REPORTS@SCM

AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

CM elliptic curves and the Coates–Wiles Theorem

*Martí Roset Julià
McGill University.
marti.rosetjulia@mail.mcgill.ca

∗Corresponding author

Resum *(CAT)*

Descrivim un dels únics casos de la Conjectura de Birch i Swinnertor-Dyer que ha estat demostrat, l'anomenat teorema de Coates–Wiles. Sigui K un cos quadràtic imaginari amb anell d'enters $\mathcal{O}$ principal i sigui E una corba el·líptica definida sobre K amb multiplicació complexa per $\mathcal{O}$. El teorema de Coates–Wiles afirma que si la sèrie L associada a E/K no s'anul·la en 1, aleshores el conjunt de punts K-racionals de E és finit. La prova que explicarem, donada per Karl Rubin, utilitza la teoria de sistemes d'Euler.

Abstract *(ENG)*

We describe one of the few cases of the Birch and Swinnerton-Dyer Conjecture that has been already proved, the so called Coates–Wiles Theorem. Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$ and class number 1 and let E be an elliptic curve defined over K with complex multiplication by $\mathcal{O}$. The Coates–Wiles Theorem states that if the L-series attached to E/K does not vanish at 1, then the set of K-rational points of E is finite. We explain a proof given by Karl Rubin, which uses the theory of Euler systems.

Keywords: *BSD Conjecture, Coates–Wiles Theorem, L-series, elliptic curves with CM, Euler systems, elliptic units.*
MSC (2010): *11G18, 14G35.*
Received: *September 4, 2020.*
Accepted: *November 7, 2020.*

Acknowledgement

I would like to express my gratitude to CFIS and to Fundació CELLEX for organizing and partially funding a mobility program to do part of this project at Princeton University. I would also like to thank the MOBINT Scholarship for partially funding this program.

Societat Catalana de Matemàtiques

Institut d'Estudis Catalans

1. Introduction

An elliptic curve E defined over a field F is a algebraic projective nonsingular curve of genus one with a distinguished F-rational point O. The Riemann–Roch Theorem shows that the set of affine F-rational points of E can be identified with the locus of solutions in $\mathbb{A}^2(F)$ of a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

with coefficients a_i in F. Then, O is the point at infinity. We will denote by $E(F)$ the set of points $P = (x, y)$ with $x, y \in F$ that satisfy (1) together with the point O.

Remarkably, $E(F)$ can be endowed with a natural group structure. It is given by the Chord-Tangent Method. Given two points $P, Q \in E(F)$, consider the point R of intersection of the line passing through P and Q with $E(F)$. Then, define $P + Q$ to be the intersection of the line through R and O with $E(F)$.

The endomorphisms of E are the morphisms $\phi\colon E \to E$ of algebraic curves that respect the group structure of E. The set $\mathrm{End}(E)$ of endomorphisms of E is a ring where the operations are addition and composition. Some examples of endomorphisms are the maps multiplication-by-m for some integer m, which are naturally defined by adding a point m times using the Chord-Tangent Method. For some curves these are all the possible endomorphisms. For others, $\mathrm{End}(E)$ can have more elements and in such a case we say that E has complex multiplication: the ring $\mathrm{End}(E)$ can be either an order in an imaginary quadratic field or a quaternion algebra, and this last option is not possible if F has characteristic 0. See [4, Chap. 2] for an outline of the main theorem of elliptic curves with complex multiplication over a field of characteristic 0.

From now on assume that F is a number field with ring of integers $\mathcal{O}_F$. It is natural to ask about the size of $E(F)$ and it turns out that we can use the group structure of $E(F)$ to say something about it. A very important example of that is the Mordell–Weil Theorem which states that $E(F)$ is a finitely generated group, i.e. $E(F) \cong \mathbb{Z}^r \oplus T$ where $r \geq 0$ is an integer and T is a finite group. We call $r = r_E$ the rank of E, a mysterious invariant that has been object of extensive study.

Based on computer calculations, a conjectural answer to find r_E was given by Birch and Swinnerton-Dyer in 1965, the so called BSD Conjecture. It connects the algebraic nature of r_E with an analytic object attached to E, the L-series. In order to define the latter suppose that every a_i lies in $\mathcal{O}_F$. Then, the L-series attached to E is defined by an infinite product over the prime ideals of $\mathcal{O}_F$

$$L(E_{/F}, s) = \prod_{\mathfrak{p}} \frac{1}{L_{\mathfrak{p}}(E_{/F}, \mathrm{N}\mathfrak{p}^{-s})},$$

where $L_{\mathfrak{p}}(E_{/F}, T)$ is a polynomial of degree ≤ 2 and it is called the local factor at $\mathfrak{p}$. To define it, consider a minimal Weierstrass equation of E (see [5, Chap. VII, §1]) and reduce it modulo $\mathfrak{p}$. It was proven by Hasse that whenever the reduced equation is an elliptic curve over the field $\mathbb{F}_{\mathrm{N}\mathfrak{p}}$, which we will denote by $\tilde{E}(\mathbb{F}_{\mathrm{N}\mathfrak{p}})$, we have $\#\tilde{E}(\mathbb{F}_{\mathrm{N}\mathfrak{p}}) = \mathrm{N}\mathfrak{p} - a_{\mathfrak{p}} + 1$, where $-2\sqrt{\mathrm{N}\mathfrak{p}} \leq a_{\mathfrak{p}} \leq 2\sqrt{\mathrm{N}\mathfrak{p}}$. In that case, we define $L_p(E_{/F}, T) = (1 - a_{\mathfrak{p}}T + \mathrm{N}\mathfrak{p}T^2)$. When the reduced curve is not smooth the definition for $L_{\mathfrak{p}}(E_{/F}, T)$ depends on the structure of the group of nonsingular points of $\tilde{E}(\mathbb{F}_{\mathrm{N}\mathfrak{p}})$ (see [5, App. C, §16]). Using the estimate of $a_{\mathfrak{p}}$ it is not hard to see that the Euler product converges on the right half plane $\{s \in \mathbb{C} : \mathrm{Re}(s) > 3/2\}$. Birch and Swinnerton-Dyer conjectured the following.

Conjecture 1.1 (BSD Conjecture)**.** *The series $L(E_{/F}, s)$ admits an analytic continuation to the entire complex plane. Moreover $r_E = \mathrm{ord}_{s=1} L(E_{/F}, s)$.*

At this point it is worth mentioning the local global principle. The definition of the L-series attached to E has information of the curve E defined over the residue fields $\mathbb{F}_{N\mathfrak{p}}$, which we can call local information, and the BSD Conjecture states that it is possible to deduce results of E over the global field F from it.

