Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer

Karl Rubin[⋆] [⋆⋆]

Department of Mathematics, Ohio State University, 231 W. 18 Avenue,
Columbus, Ohio 43210 USA, rubin@math.ohio-state.edu

The purpose of these notes is to present a reasonably self-contained exposition of recent results concerning the Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication. The goal is the following theorem.

Theorem. *Suppose E is an elliptic curve defined over an imaginary quadratic field K, with complex multiplication by K, and $L(E,s)$ is the L-function of E. If $L(E,1) \neq 0$ then*

(i) *$E(K)$ is finite,*
(ii) *for every prime $p > 7$ such that E has good reduction above p, the p-part of the Tate-Shafarevich group of E has the order predicted by the Birch and Swinnerton-Dyer conjecture.*

The first assertion of this theorem was proved by Coates and Wiles in [CW1]. We will prove this in §10 (Theorem 10.1). A stronger version of (ii) (with no assumption that E have good reduction above p) was proved in [Ru2]. The program to prove (ii) was also begun by Coates and Wiles; it can

[⋆] Partially supported by the National Science Foundation. The author also gratefully acknowledges the CIME for its hospitality.

[⋆⋆] current address: Department of Mathematics, Stanford University, Stanford, CA 94305 USA, rubin@math.stanford.edu

now be completed thanks to the recent Euler system machinery of Kolyvagin [Ko]. This proof will be given in §12, Corollary 12.13 and Theorem 12.19.

The material through §4 is background which was not in the Cetraro lectures but is included here for completeness. In those sections we summarize, generally with references to [Si] instead of proofs, the basic properties of elliptic curves that will be needed later. For more details, including proofs, see Silverman's book [Si], Chapter 4 of Shimura's book [Sh], Lang's book [La], or Cassels' survey article [Ca].

The content of the lectures was essentially §§5-12.

1 Quick Review of Elliptic Curves

1.1 Notation

Suppose F is a field. An elliptic curve E defined over F is a nonsingular curve defined by a generalized Weierstrass equation

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

with $a_1, a_2, a_3, a_4, a_6 \in F$. The points $E(F)$ have a natural, geometrically-defined group structure, with the point at infinity O as the identity element. The discriminant $\Delta(E)$ is a polynomial in the a_i and the j-invariant $j(E)$ is a rational function in the a_i. (See §III.1 of [Si] for explicit formulas.) The j-invariant of an elliptic curve depends only on the isomorphism class of that curve, but the discriminant Δ depends on the particular Weierstrass model.

Example 1.1. Suppose that E is defined by a Weierstrass equation

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

and $d \in F^\times$. The *twist of E by $\sqrt{d}$* is the elliptic curve E_d defined by

$$y^2 = x^3 + a_2dx^2 + a_4d^2x + a_6d^3.$$

Then (exercise:) E_d is isomorphic to E over the field $F(\sqrt{d})$, $\Delta(E_d) = d^6\Delta(E)$, and $j(E_d) = j(E)$. See also the proof of Corollary 5.22.

1.2 Differentials

See [Si] §II.4 for the definition and basic background on differentials on curves.

Proposition 1.2. *Suppose E is an elliptic curve defined by a Weierstrass equation* (1). *Then the space of holomorphic differentials on E defined over F is a one-dimensional vector space over F with basis*

$$\omega_E = \frac{dx}{2y + a_1x + a_3}.$$

Further, ω_E is invariant under translation by points of $E(\bar{F})$.

Proof. See [Si] Propositions III.1.5 and III.5.1. That ω_E is holomorphic is an exercise, using that ω_E is also equal to $dy/(3x^2 + 2a_2x + a_4 - a_1y)$. □

1.3 Endomorphisms

Definition 1.3. Suppose E is an elliptic curve. An *endomorphism* of E is a morphism from E to itself which maps O to O.

An endomorphism of E is also a homomorphism of the abelian group structure on E (see [Si] Theorem III.4.8).

Example 1.4. For every integer m, multiplication by m on E is a endomorphism of E, which we will denote by $[m]$. If $m \neq 0$ then the endomorphism $[m]$ is nonzero; in fact, it has degree m^2 and, if m is prime to the characteristic of F then the kernel of $[m]$ is isomorphic to $(\mathbf{Z}/m\mathbf{Z})^2$. (See [Si] Proposition III.4.2 and Corollary III.6.4.)

Example 1.5. Suppose F is finite, $\#(F) = q$. Then the map $\varphi_q : (x, y, z) \mapsto (x^q, y^q, z^q)$ is a (purely inseparable) endomorphism of E, called the q-th power Frobenius morphism.

Definition 1.6. If E is an elliptic curve defined over F, we write $\mathrm{End}_F(E)$ for the ring (under addition and composition) of endomorphisms of E defined over F. Then $\mathrm{End}_F(E)$ has no zero divisors, and by Example 1.4 there is an injection $\mathbf{Z} \hookrightarrow \mathrm{End}_F(E)$.

Definition 1.7. Write $\mathcal{D}(E/F)$ for one-dimensional vector space (see Proposition 1.2) of holomorphic differentials on E defined over F. The map $\phi \mapsto \phi^*$ defines a homomorphism of abelian groups

$$\iota = \iota_F : \mathrm{End}_F(E) \to \mathrm{End}_F(\mathcal{D}(E/F)) \cong F.$$

The kernel of ι is the ideal of inseparable endomorphisms. In particular if F has characteristic zero, then ι_F is injective.

Lemma 1.8. *Suppose* $\mathrm{char}(F) = 0$*, L is a field containing F, and $\phi \in \mathrm{End}_L(E)$. If $\iota_L(\phi) \in F$ then $\phi \in \mathrm{End}_F(E)$.*

Proof. If $\sigma \in \mathrm{Aut}(\bar{L}/F)$ then

$$\iota_L(\phi^\sigma) = \sigma(\iota_L(\phi)) = \iota_L(\phi).$$

Since L has characteristic zero, ι_L is injective so we conclude that $\phi^\sigma = \phi$. □

Definition 1.9. If $\phi \in \mathrm{End}_F(E)$ we will write $E[\phi] \subset E(\bar{F})$ for the the kernel of ϕ and $F(E[\phi])$ for the extension of F generated by the coordinates of the points in $E[\phi]$. Note that $F(E[\phi])$ is independent of the choice of a Weierstrass model of E over F. By [Si] Theorem III.4.10, $\#(E[\phi])$ divides $\deg(\phi)$, with equality if and only if ϕ is separable.

Definition 1.10. If ℓ is a rational prime define the ℓ-adic *Tate module* of E

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

inverse limit with respect to the maps $\ell : E[\ell^{n+1}] \to E[\ell^n]$. If $\ell \neq \mathrm{char}(F)$ then Example 1.4 shows that

$$T_\ell(E) \cong \mathbf{Z}_\ell^2.$$

The Galois group G_F acts $\mathbf{Z}_\ell$-linearly on $T_\ell(E)$, giving a representation

$$\rho_\ell : G_F \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbf{Z}_\ell)$$

when $\ell \neq \mathrm{char}(F)$.

Theorem 1.11. *If E is an elliptic curve then $\mathrm{End}_F(E)$ is one of the following types of rings.*

(i) $\mathbf{Z}$,
(ii) *an order in an imaginary quadratic field,*
(iii) *an order in a division quaternion algebra over $\mathbf{Q}$.*

Proof. See [Si] §III.9. □

Example 1.12. Suppose $\mathrm{char}(F) \neq 2$ and E is the curve $y^2 = x^3 - dx$ where $d \in F^\times$. Let ϕ be defined by $\phi(x, y) = (-x, iy)$ where $i = \sqrt{-1} \in \bar{F}$. Then $\phi \in \mathrm{End}_{\bar{F}}(E)$, and $\iota(\phi) = i$ so $\phi \in \mathrm{End}_F(E) \Leftrightarrow i \in F$. Also, ϕ has order 4 in $\mathrm{End}_{\bar{F}}(E)^\times$ so we see that $\mathbf{Z}[\phi] \cong \mathbf{Z}[i] \subset \mathrm{End}_{\bar{F}}(E)$. (In fact, $\mathbf{Z}[\phi] = \mathrm{End}_{\bar{F}}(E)$ if $\mathrm{char}(F) = 0$ or if $\mathrm{char}(F) \equiv 1 \pmod 4$, and $\mathrm{End}_{\bar{F}}(E)$ is an order in a quaternion algebra if $\mathrm{char}(F) \equiv 3 \pmod 4$.) The next lemma gives a converse to this example.

Lemma 1.13. *Suppose E is given by a Weierstrass equation $y^2 = x^3 + ax + b$. If $\mathrm{Aut}(E)$ contains an element of order 4 (resp. 3) then $b = 0$ (resp. $a = 0$).*

Proof. The only automorphisms of such a Weierstrass elliptic curve are of the form $(x, y) \mapsto (u^2 x, u^3 y)$ (see [Si] Remark III.1.3). The order of such an automorphism is the order of u in $F^\times$, and when u has order 3 or 4 this change of variables preserves the equation if and only if $a = 0$ (resp. $b = 0$). □

2 Elliptic Curves over C

Remark 2.1. Note that an elliptic curve defined over a field of characteristic zero can be defined over $\mathbf{Q}[a_1, a_2, a_3, a_4, a_6]$, and this field can be embedded in $\mathbf{C}$. In this way many of the results of this section apply to all elliptic curves in characteristic zero.

2.1 Lattices

Definition 2.2. Suppose L is a lattice in $\mathbf{C}$. Define the Weierstrass $\wp$-function, the Weierstrass σ-function, and the Eisenstein series attached to L

$$\begin{aligned}\wp(z;L) &= \frac{1}{z^2} + \sum_{0\neq\omega\in L} \frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\\ \sigma(z;L) &= z \prod_{0\neq\omega\in L} \left(1-\frac{z}{\omega}\right) e^{(z/\omega)+(z/\omega)^2/2}\\ G_k(L) &= \sum_{0\neq\omega\in L} \frac{1}{\omega^k} \quad \text{for } k \text{ even, } k\geq 4.\end{aligned}$$

We will suppress the L from the notation in these functions when there is no danger of confusion. See [Si] Theorem VI.3.1, Lemma VI.3.3, and Theorem VI.3.5 for the convergence and periodicity properties of these functions.

Theorem 2.3. (i) *If L is a lattice in $\mathbf{C}$ then the map*

$$z \mapsto (\wp(z;L), \wp'(z;L)/2)$$

is an analytic isomorphism (and a group homomorphism) from $\mathbf{C}/L$ to $E(\mathbf{C})$ where E is the elliptic curve $y^2 = x^3 - 15G_4(L)x - 35G_6(L)$.

(ii) *Conversely, if E is an elliptic curve defined over $\mathbf{C}$ given by an equation $y^2 = x^3+ax+b$ then there is a unique lattice $L \subset \mathbf{C}$ such that $15G_4(L) = -a$ and $35G_6(L) = -b$, so (i) gives an isomorphism from $\mathbf{C}/L$ to $E(\mathbf{C})$.*

(iii) *The correspondence above identifies the holomorphic differential ω_E with dz.*

Proof. The first statement is Proposition VI.3.6 of [Si] and the second is proved in [Sh] §4.2. For (iii), we have that

$$dx/2y = d(\wp(z))/\wp'(z) = dz.$$

□

Remark 2.4. If E is the elliptic curve defined over $\mathbf{C}$ with a Weierstrass model $y^2 = x^3+ax+b$ and ω_E is the differential $dx/2y$ of Proposition 1.2, then the lattice L associated to E by Theorem 2.3(ii) is

$$\left\{\int_\gamma \omega_E : \gamma \in H_1(E,\mathbf{Z})\right\}$$

and the map

$$P \mapsto \int_O^P \omega_E$$

is the isomorphism from $E(\mathbf{C})$ to $\mathbf{C}/L$ which is the inverse of the map of Theorem 2.3(i).

Definition 2.5. If $L \subset \mathbf{C}$ is a lattice define

$$\begin{aligned} \Delta(L) &= (60G_4(L))^3 - 27(140G_6(L))^2 \\ j(L) &= -1728(60G_4(L))^3/\Delta(L). \end{aligned}$$

Then $\Delta(L)$ is the discriminant and $j(L)$ the j-invariant of the elliptic curve corresponding to L by Theorem 2.3.

Proposition 2.6. *Suppose E is an elliptic curve defined over $\mathbf{C}$, corresponding to a lattice L under the bijection of Theorem 2.3. Then the map ι of Definition 1.7 is an isomorphism*

$$\mathrm{End}_{\mathbf{C}}(E) \xrightarrow{\sim} \{\alpha \in \mathbf{C} : \alpha L \subset L\}.$$

Proof. See [Si] Theorem VI.4.1. □

Corollary 2.7. *If E is an elliptic curve defined over a field F of characteristic zero, then $\mathrm{End}_F(E)$ is either $\mathbf{Z}$ or an order in an imaginary quadratic field.*

Proof. If E is defined over a subfield of $\mathbf{C}$ then Proposition 2.6 identifies $\mathrm{End}_{\mathbf{C}}(E)$ with $\{\alpha \in \mathbf{C} : \alpha L \subset L\}$. The latter object is a discrete subring of $\mathbf{C}$, and hence is either $\mathbf{Z}$ or an order in an imaginary quadratic field.

Using the principle of Remark 2.1 at the beginning of this section, the same holds for all fields F of characteristic zero. □

The following table gives a dictionary between elliptic curves over an arbitrary field and elliptic curves over $\mathbf{C}$.

over abitrary field	over $\mathbf{C}$
(E, ω_E)	$(\mathbf{C}/L, dz)$
x, y	$\wp(z; L), \wp'(z; L)/2$
isomorphism class of E	$\{\alpha L : \alpha \in \mathbf{C}^\times\}$
$\mathrm{End}_{\mathbf{C}}(E)$	$\{\alpha \in \mathbf{C} : \alpha L \subset L\}$
$\mathrm{Aut}_{\mathbf{C}}(E)$	$\{\alpha \in \mathbf{C}^\times : \alpha L = L\}$
$E[m]$	$m^{-1}L/L$

3 Elliptic Curves over Local Fields

For this section suppose

- p is a rational prime,
- F is a finite extension of $\mathbf{Q}_p$,
- $\mathcal{O}$ is the ring of integers of F,
- $\mathfrak{p}$ is the maximal ideal of F,
- π is a generator of $\mathfrak{p}$
- $\Bbbk = \mathcal{O}/\mathfrak{p}$ is the residue field of $\mathcal{O}$
- $v : F \to \mathbf{Z} \cup \{\infty\}$ is the valuation on F, $v(\pi) = 1$.

We fix an elliptic curve E defined over F.

3.1 Reduction

Definition 3.1. A Weierstrass equation (1) for E is *minimal* if

- $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}$,
- the valuation of the discriminant of this equation is minimal in the set of valuations of all Weierstrass equations for E with coefficients in $\mathcal{O}$.

Every elliptic curve E has a minimal Weierstrass equation, or minimal model, and the *minimal discriminant* of E is the ideal of $\mathcal{O}$ generated by the discriminant of a minimal Weierstrass model of E.

The *reduction* $\tilde{E}$ of E is the curve defined over the residue field $\Bbbk$ by the Weierstrass equation

$$y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6 \tag{2}$$

where the a_i are the coefficients of a minimal Weierstrass equation for E and $\tilde{a}_i$ denotes the image of a_i in $\Bbbk$. The reduction $\tilde{E}$ is independent (up to isomorphism) of the particular minimal equation chosen for E (see [Si] Proposition VII.1.3(b)).

The curve $\tilde{E}$ may be singular, but it has at most one singular point ([Si] Proposition III.1.4(a)). In that case the quasi-projective curve

$$\tilde{E}_{\mathrm{ns}} = \tilde{E} - \{\text{singular point on } \tilde{E}\}$$

has a geometrically-defined group law just as an elliptic curve does (see [Si] Proposition III.2.5).

If Δ is the minimal discriminant of E, then one of the following three possibilities holds (see for example [Si] Proposition III.2.5):

(i) $\Delta \in \mathcal{O}^\times$ and $\tilde{E}$ is nonsingular, i.e., $\tilde{E} = \tilde{E}_{\mathrm{ns}}$ is an elliptic curve,
(ii) $\Delta \notin \mathcal{O}^\times$, $\tilde{E}$ is singular, and $\tilde{E}_{\mathrm{ns}}(\Bbbk) \cong \Bbbk^\times$, or
(iii) $\Delta \notin \mathcal{O}^\times$, $\tilde{E}$ is singular, and $\tilde{E}_{\mathrm{ns}}(\Bbbk) \cong \Bbbk$.

We say that E has *good* (resp. *multiplicative*, resp. *additive*) *reduction* if (i) (resp. (ii), resp. (iii)) is satisfied.

We say that E has *potentially good reduction* if there is a finite extension F' of F such that E has good reduction over F'.

Lemma 3.2. (i) *E has potentially good reduction if and only if $j(E) \in \mathcal{O}$.*
(ii) *If E has potentially good reduction then E has either good or additive reduction.*

Proof. See [Si] Propositions VII.5.4 and IV.5.5. □

Definition 3.3. There is a natural *reduction map*

$$\mathbf{P}^2(F) \to \mathbf{P}^2(\Bbbk).$$

By restriction this defines a reduction map from $E(F)$ to $\tilde{E}(\Bbbk)$. We define $E_0(F) \subset E(F)$ to be the inverse image of $\tilde{E}_{\mathrm{ns}}(\Bbbk)$ and $E_1(F) \subset E(F)$ to be the inverse image of $\tilde{O} \in \tilde{E}_{\mathrm{ns}}(\Bbbk)$.

Proposition 3.4. *There is an exact sequence of abelian groups*

$$0 \to E_1(F) \to E_0(F) \to \tilde{E}_{\mathrm{ns}}(\Bbbk) \to 0$$

where the map on the right is the reduction map. If E has good reduction then the reduction map induces an injective homomorphism

$$\mathrm{End}_F(E) \to \mathrm{End}_{\Bbbk}(\tilde{E}).$$

Proof. See [Si] Proposition VII.2.1. □

If E has good reduction and $\phi \in \mathrm{End}_F(E)$, we will write $\tilde{\phi}$ for the endomorphism of $\tilde{E}$ which is the reduction of ϕ.

Lemma 3.5. *If E is defined by a minimal Weierstrass equation then*

$$E_1(F) = \{(x, y) \in E(F) : v(x) < 0\} = \{(x, y) \in E(F) : v(y) < 0\}.$$

If $(x, y) \in E_1(F)$ then $3v(x) = 2v(y) < 0$.

Proof. It is clear from the definition of the reduction map that $(x, y, 1)$ reduces to $(0, 1, 0)$ if and only if $v(y) < 0$ and $v(y) < v(x)$. If $(x, y) \in E(F)$ then, since x and y satisfy a Weierstrass equation with coefficients in $\mathcal{O}$, it is clear that

$$v(x) < 0 \Leftrightarrow v(y) < 0$$

and in that case $v(y) = (3/2)v(x) < v(x)$. □

Lemma 3.6. *Suppose E has good reduction, $\phi \in \mathrm{End}_F(E)$, and $\tilde{\phi}$ is purely inseparable. Then*

(i) *$\tilde{\phi}$ is injective on $\tilde{E}(\Bbbk)$.*
(ii) $\ker(\phi) \subset E_1(F)$

Proof. Clear. □

3.2 The Formal Group

Theorem 3.7. *Fix a minimal Weierstrass model* (1) *of E. There is a formal group $\hat{E}$ defined by a power series $\mathcal{F}_E \in \mathcal{O}[[Z, Z']]$, and a power series*

$$w(Z) = Z^3 + a_1 Z^4 + (a_1^2 + a_2)Z^5 + \cdots \in \mathcal{O}[[Z]],$$

such that if we define

$$x(Z) = Z/w(Z) \in Z^{-2}\mathcal{O}[[Z]], \qquad y(Z) = -1/w(Z) \in Z^{-3}\mathcal{O}[[Z]]$$

then

(i) $(x(Z), y(Z)) \in E(\mathcal{O}((Z)))$,

(ii) $$(x(Z),y(Z))+(x(Z'),y(Z'))=(x(\mathcal{F}_E(Z,Z')),y(\mathcal{F}_E(Z,Z')))$$

as points on E with coordinates in the fraction field of $F((Z,Z'))$,

(iii) *there is a map $\operatorname{End}_F(E)\to\operatorname{End}(\hat{E})$ (which we will denote by $\phi\mapsto\boldsymbol{\phi}(Z)\in\mathcal{O}[[Z]]$) such that for every $\phi\in\operatorname{End}_F(E)$,*

$$\phi((x(Z),y(Z)))=(x(\boldsymbol{\phi}(Z)),y(\boldsymbol{\phi}(Z)))$$

in $E(F((Z)))$.

Proof. See [Ta] or [Si], §IV.1 for an explicit construction of the power series $w(Z)$ and $\mathcal{F}_E(Z,Z)$. The idea is that $Z=-x/y$ is a uniformizing parameter at the origin of E, and everything (x, y, the group law, endomorphisms) can be expanded as power series in Z. □

For every $n\geq 1$ write $\hat{E}(\mathfrak{p}^n)$ for the commutative group whose underlying set is $\mathfrak{p}^n$, with the operation $(z,z')\mapsto\mathcal{F}_E(z,z')$.

Corollary 3.8. *With notation as in Theorem 3.7,*

$$Z\mapsto(Z/w(Z),-1/w(Z))$$

is an isomorphism from $\hat{E}(\mathfrak{p})$ to $E_1(F)$ with inverse given by

$$(x,y)\mapsto -x/y.$$

Proof. See [Si] Proposition VII.2.2. The first map is a map into $E_1(F)$ by Lemma 3.5 and Theorem 3.7(i), and is a homomorphism by Theorem 3.7(ii). It is injective because the only zero of $w(Z)$ in $\mathfrak{p}$ is $Z=0$. The second map is clearly a left-inverse of the first, and it maps into $\mathfrak{p}$ by Lemma 3.5. We only need show that the second map is also one-to-one.

If we rewrite our Weierstrass equation for E with variables $w=-1/y$ and $z=-x/y$ we get a new equation

$$a_6w^3+(a_4z+a_3)w^2+(a_2z^2+a_1z-1)w+z^3=0.$$

Fix a value of $z\in\mathfrak{p}$ and consider the set S of roots w of this equation. If (z,w) corresponds to a point in $E_1(F)$ then by Lemma 3.5, $v(w)=v(z^3)>0$. It follows easily that S contains at most one root w corresponding to a point of $E_1(F)$, and hence the map $(x,y)\mapsto -x/y$ is one-to-one on $E_1(F)$. □

Corollary 3.9. *Suppose $\#(\Bbbk)=q$, E has good reduction, and $\phi\in\operatorname{End}_K(E)$ reduces to the Frobenius endomorphism $\varphi_q\in\operatorname{End}_{\Bbbk}(\tilde{E})$. Then*

$$\boldsymbol{\phi}(Z)\equiv Z^q\pmod{\mathfrak{p}\mathcal{O}[[Z]]}.$$

Proof. If the reduction of ϕ is φ_q then by Theorem 3.7(iii)

$$\begin{aligned}(x(\boldsymbol{\phi}(Z)), y(\boldsymbol{\phi}(Z))) = \phi((x(Z), y(Z))) &\equiv (x(Z)^q, y(Z)^q) \\ &\equiv (x(Z^q), y(Z^q)) \pmod{\mathfrak{p}\mathcal{O}((Z))}.\end{aligned}$$

Since $y(Z)$ is invertible in $\mathcal{O}((Z))$, we conclude that

$$\boldsymbol{\phi}(Z) = -x(\boldsymbol{\phi}(Z))/y(\boldsymbol{\phi}(Z)) \equiv -x(Z^q)/y(Z^q) = Z^q \pmod{\mathfrak{p}\mathcal{O}((Z))}.$$

□

Definition 3.10. Recall that

$$\omega_E = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

is the holomorphic, translation-invariant differential on E from Proposition 1.2. Define

$$\hat{\omega}(Z) = \frac{\frac{d}{dZ}x(Z)}{2y(Z) + a_1x(Z) + a_3} \in 1 + Z\mathcal{O}[[Z]].$$

Let $\lambda_{\hat{E}}(Z)$ be the unique element of $Z + Z^2F[[Z]]$ such that $\frac{d}{dZ}\lambda_{\hat{E}}(Z) = \hat{\omega}(Z)$.

Lemma 3.11. (i) *The power series $\lambda_{\hat{E}}$ is the logarithm map of $\hat{E}$, the isomorphism from $\hat{E}$ to the additive formal group $\mathbf{G}_a$ such that $\lambda'_E(0) = 1$.*

(ii) *The power series $\lambda_{\hat{E}}$ converges on $\mathfrak{p}$. If $\mathrm{ord}_{\mathfrak{p}}(p) < p - 1$ then $\lambda_{\hat{E}}$ is an isomorphism from $\hat{E}(\mathfrak{p})$ to the additive group $\mathfrak{p}$.*

Proof. Let $\mathcal{F}_E \in \mathcal{O}[[Z, Z']]$ be the addition law for $\hat{E}$. We need to show that

$$\lambda_E(\mathcal{F}_E(Z, Z')) = \lambda_E(Z) + \lambda_E(Z').$$

Since ω_E is translation invariant (Proposition 1.2),

$$\hat{\omega}(\mathcal{F}_E(Z, Z'))d(\mathcal{F}_E(Z, Z')) = \hat{\omega}(Z)dZ$$

and therefore

$$\tfrac{d}{dZ}\lambda_E(\mathcal{F}_E(Z, Z')) = \tfrac{d}{dZ}\lambda_E(Z).$$

Therefore $\lambda_E(\mathcal{F}_E(Z, Z')) = \lambda_E(Z) + c(Z')$ with $c(Z') \in F[[Z']]$. Evaluating at $Z = 0$ shows $c(Z') = \lambda_E(Z')$ as desired.

The uniqueness of the logarithm map and (ii) are standard elementary results in the theory of formal groups. □

Definition 3.12. Define $\lambda_E : E_1(F) \to F$ to be the composition of the inverse of the isomorphism of Corollary 3.8 with $\lambda_{\hat{E}}$.

Corollary 3.13. *If $\mathrm{ord}_{\mathfrak{p}}(p) < p-1$ then $\lambda_E : E_1(F) \to \mathfrak{p}$ is an isomorphism.*

Proof. This is immediate from Lemma 3.11. □

Recall the map $\iota : \mathrm{End}_F(E) \to F$ of Definition 1.7 defined by the action of an endomorphism on holomorphic differentials.

Proposition 3.14. *For every $\phi \in \mathrm{End}_F(E)$, $\boldsymbol{\phi}(Z) = \iota(\phi)Z + O(Z^2)$.*

Proof. By definition of ι, $\hat{\omega}(\boldsymbol{\phi}(Z)) = \iota(\phi)\hat{\omega}(Z)$, i.e.,

$$\frac{d(x(\boldsymbol{\phi}(Z)))}{2y(\boldsymbol{\phi}(Z)) + a_1x(\boldsymbol{\phi}(Z)) + a_3} = \iota(\phi)\frac{d(x(Z))}{2y(Z) + a_1x(Z) + a_3}.$$

Using the definitions of $x(Z)$ and $y(Z)$, the right-hand side is $(\iota(\phi)+O(Z))dZ$, and the left-hand side is $(\boldsymbol{\phi}'(0) + O(Z))dZ$. This completes the proof. □

3.3 Applications to Torsion Subgroups

Theorem 3.15. *Suppose $\phi \in \mathrm{End}_F(E)$ and $\iota(\phi) \in \mathcal{O}^\times$.*

(i) *ϕ is an automorphism of $E_1(F)$.*
(ii) *If E has good reduction then the reduction map $E[\phi] \cap E(F) \to \tilde{E}(\Bbbk)$ is injective.*

Proof. By definition of a formal group, $\mathcal{F}_E(X, Y) = X + Y + O(X^2, XY, Y^2)$. Using Proposition 3.14, for every $n \geq 1$ we have a commutative diagram

$$\begin{tikzcd}
\hat{E}(\mathfrak{p}^n)/\hat{E}(\mathfrak{p}^{n+1}) \arrow[r, "\sim"] \arrow[d, "\boldsymbol{\phi}"'] & \mathfrak{p}^n/\mathfrak{p}^{n+1} \arrow[r, "\sim"] \arrow[d, "\iota(\phi)"'] & \Bbbk \arrow[d, "\iota(\phi)"'] \\
\hat{E}(\mathfrak{p}^n)/\hat{E}(\mathfrak{p}^{n+1}) \arrow[r, "\sim"] & \mathfrak{p}^n/\mathfrak{p}^{n+1} \arrow[r, "\sim"] & \Bbbk
\end{tikzcd}$$

Since $\iota(\phi) \in \mathcal{O}^\times$ we see that $\boldsymbol{\phi}$ is an automorphism of $\hat{E}(\mathfrak{p}^n)/\hat{E}(\mathfrak{p}^{n+1})$ for every $n \geq 1$, and from this it is not difficult to show that $\boldsymbol{\phi}$ is an automorphism of $\hat{E}(\mathfrak{p})$. Therefore by Corollary 3.8, ϕ is an automorphism of $E_1(F)$. This proves (i), and (ii) as well since $E_1(F)$ is the kernel of the reduction map and (i) shows that $E_1(F) \cap E[\phi] = 0$. □

Remark 3.16. Theorem 3.15 shows in particular that if E has good reduction and m is prime to p, then the reduction map $E[m] \to \tilde{E}[m]$ is injective.

Corollary 3.17. *Suppose E has good reduction, $\phi \in \mathrm{End}_F(E)$, and $\iota(\phi) \in \mathcal{O}^\times$. If $P \in E(\bar{F})$ and $\phi(P) \in E(F)$, then $F(E[\phi], P)/F$ is unramified.*

Proof. Let $F' = F(E[\phi], P)$ and let $\Bbbk'$ be its residue field. Then F'/F is Galois and we let $I \subset \mathrm{Gal}(F'/F)$ denote the inertia group.

Suppose $\sigma \in I$. Then the reduction $\tilde{\sigma}$ of σ is the identity on $\Bbbk'$, so if $R \in E(\bar{F})$ and $\phi(R) \in E(F)$ then $\sigma R - R \in E[\phi]$ and

$$\widetilde{\sigma R - R} = \tilde{\sigma}\tilde{R} - \tilde{R} = 0.$$

By Theorem 3.15(ii), since $\iota(\phi) \in \mathcal{O}^\times$ we conclude that $\sigma R = R$. In other words σ fixes $E[\phi]$ and P, so σ fixes F', i.e., $\sigma = 1$. Hence I is trivial and F'/F is unramified. □

Corollary 3.18. *Suppose $\ell \neq p$, and let I denote the inertia subgroup of G_F.*

(i) *If E has good reduction then I acts trivially on $T_\ell(E)$.*

(ii) *If E has potentially good reduction then I acts on $T_\ell(E)$ through a finite quotient.*

Proof. This is clear by Corollary 3.17. □

The converse of Corollary 3.18 is the following.

