The Analytic Class Number Formula

Gary Sivek
gsivek@mit.edu

May 19, 2005

1 Introduction

In this paper we will use tools from analysis to provide an explicit formula for the class number of a number field. We will then examine an approach to evaluating the formula in the case of a quadratic field.

This paper assumes basic knowledge of number theory and only minimal complex analysis (what it means for a function to be analytic, how to find residues, and what an L-series is, including the zeta function). For an introduction to complex analysis, see for example [Ahl79], and for an introduction to algebraic number theory, read [Ste05]. In particular, we assume an understanding of the finiteness of the class group of a number field and concepts related to its proof.

2 The Formula

Here we prove the class number formula, which puts the class number of a number field in terms of its zeta function. The formula was originally proven in terms of the number of binary quadratic forms with a given determinant by Dirichlet, and was later proven for general number fields by Dedekind [Hil97].

2.1 Definitions

From this point on, K will be a number field of degree $n = [K : \mathbb{Q}]$ with ring of integers $\mathcal{O}_K$. The class group of K will be denoted $\mathcal{C}_K$. The units contained in $\mathcal{O}_K$ will form a group of size ω_K, and K will have discriminant D_K. An ideal $\mathfrak{i} \subseteq \mathcal{O}_K$ will have norm $N(\mathfrak{i})$, which will be understood to be the $K/\mathbb{Q}$ norm.

Pick any number field K with S real embeddings $\sigma_1, \ldots, \sigma_S$ and $T = \frac{1}{2}(n - S)$ pairs of complex embeddings $\tau_1, \overline{\tau_1}, \ldots, \tau_T, \overline{\tau_T}$. Let $\mathcal{O}_K^*$ be the group of units of the ring of integers. By Dirichlet's Theorem, $\mathcal{O}_K \cong \mathbb{Z}^{S+T-1} \times U_{tor}$, where U_{tor} is a finite torsion group of even order, specifically the cyclic group of order ω_K; let $\epsilon_1, \epsilon_2, \ldots, \epsilon_{S+T-1}$ be generators of the free abelian subgroup. We define the norm of an embedding to be $\|\alpha\|_i = |\sigma_i(\alpha)|$ for $1 \leq i \leq S$

and $\|\alpha\|_{S+j} = |\tau_j(\alpha)|^2$ for $1 \le j \le T$. We now construct the following $(S+T) \times (S+T-1)$ matrix:

$$A = \begin{pmatrix} \log \|\epsilon_1\|_1 & \log \|\epsilon_2\|_1 & \cdots & \log \|\epsilon_{S+T-1}\|_1 \\ \log \|\epsilon_1\|_2 & \log \|\epsilon_2\|_2 & \cdots & \log \|\epsilon_{S+T-1}\|_2 \\ \vdots & \vdots & \ddots & \vdots \\ \log \|\epsilon_1\|_{S+T} & \log \|\epsilon_1\|_{S+T} & \cdots & \log \|\epsilon_{S+T-1}\|_{S+T} \end{pmatrix}$$

Define A_i to be the $(S+T-1) \times (S+T-1)$ submatrix obtained by deleting the ith row of A. Then the *regulator* of K, denoted R_K, is given by $|\det A_i|$, which is independent of i.

We shall also define the space $\mathcal{L}^{S,T}$ to be the set of points $(x_1, \ldots, x_S; x_{S+1}, \ldots, x_{S+T})$, where the first S coordinates are real and the remaining T are complex. This space has dimension $S + 2T = n$ over $\mathbb{R}$, since we have the basis vectors e_j for $1 \le j \le S$ and the basis vectors e_j and ie_j for $S+1 \le j \le S+T$; as such, we shall at times treat it as a subspace of $\mathbb{R}^n$. With scalar multiplication as well as componentwise addition and multiplication of points, this forms a commutative ring and a linear space. Last, we define a norm on $\mathcal{L}^{S,T}$ as $\mathcal{N}(x) = |x_1 \cdots x_S||x_{S+1}|^2 \cdots |x_{S+T}|^2$. This now gives us an injection $\phi : K \to \mathcal{L}^{S,T}$ defined by $\phi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_S(\alpha); \tau_1(\alpha), \ldots, \tau_T(\alpha))$; it is easy to show that ϕ is a homomorphism, and that $\mathcal{N}(\phi(\alpha)) = N(\alpha)$.

For convenience, denote in general $l_k(x) = \log |x_k|$ for $1 \le k \le S$ and $l_{S+k} = \log |x_{S+k}|^2$ for $1 \le k \le T$; we may then define for $x \in \mathcal{L}^{S,T}$ the vector $l(x) = (l_1(x), \ldots, l_{S+T}(x))$. The set of all points of $\mathcal{L}^{S,T}$ with nonzero components form a group under componentwise multiplication, and this mapping is a homomorphism onto the additive group of $\mathcal{L}^{S,T}$. If $\alpha \in K$ then write $l(\alpha) = l(\phi(\alpha))$; we note that the vectors $l(\epsilon_i)$ form the columns of A above. This geometric representation $l(\alpha)$ is called the *logarithmic representation* of α, and the sum of its components is equal to $\log |N(\alpha)|$.