For the case where $F = \mathbb{Q}$ the work of Wiles et al. on the Shimura–Tanyiama–Weil Conjecture implies that $L(E_{/\mathbb{Q}}, s)$ has analytic continuation. The analytic continuation for the particular case where E has complex multiplication is known since the work of Deuring, who gave an expression of $L(E_{/F}, s)$ in terms of the so called Hecke L-series and Hecke who proved the analytic continuation of the latter. In this project we outline the proof of the following particular case of the BSD Conjecture. Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$ and class number 1.

Theorem 1.2 (Coates–Wiles)**.** *Suppose E is defined over K and it has complex multiplication by $\mathcal{O}$. If $L(E_{/K}, 1) \neq 0$, then $E(K)$ is finite.*

We will expose a proof of this theorem given by Rubin in [1]. As we said, the analytic continuation of the L-series for our particular case was already known at this time so we will focus on proving that $E(K)$ is a finite group. Our exposition is organized in the following manner.

Section 2 provides an expression of the Selmer group of certain endomorphisms which will allow us to determine when they are trivial. Section 3 covers the theory of the Euler system of elliptic units. We introduce this system and explain how it is used to bound certain ideal class groups. Section 4 explains the connection between elliptic units and the L-series of E and combines the previous work to prove the theorem. It shows that if $L(E_{/K}, 1) \neq 0$, we can produce a concrete system of elliptic units. Applying the theory of Euler systems to it we will be able to give a sharp bound of the ideal class group studied in Section 3. This is precisely one of the conditions to show that certain Selmer group is trivial and with some additional work we will be able to conclude the proof.

2. The Selmer group

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$. Assume here and from now on that K has class number 1. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}$ above a rational prime $p > 3$ that splits in K and let $\pi \in K$ be such that $(\pi) = \mathfrak{p}$. Let E be an elliptic curve defined over K with complex multiplication by $\mathcal{O}$. Fix $\bar{K}$ an algebraic closure of K, let $\mathrm{End}(E)$ be the ring of endomorphisms of E defined over $\bar{K}$ and fix the unique isomorphism $[\cdot]\colon \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$ such that $[\alpha]^*\omega = \alpha\omega$ for every $\alpha \in \mathcal{O}$ and ω any invariant differential of E. When it is clear from the context, we will write α for the endomorphism $[\alpha]$. The goal of this section is to define the π-Selmer group of E over K, that will be denoted by $S_\pi(E_{/K})$ and characterize when it is trivial.

We begin by recalling the definition of $S_\alpha(E_{/F})$ for a number field $F \supset K$ and $\alpha \in \mathcal{O}$ and explaining why it will be relevant to prove the Coates–Wiles Theorem. First suppose that F is any field containing K and view E as an elliptic curve defined over F. Let $\bar{F}$ be an algebraic closure of F. If $\alpha \in \mathcal{O}$, denote by $E[\alpha]$ the kernel of $[\alpha]\colon E(\bar{F}) \to E(\bar{F})$ and if L is an extension of F contained in $\bar{F}$, let $E[\alpha](L)$ be the set of points of $E[\alpha]$ defined over L. Let $G_F = \mathrm{Gal}(\bar{F}/F)$. Consider the following exact sequence of G_F-modules

$$0 \to E[\alpha] \to E(\bar{F}) \xrightarrow{\alpha} E(\bar{F}) \to 0.$$

Taking G_F-cohomology leads to a long exact sequence, where we only write the first terms

$$0 \to E[\alpha](F) \to E(F) \xrightarrow{\alpha} E(F) \xrightarrow{\delta} H^1(F, E[\alpha]) \to H^1(F, E(\bar{F})) \xrightarrow{\alpha} H^1(F, E(\bar{F})),$$

where we are considering continuous morphisms and δ is the connecting morphism

$$\delta\colon E(F) \to H^1(F, E[\alpha]), \quad P \mapsto [\sigma \mapsto Q^\sigma - Q] \text{ for some } Q \text{ satisfying } \alpha Q = P.$$

From this sequence we can obtain the following short exact sequence

$$0 \to E(F)/\alpha E(F) \xrightarrow{\delta} H^1(F, E[\alpha]) \to H^1(F, E(\bar{F}))[\alpha] \to 0$$

(note that $H^1(F, E(\bar{F}))$ is an $\mathrm{End}(E)$-module and $H^1(F, E(\bar{F}))[\alpha]$ denotes the α-torsion of it).

We will study $E(F)/\alpha E(F)$ by studying its image by δ in $H^1(F, E[\alpha])$ for F a number field containing K. As we will see, this is easier if F is a local field containing K. This motivates the following: suppose that F is a number field containing K, fix a prime $\mathfrak{Q}$ (finite or infinite) of F and regard E as defined over the completion of F at $\mathfrak{Q}$, that from now on will be denoted by $F_\mathfrak{Q}$ (we will use similar notations to denote completions). Viewing E as an elliptic curve defined over $F_{F_\mathfrak{Q}}$ and repeating the process described above we obtain the short exact sequence

$$0 \to E(F_\mathfrak{Q})/\alpha E(F_\mathfrak{Q}) \xrightarrow{\delta} H^1(F_\mathfrak{Q}, E[\alpha]) \to H^1(F_\mathfrak{Q}, E)[\alpha] \to 0. \tag{2}$$

Using that $F \subset F_\mathfrak{Q}$, and $G_F \supset G_{F_\mathfrak{Q}}$, we have the natural map $E(F)/\alpha E(F) \to E(F_\mathfrak{Q})/\alpha E(F_\mathfrak{Q})$ and the restriction maps $H^1(F, E[\alpha]) \xrightarrow{\mathrm{res}_\mathfrak{Q}} H^1(F_\mathfrak{Q}, E[\alpha])$, $H^1(F, E(F)) \xrightarrow{\mathrm{res}_\mathfrak{Q}} H^1(F_\mathfrak{Q}, E(F_\mathfrak{Q}))$. We can consider these maps for every prime $\mathfrak{Q}$ of F to obtain the following commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(F)/\alpha E(F) & \xrightarrow{\delta} & H^1(F, E[\alpha]) & \longrightarrow & H^1(F, E)[\alpha] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_\mathfrak{Q} E(F_\mathfrak{Q})/\alpha E(F_\mathfrak{Q}) & \xrightarrow{\delta} & \prod_\mathfrak{Q} H^1(F_\mathfrak{Q}, E[\alpha]) & \longrightarrow & \prod_\mathfrak{Q} H^1(F_\mathfrak{Q}, E)[\alpha] & \longrightarrow & 0.
\end{array}$$

Instead of studying the image of $E(F)/\alpha E(F)$ by δ, we will consider a larger group that is easier to characterize.

