The Coates-Wiles Theorem

Contents

1 Introduction

In [CW77], Coates and Wiles proved that if the L-function of a CM elliptic curve defined over $\mathbb{Q}$ does not vanish at one, then it contains finitely many rational points. This provided one of the first theoretical evidence for the Birch and Swinnerton-Dyer conjecture. Their proof used p-adic methods. Rubin later used the technique of Euler systems to give a different proof. This essay is an exposition of Rubin's proof, based largely on [Rub99].

Section 2 proves the basic results concerning elliptic curves with complex multiplication, including the factorization of the L-function into Hecke L-functions and a relation between the Selmer groups and certain ideal class groups. Section 3 looks at the analytic side and prove a special value formula for the L-function at $s = 1$. Section 4 derives the fundamental properties of elliptic units, which are used in section 5 to bound the ideal class group. Section 6 combines all of the results above and prove the Coates-Wiles theorem. Finally, section 7 performs some numerical computation on an explicit curve.

Most of the algebraic number theory notations used are standard: if F is a number field, then its ring of integers is $\mathcal{O}_F$, its completion at a prime $\mathfrak{p}$ is $F_\mathfrak{p}$, and the ring of integers of $F_\mathfrak{p}$ is $\mathcal{O}_{F_\mathfrak{p}}$ or $\mathcal{O}_{F,\mathfrak{p}}$. The idele group of F is denoted by $\mathbb{I}_F$. The absolute Galois group of F is G_F. The Artin reciprocity map of global class field theory is

$$[-, F] : \mathbb{I}_F/F^\times \to G_F^{\mathrm{ab}}$$

normalized by sending a prime $\mathfrak{p}$ to the arithmetic Frobenius $\mathrm{Frob}_\mathfrak{p}$ on abelian extensions unramified at $\mathfrak{p}$. For an ideal $\mathfrak{m}$, $F(\mathfrak{m})$ is the ray class group with modulus $\mathfrak{m}$ until section 5, where it will be redefined. Locally at a prime $\mathfrak{p}$, the additive valuation $v_\mathfrak{p}$ is normalized such that $v_\mathfrak{p}(\pi) = 1$ for a uniformizer π. In the local absolute Galois group $G_{F_\mathfrak{p}}$, the inertial group is $I_{F_\mathfrak{p}}$.

In this essay, K will always be an imaginary quadratic field. We will drop the letter K from notations when convenient. For example, $\mathcal{O}_{K_\mathfrak{p}}$ will be written as $\mathcal{O}_\mathfrak{p}$.

2 Elliptic Curves with Complex Multiplication

Basic notations and results from the theory of elliptic curves will be assumed. The more involved theorems used will come with a citation, mostly to [Sil09].

2.1 Fundamental results

In this section, we state the main theorem for elliptic curves with complex multiplication and deduce a few consequences, including the factorization of the L-function into Hecke L-functions.

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$. Let E be an elliptic curve defined over a subfield F of $\mathbb{C}$. We say that E has complex multiplication by $\mathcal{O}$ if there exists an isomorphism $\mathcal{O} \xrightarrow{\sim} \mathrm{End}_F(E)$, $\alpha \mapsto [\alpha]$. We can then identify $\mathcal{O}$ as a subring of F by $[\alpha]^*\omega = \alpha\omega$ for any invariant differential ω on E. The square bracket from the notation will usually be dropped from now on.

Remark. More generally, $\mathcal{O}$ can be replaced by any order in K. We will restrict our attention to the case when $\mathcal{O}$ is the ring of integers. It will be shown that this does not lead to a loss of generality for the Coates-Wiles theorem.

The complex points of E can be parametrized as $\mathbb{C}/\mathfrak{o}$ for a lattice $\mathfrak{o}$, which satisfies $\mathcal{O}\mathfrak{o} = \mathfrak{o}$. We may assume without loss of generality that $\mathfrak{o} \subseteq K$ by scaling, so $\mathfrak{o}$ is a fractional ideal. For each ideal $\mathfrak{m}$ of $\mathcal{O}$, let $E[\mathfrak{m}] = \bigcap_{\alpha \in \mathfrak{m}} E[\alpha]$. The following proposition follows immediately by the analytic parametrization.

Proposition 2.1.

(1) $E[\mathfrak{m}] \cong \mathcal{O}/\mathfrak{m}$ *as* $\mathcal{O}$*-modules.*

(2) $\mathrm{Gal}(F(E[\mathfrak{m}])/F) \hookrightarrow \mathrm{Aut}_\mathcal{O}(\mathcal{O}/\mathfrak{m}) \cong (\mathcal{O}/\mathfrak{m})^\times$

To study the map described in part (2) of the proposition in detail, we use

Theorem 2.2 (Main theorem of complex multiplication)**.** *Let $\xi : \mathbb{C}/\mathfrak{o} \to E(\mathbb{C})$ be an analytic parametrization. For any $\sigma \in \operatorname{Aut}(\mathbb{C})$ and $s \in \mathbb{I}_K$ such that $[s, K] = \sigma|_{K^{\mathrm{ab}}}$, there exists $\xi' : \mathbb{C}/s^{-1}\mathfrak{o} \to E^\sigma(\mathbb{C})$ such that the following diagram commutes:*

$$\begin{tikzcd}
K/\mathfrak{o} \arrow[r, "\xi"] \arrow[d, "s^{-1}"'] & E(\mathbb{C})_{\mathrm{tor}} \arrow[d, "\sigma"] \\
K/s^{-1}\mathfrak{o} \arrow[r, "\xi'"] & E^\sigma(\mathbb{C})_{\mathrm{tor}}
\end{tikzcd}$$

Proof. See [Lan87], Chapter 10, theorem 3. □

Corollary 2.3. *The Hilbert class field of K is $K(j(E))$. In particular, $j(E)$ is algebraic.*

Proof. Suppose $\sigma \in \operatorname{Aut}(\mathbb{C})$ fixed $j(E)$, then $E \cong E^\sigma$, so $s^{-1}\mathfrak{o} = \lambda\mathfrak{o}$ for some $\lambda \in \mathbb{C}^\times$. This immediately implies that $\lambda \in K^\times$, so localizing shows that $s_\mathfrak{p}^{-1} \in \lambda\mathcal{O}_\mathfrak{p}^\times$ for all primes $\mathfrak{p} \subseteq K$. By class field theory, $[s, K]$ fixes H. The converse follows by reversing the above argument. □

Therefore, E can be defined over a number field. In this case, the action of ideles on torsion points can be packaged into a Hecke character.

Theorem 2.4. *Let F be a number field containing K. Suppose E is an elliptic curve defined over F with complex multiplication by $\mathcal{O}$ and analytic parametrization $\xi : \mathbb{C}/\mathfrak{o} \to E(\mathbb{C})$ for an ideal $\mathfrak{o}$ of K.*

(1) For all $t \in \mathbb{I}_F$, there exists a unique $\mu(t) \in K^\times$ such that the following diagram commutes:

$$\begin{tikzcd}
K/\mathfrak{o} \arrow[r, "\xi"] \arrow[d, "\mu(t)\mathbf{N}_{F/K}(t)^{-1}"'] & E(\mathbb{C})_{\mathrm{tor}} \arrow[d, "{[t,F]}"] \\
K/\mathfrak{o} \arrow[r, "\xi"] & E(\mathbb{C})_{\mathrm{tor}}
\end{tikzcd}$$

(2) The map $\psi : \mathbb{I}_F/F^\times \to \mathbb{C}^\times$, $t \mapsto \mu(t)\mathbf{N}_{F/K}(t)_\infty^{-1}$ is a Hecke character. It is unramified at a prime $\mathfrak{p}$ if and only if E has good reduction at $\mathfrak{p}$. In this case, $\psi(\mathfrak{p})$ as an endomorphism of E reduces modulo $\mathfrak{p}$ to the Frobenius endomorphism of the reduction of E.

Proof. (1) Let $s = \mathbf{N}_{F/K}(t)$, then $[s, K] = [t, F]|_{K^{\mathrm{ab}}}$ by class field theory. Also observe that $[t, F]$ fixes E, so by theorem 2.2, there exists a parametrization ξ' such that

$$\begin{tikzcd}
K/\mathfrak{o} \arrow[r, "\xi"] \arrow[d, "s^{-1}"'] & E(\mathbb{C})_{\mathrm{tor}} \arrow[d, "{[t,F]}"] \\
K/s^{-1}\mathfrak{o} \arrow[r, "\xi'"] & E(\mathbb{C})_{\mathrm{tor}}
\end{tikzcd}$$

commutes. In particular, $\mathfrak{o} = \mu s^{-1}\mathfrak{o}$ for some $\mu \in K^\times$. Composing with multiplication by μ on the left hand side gives the required diagram, except with a possibly different parametrization in the bottom edge. This can be fixed by changing μ by a root of unity, corresponding to an automorphism of E. The uniqueness of μ is clear since the other three sides are isomorphisms.

(2) If $t \in F^\times$, embedded into $\mathbb{I}_F$ diagonally, then $[t, F] = \mathrm{Id}_{F^{\mathrm{ab}}}$, and the action of $\mathbf{N}_{F/K}(t)^{-1}$ on $K/\mathfrak{o}$ is normal multiplication. Therefore, setting $\mu(t) = \mathbf{N}_{F/K}(t)$ makes the required diagram commute. This shows that $\psi(F^\times) = 1$. By the uniqueness part of (1), it is multiplicative.

If the finite components of t are all 1, then $\mathbf{N}_{F/K}(t)^{-1}$ acts trivially on $K/\mathfrak{o}$, and $[t, F] = \mathrm{Id}_{F^{\mathrm{ab}}}$ since t is in the connected component of 1 in $\mathbb{I}_F$. Therefore, $\mu(t) = 1$, and $\psi(t) = \mathbf{N}_{F/K}(t)_\infty^{-1}$, which is continuous in t. Now consider the finite ideles. Let

$$\mathbb{I}_{K,\mathfrak{o}} = \prod_{\mathfrak{p}|\mathfrak{o}}(1 + \mathfrak{o}\mathcal{O}_\mathfrak{p}) \prod_{\mathfrak{p}\nmid\mathfrak{o}} \mathcal{O}_\mathfrak{p}^\times$$

then $\mathbb{I}_{K,\mathfrak{o}}$ is open in the finite ideles of K, and if $s \in \mathbb{I}_{K,\mathfrak{o}}$, then $s^{-1}\mathfrak{o} = \mathfrak{o}$. Therefore, if $t \in \mathbf{N}_{F/K}^{-1}(\mathbb{I}_{K,o})$, then $\psi(t) = \mu(t)$ is a root of unity in K, corresponding to the automorphism of E determined by the action of $[t, F]$ on $E(\mathbb{C})_{\text{tor}}$. Simple case work shows that if an automorphism of E fixes $E[6]$, then it must be the identity. Since the Artin map is continuous, the above considerations give an open subgroup of the finite ideles of F in $\ker \psi$. Therefore, ψ is continuous.

Suppose $\mathfrak{p}$ is a prime of F, and $u \in \mathcal{O}_{F_\mathfrak{p}}^\times$, treated as an idele with all other components 1. Choose a rational prime ℓ not lying below $\mathfrak{p}$. Then the definition of ψ shows that $[u, F]$ acts on $T_\ell E$ via $\psi(u)$. The image of $\mathcal{O}_{F_\mathfrak{p}}^\times$ under the Artin map is the inertia group at $\mathfrak{p}$. By the criterion of Néron-Ogg-Shafarevich (theorem VII.7.1 of [Sil09]), it acts trivially if and only if $\mathfrak{p}$ is a prime of good reduction for E, as required. Finally, observe that in this set-up, $\text{Frob}_\mathfrak{p} = [\mathfrak{p}, F(E[\ell^\infty])/F]$ acts on the $T_\ell E$ via $\psi(\mathfrak{p})$. Reducing modulo $\mathfrak{p}$ shows that $\psi(\mathfrak{p})$ acts like the Frobenius endomorphism of the reduced curve $\tilde{E}$ on $T_\ell \tilde{E}$, so it must be the Frobenius endomorphism. □

Remark. In [Lan87], Chapter 10, theorem 8, the fact that $F(E(\mathbb{C})_{\text{tor}})/F$ is abelian is proven using a slight extension of the argument for (2), which shows the stronger result that $E(\mathbb{C})_{\text{tor}} \subseteq F(E[6]) \cdot K^{\text{ab}}$.

The conductor of the resulting character ψ will be denoted by $\mathfrak{f}$. By part (3) of the theorem, E has good reduction at $\mathfrak{p}$ iff $\mathfrak{p} \nmid \mathfrak{f}$. In [ST68], it was shown that the conductor of the elliptic curve is $\mathfrak{f}^2$.

Corollary 2.5. *Let E, F be as in theorem 2.4, then*

(1) For any ideal $\mathfrak{a}$ coprime to $\mathfrak{f}$, $\psi(\mathfrak{a})\mathcal{O} = \mathbf{N}_{F/K}\mathfrak{a}$.

(2) If $E[\mathfrak{p}] \subseteq F$ and $\mathfrak{p} \nmid 6$, then E has good reduction away from $\mathfrak{p}$. In particular, E has potentially good reduction everywhere.

Suppose further that $F = K$, then

(3) For any ideal $\mathfrak{a}$ coprime to $\mathfrak{f}$, the injection of proposition 2.1 is an isomorphism $\text{Gal}(K(E[\mathfrak{a}])/K) \to (\mathcal{O}_K/\mathfrak{a})^\times$.

(4) If $\mathfrak{p} \nmid \mathfrak{f}$ and $\mathfrak{a}$ is coprime to $\mathfrak{p}$, then the extension $K(E[\mathfrak{a}\mathfrak{p}^n])/K(E[\mathfrak{a}])$ is totally ramified above $\mathfrak{p}$.

(5) For any ideal $\mathfrak{a}$, $K(E[\mathfrak{a}\mathfrak{f}])$ is the ray class field $K(\mathfrak{a}\mathfrak{f})$.

(6) The projection $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{f})^\times$ is injective.

Proof. (1) This is clear from the definition of ψ.

(2) The action of G_F on $T_p E$ factors through $\text{Gal}(F(E[\mathfrak{p}^\infty])/F(E[\mathfrak{p}]))$, which by proposition 2.1 is a subgroup of $1 + \mathfrak{p}\mathcal{O}_\mathfrak{p}$. This is isomorphic to $\mathcal{O}_\mathfrak{p}$ via the logarithm since $\mathfrak{p} \nmid 6$. Hence, it has no finite subgroup. By local class field theory, the extension is unramified outside of primes above p, so by the criterion of Néron-Ogg-Shafarevich, E has good reduction away from primes above p. This shows that E has potentially good reduction everywhere. Therefore, for primes above p not equal to $\mathfrak{p}$, the action of the inertia group factors through a finite subgroups. These do not exist.

(3) Let $x \in \mathcal{O}_K$, and let s be the idele defined by $s_\mathfrak{p} = x_\mathfrak{p}$ if $\mathfrak{p}|\mathfrak{f}$ and $s_\mathfrak{p} = 1$ otherwise. If $x - 1$ is sufficiently divisible by primes dividing $\mathfrak{f}$, then $\psi(s) = 1$, so $[s, K]$ acts on $E[\mathfrak{a}]$ by x^{-1}. Each $\bar{x} \in (\mathcal{O}/\mathfrak{a})^\times$ can be lifted to such an x by the Chinese remainder theorem, so the map is surjective.

(4) The assumptions imply that $K(E[\mathfrak{a}])/K$ is unramified at $\mathfrak{p}$ (this is a slight generalization of [Sil09], theorem VII.4.1). It remains to prove that $K(E[\mathfrak{p}^n])/K$ is totally ramified at $\mathfrak{p}$. Let $u \in \mathcal{O}_\mathfrak{p}^\times$, then $[u, K]$ acts on $E[\mathfrak{p}^\infty]$ by u^{-1}, where u is embedded into $\mathbb{I}_K$ with all other components set to 1. Therefore, $\mathcal{O}_\mathfrak{p}^\times$ surjects onto $\text{Gal}(K(E[\mathfrak{p}^n])/K)$ via the local Artin map, which is equivalent to the extension being totally ramified above $\mathfrak{p}$.

(5) Let x be an idele such that $[x, K] \in G_{K(\mathfrak{af})}$, then $v_{\mathfrak{p}}(x-1) \geq v_{\mathfrak{p}}(\mathfrak{af})$ for all $\mathfrak{p}|\mathfrak{af}$. In particular, $\psi(x) = 1$, so the action of $[x, K]$ on $E[\mathfrak{af}]$ is via x^{-1}, which is 1 by the properties of x. The converse to the argument also holds.

(6) Let $u \in \mathcal{O}^{\times}$, and let x be the finite part of u as an idele. Then $\psi(x) = \psi(u^{-1}x) = u$. If u maps to 1 in $(\mathcal{O}/\mathfrak{f})^{\times}$, then $u = \psi(x) = 1$. □

Using these properties, we can produce the required factorization of the L-function.

Theorem 2.6. *Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$. Let E be an elliptic curve defined over a finite extension F of K with complex multiplication by $\mathcal{O}$. Let $\psi : \mathbb{I}_F/F^{\times} \to \mathbb{C}^{\times}$ be the Hecke character constructed in theorem 2.4. Then*

$$L(E, s) = L(\psi, s)L(\bar{\psi}, s)$$

Proof. Recall the definitions

$$L(E, s) = \prod_{\mathfrak{q} \text{ good}} (1 - a_{\mathfrak{q}}\mathbf{N}\mathfrak{q}^{-s} + \mathbf{N}\mathfrak{q}^{1-2s})^{-1}, \quad L(\psi_F, s) = \prod_{\mathfrak{q}\nmid\mathfrak{f}} (1 - \psi(\mathfrak{q})\mathbf{N}\mathfrak{q}^{-s})^{-1}$$

where $a_{\mathfrak{q}}$ is the trace of the Frobenius of E reduced modulo $\mathfrak{q}$, and the bad factors in $L(E, s)$ are one since E has additive reductions. The theorem follows since $\psi(\mathfrak{q})$ acts as the Frobenius. □

2.2 Division points

This section studies some local properties of the torsion points of E. We assume, as in the rest of the essay, that E has complex multiplication by the ring of integers $\mathcal{O}$ of an imaginary quadratic field K, and furthermore E is defined over K. By corollary 2.3, K has class number 1.

We briefly recall some facts about elliptic curves over local fields. Let F be an algebraic extension of K, and let $\mathfrak{P}$ be a prime of good reduction for $E_{/F}$, then by proposition VII.2.1 in [Sil09], there is an exact sequence of abelian groups

$$0 \to E_1(F_{\mathfrak{P}}) \to E(F_{\mathfrak{P}}) \to \tilde{E}(k_{F,\mathfrak{P}}) \to 0$$

Here, $\tilde{E}$ is the reduction of $E_{/F}$ modulo $\mathfrak{P}$, and $E_1(F_{\mathfrak{P}})$ is defined to be the kernel of the reduction map. If E is given by a Weierstrass equation minimal at $\mathfrak{P}$, then $E_1(F_{\mathfrak{P}})$ consists of all $P \in E(F_{\mathfrak{P}})$ with $v_{\mathfrak{P}}(x(P)) < 0$. Let $\hat{E}$ be the formal group law associated to E, then proposition VII.2.2 in [Sil09] gives an isomorphism

$$E_1(F_{\mathfrak{P}}) \xrightarrow{\sim} \hat{E}(\mathfrak{P}), \ (x, y) \mapsto z = -x/y$$

From the general theory of formal groups, there is a logarithm map giving an isomorphism $\lambda_E : \hat{E} \to \hat{\mathbb{G}}_a$. Explicitly, λ_E is the unique formal power series such that $\lambda_E(0) = 0$ and $\lambda'_E(Z) = \hat{\omega}(Z)$, where $\hat{\omega}$ is the formal completion of the invariant differential. This induces an isomorphism $E_1(F_{\mathfrak{P}}) \to \mathfrak{P}$ if $v_p(\mathfrak{P})/(p-1) < 1$. The condition holds for $K_{\mathfrak{p}}$ if $p > 3$.

