The Analytic Class Number Formula and the Birch and Swinnerton-Dyer Conjecture

Andrei Jorza

April 26, 2005

1 Notation

Let K be a number field, let $\mathcal{O}_K$ be the ring of integers, let $\overline{K}$ be an algebraic closure of K and let $\overline{\mathcal{O}}_K$ be the ring of integers of $\overline{K}$. Let M_K^0 be the set of finite places and let M_K^∞ be the set of infinite places. Let K_v be the completion of K at v and let $\mathcal{O}_v$ be the ring of integers of K_v. Let $\wp_v$, k_v, q_v be the maximal ideal of $\mathcal{O}_v$, the residue field $\mathcal{O}_v/\wp_v$ and the size of the residue field $|k_v|$, respectively. The r real infinite places v correspond to embeddings $i_k : K \hookrightarrow \mathbb{R}$ and the s complex infinite places v corresponds to embeddings $j_k : K \hookrightarrow \mathbb{C}$. For each finite place v, let $v(x)$ be the valuation of $x \in K_v$ at v. If v is infinite, let $v = \log|\sigma(x)|$, where σ is the embedding associated to v. For finite v, let e_v and f_v be the ramification and inertia index of K at v. If v is real, let $e_v = f_v = 1$ and if v is complex, let $e_v = 1, f_v = 2$.

Theorem 1.1 (Dirichlet Unit Theorem). *The unit group $\mathcal{O}_K^\times$ is a rank $r+s-1$ $\mathbb{Z}$-module with*

$$\mathcal{O}_K^\times \cong \mu(K) \times \bigoplus_{i=1}^{r+s-1} \mathbb{Z}\ell_i.$$

Proof. See [**?**], Theorem 1.7.4. □

Proposition 1.2. *The regulator R_K of the number field K, defined as the determinant*

$$R_K = |\det(f_{v_i} v_i(\ell_j))|,$$

where ℓ_j are the generators of the torsion-free part of the unit group and $\{v_i\}$ are any $r+s-1$ of the infinite places, is independent of choices.

Proof. See [**?**], Theorem 1.7.5. □

Let $\mathrm{Cl}(K)$ be the class group and let h_K be the class number. Let $w_K = |\mu(K)|$.

Definition 1.3. Let $H = H_K$ be the Hilbert class field of K, i.e., the maximal abelian unramified extension of K. It can be constructed as

$$H = (K^{\mathrm{ab}})^{r_K(\prod_{v\nmid\infty}\mathcal{O}_v^\times \times \prod_{v|\infty} K_v^\times)},$$

where $r_K : \mathbb{A}_K^\times / \overline{K^\times(\prod \mathbb{R}_{>0}^\times \prod \mathbb{C}^\times)} \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$ is the global Artin map.

Proposition 1.4. *For every ideal I of $\mathcal{O}_K$, the ideal $I\mathcal{O}_H$ is principal.*

Proof. See [**?**], Theorem 6.7.5. □

Definition 1.5. The ζ-function of K is

$$\zeta_K = \sum (\mathbf{N}I)^{-s},$$

where I runs through all the integral ideals of $\mathcal{O}_K$.

Let E be an elliptic curve defined over K.

Theorem 1.6 (Mordell-Weil). *The group $E(K)$ is finitely generated and*

$$E(K) \cong E(K)_{\mathrm{tors}} \times \bigoplus \mathbb{Z}e_i.$$

Proof. See [**?**], Theorem 1. □

If ℓ is a prime number, let $T_\ell E$ be the Tate module of E, i.e., $T_\ell E = \varprojlim E[\ell^n]$.

Definition 1.7. The *global L-function* is

$$L(E,s) = \prod_v \det(1 - \sigma_v q_v^{-s} | (\mathrm{Hom}(T_\ell E, \mathbb{Z}_\ell) \otimes \mathbb{Q}_\ell)^{I_v})^{-1},$$

where σ_v is a lift of $\phi_v : x \mapsto x^{-q_v}, \phi_v \in \mathrm{Gal}(\overline{k}_v/k_v)$ to $\mathrm{Gal}(\overline{K}_v/K_v)$ and I_v is the inertia at v.