Definition 2.1. Let F be a number field containing K and let $\alpha \in \mathcal{O}$. Define the α-Selmer group of E/F as

$$S_\alpha(E_{/F}) = \{c \in H^1(F, E[\alpha]) : \mathrm{res}_\mathfrak{Q}(c) \in \delta(E(F_\mathfrak{Q})/\alpha E(F_\mathfrak{Q})) \text{ for all } \mathfrak{Q}\}.$$

Remark 2.2. One can think of the Selmer group $S_\alpha(E_{/F})$ as the smallest group defined by natural local conditions containing $\delta(E(F)/\alpha E(F))$.

The following proposition explains the relevance of the Selmer group of an elliptic curve.

Proposition 2.3. *Let $\alpha \in \mathcal{O}$. Suppose $S_\alpha(E_{/F}) = 0$, then $E(F)$ is finite.*

Proof. By definition of $S_\alpha(E_{/F})$, we have the injection $E(F)/\alpha E(F) \hookrightarrow S_\alpha(E_{/F})$. Thus, $E(F)/\alpha E(F) = 0$. Now the result follows from the Mordell–Weil Theorem (see [5, Ch. VIII, Thm. 4.1] for the statement and proof of Mordell–Weil Theorem). □

Here and from now on let $\alpha = \pi^n$. We proceed to study $S_\alpha(E_{/F})$. The main point in the following calculations is noting that the local conditions that appear in the definition of the Selmer group behave differently depending on whether the prime ideal $\mathfrak{Q}$ of F divides α or not. We begin studying the primes $\mathfrak{Q}$ such that $\mathfrak{Q} \nmid \alpha$.

Definition 2.4. Define the enlarged Selmer group of α as

$$S'_\alpha(E_{/F}) = \{c \in H^1(F, E[\alpha]) : \mathrm{res}_\mathfrak{Q}(c) \in \delta(E(F_\mathfrak{Q})/\alpha E(F_\mathfrak{Q})) \text{ for all } \mathfrak{Q} \nmid \alpha\}.$$

Clearly, $S_\alpha(E_{/F}) \subset S'_\alpha(E_{/F})$.

Theorem 2.5. *Suppose E is defined over K and let $K_n = K(E[\mathfrak{p}^n])$. Then,*

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

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

Proof. This is done in two steps. First we compute

$$S'_\alpha(E_{/K_n}) = \{c \in \mathrm{Hom}(G_{K_n}, E[\mathfrak{p}^n]) : \mathrm{res}_\mathfrak{Q}(c) \in \delta(E(K_{n,\mathfrak{Q}})/\alpha E(K_{n,\mathfrak{Q}}) \text{ for all } \mathfrak{Q} \mid \alpha\},$$

where we used that G_{K_n} fixes $E[\mathfrak{p}^n]$ and $K_{n,\mathfrak{Q}}$ denotes the completion of K_n at the prime $\mathfrak{Q}$. Since E has good reduction at $\mathfrak{Q}$ (see [1, Thm. 5.7]), the inertia subgroup $I_\mathfrak{Q} \subset G_{K_{n,\mathfrak{Q}}}$ acts trivially on $E[\mathfrak{p}^m]$ for every $m \geq 1$ (see [1, Coroll. 3.17]). Therefore, the connecting morphism factors trough

$$E(K_{n,\mathfrak{Q}})/\alpha E(K_{n,\mathfrak{Q}}) \to \mathrm{Hom}(G_{K_{n,\mathfrak{Q}}}/I_\mathfrak{Q}, E[\mathfrak{p}^n]). \tag{3}$$

By (2) this map is injective and it can be seen that it is an isomorphism by showing that both groups are isomorphic to $\mathcal{O}/\mathfrak{p}^n$, see [1, Lem. 6.4]. From there it follows that $S'_\alpha(E_{/K_n}) \cong \mathrm{Hom}(M_n/K_n, E[\mathfrak{p}^n])$ by class field theory. The second step of the proof consists on applying [1, Lem. 6.2] to see that the inflation restriction exact sequence induces the isomorphism $S'_\alpha(E_{/K}) \simeq S'_\alpha(E_{/K_n})^{\mathrm{Gal}(K_n/K)}$. □

We are left with studying the local condition at $\mathfrak{p}$. Since $\mathfrak{p}$ is coprime to $\mathfrak{f}$, E has good reduction at $\mathfrak{p}$. Since $\mathrm{ord}_\mathfrak{p}(p) \leq 2 < p - 1$, the logarithm induces an isomorphism $\log_E \colon E_1(K_\mathfrak{p}) \xrightarrow{\sim} \mathfrak{p}\mathcal{O}_\mathfrak{p}$, where $E_1(K_\mathfrak{p})$ is the set of points of $E(K_\mathfrak{p})$ that reduce to 0 modulo $\mathfrak{p}$. Moreover, since the reduction of E at $\mathfrak{p}$ has no $\mathfrak{p}$-torsion, $E(K_\mathfrak{p}) = E_1(K_\mathfrak{p}) \times \tilde{E}(k)$ and $\log_E$ can be extended to a map $\log_E \colon E(K_\mathfrak{p}) \to \mathcal{O}_\mathfrak{p}$ (see [1, Lem. 6.6]). By [1, Coroll. 5.20 (iv)], K_n/K is totally ramified at $\mathfrak{p}$. For every $n \geq 1$, denote $K_{n,\mathfrak{p}}$ the completion of K at the unique prime above $\mathfrak{p}$.

Definition 2.6. Define the following Kummer pairing

$$\langle\, , \rangle_{\pi^n} \colon E(K_\mathfrak{p}) \times K_{n,\mathfrak{p}}^\times \to E[\mathfrak{p}^n], \quad P, x \mapsto \langle P, x\rangle_{\pi^n} = Q^{[x, K_{n,\mathfrak{p}}]} - Q,$$

where $Q \in E(\bar{K}_\mathfrak{p})$ is such that $\pi^n Q = P$ and $[\cdot, K_{n,\mathfrak{p}}]$ is the local Artin map.

Definition 2.7. For every $n \geq 1$, define $\delta_n \colon K_{n,\mathfrak{p}}^\times \to E[\mathfrak{p}^n]$ by $\delta_n(x) = \langle R, x\rangle_{\pi^n}$.