Lemma 2.7. *Let $\mathfrak{p}$ be a prime of good reduction for E, generated by $\pi \in \mathcal{O}$. Then*

(1) The reduction of π modulo $\mathfrak{p}$ is bijective.

(2) All $\mathfrak{p}$-torsions of E lie in $E_1(\bar{K}_{\mathfrak{p}})$.

(3) $E(K_{\mathfrak{p}})/\pi^n E(K_{\mathfrak{p}}) \cong E_1(K_{\mathfrak{p}})/\pi^n E_1(K_{\mathfrak{p}})$.

Proof. By corollary 2.5, π differs from $\psi(\mathfrak{p})$ by a unit, so by theorem 2.4, π reduces to the Frobenius endomorphism of $\tilde{E}$ up to an automorphism, which implies (1). Statements (2) and (3) follow immediately from (1), the exact sequence relating E_1, E, and $\tilde{E}$, and the snake lemma. □

Let $\mathfrak{p}$ and π be as in the lemma. Fix a Weierstrass model of E which is minimal at $\mathfrak{p}$. To study more carefully the $\mathfrak{p}$-power torsions of E, consider the power series associated with the endomorphism $[\pi]$ of $\hat{E}$. Let it be $f \in \mathcal{O}_{\mathfrak{p}}[[Z]]$, then it satisfies

- $f(Z) \equiv Z^{\mathbf{N}\mathfrak{p}} \pmod{\mathfrak{p}}$.
- $f(Z) \equiv \pi Z \pmod{Z^2}$.

The first property holds since $[\pi]$ reduces to the Frobenius. The second property follows from a short calculation using our normalization assumption that $[\pi]^*\omega = \pi\omega$. These properties make $\hat{E}$ into a Lubin-Tate formal group, first defined in [LT65]. Most of the local properties of the field of $\mathfrak{p}$-division points are consequences of this fact.

Lemma 2.8. *Let $\mathfrak{p}$ be a prime of good reduction for E, with a chosen minimal Weierstrass model at $\mathfrak{p}$. Let $P, Q \in E$ be points with coprime orders $\mathfrak{b}$ and $\mathfrak{c}$. Fix an extension of $v_{\mathfrak{p}}$ to $\bar{K}$, then*

(1) If $n > 0$ and $\mathfrak{b} = \mathfrak{p}^n$, then

$$v_{\mathfrak{p}}(x(P)) = -2/(\mathbf{N}\mathfrak{p}^{n-1}(\mathbf{N}\mathfrak{p} - 1))$$

(2) If $\mathfrak{b}$ is not a power of $\mathfrak{p}$, then $v_{\mathfrak{p}}(x(P)) \geq 0$.

(3) If $\mathfrak{b}$ and $\mathfrak{c}$ are both not powers of $\mathfrak{p}$, then $v_{\mathfrak{p}}(x(P) - x(Q)) = 0$.

Proof. (1) This follows easily from theorem 2 of [LT65]. For completeness, we prove it here again. Let $f^{(n)}$ be the n-fold iteration of f defined above. The points of exact order $\mathfrak{p}^n$ correspond to the roots of $\Phi_n = f^{(n)}/f^{(n-1)}$. Using the properties of f, the power series Φ_n satisfies

- $\Phi_n(Z) \equiv Z^{\mathbf{N}\mathfrak{p}^n - \mathbf{N}\mathfrak{p}^{n-1}} \pmod{\mathfrak{p}}$.
- $\Phi_n(Z) \equiv \pi \pmod{Z}$.

By the Weierstrass preparation theorem and Eisenstein's criterion, Φ_n has $\mathbf{N}\mathfrak{p}^n - \mathbf{N}\mathfrak{p}^{n-1}$ roots of $\mathfrak{p}$-adic valuation $-1/(\mathbf{N}\mathfrak{p}^n - \mathbf{N}\mathfrak{p}^{n-1})$. Finally, note that if P corresponds to z under the isomorphism $E_1(K_{\mathfrak{p}}) \cong \hat{E}(\mathfrak{p})$, then $v_{\mathfrak{p}}(x(P)) = -2v_{\mathfrak{p}}(z)$. The result follows.

(2) The group $E_1(\bar{K}_{\mathfrak{p}})$ has only $\mathfrak{p}$-power torsions, so P is not in it, which implies the claim.

(3) If $v_{\mathfrak{p}}(x(P) - x(Q)) > 0$, then over the reduced curve $\bar{E}$, $\bar{P} = \pm\bar{Q}$, so $\bar{P} \pm \bar{Q} = 0$, which shows that $P \pm Q \in E_1(\bar{K}_{\mathfrak{p}})$. Since $\mathfrak{b}$ and $\mathfrak{c}$ are coprime, $P \pm Q$ cannot have $\mathfrak{p}$-power order. This is a contradiction. □

The next goal is to describe the local Kummer pairing. Let $\mathfrak{p}$ and π be as above, and let $n \geq 1$. Suppose further that $\mathfrak{p} \nmid 6$. Recall that the exact sequence $0 \to E(\bar{K}_{\mathfrak{p}})[\mathfrak{p}^n] \to E(\bar{K}_{\mathfrak{p}}) \to E(\bar{K}_{\mathfrak{p}}) \to 0$ gives rise to the Kummer sequence

$$0 \to E(K_{\mathfrak{p}})/\pi^n E(K_{\mathfrak{p}}) \xrightarrow{\varphi} H^1(K_{\mathfrak{p}}, E[\mathfrak{p}^n]) \to H^1(K_{\mathfrak{p}}, E)[\mathfrak{p}^n] \to 0$$

Explicitly, given $P \in E(K_{\mathfrak{p}})$, let $Q \in E(\bar{K}_{\mathfrak{p}})$ be such that $\pi^n Q = P$, then $\varphi(P)$ is the cocycle $\sigma \mapsto \sigma Q - Q$. Let $K_n = K[\mathfrak{p}^n]$, then K_n/K is totally ramified above $\mathfrak{p}$ by corollary 2.5. By an abuse of notation, we write $K_{n,\mathfrak{p}}$ for the completion of K_n at the unique prime above $\mathfrak{p}$. Also write $G_n = \mathrm{Gal}(K_n/K)$, then we have a composite

$$E(K_{\mathfrak{p}})/\pi^n E(K_{\mathfrak{p}}) \hookrightarrow H^1(K_{\mathfrak{p}}, E[\mathfrak{p}^n]) \xrightarrow{res} \mathrm{Hom}(G_{K_{n,\mathfrak{p}}}, E[\mathfrak{p}^n])^{G_n} \longrightarrow \mathrm{Hom}(K_{n,\mathfrak{p}}^{\times}, E[\mathfrak{p}^n])^{G_n}$$

where the final map is composing with the local Artin map. Call this map d_n. This is $\mathcal{O}$-linear, so by density $\mathcal{O}_{\mathfrak{p}}$-linear. Let $P \in E(K_{\mathfrak{p}})$ the unique point such that $\lambda_E(P) = \pi$. Let $\delta_n = d_n(P)$, then $\delta_n : K_{n,\mathfrak{p}}^{\times} \to E[\mathfrak{p}^n]$ is a G_n-equivariant homomorphism, and it generates the image of d_n as a $\mathcal{O}_{\mathfrak{p}}$-module.

Lemma 2.9. $\delta_n(\mathcal{O}_{n,\mathfrak{p}}^{\times}) = E[\mathfrak{p}^n]$.

Proof. Observe that the only $G_{K_\mathfrak{p}}$-submodule of $E[\mathfrak{p}^n]$ are $E[\mathfrak{p}^m]$ for $0 \leq m \leq n$. Since δ_n has order $\mathfrak{p}^n$, its image cannot lie inside $E[\mathfrak{p}^{n-1}]$, so δ_n is surjective. The quotient $\delta_n(K_{n,\mathfrak{p}}^\times)/\delta_n(\mathcal{O}_{n,\mathfrak{p}}^\times)$ is $G_{K_\mathfrak{p}}$-invariant, but $E[\mathfrak{p}^n]/E[\mathfrak{p}^m]$ is not invariant unless $m = n$, which proves the claim. □

The above constructions can be repeated for a general Lubin-Tate group. Wiles ([Wil78]) gave an explicit formula for δ_n in that generality, which generalizes the eariler work of Artin-Hasse and Iwasawa for cyclotomic fields. We state a corollary of the result to avoid a long diversion into Lubin-Tate groups.

Theorem 2.10 (Wiles' Reciprocity Law)**.** *Suppose (z_n) is an $\mathcal{O}_\mathfrak{p}$ generator of $T_\pi \hat{E}$, i.e. z_n generates $\hat{E}[\mathfrak{p}^n]$ and $[\pi](z_n) = z_{n-1}$. Let $(u_n) \in \varprojlim \mathcal{O}_{K_n}^\times$, with the transition maps being norms. Then there exists a unique $g \in \mathcal{O}_\mathfrak{p}[[Z]]^\times$ such that $g(z_n) = u_n$. Furthermore,*

$$\delta_n(u_n) = \left[(\pi - 1)\frac{g'(0)}{g(0)}\right] z_n$$

Proof. The existence and uniqueness of g is theorem I.2.2 of [dS87]. It uses Coleman norm operators. The original explicit reciprocity law and its proof can be found in [Wil78] or section I.4.2 of [dS87]. It is stated with the different assumption that $\mathbf{N}_{K_n/K}(u_n) = \pi$ for all n. Our statement, which is theorem 12.3 of [Rub99], follows by applying the original theorem to (β_n) and $(\beta_n u_n)$ for any sequence (β_n) satisfying the original theorem's condition. □

2.3 Selmer group

This section uses the structure of complex multiplication to relate the Selmer groups of E to certain ideal class groups. The notations and assumptions from the previous subsection are kept.

Let $\alpha \in \mathrm{End}_K(E) \cong \mathcal{O}$, and F be a number field containing K. Recall that the Selmer group $S_\alpha(E_{/F})$ is a subgroup of $H^1(F, E[\alpha])$ satisfying certain local conditions. More precisely, for each place v of F, we have a restriction map $\mathrm{res}_v : H^1(F, E[\alpha]) \to H^1(F_v, E[\alpha])$ and a subgroup

$$H^1_\mathcal{F}(F_v, E[\alpha]) = \mathrm{Im}\left(E(F_v)/\alpha E(F_v) \to H^1(F_v, E[\alpha])\right)$$

given by the image of the Kummer map. The α-Selmer group of $E_{/F}$ is then

$$S_\alpha(E_{/F}) = \{c \in H^1(F, E[\alpha]) : \mathrm{res}_v(c) \in H^1_\mathcal{F}(F_v, E[\alpha]) \text{ for all places } v \text{ of } F\}$$

Let $H^1_s(F_v, E[\alpha]) = H^1(F_v, E[\alpha])/H^1_\mathcal{F}(F_v, E[\alpha])$. By Kummer theory, this is isomorphic to $H^1(F_v, E)[\alpha]$. In these terms, the above definition can be re-written as

$$S_\alpha(E_{/F}) = \{c \in H^1(F, E[\alpha]) : \mathrm{res}_v(c) = 0 \text{ in } H^1_s(F_v, E[\alpha]) \text{ for all places } v \text{ of } F\}$$

The goal of this essay is to bound the rank of $S_\pi(E)$, where π generates a prime $\mathfrak{p}$ of K.

We will first consider a modified Selmer group $S'_\alpha(E_{/F})$, formed like the normal Selmer group, except with the local conditions above α dropped, i.e.

$$S_\alpha(E_{/F}) = \{c \in H^1(F, E[\alpha]) : \mathrm{res}_v(c) \in H^1_\mathcal{F}(F_v, E[\alpha]) \text{ for all places } v \nmid \alpha\}$$

Theorem 2.11. *Let $\mathfrak{p} = \pi\mathcal{O}$ be a prime of K not dividing $6\mathfrak{f}$. Let $n \geq 1$, $K_n = K(E[\mathfrak{p}^n])$, then*

$$S'_{\pi^n}(E) = \mathrm{Hom}(\mathrm{Gal}(M_n/K_n), E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$$

where M_n is the maximal abelian p-extension of K_n unramified outside of primes above $\mathfrak{p}$.

Proof. We first compute $S'_{\pi^n}(E_{/K_n})$. By corollary 2.5, $E_{/K_n}$ has good reduction outside of $\mathfrak{p}$. Let $\mathfrak{q}$ be a prime of K_n not dividing $\mathfrak{p}$, then by the general theory of elliptic curves, $H^1_\mathcal{F}(K_{n,\mathfrak{q}}, E[\mathfrak{p}^n])$ is exactly the unramified classes $H^1(G_{K_{n,\mathfrak{q}}}/I_{K_{n,\mathfrak{q}}}, E[\mathfrak{p}^n])$ (theorem X.4.2 of [Sil09]). Therefore, $S'_{\pi^n}(E_{/K_n}) =$

$H^1(G, E[\mathfrak{p}^n])$, where G is the Galois group of the maximal extension of K_n unramified outside of primes above $\mathfrak{p}$. Since $E[\mathfrak{p}^n] \subseteq K_n$, this is equal to $\mathrm{Hom}(G, E[\mathfrak{p}^n])$. All such homomorphisms factor uniquely through $\mathrm{Gal}(M_n/K_n)$ since $E[\mathfrak{p}^n]$ is an abelian p-group.

The theorem now follows from a descent calculation. The inflation-restriction sequence gives

$$0 \to H^1(K_n/K, E[\mathfrak{p}^n]) \to H^1(K, E[\mathfrak{p}^n]) \to H^1(K_n, E[\mathfrak{p}_n])^{G_n} \to H^2(K_n/K, E[\mathfrak{p}^n])$$

By corollary 2.5, $G_n = \mathrm{Gal}(K_n/K) \cong (\mathcal{O}/\mathfrak{p}^n)^\times$, which acts on $E[\mathfrak{p}^n] \cong \mathcal{O}/\mathfrak{p}^n$ by multiplication. Let G' be the p-prime part of G_n, then $H^i(G', \mathcal{O}/\mathfrak{p}^n) = 0$ for all $i \geq 0$, so $H^i(G, \mathcal{O}/\mathfrak{p}^n) = 0$ for all $i \geq 0$ by the Hochschild-Serre spectral sequence. Therefore, $H^1(K, E[\mathfrak{p}^n]) \xrightarrow{\sim} H^1(K_n, E[\mathfrak{p}_n])^{G_n}$ via the restriction map. Moreover, restriction maps commute, so $S'_{\pi^n}(E) \subseteq S'_{\pi^n}(E_{/K_n})$. To show that equality holds, a simple diagram chase reduces it to the injectivity of $H^1_s(K_\mathfrak{q}, E[\mathfrak{p}^n]) \to H^1_s(K_{n,\mathfrak{q}'}, E[\mathfrak{p}^n])$ for each prime $\mathfrak{q} \neq \mathfrak{p}$ of K and prime $\mathfrak{q}'$ of K_n above $\mathfrak{q}$. By the inflation-restriction sequence and Kummer theory, its kernel is $H^1(K_{n,\mathfrak{q}'}/K_\mathfrak{q}, E(K_{n,\mathfrak{q}'}))[\mathfrak{p}^n]$.

The general theory of elliptic curves over local fields shows that $E(K_{n,\mathfrak{q}'})$ contains a subgroup of finite index isomorphic to $\mathcal{O}_{K_{n,\mathfrak{q}'}}$ (theorem VII.6.3 of [Sil09]). Therefore, the $\mathfrak{p}$-power torsion part of $E(K_{n,\mathfrak{q}'})$ is $E[\mathfrak{p}^m]$ for a finite $m \geq n$. By construction, $K_{n,\mathfrak{q}'} \cong K_\mathfrak{q}(E[\mathfrak{p}^n])$, so we have

$$H^1(K_{n,\mathfrak{q}'}/K_\mathfrak{q}, E(K_{n,\mathfrak{q}'}))[\mathfrak{p}^n] \subseteq H^1(K_{n,\mathfrak{q}'}/K_\mathfrak{q}, E[\mathfrak{p}^m]) = H^1(K_\mathfrak{q}(E[\mathfrak{p}^m])/K_\mathfrak{q}, E[\mathfrak{p}^m])$$

By proposition 2.1, the final term is $H^1(C, \mathcal{O}/\mathfrak{p}^m)$, where $C \subseteq (\mathcal{O}/\mathfrak{p}^m)^\times$ acts by multiplication. The proof in the previous paragraph shows that if C is not a p-group, then this is 0. Otherwise, we know that $E[\mathfrak{p}] \subseteq K_\mathfrak{q}$, since $\mathrm{Gal}(K_\mathfrak{q}(E[\mathfrak{p}])/K_\mathfrak{q})$ injects into $(\mathcal{O}/\mathfrak{p})^\times$, which has order prime to p. Corollary 2.5 shows that $E_{/K(E[\mathfrak{p}])}$ has good reduction at any prime above $\mathfrak{q}$, so $K_\mathfrak{q}(E[\mathfrak{p}^m])/K_\mathfrak{q}$ is unramified, so its Galois group is cyclic. For any element $a \in \mathcal{O}$,

$$\begin{aligned}\left|\ker(a : \mathcal{O}/\mathfrak{p}^m \to \mathcal{O}/\mathfrak{p}^m)\right| &= |\mathcal{O}/\mathfrak{p}|^{\min(m, v_\mathfrak{p}(a))}\\ \left|\mathrm{Im}(a : \mathcal{O}/\mathfrak{p}^m \to \mathcal{O}/\mathfrak{p}^m)\right| &= |\mathcal{O}/\mathfrak{p}|^{\max(0, m - v_\mathfrak{p}(a))}\end{aligned}$$

The usual formula for H^* of a cyclic group shows that in this case, $H^1(C, \mathcal{O}/\mathfrak{p}^m)$ is also trivial. □

Remark. If p splits in $\mathcal{O}$, then any p-subgroup of $(\mathcal{O}/\mathfrak{p}^m)^\times$ is cyclic, since their inverse limit is isomorphic to $\mathcal{O}_\mathfrak{p} \times \mu_{p-1}$ via the logarithm.

Using global class field theory, the group $\mathrm{Gal}(M_n/K_n)$ can be identified via the Artin map with the pro-p part of $\mathbb{I}_{K_n}/W'_n$, where

$$W'_n = K_n^\times \prod_{v \mid \infty} K_{n,v}^\times \prod_{v \nmid \mathfrak{p}\infty} \mathcal{O}_{n,v}^\times$$

Therefore, the modified Selmer group is

$$S'_{\pi^n}(E) = \mathrm{Hom}(\mathbb{I}_{K_n}/W'_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$$

The correct Selmer group $S_{\pi^n}(E)$ is obtained from it by imposing further conditions at $\mathfrak{p}$. This corresponds to adding a factor to W'_n for primes above $\mathfrak{p}$. Recall that $\mathfrak{p}$ is totally ramified, and $K_{n,\mathfrak{p}}^\times$ is the completion of K_n at the unique prime above $\mathfrak{p}$. We have $G_n = \mathrm{Gal}(K_n/K) = \mathrm{Gal}(K_{n,\mathfrak{p}}/K_\mathfrak{p})$, so there is a diagram

$$\begin{tikzcd}
S_{\pi^n}(E) \arrow[r, hook] \arrow[d] & S'_{\pi^n}(E) \arrow[r, "\sim"] \arrow[d, "\mathrm{res}"'] & \mathrm{Hom}(\mathbb{I}_{K_n}/W'_n, E[\mathfrak{p}^n])^{G_n} \arrow[d] \\
E(K_\mathfrak{p})/\pi^n E(K_\mathfrak{p}) \arrow[r, hook] & H^1(K_\mathfrak{p}, E[\mathfrak{p}^n]) \arrow[r, "f"] & \mathrm{Hom}(K_{n,\mathfrak{p}}^\times, E[\mathfrak{p}^n])^{G_n}
\end{tikzcd}$$

with the left square being cartesian by the definition of the Selmer group. The arrow f is given by restriction followed by pre-composition with the local Artin map. Using the same argument as the descent part of theorem 2.11, one can show that f is injective. The bottom row was the map d_n from the last subsection.