2.2 The Zeta Function

Analytic number theory places heavy emphasis on the celebrated Riemann Zeta Function, which is the analytic continuation of the power series $\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}$ to the entire complex plane except for the pole at $s = 1$. We define an analogue for number fields as:

$$\zeta_K(s) = \sum_{\mathfrak{i}} \frac{1}{N(\mathfrak{i})^s} \tag{1}$$

where $\mathfrak{i}$ ranges over all distinct integral ideals in $\mathcal{O}_K$. Note that in the trivial case $K = \mathbb{Q}$ each ideal is generated by a distinct positive integer, so $\zeta_{\mathbb{Q}}(s) = \zeta(s)$. Euler also factored ζ into a product over all primes $p \in \mathbb{Z}$; here we have the analogous Euler product:

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}} \tag{2}$$

where now $\mathfrak{p}$ ranges over all prime ideals of $\mathcal{O}_K$. The proof of this equation is exactly the same as the standard proof for $\zeta_{\mathbb{Q}}$ because of the unique factorization of ideals in $\mathcal{O}_K$.

Yet another analogy with $\zeta_{\mathbb{Q}}$ is the convergence of the series. For $\zeta_{\mathbb{Q}}$ we have the following.

Theorem 1. *$\zeta(s)$ converges on $\{s \in \mathbb{C} : Re(s) > 1\}$, and $Res_{s=1}\zeta(s) = \lim_{s\to 1}(s-1)\zeta(s) = 1$.*

Proof. Let $s = a + ib$, with $a, b \in \mathbb{R}$ and $a > 1$. Then $\left|\frac{1}{k^s}\right| = \left|\frac{1}{k^a k^{ib}}\right| = \frac{1}{k^a}\left|e^{-ib\log k}\right| = \frac{1}{k^a}$. So

$$|\zeta(s)| = \left|\sum_{k=1}^{\infty}\frac{1}{k^s}\right| \leq \sum_{k=1}^{\infty}\left|\frac{1}{k^s}\right| = \sum_{k=1}^{\infty}\frac{1}{k^a} = \zeta(a).$$

It therefore suffices to consider only real $s > 1$. Since $\frac{1}{k^s}$ monotonically decreases as a function of k when k is positive, we have

$$\frac{1}{(k+1)^s} < \int_k^{k+1}\frac{1}{x^s}dx < \frac{1}{k^s};$$

summing over all k gives $\zeta(s) - 1 < \int_1^{\infty}\frac{dx}{x^s} < \zeta(s)$, or $\zeta(s) - 1 < \frac{1}{s-1} < \zeta(s)$. Reducing this gives $\frac{1}{s-1} < \zeta(s) < \frac{1}{s-1} + 1$, from which the theorem follows. □

Further details about $\zeta(s)$, such as its analytic continuation, are left to any standard text on analytic number theory.

The main focus of this paper is on the analogous result for an arbitrary ζ_K. This key theorem followed from the work of Dirichlet and Dedekind.

Theorem 2. *$\zeta_K(s)$ converges for all $s \in \mathbb{C}$ satisfying $Re(s) > 1$, and at $s = 1$ it has residue given by*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^S(2\pi)^T R_K}{\omega_K|D_K|^{1/2}}h,$$

where $h = |\mathcal{C}_K|$ is the class number of K.

We will prove this following [BS66] and [Jar03], by splitting the sum as

$$\zeta_K(s) = \sum_{A\in\mathcal{C}_K}\left(\sum_{\mathfrak{i}\in A}\frac{1}{N(\mathfrak{i})^s}\right);$$

call the parenthesized sum $f_A(s)$. We will evaluate each $\lim_{s\to 1}(s-1)f_A(s)$ separately.

Choose $\mathfrak{a} \in A^{-1}$, so that for all $\mathfrak{i} \in A$, $\mathfrak{a}\mathfrak{i}$ is principal. Then multiplication by $\mathfrak{a}$ gives a bijection between integral ideals in A and principal ideals divisible by $\mathfrak{a}$. Thus

$$f_A(s) = N(\mathfrak{a})^s\sum_{(\alpha):\mathfrak{a}|(\alpha)}\frac{1}{|N(\alpha)|^s}. \quad (3)$$

Let $\mathcal{A}$ be a set of such α, where from each possible set of associate values we pick exactly one. Define $\Gamma = \phi(\mathfrak{a}) = \{x \in \mathcal{L}^{S,T} : x = \phi(b) \text{ for some } b \in \mathfrak{a}\}$, and similarly define $\Theta = \{x \in \mathcal{L}^{S,T} : x = \phi(b) \text{ for some } b \in \mathcal{A}\}$. Then

$$f_A(s) = N(\mathfrak{a})^s\sum_{\alpha\in\Theta}\frac{1}{|N(\alpha)|^s}. \quad (4)$$

We now must evaluate this sum, and we will do so geometrically.

