divisor of k is also $\leq x^{\frac{1}{3}}$. Then we have

$$\sum_{d|k} \mu(d)\sqrt{x}\log dx \leq \sum_{1}^{x^{\frac{1}{3}}} \sqrt{x}\log x = x^{\frac{5}{6}}\log x$$

Now let S denotes the set of d that is square free and has at least one prime factor$> t_1$. Then we have

$$\sum_{d|k} \frac{\mu(d)}{n} Li(x) = \sum_{n=1}^{\infty} \frac{\mu(d)}{n_d} Li(x) + \mathcal{O}(Li(x) \sum_{d \in S} \frac{\mu(d)}{\varphi(d)})$$

The error can be verified to be bounded by $\mathcal{O}(\frac{x}{\log x^2})$

For $\mathcal{O}(M_a(x,t_1,t_2))$ bound it by $\sum_{t_1<q\le t_2} P_a(x,q)$. Then plug in the formula for $P_a(x,q)$ directly and some approximation shows that it is $\mathcal{O}(\frac{x}{\log x^2})$

Thus we know that $N_a(x) = \sum_{k=1}^{\infty} \frac{\mu(k)}{n_k} \frac{x}{\log x} + \mathcal{O}(\frac{x \log\log x}{\log x^2})$. Now the last task is to evaluation $\sum_{n=1}^{\infty} \frac{\mu(k)}{n_k}$.

6.4 Formula of $A(a)$

Recall that n_k is $[\mathbb{Q}(\zeta^k, a^{\frac{1}{k_1}}) : \mathbb{Q}] = [\mathbb{Q}(\zeta^k, a^{\frac{1}{k_1}}) : \mathbb{Q}(\zeta^k)][\mathbb{Q}(\zeta^k) : \mathbb{Q}]$. We know that $[\mathbb{Q}(\zeta^k) : \mathbb{Q}] = \varphi(k)$ so only need to evaluate $[\mathbb{Q}(\zeta^k, a^{\frac{1}{k_1}}) : \mathbb{Q}(\zeta^k)]$.

Case 1.If k_1 is odd, for $k_1 = 1$ this is trivial. For $k_1 \ge 3$, let $k_1 = \prod_{i=1}^{t} q_i$. Then $\mathbb{Q}(a^{\frac{1}{k_1}})$ is the composite field of $\mathbb{Q}(a^{\frac{1}{q_i}})$. The only subfield of $\mathbb{Q}(a^{\frac{1}{q_i}})$ is $\mathbb{Q}$ or itself since the degree of extension is a prime. So $\mathbb{Q}(\zeta_k) \cap \mathbb{Q}(a^{\frac{1}{q_i}})$ is either $\mathbb{Q}$ or $\mathbb{Q}(a^{\frac{1}{q_i}})$. But for $q_i \ge 3$, $\mathbb{Q}(a^{\frac{1}{q_i}})$ is no longer a normal extension while all the subfield of $\mathbb{Q}(\zeta_k)$ is normal. Thus $\mathbb{Q}(\zeta_k) \cap \mathbb{Q}(a^{\frac{1}{q_i}}) = \mathbb{Q}$, so $\mathbb{Q}(a^{\frac{1}{k_1}}) \cap \mathbb{Q}(\zeta_k) = \mathbb{Q}$. Thus $[\mathbb{Q}(\zeta^k, a^{\frac{1}{k_1}}) : \mathbb{Q}] = k_1\varphi(k)$

Case 2. If k_1, k is even, then say $k_1 = 2m$ so m is odd. Then $[\mathbb{Q}(\zeta_k.a^{\frac{1}{m}})] = \varphi(k)m$. Then $[\mathbb{Q}(\zeta^k, a^{\frac{1}{k_1}}) : \mathbb{Q}]$ can only be $\varphi(k)m$ or $2\varphi(k)m$ and it is $\varphi(k)m$ iff $\sqrt{a} \in \mathbb{Q}(\zeta_k)$.

Now consider $a = b^2c$ where c is square free. so $\sqrt{a} \in \mathbb{Q}(\zeta_k)$ is the same as saying $\sqrt{c} \in \mathbb{Q}(\zeta_k)$. say $k = 2\prod_{i=1}^{m} q_i$. Then the only quadratic subfields of $\mathbb{Q}(\zeta_k)$ are $\mathbb{Q}(\sqrt{q_1^* q_2^* ... q_t^*})$ such that $q* = (-1)^{\frac{q-1}{2}}$. So we need that $c = q_1^* q_2^* ... q_t^*$ so $c|k$. Notice that c can't be $-q_1^* q_2^* ... q_t^*$ because otherwise $\mathbb{Q}(\zeta_k)$ will contains i, which is impossible because $4 \nmid k$. Thus $c \equiv 1 \bmod 4$ since each $q_i^* \equiv 1 \bmod 4$. Thus we have the following:

$$n_k = \begin{cases} \frac{k_1\varphi(k)}{2}, & \text{if c}\equiv 1 \bmod 4, 2c|k \\ k_1\varphi(k) & \text{if otherwise} \end{cases}$$

The last step is to evaluate $\sum_1^{\infty} \frac{\mu(k)}{n_k}$.