Theorem 2.12. *The map d_n factors through an isomorphism*

$$\bar{d}_n : E(K_\mathfrak{p})/\pi^n E(K_\mathfrak{p}) \xrightarrow{\sim} \operatorname{Hom}(K_{n,\mathfrak{p}}^\times / \ker(\delta_n), E[\mathfrak{p}^n])^G$$

Therefore, $S_{\pi^n}(E) = \operatorname{Hom}(\mathbb{I}_{K_n}/W_n, E[\mathfrak{p}^n])^{\operatorname{Gal}(K_n/K)}$*, with*

$$W_n' = K_n^\times \prod_{v|\infty} K_{n,v}^\times \prod_{v\nmid\mathfrak{p}\infty} \mathcal{O}_{n,v}^\times \cdot \ker(\delta_n)$$

Proof. Clearly d_n factors through $\bar{d}_n$. By lemma 2.9, $K_{n,\mathfrak{p}}^\times/\ker(\delta_n) \cong E[\mathfrak{p}^n]$ as G_n-modules, so the codomain of $\bar{d}_n$ is $\operatorname{End}_{G_n}(E[\mathfrak{p}^n]) \cong \operatorname{End}_{(\mathcal{O}/\mathfrak{p}^n)^\times}(\mathcal{O}/\mathfrak{p}^n) \cong \mathcal{O}/\mathfrak{p}^n$. Since d_n is injective, this proves the first claim. The rest follows from an easy diagram chase. □

From this, we prove our main criterion for the vanishing of the Selmer group.

Theorem 2.13. *Let $\mathfrak{p}$ be a prime of K not diving $6\mathfrak{f}$. Let A be the ideal class group of $K(E[\mathfrak{p}])$ and $\mathcal{E}$ be the unit group of $K(E[\mathfrak{p}])$. Then $S_{\psi(\mathfrak{p})}(E) = 0$ if and only if*

$$\operatorname{Hom}(A, E[\mathfrak{p}])^{\operatorname{Gal}(K(E[\mathfrak{p}])/K)} = 0 \textit{ and } \delta_1(\mathcal{E}) \neq 0$$

Proof. Keep the notations used throughout this section. Let $V = \ker(\delta_1) \cap \mathcal{O}_{1,\mathfrak{p}}^\times$, and let $m\mathbb{Z} = v_\mathfrak{P}(\ker(\delta_n))$, where $\mathfrak{P}$ is the unique prime above $\mathfrak{p}$ in K_1. The usual map from $\mathbb{I}_{K_1}$ to the group of fractional ideals induces an exact sequence

$$0 \to \mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V \to \mathbb{I}_{K_1}/W_1 \to A/\mathfrak{P}^m \to 0$$

where $\bar{\mathcal{E}}$ is the closure of $\mathcal{E}$ in $\mathcal{O}_{1,\mathfrak{p}}^\times$. The functor $\operatorname{Hom}(-, E[\mathfrak{p}])^{G_1}$ is exact since $E[\mathfrak{p}]$ is a cohomologically trivial G_1-module (from the proof of theorem 2.11). Applying it to the sequence gives

$$0 \to \operatorname{Hom}(A/\mathfrak{P}^m, E[\mathfrak{p}])^{G_1} \to S_\pi(E) \to \operatorname{Hom}(\mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V, E[\mathfrak{p}])^{G_1} \to 0$$

Recall that $\mathfrak{p}$ is totally ramified in K_1, so $\mathfrak{P}^{\mathbf{N}\mathfrak{p}-1} = \mathfrak{p} = (\pi)$ is trivial in A. Therefore, $\operatorname{Hom}(A/\mathfrak{P}^m, E[\mathfrak{p}]) = \operatorname{Hom}(A, E[\mathfrak{p}])$. This gives the first condition.

For the second term, note that $\mathcal{O}_{1,\mathfrak{p}}^\times/V \cong E[\mathfrak{p}]$. As a G_1-module, $E[\mathfrak{p}]$ is simple, so the vanishing of the last term of the exact sequence is equivalent to $\bar{\mathcal{E}} \neq 0$ in $\mathcal{O}_{1,\mathfrak{p}}^\times/V$, as required. □

3 Analytic Computations

In this section, we first study the property of some theta functions associated to lattices. We then derive relations between their logarithmic derivatives, some Eisenstein series, and the values of certain Hecke L-functions at positive integers. They will also be used in the next section to construct global units in abelian extensions of imaginary quadratic fields.

3.1 Theta functions

First recall a few classical special functions. Let L be a lattice in $\mathbb{C}$. Let $A(L) = \pi^{-1}\operatorname{vol}(\mathbb{C}/L)$. Define the Weierstrass σ-, ζ-, and $\wp$-functions on L by

$$\begin{aligned}
\sigma(z;L) &= z \prod_{\omega\in L\setminus\{0\}} \left(1 - \frac{z}{\omega}\right) e^{(z/\omega)+\frac{1}{2}(z/\omega)^2}, \\
\zeta(z;L) &= \frac{d}{dz}\log\sigma(z;L) = \frac{1}{z} + \sum_{\omega\in L\setminus\{0\}} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right), \\
\wp(z;L) &= -\zeta'(z;L) = \frac{1}{z^2} + \sum_{\omega\in L\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)
\end{aligned}$$

Further, recall the following standard modular forms

$$G_{2k}(L) = \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^{2k}}, \quad \Delta(L) = (60G_4(L))^3 - 27(140G_6(L))^2$$

They satisfy many interesting relations, some of which will be proven later. We state a few basic well-known properties here with only a sketch of the proof

- The σ-function is holomorphic in $\mathbb{C}$, with one simple zero at each point of L and no other zero. This follows by standard complex analysis.
- The Eisenstein series satisfy the homogeneity relation $G_{2k}(\lambda L) = \lambda^{-2k} G_{2k}(L)$ for $k \geq 2$ and $\lambda \in \mathbb{C}^\times$. In particular, $\Delta(\lambda L) = \lambda^{-12}\Delta(L)$.
- The modular discriminant has a q-product expansion

  $$\Delta([\tau, 1]) = (2\pi i)^{12} q_\tau \prod_{n=1}^{\infty} (1 - q_\tau^n)^{24}$$

  where $q_\tau = e^{2\pi i \tau}$. This can be proven by writing Δ as a product of values of the $\wp$-function and apply the product expansion for σ (corollary 3.3). Details can be found in section 18.4 of [Lan87]. Alternatively, one can derive it from properties of the Eisenstein series $G_2(L)$, which was done in section 1.2 of [DS05].

Proposition 3.1. *There exists an $\mathbb{R}$-linear function η, depending on L, such that*

$$\zeta(z + \omega; L) - \zeta(z; L) = \eta(\omega; L), \quad \frac{\sigma(z + \omega; L)}{\sigma(z; L)} = \pm e^{\eta(\omega; L)(z + \omega/2)}$$

for all $z \in \mathbb{C}$ and $\omega \in L$. The sign in the transformation law for σ is $+$ if $\omega/2 \in L$ and $-$ otherwise.

Proof. The Weierstrass $\wp$-function is periodic with respect to L. Integrate it once to get the relation for ζ, which also defines $\eta(\omega; L)$ for all $\omega \in L$. It is clearly $\mathbb{Z}$-linear, so we can extend η to an $\mathbb{R}$-linear function on $\mathbb{C}$. Integrating the relation for ζ gives

$$\frac{\sigma(z + \omega; L)}{\sigma(z; L)} = \psi(\omega; L) e^{\eta(\omega; L)(z + \omega/2)}$$

for some $\psi(\omega; L)$ to be determined. Applying this with 2ω instead of ω shows that $\psi(2\omega; L) = \psi(\omega; L)^2$. If $\omega/2 \notin L$, then setting $z = -\omega/2$ shows that $\psi(\omega; L) = -1$. Otherwise, one can recursively apply the above relation to get that $\psi(\omega; L) = 1$. □

Remark. We will see an explicit expression for $\eta(\omega; L)$ in corollary 3.9.

Proposition 3.2 (Legendre relation)**.** *If $L = [\omega_1, \omega_2]$, with $\operatorname{Im}(\omega_1/\omega_2) > 0$, then*

$$\eta(\omega_2; L)\omega_1 - \eta(\omega_1; L)\omega_2 = 2\pi i$$

Proof. This follows by integrating ζ around a fundamental parallelogram and applying the previous proposition and the residue theorem. Details can be found in section 18.1 of [Lan87]. □

Corollary 3.3. *Suppose $\operatorname{Im}(\tau) > 0$, then the σ-function has a q-product expansion*

$$\sigma(z; [\tau, 1]) = \frac{1}{2\pi i} e^{\frac{1}{2}\eta z^2} (q_z^{1/2} - q_z^{-1/2}) \prod_{n=1}^{\infty} \frac{(1 - q_\tau^n q_z)(1 - q_\tau^n q_z^{-1})}{(1 - q_\tau^n)^2}$$

where $\eta = \eta(1; [\tau, 1])$, $q_\tau = e^{2\pi i \tau}$, and $q_z = e^{2\pi i z}$.

Proof. Note that the right hand side is an absolutely convergent product since $\mathrm{Im}(\tau) > 0$. One can easily check that the right hand side satisfies the same transformation laws as σ under translation by 1 and τ. It has simple zeroes at points of $[\tau, 1]$ and no other zeroes. Therefore, the quotient of the two sides is a constant, which is easily checked to be 1 by comparing the power series expansions at $z = 0$. Details can be found in section 18.2 of [Lan87]. □

We now define some modified versions of the σ-function which will be useful in this essay. First let

$$\theta(z; L) = \Delta(L) e^{-6\eta(z;L)z} \sigma(z; L)^{12}$$

The discriminant factor is inserted to make $\theta(z; L)$ homogeneous in L, as one may easily check. This is the 12-th power of the Siegel function introduced in section 19.2 of [Lan87]. To make this periodic, let M be any auxiliary lattice containing L, and define

$$\Theta(z; L, M) = \frac{\theta(z; L)^{[M:L]}}{\theta(z; M)}$$

We now prove the periodicity claim and express Θ as a rational function of $\wp$.

Theorem 3.4. *The function $\Theta(z; L, M)$ is meromorphic and periodic with respect to L. It admits a factorization*

$$\Theta(z; L, M) = \frac{\Delta(L)^{[M:L]}}{\Delta(M)} \prod_{\substack{w \in M/L \\ w \neq L}} (\wp(z; L) - \wp(w; L))^{-6}$$

Proof. The $\bar{z}z$ term in the exponent cancels since $A(M) = [M : L]A(L)$, so Θ is meromorphic. Periodicity follows from a short calculation using proposition 3.1. Its divisor on $\mathbb{C}/L$ is $12[M : L](0) - 12 \sum_{w \in M/L}(w)$, which agrees with the divisor of the claimed product expansion. It remains to show that they agree at one point. The leading term at $z = 0$ is

$$\frac{\Delta(L)^{[M:L]}}{\Delta(M)} z^{12([M:L]-1)}$$

for both sides, which proves the result. □

For later use, we prove a distribution relation. Its proof is a simplified and expanded version of the one given in [KL81], section 2.5, which would be fairly tedious if written out in full.

Theorem 3.5. *Let $L \subseteq M$ be lattices, and let $t_0 = 0, \cdots, t_{n-1}$ be a system of coset representatives for M/L, where $n = [M : L]$. Let $z \in \mathbb{C}$ be such that $fz \in L$, then*

$$\prod_{i=0}^{n-1} \theta(z + t_i; L) = \mu\, \theta(z; M)$$

where μ satisfies $\mu^{fn} = 1$. If $z \in M$, then this should be interpreted as an equality of the leading coefficient in the power series expansions, so in particular, taking $z = 0$ gives

$$\prod_{i=1}^{n-1} \theta(t_i; L) = \mu \frac{\Delta(M)}{\Delta(L)}$$

where μ is an n-th root of unity.

Proof. First observe that the left hand side is independent of the choice of representatives, up to an fn-th root of unity. Indeed, if $\omega \in L$ and $\tau \in M$, then the transformation law for σ shows that

$$\frac{\theta(z + \tau + \omega; L)}{\theta(z + \tau; L)} = e^{-6(\eta(z+\tau;L)\omega - \eta(\omega;L)(z+\tau))}$$

Note that $fn(z+\tau) \in L$, so when this is raised to the fn-th power, the expression in the exponent is an integer multiple of $2\pi i$ by the Legendre relation.

We next reduce the general equation to the special case $z = 0$. For this step only, assume the $\{t_i\}$ are chosen such that $\sum t_i = 0$. Then we compute

$$\begin{aligned}
\left(\frac{\prod_{i=0}^{n-1}\theta(z+t_i;L)}{\theta(z;M)}\right)^n &= \prod_{i=0}^{n-1}\frac{\theta(z+t_i;L)^n}{\theta(z;M)} \\
&= \prod_{i=0}^{n-1}\Theta(z+t_i;L,M)e^{-6(\eta(z;M)t_i-\eta(t_i;M)z)} \\
&= e^{-6(\eta(z;M)\sum t_i-\eta(\sum t_i;M)z)}\prod_{i=0}^{n-1}\Theta(z+t_i;L,M) \\
&= \prod_{i=0}^{n-1}\Theta(z+t_i;L,M)
\end{aligned}$$

This function is L-periodic. Its divisor is

$$\sum_{i=0}^{n-1}\left(12n(-t_i)-12\sum_{j=0}^{n-1}(t_j-t_i)\right) = 12n\sum_{i=0}^{n-1}(t_i)-12\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}(t_j-t_i) = 0$$

Hence it is a constant. This concludes the first reduction step.

Suppose $L \subseteq M \subseteq N$, and the theorem holds for M/L and N/M. Let $\{t_0 = 0, \cdots, t_{n-1}\}$ be a system of representatives for M/L, and let $\{s_0 = 0, \cdots, s_{m-1}\}$ be a system of representatives for N/M, then $\{t_i + s_j\}$ is a system of representatives for N/L. Introduce the notation $a \sim_n b$ for $a^n = b^n$, then

$$\prod_{j=0}^{m-1}\prod_{i=0}^{n-1}\theta(z+s_j+t_i;L) \sim_{fmn} \prod_{j=0}^{m-1}\theta(z+s_j;M) \sim_{fm} \theta(z;N)$$

Therefore, we may assume that $[M : L] = p$ is prime.

By homogeneity, we may take $M = [\tau, 1]$. Then L is one of the following $p+1$ sublattices of M:

- $L = [p\tau, 1]$
- $L = [\tau + b, p]$ for $0 \le b \le p-1$.

We will use the product expansion

$$\theta(z;[\tau,1]) = e^{6A(L)^{-1}z(z-\bar{z})}q_\tau(q_z^{1/2}-q_z^{-1/2})^{12}\prod_{n=1}^{\infty}\left((1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1})\right)^{12}$$

where $\mathrm{Im}(\tau) > 0$, $q_\tau = e^{2\pi i\tau}$, and $q_z = e^{2\pi i z}$. This follows from the product expansions of σ and Δ.

In the first case, a set of representatives is $\{0, \tau, \cdots, (p-1)\tau\}$, so

$$\begin{aligned}
\prod_{k=1}^{p-1}\theta(k\tau;[p\tau,1]) &= \prod_{k=1}^{p-1}\left(e^{12\pi i\tau k^2/p}q_\tau^p(q_\tau^{k/2}-q_\tau^{-k/2})^{12}\prod_{n=1}^{\infty}\left((1-q_\tau^{pn+k})(1-q_\tau^{pn-k})\right)^{12}\right) \\
&= q_\tau^{1-p}\prod_{k=1}^{p-1}(1-q_\tau^k)^{12}\prod_{n=1}^{\infty}\prod_{k=1}^{p-1}\left((1-q_\tau^{pn+k})(1-q_\tau^{pn-k})\right)^{12} \\
&= q_\tau^{1-p}\prod_{n=0}^{\infty}\prod_{k=1}^{p-1}(1-q_\tau^{pn+k})^{12}\prod_{n=1}^{\infty}\prod_{k=1}^{p-1}(1-q_\tau^{pn-k})^{12} \\
&= q_\tau^{1-p}\prod_{n=0}^{\infty}\left(\frac{1-q_\tau^n}{1-q_\tau^{pn}}\right)^{24} = \frac{\Delta(M)}{\Delta(L)}
\end{aligned}$$

The second case can be treated similarly. A set of representatives for M/L is $\{0, 1, \cdots, p-1\}$. Let $\tau_L = \frac{\tau+b}{p}$ and $\alpha = e^{2\pi i/p}$, then

$$\begin{aligned}
\prod_{k=1}^{p-1} \theta(k; L) &= \prod_{k=1}^{p-1} \theta(\frac{k}{p}, [\tau_L, 1]) \\
&= \prod_{k=1}^{p-1} \left(q_\tau^{1/p} \alpha^b (\alpha^{k/2} - \alpha^{-k/2})^{12} \prod_{n=1}^{\infty} \left((1 - q_\tau^{n/p} \alpha^{nb+k})(1 - q_\tau^{n/p} \alpha^{nb-k}) \right)^{12} \right) \\
&= \frac{q_\tau}{q_{\tau_L}} \prod_{k=1}^{p-1} (1 - \alpha^{-k})^{12} \prod_{n=1}^{\infty} \prod_{k=1}^{p-1} \left((1 - q_\tau^{n/p} \alpha^{nb+k})(1 - q_\tau^{n/p} \alpha^{nb-k}) \right)^{12}
\end{aligned}$$

Now apply the relation $\prod_{k=1}^{p-1}(1 - \lambda\alpha^k) = \frac{1-\lambda^p}{1-\lambda}$ to get

$$\prod_{k=1}^{p-1} \theta(k; L) = p^{12} \frac{q_\tau}{q_{\tau_L}} \prod_{n=1}^{\infty} \left(\frac{1 - q_\tau^n}{1 - q_{\tau_L}^n} \right)^{24} = \frac{\Delta(M)}{\Delta(\tau_L)} p^{12} = \frac{\Delta(M)}{\Delta(L)}$$

□

3.2 Eisenstein series

Let L be a lattice in $\mathbb{C}$. The real analytic Eisenstein series of weight k associated to L is defined by

$$E_k(z, s; L) = \sum_{\omega \in L} \frac{(\bar{z} + \bar{\omega})^k}{|z + \omega|^{2s}}, \ z \notin L$$

It converges to a holomorphic function in s if $\mathrm{Re}(s) > 1 + \frac{k}{2}$.

Theorem 3.6. *Fix $z \notin L$. The function $E_k(z, s; L)$ can be analytically continued to a meromorphic function for all s. It satisfies a functional equation*

$$\tilde{E}_k(z, s; L) = \tilde{E}_k(z, k + 1 - s; L), \quad \tilde{E}_k(z, s; L) = A(L)^s \Gamma(s) E_k(z, s; L)$$

If $k \neq 0$, then the function is holomorphic. Otherwise, it has a simple pole at $s = 1$ of residue $A(L)^{-1}$.

Proof. This can be done using the standard technique of Mellin transform and Poisson summation. The full proof can be found in [Wei76], section VIII.13. □

Using this, we can define $E_k(z; L) = E_k(z, k; L)$ for all $k \geq 1$. For $k \geq 3$, this definition coincides with the classical one

$$E_k(z; L) = \sum_{\omega \in L} \frac{1}{(z + \omega)^k} = \frac{(-1)^k}{(k-1)!} \frac{d^{k-2}}{dz^{k-2}} \wp(z; L) = \frac{(-1)^{k+1}}{(k-1)!} \frac{d^k}{dz^k} \log \sigma(z; L)$$

It will be shown that if L is the lattice parametrizing a CM curve, then $E_k(z; L)$ is related to the value of its L-function at k. Therefore, we want to better understand them, especially for $k = 1$ for this essay. We first seek similar relations between E_k and σ as above for $k = 1, 2$. They turn out to take the same form, except with some correction terms

Theorem 3.7. *For $z \notin L$,*

$$\begin{aligned}
E_1(z; L) &= \frac{d}{dz} \log \sigma(z; L) - s_2(L) z - A(L)^{-1} \bar{z} \\
E_2(z; L) &= -\frac{d^2}{dz^2} \log \sigma(z; L) + s_2(L)
\end{aligned}$$

where $s_2(L) = \lim_{s \to 0^+} \sum_{\omega \in L \setminus \{0\}} \omega^{-2} |\omega|^{-2s}$, in the sense of analytic continuation.