Theorem 3.19 (Criterion of Néron-Ogg-Shafarevich). *Let $I \subset G_F$ denote the inertia group.*

(i) *If $\ell \neq p$ and I acts trivially on $T_\ell(E)$, then E has good reduction.*

(ii) *If $\ell \neq p$ and $T_\ell(E)^I \neq 0$, then E has good or multiplicative reduction.*

Proof. See [Si] Theorem VII.7.1 for (i).. The proof of (ii) is the same except that we use the fact that if E has additive reduction, then over any unramified extension F' of F with residue field $\Bbbk'$, $\tilde{E}_{\mathrm{ns}}(\Bbbk')$ is killed by p and hence has no points of order ℓ. □

4 Elliptic Curves over Number Fields

For this section suppose F is a number field and E is an elliptic curve defined over F. Our main interest is in studying the Mordell-Weil group $E(F)$.

If $\mathfrak{q}$ is a prime of F we say that E has *good* (resp. *potentially good*, *bad*, *additive*, *multiplicative*) *reduction* at $\mathfrak{q}$ if E, viewed as an elliptic curve over the local field $F_\mathfrak{q}$ (F completed at $\mathfrak{q}$) does. We will write $\mathit{\Delta}(E)$ for the minimal discriminant of E, the ideal of F which is the product over all primes $\mathfrak{q}$ of the minimal discriminant of E over $F_\mathfrak{q}$. This is well-defined because (every Weierstrass model of) E has good reduction outside of a finite set of primes.

Since F has characteristic zero, the map $\iota : \mathrm{End}_F(E) \to F$ of Definition 1.7 (giving the action of $\mathrm{End}_F(E)$ on differentials) is injective, and from now on we will *identify* $\mathrm{End}_F(E)$ with its image $\mathcal{O} \subset F$. By Corollary 2.7, $\mathcal{O}$ is either $\mathbf{Z}$ or an order in an imaginary quadratic field.

If $\alpha \in \mathcal{O}$ we will also write α for the corresponding endomorphism of E, so $E[\alpha] \subset E(\bar{F})$ is the kernel of α and $F(E[\alpha])$ is the extension of F generated by the coordinates of the points in $E[\alpha]$.

Definition 4.1. Suppose $\alpha \in \mathcal{O}$, $\alpha \neq 0$. Multiplication by α is surjective on $E(\bar{F})$, so there is an exact sequence

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

Taking G_F-cohomology yields a long exact sequence

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

where $H^1(F, E) = H^1(F, E(\bar{F}))$. We can rewrite this as

$$0 \to E(F)/\alpha E(F) \to H^1(F, E[\alpha]) \to H^1(F, E)_\alpha \to 0 \tag{3}$$

where $H^1(F, E)_\alpha$ denotes the kernel of α on $H^1(F, E)$. Concretely, the connecting map $E(F)/\alpha E(F) \hookrightarrow H^1(F, E[\alpha])$ is the "Kummer theory" map defined by

$$P \mapsto (\sigma \mapsto \sigma Q - Q) \tag{4}$$

where $Q \in E(\bar{F})$ satisfies $\alpha Q = P$.

In exactly the same way, if $\mathfrak{q}$ is a prime (finite or infinite) of F we can replace F by the completion $F_\mathfrak{q}$ in (3), and this leads to the diagram

$$\begin{tikzcd}
0 \arrow[r] & E(F)/\alpha E(F) \arrow[r] \arrow[d] & H^1(F, E[\alpha]) \arrow[r] \arrow[d, "\mathrm{res}_\mathfrak{q}"] & H^1(F, E)_\alpha \arrow[r] \arrow[d, "\mathrm{res}_\mathfrak{q}"] & 0 \\
0 \arrow[r] & E(F_\mathfrak{q})/\alpha E(F_\mathfrak{q}) \arrow[r] & H^1(F_\mathfrak{q}, E[\alpha]) \arrow[r] & H^1(F_\mathfrak{q}, E)_\alpha \arrow[r] & 0.
\end{tikzcd} \tag{5}$$

We define the *Selmer group* (relative to α)

$$\mathcal{S}_\alpha(E) = \mathcal{S}_\alpha(E_{/F}) \subset H^1(F, E[\alpha])$$

by

$$\begin{aligned}
\mathcal{S}_\alpha(E) &= \{c \in H^1(F, E[\alpha]) : \mathrm{res}_\mathfrak{q}(c) \in \mathrm{image}(E(F_\mathfrak{q})/\alpha E(F_\mathfrak{q})) \text{ for every } \mathfrak{q}\} \\
&= \{c \in H^1(F, E[\alpha]) : \mathrm{res}_\mathfrak{q}(c) = 0 \text{ in } H^1(F_\mathfrak{q}, E) \text{ for every } \mathfrak{q}\}.
\end{aligned}$$

Proposition 4.2. *Suppose $\alpha \in \mathcal{O}$, $\alpha \neq 0$. Under the Kummer map* (3), *$\mathcal{S}_\alpha(E)$ contains the image of $E(F)/\alpha E(F)$.*

Proof. Clear. □

Remark 4.3. One should think of the Selmer group $\mathcal{S}_\alpha(E)$ as the smallest subgroup of $H^1(F, E[\alpha])$ defined by natural local conditions which contains the image of $E(F)/\alpha E(F)$.

Proposition 4.4. *Suppose $\alpha \in \mathcal{O}$, $\alpha \neq 0$. Then the Selmer group $\mathcal{S}_\alpha(E)$ is finite.*

Proof. Suppose first that $E[\alpha] \subset E(F)$, so $H^1(F, E[\alpha]) = \mathrm{Hom}(G_F, E[\alpha])$. Let L be the maximal abelian extension of F of exponent $\deg(\alpha)$ which is unramified outside of the (finite) set of primes

$$\Sigma_{E,\alpha} = \{\mathfrak{p} \text{ of } F : \mathfrak{p} \text{ divides } \alpha\Delta(E) \text{ or } \mathfrak{p} \text{ is infinite}\}.$$

If $c \in \mathcal{S}_\alpha(E) \subset \mathrm{Hom}(G_F, E[\alpha])$ then c is trivial on

- commutators,
- $\deg(\alpha)$-th powers,
- inertia groups of primes outside of $\Sigma_{E,\alpha}$,

the first two because $E[\alpha]$ is abelian and annihilated by $\deg(\alpha)$, and the last because of (4) and Corollary 3.17. Therefore c factors through $\mathrm{Gal}(L/F)$, so

$$\mathcal{S}_\alpha(E) \subset \mathrm{Hom}(\mathrm{Gal}(L/F), E[\alpha]).$$

Class field theory shows that L/F is finite, so this proves the proposition in this case.

In general, the restriction map

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

sends $\mathcal{S}_\alpha(E_{/F})$ into $\mathcal{S}_\alpha(E_{/F(E[\alpha])})$. The case above shows that $\mathcal{S}_\alpha(E_{/F(E[\alpha])})$ is finite, and $H^1(F(E[\alpha])/F, E[\alpha])$ is finite, so $\mathcal{S}_\alpha(E_{/F})$ is finite. □

Corollary 4.5 (Weak Mordell-Weil Theorem). *For every nonzero $\alpha \in \mathcal{O}$, $E(F)/\alpha E(F)$ is finite.*

Proof. This is clear from Propositions 4.2 and 4.4. □

Theorem 4.6 (Mordell-Weil). *$E(F)$ is finitely generated.*

Proof. See [Si] §VIII.6. □

Definition 4.7. The *Tate-Shafarevich group* $Ш(E)$ of E over F is the subgroup of $H^1(F, E(\bar{F}))$ defined by

$$Ш(E) = \ker\left(H^1(F, E(\bar{F})) \to \prod_{v \text{ of } F} H^1(F_v, E)\right).$$

Proposition 4.8. *If $\alpha \in \mathcal{O}$, $\alpha \neq 0$, then the exact sequence* (3) *restricts to an exact sequence*

$$0 \to E(F)/\alpha E(F) \to \mathcal{S}_\alpha(E) \to Ш(E)_\alpha \to 0$$

where $Ш(E)_\alpha$ is the subgroup of elements of $Ш(E)$ killed by α.

Proof. This is clear from the definitions and the diagram (5). □

5 Elliptic Curves with Complex Multiplication

Fix a subfield F of $\mathbf{C}$ and an elliptic curve E defined over F.

Definition 5.1. We say E has *complex multiplication* over F if $\mathrm{End}_F(E)$ is an order in an imaginary quadratic field, i.e., if $\mathrm{End}_F(E) \neq \mathbf{Z}$.

Assume from now on that E has complex multiplication, and let

$$\mathcal{O} = \iota(\mathrm{End}_F(E)) \subset F.$$

As in §4 we will use ι to *identify* $\mathrm{End}_F(E)$ with $\mathcal{O}$. Let $K = \mathbf{Q}\mathcal{O} \subset F$ be the imaginary quadratic field containing $\mathcal{O}$, and denote the full ring of integers of K by $\mathcal{O}_K$. If $\mathfrak{a}$ is an ideal of $\mathcal{O}$ we will write $E[\mathfrak{a}] = \cap_{\alpha\in\mathfrak{a}} E[\alpha]$.

Fix an embedding of F into $\mathbf{C}$. Viewing E as an elliptic curve over $\mathbf{C}$ and using Proposition 2.6 we can write

$$E(\mathbf{C}) \cong \mathbf{C}/L \text{ where } L \subset K \subset \mathbf{C} \text{ and } \mathcal{O}L = L. \tag{6}$$

(A priori L is just a lattice in $\mathbf{C}$, but replacing L by λL where $\lambda^{-1} \in L$ we may assume that $L \subset K$.) Thus if $\mathcal{O} = \mathcal{O}_K$, then L is a fractional ideal of K.

5.1 Preliminaries

In this section we record the basic consequences of complex multiplication. Put most simply, if E has complex multiplication over F then all torsion points in $E(\bar{F})$ are defined over abelian extensions of F.

Remark 5.2. It will simplify the exposition to assume that $\mathcal{O} = \mathcal{O}_K$. The following proposition shows that this restriction is not too severe. Two elliptic curves are *isogenous* if there is an isogeny (a nonzero morphism sending one origin to the other) from one to the other.

Proposition 5.3. *There is an elliptic curve E', defined over F and isogenous over F to E, such that* $\mathrm{End}_F(E) \cong \mathcal{O}_K$.

Proof. Suppose the conductor of $\mathcal{O}$ is c, i.e., $\mathcal{O} = \mathbf{Z}+c\mathcal{O}_K$, and let $\mathfrak{c} = c\mathcal{O}_K \subset \mathcal{O}$. The subgroup $E[\mathfrak{c}]$ is stable under G_F, so by [Si] Proposition III.4.12 and Exercise III.3.13 there is an elliptic curve E' over F and an isogeny from E to E' with kernel $E[\mathfrak{c}]$. We only need to check that $\mathrm{End}_F(E') = \mathcal{O}_K$.

With the identification (6), $E'(\mathbf{C}) \cong \mathbf{C}/L'$ where

$$L' = \{z \in \mathbf{C} : z\mathfrak{c} \subset L\}.$$

Suppose $\alpha \in \mathcal{O}_K$. For every $z \in L'$,

$$(\alpha z)\mathfrak{c} = z(\alpha\mathfrak{c}) \in z\mathfrak{c} \subset L$$

so $\alpha z \in L'$. Therefore by Proposition 2.6, $\alpha \in \mathrm{End}_{\mathbf{C}}(E')$. By Lemma 1.8, since $\alpha \in K \subset F$ we conclude that $\alpha \in \mathrm{End}_F(E')$. □

From now on we will assume that $\mathcal{O}$ is the maximal order $\mathcal{O}_K$.

Proposition 5.4. *If $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}$ then $E[\mathfrak{a}] \cong \mathcal{O}/\mathfrak{a}$ as $\mathcal{O}$-modules.*

Proof. Using the identification (6) we see that $E[\mathfrak{a}] \cong \mathfrak{a}^{-1}L/L$ where L is a fractional ideal of K, and then $\mathfrak{a}^{-1}L/L \cong \mathcal{O}/\mathfrak{a}$. □

Corollary 5.5. *If $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}$ then the action of G_F on $E[\mathfrak{a}]$ induces an injection*

$$\mathrm{Gal}(F(E[\mathfrak{a}])/F) \hookrightarrow (\mathcal{O}/\mathfrak{a})^\times.$$

In particular $F(E[\mathfrak{a}])/F$ is abelian.

Proof. If $\beta \in \mathcal{O}$, $\sigma \in G_F$, and $P \in E(\bar{F})$ then, since the endomorphism β is defined over F, $\sigma(\beta P) = \beta(\sigma P)$. Thus there is a map

$$\mathrm{Gal}(F(E[\mathfrak{a}])/F) \hookrightarrow \mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}]).$$

By Proposition 5.4,

$$\mathrm{Aut}_{\mathcal{O}}(E[\mathfrak{a}]) \cong \mathrm{Aut}_{\mathcal{O}}(\mathcal{O}/\mathfrak{a}) = (\mathcal{O}/\mathfrak{a})^\times.$$

□

If $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}$ let $E[\mathfrak{a}^\infty] = \cup_n E[\mathfrak{a}^n]$.

Corollary 5.6. *The action of G_F on $E[\mathfrak{a}^\infty]$ induces an injection*

$$\mathrm{Gal}(F(E[\mathfrak{a}^\infty])/F) \hookrightarrow (\varprojlim_n \mathcal{O}/\mathfrak{a}^n)^\times.$$

In particular for every prime p,

$$\mathrm{Gal}(F(E[p^\infty])/F) \hookrightarrow (\mathcal{O} \otimes \mathbf{Z}_p)^\times.$$

Proof. Immediate from Corollary 5.5 □

Theorem 5.7. *Suppose F is a finite extension of $\mathbf{Q}_\ell$ for some ℓ.*

(i) *E has potentially good reduction.*

(ii) *Suppose $\mathfrak{p}$ is a prime of $\mathcal{O}$ and $n \in \mathbf{Z}^+$ is such that the multiplicative group $1 + \mathfrak{p}^n\mathcal{O}_\mathfrak{p}$ is torsion-free (where $\mathcal{O}_\mathfrak{p}$ is the completion of $\mathcal{O}$ at $\mathfrak{p}$). If $\mathfrak{p} \nmid \ell$ then E has good reduction over $F(E[\mathfrak{p}^n])$ at all primes not dividing $\mathfrak{p}$.*

Proof. Suppose p is a rational prime. By Corollary 5.6, the Galois group $\mathrm{Gal}(F(E[p^\infty])/F(E[p]))$ is isomorphic to a subgroup of the multiplicative group $1 + p\mathcal{O} \otimes \mathbf{Z}_p$. If $p > 3$ then the p-adic logarithm map shows that $1 + p\mathcal{O} \otimes \mathbf{Z}_p \cong p\mathcal{O}_\mathfrak{p} \cong \mathbf{Z}_p^2$. Thus

$$\mathrm{Gal}(F(E[p^\infty])/F(E[p])) \cong \mathbf{Z}_p^d$$

with $d \leq 2$. If $p \neq \ell$, class field theory shows that such an extension is unramified. Thus by the criterion of Néron-Ogg-Shafarevich (Theorem 3.19(i)) E has good reduction over $F(E[p])$. This proves (i).

The proof of (ii) is similar. Write $F_\infty = F(E[\mathfrak{p}^\infty])$ and $F_n = F(E[\mathfrak{p}^n])$, and suppose $\mathfrak{q}$ is a prime of F_n not dividing $\mathfrak{p}$. By (i) and Corollary 3.17, the inertia group $I_\mathfrak{q}$ of $\mathfrak{q}$ in $\mathrm{Gal}(F_\infty/F_n)$ is finite. But Corollary 5.6 shows that

$$\mathrm{Gal}(F_\infty/F_n) \subset 1 + \mathfrak{p}^n\mathcal{O}_\mathfrak{p},$$

which has no finite subgroups, so $I_\mathfrak{q}$ acts trivially on $E[\mathfrak{p}^\infty]$. Therefore by Theorem 3.19(ii), E has good or multiplicative reduction at $\mathfrak{q}$. Since we already know that the reduction is potentially good, Lemma 3.2(ii) allows us to conclude that E has good reduction at $\mathfrak{q}$. □

Remark 5.8. The hypothesis of Theorem 5.7(ii) is satisfied with $n = 1$ if the residue characteristic of $\mathfrak{p}$ is greater than 3.

Proposition 5.9. *Suppose $\mathfrak{q}$ is a prime of F where E has good reduction and $q = \mathbf{N}_{F/\mathbf{Q}}\mathfrak{q}$. There is an endomorphism $\alpha \in \mathcal{O}$ whose reduction modulo $\mathfrak{q}$ is the Frobenius endomorphism φ_q of $\tilde{E}$.*

Proof. If $\varphi_q = [m]$ for some $m \in \mathbf{Z}$ then the proposition is clear. So suppose now that $\varphi_q \notin \mathbf{Z}$, and write $\Bbbk$ for the residue field of F at $\mathfrak{q}$. Since φ_q commutes with every endomorphism of $\tilde{E}$, we see from Theorem 1.11 that the only possibility is that $\mathrm{End}_\Bbbk(\tilde{E})$ is an order in an imaginary quadratic field. But the reduction map $\mathrm{End}_F(E) \to \mathrm{End}_\Bbbk(\tilde{E})$ is injective (Proposition 3.4) so its image, the maximal order of K, must be all of $\mathrm{End}_\Bbbk(\tilde{E})$. This proves the proposition. □

5.2 The Main Theorem of Complex Multiplication

In this section we study further the action of G_F on torsion points of E. We will see that not only are torsion points abelian over F, in fact they are "almost" abelian over K, so that (using class field theory) we can describe the action of G_F on torsion points in terms of an action of the ideles of K.

The reference for this section is [Sh] Chapter 5; see also [ST]. We continue to suppose that E has complex multiplication by the *maximal* order of K.

Definition 5.10. Let $\mathbf{A}_K^\times$ denote the group of ideles of K. There is a natural map from $\mathbf{A}_K^\times$ to the group of fractional ideals of K, and if $x \in \mathbf{A}_K^\times$ and $\mathfrak{a}$ is a fractional ideal of K we will write $x\mathfrak{a}$ for the product of $\mathfrak{a}$ and the fractional ideal corresponding to x.

If $\mathfrak{p}$ is a prime of K let $\mathcal{O}_\mathfrak{p} \subset K_\mathfrak{p}$ denote the completions of $\mathcal{O}$ and K at $\mathfrak{p}$. If $\mathfrak{a}$ is a fractional ideal of K, write $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}\mathcal{O}_\mathfrak{p}$ and then

$$K/\mathfrak{a} = \mathfrak{a} \otimes (K/\mathcal{O}) = \mathfrak{a} \otimes (\oplus_\mathfrak{p}(K_\mathfrak{p}/\mathcal{O}_\mathfrak{p})) = \oplus_\mathfrak{p} K_\mathfrak{p}/\mathfrak{a}_p \tag{7}$$

If $x = (x_\mathfrak{p}) \in \mathbf{A}_K^\times$ then multiplication by $x_\mathfrak{p}$ gives an isomorphism from $K_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}$ to $K_\mathfrak{p}/x_\mathfrak{p}\mathfrak{a}_\mathfrak{p} = K_\mathfrak{p}/(x\mathfrak{a})_\mathfrak{p}$, so putting these maps together in (7) we get an isomorphism

$$x : K/\mathfrak{a} \xrightarrow{\sim} K/x\mathfrak{a}.$$

The following theorem is Theorem 5.4 in Shimura's book [Sh]. Let K^{ab} denote the maximal abelian extension of K and $[\,\cdot\,, K^{\mathrm{ab}}/K]$ the Artin map of global class field theory. If σ is an automorphism of $\mathbf{C}$ let E^σ denote the elliptic curve obtained by applying σ to the coefficients of an equation for E.

Theorem 5.11 (Main theorem of complex multiplication). *Fix a fractional ideal $\mathfrak{a}$ of K and an analytic isomorphism*

$$\xi : \mathbf{C}/\mathfrak{a} \to E(\mathbf{C})$$

as in (6). *Suppose $\sigma \in \mathrm{Aut}(\mathbf{C}/K)$ and $x \in \mathbf{A}_K^\times$ satisfies $[x, K^{\mathrm{ab}}/K] = \sigma\,|_{K^{\mathrm{ab}}}$. Then there is a unique isomorphism $\xi' : \mathbf{C}/x^{-1}\mathfrak{a} \to E^\sigma(\mathbf{C})$ such that the following diagram commutes*

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r, "\xi"] \arrow[d, "x^{-1}"'] & E_{\mathrm{tors}} \arrow[d, "\sigma"] \\ K/x^{-1}\mathfrak{a} \arrow[r, "\xi'"] & E^\sigma_{\mathrm{tors}} \end{tikzcd}$$

where E_{tors} denotes the torsion in $E(\mathbf{C})$ and similarly for E^σ_{tors}.

Proof. See [Sh] Theorem 5.4. □

Let H denote the Hilbert class field H of K.

Corollary 5.12. (i) $K(j(E)) = H \subset F$,
(ii) *$j(E)$ is an integer of H.*

Proof. Suppose $\sigma \in \mathrm{Aut}(\mathbf{C}/K)$. With the notation of Theorem 5.11, as in Proposition 2.6 we see that

$$j(E) = j(E)^\sigma \Leftrightarrow E \cong E^\sigma \Leftrightarrow \mathbf{C}/\mathfrak{a} \cong \mathbf{C}/x\mathfrak{a} \Leftrightarrow x\mathfrak{a} = \lambda\mathfrak{a} \text{ for some } \lambda \in \mathbf{C}$$
$$\Leftrightarrow x \in K^\times \prod_{\mathfrak{p}\nmid\infty} \mathcal{O}_\mathfrak{p}^\times \prod_{\mathfrak{p}\mid\infty} K_\mathfrak{p}^\times \Leftrightarrow [x, H/K] = 1 \Leftrightarrow \sigma \text{ is the identity on } H.$$

This proves (i), and (ii) follows from Theorem 5.7(i) and Lemma 3.2(i). □

Corollary 5.13. *There is an elliptic curve defined over H with endomorphism ring $\mathcal{O} = \mathcal{O}_K$.*

Proof. By Theorem 2.3(i) there is an elliptic curve E' defined over $\mathbf{C}$ with $E'(\mathbf{C}) \cong \mathbf{C}/\mathcal{O}$, and by Proposition 2.6, $\mathrm{End}_{\mathbf{C}}(E') \cong \mathcal{O}$. Corollary 5.12 shows that $j(E') \in H$, so (see Proposition III.1.4 of [Si]) there is an elliptic curve E defined over H with $j(E) = j(E')$. Hence E is isomorphic over $\mathbf{C}$ to E', so $\mathrm{End}_{\mathbf{C}}(E) \cong \mathcal{O}$.

The map $\iota : \mathrm{End}_{\mathbf{C}}(E) \to \mathbf{C}$ of Definition 1.7 is injective, so the image is $\mathcal{O} \subset H$. By Lemma 1.8 we conclude that $\mathrm{End}_{\mathbf{C}}(E) = \mathrm{End}_H(E)$. Thus E has the desired properties. □

Exercise 5.14. Let A be the ideal class group of K. If $E \cong \mathbf{C}/\mathfrak{a}$, $\mathfrak{b}$ is an ideal of K, $\sigma_{\mathfrak{b}}$ is its image under the isomorphism $A_K \xrightarrow{\sim} \mathrm{Gal}(H/K)$, and $\sigma \in G_K$ restricts to $\sigma_{\mathfrak{b}}$ on H, then

$$E^{\sigma}(\mathbf{C}) \cong \mathbf{C}/\mathfrak{b}^{-1}\mathfrak{a}.$$

For the rest of this section we suppose that F is a number field.

Theorem 5.15. *There is a Hecke character*

$$\psi = \psi_E : \mathbf{A}_F^{\times}/F^{\times} \to \mathbf{C}^{\times}$$

with the following properties.

(i) *If $x \in \mathbf{A}_F^{\times}$ and $y = \mathbf{N}_{F/K}x \in \mathbf{A}_K^{\times}$, then*

$$\psi(x)\mathcal{O} = y_{\infty}^{-1}(y\mathcal{O}) \subset \mathbf{C}.$$

(ii) *If $x \in \mathbf{A}_F^{\times}$ is a finite idele (i.e., the archimedean component is 1) and $\mathfrak{p}$ is a prime of K, then $\psi(x)(\mathbf{N}_{F/K}x)_{\mathfrak{p}}^{-1} \in \mathcal{O}_{\mathfrak{p}}^{\times}$ and for every $P \in E[\mathfrak{p}^{\infty}]$*

$$[x, F^{\mathrm{ab}}/F]P = \psi(x)(\mathbf{N}_{F/K}x)_{\mathfrak{p}}^{-1}P.$$

(iii) *If $\mathfrak{q}$ is a prime of F and $U_{\mathfrak{q}}$ denotes the local units in the completion of F at $\mathfrak{q}$, then*

$$\psi(U_{\mathfrak{q}}) = 1 \Leftrightarrow E \textit{ has good reduction at } \mathfrak{q}.$$

Proof. Suppose $x \in \mathbf{A}_F^{\times}$, and let $y = \mathbf{N}_{F/K}x$, $\sigma = [x, F^{\mathrm{ab}}/F]$. Then σ restricted to K^{ab} is $[y, K^{\mathrm{ab}}/K]$ so we can apply Theorem 5.11 with σ and y. Since σ fixes F, $E^{\sigma} = E$ so Theorem 5.11 gives a diagram with isomorphisms $\xi : \mathbf{C}/\mathfrak{a} \to E(\mathbf{C})$ and $\xi' : \mathbf{C}/y^{-1}\mathfrak{a} \to E(\mathbf{C})$. Then $\xi^{-1} \circ \xi' : \mathbf{C}/y^{-1}\mathfrak{a} \xrightarrow{\sim} \mathbf{C}/\mathfrak{a}$ is an isomorphism, so it must be multiplication by an element $\psi_{\mathrm{fin}}(x) \in K^{\times}$ satisfying $\psi_{\mathrm{fin}}(x)\mathcal{O} = y\mathcal{O}$. Define

$$\psi(x) = y_{\infty}^{-1}\psi_{\mathrm{fin}}(x).$$

It is clear that $\psi : \mathbf{A}_F^\times/F^\times \to \mathbf{C}^\times$ is a homomorphism and that (i) is satisfied. If $\mathfrak{p}$ is a prime of K and $k > 0$ then Theorem 5.11 gives a diagram

$$\begin{tikzcd}
\mathfrak{p}^{-k}\mathfrak{a}_\mathfrak{p}/\mathfrak{a}_\mathfrak{p} \arrow[r, "\sim"] \arrow[d, "y_\mathfrak{p}^{-1}"'] & \mathfrak{p}^{-k}\mathfrak{a}/\mathfrak{a} \arrow[r, "\xi"] \arrow[d, "y^{-1}"'] & E[\mathfrak{p}^k] \arrow[d, "\sigma"] \\
\mathfrak{p}^{-k}y_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p}/y_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p} \arrow[r, "\sim"] & \mathfrak{p}^{-k}y^{-1}\mathfrak{a}/y^{-1}\mathfrak{a} \arrow[r, "\psi_{\mathrm{fin}}(x)\xi"] & E[\mathfrak{p}^k]
\end{tikzcd}$$

(where the left-hand square comes from the definition of the action of y on $K/\mathfrak{a}$) which proves (ii).

Suppose $\mathfrak{q}$ is a prime of F and p is a rational prime not lying below $\mathfrak{q}$. By (ii), if $u \in U_\mathfrak{q}$ then $[u, F^{\mathrm{ab}}/F]$ acts on $T_p(E)$ as multiplication by $\psi(u)$. Since $[U_\mathfrak{q}, F^{\mathrm{ab}}/F]$ is the inertia group at $\mathfrak{q}$, (iii) follows from Theorem 3.19 and Corollary 3.18(i).

Thus for almost all $\mathfrak{q}$, $\psi(U_q) = 1$. Even for primes $\mathfrak{q}$ of bad reduction, since the reduction is potentially good (Theorem 5.7(i)) the action of $[U_\mathfrak{q}, F^{\mathrm{ab}}/F]$ on $T_p(E)$ factors through a finite quotient (Corollary 3.18(ii)) so the argument above shows that ψ vanishes on an open subgroup of $U_\mathfrak{q}$. Therefore ψ is continuous, and the proof of the theorem is complete. □

Let $\mathfrak{f} = \mathfrak{f}_E$ denote the conductor of the Hecke character ψ of Theorem 5.15. We can view ψ as a character of fractional ideals of F prime to $\mathfrak{f}$ in the usual way.

Corollary 5.16. *As a character on ideals, ψ satisfies*

(i) *if $\mathfrak{b}$ is an ideal of F prime to $\mathfrak{f}$ then $\psi(\mathfrak{b})\mathcal{O} = \mathbf{N}_{F/K}\mathfrak{b}$,*
(ii) *if $\mathfrak{q}$ is a prime of F not dividing $\mathfrak{f}$ and $\mathfrak{b}$ is an ideal of $\mathcal{O}$ prime to $\mathfrak{q}$, then $[\mathfrak{q}, F(E[\mathfrak{b}])/F]$ acts on $E[\mathfrak{b}]$ by multiplication by $\psi(\mathfrak{q})$.*
(iii) *if $\mathfrak{q}$ is a prime of F where E has good reduction and $q = \mathbf{N}_{F/\mathbf{Q}}\mathfrak{q}$ then $\psi(\mathfrak{q}) \in \mathcal{O}$ reduces modulo $\mathfrak{q}$ to the Frobenius endomorphism φ_q of $\tilde{E}$.*

Proof. The first two assertions are just translations of Theorem 5.15(i) and (ii). If $P \in E_{\mathrm{tors}}$ has order prime to $\mathfrak{q}$, $\tilde{P}$ denotes its reduction modulo a prime of $\bar{F}$ above $\mathfrak{q}$, and $\sigma_\mathfrak{q} = [\mathfrak{q}, F(E[\mathfrak{b}])/F]$, then

$$\widetilde{\psi(\mathfrak{q})}\tilde{P} = \widetilde{\sigma_\mathfrak{q} P} = \varphi_q\tilde{P}$$

where the first equality is from (ii) and the second is the definition of the Artin symbol $[\mathfrak{q}, F(E[\mathfrak{b}])/F]$. Since the reduction map is injective on prime-to-$\mathfrak{q}$ torsion (Theorem 3.15) this proves (iii). □

Remark 5.17. Note that Corollary 5.16(iii) gives an explicit version of Proposition 5.9. Proposition 5.9 is one of the key points in the proof of the Main Theorem of Complex Multiplication, of which Corollary 5.16 is a direct consequence.