Lemma 2.8 ([1, Lem. 6.8])**.** *For every n, the map δ_n is characterized by the fact that if $P \in E(K_\mathfrak{p})$ and $x \in K_{n,\mathfrak{p}}^\times$, we have $\langle P, x\rangle_{\pi^n} = (\pi^{-1} \log_E(P))\delta_n(x)$. Moreover, if $\mathcal{O}_{n,\mathfrak{p}}$ is the ring of integers of $K_{n,\mathfrak{p}}$, we have $\delta_n(\mathcal{O}_{n,\mathfrak{p}}^\times) = E[\mathfrak{p}^n]$.* □

The previous lemma shows that δ_n is essentially the connecting morphism given in (2). Combining this lemma with Theorem 2.5 and class field theory yields the following description of $S_{\pi^n}(E_{/K})$. For every number field F let $\mathbb{A}_F^\times$ denote the idele group of F.

Theorem 2.9 ([1, Thm. 6.9]). *Let $K_n = K(E[\mathfrak{p}^n])$ with idele group $\mathbb{A}_{K_n}^\times$. Define*

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

Then, $S_{\pi^n}(E_{/K}) \cong \mathrm{Hom}(\mathbb{A}_{K_n}^\times / W_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$. □

Let $\Delta = \mathrm{Gal}(K(E[\mathfrak{p}])/K)$. Then, Δ acts naturally on the $\mathcal{O}/\mathfrak{p}$-vector space $E[\mathfrak{p}]$. Let $\chi_E \colon \Delta \to \mathbb{F}_p^\times$ be the character of this representation. Let A be the p-part of the ideal class group of K_1. Note that Δ acts on A in a natural way. For every character $\chi \colon \Delta \to \mathbb{F}_p^\times$ consider the composition, also denoted by χ, $\chi \colon \Delta \to \mathbb{F}_p \hookrightarrow \mathbb{Z}_p^\times$, where the last morphism is given by Hensel's Lemma. For a given $\mathbb{Z}[\Delta]$-module M, let $M^{(p)} = M \otimes_{\mathbb{Z}} \mathbb{Z}_p$, which is a $\mathbb{Z}_p[\Delta]$-module and let M^χ be the χ-isotypical component of $M^{(p)}$. Another application of class field theory gives the following result.

Corollary 2.10. *Consider the same notation as above and suppose that p splits in K. Then, $S_\pi(E_{/K}) = 0$ if and only if $A^{\chi_E} = 0$ and $\delta_1(\mathcal{O}_{K_1}^\times) \neq 0$.*

This characterizes when $S_\pi(E_{/K}) = 0$ which is the key point to prove the Coates–Wiles Theorem since, as we explained, $S_\pi(E_{/K}) = 0$ implies that $E(K)$ is finite.

3. The Euler system of elliptic units

Let E be an elliptic curve defined over K with complex multiplication by $\mathcal{O}$. Let ψ be the Hecke character attached to E with conductor $\mathfrak{f}$ (see [4, Chap. 2, §9]), viewed as a character on ideals. Choose a prime $\mathfrak{p}$ of K not dividing $6\mathfrak{f}$, let p be the rational prime below it and suppose that p splits in K. Fix an ideal $\mathfrak{a}$ of $\mathcal{O}$ coprime to $6\mathfrak{p}\mathfrak{f}$. Let $\mathcal{R}$ be the set of square free ideals of $\mathcal{O}$ coprime to $6\mathfrak{f}\mathfrak{p}\mathfrak{a}$. Finally, for $n \geq 0$ denote by $K_n = K(E[\mathfrak{p}^n])$, if $\mathfrak{r} \in \mathcal{R}$ denote by $K_n(\mathfrak{r}) = K(E[\mathfrak{p}^n\mathfrak{r}])$ and let $G_\mathfrak{r} = \mathrm{Gal}(K_n(\mathfrak{r})/K_n)$. In this section we introduce the Euler system of elliptic units and we explain how it can be used to bound the size of A^{χ_E} defined above. We will work with the following definition of Euler system.

Definition 3.1. An Euler system is a set of global units $\{\eta(n,\mathfrak{r}) \in K_n(\mathfrak{r})^\times \mid n \geq 1 \text{ and } \mathfrak{r} \in \mathcal{R}\}$ satisfying:

(i) if $\mathfrak{r}\mathfrak{q} \in \mathcal{R}$, where $\mathfrak{q}$ is a prime ideal of $\mathcal{O}$, $\mathrm{N}_{K_n(\mathfrak{r}\mathfrak{q})/K_n(\mathfrak{r})}\eta(n,\mathfrak{r}\mathfrak{q}) = \eta(n,\mathfrak{r})^{(1-\mathrm{Frob}_\mathfrak{q}^{-1})}$, and

(ii) if $\mathfrak{r} \in \mathcal{R}$ and $n \geq 1$, $\mathrm{N}_{K_{n+1}(\mathfrak{r})/K_n(\mathfrak{r})}\eta(n+1,\mathfrak{r}) = \eta(n,\mathfrak{r})$.

We now construct the so called Euler system of elliptic units. For that we need to introduce the following rational functions. Fix here and from now on an analytic isomorphism $\xi \colon \mathbb{C}/L \xrightarrow{\sim} E(\mathbb{C})$ where $L = \Omega\mathcal{O}$ and $\Omega \in \mathbb{C}$.

Definition 3.2. Choose a Weierstrass equation for E and denote by $\Delta(E)$ its discriminant. Let $\gamma \in \mathcal{O}$ be a generator of the ideal $\mathfrak{a}$. Define

$$\Theta_{E,\mathfrak{a}} = \gamma^{-12}\Delta(E)^{\mathrm{N}\mathfrak{a}-1} \prod_{P \in E[\mathfrak{a}]-O} (x - x(P))^{-6}.$$

Suppose that E is defined over K. Let $S \in E$ be an $\mathcal{O}$-generator of $E[\mathfrak{f}]$. Define

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

where $\tau_{S^\sigma}(P) = P + S^\sigma$ for every $P \in E$ and $K(\mathfrak{f})$ is the ray class field of K modulo $\mathfrak{f}$. Define $\Theta_{L,\mathfrak{a}} = \Theta_{E,\mathfrak{a}} \circ \xi$ and $\Lambda_{L,\mathfrak{a}} = \Lambda_{E,\mathfrak{a}} \circ \xi$.

The system of elliptic units is obtained by evaluating $\Lambda_{L,\mathfrak{a}}$ at certain torsion points of E in the following way.

Definition 3.3. Given $n \geq 0$ and an integral ideal $\mathfrak{r} \in \mathcal{R}$ define $\eta_n^{(\mathfrak{a})}(\mathfrak{r}) = \Lambda_{E,\mathfrak{a}}(\xi(\psi(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega))$. The set $\{\eta_n^{(\mathfrak{a})}(\mathfrak{r})\}$ for $n \geq 1$ and $\mathfrak{r} \in \mathcal{R}$ is the set of elliptic units.

