THE ANALYTIC CLASS NUMBER FORMULA AND SPECIAL VALUES OF L-FUNCTIONS

NISHKARSH SINGH

Abstract. In this paper, we go through a gentle introduction to the analytic class number formula, which is a fundamental result in number theory. We will first be going over the algebraic and complex analytic methods which are important for understanding the class number formula but are not assumed for any reader. Then, we will dive into our actual topic and explore the class number formula and some remarks regarding it. Finally, we will go through some special consequences of the class number formula regarding Dirichlet L-functions, and how it can be used to calculate some L-functions at 1 and 0.

Mathematics is the queen of all sciences, and number theory is the queen of mathematics.

Carl Friedrich Gauss

1. Introduction and History

The analytic class number formula is a remarkable result in number theory which connects the values of the Dedekind zeta function ζ_K to fundamental values about the number field K like the discriminant Δ_K, the class number h_K, etc.

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = 2^{r_1}(2\pi)^{r_2}\frac{h_K \mathrm{reg}_K}{w_k\sqrt{\Delta_K}}$$

A class number formula is rather an ambiguous term in general which can refer to some other formulae in different contexts, but throughout this paper, we will refer to the Dirichlet's analytic class number formula which was formally proven for general number fields by Dedekind. However, the whole story is more complicated. Dedekind first proved that the limit $\lim_{s\to 1^+}(s-1)\zeta_K(s)$ exists and is equal to the given expression, but it was Landau in 1907 who proved that $\zeta_K(s)$ can be analytically continued to $\mathrm{Re}\, s \geq 1 - \frac{1}{[K:\mathbb{Q}]}$, he showed that $\zeta_K(s)$ is meromorphic around 1. By this context, the formula can be seen as a residue calculation as well. However, it is important to acknowledge that before anything, Dirichlet had already proved the class number formula for quadratic number fields. Kummer was also working on a similar formula, but could not generalize it for all number fields because he was missing a precise definition for algebraic integers.

In this article, our goal is going through an introduction to the analytic class number formula. The formula however requires a decent deal of algebraic number theory and some complex analysis, which we will also be going through in the starting sections. From Section 2 to Section 4, we will discuss some algebraic number theory. In Section 5, we will discuss a few complex analytic terms, and then finally in Section 6 and Section 7 we will delve into the real deal.

2. The Discriminant

The class number formula is by nature not entirely analytic or algebraic, but a beautiful intersection of both fields. The formula includes some algebraic number theoretic invariants and functions which we are going to discuss in this paper, the first one being the discriminant of a number field.

Date: June 9, 2024.

Definition 2.1. An *algebraic number field* or *number field* is a subfield of $\mathbb{C}$ with finite degree over $\mathbb{Q}$. Every number field is in the form $\mathbb{Q}[\alpha]$ for some algebraic number $\alpha \in \mathbb{C}$. If the degree of the irreducible polynomial (over $\mathbb{Q}$) which has α as one of it's roots is n, then

$$\mathbb{Q}[\alpha] = \left\{ \sum_{k=0}^{n-1} a_k \alpha^k ;\ a_i \in \mathbb{Q} \text{ for all } 1 \leq i \leq n-1 \right\}$$

Corollary 2.1. Any number field K has exactly $[K : \mathbb{Q}]$ embeddings into $\mathbb{C}$. (Embeddings are injective ring homomorphisms)

In this paper we omit the proof of this, however the idea behind this is very similar to the field automorphisms in Galois groups. Now we will define two of the most important functions of a number field, the trace and the norm.

Definition 2.2. For a number field K and n be $[K : \mathbb{Q}]$, if $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ is the set of embeddings from K into $\mathbb{C}$, then for each $\alpha \in K$ the *norm* $N(\alpha)$ is defined as

$$N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_n(\alpha)$$

Definition 2.3. For a number field K and n be $[K : \mathbb{Q}]$, if $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ is the set of embeddings from K into $\mathbb{C}$, then for each $\alpha \in K$ the *trace* $T(\alpha)$ is defined as

$$N(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha)$$

Note that as every embedding is a ring homomorphism, $T(\alpha) + T(\beta) = T(\alpha + \beta)$ and $N(\alpha)N(\beta) = N(\alpha\beta)$. Also, since all n embeddings fix $\mathbb{Q}$ pointwise, if $a \in \mathbb{Q}$ then $N(a) = ra$ and $T(a) = a^r$. Now we will define the discriminant of a $n-$tuple in a number field.