Corollary 5.18. *Suppose $F = K$ and $\mathfrak{p}$ is a prime of K such that the map $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{p})^\times$ is not surjective. Then $E[\mathfrak{p}] \not\subset E(K)$.*

Proof. By Theorem 5.15(ii), $[\mathcal{O}_\mathfrak{p}^\times, K^{\mathrm{ab}}/K]$ acts on $E[\mathfrak{p}]$ via the character $\psi(x)x^{-1}$ of $\mathcal{O}_\mathfrak{p}^\times$, and by Theorem 5.15(i), $\psi(\mathcal{O}_\mathfrak{p}^\times) \subset \mathcal{O}^\times$. The corollary follows. □

Corollary 5.19. *Suppose $F = K$. Then the map $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{f})^\times$ is injective. In particular E cannot have good reduction at all primes of K.*

Proof. Let $u \in \mathcal{O}^\times$, $u \neq 1$ and let x be the idele defined by $x_\infty = 1$ and $x_\mathfrak{p} = u$ for all finite $\mathfrak{p}$. Then $\psi(x) = \psi(u^{-1}x) = u \neq 1$, so by definition of $\mathfrak{f}$, $u \not\equiv 1 \pmod{\mathfrak{f}}$. The second assertion now follows from Theorem 5.15(iii). □

If $\mathfrak{a}$ is an ideal of K let $K(\mathfrak{a})$ denote the ray class field of K modulo $\mathfrak{a}$.

Corollary 5.20. *Suppose E is defined over K, $\mathfrak{a}$ is an ideal of K prime to $6\mathfrak{f}$, and $\mathfrak{p}$ is a prime of K not dividing $6\mathfrak{f}$.*

(i) *$E[\mathfrak{a}\mathfrak{f}] \subset E(K(\mathfrak{a}\mathfrak{f}))$.*
(ii) *The map $\mathrm{Gal}(K(E[\mathfrak{a}])/K) \to (\mathcal{O}/\mathfrak{a})^\times$ of Corollary 5.5 is an isomorphism.*
(iii) *If $\mathfrak{b} \mid \mathfrak{a}$ then the natural map $\mathrm{Gal}(K(\mathfrak{a}\mathfrak{f})/K(\mathfrak{b}\mathfrak{f})) \to \mathrm{Gal}(K(E[\mathfrak{a}])/K(E[\mathfrak{b}]))$ is an isomorphism.*
(iv) *$K(E[\mathfrak{a}\mathfrak{p}^n])/K(E[\mathfrak{a}])$ is totally ramified above $\mathfrak{p}$.*
(v) *If the map $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{a})^\times$ is injective then $K(E[\mathfrak{a}\mathfrak{p}^n])/K(E[\mathfrak{a}])$ is unramified outside of $\mathfrak{p}$.*

Proof. Suppose $x \in \mathbf{A}_K^\times$, $x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times$ for all finite $\mathfrak{p}$ and $x_\infty = 1$. If $x \equiv 1(\mathrm{mod}^\times \mathfrak{f})$ then Theorem 5.15(ii) shows that $[x, K^{\mathrm{ab}}/K]$ acts on E_{tors} as multiplication by x^{-1}. If $x \equiv 1(\mathrm{mod}^\times \mathfrak{a})$ Theorem 5.15 shows that $[x, K^{\mathrm{ab}}/K]$ acts on $E[\mathfrak{a}]$ as multiplication by $\psi(x)$. Thus

- if $\mathfrak{p} \mid \mathfrak{f}$ then the kernel of $\mathcal{O}_\mathfrak{p}^\times \to [\mathcal{O}_\mathfrak{p}^\times, K(E[\mathfrak{a}])/K]$ is the kernel of the composition $\mathcal{O}_\mathfrak{p}^\times \xrightarrow{\psi} \mathcal{O}^\times \to (\mathcal{O}/\mathfrak{a})^\times$;
- if $\mathfrak{p}^n \mid \mathfrak{a}$ and $\mathfrak{p}^{n+1} \nmid \mathfrak{a}$ then $\mathcal{O}_\mathfrak{p}^\times/(1 + \mathfrak{p}^n\mathcal{O}_\mathfrak{p}) \hookrightarrow [\mathcal{O}_\mathfrak{p}^\times, K(E[\mathfrak{a}])/K] \hookrightarrow (\mathcal{O}/\mathfrak{p}^n)^\times$ is an isomorphism.

All assertions of the corollary follow without difficulty from this. □

Remark 5.21. In fact, without much more difficulty one can strengthen Corollary 5.20(i) (see [CW1] Lemma 4) to show that $E[\mathfrak{a}\mathfrak{f}] = E(K(\mathfrak{a}\mathfrak{f}))$, but we will not need this.

Corollary 5.22. *Suppose $\mathfrak{q}$ is a prime of F. There is an elliptic curve E' defined over F, such that*

- *E' is isomorphic to E over $\bar{F}$,*
- *E' has good reduction at $\mathfrak{q}$.*

Proof. Let ψ_E be the Hecke character attached to E and $U_{\mathfrak{q}}$ the group of local units at $\mathfrak{q}$, viewed as a subgroup of $\mathbf{A}_F^\times$. By Theorem 5.15(i), $\psi_E(U_{\mathfrak{q}}) \subset \mathcal{O}^\times$. Therefore we can find a continuous map

$$\chi : \mathbf{A}_F^\times / F^\times \to \mathcal{O}^\times$$

such that $\chi = \psi_E$ on $U_{\mathfrak{q}}$. We will take E' to be the twist of E by χ^{-1} (see [Si] §X.5).

Explicitly, suppose E is given by a Weierstrass equation

$$y^2 = x^3 + ax + b.$$

and let $w = \#(\mathcal{O}^\times)$. By class field theory we can view χ as an element of

$$\mathrm{Hom}(G_F, \mathcal{O}^\times) = H^1(F, \boldsymbol{\mu}_w) \cong F^\times/(F^\times)^w.$$

In other words, there is a $d \in F^\times$ such that

$$(d^{1/w})^\sigma = \chi(\sigma) d^{1/w} \quad \text{for every } \sigma \in G_F.$$

Define

$$E' = \begin{cases} y^2 = x^3 + d^2ax + d^3b & \text{if } w = 2 \\ y^2 = x^3 + dax & \text{if } w = 4 \\ y^2 = x^3 + db & \text{if } w = 6 \end{cases}$$

(see Example 1.1). The map

$$(x, y) \mapsto \begin{cases} (dx, d^{3/2}y) & \text{if } w = 2 \\ (d^{1/2}x, d^{3/4}y) & \text{if } w = 4 \\ (d^{1/3}x, d^{1/2}y) & \text{if } w = 6 \end{cases}$$

defines an isomorphism $\phi : E \xrightarrow{\sim} E'$ over $F(d^{1/w})$ (where we are using Lemma 1.13). If $P \in E(\bar{F})$ and $\sigma \in G_F$, then

$$\sigma(\phi(P)) = \phi^\sigma(\sigma P) = \chi(\sigma)^{-1}\phi(\sigma P).$$

From the definition of the Hecke character $\psi_{E'}$ of E' we see that $\psi_{E'} = \chi^{-1}\psi_E$. By construction this is trivial on $U_{\mathfrak{q}}$, so by Theorem 5.15(iii) E' has good reduction at $\mathfrak{q}$. □

6 Descent

In this section we use the results of §5 to compute the Selmer group of an elliptic curve with complex multiplication. After some cohomological lemmas in §6.1, we define an enlarged Selmer group $\mathcal{S}'(E)$ in §6.2 which is easier to compute (Lemma 6.4 and Theorem 6.5) than the true Selmer group $\mathcal{S}(E)$.

The main result describing the Selmer group $\mathcal{S}(E)$ is Theorem 6.9. The methods of this section closely follow the original work of Coates and Wiles [CW1] (see for example [Co]).

We continue to assume that E is an elliptic curve defined over a field F of characteristic 0, with complex multiplication by the maximal order $\mathcal{O}$ of an imaginary quadratic field K.

6.1 Preliminaries

Lemma 6.1. *Suppose $\mathfrak{p}$ is a prime of K lying above a rational prime $p > 3$, and $n \geq 0$. Let C be a subgroup of $(\mathcal{O}/\mathfrak{p}^n)^\times$, acting on $\mathcal{O}/\mathfrak{p}^n$ via multiplication. If either C is not a p-group or C is cyclic, then for every $i > 0$*

$$H^i(C, \mathcal{O}/\mathfrak{p}^n) = 0.$$

Proof. If C is cyclic this is a simple exercise. If C', the prime-to-p-part of C, is nontrivial, then $(\mathcal{O}/\mathfrak{p}^n)^{C'} = 0$ and $H^i(C', \mathcal{O}/\mathfrak{p}^n) = 0$ for every i, so the inflation-restriction exact sequence

$$0 \to H^i(C/C', (\mathcal{O}/\mathfrak{p}^n)^{C'}) \to H^i(C, \mathcal{O}/\mathfrak{p}^n) \to H^i(C', \mathcal{O}/\mathfrak{p}^n)$$

shows that $H^i(C, \mathcal{O}/\mathfrak{p}^n) = 0$. □

Lemma 6.2. *Suppose $\mathfrak{p}$ is a prime of K lying above a rational prime $p > 3$, and $n \geq 0$.*

(i) *If $\mathcal{O}_\mathfrak{p} = \mathbf{Z}_p$ or if $E[\mathfrak{p}] \not\subset E(F)$ then the restriction map gives an isomorphism*

$$H^1(F, E[\mathfrak{p}^n]) \cong H^1(F(E[\mathfrak{p}^n]), E[\mathfrak{p}^n])^{\mathrm{Gal}(F(E[\mathfrak{p}^n])/F)}.$$

(ii) *Suppose F is a finite extension of $\mathbf{Q}_\ell$ for some $\ell \neq p$. Then the restriction map gives an injection*

$$H^1(F, E)_{\mathfrak{p}^n} \hookrightarrow H^1(F(E[\mathfrak{p}^n]), E)_{\mathfrak{p}^n}.$$

Proof. Use Proposition 5.4 and Corollary 5.5 to identify $E[\mathfrak{p}^n]$ with $\mathcal{O}/\mathfrak{p}^n$ and $\mathrm{Gal}(F(E[\mathfrak{p}^n])/F)$ with a subgroup C of $(\mathcal{O}/\mathfrak{p}^n)^\times$. Then C is cyclic if $\mathcal{O}_\mathfrak{p} = \mathbf{Z}_p$, and C is a p-group if and only if $E[\mathfrak{p}] \subset E(F)$ (since $\mathrm{Gal}(F(E[\mathfrak{p}])/F) \subset (\mathcal{O}/p)^\times$ has order prime to p). Thus (i) follows from Lemma 6.1 and the inflation-restriction exact sequence.

The kernel of the restriction map in (ii) is $H^1(F_n/F, E(F_n))_{\mathfrak{p}^n}$, where $F_n = F(E[\mathfrak{p}^n])$. We may as well assume that $n \geq 1$, or there is nothing to prove. By Theorem 5.7(ii), E has good reduction over F_n, so by Proposition 3.4 there is a reduction exact sequence

$$0 \to E_1(F_n) \to E(F_n) \to \tilde{E}(\Bbbk_n) \to 0$$

where $\Bbbk_n$ is the residue field of F_n. Thus $E_1(F_n)$ is a profinite $\mathcal{O}$-module, of finite index in $E(F_n)$, on which (by Theorem 3.15(i)) every α prime to ℓ

acts invertibly. It follows that the pro-$\mathfrak{p}$ part of $E(F_n)$ is finite, say $E[\mathfrak{p}^m]$ for some $m \geq n$, and hence

$$H^1(F_n/F, E(F_n))_{\mathfrak{p}^n} \subset H^1(F_n/F, E[\mathfrak{p}^m]) = H^1(F(E[\mathfrak{p}^m])/F, E[\mathfrak{p}^m]).$$

If $E[\mathfrak{p}] \subset E(F)$ then E has good reduction by Theorem 5.7(ii) (and Remark 5.8) so F_n/F is unramified and hence cyclic. Hence exactly as in (i), Lemma 6.1 shows that $H^1(F(E[\mathfrak{p}^m])/F, E[\mathfrak{p}^m]) = 0$, and (ii) follows. □

6.2 The Enlarged Selmer Group

Suppose for the rest of this section that F is a number field.

Definition 6.3. If $\alpha \in \mathcal{O}$ define $\mathcal{S}'_\alpha(E) = \mathcal{S}'_\alpha(E_{/F}) \subset H^1(F, E[\alpha])$ by

$$\begin{aligned}\mathcal{S}'_\alpha(E) &= \{c \in H^1(F, E[\alpha]) : \mathrm{res}_{\mathfrak{q}}(c) \in \mathrm{image}(E(F_{\mathfrak{q}})/\alpha E(F_{\mathfrak{q}})) \text{ for every } \mathfrak{q} \nmid \alpha\} \\ &= \{c \in H^1(F, E[\alpha]) : \mathrm{res}_{\mathfrak{q}}(c) = 0 \text{ in } H^1(F_{\mathfrak{q}}, E(\bar{F}_{\mathfrak{q}})) \text{ for every } \mathfrak{q} \nmid \alpha\}\end{aligned}$$

in the diagram (5). Clearly $\mathcal{S}_\alpha(E) \subset \mathcal{S}'_\alpha(E)$.

Lemma 6.4. *Suppose $\mathfrak{p}$ is a prime of K not dividing 6, $n \geq 1$, $E[\mathfrak{p}^n] \subset E(F)$ and $\mathfrak{p}^n = \alpha\mathcal{O}$. Then*

$$\mathcal{S}'_\alpha(E_{/F}) = \mathrm{Hom}(\mathrm{Gal}(M/F), E[\mathfrak{p}^n])$$

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

Proof. Since $E[\mathfrak{p}^n] \subset E(F)$,

$$H^1(F, E[\mathfrak{p}^n]) = \mathrm{Hom}(G_F, E[\mathfrak{p}^n]), \quad H^1(F_{\mathfrak{q}}, E[\mathfrak{p}^n]) = \mathrm{Hom}(G_{F_{\mathfrak{q}}}, E[\mathfrak{p}^n]).$$

Suppose $\mathfrak{q}$ is a prime of F not dividing $\mathfrak{p}$. By Theorem 5.7(ii), E has good reduction at $\mathfrak{p}$ so by (4) and Corollary 3.17, the image of $E(F_{\mathfrak{q}})/\alpha E(F_{\mathfrak{q}})$ under (5) is contained in $\mathrm{Hom}(G_{F_{\mathfrak{q}}}/I_{\mathfrak{q}}, E[\mathfrak{p}^n])$, where $I_{\mathfrak{q}}$ is the inertia group in $G_{F_{\mathfrak{q}}}$, and we have $\mathcal{O}$-module isomorphisms

$$\mathrm{Hom}(G_{F_{\mathfrak{q}}}/I_{\mathfrak{q}}, E[\mathfrak{p}^n]) \cong E[\mathfrak{p}^n] \cong \mathcal{O}/\mathfrak{p}^n\mathcal{O}.$$

On the other hand, using Theorem 3.15 and writing $\Bbbk$ for the residue field of $F_{\mathfrak{q}}$,

$$E(F_{\mathfrak{q}})/\alpha E(F_{\mathfrak{q}}) \cong \tilde{E}(\Bbbk)/\alpha\tilde{E}(\Bbbk) \cong \mathcal{O}/\mathfrak{p}^n\mathcal{O}.$$

Thus the image of $E(F_{\mathfrak{q}})/\alpha E(F_{\mathfrak{q}}) \hookrightarrow H^1(F_{\mathfrak{q}}, E[\mathfrak{p}^n])$ under (5) must be equal to $\mathrm{Hom}(G_{F_{\mathfrak{q}}}/I_{\mathfrak{q}}, E[\mathfrak{p}^n])$, and the lemma follows from the definition of $\mathcal{S}'_\alpha$. □

Theorem 6.5. *Suppose E is defined over K, $\mathfrak{p}$ is a prime of K not dividing 6, $n \geq 1$, and $\mathfrak{p}^n = \alpha\mathcal{O}$. Let $K_n = K(E[\mathfrak{p}^n])$. Then*

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

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

Proof. Let $G = \mathrm{Gal}(K_n/K)$. By Lemma 6.2(ii) and Corollary 5.18, the restriction map gives an isomorphism

$$H^1(K, E[\mathfrak{p}^n]) \cong H^1(K_n, E[\mathfrak{p}^n])^G.$$

Clearly the image of $\mathcal{S}'_\alpha(E_{/K})$ under this restriction isomorphism is contained in $\mathcal{S}'_\alpha(E_{/K_n})$. Conversely, every class in $H^1(K, E[\mathfrak{p}^n])$ whose restriction lies in $\mathcal{S}'_\alpha(E_{/K_n})$ already lies in $\mathcal{S}'_\alpha(E_{/K})$, because by Lemma 6.2(iii) the restriction map

$$H^1(K_\mathfrak{q}, E(\bar{K_\mathfrak{q}})) \to H^1(K_\mathfrak{q}(E[\mathfrak{p}^n]), E(\bar{K_\mathfrak{q}}))$$

is injective for every prime $\mathfrak{q}$ not dividing $\mathfrak{p}$. This proves that

$$\mathcal{S}'_\alpha(E_{/K}) = \mathcal{S}'_\alpha(E_{/K_n})^G,$$

and so the theorem follows from Lemma 6.4. □

6.3 The True Selmer Group

For the rest of this section we will suppose that E is defined over K, i.e., $F = K$. Recall that by Corollary 5.12 this implies that K has class number one. Fix a prime $\mathfrak{p}$ of K not dividing $6\mathfrak{f}$ and a generator π of $\mathfrak{p}$. Let $\lambda_E : E_1(K_\mathfrak{p}) \to \mathfrak{p}\mathcal{O}_\mathfrak{p}$ be the logarithm map of Definition 3.12.

Lemma 6.6. *The map λ_E extends uniquely to a surjective map $E(K_\mathfrak{p}) \twoheadrightarrow \mathfrak{p}\mathcal{O}_\mathfrak{p}$ whose kernel is finite and has no $\mathfrak{p}$-torsion.*

Proof. By Corollary 3.13, $\lambda_E : E_1(K_\mathfrak{p}) \to \mathfrak{p}\mathcal{O}_\mathfrak{p}$ is an isomorphism, and by Lemma 3.6(i) and Corollary 5.16(iii), $E(K_\mathfrak{p})/E_1(K_\mathfrak{p})$ is finite and has no $\mathfrak{p}$-torsion. □

Definition 6.7. For every $n \geq 1$ let $K_{n,\mathfrak{p}} = K_\mathfrak{p}(E[\mathfrak{p}^n])$ and define a Kummer pairing

$$\begin{array}{rcl} \langle\,\cdot\,,\,\cdot\,\rangle_{\pi^n} : E(K_\mathfrak{p}) \times K_{n,\mathfrak{p}}^\times & \to & E[\mathfrak{p}^n] \\ P \;\;,\;\; x & \mapsto & [x, K_{n,\mathfrak{p}}^{\mathrm{ab}}/K_{n,\mathfrak{p}}]Q - Q \end{array}$$

where $[\,\cdot\,, K_{n,\mathfrak{p}}^{\mathrm{ab}}/K_{n,\mathfrak{p}}]$ is the local Artin map and $Q \in E(\bar{K_\mathfrak{p}})$ satisfies $\pi^n Q = P$.

Lemma 6.8. *For every n there is a unique Galois-equivariant homomorphism $\delta_n : K_{n,\mathfrak{p}}^\times \to E[\mathfrak{p}^n]$ such that if $P \in E(K_\mathfrak{p})$ and $x \in K_{n,\mathfrak{p}}^\times$,*

$$\langle P, x\rangle_{\pi^n} = (\pi^{-1}\lambda_E(P))\delta_n(x).$$

Further, if $\mathcal{O}_{n,\mathfrak{p}}$ denotes the ring of integers of $K_{n,\mathfrak{p}}$ then $\delta_n(\mathcal{O}_{n,\mathfrak{p}}^\times) = E[\mathfrak{p}^n]$.

Proof. Define $\delta_n(x) = \langle R, x\rangle_{\pi^n}$ where $\lambda_E(R) = \pi$, and then everything except the surjectivity assertion is clear.

First note that by Theorem 5.15(ii), if $x \in \mathcal{O}_\mathfrak{p}^\times$ then $[x, K_{n,\mathfrak{p}}/K_\mathfrak{p}]$ acts on $E[\mathfrak{p}^n]$ as multiplication by x^{-1}. Therefore $E(K_\mathfrak{p})$ has no $\mathfrak{p}$-torsion and $E[\mathfrak{p}]$ has no proper $G_{K_\mathfrak{p}}$-stable subgroups.

By Lemma 6.6, $E(K_\mathfrak{p})/\mathfrak{p}^n E(K_\mathfrak{p}) \xrightarrow{\sim} \mathcal{O}/\mathfrak{p}^n$. Since

$$E(K_\mathfrak{p})/\mathfrak{p}^n E(K_\mathfrak{p}) \hookrightarrow H^1(K_\mathfrak{p}, E[\mathfrak{p}^n]) \hookrightarrow \mathrm{Hom}(K_{n,\mathfrak{p}}^\times, E[\mathfrak{p}^n])$$

is injective (the first map by (5) and the second by Lemmas 6.2(ii) and 6.6), the image of δ_n is not contained in $E[\mathfrak{p}^{n-1}]$. Since the image of δ_n is stable under $G_{K_\mathfrak{p}}$, it must be all of $E[\mathfrak{p}^n]$. But $\delta_n(K_{n,\mathfrak{p}}^\times)/\delta_n(\mathcal{O}_{\mathfrak{p},n}^\times)$ is a quotient of $E[\mathfrak{p}^n]$ on which $G_{K_\mathfrak{p}}$ acts trivially, and (as above) such a quotient must be trivial, so $\delta_n(\mathcal{O}_{\mathfrak{p},n}^\times) = E[\mathfrak{p}^n]$ as well. □

Theorem 6.9. *With notation as above, let $K_n = K(E[\mathfrak{p}^n])$ and $\mathcal{O}_n$ its ring of integers, and define*

$$W_n = K_n^\times \prod_{v\mid\infty} K_{n,v}^\times \prod_{v\nmid\mathfrak{p}\infty} \mathcal{O}_{n,v}^\times \cdot \ker(\delta_n) \subset \mathbf{A}_{K_n}^\times.$$

Then

$$\mathcal{S}_{\pi^n}(E_{/K}) = \mathrm{Hom}(\mathbf{A}_{K_n}^\times/W_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}.$$

Proof. By definition we have an injective map

$$E(K_\mathfrak{p})/\pi^n E(K_\mathfrak{p}) \hookrightarrow \mathrm{Hom}(K_{n,\mathfrak{p}}^\times/\ker(\delta_n), E[\mathfrak{p}^n])^{\mathrm{Gal}(K_{n,\mathfrak{p}}/K_\mathfrak{p})}.$$

By Lemma 6.6, $E(K_\mathfrak{p})/\pi^n E(K_\mathfrak{p}) \cong \mathcal{O}/\mathfrak{p}^n$. By Lemma 6.8 $K_{n,\mathfrak{p}}^\times/\ker(\delta_n) \cong E[\mathfrak{p}^n]$, and by Theorem 5.15(ii),

$$\mathrm{Hom}(E[\mathfrak{p}^n], E[\mathfrak{p}^n])^{\mathrm{Gal}(K_{n,\mathfrak{p}}/K_\mathfrak{p})} = \mathrm{Hom}_\mathcal{O}(E[\mathfrak{p}^n], E[\mathfrak{p}^n]) \cong \mathcal{O}/\mathfrak{p}^n.$$

Therefore the injection above is an isomorphism, and the theorem follows from Proposition 6.5 and class field theory. □

Let A denote the ideal class group of $K(E[\mathfrak{p}])$, and $\mathcal{E}$ the group of global units of $K(E[\mathfrak{p}])$.

Corollary 6.10. *With notation as above,*

$$\mathcal{S}_\pi(E) = 0 \Leftrightarrow \left(\mathrm{Hom}(A, E[\mathfrak{p}])^{\mathrm{Gal}(K(E[\mathfrak{p}])/K)} = 0 \quad \textit{and} \quad \delta_1(\mathcal{E}) \neq 0\right).$$

Proof. By Corollary 5.20, $K(E[\mathfrak{p}])/K$ is totally ramified at $\mathfrak{p}$, of degree $\mathbf{N}\mathfrak{p}-1$. We identify $K_{1,\mathfrak{p}}$ with the completion of $K(E[\mathfrak{p}])$ at the unique prime above $\mathfrak{p}$, and let $\mathcal{O}_{1,\mathfrak{p}}$ denote its ring of integers and $\bar{\mathcal{E}}$ the closure of $\mathcal{E}$ in $\mathcal{O}_{1,\mathfrak{p}}$. Let $V = \ker(\delta_1) \cap \mathcal{O}_{1,\mathfrak{p}}^\times$ and $\Delta = \mathrm{Gal}(K(E[\mathfrak{p}])/K)$. We have an exact sequence

$$0 \to \mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V \to \mathbf{A}_{K_1}^\times/W_1 \to A' \to 0$$

where W_1 is as in Theorem 6.9 and A' is a quotient of A by some power of the class of the prime $\mathcal{P}$ above $\mathfrak{p}$. Since $\mathcal{P}^{\mathbf{N}\mathfrak{p}-1} = \mathfrak{p}$ is principal, $\mathrm{Hom}(A', E[\mathfrak{p}]) = \mathrm{Hom}(A, E[\mathfrak{p}])$. Using Theorem 6.9 we conclude that

$$\mathcal{S}_\pi(E) = 0 \Leftrightarrow \left(\mathrm{Hom}(A, E[\mathfrak{p}])^\Delta = 0 \quad \text{and} \quad \mathrm{Hom}(\mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V, E[\mathfrak{p}])^\Delta = 0\right).$$

By Lemma 6.8, $\delta_1 : \mathcal{O}_{1,\mathfrak{p}}^\times/V \to E[\mathfrak{p}]$ is an isomorphism. Since $E[\mathfrak{p}]$ has no proper Galois-stable submodules, it follows that

$$\mathrm{Hom}(\mathcal{O}_{1,\mathfrak{p}}^\times/\bar{\mathcal{E}}V, E[\mathfrak{p}])^\Delta = 0 \quad \Leftrightarrow \quad \bar{\mathcal{E}} \not\subset V \quad \Leftrightarrow \quad \delta_1(\mathcal{E}) \neq 0.$$

This completes the proof of the corollary. □

7 Elliptic Units

In this section we define elliptic units and relate them to special values of L-functions. Elliptic units will be defined as certain rational functions of x-coordinates of torsion points on a CM elliptic curve. The results of §5 will allow us determine the action of the Galois group on these numbers, and hence their fields of definition. We follow closely [CW1] §5; see also [dS] Chapter II and Robert's original memoir [Ro].

Throughout this section we fix an imaginary quadratic field K with ring of integers $\mathcal{O}$, an elliptic curve E over $\mathbf{C}$ with complex multiplication by $\mathcal{O}$, and a nontrivial ideal $\mathfrak{a}$ of $\mathcal{O}$ prime to 6. For simplicity we will assume that the class number of K is one; see [dS] for the general case.

7.1 Definition and Basic Properties

Definition 7.1. Choose a Weierstrass equation (1) for E with coordinate functions x, y on E. Define a rational function on E

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

where α is a generator of $\mathfrak{a}$ and $\Delta(E)$ is the discriminant of the chosen model of E. Clearly this is independent of the choice of α.

Lemma 7.2. (i) *$\Theta_{E,\mathfrak{a}}$ is independent of the choice of Weierstrass model.*
(ii) *If $\phi : E' \xrightarrow{\sim} E$ is an isomorphism of elliptic curves then $\Theta_{E',\mathfrak{a}} = \Theta_{E,\mathfrak{a}} \circ \phi$.*

(iii) *If E is defined over F then the rational function $\Theta_{E,\mathfrak{a}}$ is defined over F.*

Proof. Any other Weierstrass model has coordinate functions x', y' given by

$$x' = u^2x + r, \quad y' = u^3y + sx + t$$

where $u \in \mathbf{C}^\times$ ([Si] Remark III.1.3), and then $a_i' = u^i a_i$ and

$$\Delta(E') = u^{12}\Delta(E).$$

Since $\#(E[\mathfrak{a}]) = \mathbf{N}\mathfrak{a}$, this proves (i), and (ii) is just a different formulation of (i). For (iii) we need only observe that $\alpha \in F$, $\Delta(E) \in F$, and G_F permutes the set $\{x(P) : P \in E[\mathfrak{a}] - O\}$, so G_F fixes $\Theta_{E,\mathfrak{a}}$. □

Lemma 7.3. *Suppose E is defined over K and $\mathfrak{p}$ is a prime of K where E has good reduction. Fix a Weierstrass model for E which is minimal at $\mathfrak{p}$. Let $\mathfrak{b}$ and $\mathfrak{c}$ be nontrivial relatively prime ideals of $\mathcal{O}$ and $P \in E[\mathfrak{b}]$, $Q \in E[\mathfrak{c}]$ points in $E(\bar{K})$ of exact orders $\mathfrak{b}$ and $\mathfrak{c}$, respectively. Fix an extension of the $\mathfrak{p}$-adic order $\mathrm{ord}_\mathfrak{p}$ to $\bar{K}$, normalized so $\mathrm{ord}_\mathfrak{p}(\mathfrak{p}) = 1$.*

(i) *If $n > 0$ and $\mathfrak{b} = \mathfrak{p}^n$ then $\mathrm{ord}_\mathfrak{p}(x(P)) = -2/(\mathbf{N}\mathfrak{p}^{n-1}(\mathbf{N}\mathfrak{p} - 1))$.*
(ii) *If $\mathfrak{b}$ is not a power of $\mathfrak{p}$ then $\mathrm{ord}_\mathfrak{p}(x(P)) \geq 0$.*
(iii) *If $\mathfrak{p} \nmid \mathfrak{b}\mathfrak{c}$ then $\mathrm{ord}_\mathfrak{p}(x(P) - x(Q)) = 0$.*

Proof. Suppose that $\mathfrak{b} = \mathfrak{p}^n$ with $n \geq 1$. Let $\hat{E}$ be the formal group over $\mathcal{O}_\mathfrak{p}$ associated to E in Theorem 3.7. Let $\pi = \psi_E(\mathfrak{p})$, let $[\pi^m](X) \in \mathcal{O}[[X]]$ be the endomorphism of $\hat{E}$ corresponding to π^m for every m, and define

$$f(X) = [\pi^n](X)/[\pi^{n-1}](X) \in \mathcal{O}[[X]].$$

Since π reduces to the Frobenius endomorphism of the reduction $\tilde{E}$ of E modulo $\mathfrak{p}$ (Corollary 5.16(iii)), it follows from Corollary 3.9 and Proposition 3.14 that

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

Thus by the Weierstrass preparation theorem,

$$f(X) = e(X)u(X)$$

where $e(X)$ is an Eisenstein polynomial of degree $\mathbf{N}\mathfrak{p}^{n-1}(\mathbf{N}\mathfrak{p}-1)$ and $u(X) \in \mathcal{O}[[X]]^\times$.