2.3 Geometry of Number Fields

Lemma 3. *Let X be a cone in $\mathbb{R}^n$ and define a function $F : X \to \mathbb{R}_{>0}$ such that $x \in X$ and $\xi \in \mathbb{R}_{>0}$ implies $F(\xi x) = \xi^n F(x)$, and $\mathcal{F} = \{x \in X : F(x) \leq 1\}$ is bounded with $v = vol(\mathcal{F}) > 0$. Also, let $\Gamma \subseteq \mathbb{R}^n$ be a lattice with volume $\Delta = vol(\Gamma)$, which we take to mean the volume of the parallelepiped formed by basis vectors of Γ. Then*

$$\zeta_{F,\Gamma}(s) = \sum_{x \in \Gamma \cap X} \frac{1}{F(x)^s}$$

converges on $Re(s) > 1$ and has $\lim_{s\to 1}(s-1)\zeta_{F,\Gamma}(s) = \frac{v}{\Delta}$.

Proof. For any positive real number r, we know $\mathrm{vol}(\frac{1}{r}\Gamma) = \frac{\Delta}{r^n}$. Thus $v = \mathrm{vol}(\mathcal{F}) = \lim_{r\to\infty}\left(\frac{\Delta}{r^n} \cdot \#\{\frac{1}{r}\Gamma \cap \mathcal{F}\}\right) = \Delta \lim_{r\to\infty} \frac{\#\{\frac{1}{r}\Gamma\cap\mathcal{F}\}}{r^n}$. But by the requirements on F, this numerator is also the number of points in $\{x \in \Gamma \cap X : F(x) \leq r^n\}$. Label the points of $\Gamma \cup X$ so that $0 \leq F(x_1) \leq F(x_2) \leq \ldots$ and define $r_k = F(x_k)^{1/n}$. If we define $\gamma(r) = \#\{\frac{1}{r}\Gamma \cap \mathcal{F}\}$, then by this choice of label we have that for $\varepsilon > 0$, $\gamma(r_k - \varepsilon) < k \leq \gamma(r_k)$. Dividing by r_k^n gives $\frac{\gamma(r_k-\varepsilon)}{(r_k-\varepsilon)^n}\left(\frac{r_k-\varepsilon}{r_k}\right)^n < \frac{k}{r_k^n} \leq \frac{\gamma(r_k)}{r_k^n}$. Since $r_k^n = F(x_k)$, taking the limit yields $\lim_{k\to\infty}\frac{k}{r_k^n} = \frac{v}{\Delta}$.

Convergence of $\zeta_{F,\Gamma}$ is a simple exercise akin to the proof of Theorem 1. We may rewrite the function, though, as

$$\zeta_{F,\Gamma}(s) = \sum_{k=1}^{\infty} \frac{1}{F(x_k)^s}. \tag{5}$$

Now given $\varepsilon > 0$, by the above inequality there exists k_0 such that $k \geq k_0$ implies

$$\left(\frac{v}{\Delta} - \varepsilon\right)^s \frac{1}{k^s} < \frac{1}{F(x_k)^s} < \left(\frac{v}{\Delta} + \varepsilon\right)^s \frac{1}{k^s}.$$

Summing over all $k \geq k_0$, we multiply by $(s-1)$ and let s approach 1 on the right to get

$$\left(\frac{v}{\Delta} - \varepsilon\right) \mathrm{Res}_{s=1}\zeta(s) \leq \lim_{s\to 1}(s-1)\zeta_{F,\Gamma}(s) \leq \left(\frac{v}{\Delta} + \varepsilon\right) \mathrm{Res}_{s=1}\zeta(s)$$

and the desired result follows. □

We may now pick a suitable choice of F and X. Pick $\epsilon_1, \ldots, \epsilon_{S+T-1}$ to be fundamental units; i.e., as in the definition of the regulator of K. Define $\lambda = (1, \ldots, 1; 2, \ldots, 2)$. Then $\{\lambda, \phi(\varepsilon_1), \ldots, \phi(\varepsilon_{S+T-1})\}$ is a basis for $\mathbb{R}^{S+T}$ (see [Ste05], §9), and we may write for $x \in \mathcal{L}^{S,T}$:

$$l(x) = c\lambda + c_1\phi(\varepsilon_1) + \ldots + c_{S+T-1}\phi(\varepsilon_{S+T-1})$$

where $c = \frac{1}{n}\log|N(x)|$. Define X to be the cone consisting of all x such that:

1. $N(x) \neq 0$.

2. The coefficients c_i satisfy $0 \leq c_i < 1$ for all i.

3. $0 \leq \arg(x_1) < \frac{2\pi}{\omega_K}$, where x_1 is the first component of x.

This is a cone because $l(cx) = (\log c)\lambda + l(x)$, preserving the coefficients of the $\phi(\varepsilon_i)$ terms, and $\arg(cx_1) = \arg(x_1)$.

