On the main conjectures of Iwasawa theory for certain elliptic curves with complex multiplication

Yukako Kezuka

Department of Pure Mathematics and Mathematical Statistics
University of Cambridge

This dissertation is submitted for the degree of
Doctor of Philosophy

Churchill College September 2016

Declaration

I hereby declare that this dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text. No part of this material has ever been submitted for any other qualification.

Yukako Kezuka
September 2016

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my supervisor, Professor John Coates, for suggesting these research topics, providing many relevant sources of information and for patiently advising and encouraging me. He has been a true mentor and a role model both academically and personally, and I have been extremely fortunate to work under his guidance. His vision, expertise and enthusiasm helped me overcome countless difficulties over the course of my doctoral studies.

I am also very grateful to Jack Lamplugh for many insightful discussions, and for sharing his mathematical experience.

Finally, I would like to thank K. Buzzard, T. Fisher, J. Choi, Y. Hachimori and S. Zhai for giving me many helpful comments on my work.

Abstract

The conjecture of Birch and Swinnerton-Dyer is unquestionably one of the most important open problems in number theory today. Let E be an elliptic curve defined over an imaginary quadratic field K contained in $\mathbb{C}$, and suppose that E has complex multiplication by the ring of integers of K. Let us assume the complex L-series $L(E/K, s)$ of E over K does not vanish at $s = 1$. K. Rubin showed, using Iwasawa theory, that the p-part of Birch and Swinnerton-Dyer conjecture holds for E for all prime numbers p which do not divide the order of the group of roots of unity in K. In this thesis, we discuss extensions of this result.

In Chapter 2, we study infinite families of quadratic and cubic twists of the elliptic curve $A = X_0(27)$, so that they have complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$. For the family of quadratic twists, we establish a lower bound for the 2-adic valuation of the algebraic part of the complex L-series at $s = 1$, and, for the family of cubic twists, we establish a lower bound for the 3-adic valuation of the algebraic part of the same L-value. We show that our lower bounds are precisely those predicted by Birch and Swinnerton-Dyer.

In the remaining chapters, we let $K = \mathbb{Q}(\sqrt{-q})$, where q is any prime number congruent to 7 modulo 8. Denote by H the Hilbert class field of K. B. Gross proved the existence of an elliptic curve $A(q)$ defined over H with complex multiplication by the ring of integers of K and minimal discriminant $-q^3$. We consider twists E of $A(q)$ by quadratic extensions of K. In the case $q = 7$, we have $A(q) = X_0(49)$, and Gonzalez-Aviles and Rubin proved, again using Iwasawa theory, that if $L(E/\mathbb{Q}, 1)$ is nonzero then the full Birch–Swinnerton-Dyer conjecture holds for E. Suppose p is a prime number which splits in K, say $p = \mathfrak{p}\mathfrak{p}^*$, and E has good reduction at all primes of H above p. Let $H_\infty = HK_\infty$, where K_∞ is the unique $\mathbb{Z}_p$-extension of K unramified outside $\mathfrak{p}$. We establish in this thesis the main conjecture for the extension H_∞/H. Furthermore, we provide the necessary ingredients to state and prove the main conjecture for E/H and p, and discuss its relation to the main conjecture for H_∞/H and the p-part of the Birch–Swinnerton-Dyer conjecture for E/H.

Table of contents

Chapter 1

Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $L(E,s)$ denote its complex L-series. We assume that $L(E,1) \neq 0$. Then, by a well-known theorem of Kolyvagin and Gross–Zagier [15, 12], both $E(\mathbb{Q})$ and the Tate–Shafarevich group $\text{Ш}(E)$ of E over $\mathbb{Q}$ are finite. Define

$$L^{(\mathrm{alg})}(E,1) = \frac{L(E,1)}{c_\infty \Omega},$$

where c_∞ denotes the number of connected real components of $E(\mathbb{R})$, and Ω is the least positive real period of the Néron differential of any global Weierstrass minimal equation for E. It is well-known that $L^{(\mathrm{alg})}(E,1)$ is a rational number. For a prime q of bad reduction for E, define

$$c_q = [E(\mathbb{Q}_q) : E^0(\mathbb{Q}_q)],$$

where $E^0(\mathbb{Q}_q)$ denotes the subgroup of $E(\mathbb{Q}_q)$ consisting of all points with non-singular reduction modulo q. The Birch–Swinnerton-Dyer conjecture for E asserts that:

Conjecture 1.0.1.

$$L^{(alg)}(E,1) = \frac{\#(\text{Ш}(E)) \prod_{q\ bad} c_q}{\#(E(\mathbb{Q}))^2}. \tag{1.0.1}$$

Since both sides of (1.0.1) are rational numbers, Conjecture 1.0.1 clearly implies that:

Conjecture 1.0.2. *For each prime number p, we have*

$$\mathrm{ord}_p\left(L^{(alg)}(E,1)\right) = \mathrm{ord}_p\left(\frac{\#(\text{Ш}(E)(p))}{\#(E(\mathbb{Q})(p))^2}\right) + \mathrm{ord}_p\left(\prod_{q\ bad} c_q\right). \tag{1.0.2}$$

When E has complex multiplication, Rubin establishes (1.0.2) in [17, Theorem 11.1] for all primes p which do not divide the order w of the group of roots of unity in the field of complex multiplication. However, these methods at present seem very difficult to apply for primes p which divide w, except when E has potential ordinary reduction at such a prime p. The most interesting case in which to make progress is when E runs over the family of twists of some fixed curve A. In Chapters 3–7, we study infinite families of quadratic twists of certain elliptic curves with complex multiplication which are no longer defined over $\mathbb{Q}$, using methods of Iwasawa theory.

Chapter 2 is independent of the rest of the chapters, but we prove results of a similar nature using techniques which are more elementary. We study the quadratic and cubic twists of the curve

$$E = X_0(27): \; Y^2 + Y = X^3 - 7 \tag{1.0.3}$$

which has conductor 27 and admits complex multiplication by the full ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega = \frac{-1+\sqrt{-3}}{2}$, of the field $K = \mathbb{Q}(\sqrt{-3})$. The associated classical Weierstrass equation is

$$E : y^2 = 4x^3 - 3^3,$$

which we obtain by the change of variables

$$\begin{aligned} x &= X \\ y &= 2Y + 1. \end{aligned}$$

Note that $c_\infty = 1$ for E, so that $L^{(\mathrm{alg})}(E,1) = \frac{L(E,1)}{\Omega}$. It is easily shown that $L^{(\mathrm{alg})}(E,1) = \frac{1}{3}$. On the other hand, classical descent theory proves that $E(\mathbb{Q}) = \{\mathcal{O}, (3, \pm 3^2)\} \cong \mathbb{Z}/3\mathbb{Z}$ and $\text{Ш}(E)(2) = \text{Ш}(E)(3) = 0$. Combining this with [17, Theorem 11.1], we conclude that Conjecture 1.0.1 is valid for E.

Given an integer $\lambda > 1$, let $E(\lambda)$ denote the elliptic curve

$$E(\lambda) : y^2 = 4x^3 - 3^3\lambda.$$

First, we consider the case when $\lambda = D^3$, for a square-free positive integer D, so that $E(D^3)$ is the twist of E by the quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$. We define a rational prime number p to be a *special split* prime for E if it splits completely in the field $K(x(E[4]))$, the field obtained by adjoining to K the x-coordinates of all non-zero points in $E[4]$, the group of 4-division points on E. In fact, we have that $K(x(E[4])) = K(\boldsymbol{\mu}_4, \sqrt[3]{2})$. Moreover, the theory of complex multiplication provides the following alternative description of the set of special split primes. Let ψ denote the Grössencharacter of E over K. Then a prime p is special split if and only if it splits in K, and $\psi(\mathfrak{p}) \equiv \pm 1 \bmod 4$ for both of the primes $\mathfrak{p}$ of K above p (see Lemma A.1 of Appendix A). In Section 2.2, we prove:

Theorem 1.0.3. *Let $D > 1$ be an integer which is a square-free product of special split primes. Then*

$$\mathrm{ord}_2\left(L^{(alg)}\left(E(D^3), 1\right)\right) \geqslant 2k(D),$$

where $k(D)$ is the number of prime factors of D.