Proof. Following [BSD65], consider the function

$$\Psi(z,s;L) = \frac{\bar{z}}{|z|^{2s}} + \sum_{\omega\in L\setminus\{0\}} \left(\left(\frac{\bar{z}+\bar{\omega}}{|z+\omega|^{2s}} - \frac{\bar{\omega}}{|\omega|^{2s}} \right) - \frac{\bar{\omega}}{|\omega|^{2s}} \left(\frac{sz}{\omega} + \frac{(s-1)\bar{z}}{\bar{\omega}} \right) \right)$$

The series converges if $\mathrm{Re}(s) > \frac{1}{2}$, and absolutely converges if $\mathrm{Re}(s) > \frac{3}{2}$. At $s = 1$, it is $\zeta(z;L)$. In the half-plane of absolute convergence, re-arranging the terms shows that

$$\Psi(z,s;L) = E_1(z,s;L) + sz \sum_{\omega\in L\setminus\{0\}} \omega^{-2}|\omega|^{2-2s} + (s-1)\bar{z}E_0(0,s;L)$$

Evaluating at $s = 1$ using theorem 3.6 gives the relation for E_1. The relation for E_2 follows by differentiating the first relation. □

Corollary 3.8. *For every $k \geq 1$,*

$$\frac{d^k}{dz^k} \log \Theta(z;L,M) = 12(-1)^{k-1}(k-1)!\big([M:L]E_k(z;L) - E_k(z;M)\big)$$

Proof. This is immediate from the definition of $\Theta(z;L,M)$ and theorem 3.7. □

Note that E_1 has period L by analytic continuation, so we get an expression for $\eta(z;L)$.

Corollary 3.9. $\eta(z;L) = s_2(L)z + A(L)^{-1}\bar{z}$

3.3 Relation with L-values

We specialize the above discussion to a more algebraic setting and express certain L-values using the functions introduced in the previous section. As before, let K be an imaginary quadratic field with ring of integers $\mathcal{O}$. Let E be an elliptic curve over K with complex multiplication by $\mathcal{O}$. Let ψ be the Grössencharakter associated to E by theorem 2.4. Consider the L-function associated to $\bar{\psi}^k$ defined by

$$L(\bar{\psi}^k, s) = \sum_{(\mathfrak{b},\mathfrak{f})=1} \frac{\bar{\psi}^k(\mathfrak{b})}{\mathbf{N}\mathfrak{b}^s}$$

where $\mathfrak{f}$ is the conductor of ψ. Following Hecke's proof of the functional equation, we break the summation into partial L-functions. Choose an ideal $\mathfrak{m}$ divisible by $\mathfrak{f}$ as the modulus. For an ideal $\mathfrak{c}$ prime to $\mathfrak{m}$, let

$$L_{\mathfrak{m}}(\bar{\psi}^k, s, \mathfrak{c}) = \sum{}' \frac{\bar{\psi}^k(\mathfrak{b})}{\mathbf{N}\mathfrak{b}^s}$$

where the sum is taken over all $\mathfrak{b}$ prime to $\mathfrak{m}$ such that $[\mathfrak{b}, K(\mathfrak{m})/K] = [\mathfrak{c}, K(\mathfrak{m})/K]$.

Lemma 3.10. *Let $v \in K^\times$. Suppose its order $\mathfrak{m} = v^{-1}\mathcal{O} \cap \mathcal{O}$ is divisible by $\mathfrak{f}$, then for every $k \geq 1$,*

$$E_k(v;\mathcal{O}) = v^{-k}\psi(\mathfrak{c})^k L_{\mathfrak{m}}(\bar{\psi}^k, k, \mathfrak{c})$$

where $\mathfrak{c} = v\mathfrak{m}$.

Proof. We prove the more general formula

$$E_k(v,s;\mathcal{O}) = \mathbf{N}\mathfrak{m}^{s-k}v^{-k}\psi(\mathfrak{c})^k L_{\mathfrak{m}}(\bar{\psi}^k, s, \mathfrak{c})$$

for s with a sufficiently large real part. The result follows by analytic continuation to $s = k$. Recall that the assumption that E is defined over K implies that K has class number 1, so let μ generate $\mathfrak{m}$, and let $c = v\mu \in \mathcal{O}$. An ideal $\mathfrak{b} = \beta\mathcal{O}$ occurs in the sum of $L_{\mathfrak{m}}(\bar{\psi}^k, s, \mathfrak{c})$ if and only if $\beta = \alpha c$, where $\alpha \in K^\times$ and $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m})$ for all prime $\mathfrak{p}|\mathfrak{m}$. This is also equivalent to $\beta = c + \omega\mu$ with $\omega \in \mathcal{O}$, so

$$L_{\mathfrak{m}}(\bar{\psi}^k, s, \mathfrak{c}) = \sum_{\omega\in\mathcal{O}} \frac{\bar{\psi}((c+\omega\mu)\mathcal{O})^k}{|c+\omega\mu|^{2s}}$$

To evaluate the character, let $\alpha = 1 + \omega\mu/c$, then $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m}) \geq v_\mathfrak{p}(\mathfrak{f})$ for all prime $\mathfrak{p}|\mathfrak{f}$, so $\psi(\alpha\mathcal{O}) = \psi(\alpha)\psi(\alpha_\infty)^{-1} = \alpha$, where α_∞ is the idele consisting of 1 at finite places and α at the infinite place. Therefore,

$$L_\mathfrak{m}(\bar{\psi}^k, s, \mathfrak{c}) = \frac{\bar{\psi}(\mathfrak{c})^k}{\bar{c}^k} \sum_{\omega \in \mathcal{O}} \frac{(\bar{c} + \bar{\omega}\bar{\mu})^k}{|c + \omega\mu|^{2s}} = \frac{\bar{\psi}(\mathfrak{c})^k}{\bar{c}^k} E_k(c, s; \mu\mathcal{O}) = \frac{\bar{\psi}(\mathfrak{c})^k}{\bar{c}^k} \cdot \frac{\bar{\mu}^k}{|\mu|^{2s}} E_k(v, s; \mathcal{O})$$

To get the required formula, note that $\psi(\mathfrak{c})/c$ is a root of unity by corollary 2.5. □

Fix an ideal $\mathfrak{a}$ of K prime to $6\mathfrak{f}$. In the definition of Θ, take the auxiliary lattice to be $\mathfrak{a}^{-1}$. Corollary 3.8 then gives a relation between values of the partial L-function and values of Θ. To get the full L-function, we multiply together translated versions of Θ. Let B be a set of ideals prime to $\mathfrak{af}$ such that their images under the Artin map exactly traverses $\mathrm{Gal}(K(\mathfrak{f})/K)$. Let f be a generator of $\mathfrak{f}$. Define

$$\Lambda(z; \mathcal{O}, \mathfrak{a}) = \prod_{\mathfrak{b} \in B} \Theta(\psi(\mathfrak{b})f^{-1} + z)$$

Theorem 3.11. *For every $k \geq 1$,*

$$\left.\frac{d^k}{dz^k}\right|_{z=0} \log \Lambda(z; \mathcal{O}, \mathfrak{a}) = 12(-1)^{k-1}(k-1)! f^k (\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a})^k) L(\bar{\psi}^k, k)$$

Proof. By corollary 3.8, the left hand side equals to

$$12(-1)^{k-1}(k-1)! \left(\mathbf{N}\mathfrak{a} \sum_{\mathfrak{b} \in B} E_k(\psi(\mathfrak{b})f^{-1}; \mathcal{O}) - \sum_{\mathfrak{b} \in B} E_k(\psi(\mathfrak{b})f^{-1}; \mathfrak{a}^{-1}) \right)$$

For the first sum, use lemma 3.10 to write it as

$$\sum_{\mathfrak{b} \in B} (\psi(\mathfrak{b})f^{-1})^{-k} \psi(\mathfrak{b})^k L_\mathfrak{f}(\bar{\psi}^k, k, \mathfrak{b}) = f^k L(\bar{\psi}^k, k)$$

For the second sum, the homogeneity property of Eisenstein series gives

$$E_k(\psi(\mathfrak{b})f^{-1}; \mathfrak{a}^{-1}) = \psi(\mathfrak{a})^k E_k(\psi(\mathfrak{ab})f^{-1}; \mathcal{O})$$

The set $\mathfrak{a}B$ is still a set of ideal representatives for $\mathrm{Gal}(K(\mathfrak{f})/K)$. Substituting everything into the expression gives the required result. □

Now, let L be the lattice associated to E, in the sense that there is an analytic parametrization.

$$\xi : \mathbb{C}/L \to E(\mathbb{C}), \ z \mapsto (\wp(z; L), \wp'(z; L))$$

when E is given by a Weierstrass equation $y^2 = 4x^3 - g_4 x - g_6$. Since E has complex multiplication by $\mathcal{O}$, there exists a compelx period Ω such that $L = \Omega\mathcal{O}$. The work we have done can be translated to the lattice L using the homogeneity properties of the functions. Pick a generator α of $\mathfrak{a}$. The expressions for Θ and Λ with respect to L and $\mathfrak{a}^{-1}$ now take the form

$$\Theta_{E,\mathfrak{a}}(P) = \alpha^{-12} \Delta(E)^{\mathbf{N}\mathfrak{a} - 1} \prod_{Q \in E[\mathfrak{a}] \setminus \{0\}} (x(P) - x(Q))^{-6}$$

$$\Lambda_{E,\mathfrak{a}}(P) = \prod_{\sigma \in \mathrm{Gal}(K(\mathfrak{f})/K)} \Theta_{E,\mathfrak{a}}(\sigma S + P)$$

where S is the point associated to Ωf^{-1} under the analytic parametrization, and we have used the definition of ψ for the second expression. Both functions are rational functions defined over K. In this setting, theorem 3.11 becomes

Corollary 3.12. *For every $k \geq 1$,*

$$\left.\frac{d^k}{dz^k}\right|_{z=0} \log \Lambda_{E,\mathfrak{a}}(\xi(z)) = 12(-1)^{k-1}(k-1)! f^k (\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a})^k) \Omega^{-k} L(\bar{\psi}^k, k)$$

It follows easily from this corollary that $L(\bar{\psi}^k, k)/\Omega^k \in K$ for all $k \geq 1$.

3.4 $\mathfrak{p}$-adic expansion

Fix a prime $\mathfrak{p}$ of K of good reduction for E with residue characteristic $p > 3$. Suppose further that $\mathfrak{p} \nmid \mathfrak{a}$. For later use, we calculate the $\mathfrak{p}$-adic expansion of $\Lambda_{E,\mathfrak{a}}$.

Fix a short Weierstrass model for E which is minimal at $\mathfrak{p}$. Let z be the stnadard uniformizer at $0 \in E$ defined by $z = -x/y$, and let $\hat{E}$ be the formal group attached to E over $\mathcal{O}_\mathfrak{p}$. Analytic functions on the complex torus associated to E correspond bijectively with rational functions in x and y via the parametrization $(x, y) = (\wp(z), \wp'(z))$. Taking completion at $\mathfrak{p}$ and the point 0 sends them to the formal power series field $K_\mathfrak{p}(\!(Z)\!)$. Denote the image of $\Lambda_{E,\mathfrak{a}}$ by $\Lambda_{\mathfrak{p},\mathfrak{a}}$.

Lemma 3.13. *Let $\hat{\omega} \in \mathcal{O}_\mathfrak{p}[[Z]]^\times$ be the formal invariant differential of $\hat{E}$. Define a derivation on $K_\mathfrak{p}(\!(Z)\!)$ by $D = \hat{\omega}^{-1}\frac{d}{dZ}$, then the following diagram commutes*

$$\begin{tikzcd}
K(\wp(z), \wp'(z)) \arrow[r, hook] \arrow[d, "\frac{d}{dz}"'] & K_\mathfrak{p}(\!(Z)\!) \arrow[d, "D"] \\
K(\wp(z), \wp'(z)) \arrow[r, hook] & K_\mathfrak{p}(\!(Z)\!)
\end{tikzcd}$$

Proof. It suffices to check this on x and y. Suppose E has the equation $y^2 = 4x^3 - g_4x - g_6$, then

$$\frac{d}{dz}\wp(z) = \wp'(z), \quad \frac{d}{dz}\wp'(z) = 6\wp(z)^2 - \frac{1}{2}g_4$$

By definition, $\hat{\omega} = \frac{1}{2y(Z)}\frac{d}{dZ}x(Z)$, so $D(x(Z)) = y(Z)$ and $D(y(Z)) = 6x(Z)^2 - \frac{1}{2}g_4$. □

The next theorem follows immediately from corollary 3.12 and the lemma.

Theorem 3.14. *For every $k \geq 1$,*

$$D^k|_{Z=0} \log \Lambda_{\mathfrak{p},\mathfrak{a}}(Z) = 12(-1)^{k-1}(k-1)! f^k(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a})^k)\Omega^{-k} L(\bar{\psi}^k, k)$$

Finally, we establish an integrality theorem for $\Lambda_{\mathfrak{p},\mathfrak{a}}$. For convenience, we assume theorem 4.1, to be proven in the next section. Its proof does not require material from this subsection.

Theorem 3.15. $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \in \mathcal{O}_\mathfrak{p}[[Z]]^\times$.

Proof. It is easy to see from the definition that the zeros of $\Lambda_{E,\mathfrak{a}}$ occur at generator of $E[\mathfrak{f}]$. Since $\mathfrak{p} \nmid \mathfrak{f}$, none of them lie in $E_1(\bar{K}_\mathfrak{p})$. Therefore, $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z)$ has no zero. It converges in the maximal ideal of $\mathcal{O}_{\bar{K}_\mathfrak{p}}$ since it comes from a rational function of x and y, so by the Weierstrass preparation theorem, it must lie in $K_\mathfrak{p} \cdot \mathcal{O}_\mathfrak{p}[[Z]]^\times$. The result follows from theorem 4.1 applied to a $\mathfrak{p}$-torsion point. □

Corollary 3.16. *Let $F_\mathfrak{P}$ be an extension of $K_\mathfrak{p}$, and let $z \in \mathfrak{P}$, then*

$$\Lambda_{\mathfrak{p},\mathfrak{a}}(z) \equiv \Lambda_{\mathfrak{p},\mathfrak{a}}(0)\big(1 + 12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a}))(L(\bar{\psi}, 1)/\Omega)z\big) \pmod{\mathfrak{P}^2}$$

Proof. Suppose $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) = a_0 + a_1Z + O(Z^2)$, then $\Lambda_{\mathfrak{p},\mathfrak{a}}(z) \equiv a_0 + a_1Z \pmod{\mathfrak{P}^2}$ for $z \in \mathfrak{P}$ by theorem 3.15. Also observe that $\hat{\omega}(Z) = 1 + O(Z^2)$ by direct computation, so

$$D(\log \Lambda_{\mathfrak{p},\mathfrak{a}}(Z))|_{Z=0} = D(\Lambda_{\mathfrak{p},\mathfrak{a}}(Z))|_{Z=0}/\Lambda_{\mathfrak{p},\mathfrak{a}}(0) = a_0^{-1}a_1$$

The result now follows from theorem 3.14. □

4 Elliptic Units

Keeping the notation from the previous section, we study some arithmetic properties of the functions $\Lambda_{E,\mathfrak{a}}$. The results are exactly the axioms of an Euler system, which will be introduced in the next section.

4.1 Divisibility properties

Recall that $\theta(z; L)$ is homogeneous of weight 0 in L, so the value of $\Theta_{E,\mathfrak{a}}$ is independent of the Weierstrass model chosen.

Theorem 4.1. *Let $\mathfrak{r}$ be an ideal of $\mathcal{O}$ coprime to $\mathfrak{af}$, and let $P \in E[\mathfrak{r}]\backslash\{0\}$. Then $\Lambda_{E,\mathfrak{a}}(P)$ is a global unit in the field $K(E[\mathfrak{r}])$.*

Proof. Each term of $\Lambda_{E,\mathfrak{a}}(P)$ is of the form $\Theta_{E,\mathfrak{a}}(S+P)$, where S has order $\mathfrak{f}$, so we just need to prove that $\Theta_{E,\mathfrak{a}}(Q)$ is a unit if Q has order divisible by at least two primes. By corollary 2.5, E has potentially good reduction, say over the extension F of K. Let $\mathfrak{P}$ be an arbitrary prime of F. Choose a minimal Weierstrass model of $E_{/F}$ at $\mathfrak{P}$, then $v_{\mathfrak{P}}(\Delta(E)) = 0$, so

$$v_{\mathfrak{P}}(\Theta_{E,\mathfrak{a}}(Q)) = -12 v_{\mathfrak{P}}(\alpha) - 6 \sum_{R \in E[\mathfrak{a}]\backslash\{0\}} v_{\mathfrak{P}}(x(Q) - x(R))$$

If the order of R in the above sum is not a power of $\mathfrak{P}$, then part (3) of lemma 2.8 implies that $v_{\mathfrak{P}}(x(Q) - x(R)) = 0$. Otherwise, $v_{\mathfrak{P}}(x(Q)) \geq 0$ and $v_{\mathfrak{P}}(x(R)) = -2/(\mathbf{N}\mathfrak{p}^m - \mathbf{N}\mathfrak{p}^{m-1})$, where $\mathfrak{p}^m$ is the exact order of R. Substituting these values into the expression shows that $v_{\mathfrak{P}}(\Theta_{E,\mathfrak{a}}(Q)) = 0$. □

4.2 Distribution relation

Theorem 4.2. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be coprime ideals of $\mathcal{O}$, and let β be a generator of $\mathfrak{b}$. Suppose further that $\mathfrak{b}$ is coprime to 6, then*

$$\prod_{R \in E[\mathfrak{b}]} \Theta_{E,\mathfrak{a}}(P+R) = \Theta_{E,\mathfrak{a}}(\beta P)$$

Proof. Both sides are rational functions on E defined over K with divisors

$$12 \sum_{Q \in E[\mathfrak{ab}]} (Q) - 12\mathbf{N}\mathfrak{a} \sum_{R \in E[\mathfrak{b}]} (R)$$

Therefore, it remains to prove their ratio is equal to 1 at a point. Let L be the lattice associated to a Weierstrass model of E. Recall that

$$\Theta_{E,\mathfrak{a}}(P) = \Theta(z; L, \mathfrak{a}^{-1}L) = \frac{\theta(z; L)^{\mathbf{N}\mathfrak{a}}}{\theta(z; \mathfrak{a}^{-1}L)}$$

if z is the point corresponding to P. Therefore, at $z = 0$, the ratio is

$$\lambda = \lim_{z \to 0} \Theta(\beta z; L, \mathfrak{a}^{-1}L)^{-1} \prod_{w \in \mathfrak{b}^{-1}L/L} \Theta(z+w; L, \mathfrak{a}^{-1}L) = \beta^{-12(\mathbf{N}\mathfrak{a}-1)} \prod_{\substack{w \in \mathfrak{b}^{-1}L/L \\ w \neq L}} \Theta(w; L, \mathfrak{a}^{-1}L)$$

Expand this using θ and apply theorem 3.5.

$$\lambda = \beta^{-12(\mathbf{N}\mathfrak{a}-1)} \prod_{\substack{w \in \mathfrak{b}^{-1}L/L \\ w \neq L}} \theta(w; L)^{\mathbf{N}\mathfrak{a}} \prod_{\substack{w \in \mathfrak{b}^{-1}L/L \\ w \neq L}} \theta(w; \mathfrak{a}^{-1}L)^{-1} = \beta^{-12(\mathbf{N}\mathfrak{a}-1)} \left(\mu \frac{\Delta(\mathfrak{b}^{-1}L)}{\Delta(L)}\right)^{\mathbf{N}\mathfrak{a}-1}$$

where μ satisfies $\mu^{\mathbf{N}\mathfrak{b}} = 1$. Since $\mathfrak{b}^{-1}L = \beta^{-1}L$, the homogeneity of Δ reduces the above expression to $\lambda = \mu^{\mathbf{N}\mathfrak{a}-1}$. Therefore, $\lambda^{\mathbf{N}\mathfrak{b}} = 1$ and $\lambda \in K$. We assumed that $\mathbf{N}\mathfrak{b}$ is coprime to 12, but roots of unities in K have order divisible by 12. These imply $\lambda = 1$, as required. □

Remark. The conclusion still holds if one drops the additional hypothesis that $\mathfrak{b}$ is coprime to 6. For details, see [dS87] Chapter II, section 2.3.