Lemma 4. *Let $\eta(\alpha) \subseteq \mathcal{O}_K$ be the set of all elements in $\mathcal{O}_K$ which are associates of α (including α itself). Then exactly one member of $\eta(\alpha)$ has image in X.*

Proof. To show this, we will show that given $y \in \mathbb{R}^n$ with nonzero norm, y can be written uniquely as $x \cdot \phi(\varepsilon)$, where $x \in X$ (multiplication is componentwise) and ε is a unit. Write $l(y) = c\lambda + c_1\phi(\varepsilon_1) + \ldots + c_{S+T-1}\phi(\varepsilon_{S+T-1})$. Split each c_i as $c_i = m_i + \mu_i$, where $m_i \in \mathbb{Z}$ and $0 \leq \mu_i < 1$, and write $u = \varepsilon_1^{m_1} \cdots \varepsilon_{S+T-1}^{m_{S+T-1}}$. Then define $z = y \cdot \phi(u^{-1})$, which has coefficients of each $\phi(\varepsilon_i)$ in the correct range. Now we can correct $\arg(z_1)$; let r be the unique integer such that $0 \leq \arg(z_1) - \frac{2\pi r}{\omega_k} < \frac{2\pi}{\omega_k}$, and choose a root of unity w such that $\sigma_1(w) = e^{\frac{2\pi i}{\omega_K}}$. Then $z \cdot \phi(w^{-r}) = y \cdot \phi(u^{-1})\phi(w^{-r}) \in X$, so we conclude that if this value is called x, then $y = x \cdot \phi(uw^r)$ as desired, and clearly this construction must be unique. $\square$

We now use the result of Lemma 4 to rewrite (4) as:

$$f_A(s) = N(\mathfrak{a})^s \sum_{x \in \Gamma \cap X} \frac{1}{N(x)^s} \tag{6}$$

which we may evaluate as in Lemma 3. We thus need $v = \mathrm{vol}(\{x \in X : N(x) \leq 1\})$ and $\Delta = \mathrm{vol}(\Gamma)$. Recall that here $\Gamma = \phi(\mathfrak{a}) = \{x \in \mathcal{L}^{S,T} : x = \phi(b) \text{ for some } b \in \mathfrak{a}\}$.

Lemma 5. *$\Delta = N(\mathfrak{a})|D_K|^{1/2}$.*

Proof. Let $\mathfrak{a}$ be generated additively by $\alpha_1, \ldots, \alpha_n$, so that Γ is generated by $\phi(\alpha_1), \ldots, \phi(\alpha_n)$. Let B be the matrix with entries $(\rho_i\alpha_j)$, where ρ_i varies over all embeddings (real and complex) of K. Then $\mathrm{Disc}(\mathfrak{a}) = \det(B)^2 = N(\mathfrak{a})^2 D_K$. Also, let C be the matrix consisting of inner products $(\langle\phi(\alpha_i), \phi(\alpha_j)\rangle) = (\sum_{k=1}^n \tau_k(\alpha_i)\overline{\tau_k}(\alpha_j)) = B^T\overline{B}$. Thus $|\det C|^{1/2} = |\det B|$, and since $\mathrm{vol}(\Gamma) = |\det C|^{1/2} = \mathrm{Disc}(\mathfrak{a})^{1/2}$, we have $\mathrm{vol}(\Gamma) = N(\mathfrak{a})|D_K|^{1/2}$. $\square$

Lemma 6. *$v = \frac{2^{S+T}\pi^T R_K}{\omega_K}$.*

Proof. Let $\mathcal{F}$ be this set whose volume we wish to compute. Define $\mathcal{F}_k$ for $0 \leq k < \omega_K$ by applying the map $x \mapsto e^{\frac{2\pi k}{\omega_K}}x$ to $\mathcal{F}$; since multiplication by a unit is volume-preserving, we have $\mathrm{vol}(\mathcal{F}) = \mathrm{vol}(\mathcal{F}_k)$. Define $\overline{\mathcal{F}}$ to be the intersection of $\cup_{k=0}^{\omega_K}\mathcal{F}_k$ with the subset $\{(x_1, \ldots, x_S; x_{S+1}, \ldots, x_{S+T}) : x_1 > 0, \ldots, x_S > 0\}$. Multiplying any point in $\overline{\mathcal{F}}$ by $(\pm1, \ldots, \pm1; 1, \ldots, 1)$ shows that $\mathrm{vol}(\mathcal{F}) = \frac{2^S}{\omega_K}\mathrm{vol}(\overline{\mathcal{F}})$, and so we will compute $\mathrm{vol}(\overline{\mathcal{F}})$ through multiple changes of variable.