Definition 2.4. For a number field K with degree n and a $n-$tuple $(a_1, a_2, \ldots, a_n)$ where each $a_i \in K$, if $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ is the set of embeddings from K to $\mathbb{C}$, then the discriminant of the tuple is defined as,

$$\operatorname{disc}(a_1, a_2, \ldots, a_n) = |\sigma_i(a_j)|^2 = \begin{vmatrix} \sigma_1(a_1) & \sigma_1(a_2) & \cdots & \sigma_1(a_n) \\ \sigma_2(a_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(a_1) & \cdots & \cdots & \sigma_n(a_n) \end{vmatrix}^2$$

Lemma 2.1. $\operatorname{disc}(a_1, a_2, \ldots, a_n) = |T(a_i a_j)|$

Proof. We know that $|AB| = |A||B|$ for matrices A and B. The proof is completed by the equation,

$$[\sigma_i(a_j)][\sigma_j(a_i)] = \left[\sum_{k=1}^{n} \sigma_k(a_i a_j) \right] = [T(a_i a_j)]$$

□

Lemma 2.2. $\operatorname{disc}(a_1, a_2, \ldots, a_n) = 0$ if $a_1, a_2, \ldots, a_n$ are linearly dependent.

We skip over the proof.

Corollary 2.2. Every basis of $K/\mathbb{Q}$ gives a nonzero discriminant.

Definition 2.5. A *free abelian group G of rank n* is a group such that it is a direct sum of n subgroups, all of which were isomorphic to $\mathbb{Z}$. Note that this also means that G is isomorphic to the n-dimensional lattice $\mathbb{Z}^n$ (i.e. - $G \cong \mathbb{Z}^n$).

Theorem 2.1. Let $\mathbb{Z}_K = \mathbb{A} \cap K$ be the ring of integers of K. $\mathbb{Z}_K$ is a free abelian group of rank $n = [K : \mathbb{Q}]$. ($\mathbb{A}$ is the ring of algebraic integers)

For the proof of this theorem, we would need some background.

Corollary 2.3. If G is an abelian group of a finite rank n, then every subgroup $H \subseteq G$ is also an abelian group of rank $\leq n$

The proof is this corollary is trivial by induction, hence skipped. It follows from this corollary that, if there are 3 groups A, B, C such that $A \subsetneq B \subsetneq C$ where A and C are both abelian groups of rank n, this would imply that B is also an abelian group of rank n. This is essentially the idea we are going to use in our proof. We just need to find two groups to sandwich $\mathbb{Z}_K$, which are abelian groups of rank n.
Firstly, we can observe that there always exists bases of K over $\mathbb{Q}$ which contain entirely of algebraic integers. In fact, they can be created by multiplying any basis by a certain integer because for every $\alpha \in K$ there always exists an $m \in \mathbb{Z}$ such that $m\alpha \in \mathbb{A}$. This means that if we take a basis $\{a_1, a_2, \dots, a_n\}$ such that every a_i is an algebraic integer, then we can create a group

$$A = \{m_1 a_1 + m_2 a_2 + \ldots + m_n a_n;\ m_i \in \mathbb{Z}\}$$

Now this is clearly an abelian group of rank n, which is a subgroup of $\mathbb{Z}_K$. So we have $A \subsetneq \mathbb{Z}_K$, now we want the other half of the sandwich.