A more explicit expression for the local L-factors is

$$L_v(E,s) = \begin{cases} \det(1 - \mathrm{Frob}_v\, q_v^{-s} | T_\ell E)^{-1}, E \text{ has good reduction at } v \\ (1 - q_v^{-s})^{-1}, E \text{ has split multiplicative reduction at } v \\ (1 + q_v^{-s})^{-1}, E \text{ has nonsplit multiplicative reduction at } v \\ 1, E \text{ has additive reduction at } v \end{cases}$$

Even more explicitly, if ℓ is prime and $a_\ell = \ell + 1 - |E(\mathbb{F}_\ell)|$, then $L_v(E,s) = (1 - a_\ell q_v^{-s} + q_v^{1-2s})^{-1}$ if E has good reduction at v.

Definition 1.8. Let $Ш(E/K) = \ker(H^1(K,E) \to \bigoplus_v H^1(K_v, E))$ be the Shafarevich-Tate group of E.

Note that a priori the restriction maps are defined into the direct product, but one can show that the image lies in the direct sum.

Let $\langle , \rangle$ be the Neron-Tate height pairing on E (see [**?**] Theorem 8.9.3).

Definition 1.9. The regulator R_E of E is the determinant

$$R_E = |\det(\langle e_i, e_j \rangle)|.$$

2 The Theorem and the Conjecture

Proposition 2.1. *The function ζ_K converges absolutely to a holomorphic function on* $\mathrm{Re}s > 1$. *There exists a meromorphic continuation of ζ_K to $\mathbb{C} \setminus \{1\}$.*

Proof. See [**?**] Corollary 5.5.11.i. □

Theorem 2.2 (Analytic Class Number Formula). *Let K be a number field and let $n = r + s - 1$ be the rank of $\mathcal{O}_K^\times$. Then*

$$\frac{1}{n!}\zeta_K^{(n)}(0) = -\frac{h_K R_K}{w_K}.$$

Proof. See [**?**] Corollary 5.5.11.ii. The statement here is not about the derivative, but about the residue at 1. However, the two statements are equivalent under the functional equation satisfied by ζ_K. □

Theorem 2.3. *There exists a holomorphic continuation of $L(E, s)$ to all of $\mathbb{C}$.*

Proof. Complicated. Uses the conjecture of Shimura and Taniyama, proven by Wiles, Taylor, Breuil, Conrad and Diamond. □

Conjecture 2.4 (Birch and Swinnerton-Dyer). *The order of vanishing of $L(E, s)$ at 1 is r, the rank of the abelian group $E(K)$. Moreover,*

$$\frac{1}{r! \int_{E(\mathbb{A}_K)} d\mu} L^{(r)}(E, 1) = \frac{R_E |Ш(E/K)|}{|E(K)_{\mathrm{tors}}|^2},$$

where $d\mu$ is a normalized Tamagawa measure with convergence factors $L_v(E, 1)$.

3 Similarities

The obvious similarities are between the definitions of $\zeta_K(s)$ and $L(E,s)$. Also, w_K is the size of the torsion of $\mathcal{O}_K^\times$, while the Conjecture has the torsion part squared. The regulators are similar in definition. The important and nontrivial similarity is that each formula looks at the derivative whose order is equal to the rank of the abelian group involved in the definitions. Moreover, there is a similarity between $\mathrm{Cl}(K)$ and $Ш(E/K)$, that will be made more precise in the following.

Let $Ш(K) = \ker(H^1(K, \overline{\mathcal{O}}^\times) \to \prod_{v \nmid \infty} H^1(K_v, \overline{\mathcal{O}}_v^\times))$.

Proposition 3.1. *There exists a homomorphism $\Phi : \mathrm{Cl}(K) \to Ш(K)$.*

Proof. For each fractional ideal I of $\mathcal{O}_K$, the ideal $I\mathcal{O}_H$ is principal, where H is the Hilbert class field of K. Therefore, there exists $x \in H^\times$ such that $I\mathcal{O}_H = x\mathcal{O}_H$. For each $\sigma \in \mathrm{Gal}(H/K)$, we have $(I\mathcal{O}_H)^\sigma = I\mathcal{O}_H$ so $(x^\sigma) = (x)$ which means that $\sigma(x)/x \in \mathcal{O}_L^\times$. Therefore, $x \in \overline{K}^\times$ such that $\sigma(x)/x \in \overline{\mathcal{O}}^\times$ so the map $\sigma \mapsto \sigma(x)/x$ is a cocycle in $Z^1(K, \overline{\mathcal{O}}_K^\times)$. If y is another generator of $I\mathcal{O}_H$, then $y/x \in \mathcal{O}_L^\times$, so $\sigma(x/y)/(x/y)$ is a coboundary, so it is trivial in $H^1(K, \overline{\mathcal{O}}_K^\times)$.