First, we change from the $(S+T)$-dimensional complex space $\mathcal{L}^{S,T}$ to $\mathbb{R}^n$ via the transformation which maps a point $(x_1, \ldots, x_S; x_{S+1}, \ldots, x_{S+T}) \in \overline{\mathcal{F}}$ to the real-valued point $(\rho_1, \ldots, \rho_S, \rho_{S+1}, \varphi_{S+1}, \ldots, \rho_{S+T}, \varphi_{S+T})$, where $\rho_j = |x_j|$ and $\varphi_j = \arg x_j$ for all j (we say $x_j = y_j + iz_j = \rho_j e^{i\varphi_j}$). A straightforward computation shows the Jacobian of this transformation to be $\rho_{S+1} \cdots \rho_{S+T}$. Then $\overline{\mathcal{F}}$ is given by the conditions $\rho_1 > 0, \ldots, \rho_{S+T} > 0$;

$\prod_{j=1}^{S+T} \rho_j^{e_j} \leq 1$, where e_j is the jth coordinate of $\lambda = (1, \ldots, 1; 2, \ldots, 2)$; and $0 \leq \xi_k < 1$ in the formula for each jth coordinate of $l(x)$:

$$\log \rho_j^{e_j} = \frac{e_j}{n} \log \left(\prod_{k=1}^{S+T} \rho_k^{e_k} \right) + \sum_{k=1}^{S+T-1} \xi_k l_j(\varepsilon_k).$$

These conditions do not restrict φ_j for any value $S+1 \leq j \leq S+T$, so they take on all values in $[0, 2\pi)$. We now change variables again, replacing $\rho_1, \ldots, \rho_{S+T}$ with $\xi, \xi_1, \ldots, \xi_{S+T-1}$ according to

$$\log \rho_j^{e_j} = \frac{e_j}{n} \log \xi + \sum_{k=1}^{S+T-1} \xi_k l_j(\varepsilon_k) \tag{7}$$

Since the sum of the e_j is n, and $\sum_{j=1}^{S+T} l_j(\varepsilon_k) = 0$, we sum all the equations (7) and find $\xi = \prod_{j=1}^{S+T} \rho_j^{e_j}$. Thus $\overline{\mathcal{F}}$ is now defined by the conditions $0 < \xi \leq 1$ and $0 \leq \xi_k < 1$ for $1 \leq k \leq S+T$; clearly this set has positive volume now. This transformation has Jacobian

$$\begin{aligned}
J &= \begin{vmatrix} \frac{\rho_1}{n\xi} & \frac{\rho_1}{e_1} l_1(\varepsilon_1) & \cdots & \frac{\rho_1}{e_1} l_1(\varepsilon_{S+T-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\rho_{S_T}}{n\xi} & \frac{\rho_{S+T}}{e_{S+T}} l_{S+T}(\varepsilon_1) & \cdots & \frac{\rho_{S+T}}{e_{S+T}} l_{S+T}(\varepsilon_{S+T-1}) \end{vmatrix} \\
&= \frac{\rho_1 \cdots \rho_{S+T}}{n\xi 2^T} \begin{vmatrix} e_1 & l_1(\varepsilon_1) & \cdots & l_1(\varepsilon_{S+T-1}) \\ \vdots & \vdots & \ddots & \vdots \\ e_{S+T} & l_{S+T}(\varepsilon_1) & \cdots & l_{S+T}(\varepsilon_{S+T-1}) \end{vmatrix} \\
&= \frac{\rho_1 \cdots \rho_{S+T}}{n\xi 2^T} \begin{vmatrix} n & 0 & \cdots & 0 \\ e_2 & l_2(\varepsilon_1) & \cdots & l_2(\varepsilon_{S+T-1}) \\ \vdots & \vdots & \ddots & \vdots \\ e_{S+T} & l_{S+T}(\varepsilon_1) & \cdots & l_{S+T}(\varepsilon_{S+T-1}) \end{vmatrix}
\end{aligned}$$

This determinant is now exactly nR_K, so $J = \frac{\rho_1 \cdots \rho_{S+T}}{n(\rho_1 \cdots \rho_S \rho_{S+1}^2 \cdots \rho_{S+T}^2) 2^T} \cdot nR_K = \frac{R_K}{2^T \rho_{S+1} \cdots \rho_{S+T}}$. We can now compute the volume of $\overline{\mathcal{F}}$:

$$\begin{aligned}
\mathrm{vol}(\overline{\mathcal{F}}) &= 2^T \int \cdots \int_{\overline{\mathcal{F}}} dx_1 \cdots dx_S dy_{S+1} dz_{S+1} \cdots dy_{S+T} dz_{S+T} \\
&= 2^T \int \cdots \int_{\overline{\mathcal{F}}} \rho_{S+1} \cdots \rho_{S+T} \cdot d\rho_1 \cdots d\rho_{S+T} d\varphi_{S+1} \cdots d\varphi_{S+T} \\
&= 2^T (2\pi)^T \int_0^1 \cdots \int_0^1 \rho_{S+1} \cdots \rho_{S+T} |J| d\xi d\xi_1 \cdots \xi_{S+T-1} \\
&= 2^T (2\pi)^T \frac{R_K}{2^T} = 2^T \pi^T R_K.
\end{aligned}$$

Thus $\mathrm{vol}(\mathcal{F}) = \frac{2^S}{\omega_K} \mathrm{vol}(\overline{\mathcal{F}}) = \frac{2^{S+T} \pi^T R_K}{\omega_K}$ as desired. □

At last, we have our goal.