Proposition 3.4 ([1, Prop. 8.2])**.** *The set $\{\eta_n^{(\mathfrak{a})}(\mathfrak{r})\}$ for $n \geq 1$ and $\mathfrak{r} \in \mathcal{R}$ is an Euler system.* □

Here and for the rest of this section we write $\eta(n, \mathfrak{r}) := \eta_n^{(\mathfrak{a})}(\mathfrak{r})$. Fix M a power of p and $n \geq 1$. We now explain how to construct a principal ideal of K_n starting from the unit $\eta(n, \mathfrak{r}) \in K_n(\mathfrak{r})$. This construction will be done only for $\mathfrak{r}$ in the following subgroup of $\mathcal{R}$.

Definition 3.5. Define $\mathcal{R}_{n,M}$ to be the subset of $\mathcal{R}$ with elements $\mathfrak{r} \in \mathcal{R}$ such that every prime $\mathfrak{q} \mid \mathfrak{r}$ satisfies:

(i) $\mathfrak{q}$ splits completely in K_n/K, and

(ii) $M \mid (\mathrm{N}\mathfrak{q} - 1)$.

In order to do the construction we will use Kolyvagin's derivative operator. For every $\mathfrak{q} \in \mathcal{R}$ prime ideal, fix $\sigma_\mathfrak{q} \in G_\mathfrak{q}$ a generator of the cyclic group $G_\mathfrak{q}$.

Definition 3.6. If $\mathfrak{q} \in \mathcal{R}$ prime, define $D_\mathfrak{q} = \sum_{i=1}^{\mathrm{N}\mathfrak{q}-2} i\sigma_\mathfrak{q}^i \in \mathbb{Z}[G_\mathfrak{q}]$. For an arbitrary ideal $\mathfrak{r} \in \mathcal{R}$, define $D_\mathfrak{r} := \prod_{\mathfrak{q}|\mathfrak{r}} D_\mathfrak{q} \in \mathbb{Z}[G_\mathfrak{r}]$.

Proposition 3.7. *Let $n \geq 1$, $\mathfrak{r} \in \mathcal{R}_{n,M}$ and $\sigma \in G_\mathfrak{r}$. Then, $\eta(n, \mathfrak{r})^{(\sigma-1)D_\mathfrak{r}} \in (K_n(\mathfrak{r})^\times)^M$. Moreover, there is a natural choice of Mth root of unity, that we will denote by $(\eta(n, \mathfrak{r})^{(\sigma-1)D_\mathfrak{r}})^{1/M}$.*

Proof. See [1, Prop. 8.4]. Note that both K_n and $K_n(\mathfrak{r})$ may contain Mth roots of unity. This is the reason why we need [1, Prop. 8.4 (i)] to specify a choice of an Mth root of $\eta(n, \mathfrak{r})^{(\sigma-1)D_\mathfrak{r}}$. For that, the so called universal Euler system is used (see [2, Chap. IV, §2] for more details). □

Definition 3.8. Let $n \geq 1$, $\mathfrak{r} \in \mathcal{R}_{n,M}$. Define the 1-cocycle $c \in H^1(G_\mathfrak{r}, K_n(\mathfrak{r})^\times)$ as

$$G_\mathfrak{r} \to K_n(\mathfrak{r})^\times, \quad c(\sigma) = (\eta(n, \mathfrak{r})^{(\sigma-1)D_\mathfrak{r}})^{1/M}.$$

By Hilbert's Theorem 90 we have that $H^1(G_\mathfrak{r}, K_n(\mathfrak{r})) = 0$, hence there exists $\beta \in K_n(\mathfrak{r})^\times$ such that $c(\sigma) = \beta^{\sigma-1}$. Raising this equality to the Mth power yields

$$z = \frac{\eta(x_{n,\mathfrak{r}})^{D_\mathfrak{r}}}{\beta^M} \in K_n^\times.$$

The element β is well defined up to multiplication by an element of K_n. Hence, z is well defined in $K_n^\times/(K_n^\times)^M$.

Definition 3.9. With the same notation used in the previous definition, define

$$\kappa_{n,M}(\mathfrak{r}) = \frac{\eta(x_{n,\mathfrak{r}})^{D_\mathfrak{r}}}{\beta^M} \in K_n^\times/(K_n^\times)^M.$$

Fix $n \geq 1$. In order to simplify the notation denote $F = K_n$ and let $\mathcal{O}_F$ be its ring of integers. We proceed to write the factorization of the ideal generated by $\kappa_{n,M}(\mathfrak{r}) \in F$ modulo Mth powers in terms of $\kappa_{n,M}(\mathfrak{s})$ for ideals $\mathfrak{s} \mid \mathfrak{r}$.

Definition 3.10. Denote the group of ideals of F additively as $\mathcal{I} = \bigoplus_\mathfrak{Q} \mathbb{Z}\mathfrak{Q}$, where the sum is over all prime ideals $\mathfrak{Q}$ of F. If $\mathfrak{q}$ is a prime ideal of K, we define $\mathcal{I}_\mathfrak{q} = \bigoplus_{\mathfrak{Q}|\mathfrak{q}} \mathbb{Z}\mathfrak{Q}$. For a given $y \in F$, denote by (y) the principal ideal generated by y, $(y)_\mathfrak{q}$ its projection to $\mathcal{I}_\mathfrak{q}$, $[y] \in \mathcal{I}/M\mathcal{I}$ the reduction modulo M and $[y]_\mathfrak{q}$ the respective projection.

Fix $\mathfrak{q} \in \mathcal{R}_{n,M}$ a prime of K. We will construct a function, $\phi_\mathfrak{q}$, that will allow us to relate $[\kappa_{n,M}(\mathfrak{r})]_\mathfrak{q}$ with the element $\kappa_{n,M}(\mathfrak{r}\mathfrak{q}^{-1})$. We start by defining a map

$$\phi'_\mathfrak{q} \colon (\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^\times \to \mathcal{I}_\mathfrak{q}/M\mathcal{I}_\mathfrak{q}$$

that after a small modification will become the desired map. Note that $\mathfrak{q}$ splits completely in F. Therefore, we have

$$(\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^\times \cong \prod_{\mathfrak{Q}|\mathfrak{q}} (\mathcal{O}_F/\mathfrak{Q})^\times,$$

where each of the terms in the right hand side is a cyclic group of order $\mathrm{N}\mathfrak{q} - 1$. On the other hand

$$\mathcal{I}_\mathfrak{q}/M\mathcal{I}_\mathfrak{q} \cong \oplus_{\mathfrak{Q}|\mathfrak{q}} (\mathbb{Z}/M\mathbb{Z}).$$