Since the reduction of π is a purely inseparable endomorphism of $\hat{E}$, Lemma 3.6 shows that $E[\mathfrak{p}^n] \subset E_1(\bar{K}_\mathfrak{p})$. Thus $z = -x(P)/y(P)$ is a root of $f(X)$, and hence of $e(X)$, so $\mathrm{ord}_\mathfrak{p}(x(P)/y(P)) = 1/(\mathbf{N}\mathfrak{p}^{n-1}(\mathbf{N}\mathfrak{p} - 1))$. Now (i) follows from Lemma 3.5.

If $\mathfrak{b}$ is not a power of $\mathfrak{p}$ then by Theorem 3.15(i), $P \notin E_1(\bar{K}_\mathfrak{p})$. Hence by Lemma 3.5, $\mathrm{ord}_\mathfrak{p}(x(P)) \geq 0$, which is (ii). Further, writing $\tilde{P}$ and $\tilde{Q}$ for the reductions of P and Q, we have

$$\mathrm{ord}_\mathfrak{p}(x(P) - x(Q)) > 0 \Leftrightarrow x(\tilde{P}) = x(\tilde{Q}) \Leftrightarrow \tilde{P} = \pm\tilde{Q} \Leftrightarrow$$
$$\Leftrightarrow \widetilde{P \mp Q} = \tilde{O} \Leftrightarrow P \mp Q \in E_1(\bar{K}_\mathfrak{p}).$$

Since $\mathfrak{b}$ and $\mathfrak{c}$ are relatively prime, the order of $P \pm Q$ is not a power of $\mathfrak{p}$. So again by Theorem 3.15(i), $P \pm Q \notin E_1(\bar{K}_\mathfrak{p})$, and (iii) follows. □

For every ideal $\mathfrak{b}$ of $\mathcal{O}$ write $K(\mathfrak{b})$ for the ray class field of K modulo $\mathfrak{b}$.

Theorem 7.4. *Suppose $\mathfrak{b}$ is a nontrivial ideal of $\mathcal{O}$ relatively prime to $\mathfrak{a}$, and $Q \in E[\mathfrak{b}]$ is an $\mathcal{O}$-generator of $E[\mathfrak{b}]$.*

(i) $\Theta_{E,\mathfrak{a}}(Q) \in K(\mathfrak{b})$.

(ii) *If $\mathfrak{c}$ is an ideal of $\mathcal{O}$ prime to $\mathfrak{b}$, c is a generator of $\mathfrak{c}$, and $\sigma_\mathfrak{c} = [\mathfrak{c}, K(\mathfrak{b})/K]$, then*
$$\Theta_{E,\mathfrak{a}}(Q)^{\sigma_\mathfrak{c}} = \Theta_{E,\mathfrak{a}}(cQ).$$

(iii) *If $\mathfrak{b}$ is not a prime power then $\Theta_{E,\mathfrak{a}}(Q)$ is a global unit. If $\mathfrak{b}$ is a power of a prime $\mathfrak{p}$ then $\Theta_{E,\mathfrak{a}}(Q)$ is a unit at primes not dividing $\mathfrak{p}$.*

Proof. Since we assumed that K has class number one, by Corollary 5.13 and Lemma 7.2(i) we may assume that E is defined over K by a Weierstrass model (1). Then by Lemma 7.2(iii) $\Theta_{E,\mathfrak{a}}$ belongs to the function field $K(E)$.

Let ψ be the Hecke character associated to E by Theorem 5.15. Suppose $x \in \prod_\mathfrak{p} \mathcal{O}_\mathfrak{p}^\times \subset \mathbf{A}_K^\times$ and $x \equiv 1 \bmod^\times \mathfrak{b}$, and let $\sigma_x = [x, K^{\mathrm{ab}}/K]$. By Theorem 5.15, $\psi(x) \in \mathcal{O}^\times = \mathrm{Aut}(E)$ and $\sigma_x Q = \psi(x)Q$. Therefore

$$\Theta_{E,\mathfrak{a}}(Q)^{\sigma_x} = \Theta_{E,\mathfrak{a}}(Q^{\sigma_x}) = \Theta_{E,\mathfrak{a}}(\psi(x)Q) = \Theta_{E,\mathfrak{a}}(Q),$$

the last equality by Lemma 7.2(ii). Since these σ_x generate $\mathrm{Gal}(\bar{K}/K(\mathfrak{b}))$, this proves (i).

For (ii), let $x \in \mathbf{A}_K^\times$ be an idele with $x\mathcal{O} = \mathfrak{c}$ and $x_\mathfrak{p} = 1$ for $\mathfrak{p}$ dividing $\mathfrak{b}$. Then Theorem 5.15 shows that $\psi(x) \in c\mathcal{O}^\times$ and $\sigma_\mathfrak{c} Q = \psi(x)Q$. So again using Lemma 7.2(ii),

$$\Theta_{E,\mathfrak{a}}(Q)^{\sigma_\mathfrak{c}} = \Theta_{E,\mathfrak{a}}(\psi(x)Q) = \Theta_{E,\mathfrak{a}}(cQ).$$

This is (ii).

For (iii), let $\mathfrak{p}$ be a prime of K such that $\mathfrak{b}$ is not a power of $\mathfrak{p}$. By Corollary 5.22 and Lemma 7.2, we may assume that our Weierstrass equation for E has good reduction at $\mathfrak{p}$, so that $\Delta(E)$ is prime to $\mathfrak{p}$. Let $n = \mathrm{ord}_\mathfrak{p}(\mathfrak{a})$. Then

$$\mathrm{ord}_\mathfrak{p}(\Theta_{E,\mathfrak{a}}(Q))/6 = -2n - \sum_{P \in E[\mathfrak{p}^n] - O} \mathrm{ord}_\mathfrak{p}(x(Q) - x(P))$$
$$- \sum_{P \in E[\mathfrak{a}] - E[\mathfrak{p}^n]} \mathrm{ord}_\mathfrak{p}(x(Q) - x(P)).$$

By Lemma 7.3, since $\mathfrak{b}$ is not a power of $\mathfrak{p}$,

$$\begin{aligned}&\operatorname{ord}_{\mathfrak{p}}(x(Q)-x(P))\\&\qquad=\begin{cases}-2/(\mathbf{N}\mathfrak{p}^m-\mathbf{N}\mathfrak{p}^{m-1}) & \text{if } P \text{ has order exactly } \mathfrak{p}^m,\ m>0\\ 0 & \text{if the order of } P \text{ is not a power of } \mathfrak{p}.\end{cases}\end{aligned}$$

From this one verifies easily that $\operatorname{ord}_{\mathfrak{p}}(\Theta_{E,\mathfrak{a}}(Q))=0$. □

7.2 The Distribution Relation

Lemma 7.5. *$\Theta_{E,\mathfrak{a}}$ is a rational function on E with divisor*

$$12\mathbf{N}\mathfrak{a}[O]-12\sum_{P\in E[\mathfrak{a}]}[P].$$

Proof. The coordinate function x is an even rational function with a double pole at O and no other poles. Thus for every point P, the divisor of $x-x(P)$ is $[P]+[-P]-2[O]$ and the lemma follows easily. □

Theorem 7.6. *Suppose $\mathfrak{b}$ is and ideal of $\mathcal{O}$ relatively prime to $\mathfrak{a}$, and β is a generator of $\mathfrak{b}$. Then for every $P\in E(\bar{K})$,*

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

Proof. Lemmas 7.2(iii) and 7.5 show that both sides of the equation in the theorem are rational functions on E, defined over K, with divisor

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

Thus their ratio is a constant $\lambda\in K^\times$, and we need to show that $\lambda=1$.

Let $w_K=\#(\mathcal{O}^\times)$ and fix a generator α of $\mathfrak{a}$. Evaluating this ratio at $P=O$ one sees that

$$\lambda=\frac{\Delta(E)^{(\mathbf{N}\mathfrak{a}-1)(\mathbf{N}\mathfrak{b}-1)}}{\alpha^{12(\mathbf{N}\mathfrak{b}-1)}\beta^{12(\mathbf{N}\mathfrak{a}-1)}}\prod_{\substack{R\in E[\mathfrak{b}]\\ R\neq 0}}\prod_{\substack{P\in E[\mathfrak{a}]\\ P\neq 0}}(x(R)-x(P))^{-6}=\mu^{w_K}$$

with

$$\mu=\frac{\Delta(E)^{(\mathbf{N}\mathfrak{a}-1)(\mathbf{N}\mathfrak{b}-1)/w_K}}{\alpha^{12(\mathbf{N}\mathfrak{b}-1)/w_K}\beta^{12(\mathbf{N}\mathfrak{a}-1)/w_K}}\prod(x(R)-x(P))^{-12/w_K},$$

where the final product is over $R\in E[\mathfrak{b}]-O$ and $P\in(E[\mathfrak{a}]-O)/\pm1$ (recall $\mathfrak{a}$ is prime to 6). Since w_K divides 12, all of the exponents in the definition of μ are integers.

Exactly as in the proof of Theorem 7.4(iii), one can show that $\mu\in\mathcal{O}^\times$, and therefore $\lambda=1$. □

Corollary 7.7. *Suppose $\mathfrak{b}$ is an ideal of $\mathcal{O}$ prime to $\mathfrak{a}$, $Q \in E[\mathfrak{b}]$ has order exactly $\mathfrak{b}$, $\mathfrak{p}$ is a prime dividing $\mathfrak{b}$, π is a generator of $\mathfrak{p}$, and $\mathfrak{b}' = \mathfrak{b}/\mathfrak{p}$. If the reduction map $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{b}')^\times$ is injective then*

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

where in the latter case $\mathrm{Frob}_\mathfrak{p}$ *is the Frobenius of* $\mathfrak{p}$ *in* $\mathrm{Gal}(K(\mathfrak{b}')/K)$.

Proof. Let C denote the multiplicative group $1 + \mathfrak{b}'(\mathcal{O}/\mathfrak{b})$. Because of our hypotheses that $\mathcal{O}^\times$ injects into $(\mathcal{O}/\mathfrak{b}')^\times$, C is isomorphic to the kernel of the map

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

Thus class field theory gives an isomorphism

$$C \xrightarrow{\sim} \mathrm{Gal}(K(\mathfrak{b})/K(\mathfrak{b}'))$$

which we will denote by $c \mapsto \sigma_c$. Therefore

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

by Theorem 7.4(ii).

One sees easily that

$$\begin{aligned} \{cQ : c \in C\} &= \{P \in E[\mathfrak{b}] : \pi P = \pi Q \text{ and } P \notin E[\mathfrak{b}']\} \\ &= \begin{cases} \{Q + R : R \in E[\mathfrak{p}]\} & \text{if } \mathfrak{p} \mid \mathfrak{b}' \\ \{Q + R : R \in E[\mathfrak{p}], R \not\equiv -Q \pmod{E[\mathfrak{b}']}\} & \text{if } \mathfrak{p} \nmid \mathfrak{b}' \end{cases} \end{aligned}$$

Thus if $\mathfrak{p} \mid \mathfrak{b}'$

$$\mathbf{N}_{K(\mathfrak{b})/K(\mathfrak{b}')}\Theta_{E,\mathfrak{a}}(Q) = \prod_{R \in E[\mathfrak{p}]} \Theta_{E,\mathfrak{a}}(Q + R) = \Theta_{E,\mathfrak{a}}(\pi Q)$$

by Theorem 7.6. Similarly, if $\mathfrak{p} \nmid \mathfrak{b}'$

$$\Theta_{E,\mathfrak{a}}(Q + R_0)\mathbf{N}_{K(\mathfrak{b})/K(\mathfrak{b}')}\Theta_{E,\mathfrak{a}}(Q) = \Theta_{E,\mathfrak{a}}(\pi Q)$$

where $R_0 \in E[\mathfrak{p}]$ satisfies $Q + R_0 \in E[\mathfrak{b}']$. But then by Theorem 7.4(ii) (note that our assumption on $\mathfrak{b}'$ implies that $\mathfrak{b}' \neq \mathcal{O}$)

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

so this completes the proof. □

7.3 Elliptic Curves over K

Since the function $\Theta_{E,\mathfrak{a}}$ depends only on the isomorphism class of E over $\mathbf{C}$, we need to provide it with information that depends on E itself to make it sensitive enough to "see" the value of the L-function of E at 1. Following Coates and Wiles [CW1] we will write down a product of translates of $\Theta_{E,\mathfrak{a}}$ and then show that it has the connections we need with L-values.

From now on suppose that our elliptic curve E is defined over K, ψ is the Hecke character attached to E by Theorem 5.15, $\mathfrak{f}$ is the conductor of ψ, and $\mathfrak{a}$ is prime to $\mathfrak{f}$ as well as to 6. For $P \in E(\bar{K})$ let τ_P denote translation P, so τ_P is a rational function defined over $K(P)$.

Fix an $\mathcal{O}$-generator S of $E[\mathfrak{f}]$. By Corollary 5.20(i) $S \in E(K(\mathfrak{f}))$, and we define

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

Proposition 7.8. (i) *$\Lambda_{E,\mathfrak{a}}$ is a rational function defined over K.*

(ii) *If B is a set of ideals of $\mathcal{O}$, prime to $\mathfrak{af}$, such that the Artin map $\mathfrak{b} \mapsto [\mathfrak{b}, K(\mathfrak{f})/K]$ is a bijection from B to $\mathrm{Gal}(K(\mathfrak{f})/K)$, then*

$$\Lambda_{E,\mathfrak{a}}(P) = \prod_{\mathfrak{b} \in B} \Theta_{E,\mathfrak{a}}(\psi(\mathfrak{b})S + P).$$

(iii) *If $\mathfrak{r}$ is an ideal of $\mathcal{O}$ and $Q \in E[\mathfrak{r}]$, $Q \notin E[\mathfrak{f}]$, then $\Lambda_{E,\mathfrak{a}}(Q)$ is a global unit in $K(E[\mathfrak{r}])$.*

Proof. The first assertion is clear, (ii) is immediate from Corollary 5.16(ii), and (iii) follows from Theorem 7.4(iii). □

7.4 Expansions over C

We continue to suppose that E is defined over K. Fix a Weierstrass model of E (over K) and let $L \subset \mathbf{C}$ be the corresponding lattice given by Theorem 2.3(ii); then $\mathcal{O}L = L$ (Proposition 2.6) so we can choose $\Omega \in \mathbf{C}^\times$ such that $L = \Omega\mathcal{O}$. The map $\xi(z) = (\wp(z; L), \wp'(z; L)/2)$ is an isomorphism $\mathbf{C}/L \xrightarrow{\sim} E(\mathbf{C})$, and we define $\Theta_{L,\mathfrak{a}} = \Theta_{E,\mathfrak{a}} \circ \xi$, i.e.,

$$\Theta_{L,\mathfrak{a}}(z) = \alpha^{-12} \Delta(L)^{\mathbf{N}\mathfrak{a}-1} \prod_{u \in \mathfrak{a}^{-1}L/L-0} (\wp(z; L) - \wp(u; L))^{-6}.$$

Definition 7.9. Define

$$\begin{aligned}
&A(L) = \pi^{-1}\mathrm{area}(\mathbf{C}/L),\\
&s_2(L) = \lim_{s \to 0^+} \sum_{0 \neq \omega \in L} \omega^{-2}|\omega|^{-2s},\\
&\eta(z; L) = A(L)^{-1}\bar{z} + s_2(L)z,\\
&\theta(z; L) = \Delta(L)e^{-6\eta(z;L)z}\sigma(z; L)^{12}.
\end{aligned}$$

Lemma 7.10. $\Theta_{L,\mathfrak{a}}(z) = \theta(z;L)^{\mathbf{N}\mathfrak{a}}/\theta(z;\mathfrak{a}^{-1}L)$.

Proof. Write $f(z) = \theta(z;L)^{\mathbf{N}\mathfrak{a}}/\theta(z;\mathfrak{a}^{-1}L)$. Note that although $\theta(z;L)$ is not holomorphic (because of the $\bar{z}$ in the definition of $\eta(z;L)$), $f(z)$ is holomorphic. One can check explicitly, using well-known properties of $\sigma(z;L)$ (see [dS] §II.2.1), that $f(z)$ is periodic with respect to L and its divisor on $\mathbf{C}/L$ is $12\mathbf{N}\mathfrak{a}[0] - 12\sum_{v\in\mathfrak{a}^{-1}L/L}[v]$.

Thus by Lemma 7.5, $\Theta_{L,\mathfrak{a}} = \lambda f$ for some $\lambda \in \mathbf{C}^\times$. At $z = 0$, both functions have Laurent series beginning $\alpha^{-12}\Delta(L)^{\mathbf{N}\mathfrak{a}-1}z^{12(\mathbf{N}\mathfrak{a}-1)}$, so $\lambda = 1$. □

Definition 7.11. for $k \geq 1$ define the Eisenstein series

$$\begin{aligned} E_k(z;L) &= \lim_{s\to k}\sum_{\omega\in L}\frac{(\bar{z}+\bar{\omega})^k}{|z+\omega|^{2s}} \\ &= \sum_{\omega\in L}\frac{1}{(z+\omega)^k} \quad \text{if } k \geq 3 \end{aligned}$$

where the limit means evaluation of the analytic continuation at $s = k$.

Proposition 7.12.

$$\begin{aligned} &E_1(z;L) = \log(\sigma(z;L))' - s_2(L)z - A(L)^{-1}\bar{z}, \\ &E_2(z;L) = \wp(z;L) + s_2(L), \\ &E_k(z;L) = \frac{(-1)^k}{(k-1)!}\left(\frac{d}{dz}\right)^{(k-2)}\wp(z;L) \quad \textit{if } k \geq 3. \end{aligned}$$

Proof. The third equality is immediate from the definition of $\wp(z;L)$. For the first two, see [CW1] pp. 242–243 or [GS] Proposition 1.5. □

Theorem 7.13. *For every* $k \geq 1$,

$$\left(\frac{d}{dz}\right)^k \log\Theta_{L,\mathfrak{a}}(z) = 12(-1)^{k-1}(k-1)!(\mathbf{N}\mathfrak{a}E_k(z;L) - E_k(z;\mathfrak{a}^{-1}L)).$$

Proof. By Lemma 7.10

$$\left(\frac{d}{dz}\right)^k \log\Theta_{L,\mathfrak{a}}(z) = \left(\frac{d}{dz}\right)^{k-1}\left(\mathbf{N}\mathfrak{a}\frac{d}{dz}\log(\theta(z;L)) - \frac{d}{dz}\log(\theta(z;\mathfrak{a}^{-1}L))\right).$$

The definition of θ shows that

$$\log(\theta(z;L)) = \log(\Delta(L)) - 6s_2(L)z^2 - 6A(L)^{-1}z\bar{z} + 12\log(\sigma(z;L)).$$

Now the theorem follows from Proposition 7.12 □

Definition 7.14. Define the Hecke L-functions associated to powers of $\bar{\psi}$ to be the analytic continuations of the Dirichlet series

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

summing over ideals $\mathfrak{b}$ of $\mathcal{O}$ prime to the conductor of $\bar{\psi}^k$. If $\mathfrak{m}$ is an ideal of $\mathcal{O}$ divisible by $\mathfrak{f}$ and $\mathfrak{c}$ is an ideal prime to $\mathfrak{m}$, we define the partial L-function $L_{\mathfrak{m}}(\bar{\psi}^k, s, \mathfrak{c})$ be the same formula, but with the sum restricted to ideals of K prime to $\mathfrak{m}$ such that $[\mathfrak{b}, K(\mathfrak{m})/K] = [\mathfrak{c}, K(\mathfrak{m})/K]$.

Recall that $\Omega \in \mathbf{C}^\times$ is such that $L = \Omega\mathcal{O}$.

Proposition 7.15. *Suppose $v \in KL/L$ has order $\mathfrak{m}$, where $\mathfrak{m}$ is divisible by $\mathfrak{f}$. Then for every $k \geq 1$,*

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

where $\mathfrak{c} = \Omega^{-1}v\mathfrak{m}$.

Proof. Let μ be a generator of $\mathfrak{m}$, so that $v = \alpha\Omega/\mu$ for some $\alpha \in \mathcal{O}$ prime to $\mathfrak{m}$. For s large,

$$\sum_{\omega \in L} \frac{(\bar{v} + \bar{\omega})^k}{|v + \omega|^{2s}} = \frac{\mathbf{N}\mu^s}{\bar{\mu}^k} \frac{\bar{\Omega}^k}{|\Omega|^{2s}} \sum_{\beta \in \mathcal{O}, \beta \equiv \alpha \pmod{\mathfrak{m}}} \frac{\bar{\beta}^k}{|\beta|^{2s}}.$$

By Corollary 5.16(i), if we define

$$\epsilon(\beta) = \psi(\beta\mathcal{O})/\beta$$

then ϵ is a multiplicative map from $\{\beta \in \mathcal{O} : \beta \text{ is prime to } \mathfrak{f}\}$ to $\mathcal{O}^\times$. By definition of the conductor, ϵ factors through $(\mathcal{O}/\mathfrak{f})^\times$. Thus if $\beta \equiv \alpha \pmod{\mathfrak{m}}$,

$$\bar{\beta} = \bar{\psi}(\beta\mathcal{O})\frac{\psi(\alpha\mathcal{O})}{\alpha}.$$

Therefore

$$\begin{aligned}\sum_{\beta \in \mathcal{O}, \beta \equiv \alpha \pmod{\mathfrak{m}}} \frac{\bar{\beta}^k}{|\beta|^{2s}} &= \frac{\psi(\alpha\mathcal{O})^k}{\alpha^k} \sum_{\mathfrak{b} \subset \mathcal{O}, [\mathfrak{b}, K(\mathfrak{m})/K] = [\alpha\mathcal{O}, K(\mathfrak{m})/K]} \frac{\bar{\psi}(\mathfrak{b})^k}{\mathbf{N}\mathfrak{b}^s} \\ &= \frac{\psi(\mathfrak{c})^k}{\alpha^k} L_{\mathfrak{m}}(\bar{\psi}^k, s, \sigma_{\mathfrak{c}})\end{aligned}$$

and the proposition follows. □

Definition 7.16. Fix a generator f of $\mathfrak{f}$ and a set B of ideals of $\mathcal{O}$, prime to $\mathfrak{a}\mathfrak{f}$, such that the Artin map $\mathfrak{b} \mapsto [\mathfrak{b}, K(\mathfrak{f})/K]$ is a bijection from B to $\mathrm{Gal}(K(\mathfrak{f})/K)$. Let $u = \Omega/f \in \mathfrak{f}^{-1}L$ and define

$$\Lambda_{L,\mathfrak{a}}(z) = \Lambda_{L,\mathfrak{a},f}(z) = \Lambda_{E,\mathfrak{a},\xi(u)}(\xi(z)) = \prod_{\mathfrak{b} \in B} \Theta_{L,\mathfrak{a}}(\psi(\mathfrak{b})u + z).$$

By Proposition 7.8(ii), $\Lambda_{L,\mathfrak{a}} = \Lambda_{E,\mathfrak{a}} \circ \xi$.

Theorem 7.17. *For every $k \geq 1$,*

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

Proof. By Theorem 7.13

$$\begin{aligned}\left(\frac{d}{dz}\right)^k \log \Lambda_{L,\mathfrak{a}}(z) \mid_{z=0} &= \sum_{\mathfrak{b}\in B}\left(\frac{d}{dz}\right)^k \log \Theta_{L,\mathfrak{a}}(z) \mid_{z=\psi(\mathfrak{b})u} \\ = 12(-1)^{k-1}(k-1)! &\left(\mathbf{N}\mathfrak{a}\sum_{\mathfrak{b}\in B} E_k(\psi(\mathfrak{b})u; L) - \sum_{\mathfrak{b}\in B} E_k(\psi(\mathfrak{b})u; \mathfrak{a}^{-1}L)\right).\end{aligned}$$

By Proposition 7.15,

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

By inspection (and Corollary 5.16(i)) $E_k(z; \mathfrak{a}^{-1}L) = \psi(\mathfrak{a})^k E_k(\psi(\mathfrak{a})z; L)$, so

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

□

Although we will not use it explicitly, the following theorem of Damerell is a corollary of this computation.

Corollary 7.18 (Damerell's Theorem). *For every $k \geq 1$,*

$$\Omega^{-k}L(\bar{\psi}^k, k) \in K.$$

Proof. By Proposition 7.8(i), $\Lambda_{L,\mathfrak{a}}(z)$ is a rational function of $\wp(z; L)$ and $\wp'(z; L)$ with coefficients in K. Differentiating the relation (from Theorem 2.3)

$$\wp'(z; L)^2 = 4\wp(z; L)^3 + 4a\wp(z; L) + 4b$$

shows that all derivatives $\wp^{(k)}(z; L)$ also belong to $K(\wp(z; L), \wp'(z; L))$, and hence $\Lambda^{(k)}_{L,\mathfrak{a}}$ does as well. Thus the corollary follows from Theorem 7.17. □

7.5 $\mathfrak{p}$-adic Expansions

Keep the notation of the previous sections. Fix a prime $\mathfrak{p}$ of K where E has good reduction, $\mathfrak{p} \nmid 6$. Suppose that our chosen Weierstrass model of E has good reduction at $\mathfrak{p}$ and that the auxiliary ideal $\mathfrak{a}$ is prime to $\mathfrak{p}$ as well as $6\mathfrak{f}$. Let $\hat{E}$ be the formal group attached to E over $\mathcal{O}_{\mathfrak{p}}$ as in §3.2, and $x(Z), y(Z) \in \mathcal{O}_{\mathfrak{p}}[[Z]]$ the power series of Theorem 3.7.

Definition 7.19. Let $\lambda_{\hat{E}}(Z) \in Z + Z^2 K_{\mathfrak{p}}[[Z]]$ be the logarithm map of $\hat{E}$ from Definition 3.10, so that $\lambda'_{\hat{E}}(Z) \in \mathcal{O}_{\mathfrak{p}}[[Z]]^{\times}$, and define an operator D on $\mathcal{O}_{\mathfrak{p}}[[Z]]$ by

$$D = \frac{1}{\lambda'_{\hat{E}}(Z)} \frac{d}{dZ}.$$

Proposition 7.20. *Identifying (x, y) both with $(\wp(z; L), \frac{1}{2}\wp'(z; L))$ and with $(x(Z), y(Z))$ leads to a commutative diagram*

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

Proof. Differentiating the relation $\wp'(z)^2 = 4\wp(z)^3 + 4a\wp(z) + 4b$ shows that

$$\wp''(z) = 6\wp(x)^2 + 2a \in K_{\mathfrak{p}}(\wp(z), \wp'(z)).$$

Thus, since both vertical maps are derivations, we need only check that $D(x(Z)) = 2y(Z)$ and $D(y(Z)) = 3x(Z)^2 + a$. (In fact, it would be enough to check either equality.) Both equalities are immediate from the definition (Definition 3.10) of $\hat{\omega}$ and $\lambda_{\hat{E}}$. □

Definition 7.21. Let $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z)$ be the image of $\Lambda_{E,\mathfrak{a}}$ in $K_{\mathfrak{p}}((Z))$ under the map of Proposition 7.20.

Theorem 7.22. (i) $\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) \in \mathcal{O}_{\mathfrak{p}}[[Z]]^{\times}$.
(ii) *For every $k \geq 1$,*

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

Proof. Fix an embedding $\bar{K} \hookrightarrow \bar{K_{\mathfrak{p}}}$ so that we can view $x(R) \in \bar{K_{\mathfrak{p}}}$ when $R \in E[\mathfrak{f}]$. Let $\mathcal{R}$ be the ring of integers of $\bar{K_{\mathfrak{p}}}$.

Consider one of the factors $x(\psi(\mathfrak{b})S + P) - x(Q)$ of $\Lambda_{E,\mathfrak{a}}(P)$, with $Q \in E[\mathfrak{a}] - O$. The explicit addition law for $x(P)$ ([Si] §III.2.3) shows that

$$x(\psi(\mathfrak{b})S + P) - x(Q) = \frac{(y(P) - y(\psi(\mathfrak{b})S))^2}{(x(P) - x(\psi(\mathfrak{b})S))^2} - x(P) - x(\psi(\mathfrak{b})S) - x(Q).$$

By Lemmas 7.3(ii) and 3.5, $x(\psi(\mathfrak{b})S), y(\psi(\mathfrak{b})S), x(Q) \in \mathcal{R}$. Substituting $x(Z)$ for $x(P)$, $y(Z)$ for $y(P)$ and using the expansions in Theorem 3.7 to show that

$$x(Z) \in Z^{-2} + Z\mathcal{O}_{\mathfrak{p}}[[Z]], \quad y(Z) \in -Z^{-3} + \mathcal{O}_{\mathfrak{p}}[[Z]]$$

gives

$$x(\psi(\mathfrak{b})S + P) - x(Q) \quad \mapsto \quad g_{\mathfrak{b},Q}(Z) \in \mathcal{R}[[Z]]$$

under the map of Proposition 7.20, where $g_{\mathfrak{b},Q}$ satisfies

$$g_{\mathfrak{b},Q}(0) = x(\psi(\mathfrak{b})S) - x(Q) \in \mathcal{R}^\times$$

by Lemma 7.3(iii), so $g_{\mathfrak{b},Q}(Z) \in \mathcal{R}[[Z]]^\times$. Also $\Delta(E), \alpha \in \mathcal{O}_{\mathfrak{p}}^\times$ since our Weierstrass equation has good reduction at $\mathfrak{p}$ and $\mathfrak{p} \nmid \mathfrak{a}$. Thus

$$\Lambda_{\mathfrak{p},\mathfrak{a}}(Z) = \Delta(E)^{(\mathbf{N}\mathfrak{a}-1)\#(B)} \alpha^{-12\#(B)} \prod_{\mathfrak{b},Q} g_{\mathfrak{b},Q}(Z)^{-6} \in \mathcal{R}[[Z]]^\times.$$

Since we already know $\Lambda_{\mathfrak{p},\mathfrak{a}} \in K_{\mathfrak{p}}((Z))$, this proves (i).

The second assertion is immediate from Theorem 7.17 and Proposition 7.20. □

8 Euler Systems

In this section we introduce Kolyvagin's concept of an Euler system (of which the elliptic units of §7 are an example) and we show how to use an Euler system to construct certain principal ideals in abelian extensions of K. In the next section we use these principal ideals (viewed as relations in ideal class groups) to bound the ideal class groups of abelian extensions of K.