Clearly, the map Φ that takes I to the cocycle $\Phi(I)(\sigma) = \sigma(x)/x$ is a homomorphism. To show that it induces the desired homomorphism, it is enough to check that if $I = (\alpha)$ for $\alpha \in K^\times$, then $\Phi(I)$ is trivial. Then, we may choose $x = \alpha$ so $\Phi(I)(\sigma) = \sigma(\alpha)/\alpha = \alpha/\alpha = 1$, since $\alpha \in K$. Therefore, the cocycle is trivial. □

Lemma 3.2. *For every $f \in Ш(K)$, there exists a finite Galois extension L/K and $x \in L^\times$ such that $f(\sigma) = \sigma(x)/x$ and $(x) = (x^\sigma)$ as ideals of $\mathcal{O}_L$.*

Proof. Let $f \in H^1(K, \overline{\mathcal{O}}_K^\times)$ be a cocycle, such that the image of f in $H^1(K_v, \overline{\mathcal{O}}_v^\times)$ is trivial for each v. The injection $\overline{\mathcal{O}}_K^\times \to K^\times$ induces an map $H^1(K, \overline{\mathcal{O}}_K^\times) \to H^1(K, \overline{K}^\times) = 0$ (by Hilbert 90). Therefore, there exists $x \in \overline{K}$, such that $f(\sigma) = \sigma(x)/x$. Let L be the Galois closure of $K(x)$. Then $f(\sigma) = \sigma(x)/x$ for all $\sigma \in \mathrm{Gal}(L/K)$. Therefore, $f(\sigma) = \sigma(x)/x \in \mathcal{O}_L^\times$ so $(x) = (x^\sigma)$ for all $\sigma \in \mathrm{Gal}(L/K)$. □

Lemma 3.3. *There exists a homomorphism $Ш(K) \to \mathrm{Pic}(K) \otimes \mathbb{Q}$.*

Proof. To $f \in Ш(K)$ we have associated a finite Galois extension L/K and $x \in L^\times$ such that $f(\sigma) = \sigma(x)/x$. For each place v of K such that $v(x) > 0$, the group $\mathrm{Gal}(L/K)$ acts tranzitively on $w \mid v$. Therefore, all the exponents $w(x)$ are equal to a positive integer m_v. Consider the map

$$f \mapsto \sum_v \frac{m_v}{e_{w/v}}(v),$$

for some $w \mid v$, where $e_{w/v}$ is the ramification index of L_w/K_v. If $M/L/K$ is a Galois tower, and $u \mid w \mid v$ is a tower of valuations, then $m_u = m_w e_{u/w}$ so

$$\frac{m_u}{e_{u/v}} = \frac{m_w e_{u/w}}{e_{u/v}} = \frac{m_w}{e_{w/v}},$$

so the map is independent of the choice of L.

If $g = f$ in $H^1(K, \overline{\mathcal{O}}_K^\times)$, and (y) is the ideal associated to g (for a common Galois extension L), then $f(\sigma) = \sigma(x)/x = g(\sigma)\sigma(t)/t = \sigma(yt)/(yt)$ for some $t \in \mathcal{O}_L^\times$. Therefore, $\sigma(yt/x) = yt/x$ for all $\sigma \in \mathrm{Gal}(L/K)$. Therefore, $yt/x \in \mathcal{O}_K^\times$ so $w(y) = w(x) \pmod{e_{w/v}}$ for an extension of places $w \mid v$. Let $\pi_v \in K^\times$ be uniformizers for K_v. Then, the element of $\mathrm{Div}(K) \otimes \mathbb{Q}$ associated to $\prod_v \pi_v^{v(yt/x)} \in K^\times$ is