Since $M \mid (\mathrm{N}\mathfrak{q} - 1)$, in order to define a map $(\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^\times \to \mathcal{I}_\mathfrak{q}/M\mathcal{I}_\mathfrak{q}$ it is enough to choose a generator of the cyclic group $(\mathcal{O}_F/\mathfrak{Q})^\times$ for every $\mathfrak{Q} \mid \mathfrak{q}$ and map it to $1 \in \mathbb{Z}/M\mathbb{Z}$. Now we explain how we choose these generators. For $\mathfrak{Q}$ dividing $\mathfrak{q}$ choose a prime $\mathfrak{Q}'$ of $F(\mathfrak{q})$ above it and consider $\pi_\mathfrak{Q}$ a local parameter at the prime $\mathfrak{Q}'$. Since the local field extension $F(\mathfrak{q})_{\mathfrak{Q}'}/F_\mathfrak{Q}$ is totally tamely ramified we have that the map

$$\mathrm{Gal}(F(\mathfrak{q})/F) \to \mathcal{O}_{F(\mathfrak{q}),\mathfrak{Q}'}{}^\times \to (\mathcal{O}_F/\mathfrak{Q})^\times, \quad \sigma \mapsto \pi_\mathfrak{Q}^{(1-\sigma)} \mapsto [\pi_\mathfrak{Q}^{(1-\sigma)}] \tag{4}$$

is a group isomorphism ([3, Chap. IV, Prop. 5]).

Definition 3.11. For $\mathfrak{Q}$ as above, define $\gamma_\mathfrak{Q} \in (\mathcal{O}_F/\mathfrak{Q})^\times$ to be the image of the fixed generator $\sigma_\mathfrak{q} \in G_\mathfrak{q}$ by the map in (4). It is a generator of $(\mathcal{O}_F/\mathfrak{Q})^\times$.

Definition 3.12. Define a map $\phi'_{\mathfrak{q}}\colon (\mathcal{O}_F/\mathfrak{q})^\times \to \mathcal{I}_{\mathfrak{q}}/M\mathcal{I}_{\mathfrak{q}}$ as follows. Given $\alpha \in (\mathcal{O}_F/\mathfrak{q})^\times$ and $\mathfrak{Q} \mid \mathfrak{q}$, let $a_{\mathfrak{Q}}(\alpha) \in \mathbb{Z}$ be such that $\alpha \equiv \gamma_{\mathfrak{Q}}^{a_{\mathfrak{Q}}(\alpha)} \mod \mathfrak{Q}$. Then define

$$\phi'_{\mathfrak{q}}(\alpha) = \sum_{\mathfrak{Q}\mid\mathfrak{q}} (a_{\mathfrak{Q}}(\alpha) \mod M)\mathfrak{Q}.$$

Finally, note that $\phi_{\mathfrak{q}}$ factors trough $(\mathcal{O}_F/\mathfrak{q})^\times/((\mathcal{O}_F/\mathfrak{q})^\times)^M$. Define $\phi_{\mathfrak{q}} = \phi'_{\mathfrak{q}} \circ j_{\mathfrak{q}}$, where $j_{\mathfrak{q}}$ is the natural map $\{\kappa \in F^\times/(F^\times)^M : [\kappa]_{\mathfrak{q}} = 0\} \to (\mathcal{O}_F/\mathfrak{q})^\times/((\mathcal{O}_F/\mathfrak{q})^\times)^M$. It is plain to see that $\phi_{\mathfrak{q}}$ is an isomorphism.

Theorem 3.13 (Factorization Theorem; [1, Prop. 8.10])**.** *Consider $\kappa_{n,M}(\mathfrak{r})$ and $\mathfrak{q}$ a prime ideal of K. Then,*

(i) if $\mathfrak{q} \nmid \mathfrak{r}$, $[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = 0$, and

(ii) if $\mathfrak{q} \mid \mathfrak{r}$: $[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = \phi_{\mathfrak{q}}(\kappa_{n,M}(\mathfrak{r}\mathfrak{q}^{-1}))$. □

Here and from now on suppose that $F = K_1$, i.e. $n = 1$. Note that $\eta(1,\mathcal{O}) \in \mathcal{O}_F^\times$ and denote by μ_F the subgroup of roots of unity of $\mathcal{O}_F^\times$. Let $\mathcal{C}$ be the $\mathbb{Z}[\Delta]$-submodule of $\mathcal{O}_F^\times$ generated by $\eta(1,\mathcal{O})$ and μ_F. The Factorization Theorem gives the factorization of principal ideals of the form $(\kappa_{1,M}(\mathfrak{r}))$ modulo M-th powers. If M is large enough, these factorizations give relations between the classes of the prime ideals generating A. This allows to give the following bound of the χ-isotypical component of A for every irreducible representation χ of Δ.

Theorem 3.14 ([1, Thm. 9.5])**.** *For every irreducible $\mathbb{Z}_p$-representation of Δ we have $\#A^\chi \leq \#(\mathcal{O}_F^\times/\mathcal{C})^\chi$.* □

Corollary 3.15. *Consider the same notation as above. Suppose that $\eta(1,\mathcal{O})^\chi \notin \mu_F^\chi((\mathcal{O}_F^\times)^\chi)^p$. Then, $A^\chi = 0$.*

4. Complex L-function of E and proof of Coates–Wiles Theorem

Let E be an elliptic curve defined over K with complex multiplication by $\mathcal{O}$. Let ψ be the Hecke character attached to E, viewed as a character on ideals, with conductor $\mathfrak{f}$ and denote by $\bar{\psi}$ its conjugate. Let $L(E_{/K}, s)$ be the complex L-function attached to E viewed as an elliptic curve over K. For a given ideal $\mathfrak{m}$ such that $\mathfrak{f} \mid \mathfrak{m}$ and $k \geq 1$ define $L_{\mathfrak{m}}(\psi^k, s) = \sum \psi^k(\mathfrak{b})/\mathrm{N}\mathfrak{b}^s$, where the sum is restricted to the ideals $\mathfrak{b}$ coprime to $\mathfrak{m}$. We similarly define $L_{\mathfrak{m}}(\bar{\psi}^k, s)$. The following theorem is due to Deuring.

Theorem 4.1 (Deuring; [4, Thm. 10.5 (a)])**.** *We have $L(E_{/K}, s) = L_{\mathfrak{f}}(\psi, s)L_{\mathfrak{f}}(\bar{\psi}, s)$.* □

Now we proceed to relate elliptic units with $L_{\mathfrak{f}}(\bar{\psi}^k, s)$ for $k \geq 1$.