As in the previous section, fix an imaginary quadratic field K and an elliptic curve E defined over K with complex multiplication by the ring of integers $\mathcal{O}$ of K. Let $\mathfrak{f}$ be the conductor of the Hecke character ψ of E, and fix a generator f of $\mathfrak{f}$.

Fix a prime $\mathfrak{p}$ of K not dividing $6\mathfrak{f}$, and for $n \geq 1$ let $K_n = K(E[\mathfrak{p}^n])$. Let p denote the rational prime below $\mathfrak{p}$. Fix a nontrivial ideal $\mathfrak{a}$ of $\mathcal{O}$ prime to $6\mathfrak{f}\mathfrak{p}$. Let $\mathcal{R} = \mathcal{R}(\mathfrak{a})$ denote the set of squarefree ideals of $\mathcal{O}$ prime to $6\mathfrak{f}\mathfrak{a}\mathfrak{p}$, and if $\mathfrak{r} \in \mathcal{R}$ let $K_n(\mathfrak{r}) = K_n(E[\mathfrak{r}]) = K(E[\mathfrak{r}\mathfrak{p}^n])$. The letter $\mathfrak{q}$ will always denote a prime of $\mathcal{R}$.

Also as in the previous section, fix a Weierstrass model of E which is minimal at $\mathfrak{p}$, let $L = \Omega\mathcal{O} \subset \mathbf{C}$ be the corresponding lattice given by Theorem 2.3(ii), and define $\xi = (\wp(\,\cdot\,; L), \wp'(\,\cdot\,; L)/2) : \mathbf{C}/L \xrightarrow{\sim} E(\mathbf{C})$.

8.1 The Euler System

Definition 8.1. If $\mathfrak{r} \in \mathcal{R}$ and $n \geq 0$ define

$$\eta_n(\mathfrak{r}) = \eta_n^{(\mathfrak{a})}(\mathfrak{r}) = \Lambda_{E,\mathfrak{a},\xi(\Omega/f)}(\xi(\psi(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega)) = \Lambda_{L,\mathfrak{a}}(\psi(\mathfrak{p}^n\mathfrak{r})^{-1}\Omega).$$

where $\Lambda_{L,\mathfrak{a}}$ is as in Definition 7.16.

Proposition 8.2. *Suppose* $\mathfrak{r} \in \mathcal{R}$ *and* $n \geq 1$.

(i) $\eta_n(\mathfrak{r})$ *is a global unit in* $K_n(\mathfrak{r})$.

(ii) *If $\mathfrak{q}$ is a prime and $\mathfrak{r}\mathfrak{q} \in \mathcal{R}$, then*

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

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

Proof. Assertion (i) is just a restatement of Proposition 7.8(iii), and (ii) and (iii) are immediate from Corollary 7.7. □

8.2 Kolyvagin's Derivative Construction

Definition 8.3. Write $G_{\mathfrak{r}} = \mathrm{Gal}(K_n(\mathfrak{r})/K_n)$. By Corollary 5.20(ii), $G_{\mathfrak{r}}$ is independent of $n \geq 1$, and we have natural isomorphisms

$$\begin{tikzcd}
G_{\mathfrak{r}} \arrow[r, equal] \arrow[d] & \prod_{\mathfrak{q}|\mathfrak{r}} G_{\mathfrak{q}} \arrow[d] \\
(\mathcal{O}/\mathfrak{r})^{\times} \arrow[r, equal] & \prod_{\mathfrak{q}|\mathfrak{r}} (\mathcal{O}/\mathfrak{q})^{\times}.
\end{tikzcd}$$

If $\mathfrak{q} \mid \mathfrak{r}$ this allows us to view $G_{\mathfrak{q}}$ either as a quotient or a subgroup of $G_{\mathfrak{r}}$. By Corollary 5.20 if $\mathfrak{q}\mathfrak{r} \in \mathcal{R}$ then $K_n(\mathfrak{q}\mathfrak{r})/K_n(\mathfrak{r})$ is cyclic of degree $\mathbf{N}\mathfrak{q} - 1$, totally ramified at all primes above $\mathfrak{q}$ and unramified at all other primes.

For every $\mathfrak{r} \in \mathcal{R}$ define

$$N_{\mathfrak{r}} = \sum_{\sigma \in G_{\mathfrak{r}}} \sigma \in \mathbf{Z}[G_{\mathfrak{r}}]$$

so we clearly have

$$N_{\mathfrak{r}} = \prod_{\mathfrak{q}|\mathfrak{r}} N_{\mathfrak{q}}.$$

For every $n \geq 1$ and $\mathfrak{r} \in \mathcal{R}$, let $x_{n,\mathfrak{r}}$ be an indeterminate and define $X_{n,\mathfrak{r}}$ to be the $\mathrm{Gal}(K_n(\mathfrak{r})/K)$-module $Y_{n,\mathfrak{r}}/Z_{n,\mathfrak{r}}$ where

$$\begin{aligned}
Y_{n,\mathfrak{r}} &= \bigoplus_{\mathfrak{s}|\mathfrak{r}} \mathbf{Z}[\mathrm{Gal}(K_n(\mathfrak{s})/K)]x_{n,\mathfrak{s}}, \\
Z_{n,\mathfrak{r}} &= \sum_{\mathfrak{q}\mathfrak{s}|\mathfrak{r}} \mathbf{Z}[\mathrm{Gal}(K_n(\mathfrak{r})/K)]\left(N_{\mathfrak{q}}x_{n,\mathfrak{q}\mathfrak{s}} - (1-\mathrm{Frob}_{\mathfrak{q}}^{-1})x_{n,\mathfrak{s}}\right) \subset Y_{n,\mathfrak{r}}.
\end{aligned}$$

In other words, $X_{n,\mathfrak{r}}$ is the quotient of the free $\mathbf{Z}[\mathrm{Gal}(K_n(\mathfrak{r})/K)]$-module on $\{x_{n,\mathfrak{s}} : \mathfrak{s} \mid \mathfrak{r}\}$ by the relations

- $G_{\mathfrak{r}/\mathfrak{s}}$ acts trivially on $x_{n,\mathfrak{s}}$, and
- $N_{\mathfrak{q}}x_{n,\mathfrak{q}\mathfrak{s}} = (1-\mathrm{Frob}_{\mathfrak{q}}^{-1})x_{n,\mathfrak{s}}$ if $\mathfrak{q}\mathfrak{s} \mid \mathfrak{r}$.

For every prime $\mathfrak{q} \in \mathcal{R}$ fix once and for all a generator $\sigma_{\mathfrak{q}}$ of $G_{\mathfrak{q}}$ and define

$$D_{\mathfrak{q}} = \sum_{i=1}^{\mathbf{N}\mathfrak{q}-2} i\sigma_{\mathfrak{q}}^i \in \mathbf{Z}[G_{\mathfrak{q}}]$$

and for $\mathfrak{r} \in \mathcal{R}$

$$D_{\mathfrak{r}} = \prod_{\mathfrak{q}|\mathfrak{r}} D_{\mathfrak{q}} \in \mathbf{Z}[G_{\mathfrak{r}}].$$

If M is a power of p and $n \geq 1$ define $\mathcal{R}_{n,M} \subset \mathcal{R}$ to be the set of ideals $\mathfrak{r} \in \mathcal{R}$ such that for every prime $\mathfrak{q}$ dividing $\mathfrak{r}$,

– $\mathfrak{q}$ splits completely in K_n/K
– $\mathbf{N}\mathfrak{q} \equiv 1 \pmod{M}$.

Proposition 8.4. *Suppose M is a power of p, $n \geq 1$, and $\mathfrak{r} \in \mathcal{R}_{n,M}$.*

(i) *$X_{n,\mathfrak{r}}$ has no $\mathbf{Z}$-torsion.*
(ii) *$D_{\mathfrak{r}} x_{n,\mathfrak{r}} \in (X_{n,\mathfrak{r}}/MX_{n,\mathfrak{r}})^{G_{\mathfrak{r}}}$.*

Proof. For every prime $\mathfrak{q} \in \mathcal{R}$ and divisor $\mathfrak{s}$ of $\mathfrak{r}$, define

$$\begin{aligned} B_{\mathfrak{q}} &= G_{\mathfrak{q}} - \{1\}, \\ B_{\mathfrak{s}} &= \prod_{\mathfrak{q}|\mathfrak{s}} B_{\mathfrak{q}} = \left\{ \prod_{\mathfrak{q}|\mathfrak{s}} g_{\mathfrak{q}} : g_q \in B_{\mathfrak{q}} \right\} \subset G_{\mathfrak{r}}, \\ B &= \cup_{\mathfrak{s}|\mathfrak{r}} B_{\mathfrak{s}} x_{n,\mathfrak{s}} \subset X_{n,\mathfrak{r}} \end{aligned}$$

Then one can show by an easy combinatorial argument (see [Ru2] Lemma 2.1) that $X_{n,\mathfrak{r}}$ is a free $\mathbf{Z}$-module with basis B, which proves (i).

Note that

$$(\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{q}} = \mathbf{N}\mathfrak{q} - 1 - N_{\mathfrak{q}}.$$

We will prove (ii) by induction on the number of primes dividing $\mathfrak{r}$. Suppose $\mathfrak{q} \mid \mathfrak{r}$, $\mathfrak{r} = \mathfrak{q}\mathfrak{s}$. Then

$$\begin{aligned} (\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{r}} x_{n,\mathfrak{r}} &= (\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{q}} D_{\mathfrak{s}} x_{n,\mathfrak{r}} \\ &= (\mathbf{N}\mathfrak{q} - 1)D_{\mathfrak{s}} x_{n,\mathfrak{r}} - (1 - \mathrm{Frob}_{\mathfrak{q}}^{-1})D_{\mathfrak{s}} x_{n,\mathfrak{s}}. \end{aligned}$$

Since $\mathfrak{q} \in \mathcal{R}_{n,M}$, $M \mid \mathbf{N}\mathfrak{q} - 1$ and $\mathrm{Frob}_{\mathfrak{q}} \in G_{\mathfrak{s}}$, so by the induction hypothesis

$$(\sigma_{\mathfrak{q}} - 1)D_{\mathfrak{r}} x_{n,\mathfrak{r}} \in MX_{n,\mathfrak{r}}.$$

Since the $\sigma_{\mathfrak{q}}$ generate $G_{\mathfrak{r}}$, this proves the proposition. □

Definition 8.5. An *Euler system* is a collection of global units

$$\{\boldsymbol{\eta}(n,\mathfrak{r}) \in K_n(\mathfrak{r})^\times : n \geq 1, \mathfrak{r} \in \mathcal{R}\}$$

satisfying

$$\mathbf{N}_{K_n(\mathfrak{q}\mathfrak{r})/K_n(\mathfrak{r})}\boldsymbol{\eta}(n,\mathfrak{q}\mathfrak{r}) = \boldsymbol{\eta}(n,\mathfrak{r})^{1-\mathrm{Frob}_\mathfrak{q}^{-1}}, \tag{8}$$

$$\mathbf{N}_{K_{n+1}(\mathfrak{r})/K_n(\mathfrak{r})}\boldsymbol{\eta}(n+1,\mathfrak{r}) = \boldsymbol{\eta}(n,\mathfrak{r}). \tag{9}$$

Equivalently, an Euler system is a Galois equivariant map

$$\boldsymbol{\eta} : \varinjlim_{n,\mathfrak{r}} X_{n,\mathfrak{r}} \to \bigcup_{n,\mathfrak{r}} K_n(\mathfrak{r})^\times$$

such that $\boldsymbol{\eta}(x_{n,\mathfrak{r}})$ is a global unit for every n and $\mathfrak{r}$. We will use these two definitions interchangeably.

For example, by Proposition 8.2 we can define an Euler system by

$$\boldsymbol{\eta}(n,\mathfrak{r}) = \eta_n(\mathfrak{r}).$$

Proposition 8.6. *Suppose $\boldsymbol{\eta}$ is an Euler system and $\mathfrak{q} \in \mathcal{R}$ is a prime. Write $\mathbf{N}\mathfrak{q} - 1 = dp^k$ with d prime to p. Then for every $n \geq 1$ and every $\mathfrak{r} \in \mathcal{R}$ prime to $\mathfrak{q}$,*

$$\boldsymbol{\eta}(n,\mathfrak{q}\mathfrak{r})^d \equiv \boldsymbol{\eta}(n,\mathfrak{r})^{d\mathrm{Frob}_\mathfrak{q}^{-1}}$$

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

Proof. Suppose $m \geq n$, and let $G = \mathrm{Gal}(K_m(\mathfrak{q}\mathfrak{r})/K_n(\mathfrak{q}\mathfrak{r}))$. Fix a prime $\mathfrak{Q}$ of $K_m(\mathfrak{q}\mathfrak{r})$ above $\mathfrak{q}$, and let H be the decomposition group of $\mathfrak{q}$ in G. Let $H' \subset G$ be a set of coset representatives for G/H, and define

$$N_H = \sum_{\gamma \in H} \gamma, \quad N_{H'} = \sum_{\gamma \in H'} \gamma$$

so that $N_H N_{H'} = \sum_{\gamma \in G} \gamma$.

Since $\mathfrak{q}$ is totally ramified in $K_m(\mathfrak{q}\mathfrak{r})/K_m(\mathfrak{r})$, the Euler system distribution relation (8) reduces modulo $\mathfrak{Q}$ to

$$\boldsymbol{\eta}(m,\mathfrak{q}\mathfrak{r})^{\mathbf{N}\mathfrak{q}-1} \equiv (\boldsymbol{\eta}(m,\mathfrak{r})^{\mathrm{Frob}_\mathfrak{q}^{-1}})^{\mathbf{N}\mathfrak{q}-1} \pmod{\mathfrak{Q}}.$$

On the other hand, since H is generated by the Frobenius of $\mathfrak{q}$, if h denotes the degree of the residue field extension at $\mathfrak{q}$ in $K_n(\mathfrak{r})/K$ then (9) reduces to

$$\boldsymbol{\eta}(n,\mathfrak{r}) = \boldsymbol{\eta}(m,\mathfrak{r})^{N_{H'}N_H} \equiv (\boldsymbol{\eta}(m,\mathfrak{r})^{N_{H'}})^t \pmod{\mathfrak{Q}}$$

and similarly $\boldsymbol{\eta}(n,\mathfrak{q}\mathfrak{r}) \equiv (\boldsymbol{\eta}(m,\mathfrak{q}\mathfrak{r})^{N_{H'}})^t \pmod{\mathfrak{Q}}$, where

$$t = \sum_{i=0}^{\#(H)-1} (\mathbf{N}\mathfrak{q}^h)^i \equiv \#(H) \pmod{\mathbf{N}\mathfrak{q} - 1}.$$

Recall that p^k is the highest power of p dividing $\mathbf{N}\mathfrak{q} - 1$. Since the decomposition group of $\mathfrak{q}$ in K_∞/K is infinite, for m sufficiently large we will have $p^k \mid t$, and then combining the congruences above proves the proposition. □

For the Euler system of elliptic units, one can prove directly, using Lemma 7.3, that the congruence of Proposition 8.6 holds with $d = 1$.

Definition 8.7. Suppose $\boldsymbol{\eta}$ is an Euler system, $n \geq 1$ and $\mathfrak{r} \in \mathcal{R}$. Using the map $X_{n,\mathfrak{r}} \to K_n(\mathfrak{r})^\times$ corresponding to $\boldsymbol{\eta}$, we define a 1-cocycle $c = c_{\boldsymbol{\eta},n,\mathfrak{r}} : G_\mathfrak{r} \to K_n(\mathfrak{r})^\times$ by

$$c(\sigma) = \boldsymbol{\eta}\left(\frac{(\sigma - 1)D_\mathfrak{r} x_{n,\mathfrak{r}}}{M}\right) \quad \text{for } \sigma \in G_\mathfrak{r}.$$

This is well defined by Proposition 8.4. Since $H^1(G_\mathfrak{r}, K_n(\mathfrak{r})^\times) = 0$, there is a $\beta \in K_n(\mathfrak{r})^\times$ such that $c(\sigma) = \beta^\sigma/\beta$ for every $\sigma \in G_\mathfrak{r}$. Then $\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_\mathfrak{r}}/\beta^M \in K_n^\times$ and we define

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

Since β is uniquely determined modulo $K_n^\times$, $\kappa_{n,M}(\mathfrak{r})$ is independent of the choice of β.

Remark 8.8. It is quite easy to show for every Euler system $\boldsymbol{\eta}$, every n, and every $\mathfrak{r} \in \mathcal{R}_{n,M}$ that $\boldsymbol{\eta}(n, \mathfrak{r})^{(\sigma-1)D_\mathfrak{r}}$ is an M-th power (Proposition 8.4(ii)). The reason for introducing the "universal Euler system" $X_{n,\mathfrak{r}}$ is to show that $\boldsymbol{\eta}(n, \mathfrak{r})^{(\sigma-1)D_\mathfrak{r}}$ has a *canonical* M-th root, even when $K_n(\mathfrak{r})$ contains M-th roots of unity (Proposition 8.4(i)). This fact was used to construct the cocycle c above.

We next want to determine the ideal generated by $\kappa_{n,M}(\mathfrak{r})$ (modulo M-th powers).

Definition 8.9. Fix $n \geq 1$, a power M of p, and temporarily write $F = K_n$, $\mathcal{R}_{F,M} = \mathcal{R}_{n,M}$. Let $\mathcal{O}_F$ denote the ring of integers of F and

$$\mathcal{I}_F = \mathcal{I} = \oplus_\mathfrak{Q} \mathbf{Z}\mathfrak{Q}$$

the group of fractional ideals of F, written additively. For every prime $\mathfrak{q}$ of K let

$$\mathcal{I}_{F,\mathfrak{q}} = \mathcal{I}_\mathfrak{q} = \oplus_{\mathfrak{Q}|\mathfrak{q}} \mathbf{Z}\mathfrak{Q},$$

and if $y \in F^\times$ let $(y) \in \mathcal{I}$ denote the principal ideal generated by y, and $(y)_\mathfrak{q}$, $[y]$, and $[y]_\mathfrak{q}$ the projections of (y) to $\mathcal{I}_\mathfrak{q}$, $\mathcal{I}/M\mathcal{I}$, and $I_\mathfrak{q}/M\mathcal{I}_\mathfrak{q}$, respectively. Note that $[y]$ and $[y]_\mathfrak{q}$ are well defined for $y \in F^\times/(F^\times)^M$.

Suppose $\mathfrak{q} \in \mathcal{R}_{F,M}$, $\mathfrak{Q}$ is a prime of F above $\mathfrak{q}$, and $\bar{\mathfrak{Q}}$ is a prime of $\bar{K}$ above $\mathfrak{Q}$. Recall that $\mathfrak{Q}$ is completely split in F/K, and totally ramified of degree $\mathbf{N}\mathfrak{q} - 1 = \mathbf{N}\mathfrak{Q} - 1$ in $F(\mathfrak{q})/F$. Fix a lift $\sigma_\mathfrak{Q}$ of $\sigma_\mathfrak{q}$ to G_K so that $\sigma_\mathfrak{Q}$ belongs to the inertia group of $\bar{\mathfrak{Q}}$. Then there is an isomorphism

$$\mathbf{Z}/M\mathbf{Z} \xrightarrow{\sim} \boldsymbol{\mu}_M$$

given by $a \mapsto (\pi^{a/M})^{1-\sigma_{\mathfrak{Q}}}$ where $\pi \in K$ is a generator of $\mathfrak{q}$. Let $\mathrm{Frob}_{\bar{\mathfrak{Q}}} \in G_{F_{\mathfrak{Q}}}$ denote a Frobenius of $\mathfrak{Q}$ and define

$$\phi_{\mathfrak{Q}} : F_{\mathfrak{Q}}^{\times}/(F_{\mathfrak{Q}}^{\times})^M \to \mathbf{Z}/M\mathbf{Z}$$

to be the image of $\mathrm{Frob}_{\mathfrak{Q}}$ under the composition

$$G_{F_{\mathfrak{Q}}} \to \mathrm{Hom}(F_{\mathfrak{Q}}^{\times}, \boldsymbol{\mu}_M) \xrightarrow{\sim} \mathrm{Hom}(F_{\mathfrak{Q}}^{\times}, \mathbf{Z}/M\mathbf{Z})$$

where the first map is the Kummer map and the second is induced by the isomorphism above. Concretely, since $\sigma_{\mathfrak{Q}}$ belongs to the inertia group, we have $\phi_{\mathfrak{Q}}(\alpha) = a$ where a is characterized by

$$(\alpha^{1/M})^{\mathrm{Frob}_{\mathfrak{Q}}-1} = (\pi^{a/M})^{1-\sigma_{\mathfrak{Q}}} \equiv (\beta^{1/M})^{1-\sigma_{\mathfrak{Q}}} \tag{10}$$

modulo the maximal ideal of $\bar{F_{\mathfrak{Q}}}$, where $\beta \in \bar{F_{\mathfrak{Q}}}^{\times}$ is an element satisfying $\mathrm{ord}_{\mathfrak{Q}}(\beta) = a$.

Finally, define

$$\phi_{\mathfrak{q}} : F^{\times}/(F^{\times})^M \to \mathcal{I}_{\mathfrak{q}}/M\mathcal{I}_{\mathfrak{q}}$$

by $\phi_{\mathfrak{q}}(\alpha) = \sum_{\mathfrak{Q}|\mathfrak{q}} \phi_{\mathfrak{Q}}(\alpha)\mathfrak{Q}$. It is not difficult to check that $\phi_{\mathfrak{q}}$ is $\mathrm{Gal}(F/K)$-equivariant, and that $\phi_{\mathfrak{q}}$ induces an isomorphism

$$\phi_{\mathfrak{q}} : (\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^{\times}/((\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^{\times})^M \xrightarrow{\sim} \mathcal{I}_{\mathfrak{q}}/M\mathcal{I}_{\mathfrak{q}}.$$

Proposition 8.10. *Suppose $\boldsymbol{\eta}$ is an Euler system, $n \geq 1$, $\mathfrak{r} \in \mathcal{R}_{n,M}$ and $\mathfrak{q}$ is a prime of K.*

(i) *If $\mathfrak{q} \nmid \mathfrak{r}$ then $[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = 0$.*
(ii) *If $\mathfrak{q} \mid \mathfrak{r}$ then $[\kappa_{n,M}(\mathfrak{r})]_{\mathfrak{q}} = \phi_{\mathfrak{q}}(\kappa_{n,M}(\mathfrak{r}/\mathfrak{q}))$.*

Proof. Suppose first that $\mathfrak{q} \nmid \mathfrak{r}$. Then $\mathfrak{q}$ is unramified in $K_n(\mathfrak{r})/K_n$, and by definition $\kappa_{n,M}(\mathfrak{r})$ is a global unit times an M-th power in $K_n(\mathfrak{r})^{\times}$, so $\mathrm{ord}_{\mathfrak{Q}}(\kappa_{n,M}(\mathfrak{r})) \equiv 0 \pmod{M}$ for every prime $\mathfrak{Q}$ of K_n above $\mathfrak{q}$. This proves (i).

Now suppose $\mathfrak{q} \mid \mathfrak{r}$, say $\mathfrak{r} = \mathfrak{q}\mathfrak{s}$. By definition

$$\kappa_{n,M}(\mathfrak{r}) = \boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}}/\beta_{\mathfrak{r}}^M, \quad \kappa_{n,M}(\mathfrak{s}) = \boldsymbol{\eta}(x_{n,\mathfrak{s}})^{D_{\mathfrak{s}}}/\beta_{\mathfrak{s}}^M$$

where $\beta_{\mathfrak{r}} \in K_n(\mathfrak{r})^{\times}, \beta_{\mathfrak{s}} \in K_n(\mathfrak{s})^{\times}$ satisfy

$$\beta_{\mathfrak{r}}^{\sigma-1} = \boldsymbol{\eta}((\sigma-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}/M), \quad \beta_{\mathfrak{s}}^{\sigma-1} = \boldsymbol{\eta}((\sigma-1)D_{\mathfrak{s}}x_{n,\mathfrak{s}}/M)$$

for every $\sigma \in G_{\mathfrak{r}}$.

We will use (10) to evaluate $\phi_{\mathfrak{q}}(\kappa(\mathfrak{s}))$. Fix a prime $\mathfrak{Q}$ of K_n above $\mathfrak{q}$, let $\sigma_{\mathfrak{Q}}$ be as in Definition 8.9, and let d be the prime-to-p-part of $\mathbf{N}\mathfrak{q} - 1$ as in

Proposition 8.6. Modulo every prime above $\mathfrak{Q}$ we have

$$\begin{aligned}
(\kappa_{n,M}(\mathfrak{r})^{d/M})^{1-\sigma_{\mathfrak{Q}}} &= ((\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{r}}})^{1/M}/\beta_{\mathfrak{r}})^{d(1-\sigma_{\mathfrak{Q}})} \equiv \beta_{\mathfrak{r}}^{d(\sigma_{\mathfrak{q}}-1)} \\
&= \boldsymbol{\eta}((\sigma_{\mathfrak{q}}-1)D_{\mathfrak{r}}x_{n,\mathfrak{r}}/M)^d \\
&= \boldsymbol{\eta}((\mathbf{N}\mathfrak{q}-1-N_{\mathfrak{q}})D_{\mathfrak{s}}x_{n,\mathfrak{r}}/M)^d \\
&= \boldsymbol{\eta}((\mathbf{N}\mathfrak{q}-1)D_{\mathfrak{s}}x_{n,\mathfrak{r}}/M)^d\boldsymbol{\eta}((\mathrm{Frob}_{\mathfrak{q}}^{-1}-1)D_{\mathfrak{s}}x_{n,\mathfrak{s}}/M)^d \\
&= (\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{s}}})^{d(\mathbf{N}\mathfrak{q}-1)/M}/\beta_{\mathfrak{s}}^{d(1-\mathrm{Frob}_{\mathfrak{q}}^{-1})} \\
&= (\boldsymbol{\eta}(x_{n,\mathfrak{r}})^{D_{\mathfrak{s}}})^{\mathrm{Frob}_{\mathfrak{q}}^{-1}d(\mathbf{N}\mathfrak{q}-1)/M}/\beta_{\mathfrak{s}}^{d(1-\mathrm{Frob}_{\mathfrak{q}}^{-1})} \\
&\equiv ((\boldsymbol{\eta}(x_{n,\mathfrak{s}})^{D_{\mathfrak{s}}}/\beta_{\mathfrak{s}}^{M})^{1/M})^{d(1-\mathrm{Frob}_{\mathfrak{Q}}^{-1})} \\
&\equiv (\kappa_{n,M}(\mathfrak{s})^{d/M})^{\mathrm{Frob}_{\mathfrak{Q}}-1}
\end{aligned}$$

using Proposition 8.6 for the second-to-last congruence. By (10) it follows that

$$d\phi_{\mathfrak{Q}}(\kappa_{n,M}(\mathfrak{s})) = d\mathrm{ord}_{\mathfrak{Q}}(\kappa_{n,M}(\mathfrak{r})),$$

and since d is prime to p, (ii) follows. □

9 Bounding Ideal Class Groups

In this section we describe Kolyvagin's method of using the Euler system of elliptic units, or rather the principal ideals deduced from elliptic units as in §8.2, to bound the size of certain ideal class groups. For a similar argument in the case of cyclotomic units and real abelian extensions of $\mathbf{Q}$, see [Ru1].

Keep the notation of the previous section. Let $F = K_1 = K(E[\mathfrak{p}])$ and let $\boldsymbol{\mu}_F$ denote the roots of unity in F. Let $\varDelta = \mathrm{Gal}(F/K)$, so $\varDelta \cong (\mathcal{O}/\mathfrak{p})^\times$ is cyclic of order $p-1$ or p^2-1.

Since $\#(\varDelta)$ is prime to p, the group ring $\mathbf{Z}_p[\varDelta]$ is semisimple, i.e.,

$$\mathbf{Z}_p[\varDelta] \cong \bigoplus_{\chi\in\varXi} R_\chi$$

where $\varXi$ denotes the set of all irreducible $\mathbf{F}_p$-representations of $\varDelta$ and R_χ denotes the corresponding direct summand of $\mathbf{Z}_p[\varDelta]$. (We will also refer to elements of $\varXi$ as irreducible $\mathbf{Z}_p$-representations of $\varDelta$.) Since $\#(\varDelta)$ divides p^2-1, we have two cases:

- $\dim(\chi) = 1$, $R_\chi = \mathbf{Z}_p$,
- $\dim(\chi) = 2$, R_χ is the ring of integers of the unramified quadratic extension of $\mathbf{Q}_p$, and χ splits into two one-dimensional pieces over $\mathcal{O}_{\mathfrak{p}}$.

If $\chi \in \varXi$ and B is a $\mathbf{Z}[\varDelta]$-module, we let $M^{(p)}$ denote the p-adic completion of M and

$$M^\chi = M^{(p)} \otimes_{\mathbf{Z}_p[\varDelta]} R_\chi.$$

Then $M^{(p)} = \oplus_{\chi\in\varXi} M^\chi$, so we can view M^χ either as a quotient of M or a submodule of $M^{(p)}$. If $m \in M$ we write m^χ for the projection of m into M^χ.

Lemma 9.1. *For every nontrivial $\chi \in \varXi$, $(\mathcal{O}_F^\times/\boldsymbol{\mu}_F)^\chi$ is free of rank one over R_χ.*

Proof. The Dirichlet unit theorem gives an exact sequence

$$0 \to \mathcal{O}_F^\times \otimes \mathbf{Q} \to \mathbf{Q}[\varDelta] \to \mathbf{Q} \to 0$$

and the lemma follows by taking χ-components. □

Let A denote the ideal class group of F, and fix a $\chi \in \varXi$. We wish to bound the size of A^χ. Fix a power M of p, which we will later take to be large, and set $F_M = F(\boldsymbol{\mu}_M)$.

Lemma 9.2. *The composition*

$$\mathrm{Hom}(A, \mathbf{Z}/M\mathbf{Z}) \to \mathrm{Hom}(G_F, \mathbf{Z}/M\mathbf{Z}) \to \mathrm{Hom}(G_{F_M}, \mathbf{Z}/M\mathbf{Z}),$$

given by class field theory and restriction to G_{F_M}, is injective.

Proof. The first map is clearly injective, and the kernel of the second is equal to $\mathrm{Hom}(\mathrm{Gal}(F_M/F), \mathbf{Z}/M\mathbf{Z})$. Thus to prove the lemma it suffices to show that there is no unramified p-extension of F in F_M. But the p-part of $\mathrm{Gal}(F_M/F)$ is $\mathrm{Gal}(F_M/F(\boldsymbol{\mu}_p))$, which is totally ramified at all primes above p. This completes the proof. □

Lemma 9.3. *The map*

$$F^\times/(F^\times)^M \to {F_M}^\times/({F_M}^\times)^M$$

is injective.