Theorem 2.2. If $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is a basis for K over $\mathbb{Q}$ consisting of only algebraic integers. Then every $\alpha \in \mathbb{Z}_K$ can be written as,

$$\frac{m_1\alpha_1 + m_2\alpha_2 + \ldots + m_n\alpha_n}{\operatorname{disc}(\alpha_1, \alpha_2, \dots, \alpha_n)}$$

where $m_i \in \mathbb{Z}$ for all i,

Proof. Write $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$ with the $x_j \in \mathbb{Q}$. Letting $\sigma_1, \dots, \sigma_n$ denote the embeddings of K in $\mathbb{C}$ and applying each σ_i to the above equation, we obtain the system

$$\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n), \quad i = 1, \dots, n.$$

Solving for the x_j via Cramer's rule, we find that $x_j = \frac{y_j}{\delta}$ where δ is the determinant $|\sigma_i(\alpha_j)|$ and y_j is obtained from δ by replacing the j-th column by $\sigma_i(\alpha)$. It is clear that y_j and δ are algebraic integers, and in fact $\delta^2 = d$. Thus $dx_j = \delta y_j$, which shows that the rational number dx_j is an algebraic integer. As we have seen, that implies $dx_j \in \mathbb{Z}$. Call it m_j. □

From this theorem, we know that $\mathbb{Z}_K$ is contained in the abelian group of rank n

$$\frac{1}{d}A = \mathbb{Z}\frac{\alpha_1}{d} \oplus \mathbb{Z}\frac{\alpha_2}{d} \oplus \ldots \oplus \mathbb{Z}\frac{\alpha_n}{d}$$

where $d = \operatorname{disc}(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Corollary 2.4. $\mathbb{Z}_K$ is an abelian group of rank n.

This means that $\mathbb{Z}_K$ has a basis over $\mathbb{Z}$, we call this basis the integral basis of $\mathbb{Z}_K$. The discriminant of any integral basis is an invariant of a number field, so we can define the discriminant of a number field.

Definition 2.6. If K is a number field, and $\mathbb{Z}_K$ is its ring of integers, then the *discriminant of the ring of integers*, $\operatorname{disc}(K)$ or $\operatorname{disc}(\mathbb{Z}_K) = \operatorname{disc}(\beta_1, \beta_2, \dots \beta_n)$. Where $\{\beta_1, \beta_2, \dots \beta_n\}$ is the integral basis of $\mathbb{Z}_K$.

Example 1. Let $K = \mathbb{Q}[\sqrt{m}]$ where m is square-free,

$$\operatorname{disc}(K) = \begin{cases} m;\ m \equiv 1 \mod 4 \\ 4m;\ m \equiv 2, 3 \mod 4 \end{cases}$$

We omit the proof as it is is mostly just casing.

Definition 2.7. Let K be a number field, and let $p \in K$ be a prime element, if (p) factors into ${\mathfrak{p}_1}^{e_1}{\mathfrak{p}_2}^{e_2} \ldots {\mathfrak{p}_n}^{e_n}$ where $\mathfrak{p}_i$ are prime ideals, then

- p is said to be **ramified** if there exists atleast one $e_i \geq 2$.
- p is said to be **split** if all $e_i = 1$.
- p is said to be **inert** if it doesn't split.

Proposition 2.1. If $K = \mathbb{Q}(\sqrt{d})$

- p is ramified if $p|\text{disc}(K)$.
- p is split if $p \nmid \text{disc}(K)$ and d is a quadratic residue modulo p.
- p is inert if $p \nmid \text{disc}(K)$ and d is a quadratic non-residue modulo p.

3. The Class Number and some other terms

We will first start by defining some terms regarding the ring theoretic part of algebraic number theory, which is important to analyze the further prerequisites.

Definition 3.1. A Dedekind domain D is an integral domain such that it satisfies the following,

- Every ideal is finitely generated;
- Every nonzero prime ideal is maximal;
- D is integrally closed in it's field of fractions, this means that if $\alpha/\beta \in K$ is a root of some monic polynomial over D, then $\alpha/\beta \in D$.

One need not think too much about this definition as we aren't going to directly use any propositionerties of this in our paper, however the next proposition is the reason we are including this.

Proposition 3.1. For a number field K, its ring of integers $\mathbb{Z}_K$ is a Dedekind domain

Now we are going to introduce some terms regarding the class group.