This bound is sharp, as we will see in Remark 2.2.15. Some numerical examples are listed in Appendix B. We show in Section 2.1, using Tate's algorithm, that

$$\mathrm{ord}_2\left(\frac{\prod\limits_{q \text{ bad}} c_q}{\#(E(D^3)(\mathbb{Q}))^2}\right) = 2k(D).$$

Hence the 2-part of the Birch–Swinnerton-Dyer conjecture predicts that if $L(E(D^3), 1) \neq 0$, then

$$\mathrm{ord}_2\left(L^{(\mathrm{alg})}(E(D^3), 1)\right) = 2k(D) + \mathrm{ord}_2\left(\#\text{Ш}(E(D^3))\right).$$

In particular, it predicts that equality occurs in the lower bound of Theorem 2.2.14 if and only if $\mathrm{ord}_2\left(\#\text{Ш}\left(E(D^3)\right)\right) = 0$.

Next consider the case when $\lambda = D^2$ for a cube-free positive integer D, so that $E(D^2)$ is a cubic twist of E. We say a prime number p is *cubic-special* if it splits completely in the field $K(E[27])$, but does not split completely in the strictly larger field $K(E[27])((1-\omega)^{1/9})$, where ω denotes a non-trivial cube root of unity. We then prove in Section 2.3:-

Theorem 1.0.4. *Let $D > 1$ be an integer which is a cube-free product of cubic-special primes. Then*

$$\mathrm{ord}_3\left(L^{(alg)}\left(E(D^2), 1\right)\right) \geqslant k(D) + 1,$$

where $k(D)$ is the number of distinct prime factors of D.

Numerical examples show that this lower bound is sometimes sharp. In fact, the Birch–Swinnerton-Dyer conjecture predicts that the lower bound of this theorem holds for all odd cube free positive integers D with $D \equiv 1 \bmod 9$ whose prime factors are congruent to 1 modulo 3. Indeed, using Tate's algorithm, it can be shown (see Section

2.1) that, for all such D, we have

$$\mathrm{ord}_3\left(\frac{\prod\limits_{q \text{ bad}} c_q}{\#(E(D^2)(\mathbb{Q}))^2}\right) = k(D) + 1.$$

Hence the 3-part of the Birch–Swinnerton-Dyer conjecture predicts that if $L(E(D^2), 1) \neq 0$, we have

$$\mathrm{ord}_3\left(L^{(\mathrm{alg})}(E(D^2), 1)\right) = k(D) + 1 + \mathrm{ord}_3\left(\#\text{Ш}(E(D^2))\right).$$

In particular, it predicts that equality is attained in the theorem above if and only if $\mathrm{ord}_3\left(\#\text{Ш}\left(E(D^2)\right)\right) = 0$. We will prove these theorems by first expressing the value of the complex L-series as a sum of Eisenstein series, and then combining an averaging argument over quadratic or cubic twists with an induction on the number of distinct primes divisors. In the case of quadratic twists, this method is essentially due to Zhao [24, 25] who established similar results for the congruent number curves with respect to the prime $p = 2$. In Section 2.3, we will generalise his ideas in order to apply to the cubic twists of E with respect to the prime $p = 3$.