Proof. Kummer theory shows that $F^\times/(F^\times)^M \cong H^1(F, \boldsymbol{\mu}_M)$ and similarly for F_M, so the kernel of the map in the lemma is $H^1(F_M/F, \boldsymbol{\mu}_M)$. Since $\mathrm{Gal}(F_M/F)$ is cyclic and acts faithfully on $\boldsymbol{\mu}_M$, and $p > 2$, it is easy to check that $H^1(F_M/F, \boldsymbol{\mu}_M) = 0$. (See also Lemma 6.1.) □

Write $\mathcal{R}_{F,M}$ for $\mathcal{R}_{1,M}$, the set of primes of K defined in §8.

Proposition 9.4. *Suppose $\kappa \in F^\times/(F^\times)^M$ and $\alpha \in \mathrm{Hom}(A, \mathbf{Z}/M\mathbf{Z})$, $\alpha \neq 0$. Then there is a prime $\mathfrak{q} \in \mathcal{R}_{F,M}$ and a prime $\mathfrak{Q}$ of F above $\mathfrak{q}$ such that*

(i) *$\alpha(\mathfrak{c}) \neq 0$, where $\mathfrak{c}$ denotes the class of $\mathfrak{Q}$ in A,*
(ii) *$[\kappa]_\mathfrak{q} = 0$ and for every $d \in \mathbf{Z}$, $d\phi_\mathfrak{q}(\kappa) = 0 \Leftrightarrow \kappa^d \in (F^\times)^M$.*

Proof. Let t be the order of κ in $F^\times/(F^\times)^M$, and let $\rho \in \mathrm{Hom}(G_{F_M}, \boldsymbol{\mu}_M)$ be the image of κ under the Kummer map. We view α as a map on G_{F_M} via the map of Lemma 9.2. Define two subgroups of G_{F_M}

$$\begin{aligned} H_\alpha &= \{\gamma \in G_{F_M} : \alpha(\gamma) = 0\}, \\ H_\kappa &= \{\gamma \in G_{F_M} : \rho(\gamma) \text{ has order less than } t \text{ in } \boldsymbol{\mu}_M\}. \end{aligned}$$

Since $\alpha \neq 0$, Lemma 9.2 shows that $H_\alpha \neq G_{F_M}$. Similarly it follows from Lemma 9.3 that $H_\kappa \neq G_{F_M}$. Since a group cannot be a union of two proper subgroups, we can choose a $\gamma \in G_{F_M}$, $\gamma \notin H_\alpha \cup H_\kappa$. Let L be a finite Galois extension of F containing F_M such that both ρ and α are trivial on G_L. By the Cebotarev theorem we can choose a prime $\tilde{\mathfrak{Q}}$ of L, not dividing $6\mathfrak{a}\mathfrak{f}\mathfrak{p}$ and such that $[\kappa]_\mathfrak{q} = 0$, whose Frobenius in L/K is γ. Let $\mathfrak{Q}$ and $\mathfrak{q}$ denote the primes of F and K, respectively, below $\tilde{\mathfrak{Q}}$. We will show that these primes satisfy the conditions of the proposition.

First, the fact that γ fixes $F(\boldsymbol{\mu}_M)$ means that $\mathfrak{q}$ splits completely in $F(\boldsymbol{\mu}_M)$ and thus $\mathfrak{q} \in \mathcal{R}_{F,M}$.

The class field theory inclusion $\mathrm{Hom}(A, \mathbf{Z}/M\mathbf{Z}) \hookrightarrow \mathrm{Hom}(G_F, \mathbf{Z}/M\mathbf{Z})$ identifies $\alpha(\mathfrak{c})$ with $\alpha(\mathrm{Frob}_\mathfrak{Q}) = \alpha(\gamma)$, so (i) follows from the fact that $\gamma \notin H_\alpha$.

Since $\gamma \notin H_\kappa$, $(\kappa^{1/M})^{\mathrm{Frob}_\mathfrak{Q} - 1}$ is a primitive t-th root of unity. Therefore κ has order $t(\mathbf{N}\mathfrak{q} - 1)/M$ modulo $\mathfrak{Q}$, and hence has order at least t (and hence exactly t) in $(\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^\times/((\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^\times)^M$. Since $\phi_\mathfrak{q}$ is an isomorphism on $(\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^\times/((\mathcal{O}_F/\mathfrak{q}\mathcal{O}_F)^\times)^M$, this proves (ii). □

Suppose $\boldsymbol{\eta}$ is an Euler system as defined in Definition 8.5. Define $\mathcal{C} = \mathcal{C}_{\boldsymbol{\eta}} \subset \mathcal{O}_F^\times$ to be the group generated over $\mathbf{Z}[\Delta]$ by $\boldsymbol{\mu}_F$ and $\boldsymbol{\eta}(1, \mathcal{O})$.

Theorem 9.5. *With notation as above, if $\boldsymbol{\eta}$ is an Euler system and χ is an irreducible $\mathbf{Z}_p$-representation of Δ then*

$$\#(A^\chi) \leq \#((\mathcal{O}_F^\times/\mathcal{C}_{\boldsymbol{\eta}})^\chi).$$

Proof. If χ is the trivial character then A^χ is the p-part of the ideal class group of K, which is zero. Hence we may assume that $\chi \neq 1$.

By Lemma 9.1

$$(\mathcal{O}_F^\times/\mathcal{C})^\chi \cong R_\chi/mR_\chi$$

for some $m \in R_\chi$. If $m = 0$ then there is nothing to prove, so we may assume $m \neq 0$. Choose M large enough so that M/m annihilates A. For $\mathfrak{r} \in \mathcal{R}_{F,M}$ we will write $\kappa(\mathfrak{r})$ for the element $\kappa_{1,M}(\mathfrak{r}) \in F^\times/(F^\times)^M$ constructed in Definition 8.7.

Number the elements of $\mathrm{Hom}(A^\chi, \mathbf{Z}/M\mathbf{Z}) \subset \mathrm{Hom}(A, \mathbf{Z}/M\mathbf{Z})$ so that

$$\mathrm{Hom}(A^\chi, \mathbf{Z}/M\mathbf{Z}) = \{\alpha_1, \ldots, \alpha_k\}.$$

Using Proposition 9.4 we choose inductively a sequence of primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_k \in \mathcal{R}_{F,M}$ and $\mathfrak{Q}_i$ of F above $\mathfrak{q}_i$ such that, if $\mathfrak{c}_i$ denotes the class of $\mathfrak{Q}_i$ in A and

$\mathfrak{r}_i = \prod_{j \le i} \mathfrak{q}_j$ for $0 \le i \le k$,

$$\alpha_i(\mathfrak{c}_i) \neq 0, \tag{11}$$
$$d\phi_{\mathfrak{q}_i}(\kappa(\mathfrak{r}_{i-1})^\chi) = 0 \Leftrightarrow (\kappa(\mathfrak{r}_{i-1})^\chi)^d = 0 \in F^\times/(F^\times)^M \tag{12}$$

(just apply Proposition 9.4 with $\kappa = \kappa(\mathfrak{r}_{i-1})^\chi$ and $\alpha = \alpha_i$ to produce $\mathfrak{q}_i$ and $\mathfrak{Q}_i$).

First we claim that the classes $\{\mathfrak{c}_i^\chi\}$ generate A^χ. For if not, then there is an $\alpha \in \mathrm{Hom}(A^\chi, \mathbf{Z}/M\mathbf{Z})$ such that $\alpha(\mathfrak{c}_j) = 0$ for every j. But $\alpha = \alpha_i$ for some i, so (11) shows this is not the case.

If $1 \le i \le k$ let s_i denote the order of $\mathfrak{c}_i^\chi$ in $A^\chi/\langle \mathfrak{c}_1^\chi, \dots, \mathfrak{c}_{i-1}^\chi \rangle$. Since the $\mathfrak{c}_i^\chi$ generate A^χ we have

$$\#(A^\chi) = \prod_{i=1}^{k} [R_\chi : s_i R_\chi].$$

If $0 \le i \le k-1$ let t_i denote the order of $\kappa(\mathfrak{r}_i)^\chi$ in $F^\times/(F^\times)^M$. By (12) and Proposition 8.10(ii), for $i \ge 1$ the order of $[\kappa(\mathfrak{r}_i)^\chi]_{\mathfrak{q}_i}$ is t_{i-1}. In particular it follows that $t_{i-1} \mid t_i$. Since $\kappa(\mathfrak{r}_0)$ is the image of $\boldsymbol{\eta}(1, \mathcal{O})$ in $\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^M$, the exact sequence

$$0 \to R_\chi \kappa(\mathfrak{r}_0)/\boldsymbol{\mu}_F \cap R_\chi \kappa(\mathfrak{r}_0) \to (\mathcal{O}_F^\times/\boldsymbol{\mu}_F(\mathcal{O}_F^\times)^M)^\chi \to (\mathcal{O}_F^\times/\mathcal{C})^\times \to 0$$

shows that $M \mid t_0 m$.

For each i we can choose $\nu_i \in F^\times/(F^\times)^M$ such that $\nu_i^{M/t_i} = \kappa(\mathfrak{r}_i)^\chi \zeta$ with $\zeta \in \boldsymbol{\mu}_F$. In particular

$$(M/t_i)[\nu_i]_{\mathfrak{q}_i} = [\kappa(\mathfrak{r}_i)^\chi]_{\mathfrak{q}_i}$$

so $[\nu_i]_{\mathfrak{q}_i}$ has order $t_{i-1}M/t_i$ in $(\mathcal{I}_\mathfrak{q}/M\mathcal{I}_\mathfrak{q})^\chi \cong R_\chi/MR_\chi$. Thus, using Proposition 8.10(i), there is a unit $u \in R_\chi^\times$ such that

$$(\nu_i) \equiv u(t_i/t_{i-1})\mathfrak{q}_i^\chi \pmod{\mathcal{I}_{\mathfrak{q}_1}, \dots, \mathcal{I}_{\mathfrak{q}_{i-1}}, t_i\mathcal{I}}.$$

We know that $t_0 \mid t_i$ and $(M/m) \mid t_0$. Thus by our choice of M, t_i annihilates A and we conclude that

$$(t_i/t_{i-1})\mathfrak{c}_i^\chi = 0 \quad \text{in } A^\chi/\langle \mathfrak{c}_1^\chi, \dots, \mathfrak{c}_{i-1}^\chi \rangle.$$

Therefore $s_i \mid (t_i/t_{i-1})$ for every $i \ge 1$, so

$$\#(A^\chi) = \prod_{i=1}^{k} [R_\chi : s_i R_\chi] \ \text{ divides } \ [t_0 R_\chi : t_k R_\chi].$$

Since $t_k \mid M$ and $M \mid t_0 m$, this index divides $[R_\chi : mR_\chi]$. This proves the theorem. □

Corollary 9.6. *Let $\mathcal{C}_{\mathfrak{a}}$ denote the group of (elliptic) units of F generated over $\mathbf{Z}_p[\Delta]$ by $\boldsymbol{\mu}_F$ and by $\eta_1^{(\mathfrak{a})}$. If χ is an irreducible $\mathbf{Z}_p$-representation of Δ then*

$$\#(A^\chi) \quad \textit{divides} \quad \#((\mathcal{O}_F^\times/\mathcal{C}_{\mathfrak{a}})^\chi).$$

Proof. Apply Theorem 9.5 with the Euler system $\boldsymbol{\eta}(n,\mathfrak{r}) = \eta_n^{(\mathfrak{a})}(\mathfrak{r})$. □

Remark 9.7. If $\mathcal{C}_F$ denotes the full group of elliptic units of F (see for example [Ru2] §1), then one can combine Theorem 9.5 with a well-known argument using the analytic class number formula to prove that for every χ,

$$\#(A^\chi) = \#((\mathcal{O}_F^\times/\mathcal{C}_F)^\chi).$$

See Theorem 3.3 of [Ru2].

Corollary 9.8. *With notation as above, if $(\eta_1^{(\mathfrak{a})})^\chi \notin \boldsymbol{\mu}_F^\chi((\mathcal{O}_F^\times)^\chi)^p$ then $A^\chi = 0$.*

Proof. Immediate from Corollary 9.6 and Lemma 9.1. □

10 The Theorem of Coates and Wiles

Keep the notation of the previous sections. In this section we will prove the following theorem.

Theorem 10.1 (Coates-Wiles [CW1]). *If $L(\bar{\psi},1) \neq 0$ then $E(K)$ is finite.*

Suppose for the rest of this section that $\mathfrak{p}$ is a prime of K not dividing $\mathfrak{f}$, of residue characteristic $p > 7$ (see remark 10.3 below). As in §9 we let $F = K(E[\mathfrak{p}])$, $\Delta = \mathrm{Gal}(F/K)$ and A is the ideal class group of F.

Lemma 10.2. *There is an ideal $\mathfrak{a}$ of $\mathcal{O}$, prime to $6\mathfrak{p}\mathfrak{f}$, such that $\mathbf{N}\mathfrak{a} \not\equiv \psi(\mathfrak{a}) \pmod{\mathfrak{p}}$.*

Proof. By Corollary 5.18, $E[\bar{\mathfrak{p}}] \not\subset E(K)$. Choose a prime $\mathfrak{q}$ of K, not dividing $6p\mathfrak{f}$, such that $[\mathfrak{q}, K(E[\bar{\mathfrak{p}}])/K] \neq 1$. By Corollary 5.16(ii) we deduce that $\psi(\mathfrak{q}) \not\equiv 1 \pmod{\bar{\mathfrak{p}}}$, and so $\bar{\psi}(\mathfrak{q}) \not\equiv 1 \pmod{\mathfrak{p}}$. Since $\psi(\mathfrak{q})\bar{\psi}(\mathfrak{q}) = \mathbf{N}\mathfrak{q}$, the lemma is satisfied with $\mathfrak{a} = \mathfrak{q}$. □

Remark 10.3. Lemma 10.2 is not in general true without the assumption $p > 7$, since for small p it may happen that $E[\bar{\mathfrak{p}}] \subset E(K)$.

By Corollary 5.20(iv), F/K is totally ramified at $\mathfrak{p}$. Let $\mathcal{P}$ denote the prime of F above $\mathfrak{p}$. By Lemma 3.6 and Corollary 5.16 $E[\mathfrak{p}] \subset E_1(F_{\mathcal{P}})$, so the isomorphism of Corollary 3.8 restricts to an isomorphism

$$E[\mathfrak{p}] \xrightarrow{\sim} \hat{E}[\mathfrak{p}] \subset \hat{E}(F_{\mathcal{P}})$$

where $\hat{E}$ is the formal group attached to E. Let $\mathcal{O}_{F,\mathcal{P}}$ denote the completion of $\mathcal{O}_F$ at $\mathcal{P}$.

Lemma 10.4. *The map*

$$E[\mathfrak{p}] \xrightarrow{\sim} \hat{E}[\mathfrak{p}] \xrightarrow{1+\cdot} (1 + \mathcal{P}\mathcal{O}_{F,\mathcal{P}})/(1 + \mathcal{P}^2\mathcal{O}_{F,\mathcal{P}})$$

is a Δ-equivariant isomorphism.

Proof. The map in question is a well-defined homomorphism, and by Lemma 7.3 it is injective. Both groups have order $\mathbf{N}\mathfrak{p}$, so it is an isomorphism. The Δ-equivariance is clear. □

Now fix an ideal $\mathfrak{a}$ satisfying Lemma 10.2, a generator Ω of the period lattice of E as in §7.4, and a generator f of the conductor $\mathfrak{f}$. With these choices define the elliptic units $\eta_n(\mathfrak{r})$ as in §8.1. Let $\eta = \eta_1(\mathcal{O})$, a global (elliptic) unit of F which depends on the choice of $\mathfrak{a}$.

Definition 10.5. Define

$$\delta : \mathcal{O}_{F,\mathcal{P}}^{\times} \to E[\mathfrak{p}]$$

to be the composition of the natural projection

$$\mathcal{O}_{F,\mathcal{P}}^{\times} \twoheadrightarrow (1 + \mathcal{P}\mathcal{O}_{F,\mathcal{P}})/(1 + \mathcal{P}^2\mathcal{O}_{F,\mathcal{P}})$$

with the inverse of the isomorphism of Lemma 10.4.

Recall that by Corollary 7.18, $L(\bar{\psi}, 1)/\Omega \in K$.

Proposition 10.6. *$L(\bar{\psi}, 1)/\Omega$ is integral at $\mathfrak{p}$, and*

$$L(\bar{\psi}, 1)/\Omega \equiv 0 \pmod{\mathfrak{p}} \Leftrightarrow \delta(\eta) = 0.$$

Proof. Let $P = (\wp(\Omega/\psi(\mathfrak{p}); \Omega\mathcal{O}), \wp'(\Omega/\psi(\mathfrak{p}); \Omega\mathcal{O})/2) \in E[\mathfrak{p}]$ and

$$z = -x(P)/y(P) \in \mathcal{P},$$

the image of P in $\hat{E}[\mathfrak{p}]$. Then $\eta = \Lambda_{\mathfrak{p},\mathfrak{a}}(z)$, where $\Lambda_{\mathfrak{p},\mathfrak{a}}$ is the power series of Definition 7.21.

By Theorem 7.22, $\Lambda_{\mathfrak{p},\mathfrak{a}}(0) \in \mathcal{O}_{\mathfrak{p}}^{\times}$, $12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a}))(L(\bar{\psi}, 1)/\Omega) \in \mathcal{O}_{\mathfrak{p}}$, and

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

Thus

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

and with our choice of $\mathfrak{a}$, $12f(\mathbf{N}\mathfrak{a} - \psi(\mathfrak{a})) \in \mathcal{O}_{\mathfrak{p}}^{\times}$. This proves the proposition. □

Definition 10.7. Let χ_E denote the representation of Δ on $E[\mathfrak{p}]$; by Corollary 5.20 χ_E is $\mathbf{F}_p$-irreducible. Then in the notation of §9 we have $E[\mathfrak{p}] \cong R_{\chi_E}/\mathfrak{p}R_{\chi_E}$ as Δ-modules.

Theorem 10.8. *Suppose $L(\bar{\psi},1)/\Omega$ is a unit at $\mathfrak{p}$. Then*

$$A^{\chi_E} = 0.$$

Proof. Since the map δ is Δ-equivariant,

$$\delta(\eta^{\chi_E}) = \delta(\eta)^{\chi_E} = \delta(\eta) \neq 0$$

by Proposition 10.6. Hence

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

The Weil pairing (see [Si] Proposition III.8.1) gives a Galois-equivariant isomorphism

$$E[p] \cong \mathrm{Hom}(E[p], \boldsymbol{\mu}_p).$$

If $\boldsymbol{\mu}_F^{\chi_E}$ were nontrivial, then $E[p]^{G_K}$ would be nontrivial, and this is impossible by Corollary 5.18. Now the theorem follows from Corollary 9.8. □

Lemma 10.9. *Suppose p splits into two primes in K and $\mathrm{Tr}_{K/\mathbf{Q}}\psi(\mathfrak{p}) \neq 1$. Then*

(i) $\boldsymbol{\mu}_p \not\subset F_{\mathcal{P}}$,
(ii) $(\mathcal{O}_{F,\mathcal{P}}^\times)^{\chi_E}$ *is free of rank one over* R_{χ_E}.

Proof. By Theorem 5.15(ii), $[\psi(\mathfrak{p}), F_{\mathcal{P}}/K_{\mathfrak{p}}] = 1$. On the other hand, class field theory over $\mathbf{Q}$ shows that $[p, \mathbf{Q}_p(\boldsymbol{\mu}_p)/\mathbf{Q}_p] = 1$. Thus we have (again using Theorem 5.15(ii))

$$\begin{aligned}\boldsymbol{\mu}_p \subset F_{\mathcal{P}} \Rightarrow F_{\mathcal{P}} = K_{\mathfrak{p}}(\boldsymbol{\mu}_p) &\Rightarrow [p/\psi(\mathfrak{p}), F_{\mathcal{P}}/K_{\mathfrak{p}}] = 1 \\ &\Rightarrow p/\psi(\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}} \\ &\Rightarrow \mathrm{Tr}_{K/\mathbf{Q}}\psi(\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}} \\ &\Rightarrow \mathrm{Tr}_{K/\mathbf{Q}}\psi(\mathfrak{p}) = 1,\end{aligned}$$

the last implication because $|\mathrm{Tr}_{K/\mathbf{Q}}\psi(\mathfrak{p})| \leq 2\sqrt{p} < p-1$. This proves (i).

We have isomorphisms

$$\mathcal{O}_{F,\mathcal{P}}^\times \otimes \mathbf{Q}_p \xrightarrow{\sim} \mathcal{O}_{F,\mathcal{P}} \otimes \mathbf{Q}_p \cong K_{\mathfrak{p}}[\Delta],$$

the first one given by the $\mathfrak{p}$-adic logarithm map. Together with (i) this proves (ii). □

Theorem 10.10. *Suppose $L(\bar{\psi},1)/\Omega$ is a unit at $\mathfrak{p}$, p splits into two primes in K, and $\mathrm{Tr}_{K/\mathbf{Q}}\psi(\mathfrak{p}) \neq 1$. Then the natural (injective) map*

$$(\mathcal{O}_F^\times)^{\chi_E} \to (\mathcal{O}_{F,\mathcal{P}}^\times)^{\chi_E}$$

is surjective.

Proof. As in the proof of Theorem 10.8, $\delta(\eta^{\chi_E}) = \delta(\eta)$. Thus by Proposition 10.6 $(\mathcal{O}_F^\times)^{\chi_E} \not\subset ((\mathcal{O}_{F,\mathcal{P}}^\times)^{\chi_E})^p$, so the Theorem follows from Lemma 10.9. □

Proof (of the Coates-Wiles Theorem 10.1). Using the Cebotarev theorem we can find infinitely many primes $\mathfrak{p}$ which split in K and such that $\mathrm{Tr}_{K/\mathbf{Q}}\psi(\mathfrak{p}) \neq 1$. Choose one which does not divide $6\mathfrak{f}$ or $L(\bar{\psi}, 1)/\Omega$. Then by Theorems 10.8 and 10.10 and Corollary 6.10, the Selmer group $S_{\psi(\mathfrak{p})}(E) = 0$. In particular $E(K)/\mathfrak{p}E(K) = 0$, so (using the Mordell-Weil Theorem 4.6), $E(K)$ is finite. □

Remark 10.11. This proof also shows that for primes $\mathfrak{p}$ satisfying the hypotheses of Theorem 10.10, the $\mathfrak{p}$-part of the Tate-Shafarevich group Ш(E) is trivial.

Using the Explicit Reciprocity Law of Wiles ([Wil] or [dS] §I.4) one can show that $\delta = -\delta_1$ where δ_1 is the map of Lemma 6.8. Together with Proposition 10.6, Theorem 10.8 and Corollary 6.10, this shows that $S_{\psi(\mathfrak{p})}(E) = 0$ for every $\mathfrak{p}$ not dividing $2 \cdot 3 \cdot 5 \cdot 7 \cdot \mathfrak{f} \cdot (L(\bar{\psi}, 1)/\Omega)$. We will prove a stronger version of this (Corollary 12.13 and Theorem 12.19) in §12.

11 Iwasawa Theory and the "Main Conjecture"

In order to study the Selmer group under more general conditions than in §10, we need to prove Iwasawa-theoretic versions (Theorem 11.7 and Corollary 11.8 below) of Theorem 9.5 and Remark 9.7. As in the previous sections, we fix an elliptic curve E defined over an imaginary quadratic field K, with $\mathrm{End}_K(E) = \mathcal{O}$, the ring of integers of K. We fix a prime $\mathfrak{p}$ of K where E has good reduction, and for simplicity we still assume that $p > 7$ (in order to apply Lemma 10.2).

Write $K_n = K(E[\mathfrak{p}^n])$, $n = 0, 1, 2, \ldots, \infty$, and let $G_\infty = \mathrm{Gal}(K_\infty/K)$. By Corollary 5.20(ii), we have

$$G_\infty \cong \mathcal{O}_\mathfrak{p}^\times \cong \Delta \times \Gamma$$

where

$$\Delta \cong \mathrm{Gal}(K_1/K) \cong (\mathcal{O}/\mathfrak{p})^\times$$

is the prime-to-p part of G_∞ and

$$\Gamma = \mathrm{Gal}(K_\infty/K_1) \cong 1 + \mathfrak{p}\mathcal{O}_\mathfrak{p} \cong \mathbf{Z}_p^{[K_\mathfrak{p}:\mathbf{Q}_p]}$$

is the p-part.

11.1 The Iwasawa Algebra

Define the *Iwasawa algebra*

$$\Lambda = \mathbf{Z}_p[[G_\infty]] = \varprojlim_n \mathbf{Z}_p[\mathrm{Gal}(K_n/K)] = \varprojlim_n \mathbf{Z}_p[\Delta][\mathrm{Gal}(K_n/K_1)].$$

Then

$$\Lambda = \bigoplus_{\chi \in \Xi} \Lambda_\chi$$

where Ξ is the set of irreducible $\mathbf{Z}_p$-representations of Δ as in §9 and

$$\Lambda_\chi = \Lambda \otimes_{\mathbf{Z}_p[\Delta]} R_\chi \cong R_\chi[[\Gamma]].$$

The following algebraic properties of the Iwasawa algebra and its modules are well-known. For proofs, see for example [Iw] and [Se].

For every irreducible $\mathbf{Z}_p$-representation χ of Δ, Λ_χ is a complete local noetherian ring, noncanonically isomorphic to a power series ring in $[K_\mathfrak{p} : \mathbf{Q}_p]$ variables over R_χ. In particular Λ is not an integral domain, but rather is a direct sum of local integral domains. Let $\mathcal{M}$ denote the (finite) intersection of all maximal ideals of Λ, i.e., $\mathcal{M}$ is the kernel of the natural map $\Lambda \twoheadrightarrow \mathbf{F}_p[\Delta]$.

A Λ-module M will be called a torsion Λ-module if it is annihilated by a non-zero-divisor in Λ. A Λ-module will be called pseudo-null if it is annihilated by an ideal of height at least two in Λ. If $\Gamma \cong \mathbf{Z}_p$ then a module is pseudo-null if and only if it is finite.

If M is a finitely generated torsion Λ-module, then there is an injective Λ-module homomorphism

$$\bigoplus_{i=1}^{r} \Lambda/f_i\Lambda \hookrightarrow M$$

with pseudo-null cokernel, where the elements $f_i \in \Lambda$ can be chosen to satisfy $f_{i+1} \mid f_i$ for $1 \le i \le r$. The elements f_i are not uniquely determined, but the ideal $\prod_i f_i\Lambda$ is. We call the ideal $\prod_i f_i\Lambda$ the *characteristic ideal* $\mathrm{char}(M)$ of the torsion Λ-module M. The characteristic ideal is multiplicative in exact sequences: if $0 \to M' \to M \to M'' \to 0$ is an exact sequence of torsion Λ-modules then

$$\mathrm{char}(M) = \mathrm{char}(M')\mathrm{char}(M'').$$

11.2 The Iwasawa Modules

Define

$A_n =$ the p-part of the ideal class group of K_n,

$U_n =$ the p-adic completion of the local units of $K_n \otimes K_\mathfrak{p}$ (equivalently, the 1-units of $K_n \otimes K_\mathfrak{p}$),

$\mathcal{E}_n =$ the global units of K_n,

$\bar{\mathcal{E}}_n =$ the p-adic completion of $\mathcal{E}_n$ (equivalently, since Leopoldt's conjecture holds for K_n, the closure of the image of $\mathcal{E}_n$ in U_n),

$\mathcal{C}_n =$ the elliptic units of K_n, the subgroup of $\mathcal{E}_n$ generated over the group ring $\mathbf{Z}[\mathrm{Gal}(K_n/K)]$ by the $\eta_n^{(\mathfrak{a})} = \eta_n^{(\mathfrak{a})}(\mathcal{O})$ (see Definition 8.1) for *all* choices of ideal $\mathfrak{a}$ prime to $6\mathfrak{pf}$, and the roots of unity in K_n,

$\bar{\mathcal{C}_n} =$ the p-adic completion of $\mathcal{C}_n$ (equivalently, the closure of the image of $\mathcal{C}_n$ in U_n),

and

$$A_\infty = \varprojlim_n A_n, \;\; U_\infty = \varprojlim_n U_n, \;\; \mathcal{E}_\infty = \varprojlim_n \bar{\mathcal{E}_n}, \;\; \mathcal{C}_\infty = \varprojlim_n \bar{\mathcal{C}_n},$$

inverse limits with respect to norm maps. Also define $X_\infty = \mathrm{Gal}(M_\infty/K_\infty)$ where M_∞ is the maximal abelian p-extension of K_∞ unramified outside of the prime above $\mathfrak{p}$.

Class field theory identifies A_∞ with $\mathrm{Gal}(L_\infty/K_\infty)$, where L_∞ is the maximal everywhere-unramified abelian p-extension of K_∞, and identifies the inertia group in X_∞ of the unique prime above $\mathfrak{p}$ with $U_\infty/\mathcal{E}_\infty$. Thus there is an exact sequence of Λ-modules

$$0 \to \mathcal{E}_\infty/\mathcal{C}_\infty \to U_\infty/\mathcal{C}_\infty \to X_\infty \to A_\infty \to 0. \tag{13}$$

For every $n \geq 0$, let $\Lambda_n = \mathbf{Z}_p[\mathrm{Gal}(K_n/K)]$ and let $\mathcal{J}_n \subset \Lambda$ denote the kernel of the restriction map $\Lambda \to \Lambda_n$. In particular $\mathcal{J}_0$ is the augmentation ideal of Λ.

Lemma 11.1. *For every $n \geq 1$, the natural map*

$$A_\infty/\mathcal{J}_n A_\infty \to A_n$$

is an isomorphism.

Proof. When $\Gamma = \mathbf{Z}_p$ this is a standard argument going back to Iwasawa [Iw], using the fact that only one prime of K ramifies in K_∞ and it is totally ramified.

For the general case, consider the diagram of fields below, where L_n is the maximal unramified abelian p-extension of K_n, and L'_n is the fixed field of $\mathcal{J}_n A_\infty$ in L_∞. Since K_∞/K_n is totally ramified above $\mathfrak{p}$, $K_\infty \cap L_n = K_n$, and so $\mathrm{Gal}(K_\infty L_n/K_\infty) = A_n$ and the map $A_\infty/\mathcal{J}_n A_\infty \to A_n$ is just the restriction map. We will show that $K_\infty L_n = L'_n$, and the lemma will follow.

Since $\mathrm{Gal}(K_\infty/K_n)$ acts on $\mathrm{Gal}(L_\infty/K_\infty)$ by conjugation, $\mathcal{J}_n A_\infty$ is generated by commutators

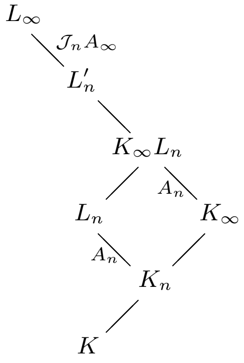
$$\mathrm{Gal}(L_\infty/L'_n) = [\mathrm{Gal}(L_\infty/K_n), \mathrm{Gal}(L_\infty/K_\infty)].$$

Such commutators are trivial on L_n, so $K_\infty L_n \subset L'_n$.