Definition 3.2. Let R be an integral domain, a fractional ideal F of R is a finitely generated R-submodule such that there exists a $r \in R \setminus \{0\}$ so that $rF \subseteq R$, i.e.- is an ideal of R.

Lemma 3.1. Every fractional ideal in a Dedekind domain is invertible.

Remark 1. Lemma 3.2 is also something that characterizes Dedekind domains, it is often used as an alternate definition in some books!

Corollary 3.1. All fractional ideals in $\mathbb{Z}_K$ form a group $\mathcal{F}_K$. (More generally, for any Dedekind domain)

Proof. The identity and closure properties are trivial, and we gaurantee the existence of an inverse by Lemma 3.2, which completes the proof. □

Definition 3.3. A fractional ideal P is called a principal fractional ideal if there exists some $x \in K$ (more generally, the quotient field of R) such that $P = \mathbb{Z}_K x$.

Definition 3.4. The Ideal Class Group Cl_K is defined as the quotient group $\mathcal{F}_K \setminus \mathcal{P}_K$

Definition 3.5. The class number h_K is defined as the order of the ideal class group $|Cl_K|$. This in a way is a measure of how far $\mathbb{Z}_K$ is from being a UFD (unique factorization domain) as $h_K = 1$ when $\mathbb{Z}_K$ is a UFD.

Corollary 3.2. The number of roots of unity in K is denoted by w_K, therefore it is

$$w_K = \begin{cases} 3 \ K = \mathbb{Q}(\iota) \\ 6 \ K = \mathbb{Q}(\sqrt{-3}) \\ 2 \text{ otherwise} \end{cases}$$

4. The Regulator

The regulator is the last, and perhaps the most challenging invariant we are going to deal with in this paper. We have till now included the nature of the structure of the field, the structure of the ring of integers, now we are going to see the structure of the units in the field.

Definition 4.1. All the units in a number field form a group, called the Unit Group $\mathbb{Z}_K^*$.

Definition 4.2. The fundamental unit of a number field K is the generator for all units in the unit group when the group has rank 1, i.e. - it is a real quadratic field, imaginary cubic field, or a totally imaginary quartic field.

We will unfortunately not be able to go through the formal definition of a regulator as that would require a heavy background on the geometric methods in algebraic number theory and would take a lot of time so we will rather do an intuitive definition and go through it's values for different cases.

Dirichlet's unit theorem says the unit group is actually isomorphic to $\mathbb{Z}^{r_1+r_2-1} \times \mu_K$ where μ_K is the group of the roots of unity in K and r_1 and r_2 are the number of real and complex embeddings of K into $\mathbb{C}$. Using this, we can map every unit to $\mathbb{R}^{r_1+r_2}$, this gives us some vectors, which in turn form a parallelepiped (a complicated multidimensional shape). When we calculate the volume of this, we are essentially calculating the size of $\mathbb{Z}_K^*$, this is the regulator Reg_K.

Proposition 4.1. Reg_K is 1 when K is an imaginary quadratic field, and it is the logarithm of its fundamental unit $\log \epsilon$ when it's real quadratic, imaginary cubic, or totally imaginary quartic.

5. A pinch of complex analysis

In this section, we are going to talk about complex analysis which is an important part of the class number formula. We are going to be relatively non-rigorous here as it would not make sense to punch down a semester worth of complex analysis into 2 or 3 pages, rather we are only going to discuss the terms which will be useful to us so that we can understand what's going on in our main theorem.

Definition 5.1. Let U be an open set and let $f : U \to \mathbb{C}$ be a function. We say that f is *differentiable (or complex differentiable)* at some $z \in U$ if the limit

$$\lim_{z' \to z} \frac{f(z) - f(z')}{z - z'}$$

exists.

Definition 5.2. Let U be an open set and let $f ; U \to \mathbb{C}$ be a function. We say that f is *holomorphic* if f is complex differentiable at all points in U.

Definition 5.3. A complex function f is said to have a *singularity* at z_0 if f fails to be analytic at some point in every neighbourhood of z_0.