Proof of Theorem 2. Combining (6), Lemma 3, Lemma 5, and Lemma 6, we have that $\lim_{s\to 1}(s-1)f_A(s) = N(\mathfrak{a})\frac{2^{S+T}\pi^T R_K}{\omega_K N(\mathfrak{a})|D_K|^{1/2}} = \frac{2^{S+T}\pi^T R_K}{\omega_K |D_K|^{1/2}}$. Summing over each class $A \in \mathcal{C}_K$ gives $\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{S+T}\pi^T R_K}{\omega_K |D_K|^{1/2}}h$. □

3 Applications

The most immediate (but unnecessary) application of the class number formula is for $K = \mathbb{Q}$. Here $\zeta_{\mathbb{Q}}(s)$ has residue 1 at $s = 1$ and values $S = 1$, $T = 0$, $R_K = 1$, $\omega_K = 2$ (corresponding to -1 and 1), and $D_K = 1$, from which we compute $h = 1$. This agrees with our knowledge that $\mathbb{Z}$ is a principal ideal domain. We will now explore a less trivial application of this formula.

We can use (2) to write the class number formula in terms of a Dirichlet L-series. Assume $m \in \mathbb{Z}$ is square-free, and let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic number field with discriminant D_K. If $m = -1$ then $\omega_K = 4$, and we know $\mathbb{Q}(i)$ to be a principal ideal domain (i.e., $h_K = 1$). If $m = -3$ then $\omega_K = 6$, and we also know this to have $h_K = 1$. Otherwise, it can be shown easily that if $K/\mathbb{Q}$ is a quadratic extension, then $\omega_K = 2$, with ± 1 the only units in $\mathcal{O}_K$, so assume that K is not one of those two special cases. It can also be shown that $D_K = m$ if $m \equiv 1 \pmod 4$ and $D_K = 4m$ otherwise.

First, suppose $m > 0$. Then $S = 2$ and $T = 0$, so we have $\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{4hR_K}{2\sqrt{D_K}} = \frac{2hR_K}{\sqrt{D_K}}$. By Dirichlet's theorem on units there is a unique (up to inversion) fundamental unit ε, and then $R_K = \log|\varepsilon|$. Thus $h = \frac{\sqrt{D_K}}{2\log|\varepsilon|}\lim_{s\to 1}(s-1)\zeta_K(s)$.

Second, suppose $m < 0$, so that $S = 0$ and $T = 1$. Then instead the residue of $\zeta_K(s)$ at $s = 1$ is $\frac{\pi R_K h}{\sqrt{-D_K}}$. Here, though, the entire group of units has rank $S + T - 1 = 0$ and so the regulator is the trivial determinant; that is, $R_K = 1$. So $h = \frac{\sqrt{|D_K|}}{\pi}\lim_{s\to 1}(s-1)\zeta_K(s)$. We now wish to evaluate the limit factor, for which we need a lemma about Kronecker symbols.

Lemma 7. *If* $\left(\frac{D_K}{p}\right) = 1$*, then* (p) *decomposes into a product of two distinct prime ideal factors. If* $\left(\frac{D_K}{p}\right) = -1$*, then* (p) *remains prime. Otherwise, if* $\left(\frac{D_K}{p}\right) = 0$*, then* (p) *is the square of a prime ideal.*

Proof. We know that (p) has at most two prime factors. Suppose first that p does not divide D_K and that $\left(\frac{D_K}{p}\right) = 1$; then $x^2 \equiv D_K \pmod{4p}$ has a solution, which we will call a. Let $r = \frac{a-D_K}{2}$ and define $\mathfrak{p} = (p, r + \frac{D_K+\sqrt{D_K}}{2})$ and $\mathfrak{q} = (p, r + \frac{D_K-\sqrt{D_K}}{2})$. Set $w = \frac{a+\sqrt{D_K}}{2}$, which is the root of $x^2 - ax + tp$ for some $t \in \mathbb{Z}$ and so is an integer. However, w/p is not an integer, since that would imply $\frac{w-\overline{w}}{p}$ is an integer, as is $\left(\frac{w-\overline{w}}{p}\right)^2 = \frac{D_K}{p^2}$, a contradiction. Thus p divides neither w nor $\overline{w}$, but it does divide $w\overline{w} = tp$ and so (p) is not prime. An easy calculation verifies that $\mathfrak{p}\mathfrak{q} = (p)(p, r + \frac{D_K+\sqrt{D_K}}{2}, r + \frac{D_K-\sqrt{D_K}}{2}, \frac{a^2-D_K}{4p}) = (p)$, since the middle two generators in the right factor have difference $\sqrt{D_K}$ and so generate D_K, which is relatively prime to p, making that ideal equal to (1). We last check that $\mathfrak{p} \neq \mathfrak{q}$, subce $(\mathfrak{p}, \mathfrak{q}) = (p, r + \frac{D_K+\sqrt{D_K}}{2}, r + \frac{D_K-\sqrt{D_K}}{2})$ again contains both p and D_K and so is (1).