In Chapters 3–7, we let $K = \mathbb{Q}(\sqrt{-q})$, where q is a prime congruent to 7 modulo 8. Then the discriminant of K is equal to $-q$, so the class number h of K is odd by genus theory. We fix an embedding of K into $\mathbb{C}$. Let $\mathcal{O}$ denote the ring of integers of K, and let $H = K(j(\mathcal{O}))$ be the Hilbert class of K where $j(\mathcal{O})$ denotes the complex modular invariant of the curve $\mathbb{C}/\mathcal{O}$. In fact, $j(\mathcal{O})$ is a real number, so the field $J = \mathbb{Q}(j(\mathcal{O}))$ has index 2 in H and is embedded in $\mathbb{R}$. In [13], Gross proved the existence of an elliptic curve $A(q)$ defined over J with complex multiplication by $\mathcal{O}$ and minimal discriminant $-q^3$. In the case $q = 7$,

$$A(7) = X_0(49) : y^2 + xy = x^3 - x^2 - 2x - 1$$

is defined over $\mathbb{Q}$ because $\mathbb{Q}(\sqrt{-7})$ has class number one. The following result was proved by Gonzalez-Aviles and Rubin using Iwasawa theory.

Theorem 1.0.5. *[Gonzalez-Aviles–Rubin] Let E be a quadratic twist of $X_0(49)$, so that it has complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-7})$. If $L(E, 1) \neq 0$, then the full Birch–Swinnerton-Dyer conjecture is valid for E.*

We discuss an extension of this theorem. Let E be any quadratic twist of $A(q)$ by a quadratic extension of the form $H(\sqrt{\lambda})/H$ of discriminant prime to $2q$, $\lambda \in K^\times$. From Chapter 3, p will denote a prime such that E has good reduction at all places of H

above p, and p splits in K, say $p = \mathfrak{p}\mathfrak{p}^*$. In particular, $p = 2$ satisfies these conditions. Let $F_n = H(E_{\mathfrak{p}^n})$, and $F = F_1$ or F_2, according as $p > 2$ or $p = 2$. Set

$$F_\infty = H(E_{\mathfrak{p}^\infty}), \quad \mathfrak{H} = \mathrm{Gal}(F_\infty/H).$$

Let $\mathcal{O}_\mathfrak{p}$ be the ring of integers of $K_\mathfrak{p} = \mathbb{Q}_p$. We have, via an argument which involves relative Lubin–Tate groups, a canonical isomorphism $\chi_\mathfrak{p} : \mathfrak{H} \to \mathcal{O}_\mathfrak{p}^\times$ given by the action of $\mathfrak{H}$ on $E_{\mathfrak{p}^\infty}$, and

$$\mathfrak{H} = \Delta \times \Gamma,$$

where Δ is cyclic of order $p - 1$ or 2 according as $p > 2$ or $p = 2$, and Γ is isomorphic to $\mathcal{O}_\mathfrak{p}$.

In Chapter 3, we study the $\mathfrak{p}^\infty$-Selmer groups $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/H)$ and $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F)$ of E over H and F respectively, and show how their orders are related to the order of $\text{Ш}(E/H)(\mathfrak{p})$. We also introduce the Selmer group $\mathrm{Sel}(E/F_\infty)$ of E over F_∞, which is closely related to Iwasawa modules, as shown in more detail in Chapter 7. Then in Chapter 4, we construct the $\mathfrak{p}$-adic L-functions attached to E/H, which will be needed to formulate the main conjectures. Let $\psi_{E/H}$ denote the Grössencharacter of E/H. We show in Chapter 3 that

$$\psi_{E/H} = \varphi_K \circ \mathrm{N}_{H/K},$$

where φ_K is a Grössencharacter of K of conductor $\mathfrak{g}$, say. Let $\mathscr{I}$ be the ring of integers of the completion of the maximal unramified extension $K_\mathfrak{p}^{\mathrm{ur}}$ of $K_\mathfrak{p}$. Then we show in Section 4.1 that there exists a natural $\mathfrak{p}$-adic analogue $\Omega_\mathfrak{p}(E/H) \in \mathscr{I}^\times$ of the complex period $\Omega_\infty(E/H)$, and