Theorem 4.3. *Let $\mathfrak{b}$ be an ideal of $\mathcal{O}$ coprime to $\mathfrak{a}$. Let Q be a generator of $E[\mathfrak{b}]$. Suppose $\mathfrak{b} = \mathfrak{p}\mathfrak{b}'$, where $\mathfrak{p} \nmid 6\mathfrak{f}$ is prime and $\mathfrak{f}|\mathfrak{b}'$, then*

$$\mathbf{N}_{K(E[\mathfrak{b}])/K(E[\mathfrak{b}'])}\Theta_{E,\mathfrak{a}}(Q) = \begin{cases} \Theta_{E,\mathfrak{a}}(\psi(\mathfrak{p})Q) & \text{if } \mathfrak{p}|\mathfrak{b}' \\ \Theta_{E,\mathfrak{a}}(\psi(\mathfrak{p})Q)^{1-\mathrm{Frob}_{\mathfrak{p}}^{-1}} & \text{if } \mathfrak{p} \nmid \mathfrak{b}' \end{cases}$$

Proof. This follows essentially formally from the distribution relation (theorem 4.2) and the description of the Galois action on $\Theta_{E,\mathfrak{a}}$.

The Galois group Gal $\big(K(E[\mathfrak{b}])/K(E[\mathfrak{b}'])\big)$ is isomorphic to the kernel of

$$(\mathcal{O}/\mathfrak{b})^\times/\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{b}')^\times/\mathcal{O}^\times$$

via the global Artin map by corollary 2.5. Denote this group by C, and denote the element corresponding to $c \in C$ by σ_c. Then σ_c acts on $E[\mathfrak{b}]$ by $[c\mathcal{O}, K]$, which is multiplication by $\psi(c\mathcal{O})$ by the construction of ψ. By corollary 2.5, $\psi(c\mathcal{O}) \in c\mathcal{O}^\times$, so

$$\mathbf{N}_{K(E[\mathfrak{b}])/K(E[\mathfrak{b}'])}\Theta_{E,\mathfrak{a}}(Q) = \prod_{c\in C}\Theta_{E,\mathfrak{a}}(Q)^{\sigma_c} = \prod_{c\in C}\Theta_{E,\mathfrak{a}}(\psi(c\mathcal{O})Q) = \prod_{c\in C}\Theta_{E,\mathfrak{a}}(cQ)$$

If $\mathfrak{p}|\mathfrak{b}'$, then $\{cQ - Q : c \in C\} = E[\mathfrak{p}]$, so the desired result follows from the distribution relation. Otherwise, $\{cQ - Q : c \in C\} = E[\mathfrak{p}]\backslash\{R_0\}$, where $R_0 \in E[\mathfrak{p}]$ satisfies $Q + R_0 \in E[\mathfrak{b}']$. Note that

$$\Theta_{E,\mathfrak{a}}(Q + R_0)^{\mathrm{Frob}_{\mathfrak{p}}} = \Theta_{E,\mathfrak{a}}(\psi(\mathfrak{p})Q + \psi(\mathfrak{p})R_0) = \Theta_{E,\mathfrak{a}}(\psi(\mathfrak{p})Q)$$

The result follows since $Q + R_0 \neq 0$ by the hypothesis that $\mathfrak{f}|\mathfrak{b}'$. □

Corollary 4.4. *Let $\mathfrak{r}$ be an ideal of $\mathcal{O}$ coprime to $\mathfrak{a}\mathfrak{f}$, and let P be a generator of $E[\mathfrak{r}]$. Suppose $\mathfrak{p}$ is a prime and $\mathfrak{r} = \mathfrak{p}\mathfrak{s}$, then*

$$\mathbf{N}_{K(E[\mathfrak{r}])/K(E[\mathfrak{s}])}\Lambda_{E,\mathfrak{a}}(P) = \begin{cases} \Lambda_{E,\mathfrak{a}}(\psi(\mathfrak{p})P) & \text{if } \mathfrak{p}|\mathfrak{s} \\ \Lambda_{E,\mathfrak{a}}(\psi(\mathfrak{p})P)^{1-\mathrm{Frob}_{\mathfrak{p}}^{-1}} & \text{if } \mathfrak{p} \nmid \mathfrak{s} \end{cases}$$

Proof. Each term of $\Lambda_{E,\mathfrak{a}}(P)$ is of the form $\Theta_{E,\mathfrak{a}}(S+P)$, where S has order $\mathfrak{f}$. The result therefore follows from the previous theorem by taking $Q = S + P$, which generates $E[\mathfrak{r}\mathfrak{f}]$. □

4.3 Congruence relation

Theorem 4.5. *Let $\mathfrak{p}$ be a prime of K not dividing $\mathfrak{a}\mathfrak{f}$. Let $\mathfrak{b}$ be an ideal of $\mathcal{O}$ coprime to $\mathfrak{a}$ such that $v_{\mathfrak{p}}(\mathfrak{b}) = 1$ and $\mathfrak{b} \neq \mathfrak{p}$. Let Q be a generator of $E[\mathfrak{b}]$, then*

$$\Theta_{E,\mathfrak{a}}(Q) \equiv \Theta_{E,\mathfrak{a}}(\psi(\mathfrak{p})Q)^{\mathrm{Frob}_{\mathfrak{p}}^{-1}}$$

modulo every prime above $\mathfrak{p}$.

Proof. By theorem 4.2,

$$\Theta_{E,\mathfrak{a}}(\psi(\mathfrak{p})Q) = \prod_{R\in E[\mathfrak{p}]}\Theta_{E,\mathfrak{a}}(Q + R)$$

It remains to prove that $\Theta_{E,\mathfrak{a}}(Q + R) \equiv \Theta_{E,\mathfrak{a}}(Q)$ modulo every prime above $\mathfrak{p}$, since $\mathrm{Frob}_{\mathfrak{p}}$ acts as $x \mapsto x^{\mathbf{N}\mathfrak{p}}$. By definition,

$$\frac{\Theta_{E,\mathfrak{a}}(Q + R)}{\Theta_{E,\mathfrak{a}}(Q)} = \prod_{S\in E[\mathfrak{a}]\backslash\{0\}}\left(1 + \frac{x(Q + R) - x(Q)}{x(Q) - x(S)}\right)^{-6}$$

Part (3) of lemma 2.8 shows that $v_{\mathfrak{p}}(x(Q) - x(S)) = 0$. For the numerator, modulo any prime above $\mathfrak{p}$, R reduces to 0, so $v_{\mathfrak{p}}(x(Q + R) - x(Q)) > 0$. This proves the claim. □

5 Euler Systems and Kolyvagin Systems

In [Rub00], a general method was given to study Selmer groups associated to p-adic Galois representations. It takes as input a family of compatible cohomology classes, which is called an Euler system. The elliptic units form an Euler system thanks to the work done in the last section, and from the general machinery, they give rise to bounds on the rank of certain ideal class groups. In this section, we give the details of the argument for our special case.

The basic set up is the same: K is an imaginary quadratic field with ring of integers $\mathcal{O}$, and E is an elliptic curve over K with complex multiplication by $\mathcal{O}$. Fix a prime $\mathfrak{p} \nmid 6\mathfrak{f}$ of K and an ideal $\mathfrak{a}$ of K coprime to $6\mathfrak{p}\mathfrak{f}$. Let $\mathcal{P}$ be the set of prime ideals not dividing $6\mathfrak{p}\mathfrak{f}\mathfrak{a}$. Let $\mathcal{R}$ be the set of square-free products of primes in $\mathcal{P}$. Let $K_n = K(E[\mathfrak{p}^n])$, and for each $\mathfrak{r} \in \mathcal{R}$, let $K_n(\mathfrak{r}) = K_n(E[\mathfrak{r}])$. This is a change of notation from earlier, when it represented the ray class group associated to $\mathfrak{r}$.

By corollary 2.5, $G_\mathfrak{r} = \mathrm{Gal}(K_n(\mathfrak{r})/K_n) \cong (\mathcal{O}/\mathfrak{r})^\times$ is cyclic and independent of n. The natural projections $G_\mathfrak{r} \to G_\mathfrak{q}$ for all $\mathfrak{q}|\mathfrak{r}$ together give an isomorphism

$$G_\mathfrak{r} \xrightarrow{\sim} \prod_{\mathfrak{q}|\mathfrak{r}} G_\mathfrak{q}$$

We use this to identify $G_\mathfrak{q}$ with a subgroup of $G_\mathfrak{r}$ if $\mathfrak{q}|\mathfrak{r}$. For each $\mathfrak{q} \in \mathcal{P}$, fix a generator $\sigma_\mathfrak{q}$ of $G_\mathfrak{q}$. The field diagram is shown in figure 1.

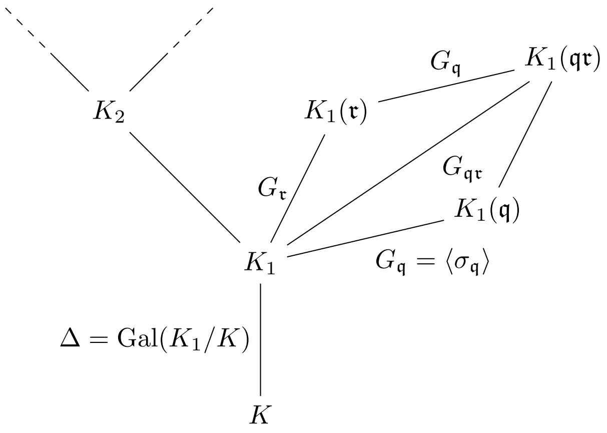
$G_\mathfrak{q}$
$K_1(\mathfrak{q}\mathfrak{r})$
K_2
$K_1(\mathfrak{r})$
$G_{\mathfrak{q}\mathfrak{r}}$
$G_\mathfrak{r}$
$K_1(\mathfrak{q})$
K_1
$G_\mathfrak{q} = \langle\sigma_\mathfrak{q}\rangle$
$\Delta = \mathrm{Gal}(K_1/K)$
K

Figure 1: Various fields

5.1 Euler system

Suppose we are given a p-adic Galois module T, an infinite abelian extension $\mathcal{K}/K$ containing a $\mathbb{Z}_p^d$-extension K_∞/K, and a finite set of primes S containing primes above p and all primes where T is ramified. According to [Rub00], an Euler system is a family $\{\eta_F \in H^1(F,T) : K \subseteq_\mathrm{f} F \subseteq \mathcal{K}\}$ satisfying certain corestriction conditions. We consider an example of this set-up.

Let the Galois module be $\mathcal{O}_\mathfrak{p}$ with G_K acting by the p-adic cyclotomic character, and let $\mathcal{K}$ be generated by $\mathfrak{p}^n\mathfrak{r}$-torsions of E for all $n \geq 1$ and $\mathfrak{r} \in \mathcal{R}$. The cohomology groups can be identified with $\mathfrak{p}$-adic completions of multiplicative groups, and the corestriction maps are norms. Denote $\mathfrak{p}$-adic completion of an abelian group M by $\hat{M}$. Explicitly, the definition is equivalent to

Definition 5.1. An *Euler system* is a family $\{\eta_n(\mathfrak{r}) \in \widehat{K_n(\mathfrak{r})^\times} : n \geq 1, \mathfrak{r} \in \mathcal{R}\}$ such that

(i) $\mathbf{N}_{K_{n+1}(\mathfrak{r})/K_n(\mathfrak{r})}\eta_{n+1}(\mathfrak{r}) = \eta_n(\mathfrak{r})$.

(ii) If $\mathfrak{q} \in \mathcal{P}$ and $\mathfrak{q} \nmid \mathfrak{r}$, then

$$\mathbf{N}_{K_n(\mathfrak{r}\mathfrak{q})/K_n(\mathfrak{r})}\eta_n(\mathfrak{r}\mathfrak{q}) = \eta_n(\mathfrak{r})^{1-\mathrm{Frob}_\mathfrak{q}^{-1}}$$

(iii) $\eta_n(\mathfrak{r}) \in \widehat{\mathcal{O}_{K_n(\mathfrak{r})}^\times}$.

(iv) $\eta_n(\mathfrak{q}\mathfrak{r}) \equiv \eta_n(\mathfrak{r})^{\mathrm{Frob}_\mathfrak{q}^{-1}}$ modulo every prime above $\mathfrak{q}$.

By theorem 4.1, corollary 4.4, and theorem 4.5, the elliptic units $\eta_n(\mathfrak{r}) = \Lambda_{E,\mathfrak{a}}(\xi(\psi(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega))$ form an Euler system, where ξ is an analytic parametrization for E with period lattice $\Omega\mathcal{O}$. The input to $\Lambda_{E,\mathfrak{a}}$ is simply a canonical generator for the ideal $\mathfrak{p}^n\mathfrak{r}$.

Remark. The definition given in [Rub00] does not assume conditions (iii) and (iv), instead deriving (weakened forms of) them from the other axioms. Since their proof in the special case of elliptic units is simpler, we have included them in the axioms for convenience.

Remark. Strictly speaking, this specializes the more general definition only if p splits in K, since otherwise the cohomology group should be the direct sum of two copies of the multiplicative groups. However, the explicit arguments we present here still work when p is inert.

The Euler system constructed is expected to give bounds on the ideal class group of K_n, which we denote by A_n. The general machinery does not actually give anything new in this case, since one can analytically derive precise relations between the size of A_n and the index of certain groups of elliptic units within the global units (see [Rob73]). For our purpose, we need to look at the details of the $\mathrm{Gal}(K_n/K)$-action on A_n, in particular for $n = 1$. We accomplish this by twisting our Euler system above by a character using a process described in general in section II.4 of [Rub00].

Let $F = K_1$. Let $\Delta = \mathrm{Gal}(F/K) \cong (\mathcal{O}/\mathfrak{p})^\times$, which is cyclic of order $\mathbf{N}\mathfrak{p} - 1$. For any $\mathcal{O}[\Delta]$-module M, its $\mathfrak{p}$-adic completion $\hat{M} = \varprojlim M/\mathfrak{p}^n M$ is a $\mathcal{O}_\mathfrak{p}[\Delta]$-module. The algebra $\mathcal{O}_\mathfrak{p}[\Delta]$ is semisimple and decomposes as

$$\mathcal{O}_\mathfrak{p}[\Delta] = \bigoplus_{\chi\in\Xi} R_\chi$$

where Ξ is the set of irreducible $\mathcal{O}_\mathfrak{p}$-representations of Δ, which are equivalent to $k_\mathfrak{p}$-representations by the Teichmüller lifting. Each R_χ is isomorphic to $\mathcal{O}_\mathfrak{p}$. For any $\chi \in \Xi$, we can consider the χ-part of $\hat{M}$, defined by $M^\chi = \hat{M} \otimes_{\mathcal{O}_\mathfrak{p}[\Delta]} R_\chi$. It is canonically both a subgroup and a quotient of $\hat{M}$, and satisfies the property that $\sigma a = \chi(\sigma)a$ for all $a \in \hat{M}$. In particular, this process can be applied to the multiplicative groups $F(\mathfrak{r})^\times$.

Definition 5.2. An *Euler system* with character χ is a family $\{\eta^\chi(\mathfrak{r}) \in \left(F(\mathfrak{r})^\times\right)^\chi : \mathfrak{r} \in \mathcal{R}\}$ such that

(i) If $\mathfrak{q} \in \mathcal{P}$ and $\mathfrak{q} \nmid \mathfrak{r}$, then
$$\mathbf{N}_{F(\mathfrak{r}\mathfrak{q})/F(\mathfrak{r})}\eta^\chi(\mathfrak{r}\mathfrak{q}) = \eta^\chi(\mathfrak{r})^{1-\mathrm{Frob}_\mathfrak{q}^{-1}}$$

(ii) $\eta^\chi(\mathfrak{r}) \in \left(\mathcal{O}_{F(\mathfrak{r})}^\times\right)^\chi$.

(iii) $\eta^\chi(\mathfrak{q}\mathfrak{r}) \equiv \eta^\chi(\mathfrak{r})^{\mathrm{Frob}_\mathfrak{q}^{-1}}$ modulo every prime above $\mathfrak{q}$.

Suppose $\{\eta_n(\mathfrak{r})\}$ is an Euler system in the sense of definition 5.1, define

$$\eta^\chi(\mathfrak{r}) = \left(\frac{1}{\mathbf{N}\mathfrak{p}-1}\sum_{\sigma\in\Delta}\chi^{-1}(\sigma)\sigma\right)\eta_1(\mathfrak{r}) = \prod_{\sigma\in\Delta}\left(\sigma\eta_1(\mathfrak{r})\right)^{\chi^{-1}(\sigma)/(\mathbf{N}\mathfrak{p}-1)} \in \left(\mathcal{O}_{F(\mathfrak{r})}^\times\right)^\chi$$

This is just the image of $\eta_1(\mathfrak{r})$ under the projection to the χ-component, so it is easy to see that $\{\eta^\chi(\mathfrak{r})\}$ is an Euler system with character χ.

Remark. In the twisted system, we have restricted ourselves to only one "layer" of the Euler system for convenience. The definitions for higher layers ($K_n(\mathfrak{r})$ for $n > 1$) appear somewhat un-natural in the explicit language, and we do not need them for this essay. Of course, they are used in deriving Iwasawa-theoretical results, but moreover, when we construct the Kolyvagin system, it will be remarked that one needs the entire Euler system in general.

5.2 Kolyvagin system

The next step in the general machinery is to construct elements in certain cohomology groups associated to K with prescribed behaviours locally. This is made precise using a *finite-to-singular* transfer map. We describe the map explicitly here and define a Kolyvagin system. In the next section, we will construct them from Euler systems.

Let M be a power of p greater than one. In later application, we will take M to be large. Let $\mathcal{P}_M$ be the set of $\mathfrak{q} \in \mathcal{P}$ such that

- $\mathfrak{q}$ splits completely in $F = K_1$.
- $M | \mathbf{N}\mathfrak{q} - 1$.