Case 1. if $c \not\equiv 1 \bmod 4$ then $\mu(k), n_k$ are both completely multiplicative, so decompose the sum as product of terms involving prime. We eventually have

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{n_k} = \prod_{q|h}(1 - \frac{1}{\varphi(q)}) \prod_{q\nmid h}(1 - \frac{1}{q\varphi(q)})$$

Let's denote this as $C(h)$ [7]

Case 2. if $c \equiv 1 \bmod 4$. Then for $2c|k, n_k = \frac{k_1\varphi(k)}{2}$ and otherwise $n_k = k_1\varphi(k)$. Then we have

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{n_k} = \sum_{k=1}^{\infty} \frac{\mu(k)}{k_1\varphi(k)} + \sum_{2c|k}^{\infty} \frac{(k,h)\mu(k)}{k\varphi(k)}$$

We already know the first sum, and the second sum is $\sum_{k,(k,2c)=1}^{\infty} \frac{\mu(2|c|k)(2|c|k,h)}{2|c|k\varphi(2|c|k)}$. This is similar to the previous sum, except that we have to get rid of the terms corresponds to prime factors of $2|c|k$. Eventually we will get

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{n_k} = C(h)(1-\mu(|c|)) \prod_{q|h,q|c} (\frac{1}{q-2}) \prod_{q\nmid h,q|c} (1-\frac{1}{q^2-q-1})$$

This is the formula for $A(a)$.

Acknowledgement

I would like to thank my friend Sophia for accompanying me during the program. I would like to thank little baby Deepesh Singhal for teaching me most of the materials. I would like to thank professor Andrei Jorza from my home institution who provides references I needed for this paper. I would like to thank my mentor Noah Taylor for guiding me throughout the process of writing the paper. I would also like to thank Peter May for organizing this program and offering the opportunities.

References

[1] Serge Lang, Algebraic Number Theory. 2nd ed., Springer-Verlag, 1994.

[2] Chan Heng Huat, Introduction to Analytic Number Theory.(`http://www.math.nus.edu.sg/~chanhh/notes/MA4263.pdf`)

[3] Bernhard Riemann, On the Number of Prime Numbers less than a Given Quantity. (`https://www.claymath.org/sites/default/files/ezeta.pdf`)

[4] Joseph Bak, Donald J.Newman. Complex Analysis. 3rd ed., Springer Science Business Media, LLC, 2010.

[5] Peter Borwein, Stephen Choi, Brendan Rooney, Andrea WeirathmuellerThe Riemann Hypothesis: A Resource for the Afficionado and Virtuoso Alike. (`https://pdfs.semanticscholar.org/d498/a6c9fda1bef6a3e4feec2034e33fd864826f.pdf`)

[6] Harold M. Edwards, Riemann's Zeta Function. Academic Press, 1974.

[7] Christopher Hooley, On Artin's conjecture. Journal für die reine und angewandte Mathematik 225 (1967): 209-220. (`<http://eudml.org/doc/150785>.`)

[8] M.Ram.Murphy, Artin's Conjecture on Primitive Roots, (`http://web.math.ucsb.edu/~agboola/teaching/2005/winter/old-115A/murty.pdf`)

[9] David Steven Dummit, Richard M. Foote, Abstract Algebra Third edition, 1950- Hoboken, NJ : Wiley, c2004. Section 18.1 and 18.3

[10] Daniel A. Marcus, Number Fields, Springer-Verlag, 1977.

[11] Nicholas George Triantafillou, The Chebotarev Density Theorem, (https://math.mit.edu/~ngtriant/notes/chebotarev.pdf)

[12] S. Martin, Representation Theory, (https://math.uchicago.edu/~margalit/repthy/Martin,Representation_Theory.pdf)

[13] R.Ash, The Prime number theorem, page 10. (https://faculty.math.illinois.edu/~r-ash/CV/CV7.pdf)

[14] Chan Heng Huat, Introduction to Analytic Number Theory. Page 29. (http://www.math.nus.edu.sg/~chanhh/notes/MA4263.pdf)

[15] J.S. Milne, Class Field Theory. (http://www.jmilne.org/math/CourseNotes/CFT.pdf)

[16] J.W.S. Cassels. A Frohlich, Algebraic Number Theory. (https://www.math.arizona.edu/~cais/scans/Cassels-Frohlich-Algebraic_Number_Theory.pdf)

[17] Tom M Apostol, Introduction to Analytic Number Theory. Springer-Verlag, 1976.

[18] Jose Alfredo Ca˜nizo Rincon, The Dedekind Zeta Function and the Class Number Formula, (https://kskedlaya.org/Math254B/zetafunction.pdf)