Theorem 4.2. *For every $k \geq 1$,*

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

Proof. This proof is done in several steps. First it is possible to relate the kth derivative of $\log \Theta_{L,\mathfrak{a}}(z)$ with respect to z with the Eisenstein series $E_k(z,L) = \lim_{s\to k} \sum_{\omega\in L'} (\bar{z}+\bar{\omega})^k/|z+\omega|^{2s}$, where $\lim_{s\to k}$ denotes evaluation at the analytic continuation. This is done in [1, Thm. 7.13]. Then, [1, Prop. 7.15] shows how to relate $E_k(z,L)$ with partial sums of $L_{\mathfrak{f}}(\bar{\psi},k)$. Finally, since $\log \Lambda_{L,\mathfrak{a}}(z)$ is a sum of translates of $\log \Theta_{L,\mathfrak{a}}(z)$ (see Definition 3.2), it is possible to add all partial sums of $L_{\mathfrak{f}}(\bar{\psi},k)$ to obtain the desired theorem (see [1, Thm. 7.17]). □

Let $\mathfrak{p}$ be a prime of K above p where E has good reduction and $\mathfrak{p} \nmid 6\mathfrak{f}$. Fix a Weierstrass model for E with coordinate functions x, y that has good reduction at $\mathfrak{p}$ and fix $\mathfrak{a}$ an ideal coprime to $6\mathfrak{f}\mathfrak{p}$. Let $\hat{E}$ be the formal group attached to E and let $x(Z) \in z^{-2}\mathcal{O}_{\mathfrak{p}}[[Z]], y(Z) \in z^{-3}\mathcal{O}_{\mathfrak{p}}[[Z]]$ be the power series corresponding to x and y as in [5, Chap. IV, §1]. Let $\lambda_{\hat{E}}(Z) \in Z + Z^2 K_{\mathfrak{p}}[[Z]]$ be the logarithm map of the formal group $\hat{E}$ (see [5, Chap. IV, §1]) and consider the operator $D = \frac{1}{\lambda'_{\hat{E}}(Z)}\frac{d}{dZ}$. Denote by $K(E)$ the function field of E and by identifying the coordinates (x,y) with $(x(Z),y(Z))$ and with $(\wp(z),\wp'(z)/2)$, where $\wp$ is the Weierstrass $\wp$-function. We have the following commutative diagram (see [1, Prop. 7.20]).

$$\begin{array}{ccccccc} K(\wp(z),\wp'(z)) & \longleftarrow & K(E) & \longrightarrow & K(x(Z),y(Z)) & \longrightarrow & K_{\mathfrak{p}}((Z)) \\ \downarrow{\scriptstyle \frac{d}{dz}} & & \downarrow & & \downarrow{\scriptstyle D} & & \downarrow{\scriptstyle D} \\ K(\wp(z),\wp'(z)) & \longleftarrow & K(E) & \longrightarrow & K(x(Z),y(Z)) & \longrightarrow & K_{\mathfrak{p}}((Z)). \end{array} \tag{5}$$

Theorem 4.3. *Denote by $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \in K_{\mathfrak{p}}((Z))$ the image of $\Lambda_{E,\mathfrak{a}} \in K((E))$ by the map given in (5). Then, $\Lambda_{\mathfrak{p},\mathfrak{a}} \in \mathcal{O}_{\mathfrak{p}}[[Z]]^\times$ and for every $k \geq 1$*

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

Proof. The first statement is proven in [1, Thm. 7.22] while the second one follows from the fact that (5) is commutative and Theorem 4.2. □

Suppose here and from now on that $p > 7$ and p splits in K. Then, we can suppose that $\mathrm{N}\mathfrak{a} \neq \psi(\mathfrak{a})$ modulo $\mathfrak{p}$ (for every $\mathfrak{p}$ such that $p > 7$ such an $\mathfrak{a}$ exists by [1, Lem. 10.2]). Let $F = K_1 = K(E[\mathfrak{p}])$, which is totally ramified at $\mathfrak{p}$ and let $\mathfrak{P}$ be the unique prime above $\mathfrak{p}$. Consider $\eta(1,\mathcal{O}) = \Lambda_{L,\mathfrak{a}}(\psi(\mathfrak{p})^{-1}\Omega) = \Lambda_{\mathfrak{p},\mathfrak{a}}(z) \in \mathcal{O}_F^\times$. Let $\delta\colon \mathcal{O}_{F_{\mathfrak{P}}}^\times \to (1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}})/(1+\mathfrak{P}^2\mathcal{O}_{F_{\mathfrak{P}}})$ be the natural projection, which is Δ-equivariant.

Proposition 4.4. *$L_{\mathfrak{f}}(E,1)/\Omega$ is integral at $\mathfrak{p}$. Moreover, $\delta(\eta(1,\mathcal{O})) = 1$ if and only if $L(\bar{\psi},1)/\Omega \equiv 0 \mod \mathfrak{p}$. In particular, $L(\bar{\psi},1)/\Omega \not\equiv 0 \mod \mathfrak{p}$ implies that $\eta(1,\mathcal{O})^{\chi_E} \notin ((\mathcal{O}_{F,\mathfrak{P}}^\times)^{\chi_E})^p$.*

Proof. Let $P = \xi(\psi(\mathfrak{p})^{-1}\Omega) = (x,y)$ and $z = -x/y$. It follows from [1, Lem. 7.3] that $z = -y/x \in \mathcal{O}_{F,\mathfrak{P}}$ has valuation 1 at the prime $\mathfrak{P}$. Theorem 4.3 allows to write $\eta(1,\mathcal{O}) = \Lambda_{\mathfrak{p},\mathfrak{a}}(z)$ as a power series on z. The first terms are

$$\Lambda_{\mathfrak{p},\mathfrak{a}}(z) = \Lambda_{\mathfrak{p},\mathfrak{a}}(0) + \Lambda_{\mathfrak{a},\mathfrak{a}}(0)12f(\mathrm{N}\mathfrak{a} - \psi(\mathfrak{a}))\frac{L_{\mathfrak{f}}(\bar{\psi},1)}{\Omega}z + O(z^2). \tag{6}$$

Since $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \in \mathcal{O}_{\mathfrak{p}}[[Z]]^\times$ we have that $\Lambda_{\mathfrak{p},\mathfrak{a}}(0) \in \mathcal{O}_{\mathfrak{p}}^\times$. Since $\mathfrak{a}$ is chosen so that $\mathrm{N}\mathfrak{a} \neq \psi(\mathfrak{a})$ modulo $\mathfrak{p}$ we have $\Lambda_{\mathfrak{p},\mathfrak{a}}(0)12f(\mathrm{N}\mathfrak{a} - \psi(\mathfrak{a})) \in \mathcal{O}_{\mathfrak{p}}^\times$ which shows that $L_{\mathfrak{f}}(\bar{\psi},1)/\Omega$ is integral at $\mathfrak{p}$.