Theorem 1.0.6. *There exists a unique $\mathscr{I}$-valued measure μ_E on the Galois group $\mathfrak{G}$ of F_∞ over K such that for all integers $k \geqslant 1$ with $k \equiv 1 \bmod \#(\Delta)$, we have*

$$\Omega_\mathfrak{p}(E/H)^{-k} \int_\mathfrak{G} \chi_\mathfrak{p}^k d\mu_E = \left((k-1)!\right)^h f^{kh} \Omega_\infty(E/H)^{-k} L(\overline{\psi}_{E/H}^k, k) \prod_{v|\mathfrak{p}} \left(1 - \frac{\psi_{E/H}^k(v)}{\mathrm{N}v}\right),$$

where the product runs over the primes v of H which lie above $\mathfrak{p}$, and f is a fixed generator of the principal ideal $\mathfrak{f} = \mathfrak{g}^h$.

See Section 4.1 for a more detailed account of the notations used. The measure μ_E will be used in Chapter 7 to state the main conjectures attached to E/H. In this thesis, however, we shall concentrate on the proof the main conjecture for the extension H_∞/H, where $H_\infty = HK_\infty$ and K_∞ is the unique $\mathbb{Z}_p$-extension of K unramified outside $\mathfrak{p}$.

In order to state the main conjecture for H_∞/H, let $\mathscr{G} = \mathrm{Gal}(H_\infty/K)$ and assume $(p,h)=1$. Let $\Gamma = \mathrm{Gal}(K_\infty/K)$, $G = \mathrm{Gal}(H_\infty/K_\infty)$. We fix an identification

$$\mathscr{G} = G \times \Gamma$$

so that characters of G can naturally be considered as characters of $\mathscr{G}$. Given a $\mathscr{I}[[\mathscr{G}]]$-module M and $\chi \in G^* = \mathrm{Hom}(G, \mathbb{C}_p^\times)$, write M^χ for the largest submodule of M on which G acts via χ. Since $p \nmid [H:K]$ by assumption, we have

$$\mathscr{I}[[\mathscr{G}]] = \oplus_\chi e_\chi \mathscr{I}[[\Gamma]]$$

where e_χ is the idempotent corresponding to χ, and any $\mathscr{I}[[\mathscr{G}]]$-module breaks up into the direct sum of its χ-components. Fix a topological generator of Γ, and identify $\mathscr{I}[[\Gamma]]$ with the ring $\mathscr{I}[[T]]$ of formal power series in the variable T with coefficients in $\mathscr{I}$ via the map sending γ to $1+T$. We prove the following in Section 4.2.

Theorem 1.0.7. *There exists a unique $\mathscr{I}$-valued pseudo-measure $\nu_\mathfrak{p}$ on $\mathscr{G}$ such that for all integers $k \geqslant 1$ with $k \equiv 0 \bmod \#(\Delta)$, we have*

$$\Omega_\mathfrak{p}(E/H)^{-k} \int_\mathscr{G} \chi_\mathfrak{p}^k d\nu_\mathfrak{p} = ((k-1)!)^h \, \Omega_\infty(E/H)^{-k} L(\overline{\psi}_{E/H}^k, k) \prod_{v|\mathfrak{p}} \left(1 - \frac{\psi_{E/H}^k(v)}{\mathrm{N}v}\right),$$

where the product runs over the primes v of H which lie above $\mathfrak{p}$. Furthermore, we have $\nu_\mathfrak{p}^\chi \in \mathscr{I}[[T]]$ if $\chi \in G^*$ is non-trivial, and $\nu_\mathfrak{p}^\chi \in \mathscr{I}[[T]]/T$ if χ is the trivial character.

Define $\boldsymbol{\varphi} = I(\mathscr{G})\nu_\mathfrak{p}$, where $I(\mathscr{G})$ denotes the augmentation ideal of $\mathscr{I}[[\mathscr{G}]]$, and let $\boldsymbol{\varphi}^\chi = (I(\mathscr{G})\nu_\mathfrak{p})^\chi \subset \mathscr{I}[[T]]$. We will show in Lemma 4.4.2 that $\boldsymbol{\varphi}$ is independent of E.