Now suppose that $(p) = \mathfrak{p}\mathfrak{q}$ with $\mathfrak{p} \neq \mathfrak{q}$. Then $N(\mathfrak{p}) = p$, and $1, 2, \ldots, p-1$ are all distinct modulo $\mathfrak{p}$, so for some $r \in \mathbb{Z}$ we have $\frac{D_K+\sqrt{D_K}}{2} \equiv r \pmod{p}$, or $(2r - D_K)^2 \equiv D_K \pmod{4p}$. The same holds modulo $4\mathfrak{q}$ as well, and thus modulo $4p$. But this implies that $\left(\frac{D_K}{p}\right) = 1$, so (p) decomposes into a product of distinct prime ideals if and only if $\left(\frac{D_K}{p}\right) = 1$.

On the other hand, we consider the case $p|D_K$ with p odd. Set $\mathfrak{q} = (p, \frac{D_K+\sqrt{D_K}}{2})$; then $\overline{\mathfrak{q}} = (p, \frac{D_K-\sqrt{D_K}}{2}) = (p, \frac{D_K-\sqrt{D_K}}{2} - D_K) = (p, \frac{D_K+\sqrt{D_K}}{2}) = \mathfrak{q}$. But we then compute $\mathfrak{q}^2 = \mathfrak{q}\overline{\mathfrak{q}} = (p)(p, \frac{D_K+\sqrt{D_K}}{2}, \frac{D_K+\sqrt{D_K}}{2}, \frac{D_K(D_K-1)}{4p}) = (p)$. Last, if $p = 2|D_K$, then we have two remaining cases: if $m \equiv 2 \pmod 4$, then $(2) = (2, \sqrt{m})^2$, and if $m \equiv 3 \pmod 4$, then $(2) = (2, 1 + \sqrt{m})^2$, and this completes the proof of the lemma. □

Theorem 8. *$\zeta_K(s) = \zeta(s)L(s, \chi)$, where $L(s, \chi) = \sum_{k=1}^{\infty} \left(\frac{D_K}{k}\right) k^{-s}$.*

Proof. In the above statement, we have the character $\chi(k) = \left(\frac{D_K}{k}\right)$, which we must first show is nonprincipal. We know that the discriminant D_K, which is not a square, is either 0 or 1 (mod 4), and we split this into two cases. First, suppose $D_K \equiv 1 \pmod 4$. Then write $D_K = p^a r$ where $(p, r) = 1$ and p, a, r are all odd. Pick a quadratic nonresidue s modulo p and solve $x \equiv s \pmod p$, $x \equiv 1 \pmod{|r|}$, respectively. Then we evaluate $\left(\frac{D_K}{x}\right) = \left(\frac{x}{|D_K|}\right) = \left(\frac{x}{p}\right)^a \left(\frac{x}{|r|}\right) = \left(\frac{s}{p}\right)^a = (-1)^a = -1$, so the character is nonprincipal. Second, suppose $D_K = 4^a b$ with b odd. The $b \equiv 3 \pmod 4$ case falls to similar analysis with the system $x \equiv 3 \pmod 4$, $x \equiv 1 \pmod{|b|}$, and $x > 0$. The remaining $b \equiv 1 \pmod 4$ case requires only slightly more work; let $b = p^c q$ with p, c, q all odd and $(p, q) = 1$, choose a nonresidue s modulo p, and solve $x \equiv s \pmod p$, $x \equiv 1 \pmod{|q|}$, and $x \equiv 1 \pmod 2$. This analysis shows that in all cases we may find x with $\left(\frac{D_K}{x}\right) = -1$.

Now we may use the Euler product and write:

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p}^{-s})} = \prod_{p} \prod_{\mathfrak{p}|p} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

since each prime ideal $\mathfrak{p}$ divides some rational prime ideal. If $\left(\frac{D_K}{p}\right) = 1$, then $(p) = \mathfrak{p}\mathfrak{q}$ splits, with $N(\mathfrak{p}) = N(\mathfrak{q}) = p$, so

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \frac{1}{1 - N(\mathfrak{p})^{-s}} \frac{1}{1 - N(\mathfrak{q})^{-s}} = \frac{1}{1 - p^{-s}} \frac{1}{1 - \left(\frac{D_K}{p}\right) p^{-s}}.$$

If instead $\left(\frac{D_K}{p}\right) = -1$, then (p) is prime with $N(p) = p^2$, so

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \frac{1}{1 - p^{-2s}} = \frac{1}{1 - p^{-s}} \frac{1}{1 - \left(\frac{D_K}{p}\right) p^{-s}}.$$

Last, if $\left(\frac{D_K}{p}\right) = 0$, then $(p) = \mathfrak{p}^2$ with $N(\mathfrak{p}) = p$, and we get the same result as before for the product. Thus, by collapsing Euler products, we have the desired result:

$$\zeta_K(s) = \prod_p \left(1 - p^{-s}\right)^{-1} \prod_p \left(1 - \left(\frac{D_K}{p}\right) p^{-s}\right)^{-1} = \zeta(s) L(s, \chi).$$