For completeness, let $\mathcal{P}_1 = \mathcal{P}$. Let $\mathcal{R}_M$ be the set of square-free products of primes in $\mathcal{P}_M$. For any $\mathfrak{q} \in \mathcal{P}_M$, let $I_{\mathfrak{q}}$ be the group of fractional ideals in F which is only divisible by primes above $\mathfrak{q}$. Then $I_{\mathfrak{q}} = \bigoplus_{\mathfrak{Q}|\mathfrak{q}} \mathbb{Z}\mathfrak{Q}$. Given an element $\kappa \in F^\times/(F^\times)^M$, let $[\kappa]_{\mathfrak{q},M}$ denote the projection of the principal ideal $(\tilde{\kappa})$ to $I_{\mathfrak{q}}/MI_{\mathfrak{q}}$ for any lift $\tilde{\kappa}$ of κ to $F^\times$. The desired finite-to-singular map is an isomorphism

$$\varphi_{\mathfrak{q},M} : \mathcal{O}_{F,\mathfrak{q}}^\times/((\mathcal{O}_{F,\mathfrak{q}})^\times)^M \to I_{\mathfrak{q}}/MI_{\mathfrak{q}}$$

where $\mathcal{O}_{F,\mathfrak{q}}$ is the localization of $\mathcal{O}_F$ at the ideal $\mathfrak{q}$. Since $\mathfrak{q}$ splits completely in F,

$$\mathcal{O}_{F,\mathfrak{q}}^\times \cong \prod_{\mathfrak{Q}|\mathfrak{q}} \mathcal{O}_{F,\mathfrak{Q}}^\times$$

so we need to construct an isomorphism

$$\varphi_{\mathfrak{Q},M} : \mathcal{O}_{F,\mathfrak{Q}}^\times/(\mathcal{O}_{F,\mathfrak{Q}}^\times)^M \to \mathbb{Z}/M\mathbb{Z}$$

for each $\mathfrak{Q}|\mathfrak{q}$. Fix one such $\mathfrak{Q}$. In the extension $F(\mathfrak{q})/F$, the prime $\mathfrak{Q}$ is tamely totally ramified. Let $\mathcal{Q}$ be the unique prime in $F(\mathfrak{q})$ above $\mathfrak{Q}$, and let π be a uniformizer for $\mathfrak{Q}$, then we have an injection

$$G_{\mathfrak{q}} \to k_{F,\mathfrak{Q}}^\times,\ \sigma \mapsto \frac{\pi}{\sigma\pi} \pmod{\mathcal{Q}}$$

This is an isomorphism since both groups have the same order. Let $\gamma_{\mathfrak{Q}}$ be the image of $\sigma_{\mathfrak{q}}$ under this map. Given $\alpha \in \mathcal{O}_{F,\mathfrak{Q}}^\times$, suppose $\bar{\alpha} = \gamma_{\mathfrak{Q}}^{\varphi_{\mathfrak{Q}}(\alpha)}$, where the bar denotes reduction modulo $\mathfrak{Q}$. The number $\varphi_{\mathfrak{Q}}(\alpha)$ is well defined in $\mathbb{Z}/(\mathbf{N}\mathfrak{q}-1)\mathbb{Z}$, so by the second condition on $\mathcal{R}_M$, it gives a map to $\mathbb{Z}/M\mathbb{Z}$. It is clear from this description that $\varphi_{\mathfrak{Q}}$ is an isomorphism. We define

$$\varphi_{\mathfrak{q},M}(\alpha) = \sum_{\mathfrak{Q}|\mathfrak{q}} \varphi_{\mathfrak{Q},M}(\alpha)\mathfrak{Q} \in I_{\mathfrak{q}}/MI_{\mathfrak{q}}$$

This is the required finite-to-singular map.

For each $\mathfrak{r} \in \mathcal{R}$, let $\nu(\mathfrak{r})$ be the largest M such that $\mathfrak{r} \in \mathcal{R}_M$. It is decreasing in $\mathfrak{r}$ in the sense that $\nu(\mathfrak{r}) \leq \nu(\mathfrak{s})$ if $\mathfrak{s}|\mathfrak{r}$. In particular, $\nu(\mathcal{O}) = \infty$. In the next definition, interpret $F^\times/(F^\times)^\infty$ to be the $\mathfrak{p}$-adic completion $\widehat{F^\times}$. With this convention, if $m \leq M$, then there exists a natural projection $F^\times/(F^\times)^M \to F^\times/(F^\times)^m$, which will be used without comment.

Definition 5.3. A family $\{\kappa(\mathfrak{r}) \in F^\times/(F^\times)^{\nu(\mathfrak{r})} : \mathfrak{r} \in \mathcal{R}_M\}$ forms a *Kolyvagin system* if

(i) If $\mathfrak{q} \nmid \mathfrak{p}\mathfrak{r}$, then $[\kappa(\mathfrak{r})]_{\mathfrak{q},\nu(\mathfrak{r})} = 0$.

(ii) If $\mathfrak{q}|\mathfrak{r}$, then $[\kappa(\mathfrak{r})]_{\mathfrak{q},\nu(\mathfrak{r})} = \varphi_{\mathfrak{q},\nu(\mathfrak{r})}(\kappa(\mathfrak{r}/\mathfrak{q}))$.

Remark. In [MR04], this is called a weak Kolyvagin system. It imposes a third condition: if $\mathfrak{q}|\mathfrak{r}$, then it requires the restriction of $\kappa(\mathfrak{r})$ at $\mathfrak{q}$ to lie in a *transverse cohomology group*, which in this case says that adjoining an $\nu(\mathfrak{r})$-th root of $\kappa(\mathfrak{r})$ to K is totally ramified at $\mathfrak{q}$. We will not need this condition, but it adds rigidity to the definition, which is used by Mazur and Rubin to classify all Kolyvagin systems in favourable situations.

5.3 The derivative construction

This section performs the technical computations which associates a Kolyvagin system to an Euler system. For convenience, we assume that χ is not the mod-p cyclotomic character, or equivalently $\mu_F^\chi = 0$. For the application to the Coates-Wiles theorem, this is satisfied. When it is used, we will remark on why the condition is assumed and ways to avoid it.

Recall that for each $\mathfrak{q} \in \mathcal{P}$, we chose a canonical generator $\sigma_\mathfrak{q}$ of $G_\mathfrak{q} = \mathrm{Gal}(F(\mathfrak{q})/F)$. Define the following elements of $\mathbb{Z}[G_\mathfrak{q}]$

$$N_\mathfrak{q} = \sum_{\sigma \in G_\mathfrak{q}} \sigma = \sum_{i=0}^{\mathbf{N}\mathfrak{q}-2} \sigma_\mathfrak{q}^i, \quad D_\mathfrak{q} = \sum_{i=0}^{\mathbf{N}\mathfrak{q}-2} i\sigma_\mathfrak{q}^i$$

For any $\mathfrak{r} \in \mathcal{R}$, let

$$N_\mathfrak{r} = \sum_{\sigma \in G_\mathfrak{r}} \sigma = \prod_{\mathfrak{q}|\mathfrak{r}} N_\mathfrak{q}, \quad D_\mathfrak{r} = \prod_{\mathfrak{q}|\mathfrak{r}} D_\mathfrak{q}$$

They satisfy the relation $(\sigma_\mathfrak{q} - 1)D_\mathfrak{q} = \mathbf{N}\mathfrak{q} - 1 - N_\mathfrak{q}$. In this section, we will generally write the group action multiplicatively, so for example $(\sigma_\mathfrak{q} - 1)\alpha = \frac{\sigma_\mathfrak{q}\alpha}{\alpha}$ for $\alpha \in F(\mathfrak{q})^\times$.

Lemma 5.4. *Suppose $\{\eta^\chi(\mathfrak{r})\}$ is an Euler system (with character χ), and $\mathfrak{r} \in \mathcal{R}_M$ for $M > 1$, then the image of $D_\mathfrak{r}\eta^\chi(\mathfrak{r})$ in $F(\mathfrak{r})^\times/(F(\mathfrak{r})^\times)^M$ is fixed by $G_\mathfrak{r}$.*

Proof. We prove by induction on the number of prime factors of $\mathfrak{r}$. Suppose $\mathfrak{r} = \mathfrak{q}\mathfrak{s}$, where $\mathfrak{q} \in \mathcal{P}_M$, then the definition of an Euler system implies that

$$(\sigma_\mathfrak{q} - 1)D_\mathfrak{r}\eta^\chi(\mathfrak{r}) = (\mathbf{N}\mathfrak{q} - 1)D_\mathfrak{s}\eta^\chi(\mathfrak{r})/D_\mathfrak{s}N_\mathfrak{q}\eta^\chi(\mathfrak{r}) = (\mathbf{N}\mathfrak{q} - 1)D_\mathfrak{s}\eta^\chi(\mathfrak{r}) \cdot D_\mathfrak{s}(\mathrm{Frob}_\mathfrak{q}^{-1} - 1)\eta^\chi(\mathfrak{s})$$

Since $\mathfrak{q}$ splits completely in F, its Frobenius is the identity on F, so the second term is in $(F(\mathfrak{s})^\times)^M$ by induction hypothesis. We also have $M|\mathbf{N}\mathfrak{q} - 1$, so $(\sigma_\mathfrak{q} - 1)D_\mathfrak{r}\eta^\chi(\mathfrak{r}) \in (F(\mathfrak{r})^\times)^M$, which proves the lemma because $\sigma_\mathfrak{q}$ as $\mathfrak{q}$ ranges over all prime divisors of $\mathfrak{r}$ generate $G_\mathfrak{r}$. □

The inflation-restriction sequence gives an exact sequence

$$\begin{aligned} 0 \to H^1\big(F(\mathfrak{r})/F, (\mu_M \otimes \chi^{-1})^{F(\mathfrak{r})}\big) \to H^1(F, \mu_M \otimes \chi^{-1}) \to H^1(F(\mathfrak{r}), \mu_M \otimes \chi^{-1})^{G_\mathfrak{r}} \\ \to H^2\big(F(\mathfrak{r})/F, (\mu_M \otimes \chi^{-1})^{K_n(\mathfrak{r})}\big) \end{aligned}$$

Here, $\mu_M \otimes \chi^{-1}$ means $\mu_M \otimes \mathcal{O}_\mathfrak{p}$, where G_K acts on $\mathcal{O}_\mathfrak{p}$ via χ. Thanks to our assumption that χ is not the cyclotomic character, $(\mu_M \otimes \chi^{-1})^{F(\mathfrak{r})} = 0$. Therefore, the restriction in the middle is an isomorphism, which Kummer theory allows us to write explicitly as

$$\big(F^\times/(F^\times)^M\big)^\chi \xrightarrow{\sim} \big(F(\mathfrak{r})^\times/(F(\mathfrak{r})^\times)^M\big)^{\chi, G_\mathfrak{r}}$$

In particular, for each $\mathfrak{r} \in \mathcal{R}_M$, there exists a unique $\kappa_M^\chi(\mathfrak{r}) \in \big(F^\times/(F^\times)^M\big)^\chi$ such that $\kappa_M^\chi(\mathfrak{r}) = D_\mathfrak{r}\eta^\chi(\mathfrak{r})/\beta^M$ for some $\beta \in F(\mathfrak{r})^\times$. These will form a Kolyvagin system. We put χ in the superscript to emphasize that they lie in the χ-component of the multiplicative group. If $\mathfrak{r} = \mathcal{O}$, then $D_\mathfrak{r} = 1$, and $\eta^\chi(\mathfrak{r}) \in (F^\times)^\chi$. Define $\kappa_\infty^\chi(\mathcal{O}) = \eta^\chi(\mathcal{O})$. This is consistent with the above construction.

Remark. If χ is the cyclotomic character, then we can no longer find a unique lift this way. One can get around this problem by introducing a *universal Euler system.* It allows one to pass from the original Galois module to an induced module, which is cohomologically trivial. The details can be found in Chapter IV of [Rub00]. This is another instance where the entire Euler system is required.

Theorem 5.5. *Suppose $\{\eta^\chi(\mathfrak{r})\}$ is an Euler system, then $\{\kappa_{\nu(\mathfrak{r})}^\chi(\mathfrak{r})\}$ is a Kolyvagin system.*

Proof. If $\mathfrak{q} \nmid \mathfrak{p}\mathfrak{r}$, then $\kappa^{\chi}_{\nu(\mathfrak{r})}(\mathfrak{r})$ is a global unit times an M-th power in $F(\mathfrak{r})^{\times}$. The extension $F(\mathfrak{r})/F$ is unramified at $\mathfrak{q}$ since $E[\mathfrak{p}] \subseteq F$ (corollary 2.5), so $\nu(\mathfrak{r}) | v_{\mathfrak{Q}}(\kappa^{\chi}_{\nu(\mathfrak{r})}(\mathfrak{r}))$ for all $\mathfrak{Q}$ in F lying above $\mathfrak{q}$.

Now suppose $\mathfrak{r} = \mathfrak{q}\mathfrak{s}$, where $\mathfrak{q}$ is prime. Let $M = \nu(\mathfrak{r})$, then $\mathfrak{r}, \mathfrak{s}, \mathfrak{q} \in \mathcal{R}_M$. Choose $\beta_{\mathfrak{r}} \in \left(F(\mathfrak{r})^{\times}\right)^{\chi}$ and $\beta_{\mathfrak{s}} \in \left(F(\mathfrak{s})^{\times}\right)^{\chi}$ such that

$$\kappa^{\chi}_{\nu(\mathfrak{r})}(\mathfrak{r}) = D_{\mathfrak{r}}\eta^{\chi}(\mathfrak{r})/\beta_{\mathfrak{r}}^{M}, \quad \kappa^{\chi}_{\nu(\mathfrak{s})}(\mathfrak{s}) = D_{\mathfrak{s}}\eta^{\chi}(\mathfrak{s})/\beta_{\mathfrak{s}}^{M}$$

We will drop the subscripts on κ^{χ} in the rest of the proof.

Fix a prime $\mathcal{Q}$ above $\mathfrak{q}$ in $F(\mathfrak{r})$. The identification of $G_{\mathfrak{q}}$ with a subgroup of $G_{\mathfrak{r}}$ makes $\sigma_{\mathfrak{q}}$ an element of the inertia group of $\mathcal{Q}$. Let $\pi_{\mathcal{Q}}$ be a uniformizer, and let $\gamma_{\mathcal{Q}}$ be the residue of $(1-\sigma_{\mathfrak{q}})\pi_{\mathcal{Q}}$. Let $\mathfrak{Q} = \mathcal{Q} \cap F$. The natural embedding $k^{\times}_{F,\mathfrak{Q}} \to k^{\times}_{F(\mathfrak{r}),\mathcal{Q}}$ sends $\gamma_{\mathfrak{Q}}$ defined in the previous subsection to $\gamma_{\mathcal{Q}}$. Since $\eta^{\chi}(\mathfrak{r})$ is a global unit and the ramification index of $\mathcal{Q}$ in $F(\mathfrak{r})/F$ is $\mathbf{N}\mathfrak{q} - 1$, we have

$$v_{\mathfrak{Q}}(\kappa^{\chi}(\mathfrak{r})) \equiv -\frac{M}{\mathbf{N}\mathfrak{q} - 1} c_{\mathfrak{Q}} \pmod{M}$$

where $c_{\mathfrak{Q}} = v_{\mathcal{Q}}(\beta_{\mathfrak{r}})$. The element $\sigma_{\mathfrak{q}}$ is in the inertia group, so $(1 - \sigma_{\mathfrak{q}})\beta_{\mathfrak{r}} \equiv \gamma_{\mathcal{Q}}^{c_{\mathfrak{Q}}} \pmod{\mathcal{Q}}$. Therefore, comparing with the definition of $\varphi_{\mathfrak{q},M}$, we need to show that

$$(\sigma_{\mathfrak{q}} - 1)\beta_{\mathfrak{r}} \equiv \left(\kappa^{\chi}(\mathfrak{s})\right)^{(\mathbf{N}\mathfrak{q}-1)/M} \pmod{\mathcal{Q}}$$

Our earlier calculation gives

$$\begin{aligned}
\beta_{\mathfrak{r}}^{(\sigma_{\mathfrak{q}}-1)M} &= (\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{r}}\eta^{\chi}(\mathfrak{r}) \\
&= (\mathbf{N}\mathfrak{q} - 1)D_{\mathfrak{s}}\eta^{\chi}(\mathfrak{r}) \cdot D_{\mathfrak{s}}(\mathrm{Frob}_{\mathfrak{q}}^{-1} - 1)\eta^{\chi}(\mathfrak{s}) \\
&= \left(\mathrm{Frob}_{\mathfrak{q}}^{-1} - 1\right)\left(\kappa^{\chi}(\mathfrak{s})\beta_{\mathfrak{s}}^{M}\right) \cdot (\mathbf{N}\mathfrak{q} - 1)D_{\mathfrak{s}}\eta^{\chi}(\mathfrak{r}) \\
&= \left(\mathrm{Frob}_{\mathfrak{q}}^{-1} - 1\right)\beta_{\mathfrak{s}}^{M} \cdot (\mathbf{N}\mathfrak{q} - 1)D_{\mathfrak{s}}\eta^{\chi}(\mathfrak{r})
\end{aligned}$$

where we have used again the fact that $\mathrm{Frob}_{\mathfrak{q}}$ acts trivially on F. Take M-th root to get

$$(\sigma_{\mathfrak{q}} - 1)\beta_{\mathfrak{r}} = (\mathrm{Frob}_{\mathfrak{q}}^{-1} - 1)\beta_{\mathfrak{s}} \cdot \frac{\mathbf{N}\mathfrak{q} - 1}{M} D_{\mathfrak{s}}\eta^{\chi}(\mathfrak{r})$$

A priori, there could be a root of unity, but by the observation made during the construction of $\kappa^{\chi}_{M}(\mathfrak{r})$, there is no M-th root of unity in $\left(F(\mathfrak{r})^{\times}\right)^{\chi}$. Both sides lie in the group, so the equality holds.

Finally, apply the congruence relation to get that

$$\begin{aligned}
(\sigma_{\mathfrak{q}} - 1)\beta_{\mathfrak{r}} &\equiv (\mathrm{Frob}_{\mathfrak{q}}^{-1} - 1)\beta_{\mathfrak{s}} \cdot \frac{\mathbf{N}\mathfrak{q} - 1}{M} D_{\mathfrak{s}}\, \mathrm{Frob}_{\mathfrak{q}}^{-1}\, \eta^{\chi}(\mathfrak{s}) \\
&\equiv \mathrm{Frob}_{\mathfrak{q}}^{-1} \left(\beta_{\mathfrak{s}}^{1-\mathbf{N}\mathfrak{q}} \cdot \left(\kappa^{\chi}(\mathfrak{s})\beta_{\mathfrak{s}}^{M}\right)^{(\mathbf{N}\mathfrak{q}-1)/M}\right) \\
&\equiv \mathrm{Frob}_{\mathfrak{q}}^{-1} \left(\kappa^{\chi}(\mathfrak{s})\right)^{(\mathbf{N}\mathfrak{q}-1)/M} \\
&= \left(\kappa^{\chi}(\mathfrak{s})\right)^{(\mathbf{N}\mathfrak{q}-1)/M} \pmod{\mathcal{Q}}
\end{aligned}$$

□

5.4 Bounding the ideal class group

In the general framework, elements in a Kolyvagin system produce relations in the dual Selmer group via local duality. In our case, this is simply saying that elements of $F^{\times}$ give relations in the ideal class group. The main theorem is

Theorem 5.6. *Let $\chi : \Delta \to \mathcal{O}_{\mathfrak{p}}^{\times}$ be a non-trivial character. Let $\{\kappa^{\chi}(\mathfrak{r})\}$ be a Kolyvagin system for F/K. Let $\mathcal{C} \subseteq \mathcal{O}_F^{\times}$ be the subgroup generated by the roots of unities and $\kappa^{\chi}(1)$. Then*

$$|A^{\chi}| \leq |(\mathcal{O}_F^{\times}/\mathcal{C})^{\chi}|$$

Following [Rub00], there are two main steps to the proof, presented here as two lemmas. The first is to produce a set of useful primes. The second shows that the elements of the Kolyvagin systems at those primes contribute to enough relations in the ideal class group.

We first set up some notations. Since χ is not trivial, by the Dirichlet unit theorem, $(\mathcal{O}_F^\times/\mu_F)^\chi$ is free of rank one over R_χ, so $(\mathcal{O}_F^\times/\mathcal{C})^\chi \cong R_\chi/cR\chi$ for some $c \in R_\chi$. Let m be the exponent of A^χ. Choose M to be a sufficiently large power of p such that $mc|M$. Let $L = F(\mu_M)$.