There are two types of singularities, isolated and non isolated, and there are further divisions as well. But we are going to only look at one type of isolated singularity, known as a simple pole.

Definition 5.4. Let $f : U \to \mathbb{C}$ be a complex function, f is said to have a *simple pole* at z_0 if $\frac{1}{f}$ is holomorphic in some neighbourhood of z_0 and has a zero at z_0.

Definition 5.5. Let U be an open set, a complex function $f : U \to \mathbb{C}$ is said to be *meromorphic* if f is holomorphic for every point in U except a set of isolated points which are poles.

In complex analysis, we have something like an extension to the general Taylor expansion, it's called a Laurent expansion.

Corollary 5.1. Every holomorphic function f can be written as *Laurent expansion centered at* z_0, which means it can be written as,

$$f(z) = \sum_{i=0}^{\infty} a_i(z - z_0)^i + \sum_{j=1}^{\infty} \frac{b_j}{(z - z_0)^j}$$

It would be out of our scope to prove this. a_i and b_j are determined by a complex integral, b_j becomes 0 for every $j \geq 2$ in the case of a simple pole at z_0.

We, moreover, did all these definitions for understanding one important concept in complex analysis which occurs in the class number formula, the residue. However, obviously residues, in general, are not so simple. Luckily, we have to only deal with residues at a simple pole in our formula, and that is what we will be defining in this paper. Residue by essence is a complex number which describes the *intensity* of a singularity. It is propositionortional to a line integral which goes *around* the singularity. We will not be going through the formal definition of a residue as it would require a lot of theory, but we will be going through a glimpse of what is the expression for the residue at a simple pole and why it is so. If f is a meromorphic function with a simple pole at z_0 then we know that,

$$\begin{aligned} f(z) &= \sum_{i=0}^{\infty} a_i(z - z_0)^i + \sum_{j=1}^{\infty} \frac{b_j}{(z - z_0)^j} \\ &= \sum_{i=0}^{\infty} a_i(z - z_0)^i + \frac{b_1}{(z - z_0)} \end{aligned}$$

Here b_1 is the residue (by the definition of the coefficients),

$$(z - z_0)f(z) = (z - z_0)\sum_{i=0}^{\infty} a_i(z - z_0)^i + b_1$$

If we take limit $z \to z_0$ then,

$$\text{Res}_{z_0}(f) = \lim_{z \to z_0} (z - z_0)f(z)$$

6. The Class Number Formula

We are finally now arriving at the main result of this paper, the class number formula. We will define a few terms and then move on to our formula.

Definition 6.1. Let K be a number field and let $\mathbb{Z}_K$ be its ring of integers. If $\mathfrak{a}$ is a non-zero integral ideal from $\mathbb{Z}_K$, then the *absolute norm* of $\mathfrak{a}$ is defined as

$$\mathcal{N}(\mathfrak{a}) = [\mathbb{Z}_K : \mathfrak{a}]$$

or the number of elements in the quotient $\mathbb{Z}_K/\mathfrak{a}$.

Corollary 6.1. The absolute norm is completely multiplicative, which means

$$\mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}) = \mathcal{N}(\mathfrak{ab})$$

We skip over the proof.

Definition 6.2. For a number field K and its ring of integers $\mathbb{Z}_K$, the *Dedekind zeta function* ζ_K is defined as,

$$\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathbb{Z}_K} \frac{1}{(\mathcal{N}(\mathfrak{a}))^s}$$

where $\mathfrak{a}$ runs through all the nonzero integral ideals of $\mathbb{Z}_K$.

This is an extension of the Riemann zeta function, its easy to observe that $\zeta_{\mathbb{Q}}(s) = \zeta(s)$. There is also something analogous to the euler product for this zeta function,

Corollary 6.2.

$$\zeta_K(s) = \prod_{\mathfrak{p} \subseteq \mathbb{Z}_K} \left(1 - \frac{1}{(\mathcal{N}(\mathfrak{p}))^s}\right)^{-1}$$

where $\mathfrak{p}$ runs through all the prime nonzero ideals of $\mathbb{Z}_K$.