□

Since $L(s, \chi)$ is nonprincipal, it does not have a pole at $s = 1$. Thus $\lim_{s \to 1}(s-1)\zeta_K(s) = \lim_{s \to 1}(s-1)\zeta(s)L(s,\chi) = \mathrm{Res}_{s=1}\zeta(s) \cdot L(1,\chi) = L(1,\chi)$ by Theorem 1. So we now have:

Theorem 9. *Let m be a square-free integer which is neither -1 nor -3, and let $K = \mathbb{Q}(\sqrt{m})$. Then $\mathcal{O}_K$ contains exactly two units, and so:*

$$h = \begin{cases} \frac{\sqrt{D_K}}{2 \log |\varepsilon|} L(1, \chi) & \textit{if } m > 0 \\ \frac{\sqrt{|D_K|}}{\pi} L(1, \chi) & \textit{if } m < 0. \end{cases} \tag{8}$$

There are many ways to reduce $L(1, \chi)$ to a finite sum; for example, Theorem 3.3 of §3 of [Ayo63] shows that for imaginary quadratic fields, $h = \frac{-1}{D_K} \sum_{r=1}^{|D_K|-1} r \left(\frac{D_K}{r}\right)$, and for real quadratic fields, $h = \frac{-1}{2\log|\varepsilon|} \sum_{r=1}^{D_K - 1} \left(\frac{D_K}{r}\right) \log \sin \frac{\pi r}{D_K}$. We will conclude, though, with three examples where the L-series can be evaluated directly.

First, take $K = \mathbb{Q}(i)$. We must remember that this was one of our special cases ($\omega = 4$ instead of $\omega_K = 2$), so we actually have $h = \frac{\omega_K \sqrt{|D_K|}}{2\pi} L(1,\chi) = \frac{4 \cdot 2}{2\pi} L(1,\chi) = \frac{4}{\pi} L(1,\chi)$. The L-series here evaluates to $L(1,\chi) = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots$, which we may recognize as Gregory's formula for $\arctan 1 = \frac{\pi}{4}$. Therefore we see that $h = 1$.

Second, take $K = \mathbb{Q}(\sqrt{5})$, with $D_K = 5$. Our formula produces $h = \frac{\sqrt{5}}{2 \log \frac{1+\sqrt{5}}{2}} L(1,\chi)$; we then use generating function techniques to compute:

$$\begin{aligned} L(1,\chi) &= \sum_{r=0}^{\infty} \left(\frac{1}{5r+1} - \frac{1}{5r+2} - \frac{1}{5r+3} + \frac{1}{5r+4} \right) \\ &= \int_0^1 (1 - x - x^2 + x^3)(1 + x^5 + x^{10} + x^{15} + \ldots) dx \\ &= \int_0^1 \frac{1 - x - x^2 + x^3}{1 - x^5} dx = 0.4304089410\ldots \end{aligned}$$

from which we can evaluate $h = 1$. Note that this also suggests a more general way to compute h with finitely many terms for a quadratic field; the integral may even be approximated with any of a variety of fast approximation algorithms, since it should typically be obvious which is the expected integer value of h.

Third, the smallest such discriminant associated with a quadratic field with nontrivial class group is $D_K = -15$ for $K = \mathbb{Q}(\sqrt{-15})$. In this case, $h = \frac{\sqrt{15}}{\pi} L(1,\chi)$, and we compute as before:

$$\begin{aligned} L(1,\chi) &= \sum_{r=0}^{\infty}\left(\frac{1}{15r+1}+\frac{1}{15r+2}+\frac{1}{15r+4}-\frac{1}{15r+7}+\frac{1}{15r+8}-\frac{1}{15r+11}-\frac{1}{15r+13}-\frac{1}{15r+14}\right) \\ &= \int_0^1 \frac{1+x+x^3-x^6+x^7-x^{10}-x^{12}-x^{13}}{1-x^{15}}dx = 1.622311470\ldots \end{aligned}$$

from which we conclude correctly that $h = 2$. This can be verified using the extensive tables provided in [BS66].

References

[Ahl79] L. V. Ahlfors, *Complex Analysis*, McGraw-Hill, Inc., 1979.

[Ayo63] R. Ayoub, *An Introduction to the Analytic Theory of Numbers*, American Mathematical Society, 1963.

[BS66] Z. I. Borevich and I. R. Shafarevich. *Number Theory*, translated by N. Greenleaf, Academic Press, Inc., 1966.

[Hil97] D. Hilbert, *Zahlbericht*, 1897, translated by I. T. Adamson as *The Theory of Algebraic Number Fields*, Springer-Verlag Berlin Heidelberg, 1998.

[Jar03] F. Jarvis, *Zeta Functions of Number Fields I*, `http://www.sheffield.ac.uk/~pm1afj/courses/zeta/zeta_k1.ps`.

[Lan70] S. Lang, *Algebraic Number Theory*, Addison-Wesley Publishing Company, Inc., 1970.

[Ste05] W. A. Stein, *Introduction to Algebraic Number Theory*, `http://modular.fas.harvard.edu/129-05/notes/129.pdf`.