Lemma 5.7. *Let $\{\alpha_1, \cdots, \alpha_k\}$ be the elements of* $\mathrm{Hom}(A^\chi, \mathbb{Z}/M\mathbb{Z})$*, treated as elements of* $\mathrm{Hom}(G_F, \mathbb{Z}/M\mathbb{Z})$ *via the global Artin map. There exists primes $\mathfrak{q}_1, \cdots, \mathfrak{q}_k \in \mathcal{R}_M$ such that for every i, $1 \leq i \leq k$, we have*

(i) $\mathrm{ord}\left(\kappa^\chi(\mathfrak{r}_{i-1}), \mathcal{O}_{F,\mathfrak{q}_i}^\times/(\mathcal{O}_{F,\mathfrak{q}_i}^\times)^M\right) \geq \mathrm{ord}\left(\kappa^\chi(\mathfrak{r}_{i-1}), L^\times/(L^\times)^M\right)$.

(ii) $\mathrm{ord}(\alpha_i(\mathfrak{q}_i), \mathbb{Z}/M\mathbb{Z}) \geq \mathrm{ord}(\alpha_i, \mathrm{Hom}(G_L, \mathbb{Z}/M\mathbb{Z}))$.

where $\mathfrak{r}_i = \prod_{j \leq i} \mathfrak{q}_j$.

Proof. We inductively choose $\mathfrak{q}_i \in \mathcal{R}_M$ satisfying the two properties. Suppose $\mathfrak{q}_1, \cdots, \mathfrak{q}_{i-1}$ have been constructed. Let $\rho \in H^1(L, \mu_M) \cong \mathrm{Hom}(G_L, \mu_M)$ be the image of $\kappa^\chi(\mathfrak{r}_{i-1})$ under the Kummer map for L. Consider the following subgroups of G_L:

$$B_\kappa = \{\gamma \in G_L : \mathrm{ord}(\rho(\gamma), \mu_M) < \mathrm{ord}(\rho, \mathrm{Hom}(G_L, \mu_M))\}$$
$$B_\alpha = \{\gamma \in G_L : \mathrm{ord}(\alpha_i(\gamma), \mathbb{Z}/M\mathbb{Z}) < \mathrm{ord}(\alpha_i, \mathrm{Hom}(G_L, \mathbb{Z}/M\mathbb{Z})\}$$

These are both proper subgroups of G_L, so there exists $\gamma \in G_L \backslash (B_\kappa \cup B_\alpha)$. Let L' be an extension of L such that ρ and α_i are trivial when restricted to L'. By the Chebotarev density theorem, there exists a prime $\mathfrak{q}_i$ in K not dividing $6\mathfrak{p}\mathfrak{f}\mathfrak{a}\mathfrak{r}_{i-1}$ whose Frobenius in L'/K is γ. This implies that it splits completely in L/K, so $\mathfrak{q}_i \in \mathcal{R}_M$.

The Kummer map is injective, so $\mathrm{ord}\left(\kappa^\chi(\mathfrak{r}_{i-1}), L^\times/(L^\times)^M\right) = \mathrm{ord}(\rho, \mathrm{Hom}(G_L, \mu_M))$. We also have an isomorphism

$$\mathcal{O}_{F,\mathfrak{q}_i}^\times/(\mathcal{O}_{F,\mathfrak{q}_i}^\times)^M = \bigoplus_{\mathfrak{Q}|\mathfrak{q}_i} \mathcal{O}_{F,\mathfrak{Q}}^\times/(\mathcal{O}_{F,\mathfrak{Q}}^\times)^M \xrightarrow{\sim} \bigoplus_{\mathfrak{Q}|\mathfrak{q}_i} H^1_{\mathrm{ur}}(F_\mathfrak{Q}, \mu_M) \xrightarrow{\sim} \bigoplus_{\mathfrak{Q}|\mathfrak{q}_i} \mu_M$$

where the first arrow is the Kummer map, and the second arrow is evaluation as 1-cocycles at the Frobenius of $\mathfrak{q}_i$. The group Δ acts on the left hand side naturally, and on the right hand side by permuting its factors. The isomorphism is Δ-equivariant, so the χ-component of $\mathcal{O}_{F,\mathfrak{q}_i}/(\mathcal{O}_{F,\mathfrak{q}_i})^M$ is isomorphic to μ_M by projecting to a factor. Under these identifications, the image of $\kappa^\chi(\mathfrak{r}_{i-1})$ is $\rho(\gamma)$, up to an automorphism of μ_M which depends on the choice of a place above $\mathfrak{q}$ in $\bar{K}$. This proves (i). Condition (ii) is immediate since $\mathfrak{q}_i$ maps to $\mathrm{Frob}_{\mathfrak{q}_i} = \gamma$ in $G_K/\ker(\alpha_i)$ under the Artin map. □

Lemma 5.8. *Let $\{\mathfrak{q}_1, \cdots, \mathfrak{q}_k\}$ be the primes constructed in lemma 5.7. Let v be the valuation map*

$$\mathcal{O}_F[\mathfrak{q}_1^{-1}, \cdots, \mathfrak{q}_k^{-1}, \mathfrak{p}^{-1}]^\times \otimes \mathbb{Z}/m\mathbb{Z} \to \bigoplus_{i=1}^k I_{\mathfrak{q}_i}/mI_{\mathfrak{q}_i}$$

Then the χ-component of its cokernel satisfies

$$|\operatorname{coker}(v)^\chi| \leq |(\mathcal{O}_F^\times/\mathcal{C})^\chi|$$

Proof. The map $H^1(F, \mu_M) \to H^1(L, \mu_M)$ is injective. Indeed, its kernel is $H^1(L/F, \mu_M)$, which is easily shown to be 0 using the formula for the cohomology of cyclic groups. For each i, let $\mathfrak{r}_i = \prod_{j \leq i} \mathfrak{q}_j$, and let

$$\delta_i = \mathrm{ord}\left(\kappa^\chi(\mathfrak{r}_i), L^\times/(L^\times)^M\right) = \mathrm{ord}\left(\kappa^\chi(\mathfrak{r}_i), F^\times/(F^\times)^M\right)$$

Then by construction,

$$\delta_i \geq \mathrm{ord}([\kappa^\chi(\mathfrak{r}_i)]_\mathfrak{q}, I_\mathfrak{q}/MI_\mathfrak{q}) = \mathrm{ord}\left(\kappa^\chi(\mathfrak{r}_{i-1}), \mathcal{O}_{F,\mathfrak{q}_i}^\times/(\mathcal{O}_{F,\mathfrak{q}_i}^\times)^M\right) = \delta_{i-1}$$

where for the first equality, we used the definition of a Kolyvagin system, and for the second equality, observe that there is an isomorphism

$$\mathcal{O}_{F,\mathfrak{q}_i}^\times \otimes \mathbb{Z}/M\mathbb{Z} \xrightarrow{\sim} (\mathcal{O}_F/\mathfrak{q}_i\mathcal{O}_F)^\times \otimes \mathbb{Z}/M\mathbb{Z}$$

by Hensel's lemma. The choice of M to be sufficiently large and the definition of $\mathcal{C}$ gives an exact sequence

$$0 \to R_\chi \kappa^\chi(1)/\mu_F \cap R_\chi \kappa^\chi(1) \to R_\chi/MR_\chi \to (\mathcal{O}_F^\times/\mathcal{C})^\chi \to 0$$

Therefore,

$$\delta_0 = \mathrm{ord}\left(\kappa^\chi(1), F^\times/(F^\times)^M\right) = \mathrm{ord}\left(\kappa^\chi(1), \mathcal{O}_F^\times/(\mathcal{O}_F^\times)^M\right) \geq M/|(\mathcal{O}_F^\times/\mathcal{C})^\chi| \geq m$$

For each i, choose $\bar{\kappa}_i \in \mathcal{O}_F[\mathfrak{r}_i^{-1}, \mathfrak{p}^{-1}]^\times$ such that $\bar{\kappa}_i^M = \kappa^\chi(\mathfrak{r}_i)^{\delta_i}$. Let $A^{(i)}$ be the subgroup of $F^\times/(F^\times)^m$ generated by $\{\bar{\kappa}_1, \cdots, \bar{\kappa}_i\}$. Then

$$\left|v(A^{(i)})/v(A^{(i-1)})\right| \geq \mathrm{ord}([\bar{\kappa}_i]_{\mathfrak{q}_i}, I_{\mathfrak{q}_i}/mI_{\mathfrak{q}_i}) \geq \mathrm{ord}([\kappa^\chi(\mathfrak{r}_i)], I_{\mathfrak{q}_i}/MI_{\mathfrak{q}_i})m/\delta_i \geq \delta_{i-1}m/\delta_i$$

Multiply these inequalities together for all i gives

$$|\operatorname{Im}(v)| \geq m^k \delta_0/\delta_k \geq m^k/|(\mathcal{O}_F^\times/\mathcal{C})^\chi|$$

where we have used the trivial bound $\delta_k \leq M$. The codomain of v has size m^k, so the result follows. □

Proof of Theorem 5.6. It remains to show that $\{\mathfrak{q}_1, \cdots, \mathfrak{q}_k\}$ constructed above generate A^χ, since then coker(v) surjects onto A^χ. Suppose for contradiction that there exists a j such that $\alpha_j : A^\chi \to \mathbb{Z}/M\mathbb{Z}$ vanishes on all $\mathfrak{q}_i$. In particular, it must restrict to 0 on G_L by condition (ii) of lemma 5.7, so α_j belongs to Hom(Gal$(L/F), \mathbb{Z}/M\mathbb{Z})$. The extension L/F is totally ramified at primes above p, so $\alpha_j = 0$. □

Combining the results from this section, we get

Corollary 5.9. *Let $\chi : \Delta \to \mathcal{O}_\mathfrak{p}^\times$ be a character which is neither trivial nor the cyclotomic character. Let $\mathfrak{a}$ be an ideal coprime to $6\mathfrak{p}\mathfrak{f}$, and let $\eta^{(\mathfrak{a})} = \Lambda_{E,\mathfrak{a}}(\xi(\psi(\mathfrak{p})^{-1}\Omega))$ be an elliptic unit associated to $\mathfrak{a}$. Then*

$$|A^\chi| \leq |(\mathcal{O}_F^\times/\mathcal{C}_\mathfrak{a})^\chi|$$

where $\mathcal{C}_\mathfrak{a}$ is the $\mathbb{Z}[\Delta]$-submodule of $\mathcal{O}_F^\times$ generated by μ_F and $\eta^{(\mathfrak{a})}$.

Remark. The corollary holds for all χ. If χ is trivial, then the inequality holds trivially since A^χ is the ideal class group of K. If χ is cyclotomic, then the more robust construction of Kolyvagin systems we referenced to earlier proves the inequality.

6 The Coates-Wiles Theorem

In this section, we prove the main theorem:

Theorem 6.1 (Coates-Wiles)**.** *Let K be an imaginary quadratic field. Let E be an elliptic curve over K with complex multiplication. If $L(E, 1) \neq 0$, then $E(K)$ is finite.*

First observe that if E has complex multiplication by the order $\mathbb{Z} + c\mathcal{O}$ for some $c > 1$, then there exists an isogeny $E \to E'$ with kernel $E[c\mathcal{O}]$. The curve E' has complex multiplication by $\mathcal{O}$. Since isogenies do not change rank $E(K)$ or $L(E, s)$, we may assume that we are in the usual case where E has complex multiplicaiton by the maximal order $\mathcal{O}$.

Recall some notations from the previous sections. Let $\mathfrak{p}$ be a prime of K not dividing $\mathfrak{f}$ with residue characteristics $p > 7$. Let $F = K(E[\mathfrak{p}])$, then F is totally ramified above $\mathfrak{p}$ with Galois group $\Delta \cong (\mathcal{O}/\mathfrak{p})^\times$. Let $\chi_E : G_K \to k_\mathfrak{p}^\times$ be the character of G_K acting on $E[\mathfrak{p}]$. Let $\mathfrak{P}$ be the unique prime of F above $\mathfrak{p}$, and A be the ideal class group of F. On the analytic side, let $\xi : \mathbb{C}/L \to E(\mathbb{C})$ be an analytic parametrization with period lattice $L = \Omega\mathcal{O}$, and let $\eta^{(\mathfrak{a})} = \Lambda_{E,\mathfrak{a}}(\xi(\psi(\mathfrak{p})^{-1}\Omega))$ be the elliptic unit defined in section 5. It is a global unit in F.

Lemma 6.2. *The character χ_E is neither trivial nor cyclotomic.*

Proof. By the construction of ψ, $\chi_E([x, K]) = x^{-1}$ for $x \in \mathcal{O}_{\mathfrak{p}}^\times$ since $\mathfrak{p} \nmid \mathfrak{f}$. Therefore, $\chi_E \neq 1$. The Weil pairing $E[p] \times E[p] \to \mu_p$ is non-degenerate and Galois-equivariant (proposition III.8.1 of [Sil09]). If χ_E is cyclotomic, then $\sigma Q - Q \in E[\mathfrak{p}]^\perp$ for all $Q \in E[p]$, $\sigma \in G_K$, so $E[p]^{G_K} \neq 0$. We have shown above that $E[\mathfrak{p}]^{G_K} = 0$, so this can only happen if p splits in K and $E[\bar{\mathfrak{p}}] \subseteq E(K)$. For $x \in \mathcal{O}_{\bar{\mathfrak{p}}}^\times$, $[x, K]$ acts on $E[\bar{\mathfrak{p}}]$ by $\psi(x)x^{-1}$, where $\psi(x) \in \mathcal{O}^\times$ (corollary 2.5). We therefore need $\mathcal{O}^\times \to (\mathcal{O}/\bar{\mathfrak{p}})^\times$ to be surjective, which is impossible since $\bar{\mathfrak{p}}$ has residue characteristics at least 7. □

Lemma 6.3. *There exists $\mathfrak{a}$ coprime to $6\mathfrak{p}\mathfrak{f}$ such that $\mathbf{N}\mathfrak{a} \not\equiv \psi(\mathfrak{a}) \pmod{\mathfrak{p}}$.*

Proof. By corollary 2.5, $\psi(\mathfrak{a})$ generate $\mathfrak{a}$, so $\mathbf{N}\mathfrak{a} = \psi(\mathfrak{a})\bar{\psi}(\mathfrak{a})$, so we just need $\bar{\psi}(\mathfrak{a}) \not\equiv 1 \pmod{\mathfrak{p}}$, or equivalently $\psi(\mathfrak{a}) \not\equiv 1 \pmod{\bar{\mathfrak{p}}}$. For each prime $\mathfrak{q}$ not dividing $6p\mathfrak{f}$, $[\mathfrak{q}, K]$ acts on $E[\bar{\mathfrak{p}}]$ by $\psi(\mathfrak{q})$. By the Chebotarev density theorem applied to $K(E[\bar{\mathfrak{p}}])/K$, we are done if $E[\bar{\mathfrak{p}}] \not\subseteq E(K)$, which was shown in the previous lemma. □

Remark. In the previous two lemmas, the condition $p > 7$ was necessary. Explicitly, consider the following elliptic curve defined over $\mathbb{Q}(\omega)$, where $\omega = \frac{1+\sqrt{-3}}{2}$

$$E : y^2 + (\omega + 1)y = x^3 - (\omega + 1)x^2 + \omega x - \omega$$

It has complex multiplication by $\mathbb{Z}[\omega]$ defined by $\omega(x, y) = (-\omega(x - 1), -y - (\omega + 1))$. Let $\mathfrak{p} = (3\omega - 2)$, then the conductor of the curve is $\bar{\mathfrak{p}}^2$. The point $(0, -1)$ generates the torsion subgroup $E[\bar{\mathfrak{p}}]$. One can check that the two results above fail for $\mathfrak{p}$. However, the condition can be dropped if E is defined over $\mathbb{Q}$ since then $\mathfrak{p} \nmid \mathfrak{f}$ implies $\bar{\mathfrak{p}} \nmid \mathfrak{f}$.

Theorem 6.4. *If $\mathfrak{p} \nmid L(\bar{\psi}, 1)/\Omega$, then $A^{\chi_E} = 0$.*

Proof. Choose an ideal $\mathfrak{a}$ as in lemma 6.3 and consider its associated elliptic unit η. By lemma 6.2, we may apply corollary 5.9. Since $(\mathcal{O}_F^\times/\mu_F)^{\chi_E}$ is free of rank one over R_χ, the theorem reduces to showing

$$\eta^{\chi_E} \notin \mu_F^{\chi_E}\big((\mathcal{O}_F^\times)^{\chi_E}\big)^p$$

Let $P = \xi(\psi(\mathfrak{p})^{-1}\Omega) \in E[\mathfrak{p}]$, and let $z = -x(P)/y(P) \in \mathfrak{P}$ be the corresponding point in $\hat{E}[\mathfrak{p}]$. By corollary 3.16, we have an expansion

$$\eta \equiv \Lambda_{\mathfrak{p},\mathfrak{a}}(0)\big(1 + 12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a}))(L(\bar{\psi}, 1)/\Omega)z\big) \pmod{\mathfrak{P}^2}$$

The proof of lemma 2.8 shows that $v_{\mathfrak{P}}(z) = 1$. Our choice of $\mathfrak{p}$ and $\mathfrak{a}$ implies that $12f(\mathbf{N}\mathfrak{a}-\psi(\mathfrak{a}))(L(\bar{\psi}, 1)/\Omega)$ is a $\mathfrak{p}$-adic unit. By theorem 3.15, $\Lambda_{\mathfrak{p},\mathfrak{a}}(0) \in \mathcal{O}_{\mathfrak{p}}^\times$. Let S be the Teichmüller representatives of $k_{\mathfrak{P}}$, which consists of the roots of unities in $\mathcal{O}_{F,\mathfrak{P}}$ and 0. Since $F_{\mathfrak{P}}/K_{\mathfrak{p}}$ is totally ramified, $S \subseteq \mathcal{O}_{\mathfrak{p}}$. The above discussion shows that the $\mathfrak{P}$-adic expansion of η with respect to S has the form $a_0\big(1+a_1z+O(z^2)\big)$, with $a_0, a_1 \neq 0$. We now compute

$$\begin{aligned}\eta^{\chi_E} &= \left(\frac{1}{\mathbf{N}\mathfrak{p} - 1}\sum_{\sigma\in\Delta}\chi_E^{-1}(\sigma)\sigma\right)a_0\big(1 + a_1z + O(z^2)\big)\\ &= a_0\prod_{\sigma\in\Delta}\left(1 + \frac{1}{\mathbf{N}\mathfrak{p} - 1}\sum_{\sigma\in\Delta}\chi_E^{-1}(\sigma)\sigma(a_1z) + O(z^2)\right)\\ &= a_0\left(1 + a_1 \cdot \frac{1}{\mathbf{N}\mathfrak{p} - 1}\sum_{\sigma\in\Delta}(\chi_E^{-1}i)(\sigma)z + O(z^2)\right)\end{aligned}$$

where $i : \Delta \to \mathcal{O}_{\mathfrak{P}}^\times$ is defined by $\sigma z = i(\sigma)z$. By definition, $\sigma P = \chi_E(\sigma)P$, so $i = \chi_E$. Therefore, the expansion of η^{χ_E} is still $a_0\big(1 + a_1z + O(z^2)\big)$.

Again by lemma 6.2, $\mu_F^{\chi_E} = 0$, so the theorem follows from the stronger claim that $\eta^{\chi_E} \notin (\mathcal{O}_{F,\mathfrak{P}}^\times)^p$. Let $x = x_0 + x_1z + O(z^2) \in \mathcal{O}_{F,\mathfrak{P}}^\times$ with $x_0, x_1 \in S$, then $x^p = x_0^p + O(z^p)$ since $v_{\mathfrak{P}}(p) = \mathbf{N}\mathfrak{p} - 1 \geq p - 1$. Since $\mathfrak{P}$-adic expansion with respect to S is unique, this cannot equal to η^{χ_E}, as required. □

Proof of the Coates-Wiles Theorem. By theorem 2.6, $L(E,1) = L(\psi,1)L(\bar{\psi},1)$. If $L(E,1) \neq 0$, then $L(\bar{\psi},1) \neq 0$, so we can choose a prime $\mathfrak{p}$ in K not dividing $\mathfrak{f}(L(\bar{\psi},1)/\Omega)$ with residue characteristic $p > 7$. We will show that $S_{\psi(\mathfrak{p})}(E) = 0$. By theorem 2.13, we need $A^{\chi_E} = 0$ and $\delta_1(\mathcal{O}_F^\times) \neq 0$. The first condition is guaranteed by the previous theorem.