Now we can state the analytic class number formula,

Theorem 6.1. Let K be a number field and $\mathbb{Z}_K$ its ring of integers, $\zeta_K(s)$ has an analytic continuation in $\Re s > 1 - \frac{1}{n}$, which is meromorphic with a simple pole at 1 with residue,

$$\lim_{s \to 1} (s-1)\zeta_K(s) = 2^{r_1}(2\pi)^{r_2} \frac{h_K \mathrm{Reg}_K}{\sqrt{\mathrm{disc}(K)} w_K}$$

where r_1 and r_2 are the number of real and complex places in K respectively, h_K is the class number, Reg_K is the regulator, $\mathrm{disc}(K)$ is the discriminant and w_K is the number of roots of unity in the number field K.

The proof of the theorem is out of the scope of this paper as it is very lengthy. However, we will discuss some analytic applications of this.

Remark 2. In the class number formula, the left hand side can be calculated to any accuracy by expanding the zeta function numerically. The right hand side is also easy to calculate mostly, except the class number itself which is usually the hardest to calculate. This is the reason why the formula is named the 'class number' formula.

7. Applications to the theory of L-functions

One of the most special propositionerties of the Dedekind zeta function is that it can be factored into L-functions. This is a fact linked to one of the most important conjectures in number theory, Artin's conjecture on L-functions. We will first start proving this for quadratic fields.

Lemma 7.1. Let $K = \mathbb{Q}(\sqrt{m})$ where m is square-free, we have

$$\zeta_K(s) = L(s, \chi)\zeta(s)$$

where χ is the Legendre symbol modulo $\mathrm{disc}(K)$.

Proof. We compare compare Euler products, for $L(s,\chi)\zeta(s)$ we know the Euler factor at some p is $(1 - 1/p^s)^{-1}(1 - \chi(p)/p^s)^{-1}$. We know that,

$$\chi(p) = \begin{cases} 1;\ p \text{ is a quadratic residue} \\ 0;\ p | \mathrm{disc}(K) \\ -1;\ p \text{ is not a quadratic residue} \end{cases} = \begin{cases} 1;\ p \text{ splits} \\ 0;\ p \text{ ramifies} \\ -1;\ p \text{ is inert} \end{cases}$$

which means that the Euler factor is going to be $(1 - 1/p^s)^{-2}$ when p splits, $(1 - 1/p^s)^{-1}$ when p ramifies, and $(1 - 1/p^{2s})^{-1}$ if p is inert. Now for $\zeta_K(s)$,

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})^s}\right)^{-1} = \prod_p \prod_{\mathfrak{p} | p\mathbb{Z}_K} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})^s}\right)^{-1}$$

So the Euler factor at p is $\prod_{\mathfrak{p}|p\mathbb{Z}_K} (1 - \mathcal{N}(\mathfrak{p})^{-s})^{-1}$, which is also $(1 - 1/p^s)^{-2}$ when p splits, $(1 - 1/p^s)^{-1}$ when p ramifies, and $(1 - 1/p^{2s})^{-1}$ if p is inert. As the Euler factors are same and ranging through the same primes, our lemma is true. □

Example 2. Now it is possible to calculate class numbers of specific quadratic fields like, say $\mathbb{Q}(-3)$,

$$L(1,\chi)\frac{3\sqrt{3}}{\pi} = h_K$$

Note that $L(1,\chi)$ is numerically computable easily, we can calculate it and it is ≈ 0.596. As $3\sqrt{3}/\pi \approx 1.65$, we know that $h_K = 1$. Note that this also tells us that $\mathbb{Q}(-3)$ is a unique factorization domain!

References

[1] The analytic class number formula lecture 19 notes. `https://math.mit.edu/classes/18.785/2017fa/LectureNotes19.pdf`. Accessed: 2024-06-09.

[2] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53. American Mathematical Soc., 2021.

[3] Daniel A Marcus and Emanuele Sacco. *Number fields*, volume 1995. Springer, 1977.

[4] Ian Stewart and David Orme Tall. *Algebraic number theory*, volume 1987. Chapman and Hall London, 1979.