On the other hand, only the unique prime above $\mathfrak{p}$ ramifies in the abelian extension L'_n/K_n, and it is totally ramified in K_∞/K_n. If we write $\mathcal{I}$ for the inertia group of this prime in $\mathrm{Gal}(L'_n/K_n)$, the inverse of the projection isomorphism $\mathcal{I} \xrightarrow{\sim} \mathrm{Gal}(K_\infty/K_n)$ gives a splitting of the exact sequence

$$0 \to A_\infty/\mathcal{J}_n A_\infty \to \mathrm{Gal}(L'_n/K_n) \to \mathrm{Gal}(K_\infty/K_n) \to 0.$$

It follows that ${L'_n}^{\mathcal{I}}$ is an abelian, everywhere-unramified p-extension of K_n, and hence ${L'_n}^{\mathcal{I}} \subset L_n$ and so $L'_n = K_\infty L_n$. □



Proposition 11.2. *A_∞ is a finitely-generated torsion Λ-module.*

Proof. By Lemma 11.1, $A_\infty/\mathcal{J}_n A_\infty$ is finite for every n, and the proposition follows. □

Proposition 11.3. (i) *X_∞ is a finitely-generated Λ-module and for every χ*

$$\mathrm{rank}_{\Lambda_\chi} X_\infty^\chi = [K_\mathfrak{p} : \mathbf{Q}_p] - 1.$$

(In particular if $K_\mathfrak{p} = \mathbf{Q}_p$ then X_∞ is a finitely-generated torsion Λ-module.)

(ii) *X_∞ has no nonzero pseudo-null submodules.*

Proof. See [Gr]. □

Proposition 11.4. *U_∞ is a finitely-generated, torsion-free Λ-module, and for every χ*

$$\mathrm{rank}_{\Lambda_\chi}(U_\infty^\chi) = [K_\mathfrak{p} : \mathbf{Q}_p].$$

Further, if $[K_\mathfrak{p} : \mathbf{Q}_p] = 2$ then $U_\infty^{\chi_E}$ is free of rank 2 over Λ_χ.

Proof. See [Iw] §12 or [Win]. □

Proposition 11.5. *$\mathcal{E}_\infty$ is a finitely-generated Λ-module, and for every χ*

$$\mathrm{rank}_{\Lambda_\chi}(\mathcal{E}_\infty^\chi) = 1.$$

Proof. The natural map $\mathcal{E}_\infty \to U_\infty$ is injective, so the proposition follows from (13) and Propositions 11.2, 11.3 and 11.4 □

Proposition 11.6. *$\mathcal{C}_\infty^{\chi_E}$ is free of rank one over Λ_{χ_E}.*

Proof. Choose an ideal $\mathfrak{a}$ of $\mathcal{O}$ such that $\psi(\mathfrak{a}) \not\equiv \mathbf{N}\mathfrak{a} \pmod{\mathfrak{p}}$ (Lemma 10.2). We will show that $\mathcal{C}_\infty^{\chi_E}$ is generated over Λ_{χ_E} by $\{(\eta_n^{(\mathfrak{a})})^{\chi_E}\}_n$ with this choice of $\mathfrak{a}$. Suppose $\mathfrak{b}$ is some other ideal of $\mathcal{O}$ prime to $6\mathfrak{p}\mathfrak{f}$. It follows from Theorem 7.4(ii) and Lemma 7.10 that for every n

$$(\eta_n^{(\mathfrak{a})})^{\sigma_\mathfrak{b} - \mathbf{N}\mathfrak{b}} = (\eta_n^{(\mathfrak{b})})^{\sigma_\mathfrak{a} - \mathbf{N}\mathfrak{a}}$$

where $\sigma_\mathfrak{a} = [\mathfrak{a}, K_n/K]$, $\sigma_\mathfrak{b} = [\mathfrak{b}, K_n/K]$. Since $\psi(\mathfrak{a}) \not\equiv \mathbf{N}\mathfrak{a} \pmod{\mathfrak{p}}$, and $\sigma_\mathfrak{a}$ acts as $\psi(\mathfrak{a})$ on $E[\mathfrak{p}]$ (Corollary 5.16(ii)), we see that $\sigma_\mathfrak{a} - \mathbf{N}\mathfrak{a}$ acts bijectively on $E[\mathfrak{p}]$. But $E[\mathfrak{p}] \cong \Lambda_{\chi_E}/\mathcal{M}_{\chi_E}$ where $\mathcal{M}_{\chi_E}$ denotes the maximal ideal of the local ring Λ_{χ_E}. Therefore $\sigma_\mathfrak{a} - \mathbf{N}\mathfrak{a}$ is invertible in Λ_{χ_E}, so

$$\{(\eta_n^{(\mathfrak{b})})^{\chi_E}\}_n \in \Lambda_{\chi_E}\{(\eta_n^{(\mathfrak{a})})^{\chi_E}\}_n$$

as claimed. Since U_∞ is torsion-free (Proposition 11.4), $\mathcal{C}_\infty^{\chi_E}$ must free of rank 1. □

11.3 Application of the Euler System of Elliptic Units

Theorem 11.7. $\mathrm{char}(A_\infty)$ *divides* $\mathrm{char}(\mathcal{E}_\infty/\mathcal{C}_\infty)$.

The rest of this section will be devoted to a proof of this theorem. The techniques are similar to those of the proof of Theorem 9.5, but messier and more technically complicated because one needs to study modules over $\mathbf{Z}_p[\mathrm{Gal}(K_n/K)]$ rather than $\mathbf{Z}_p[\Delta]$. See [Ru2] for the details which are not included below, and see [Ru1] for the analogous result for cyclotomic fields.

We also record, but will not prove, the following corollary. With a better definition of elliptic units, it would hold for more representations χ of Δ. See [Ru2] Theorem 4.1 for a precise statement and [Ru2] §10 (see also [dS] §III.2) for the proof, which is an application of the analytic class number formula.

Corollary 11.8. $\mathrm{char}(A_\infty^{\chi_E}) = \mathrm{char}(\mathcal{E}_\infty^{\chi_E}/\mathcal{C}_\infty^{\chi_E})$.

Definition 11.9. Since A_∞ is a torsion Λ-module, we can fix once and for all an injective Λ-module map with pseudo-null cokernel

$$\bigoplus_{i=1}^{r} \Lambda/f_i\Lambda \hookrightarrow A_\infty$$

with $f_i \in \Lambda$, $f_{i+1} \mid f_i$ for $1 \le i \le r$. Let A_∞^0 denote the image of this map, so

$$A_\infty^0 = \oplus_{i=1}^r \Lambda y_i \subset A_\infty$$

where $y_i \in A_\infty$ is the image of $1 \in \Lambda/f_i\Lambda$. Then A_∞^0 is an "elementary" submodule of A_∞ and A_∞/A_∞^0 is pseudo-null.

Let $\Omega = K_\infty(\boldsymbol{\mu}_{p^\infty})$. If $\sigma \in G_\Omega$ we write $[\sigma] \in A_\infty$ for the restriction of σ to L_∞. Note that if $K_\mathfrak{p} \neq \mathbf{Q}_p$ then the Weil pairing (see [Si] Proposition

III.8.1) shows that $\Omega = K_\infty$, and if $K_\mathfrak{p} = \mathbf{Q}_p$ then Ω/K_∞ is totally ramified at the prime $p/\mathfrak{p}$. Thus in either case the map $G_\Omega \to A_\infty$ is surjective.

If $0 \le k \le r$, a *Frobenius sequence* $\boldsymbol{\sigma}$ of length k is a k-tuple $(\sigma_1, \dots, \sigma_k)$ of elements of G_Ω satisfying

$$[\sigma_i] - y_i \in \mathcal{M}A_\infty^0$$

for $1 \le i \le k$, where $\mathcal{M}$ is as defined in §11.1, the intersection of all maximal ideals of Λ.

Suppose $n \ge 1$ and M is a power of p. Recall the subset $\mathcal{R}_{n,M}$ of $\mathcal{R}$ defined in §8.2. For $0 \le k \le r$ we call a k-tuple $(\tilde{\pi}_1, \dots, \tilde{\pi}_k)$ of primes of K_n a *Kolyvagin sequence* (for n and M) if

- the $\tilde{\pi}_i$ lie above distinct primes of K belonging to $\mathcal{R}_{n,M}$, and
- there is a Frobenius sequence $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_k)$ such that for $1 \le i \le k$,

$$\mathrm{Frob}_{\tilde{\pi}_i} = \sigma_i \quad \text{on } L_n$$

where L_n is the maximal unramified abelian p-extension of K_n.

If $\boldsymbol{\pi}$ is a Kolyvagin sequence of length k we will write π_i for the prime of K below $\tilde{\pi}_i$ and we define

$$\mathfrak{r}(\boldsymbol{\pi}) = \prod_{i=1}^{k} \pi_i \in \mathcal{R}_{n,M}.$$

Let $\Pi(k, n, M)$ be the set of all Kolyvagin sequences of length k for n and M.

Fix an ideal $\mathfrak{a}$ so that $\{(\eta_n^{(\mathfrak{a})})^{\chi_E}\}_n$ generates $\mathcal{C}_\infty^{\chi_E}$, as in the proof of Proposition 11.6. Using the Euler system of elliptic units $\eta_n^{(\mathfrak{a})}(\mathfrak{r})$, for $\mathfrak{r} \in \mathcal{R}_{n,M}$ we obtain the Kolyvagin derivative classes

$$\kappa_{n,M}(\mathfrak{r}) \in K_n^\times/(K_n^\times)^M$$

as in Definition 8.7. For every n recall that $\Lambda_n = \mathbf{Z}_p[\mathrm{Gal}(K_n/K)]$ and let $\Lambda_{n,M} = (\mathbf{Z}/M\mathbf{Z})[\mathrm{Gal}(K_n/K)] = \Lambda_n/M\Lambda_n$. If $0 \le k \le r$ define $\Psi(k, n, M)$ to be the ideal of $\Lambda_{n,M}$ generated by

$$\{\psi(\kappa_{n,M}(\mathfrak{r}(\boldsymbol{\pi}))) : \boldsymbol{\pi} \in \Pi(k, n, M), \psi \in \mathrm{Hom}_{\Lambda_n}(\Lambda_{n,M}\kappa_{n,M}(\mathfrak{r}(\boldsymbol{\pi})), \Lambda_{n,M})\}$$

When $k = 0$, $\Pi(k, n, M)$ has a single element (the empty sequence) and

$$\Psi(0, n, M) \supset \{\psi(\eta_n^{(\mathfrak{a})}) \pmod{M} : \psi \in \mathrm{Hom}_{\Lambda_n}(\mathcal{E}_n, \Lambda_n)\} \qquad (14)$$

It follows from Lemma 11.1 that $A_\infty/\mathcal{J}_n A_\infty$ is finite for every n. From this it is not difficult to show that $\Lambda_n/\mathrm{char}(A_\infty)\Lambda_n$ is also finite for every n. For every n define N_n to be the product of $\#(A_n)$ and the smallest power of p which annihilates $\Lambda_n/\mathrm{char}(A_\infty)\Lambda_n$.

The following proposition is the key to the proof of Theorem 11.7.

Proposition 11.10. *There is an ideal $\mathcal{B}$ of height at least two in Λ such that for every $n \geq 1$, power M of p, and $0 \leq k < r$,*

$$\mathcal{B}\Psi(k, n, MN_n)\Lambda_{n,M} \subset f_{k+1}\Psi(k+1, n, M).$$

We will first show how to complete the proof of Theorem 11.7 assuming Proposition 11.10, and then we will prove Proposition 11.10.

Lemma 11.11. *Suppose G is a finite abelian group and B is finitely generated $\mathbf{Z}_p[G]$-module with no p-torsion. If $f \in \mathbf{Z}_p[G]$ is not a zero-divisor, $b \in B$, and*

$$\{\psi(b) : \psi \in \operatorname{Hom}_{\mathbf{Z}_p[G]}(B, \mathbf{Z}_p[G])\} \subset f\mathbf{Z}_p[G],$$

then $b \in fB$.

Proof. Let $B' = \mathbf{Z}_p[G]b + fB$. Since f is not a zero-divisor, we have a commutative diagram

$$\begin{tikzcd}
\operatorname{Hom}_{\mathbf{Z}_p[G]}(B', f\mathbf{Z}_p[G]) \arrow[d] & \operatorname{Hom}_{\mathbf{Z}_p[G]}(B', \mathbf{Z}_p[G]) \arrow[l, "f"'] \arrow[r, "\sim"] \arrow[d] & \operatorname{Hom}_{\mathbf{Z}_p}(B', \mathbf{Z}_p) \arrow[d] \\
\operatorname{Hom}_{\mathbf{Z}_p[G]}(fB, f\mathbf{Z}_p[G]) & \operatorname{Hom}_{\mathbf{Z}_p[G]}(fB, \mathbf{Z}_p[G]) \arrow[l, "f"'] \arrow[r, "\sim"] & \operatorname{Hom}_{\mathbf{Z}_p}(fB, \mathbf{Z}_p)
\end{tikzcd}$$

in which the horizontal maps are all isomorphisms.

Choose $\bar{\varphi} \in \operatorname{Hom}_{\mathbf{Z}_p[G]}(fB, f\mathbf{Z}_p[G])$. Since B has no p-torsion and f is not a zero-divisor, $\bar{\varphi}$ extends uniquely to a map $\varphi : B \to \mathbf{Z}_p[G]$, and by our assumption, $\varphi \in \operatorname{Hom}_{\mathbf{Z}_p[G]}(B', f\mathbf{Z}_p[G])$. Thus all the vertical maps in the diagram above are isomorphisms. Since B' and fB are free $\mathbf{Z}_p$-modules, the surjectivity of the right-hand vertical map shows that $B' = fB$, which proves the lemma. □

Proof (of Theorem 11.7, assuming Proposition 11.10). Fix $n \geq 1$ and $\psi \in \operatorname{Hom}_{\Lambda_n}(\bar{\mathcal{E}_n}, \Lambda_n)$, and let $\mathcal{B} \subset \Lambda$ be an ideal of height at least two satisfying Proposition 11.10. We will show that, for every choice of $\mathfrak{a}$,

$$\mathcal{B}^r\psi(\eta_n^{(\mathfrak{a})}) \subset \operatorname{char}(A_\infty)\Lambda_n. \tag{15}$$

Assuming this, Lemma 11.11 applied with $B = \bar{\mathcal{E}_n}/(\bar{\mathcal{E}_n})_{\text{tors}}$ shows that

$$\mathcal{B}^r\eta_n^{(\mathfrak{a})} \subset \operatorname{char}(A_\infty)\bar{\mathcal{E}_n} + (\bar{\mathcal{E}_n})_{\text{tors}}.$$

Since $\mathcal{E}_\infty$ has no Λ-torsion (Lemma 11.5), it follows that

$$\mathcal{B}^r\{\eta_n^{(\mathfrak{a})}\}_n \subset \operatorname{char}(A_\infty)\mathcal{E}_\infty.$$

Thus $\mathcal{B}^r\mathcal{C}_\infty \subset \operatorname{char}(A_\infty)\mathcal{E}_\infty$, and since $\mathcal{B}^r$ is an ideal of height at least two the theorem follows.

It remains to prove (15). Suppose $0 \le k < r$ and M is a power of p. Proposition 11.10 shows that

$$\mathcal{B}\Psi(k,n,MN_n^{r-k})\Lambda_{n,M} \subset f_{k+1}\Psi(k+1,n,MN_n^{r-k-1})\Lambda_{n,M},$$

so by induction we conclude that

$$\mathcal{B}^r\Psi(0,n,MN_n^r)\Lambda_{n,M} \subset \left(\prod_{i=1}^r f_i\right)\Psi(r,n,M) \subset \mathrm{char}(A_\infty)\Lambda_{n,M}. \qquad (16)$$

Using (14) it follows that

$$\mathcal{B}^r\psi(\eta_n^{(\mathfrak{a})})\Lambda_{n,M} \subset \mathrm{char}(A_\infty)\Lambda_{n,M},$$

and since this holds for every M, it proves (15). This completes the proof of Theorem 11.7. □

The rest of this section is devoted to proving Proposition 11.10. If $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_k)$ is a Frobenius sequence define

$$A_{\boldsymbol{\sigma}} = \sum_{i=1}^k \Lambda[\sigma_i] \subset A_\infty^0.$$

Lemma 11.12. *If $\boldsymbol{\sigma}$ is a Frobenius sequence of length k then $A_{\boldsymbol{\sigma}}$ is a direct summand of A_∞^0 and $A_{\boldsymbol{\sigma}} = \oplus_{i=1}^k \Lambda/f_i\Lambda$.*

Proof. Recall that $A_\infty^0 = \oplus_{i=1}^r \Lambda y_i$. Define $Y_k = \sum_{i=k+1}^r \Lambda y_i$. The image of $A_{\boldsymbol{\sigma}} + Y_k$ in $A_\infty^0/\mathcal{M}A_\infty^0$ contains all the y_i, so by Nakayama's Lemma, $A_{\boldsymbol{\sigma}} + Y_k = A_\infty^0$. We will show that $A_{\boldsymbol{\sigma}} \cap Y_k = 0$, and thus $A_\infty^0 = A_{\boldsymbol{\sigma}} \oplus Y_k$ and

$$A_{\boldsymbol{\sigma}} \cong A_\infty^0/Y_k \cong \oplus_{i=1}^k \Lambda/f_i\Lambda.$$

For $1 \le i \le k$ write

$$[\sigma_i] = y_i + v_i + w_i$$

where $v_i \in \mathcal{M}(\oplus_{i\le k}\Lambda y_i)$ and $w_i \in \mathcal{M}Y_k$. Suppose

$$\sum_{i=1}^k a_i[\sigma_i] \in Y_k$$

with $a_i \in \Lambda$. Then we must have $\sum_{i=1}^k a_i(y_i + v_i) = 0$. We can write this in matrix form, using the basis $y_1, \dots, y_k$ of $\oplus_{i\le k}\Lambda y_i$, as

$$(a_1, \dots, a_k)B \in (f_1\Lambda, \dots, f_k\Lambda)$$

where B is a $k \times k$ matrix with entries in Λ, congruent to the identity matrix modulo $\mathcal{M}$. Therefore B is invertible, and, since $f_k \mid f_i$ for every $i \le k$, we conclude that each a_i is divisible by f_k. But f_k annihilates Y_k, so we deduce that

$$\sum_{i=1}^{k} a_i[\sigma_i] = \sum_{i=1}^{k} a_i w_i = 0.$$

This completes the proof of the lemma. □

Recall $\varOmega = K_\infty(\boldsymbol{\mu}_{p^\infty})$.

Proposition 11.13. *Suppose W is a finite subgroup of $K_n^\times/(K_n^\times)^M$ for some n and M. Then G_K acts trivially on the cokernel of the natural Kummer map*

$$G_\varOmega \to \operatorname{Hom}(W, \boldsymbol{\mu}_M).$$

Proof. Let $\bar{W}$ denote the image of W in $\varOmega^\times/(\varOmega^\times)^M$. The map in question factors

$$G_\varOmega \to \operatorname{Hom}(\bar{W}, \boldsymbol{\mu}_M) \to \operatorname{Hom}(W, \boldsymbol{\mu}_M).$$

where the first (Kummer) map is surjective and the cokernel of the second is $\operatorname{Hom}(V, \boldsymbol{\mu}_M)$ with

$$V = \ker(W \to \bar{W}) \subset \ker(H^1(K_n, \boldsymbol{\mu}_M) \to H^1(\varOmega, \boldsymbol{\mu}_M)) = H^1(\varOmega/K_n, \boldsymbol{\mu}_M).$$

Since $\varOmega$ is abelian over K, G_K acts on V via the cyclotomic character, and hence G_K acts trivially on $\operatorname{Hom}(V, \boldsymbol{\mu}_M)$. The proposition follows. □

Let $\mathcal{A}$ denote the annihilator in $\varLambda$ of A_∞/A_∞^0, so $\mathcal{A}$ is an ideal of height at least two.

Lemma 11.14. *Suppose $n \geq 0$, M is a power of p, $k < r$, and $\boldsymbol{\pi} = \{\tilde{\pi}_1, \ldots, \tilde{\pi}_{k+1}\} \in \varPi(k+1, n, MN_n)$. Let $\mathfrak{Q} = \tilde{\pi}_{k+1}$, $\mathfrak{q} = \pi_{k+1}$ and $\mathfrak{r} = \mathfrak{q}^{-1}\mathfrak{r}(\boldsymbol{\pi})$. If $\rho \in \mathcal{A}$ then there is a Galois-equivariant homomorphism*

$$\psi : \varLambda_{n,M}\kappa_{n,M}(\mathfrak{r}\mathfrak{q}) \to \varLambda_{n,M}$$

such that

$$\rho\phi_{\mathfrak{q}}(\kappa_{n,M'}(\mathfrak{r})) \equiv f_{k+1}\psi(\kappa_{n,M}(\mathfrak{r}\mathfrak{q}))\mathfrak{Q} \pmod{M}$$

where $\phi_{\mathfrak{q}} : \varLambda_{n,MN_n}\kappa_{n,MN_n}(\mathfrak{r}) \to \varLambda_{n,MN_n}\mathfrak{Q}$ is the map of Definition 8.9.

Proof. Write $M' = MN_n$, and let $\boldsymbol{\sigma}$ be a Frobenius sequence corresponding to $\boldsymbol{\pi}$. Let $\bar{A}_n$ denote the quotient of A_n by the $\varLambda_n$-submodule generated by the classes of $\tilde{\pi}_1, \ldots, \tilde{\pi}_k$, and let $[\mathfrak{Q}]$ denote the class of $\mathfrak{Q}$ in $\bar{A}_n$. Since the Frobenius of $\mathfrak{Q}$ on the Hilbert class field of K_n is σ, $[\mathfrak{Q}]$ is the projection of $[\sigma]$ to $\bar{A}_n$. By Lemma 11.12 the annihilator of $[\sigma]$ in $A_\infty^0/A_{\boldsymbol{\sigma}}$ is $f_{k+1}\varLambda$ and $A_{\boldsymbol{\sigma}}$ is a direct summand of A_∞^0, so the annihilator of $[\sigma]$ in $(A_\infty^0/A_{\boldsymbol{\sigma}}) \otimes \varLambda_n$ is $f_{k+1}\varLambda_n$. By Lemma 11.1, $\bar{A}_n = A_\infty/(A_{\boldsymbol{\sigma}} + \mathcal{J}_n A_\infty)$ so the kernel of the natural map $(A_\infty^0/A_{\boldsymbol{\sigma}})\otimes\Lambda_n \to \bar{A}_n$ is annihilated by $\mathcal{A}$. Therefore if $\mathcal{A}' \subset \Lambda_n$ is the annihilator of $[\mathfrak{Q}]$ in $\bar{A}_n$, then

$$\mathcal{A}\mathcal{A}' \subset f_{k+1}\Lambda_n.$$

Since $\#(A_n)$ divides N_n, Proposition 8.10(i) shows that $[\kappa_{n,M'}(\mathfrak{r}\mathfrak{q})]_{\mathfrak{q}}$ is 0 in $\bar{A}_n$. Therefore $[\kappa_{n,M'}(\mathfrak{r}\mathfrak{q})]_{\mathfrak{q}} \in \mathcal{A}'\Lambda_{n,M'}\mathfrak{Q}$, so if $\rho \in \mathcal{A}$ then

$$\rho[\kappa_{n,M'}(\mathfrak{r}\mathfrak{q})]_{\mathfrak{q}} \in f_{k+1}\Lambda_{n,M'}\mathfrak{Q}.$$

Since f_{k+1} divides f_1 and f_1 divides N_n in Λ_n, the map

$$f_{k+1}^{-1} : \Lambda_{n,M'} \to \Lambda_{n,M}$$

is well-defined, and we will define $\psi : \Lambda_{n,M}\kappa_{n,M}(\mathfrak{r}\mathfrak{q}) \to \Lambda_{n,M}\mathfrak{Q}$ by

$$\psi(\kappa_{n,M}(\mathfrak{r}\mathfrak{q}))\mathfrak{Q} = f_{k+1}^{-1}\rho[\kappa_{n,M'}(\mathfrak{r}\mathfrak{q})]_{\mathfrak{q}}.$$

If we can show that ψ is well-defined, then by Proposition 8.10(ii) we will have

$$\rho\phi_{\mathfrak{q}}(\kappa_{n,M'}(\mathfrak{r})) = \rho[\kappa_{n,M'}(\mathfrak{r}\mathfrak{q})]_{\mathfrak{q}} \equiv f_{k+1}\psi(\kappa_{n,M}(\mathfrak{r}\mathfrak{q}))\mathfrak{Q} \pmod{M}$$

as desired.

We need to show that ψ is well-defined, i.e., if $\eta \in \Lambda_n$ and $\kappa_{n,M}(\mathfrak{r}\mathfrak{q})^\eta \in (K_n^\times)^M$ then $\eta\rho[\kappa_{n,M'}(\mathfrak{r}\mathfrak{q})]_{\mathfrak{q}} \in f_{k+1}M\Lambda_{n,M'}\mathfrak{Q}$. But this is essentially the same argument as above. If η annihilates $\kappa_{n,M}(\mathfrak{r}\mathfrak{q})$ then $\kappa_{n,M'}(\mathfrak{r}\mathfrak{q})^\eta = \alpha^M$ for some $\alpha \in K_n^\times$. Again using Proposition 8.10(i), $[\alpha]_{\mathfrak{q}}$ is 0 in $\bar{A}_n$, so $\rho[\alpha]_{\mathfrak{q}} \in f_{k+1}\Lambda_{n,N_n}\mathfrak{Q}$ and the desired inclusion follows. □

Proof (of Proposition 11.10). Let $\Lambda_\Omega = \mathbf{Z}_p[[\mathrm{Gal}(\Omega/K)]]$ and denote by ϵ both the cyclotomic character $\mathrm{Gal}(\Omega/K) \to \mathbf{Z}_p^\times$ and the induced map $\Lambda_\Omega \to \mathbf{Z}_p$. Define

$$\mathrm{tw}_\epsilon : \Lambda_\Omega \to \Lambda_\Omega$$

to be the homomorphism induced by $\gamma \mapsto \epsilon(\gamma)\gamma^{-1}$ for $\gamma \in \mathrm{Gal}(\Omega/K)$.

Recall that $\mathcal{A}$ is the annihilator of A_∞/A_∞^0, and define

$$\mathcal{B} = \begin{cases} \mathcal{A} & \text{if } K_{\mathfrak{p}} = \mathbf{Q}_p \\ \mathcal{A}\,\mathrm{tw}_\epsilon(\mathcal{M}\mathcal{A}\mathcal{J}_0) & \text{if } K_{\mathfrak{p}} \neq \mathbf{Q}_p \end{cases}$$

(recall that $\Omega = K_\infty$ if $K_{\mathfrak{p}} \neq \mathbf{Q}_p$). Then $\mathcal{B}$ is an ideal of height at least two, and we will show that Proposition 11.10 holds with this choice of $\mathcal{B}$.

Fix n and M, and write $M' = MN_n$. Fix a Kolyvagin sequence $\boldsymbol{\pi} \in \Pi(k,n,M')$, let $\mathfrak{r} = \mathfrak{r}(\boldsymbol{\pi})$, and suppose $\psi : \Lambda_{n,M'}\kappa_{n,M'}(\mathfrak{r}) \to \Lambda_{n,M'}$. We need to show that

$$\mathcal{B}\psi(\kappa_{n,M'}(\mathfrak{r}))\Lambda_{n,M} \subset f_{k+1}\Psi(k+1,n,M).$$

We will do this by constructing suitable Kolyvagin sequences of length $k+1$ extending $\boldsymbol{\pi}$.

There is a $\mathbf{Z}_p$-module isomorphism

$$\iota : \mathrm{Hom}_{\Lambda_n}(\Lambda_{n,M'}\kappa_{n,M'}(\mathfrak{r}), \Lambda_{n,M'}) \otimes \boldsymbol{\mu}_{M'} \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_p}(\Lambda_{n,M'}\kappa_{n,M'}(\mathfrak{r}), \boldsymbol{\mu}_{M'})$$

induced by

$$(\sum_{\gamma} a_\gamma \gamma) \otimes \zeta \mapsto \zeta^{a_1}.$$

One can check that if $\phi \in \mathrm{Hom}_{\Lambda_n}(\Lambda_{n,M'}\kappa_{n,M'}(\mathfrak{r}), \Lambda_{n,M'})$, $\zeta \in \boldsymbol{\mu}_{M'}$, and $\rho \in \Lambda_\Omega$ then

$$\rho\iota(\phi \otimes \zeta) = \iota((\mathrm{tw}_\epsilon(\rho)\phi) \otimes \zeta).$$

Suppose $\tau \in G_K$, fix a primitive M'-th root of unity $\zeta_{M'}$, and let $\mathrm{Kum}_{M'}$ denote the Kummer map $G_\Omega \to \mathrm{Hom}(K_n^\times, \boldsymbol{\mu}_{M'})$. By Proposition 11.13 there is a $\gamma_0 \in G_\Omega$ such that

$$\mathrm{Kum}_{M'}(\gamma_0) = (\tau - 1)\iota(\psi \otimes \zeta_{M'}) \quad \text{on } \Lambda_{n,M'}\kappa_{n,M'}(\mathfrak{r}).$$

Choose $\rho \in \Lambda_\Omega$ such that the projection of ρ to Λ lies in $\mathcal{M}\mathcal{A}$ and let $\gamma \in G_\Omega$ be such that $\gamma = \gamma_0^\rho$ on Ω^{ab} (we view $\mathrm{Gal}(\Omega/K)$ as acting on $\mathrm{Gal}(\Omega^{\mathrm{ab}}/\Omega)$ in the usual way).

Let $\boldsymbol{\sigma}$ be a Frobenius sequence corresponding to $\boldsymbol{\pi}$. We define two Frobenius sequences $\boldsymbol{\sigma}'$ and $\boldsymbol{\sigma}''$ of length $k+1$ extending $\boldsymbol{\sigma}$ as follows. Let σ'_{k+1} be an element of G_Ω such that $[\sigma'_{k+1}] = y_{k+1}$, and let $\sigma''_{k+1} = \sigma'_{k+1}\gamma$ with γ as above.

Since $[\gamma] = \rho[\gamma_0] \in \mathcal{M}A^0_\infty$, both $\boldsymbol{\sigma}'$ and $\boldsymbol{\sigma}''$ are Frobenius sequences.