To prove the second part of the statement we need to compute the projection of $\Lambda_{\mathfrak{p},\mathfrak{a}}(z)$ in $(1+\mathfrak{P}\mathcal{O}_{F,\mathfrak{P}})/(1+\mathfrak{P}^2\mathcal{O}_{F,\mathfrak{P}})$. Since $\mathrm{ord}_{\mathfrak{P}}(z)=1$, (6) reduces to

$$\eta(1,\mathcal{O}) \equiv \Lambda_{\mathfrak{p},\mathfrak{a}}(0)\left(1+12f(\mathrm{N}\mathfrak{a}-\psi(\mathfrak{a}))\frac{L_{\mathfrak{f}}(\bar{\psi},1)}{\Omega}z\right) \mod \mathfrak{P}^2.$$

Using again that $\Lambda_{\mathfrak{p},\mathfrak{a}}(0)\in\mathcal{O}_{\mathfrak{p}}^{\times}$ and that $\mathfrak{p}$ is totally ramified in F it follows that $\delta(\Lambda_{\mathfrak{p},\mathfrak{a}}(0))=1$. Hence, $\delta(\eta(1,\mathcal{O}))=1+12f(\mathrm{N}\mathfrak{a}-\psi(\mathfrak{a}))\frac{L(\bar{\psi},1)}{\Omega}z$ and the second result follows. Finally, the study of the formal group $\hat{E}$ gives a Δ-equivariant isomorphism $(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}})/(1+\mathfrak{P}^2\mathcal{O}_{F_{\mathfrak{P}}})\simeq E[\mathfrak{p}]$ (see [1, Lem. 10.4]). From there we see that $\delta(\eta(1,\mathcal{O})^{\chi_E})=\delta(\eta(1,\mathcal{O}))^{\chi_E}=\delta(\eta(1,\mathcal{O}))\neq 0$. Thus $\eta(1,\mathcal{O})^{\chi_E}\notin((\mathcal{O}_{F,\mathfrak{P}}^{\times})^{\chi_E})^p$, since otherwise its image by δ would be 1 (because $(1+\mathfrak{P}\mathcal{O}_{F_{\mathfrak{P}}})/(1+\mathfrak{P}^2\mathcal{O}_{F_{\mathfrak{P}}})$ is killed by $\mathrm{N}\mathfrak{P}=\mathrm{N}\mathfrak{p}\mid p$). □

Theorem 4.5. *Suppose that* $L(\bar{\psi},1)/\Omega\not\equiv 0 \mod \mathfrak{p}$ *and that* $\mathrm{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p})\neq 1$. *Let* δ_1 *be as in Definition 2.7. Then,* $\delta_1(\mathcal{O}_F^{\times})\neq 0$.

Proof. By Lemma 2.8 it is enough to see that $(\mathcal{O}_F^{\times})^{\chi_E}\twoheadrightarrow(\mathcal{O}_{F,\mathfrak{P}}^{\times})^{\chi_E}$. For that we make the following observation. Using the p-adic logarithm we see that $(\mathcal{O}_{F,\mathfrak{P}}^{\times}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p)^{\chi_E}$ is 1-dimensional (recall that χ_E is 1-dimensional). Moreover, since $\mathrm{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p})\neq 1$ it can be seen that $\mu_p\not\subset\mathcal{O}_{F,\mathfrak{P}}^{\times}$ (see [1, Lem. 10.9 (i)]). Therefore, $(\mathcal{O}_{F,\mathfrak{P}}^{\times})^{\chi_E}$ is free of rank 1 over $\mathbb{Z}_p$. Since $\eta(1,\mathcal{O})^{\chi_E}\notin((\mathcal{O}_{F,\mathfrak{P}}^{\times})^{\chi_E})^p$ by Proposition 4.4, $\eta(1,\mathcal{O})^{\chi_E}\in\mathcal{O}_F^{\times}$ is a generator of $(\mathcal{O}_{F,\mathfrak{P}})^{\chi_E}$ giving the desired surjectivity. □

We can finally give the proof of the Coates–Wiles Theorem.

Theorem 4.6 (Coates–Wiles)**.** *Suppose that* $L(E_{/K},1)\neq 0$. *Then* $E(K)$ *is finite.*

Proof. Theorem 4.1 shows that $L_{\mathfrak{f}}(\bar{\psi},1)\neq 0$. By the Chebotarev Theorem there are infinite primes $\mathfrak{p}$ of K above a rational prime p such that p splits in K and $\mathrm{Tr}_{K/\mathbb{Q}}\psi(\mathfrak{p})\neq 1$. We can choose one such that $p>7$, $\mathfrak{p}$ coprime to $6\mathfrak{f}$ and $L_{\mathfrak{f}}(\bar{\psi},1)/\Omega$ is a unit at $\mathfrak{p}$.

Therefore we can apply the previous results of this section to $\mathfrak{p}$. Since $\mu_p\notin F_{\mathfrak{P}}$ by [1, Lem. 10.9 (i)], by Proposition 4.4 and Corollary 3.15, $A^{\chi_E}=0$. In addition, Theorem 4.5 shows that $\delta_1(\mathcal{O}_F^{\times})\neq 0$. The conditions of Corollary 2.10 are satisfied so we can affirm $S_{\pi}(E_{/K})=0$, where $\pi\in\mathcal{O}$ such that $\mathfrak{p}=\pi\mathcal{O}$. Therefore $E(K)/\mathfrak{p}E(K)=0$, by the Mordell–Weil Theorem $E(K)$ has to be finite (see Proposition 2.3) and we are done. □

Expression of gratitude

I would like to start expressing my very great appreciation to Francesc Fité. He has been extremely generous with his time as well as patient when giving me advice about the project. I would also like to thank Christopher Skinner for giving me the opportunity of visiting Princeton University for 6 months and for being available whenever I needed. My thanks are also extended to Victor Rotger for suggesting me to work on this project. I would also like to thank the referee for a careful reading of the manuscript and for giving useful corrections and suggestions.

References

[1] K. Rubin. Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer, in: *Arithmetic theory of elliptic curves* (Cetraro, 1997), Lecture Notes in Math. **1716**, Springer, Berlin, 1999, 167–234.

[2] K. Rubin. *Euler Systems*, Princeton University Press, 2000.

[3] J.-P. Serre. *Local fields*, Graduate Texts in Mathematics **67**, Springer Science & Business Media, 2013.

[4] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer Science & Business Media, 1994.

[5] J.H. Silverman. *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer Science & Business Media, 2009.