For the second condition, the more informative way of proving it is to apply Wiles' explicit reciprocity law (theorem 2.10). It shows that

$$\delta_1(\eta) = -12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a}))(L(\bar{\psi},1)/\Omega)P$$

Since we did not prove the reciprocity law, we will follow [Rub99] and show that $(\mathcal{O}_F^\times)^{\chi_E} \to (\mathcal{O}_{F,\mathfrak{P}}^\times)^{\chi_E}$ is surjective for a set of $\mathfrak{p}$ with positive density, which suffices for the theorem by lemma 2.9.

If p splits, then the absolute ramification index of $\mathfrak{P}$ is $\mathbf{N}\mathfrak{p} - 1 = p-1$, so the logarithm and exponential maps define isomorphisms $1 + \mathfrak{P}^2\mathcal{O}_{F,\mathfrak{P}} \cong \mathfrak{P}^2\mathcal{O}_{F,\mathfrak{P}}$. Therefore,

$$\mathcal{O}_{F,\mathfrak{P}}^\times \otimes \mathbb{Q}_p \cong (1 + \mathfrak{P}^2\mathcal{O}_{F,\mathfrak{P}}) \otimes \mathbb{Q}_p \cong \mathcal{O}_{F,\mathfrak{P}} \otimes \mathbb{Q}_p \cong F_{\mathfrak{P}} \cong K_{\mathfrak{p}}[\Delta]$$

All of the isomorphisms above are Δ-equivariant, with the existence of the final one guaranteed by the normal basis theorem. Taking the χ_E component implies $\left(\mathcal{O}_{F,\mathfrak{P}}^\times\right)^{\chi_E} \otimes \mathbb{Q}_p \cong K_{\mathfrak{p}}$. This shows that $\left(\mathcal{O}_{F,\mathfrak{P}}^\times\right)^{\chi_E} \cong \mathcal{O}_{\mathfrak{p}}$ is either isomorphic to $\mathcal{O}_{\mathfrak{p}}$ or $\mathcal{O}_{\mathfrak{p}} \oplus \mathbb{Z}/p\mathbb{Z}$, the latter case occurring if and only if $F_{\mathfrak{P}}$ contains the p-th roots of unity. In the first case, we are done since our earlier work shows that $\left(\mathcal{O}_F^\times\right)^{\chi_E} \not\subseteq \left((\mathcal{O}_{F,\mathfrak{P}}^\times)^{\chi_E}\right)^p$. We therefore need to choose p to rule out the second case.

If $F_{\mathfrak{P}}$ contains μ_p, then $F_{\mathfrak{P}} = K_{\mathfrak{p}}(\mu_p)$ since both are totally ramified extensions of degree $p-1$. In particular, p is a norm in $F_{\mathfrak{P}}/K_{\mathfrak{p}}$, so $[p, F_{\mathfrak{P}}/K_{\mathfrak{p}}] = \mathrm{Id}_{F_{\mathfrak{P}}}$. Globally, $[\psi(\mathfrak{p}), F/K]$ acts by $\psi(\mathfrak{p})\psi(\mathfrak{p})^{-1} = 1$ on $E[\mathfrak{p}^\infty]$, so $[\psi(\mathfrak{p}), F_{\mathfrak{P}}/K_{\mathfrak{p}}] = \mathrm{Id}_{F_{\mathfrak{P}}}$. Therefore, $p/\psi(\mathfrak{p})$ is a norm from $F_{\mathfrak{P}}$. It is a unit, so it must be in $1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ (alternatively, one may derive this using Lubin-Tate theory). But $p/\psi(\mathfrak{p}) = \bar{\psi}(\mathfrak{p})$, so $\mathrm{Tr}_{K/\mathbb{Q}}\,\psi(\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}}$. For $p > 5$, which is assumed, this implies $\mathrm{Tr}_{K/\mathbb{Q}}\,\psi(\mathfrak{p}) = 1$ by Hasse's bound. If this happens, we call p *anomalous*. We will show that the set of primes which splits minus the set of anomalous primes has positive density.

Let $\mathcal{O} = \mathbb{Z}[\tau]$. Suppose $p = \mathfrak{p}\bar{\mathfrak{p}}$ splits and is anomalous. Let $\psi(\mathfrak{p}) = a + b\tau$ with $a, b \in \mathbb{Z}$, then $\mathrm{Tr}_{K/\mathbb{Q}}\,\psi(\mathfrak{p}) = 2a + b\,\mathrm{Tr}_{K/\mathbb{Q}}\,\tau = 1$. If 2 ramifies in K, then τ can be taken to be $\sqrt{-D}$, with trace zero, so $2a = 1$, which is a contradiction. Otherwise, τ may be chosen to have trace one, so $2a + b = 1$. We also have $p = (a + b\tau)(a + b\bar{\tau})$, which implies

$$4p = 1 + b^2(\mathbf{N}_{K/\mathbb{Q}}\tau - 1)$$

Take remainder modulo a large prime q coprime to the discriminant of K. The equation shows that for at least half of the residue classes modulo q, no anomalous primes exist in them. Therefore, by Dirichlet's theorem on primes in arithmetic progression, there exists infinitely many primes which split but are not anomalous. Choosing any one of them finishes the proof of the theorem. □

Corollary 6.5. *If E is an elliptic curve over $\mathbb{Q}$ with complex multiplication (over $\mathbb{C}$), and $L(E,1) \neq 0$, then $E(\mathbb{Q})$ is finite.*

Proof. Let ψ be the Grössencharakter associated to $E_{/K}$, where K is an imaginary quadratic field over which E has complex multiplication. One can check from the definition that $L(\psi,s) = L(\bar{\psi},s)$, and that $L(E/\mathbb{Q},s) = L(\psi,s)$, up to a finite number of Euler factors which do not vanish at 1. For details of these, see section 10.4 of [Lan87]. The result now follows from the Coates-Wiles theorem. □

7 Explicit Computations

In [Rub99], Rubin ended with an explicit computation with the curve $y^2 = x^3 - x$ defined over $\mathbb{Q}(i)$. We will perform a similar computation with a curve with j-invariant 0. This isomorphism class in particular includes the Fermat curve $x^3 + y^3 = 1$ and was also extensively studied.

Let $\omega = \frac{1+\sqrt{-3}}{2}$, and let $K = \mathbb{Q}(\omega)$. Let $\mathfrak{p}_3 = (1+\omega)$ be the unique prime above 3 in K. We consider the elliptic curve

$$E : y^2 + y = x^3$$

defined over K. It has complex multiplication by $\mathcal{O}_K = \mathbb{Z}[\omega]$ given by $\omega(x, y) = (-\omega x, -y-1)$. The goal of this section is to explicitly compute the various objects we looked at in this essay, and to verify some of the results we proved.

The curve is labelled 81.0.9-CMa1 in the LMFDB. From it, we get $j(E) = 0$, $\Delta(E) = -27$, $\mathfrak{f}_E = \mathfrak{p}_3^4$, and $E(K) = E[\mathfrak{p}_3^2] \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, generated by $(-1, -\omega)$ and $(0, -1)$. Among the generators, $(0, -1)$ generate $E[\mathfrak{p}_3]$. The curve E has additive reduction at $\mathfrak{p}_3$ with Tamagawa number 3. Most of these data come either immediately from the equation or via Tate's algorithm. The torsion part of $E(K)$ can be determined using the Lutz-Nagell theorem. One can use isogeny descent to show that the rank of E is 0. Alternatively, LMFDB data shows that $L(E/\mathbb{Q}, 1) \neq 0$, so $L(\bar{\psi}, 1) \neq 0$, and the claim follows by the Coates-Wiles theorem.

Hecke character We compute the Grössencharakter $\psi : \mathbb{I}_K/K^\times \to \mathbb{C}^\times$ attached to E. When restricted to the archimedean places, this is just $\mathbb{C}^\times \to \mathbb{C}^\times$, $x \mapsto x^{-1}$. For the finite places, first consider the primes away from $\mathfrak{p}_3 = (1+\omega)$. Let $\mathfrak{p} \neq \mathfrak{p}_3$, then E has good reduction at $\mathfrak{p}$, so $\psi(\mathcal{O}_\mathfrak{p}^\times) = 1$, and $\psi(\mathfrak{p})$ is a generator of $\mathfrak{p}$. The Frobenius at $\mathfrak{p}$ acts trivially on $E[\mathfrak{p}_3^2]$, so $\psi(\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}_3^2}$. These conditions uniquely determine $\psi(\mathfrak{p})$. For example, take $\mathfrak{p} = 2\mathcal{O}$, then $\psi(\mathfrak{p}) = -2$. One can easily check using the point doubling formula that $\psi(\mathfrak{p})$ reduces to the Frobenius $(x, y) \mapsto (x^4, y^4)$.

Next, consider the behaviour of ψ on $K_{\mathfrak{p}_3}^\times$. If $u \in \mathcal{O}$ and $u \equiv 1 \pmod{\mathfrak{p}_3^2}$, then $\psi(u\mathcal{O})$ is the unique generator of (u) which is congruent to 1 modulo $\mathfrak{p}_3^2$, so it equals to u. Comparing this with $\psi(u) = 1$ and the above computation of the archimedean part of ψ shows that $\psi(u_{\mathfrak{p}_3}) = 1$. Such elements are dense in $1 + \mathfrak{p}_3^2\mathcal{O}_{\mathfrak{p}_3}$, so the conductor of ψ is $\mathfrak{p}_3^2$, which agrees with the result of Serre and Tate remarked earlier in the essay. For completeness, the same method shows that $\psi((1+\omega)_{\mathfrak{p}_3}) = 1 + \omega$, and $\psi((\omega)_{\mathfrak{p}_3}) = \omega$. These results completely determine ψ.

Observe that a prime $p \neq 3$ splits in K iff $p \equiv 1 \pmod 3$ by quadratic reciprocity. Using the description of ψ given above, we see that $\psi(p) = -p$ if p is inert, whose trace reduces to 0 modulo p, so the reduction is supersingular. If p splits, then $p = a^2 + ab + b^2$ for $a, b \in \mathbb{Z}$, and $p = \mathfrak{p}^+\mathfrak{p}^-$, with $\mathfrak{p}^\pm = (a + b\omega^{\pm 1})\mathcal{O}$. Let $\epsilon, \delta \in \{0, \pm 1\}$ be such that $a \equiv \epsilon, b \equiv \delta \pmod 3$. One can check that $a \not\equiv b \pmod 3$, so $\epsilon \neq \delta$, and $\epsilon + \delta\omega^{\pm 1} \in \langle \omega \rangle$. Therefore, $\psi(\mathfrak{p}^\pm) = (a + b\omega^{\pm 1})(\epsilon + \delta\omega^{\mp 1})$, and its trace is

$$a_p = a_{\mathfrak{p}^\pm} = a(2\epsilon + \delta) + b(2\delta + \epsilon)$$

For example, if $p = 7$, then $a = 2, b = 1, \epsilon = -1, \delta = 1$, so $a_7 = -1$, in agreement with the data from the LMFDB. It is easy to see that $a_p \equiv -1 \pmod 3$. In particular, $a_p \neq 0$, so it is also non-zero when reduced modulo p (we need $p > 5$ to use the Hasse bound, but 2 and 5 are inert). We have therefore proven that E has supersingular reduction at a prime above $p \neq 3$ if and only if p is inert. This is a special case of Deuring's criterion for reduction (section 13.4, theorem 12 of [Lan87]).

Division points Let $\mathfrak{p} = (2 + \omega)$. We expect $F = K(E[\mathfrak{p}])$ to be an abelian extension of K of degree $\mathbf{N}\mathfrak{p} - 1 = 6$, totally ramified above 7. A computation shows that in fact $F = K(\alpha)$, where $\alpha^6 = -\frac{3}{7}(\omega + 4)$, and the $\mathfrak{p}$-torsion points are generated by

$$P_7 = \left(\frac{1}{3}(\omega + 1)\alpha^2, -\frac{1}{2}\omega\alpha^3 - \frac{1}{2}\right)$$

One can further show that F has class number one, which satisfies the bounds derived earlier, albeit trivially. Finally, observe that if $\sigma \in G_K$ is such that $\sigma\alpha = \omega\alpha$, then $\sigma P = 3P$. This determines χ_E.

Next let $\mathfrak{q} = (5)$, which remains prime in K. The x-coordinates of points in $E[5]\backslash\{0\}$ are roots of the division polynomial ψ_5 (see exercise 3.7 of [Sil09]), given by

$$\psi_5(x) = 5x^{12} + 95x^9 - 15x^6 - 25x^3 - 1$$

Instead of computing $K(E[5])$, a field of absolute degree 48, and its associated quantities, we take $\mathfrak{q}$ to be our auxilliary ideal $\mathfrak{a}$. Then

$$\Theta_{E,\mathfrak{q}}(P) = 5^{-12}(-27)^{24}\Bigg(\prod_{Q\in E[\mathfrak{a}]\backslash\{0\}} (x(P) - x(Q))\Bigg)^{-6} = 3^{72}\psi_5(x(P))^{-12}$$

Let $P = (2^{1/3}, 1) \in E(\bar{K})$. It is the sum of a 2-torsion point and a $\mathfrak{p}_3$-torsion point. By the proof of theorem 4.1, we expect $\Theta_{E,\mathfrak{q}}(P)$ to be a global unit. Plugging the values in gives the value 1, which is indeed a global unit. More excitingly, take P to be $P_7 + (0, -1)$, we obtain

$$\begin{aligned}\psi_5(x(P)) &= 2^{-1} \cdot 3^6 \cdot \big((105 - 140\omega)\alpha^3 + (127 + 75\omega)\big)\\ \Theta_{E,\mathfrak{q}}(P) &= 2^{12}\big((105 - 140\omega)\alpha^3 + (127 + 75\omega)\big)^{-12}\end{aligned}$$

By computing norm, one can verify that this is the 12-th power of a global unit.

From the expression, one can also compute the expansion of $\Theta_{E,\mathfrak{q}}(z)$ around $z = 0$. The expansion for $\wp(z)$ is $z^{-2}\big(1 - \frac{1}{140}z^6 + O(z^{10})\big)$, so

$$\Theta_{E,\mathfrak{q}}(z) = 3^{72} \cdot 5^{-12} z^{12\cdot 24}\big(1 + 3 \cdot 23^2 \cdot 7^{-1} z^6 + O(z^{10})\big)$$

which has the expected leading term. Furthermore, observe that

$$\frac{d}{dz} \log \Theta_{E,\mathfrak{q}}(z) = -12\frac{\psi_5'(\wp(z))}{\psi_5(\wp(z))}\wp'(z) = -12\frac{\psi_5'(x)}{\psi_5(x)}(2y + 1)$$

Choose $f = 3$ to be the generator of $\mathfrak{f}$. Given a complex period $\Omega_{\mathbb{C}}$, let P be the point corresponding to $\frac{1}{3}\Omega_{\mathbb{C}}$. By corollary 3.12,

$$L(\bar{\psi}, 1)/\Omega_{\mathbb{C}} = -\frac{1}{2 \cdot 3^2 \cdot 5} \operatorname{Tr}_{K(\mathfrak{f})/K}\left(\frac{\psi_5'(x(P))}{\psi_5(x(P))}(2y(P) + 1)\right)$$

We will compute a value of $\Omega_{\mathbb{C}}$ in the next part. With that choice, $P = (-1, \omega - 1)$. This formula then gives $L(\bar{\psi}, 1)/\Omega_{\mathbb{C}} = \frac{\sqrt{-3}}{9}$. Therefore, $L(E, 1) = \frac{1}{27}\Omega_{\mathbb{C}}\bar{\Omega}_{\mathbb{C}}$.

Analytic invariants Finally, we consider E as a curve over $\mathbb{Q}$ and look at the predictions of the Birch and Swinnerton-Dyer conjecture. According to the LMFDB, $L(E/\mathbb{Q}, 1) \approx 0.58888$.

The curve E has the short Weierstrass equation $y'^2 = x'^3 + \frac{1}{4}$, so we seek a period $\Omega_{\mathbb{C}} \in \mathbb{C}^\times$ such that $35\Omega_{\mathbb{C}}^{-6}G_6(\mathcal{O}) = -\frac{1}{4}$. In fact

$$G_6(\mathcal{O}) = \frac{1}{2^6 \cdot 3^3 \cdot 5 \cdot 7 \cdot \pi^3}\Gamma\Big(\frac{1}{3}\Big)^6\Gamma\Big(\frac{1}{6}\Big)^6$$

This is stated in section 1.1 of [DS05]. It can be proven by transforming the associated elliptic integral into a beta integral. From this statement, we deduce that

$$\Omega_{\mathbb{C}} = \frac{1}{2^{2/3}\sqrt{-3\pi}}\Gamma\Big(\frac{1}{3}\Big)\Gamma\Big(\frac{1}{6}\Big),\ \Omega = \frac{1}{2^{2/3}\sqrt{\pi}}\Gamma\Big(\frac{1}{3}\Big)\Gamma\Big(\frac{1}{6}\Big) \approx 5.2992$$

where to get the real period, we multiplied $\Omega_{\mathbb{C}}$ by $\sqrt{-3}$. Therefore, the algebraic part of $L(E/\mathbb{Q}, 1)$ is equal to $\frac{1}{9}$. Based on this computation, the Birch and Swinnerton-Dyer conjecture predicts that $\text{Ш}(E/\mathbb{Q})$ is trivial. If we apply Wiles' reciprocity law in the proof of the Coates-Wiles theorem, then we can deduce from what has been proven that $S_p(E_{/\mathbb{Q}}) = 0$ for $p > 3$.

References

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. reine angew. Math.*, 218:79–108, 1965.

[CW77] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Inventiones math.*, 39:223–251, 1977.

[dS87] E. de Shalit. *Iwasawa Theory of Elliptic Curves with Complex Multiplication*, volume 3 of *Perspectives in Mathematics.* Academic Press, Inc., Orlando, 1987.

[DS05] F. Diamond and J. Shurman. *A First Course in Modular Forms*, volume 228 of *Graduate Texts in Mathematics.* Springer, New York, 2005.

[KL81] D. S. Kubert and S. Lang. *Modular Units*, volume 244 of *Grundlehren der mathematischen Wissenschaften.* Springer, New York, 1981.

[Lan87] S. Lang. *Elliptic Functions*, volume 112 of *Graduate Texts in Mathematics.* Springer, New York, 1987.

[LMF17] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2017. [Online; accessed 01 May 2017].

[LT65] J. Lubin and J. Tate. Formal complex multiplication in local fields. *Annals of Mathematics*, 81(2):380–387, 1965.

[MR04] B. Mazur and K. Rubin. *Kolyvagin systems*, volume 168 of *Mem. Amer. Math. Soc.* American Mathematical Society, Providence, 2004.

[Rob73] G. Robert. Unités elliptiques et formules pour le nombre de classes des extensions abéliennes d'un corps quadratique imaginaire. *Mémoires de la S.M.F*, 36:5–77, 1973.

[Rub99] K. Rubin. Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. In *Arithmetic Theory of Elliptic Curves (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Mathematics*, pages 167–234. Springer, Berlin, 1999.

[Rub00] K. Rubin. *Euler Systems*, volume 147 of *Annals of Mathematics Studies.* Princeton University Press, Princeton, 2000.

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, New York, 2nd edition, 2009.

[ST68] J-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math.*, 88:492–517, 1968.

[Wei76] A. Weil. *Elliptic Functions according to Eisenstein and Kronecker*, volume 88 of *Ergebnisse der Mathematik und ihre Grenzgebiete.* Springer, Berlin, 1976.

[Wil78] A. Wiles. Higher explicit reciprocity laws. *Annals of Math.*, 107:235–254, 1978.