$$\sum_v v(yt/x)(v) = \sum_v \frac{w(y)}{e_{w/v}}(v) - \sum_v \frac{w(x)}{e_{w/v}}(v),$$

so the elements $\sum_v \frac{w(x)}{e_{w/v}}(v)$ and $\sum_v \frac{w(y)}{e_{w/v}}(v)$ are equal modulo the image of principal ideals in $\mathrm{Div}(K) \otimes \mathbb{Q}$. Therefore, the map defined is a homomorphism from $Ш(K) \to \mathrm{Pic}(K) \otimes \mathbb{Q}$, which is independent of the choices of cocycle representative and trivializer of the cocycle in $H^1(K, \overline{K}^\times)$. □

Lemma 3.4. *There exists a homomorphism* $\Psi : Ш(K) \to \mathrm{Cl}(K)$.

Proof. For each cocycle $f \in Ш(K)$ we have defined an element $d_f \in \mathrm{Pic}(K) \otimes \mathbb{Q}$. For each finite place v, the restriction $\mathrm{res}_v f \in H^1(K_v, \overline{\mathcal{O}}_v^\times)$ is trivial, so there exists a finite Galois extension L_v/K_v and $x_v \in \mathcal{O}_{L_v}^\times$, such that $\mathrm{res}_v f(\sigma) = \sigma(x_v)/x_v$ for all $\sigma \in \mathrm{Gal}(L_/K_v)$. If $d_f = \sum d_v(v)$, then $\mathrm{res}_v d_f = d_v(v)$ is the element of $\mathrm{Pic}(K_v) \otimes \mathbb{Q}$ associated to $\mathrm{res}_v f$ (by definition). So $\sigma(x)/x = \sigma(x_v)/x_v$, which implies that $\sigma(x_v/x) = x_v/x$ for all $\sigma \in \mathrm{Gal}(L_v/K_v)$. Therefore, $x_v/x \in \mathcal{O}_v^\times$ so $0 = w(x_v) \in w(x) + e_{w/v}\mathbb{Z}$, which means that $d_v \in e_{w/v}\mathbb{Z}/e_{w/v} = \mathbb{Z}$ (for all v). Therefore, $d_f \in \mathrm{Pic}(K) = \mathrm{Cl}(K)$. □

Proposition 3.5. *There exists an isomorphism* $\mathrm{Cl}(K) \cong Ш(K)$.

Proof. It is enough to show that the maps Φ and Ψ are inverses to each other. Clearly, $\Psi \circ \Phi$ is the identity, by construction. Therefore, the result would follow from the injectivity of Ψ. Let $f \in Ш(K)$ be a cocycle such that $\Psi(f) = \mathcal{O}_K$, i.e., there exists $y \in K^\times$, such that $d_f = \mathrm{div} y = \sum_v v(y)(v)$. Then $y = \prod \pi_v^{v(y)} \in K^\times$ and we see that $x/y \in \overline{\mathcal{O}}_K^\times$ and $g(\sigma) = \sigma(x/y)/(x/y)$ is the trivial cocycle. But $f(\sigma) = g(\sigma)\sigma(y)/y = g(\sigma)$ so f is the trivial cocycle (since σ acts trivially on $K^\times$). □

There is a more sophisticated approach to showing that $Ш(K)$ and $\mathrm{Cl}(K)$ are isomorphic. One of Mazur's theorems says that $\ker(H^1(K,E) \to \prod_{v \nmid \infty} H^1(K_v, E))$ is equal to the image of $H^1_{\text{ét}}(\operatorname{Spec} \mathcal{O}_K, \mathcal{E}^0)$ in $H^1_{\text{ét}}(\operatorname{Spec} \mathcal{O}_K, \mathcal{E})$, where $\mathcal{E}$ is the Néron model of E over $\mathcal{O}_K$ and $\mathcal{E}^0$ is the connected component of the identity of $\mathcal{E}$. Then, we can interpret Cl to use the integral model $\mathbb{G}_m$ over $\mathcal{O}_K$, in which case $Ш(K)$ would be the identified with $H^1(\operatorname{Spec} \mathcal{O}_K, \mathbb{G}_m) = \mathrm{Pic}(K) = \mathrm{Cl}(K)$.

References

[Neu99] Jürgen Neukirch, *Algebraic number theory*, vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.