Let $\mathfrak{q}'$ and $\mathfrak{q}''$ be primes of K whose Frobenius elements (for some choice of primes "upstairs") in $H_n(\boldsymbol{\mu}_{M'}, (\Lambda_n\kappa_{n,M'}(\mathfrak{r}))^{1/M'})/K$ are the restrictions of σ' and σ'', respectively, where H_n is the Hilbert class field of K_n. Let $\mathfrak{Q}'$ and $\mathfrak{Q}''$ be primes of K_n above $\mathfrak{q}'$ and $\mathfrak{q}''$ with these Frobenius elements. It follows from Definition 8.9 that there are integers a' and a'' such that

$$\iota(\bar\phi_{\mathfrak{q}'} \otimes \zeta_{M'}^{a'}) = \mathrm{Kum}_{M'}(\sigma'), \quad \iota(\bar\phi_{\mathfrak{q}''} \otimes \zeta_{M'}^{a''}) = \mathrm{Kum}_{M'}(\sigma'')$$

where $\phi_{\mathfrak{q}'} : \Lambda_{n,M'}\kappa_{n,M'}(\mathfrak{r}) \to \Lambda_{n,M'}\mathfrak{Q}'$ is the map of Definition 8.9, $\bar\phi_{\mathfrak{q}'} \in \mathrm{Hom}(\Lambda_{n,M'}\kappa_{n,M'}(\mathfrak{r}), \Lambda_{n,M'})$ is defined by $\phi_{\mathfrak{q}'} = \bar\phi_{\mathfrak{q}'}\mathfrak{Q}'$, and similarly for $\mathfrak{q}''$. Now

$$\begin{aligned}\iota(\mathrm{tw}_\epsilon(\rho(\tau-1))\psi) \otimes \zeta_{M'} &= \rho\mathrm{Kum}_{M'}(\gamma_0)\\ &= \mathrm{Kum}_{M'}(\sigma'') - \mathrm{Kum}_{M'}(\sigma')\\ &= \iota(a''\bar\phi_{\mathfrak{q}''} \otimes \zeta_{M'} - a'\bar\phi_{\mathfrak{q}'} \otimes \zeta_{M'})\end{aligned}$$

and so finally

$$\mathrm{tw}_\epsilon(\rho(\tau-1))\psi = a''\bar\phi_{\mathfrak{q}''} - a'\bar\phi_{\mathfrak{q}'}. \qquad (17)$$

If $K_{\mathfrak{p}} \neq \mathbf{Q}_p$, then the $\mathrm{tw}_\epsilon(\rho)(\epsilon(\tau)\tau - 1)$, with our choices of τ and ρ, generate $\mathrm{tw}_\epsilon(\mathcal{MAJ}_0)$. If $K_{\mathfrak{p}} = \mathbf{Q}_p$, then $\boldsymbol{\mu}_p \not\subset K_\infty$ (since K_∞/K is unramified at $p/\mathfrak{p}$) and so we can choose τ and ρ so that $\mathrm{tw}_\epsilon(\rho(\tau - 1))$ projects to a unit in Λ. Now Lemma 11.14 completes the proof of Proposition 11.10. □

12 Computing the Selmer Group

In this section we compute the order of the p-power Selmer group for primes $p > 7$ of dood reduction, and thereby prove assertion (ii) of the theorem of the introduction. The computation divides naturally into two cases depending on whether p splits in K or not.

Keep the notation of the previous section. In particular E is an elliptic curve defined over an imaginary quadratic field K, with complex multiplication by the full ring of integers of K, and $\mathfrak{p}$ is a prime of K of residue characteristic greater than 7 where E has good reduction.

Definition 12.1. Let $\pi = \psi(\mathfrak{p})$ and recall that the π-adic Tate module of E is defined by

$$T_\pi(E) = \varprojlim_n E[\mathfrak{p}^n],$$

inverse limit with respect to multiplication by π. For every n let $\delta_n : U_n \to E[\mathfrak{p}^n]$ be the map of Lemma 6.8. It is clear from the definition that we have commutative diagrams

$$\begin{tikzcd} U_{n+1} \arrow[r, "\delta_{n+1}"] \arrow[d, "\mathbf{N}_{K_{n+1}/K_n}"'] & E[\mathfrak{p}^{n+1}] \arrow[d, "\pi"] \\ U_n \arrow[r, "\delta_n"] & E[\mathfrak{p}^n], \end{tikzcd}$$

and we define

$$\delta_\infty = \varprojlim_n \delta_n : U_\infty \to T_\pi(E).$$

Recall the Selmer group $\mathcal{S}_{\pi^n}(E)$ of Definition 4.1 and the extended Selmer group $\mathcal{S}'_{\pi^n}(E)$ of Definition 6.3. Define

$$\mathcal{S}_{\mathfrak{p}^\infty} = \varinjlim_n \mathcal{S}_{\pi^n}(E), \quad \mathcal{S}'_{\mathfrak{p}^\infty} = \varinjlim_n \mathcal{S}'_{\pi^n}(E).$$

Thus there is an exact sequence

$$0 \to E(K) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to \mathcal{S}_{\mathfrak{p}^\infty} \to \text{Ш}(E)_{\mathfrak{p}^\infty} \to 0. \tag{18}$$

Proposition 12.2. (i) $\mathcal{S}'_{\mathfrak{p}^\infty} = \mathrm{Hom}(X_\infty, E[\mathfrak{p}^\infty])^{G_\infty} = \mathrm{Hom}(X_\infty^{\chi_E}, E[\mathfrak{p}^\infty])^\Gamma$.
(ii) $\mathcal{S}_{\mathfrak{p}^\infty}$ *is the kernel of the composition*

$$\mathcal{S}'_{\mathfrak{p}^\infty} \xrightarrow{\sim} \mathrm{Hom}(X_\infty^{\chi_E}, E[\mathfrak{p}^\infty])^\Gamma \to \mathrm{Hom}(\ker(\delta_\infty), E[\mathfrak{p}^\infty])$$

induced by (i) and local class field theory.

Proof. The first assertion is just a restatement of Proposition 6.5, and the second follows from Theorem 6.9. □

Theorem 12.3 (Wiles' explicit reciprocity law [Wil]). *Suppose* $\mathbf{x}$ *is an* $\mathcal{O}_\mathfrak{p}$*-generator of* $T_\pi(E)$*,* $\mathbf{z} = (z_n)$ *is the corresponding generator of* $T_\pi(\hat{E})$*,* $\mathbf{u} = (u_n) \in U_\infty$*, and* $f(Z) \in \mathcal{O}_\mathfrak{p}[[Z]]$ *is such that* $f(z_n) = u_n$ *for every* n*. Then*

$$\delta_\infty(\mathbf{u}) = (\psi(\mathfrak{p}) - 1)\frac{f'(0)}{f(0)}\mathbf{x}.$$

See [Wil] or [dS] Theorem I.4.2 for the proof.

Corollary 12.4. $\delta_\infty(\mathcal{C}_\infty) = \dfrac{L(\bar{\psi}, 1)}{\Omega} T_\pi(E)$

Proof. Using Theorem 12.3, we see that $\delta_\infty(\mathcal{C}_\infty)$ is the ideal of $\mathcal{O}_\mathfrak{p}$ generated by the values $(\Lambda'_{\mathfrak{p},\mathfrak{a}}(0)/\Lambda_{\mathfrak{p},\mathfrak{a}}(0))$ where $\Lambda_{\mathfrak{p},\mathfrak{a}}$ is defined in Definition 7.21, and we allow the ideal $\mathfrak{a}$ to vary. The corollary now follows from Theorem 7.22(ii) and Lemma 10.2. □

Remark 12.5. In fact, for every $\mathbf{u} \in U_\infty$ there is a power series $f_\mathbf{u} \in \mathcal{O}_\mathfrak{p}[[X]]$ such that $f_\mathbf{u}(z_n) = u_n$ for every n as in Theorem 12.3. See [Col] or [dS] §I.2.

Definition 12.6. Let $\rho_E : G_\infty \to \mathcal{O}_\mathfrak{p}^\times$ be the character giving the action of G_∞ on $E[\mathfrak{p}^\infty]$. We can also view ρ_E as a homomorphism from Λ to $\mathcal{O}_\mathfrak{p}$, and we define $\mathcal{A}_E \subset \Lambda$ to be the kernel of this homomorphism.

If $a, b \in K_\mathfrak{p}$ we will write $a \sim b$ to mean that $a/b \in \mathcal{O}_\mathfrak{p}^\times$.

12.1 Determination of the Selmer Group when $K_\mathfrak{p} = \mathbf{Q}_p$

For this subsection we suppose (in addition to our other assumptions) that $K_\mathfrak{p} = \mathbf{Q}_p$.

If M is a Λ-module we will write

$$M^{\mathcal{A}_E=0} = \{m \in M : \mathcal{A}_E m = 0\}.$$

Proposition 12.7. *Suppose that* M *is a finitely-generated torsion* Λ *module.*

(i) $\mathrm{Hom}(M, E[\mathfrak{p}^\infty])^{G_\infty}$ *is finite* $\Leftrightarrow \rho_E(\mathrm{char}(M)) \neq 0 \Leftrightarrow M^{\mathcal{A}_E=0}$ *is finite.*

(ii) $\#(\mathrm{Hom}(M, E[\mathfrak{p}^\infty])^{G_\infty}) \sim \rho_E(\mathrm{char}(M))\#(M^{\mathcal{A}_E=0})$.

Proof. Fix an exact sequence of Λ-modules

$$0 \to \bigoplus_{i=1}^{k} \Lambda/f_i\Lambda \to M \to Z \to 0$$

with pseudo-null (in this case, finite) cokernel Z. Fix a topological generator γ of $G_\infty = \Delta \times \Gamma$. Then $\mathcal{A}_E = (\gamma - \rho_E(\gamma))\Lambda$, so multiplication by $\gamma - \rho_E(\gamma)$ leads to a snake lemma exact sequence of kernels and cokernels

$$0 \to \bigoplus_{i=1}^{k} (\Lambda/f_i\Lambda)^{\mathcal{A}_E=0} \to M^{\mathcal{A}_E=0} \to Z^{\mathcal{A}_E=0}$$

$$\to \bigoplus_{i=1}^{k} \Lambda/(f_i\Lambda + \mathcal{A}_E) \to M/\mathcal{A}_E M \to Z/\mathcal{A}_E \to 0.$$

Also

$$\mathrm{Hom}(M, E[\mathfrak{p}^\infty])^{G_\infty} = \mathrm{Hom}(M/\mathcal{A}_E M, E[\mathfrak{p}^\infty]).$$

The map ρ_E induces an isomorphism $\Lambda/(f_i\Lambda + \mathcal{A}_E) \xrightarrow{\sim} \mathbf{Z}_p/\rho_E(f_i)\mathbf{Z}_p$, and

$$(\Lambda/f_i\Lambda)^{\mathcal{A}_E=0} = \{g \in \Lambda, g\mathcal{A}_E \subset f_i\Lambda\}/f_i\Lambda$$

so since $\mathcal{A}_E$ is a prime ideal,

$$(\Lambda/f_i\Lambda)^{\mathcal{A}_E=0} \neq 0 \Leftrightarrow f_i \in \mathcal{A}_E \Leftrightarrow (\Lambda/f_i\Lambda)^{\mathcal{A}_E=0} \text{ is infinite.}$$

Since Z is finite, the exact sequence

$$0 \to Z^{\mathcal{A}_E=0} \to Z \xrightarrow{\gamma-\rho_E(\gamma)} Z \to Z/\mathcal{A}_E Z \to 0$$

shows that $\#(Z^{\mathcal{A}_E=0}) = \#(Z/\mathcal{A}_E Z)$. Since $\mathrm{char}(M) = \prod_i f_i\Lambda$, the lemma follows. □

Theorem 12.8. $\#(\mathcal{S}'_{\mathfrak{p}^\infty}) = [\mathbf{Z}_p : \rho_E(\mathrm{char}(X_\infty))]$.

Proof. This is immediate from Propositions 12.2(i), 11.3, and 12.7 (note that if $\rho_E(\mathrm{char}(X_\infty)) \neq 0$ then $X_\infty^{\mathcal{A}_E=0}$ is finite by Proposition 12.7 and hence zero by Proposition 11.3). □

Theorem 12.9. $\mathrm{char}(X_\infty^{\chi_E}) = \mathrm{char}(U_\infty^{\chi_E}/\mathcal{C}_\infty^{\chi_E})$.

Proof. Immediate from Corollary 11.8 and (13). □

Theorem 12.10 (Coates and Wiles). *Let $\mathcal{D}$ denote the ring of integers of the completion of the maximal unramified extension of $\mathbf{Q}_p$. Then there is a $\mathfrak{p}$-adic period $\Omega_{\mathfrak{p}} \in \mathcal{D}^\times$ such that* $\mathrm{char}(U_\infty/\mathcal{C}_\infty)\mathcal{D}[[G_\infty]]$ *has a generator $\mathcal{L}_E$ satisfying*

$$\rho_E^k(\mathcal{L}_E) = \Omega_{\mathfrak{p}}^k(1 - \psi(\mathfrak{p}^k)/p)\frac{L(\bar{\psi}^k, k)}{\Omega^k}$$

for every $k \geq 1$.

Proof. See [CW2] or [dS] Corollary III.1.5. □

Corollary 12.11. $\#(\mathcal{S}'_{\mathfrak{p}^\infty}) \sim (1-\psi(\mathfrak{p})/p)\dfrac{L(\bar{\psi},1)}{\Omega}$.

Proof. Immediate from Theorem 12.8, Theorem 12.9, and Theorem 12.10. □

Proposition 12.12. $[\mathcal{S}'_{\mathfrak{p}^\infty} : \mathcal{S}_{\mathfrak{p}^\infty}] \sim (1-\psi(\mathfrak{p})/p)$.

For a proof see [PR] Proposition II.8 or [Co] Proposition 2 and Lemma 3.

Corollary 12.13. *Suppose $\mathfrak{p} \nmid \mathfrak{f}$, $p > 7$, and $K_\mathfrak{p} = \mathbf{Q}_p$.*

(i) *If $L(\bar{\psi},1) = 0$ then $\mathcal{S}_{\mathfrak{p}^\infty}$ is infinite.*
(ii) *If $L(\bar{\psi},1) \neq 0$ then*

$$\#(\text{Ш}(E)_{\mathfrak{p}^\infty}) \sim \frac{L(\bar{\psi},1)}{\Omega}.$$

Proof. This is immediate from Corollary 12.11 and Proposition 12.12. (For (ii), we also use (18).) □

12.2 Determination of the Selmer Group when $[K_\mathfrak{p} : \mathbf{Q}_p] = 2$

For this subsection we suppose that $[K_\mathfrak{p} : \mathbf{Q}_p] = 2$, so $\Gamma \cong \mathbf{Z}_p^2$ and $E[\mathfrak{p}^\infty] \cong K_\mathfrak{p}/\mathcal{O}_\mathfrak{p}$ has $\mathbf{Z}_p$-corank 2.

Lemma 12.14. *There is a decomposition*

$$U_\infty^{\chi_E} = V_1 \oplus V_2$$

where V_1 and V_2 are free of rank one over Λ_{χ_E}, $\delta_\infty(V_2) = 0$, and $\mathcal{E}_\infty^{\chi_E} \not\subset V_2$.

Proof. By Proposition 11.4, $U_\infty^{\chi_E}$ is free of rank two over Λ_{χ_E}. Fix a splitting $U_\infty^{\chi_E} = \Lambda_{\chi_E} v_1 \oplus \Lambda_{\chi_E} v_2$. By Corollary 5.20(ii), ρ_E is surjective, and it follows that $\delta_\infty(\Lambda_{\chi_E} v_1)$ and $\delta_\infty(\Lambda_{\chi_E} v_2)$ are $\mathcal{O}_\mathfrak{p}$-submodules of $T_\pi(E)$. Since δ_∞ is surjective (Lemma 6.8) and $\delta_\infty(U_\infty) = \delta_\infty(U_\infty^{\chi_E})$, it follows that either $\delta_\infty(\Lambda_{\chi_E} v_1) = T_\pi(E)$ or $\delta_\infty(\Lambda_{\chi_E} v_2) = T_\pi(E)$.

Thus, by renumbering if necessary, we may assume that $\delta_\infty(\Lambda_{\chi_E} v_1) = T_\pi(E)$. In particular we can choose $g \in \Lambda_{\chi_E}$ so that $\delta_\infty(v_2) = \delta_\infty(g v_1)$, and (by adjusting g if necessary by an element of the kernel of ρ_E) we may assume that $\mathcal{E}_\infty \not\subset \Lambda_{\chi_E}(v_2 - g v_1)$. Now the lemma is satisfied with

$$V_1 = \Lambda_{\chi_E} v_1, \quad V_2 = \Lambda_{\chi_E}(v_2 - g v_1).$$

□

Definition 12.15. Fix a decomposition of $U_\infty^{\chi_E}$ as in Lemma 12.14 and define

$$\tilde{U} = U_\infty^{\chi_E}/V_2, \quad \tilde{X} = X_\infty^{\chi_E}/\text{image}(V_2)$$

where image(V_2) denotes the image of V_2 in X_∞ under the Artin map of local class field theory.

Lemma 12.16. (i) $\tilde{X}$ *is a torsion* Λ_{χ_E}*-module with no nonzero pseudo-null submodules.*
(ii) $\operatorname{char}(\tilde{X}) = \operatorname{char}(\tilde{U}/\operatorname{image}(\mathcal{C}_\infty^{\chi_E}))$

Proof. Since $\mathcal{E}_\infty \not\subset V_2$ and V_2 is free, (i) follows from Proposition 11.3. Also, the exact sequence (13) induces an exact sequence

$$0 \to \mathcal{E}_\infty^{\chi_E}/\mathcal{C}_\infty^{\chi_E} \to \tilde{U}/\operatorname{image}(\mathcal{C}_\infty^{\chi_E}) \to \tilde{X} \to A_\infty^{\chi_E} \to 0.$$

so (ii) follows from Corollary 11.8. □

Proposition 12.17. $\mathcal{S}_{\mathfrak{p}^\infty} = \operatorname{Hom}(\tilde{X}, E[\mathfrak{p}^\infty])^\Gamma$

Proof. By our choice of V_1 and V_2 (Proposition 12.14), we see that $\ker(\delta_\infty) = \mathcal{A}_E V_1 + V_2$. Thus

$$\tilde{X}/\mathcal{A}_E\tilde{X} = X_\infty/(\mathcal{A}_E X_\infty + \operatorname{image}(V_2)) = X_\infty/(\mathcal{A}_E X_\infty + \operatorname{image}(\ker(\delta_\infty)))$$

and so by Proposition 12.2(ii)

$$\mathcal{S}_{\mathfrak{p}^\infty} = \operatorname{Hom}(X_\infty/(\mathcal{A}_E X_\infty + \operatorname{image}(\ker(\delta_\infty))), E[\mathfrak{p}^\infty]) = \operatorname{Hom}(\tilde{X}, E[\mathfrak{p}^\infty])^\Gamma.$$

□

Proposition 12.18. *Suppose M is a finitely-generated torsion Λ_{χ_E}-module and F is a $\mathbf{Z}_p$-extension of K_1 in K_∞ satisfying*

(i) *M has no nonzero pseudo-null submodules,*
(ii) *If γ generates* $\operatorname{Gal}(K_\infty/F)$ *then char*$(M) \not\subset (\gamma - 1)\Lambda_{\chi_E}$*, char*$(M) \not\subset (\gamma - \rho_E(\gamma))\Lambda_{\chi_E}$*, and $M/(\gamma-1)M$ has no nonzero finite submodules.*

Then

$$\#(\operatorname{Hom}(M, E[\mathfrak{p}^\infty])^\Gamma) = [\mathcal{O}_\mathfrak{p} : \rho_E(\operatorname{char}(M))].$$

Proof (sketch). For a complete proof see [Ru2], Lemmas 6.2 and 11.15.

Let $\hat{T}_\pi = \operatorname{Hom}(T_\pi, \mathcal{O}_\mathfrak{p})$, let $\Lambda_F = \mathbf{Z}_p[[\operatorname{Gal}(F/K)]]$, and let $\bar{M}$ denote the $\Lambda_F^{\chi_E}$-module $(M \otimes \hat{T}_\pi)/(\gamma-1)(M \otimes \hat{T}_\pi)$. Using the hypotheses on M and F it is not difficult to show (see [Ru2] Lemma 11.15) that $\bar{M}$ has no nonzero finite submodules. Therefore exactly as in Proposition 12.7,

$$\begin{aligned}\#(\operatorname{Hom}(M, E[\mathfrak{p}^\infty])^\Gamma) &= \#(\operatorname{Hom}(M \otimes \hat{T}_\pi, \mathcal{O}_\mathfrak{p})^\Gamma)\\ &= \#(\operatorname{Hom}(\bar{M}, \mathcal{O}_\mathfrak{p})^{\operatorname{Gal}(F/K)})\\ &= [\mathcal{O}_\mathfrak{p} : \mathbb{1}(\operatorname{char}_F(\bar{M}))]\end{aligned}$$

where $\mathbb{1}$ denotes the trivial character and $\operatorname{char}_F(\bar{M})$ is the characteristic ideal of $\bar{M}$ as a $\Lambda_F^{\chi_E}$-module.

By an argument similar to the proof of Proposition 12.7, one can show that $\operatorname{char}_F(\bar{M}) = \operatorname{char}(M \otimes \hat{T}_\pi)\Lambda_F^{\chi_E}$. Therefore

$$\#(\operatorname{Hom}(M, E[\mathfrak{p}^\infty])^\Gamma) = [\mathcal{O}_\mathfrak{p} : \mathbb{1}(\operatorname{char}(M \otimes \hat{T}_\pi))] = [\mathcal{O}_\mathfrak{p} : \rho_E(\operatorname{char}(M))].$$

□

Theorem 12.19. *Suppose* $\mathfrak{p} \nmid \mathfrak{f}$, $p > 7$, *and* $K_{\mathfrak{p}} \neq \mathbf{Q}_p$.

(i) *If* $L(\bar{\psi}, 1) = 0$ *then* $\mathcal{S}_{\mathfrak{p}^\infty}$ *is infinite.*
(ii) *If* $L(\bar{\psi}, 1) \neq 0$ *then*

$$\#(\text{Ш}(E)_{\mathfrak{p}^\infty}) = [\mathcal{O}_{\mathfrak{p}} : (L(\bar{\psi}, 1)/\Omega)\mathcal{O}_{\mathfrak{p}}].$$

Proof. Lemma 12.16(i) shows that $\tilde{X}$ satisfies the first hypothesis of Proposition 12.18, and the same argument with K_∞ replaced by F verifies the second hypothesis for all but finitely many choices of F. Also, $\tilde{U}/\text{image}(\mathcal{C}_\infty^{\chi_E})$ satisfies the hypotheses of Proposition 12.18 since it is a quotient of one free Λ_{χ_E}-module by another (Proposition 11.6). Therefore by Proposition 12.18 and Lemma 12.16(ii),

$$\#(\text{Hom}(\tilde{X}, E[\mathfrak{p}^\infty])^\Gamma) = \#(\text{Hom}(\tilde{U}/\text{image}(\mathcal{C}_\infty^{\chi_E}), E[\mathfrak{p}^\infty])^\Gamma).$$

The left-hand side of this equality is $\#(\mathcal{S}_{\mathfrak{p}^\infty})$ by Proposition 12.17. On the other hand,

$$\text{Hom}(\tilde{U}/\text{image}(\mathcal{C}_\infty^{\chi_E}), E[\mathfrak{p}^\infty])^\Gamma = \text{Hom}(\tilde{U}/(\text{image}(\mathcal{C}_\infty^{\chi_E} + \mathcal{A}_E\tilde{U})), E[\mathfrak{p}^\infty]),$$

and $\delta_\infty : \tilde{U}/\mathcal{A}_E\tilde{U} \to T_\pi(E)$ is an isomorphism (Lemmas 6.8 and 12.14). Therefore

$$\#(\text{Hom}(\tilde{U}/\text{image}(\mathcal{C}_\infty^{\chi_E}), E[\mathfrak{p}^\infty])^\Gamma) = \#(T_\pi/\delta_\infty(\mathcal{C}_\infty))$$

and the Theorem follows from Wiles' explicit reciprocity law (Corollary 12.4) and (18). □

12.3 Example

We conclude with one example. Let E be the elliptic curve $y^2 = x^3 - x$. The map $(x, y) \mapsto (-x, iy)$ is an automorphism of order 4 defined over $K = \mathbf{Q}(i)$, so $\text{End}_K(E) = \mathbf{Z}[i]$. Let $\mathfrak{p}_2$ denote the prime $(1 + i)$ above 2.

Clearly $E(\mathbf{Q})_{\text{tors}} \supset E[2] = \{O, (0, 0), (1, 0), (-1, 0)\}$. With a bit more effort one checks that $E(K)$ contains the point $(-i, 1 + i)$ of order $\mathfrak{p}_2^3$, and using the Theorem of Nagell and Lutz ([Si] Corollary VIII.7.2) or Corollary 5.18 one can show that in fact $E(K)_{\text{tors}} = E[\mathfrak{p}_2^3]$.

The discriminant of E is 64, so E has good reduction at all primes of K different from $\mathfrak{p}_2$. Since $E[\mathfrak{p}_2^3] \subset E(K)$, if we write ψ_E for the Hecke character of K attached to E, Corollary 5.16 shows that $\psi_E(\mathfrak{a}) \equiv 1 \pmod{\mathfrak{p}_2^3}$ for every ideal $\mathfrak{a}$ prime to $\mathfrak{p}_2$. But every such ideal has a *unique* generator congruent to 1 modulo $\mathfrak{p}_2^3$, so this characterizes ψ_E and shows that its conductor is $\mathfrak{p}_2^3$.

Standard computational techniques now show that

$$L(\bar{\psi}, 1) = .6555143885...$$
$$\Omega = 2.622057554...$$

Therefore by the Coates-Wiles theorem (Theorem 10.1), $E(K) = E[\mathfrak{p}_2^3]$ and $E(\mathbf{Q}) = E[2]$. Further, $L(\bar{\psi}, 1)/\Omega$ is approximately $1/4$. By Proposition 10.6 $L(\bar{\psi}, 1)/\Omega$ is integral at all primes $\mathfrak{p}$ of residue characteristic greater than 7. In fact the same techniques show that $L(\bar{\psi}, 1)/\Omega$ is integral at all primes $\mathfrak{p} \neq \mathfrak{p}_2$, and give a bound on the denominator at $\mathfrak{p}_2$ from which we can conclude that $L(\bar{\psi}, 1)/\Omega = 1/4$.

Therefore by Corollary 12.13 and Theorem 12.19, $\mathcal{S}_{\mathfrak{p}^\infty} = Ш(E_{/K})_{\mathfrak{p}^\infty} = 0$ for all primes $\mathfrak{p}$ of residue characteristic greater than 7, and again the same proof works for all $\mathfrak{p} \neq \mathfrak{p}_2$. It follows easily from this that $Ш(E_{/\mathbf{Q}})_p = 0$ for all odd rational primes. Fermat did the 2-descent necessary to show that $Ш(E_{/\mathbf{Q}})_2 = 0$ (see [We] Chap. II), so in fact $Ш(E_{/\mathbf{Q}}) = 0$. Together with the fact that the Tamagawa factor at 2 is equal to 4, this shows that the full Birch and Swinnerton-Dyer conjecture holds for E over $\mathbf{Q}$.

References

[Ca] Cassels, J.W.S., Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* **41** (1966) 193–291.

[Co] Coates, J., Infinite descent on elliptic curves with complex multiplication. In: Arithmetic and Geometry, M. Artin and J. Tate, eds., *Prog. in Math.* **35**, Boston: Birkhäuser (1983) 107–137.

[CW1] Coates, J., Wiles, A., On the conjecture of Birch and Swinnerton-Dyer, *Inventiones math.* **39** (1977) 223–251.

[CW2] Coates, J., Wiles, A., On p-adic L-functions and elliptic units, *J. Austral. Math. Soc. (ser. A)* **26** (1978) 1–25.

[Col] Coleman, R., Division values in local fields, *Inventiones math.* **53** (1979) 91–116.

[dS] de Shalit, E., Iwasawa theory of elliptic curves with complex multiplication, *Perspectives in Math.* **3**, Orlando: Academic Press (1987).

[GS] Goldstein, C., Schappacher, N., Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe, *J. für die reine und angew. Math.* **327** (1981) 184–218

[Gr] Greenberg, R., On the structure of certain Galois groups, *Inventiones math.* **47** (1978) 85–99.

[Iw] Iwasawa, K., On $\mathbf{Z}_\ell$-extensions of algebraic number fields, *Annals of Math.* (2) **98** (1973) 246–326.

[Ko] Kolyvagin, V. A., Euler systems. In: The Grothendieck Festschrift (Vol. II), P. Cartier et al., eds., *Prog. in Math* **87**, Boston: Birkhäuser (1990) 435–483.

[La] Lang, S., Elliptic Functions, Reading: Addison Wesley (1973)

[PR] Perrin-Riou, B., Arithmétique des courbes elliptiques et théorie d'Iwasawa, *Bull. Soc. Math. France, Mémoire* Nouvelle série **17** 1984.

[Ro] Robert, G., Unités elliptiques, *Bull. Soc. Math. France, Mémoire* **36** (1973).

[Ru1] Rubin, K., The main conjecture. Appendix to: Cyclotomic fields I and II, S. Lang, *Graduate Texts in Math.* **121**, New York: Springer-Verlag (1990) 397–419.

[Ru2] Rubin, K., The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Inventiones Math.* **103** (1991) 25–68.

[Se] Serre, J-P., Classes des corps cyclotomiques (d'après K. Iwasawa), Séminaire Bourbaki exposé 174, December 1958. In: Séminaire Bourbaki vol. 5, Paris: Société de France (1995) 83–93.

[ST] Serre, J-P., Tate, J., Good reduction of abelian varieties, *Ann. of Math.* **88** (1968) 492–517.

[Sh] Shimura, G., Introduction to the arithmetic theory of automorphic functions, Princeton: Princeton Univ. Press (1971).

[Si] Silverman, J., The arithmetic of elliptic curves, *Graduate Texts in Math.* **106**, New York: Springer-Verlag (1986).

[Ta] Tate, J., Algorithm for determining the type of a singular fiber in an elliptic pencil. In: Modular functions of one variable IV, *Lecture Notes in Math.* **476**, New York: Springer-Verlag (1975) 33–52.

[We] Weil, A., Number theory. An approach through history. From Hammurapi to Legendre, Boston: Birkhäuser (1984).

[Wil] Wiles, A., Higher explicit reciprocity laws, *Annals of Math.* **107** (1978) 235–254.

[Win] Wintenberger, J-P., Structure galoisienne de limites projectives d'unités locales, *Comp. Math.* **42** (1981) 89–103.