If M is a finitely generated torsion $\mathscr{I}[[\mathscr{G}]]$-module, we write $\mathrm{char}\,(M)^\chi$ for the characteristic ideal of the $\mathscr{I}[[\Gamma]]$-module M^χ given by the structure theory. Denote by $M(H_\infty)$ the maximal abelian p-extension of H_∞ unramified outside the primes above $\mathfrak{p}$, and write

$$X(H_\infty) = \mathrm{Gal}(M(H_\infty)/H_\infty).$$

Then $X(H_\infty)$ is a finitely generated torsion $\mathscr{I}[[\mathscr{G}]]$-module, and

Theorem 1.0.8 (Main Conjecture for H_∞/H)**.** *For every $\chi \in G^*$, we have*

$$\mathrm{char}\,(X(H_\infty))^\chi = \boldsymbol{\varphi}^\chi$$

For every $n \geqslant 0$, define $H_n = F_n \cap H_\infty$. Write $\mathcal{E}_{H_n}$ for the group of global units of H_n, and U_{H_n} for the group of semi-local units of $H_n \otimes_K K_\mathfrak{p} = \oplus_{\mathfrak{P}|\mathfrak{p}} H_{n,\mathfrak{P}}$ which are congruent to 1 modulo the primes above $\mathfrak{p}$. Let $\bar{\mathcal{E}}_{H_n}$ be the closure of $\mathcal{E}_{H_n} \cap U_{H_n}$ in U_{H_n} in the p-adic topology, and define

$$\bar{\mathcal{E}}_{H_\infty} = \varprojlim \bar{\mathcal{E}}_{H_n} \text{ and } U_{H_\infty} = \varprojlim U_{H_n},$$

where the inverse limits are taken with respect to the norm maps. Let $A(H_n)$ denote the p-primary part of the ideal class group of H_n, and write $A(H_\infty)$ for the projective limit of $A(H_n)$ with respect to the norm maps. Let $\bar{\mathcal{C}}_{H_\infty}$ be the group of elliptic units defined in Section 4.3. Global class field theory provides an exact sequence of $\mathbb{Z}_p[[\mathscr{G}]]$-modules

$$0 \to \bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty} \to U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty} \to X(H_\infty) \to A(H_\infty) \to 0. \tag{1.0.4}$$

We prove in Chapter 4 that

$$\operatorname{char}\left(U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}\right)^\chi = \boldsymbol{\varphi}^\chi$$

for every $\chi \in G^*$. In Chapter 5, we construct an Euler system of the elliptic units $\bar{\mathcal{C}}_{H_\infty}$, and use a variant of Čebotarev's theorem and induction to establish a divisibility relation between the characteristic ideal of $\left(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}\right)^\chi$ and that of $A(H_\infty)^\chi$ in $\mathbb{Z}_p[[\Gamma]]$. Since the characteristic ideals of a Γ-module behave well under extension of scalars, this implies the following divisibility relation in $\mathscr{I}[[\Gamma]]$:

Theorem 1.0.9. *For some integer $k \geqslant 0$,*

$$\operatorname{char}(X(H_\infty))^\chi \mid \boldsymbol{\pi}^{ke}\operatorname{char}\left(U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}\right)^\chi$$

where $\boldsymbol{\pi}$ is a uniformiser of $\mathscr{I}$, and $e = 0$ or 1 according as $p > 2$ or $p = 2$.

In Chapter 6, we finish the proof of the main conjecture by showing that $X(H_\infty)$ and $U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}$ have the same Iwasawa invariants. We first follow the paper of Coates and Wiles [6] to compute the Iwasawa invariants of $X(H_\infty)$, and then compute the Iwasawa invariants of $U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}$ using the analytic class number formula. In Chapter 7, we briefly discuss the main conjectures attached to E/H, how they relate to the main conjecture for H_∞/H and the p-part of the Birch–Swinnerton-Dyer conjecture.

Finally, all numerical examples in this paper are computed using the computer package Magma.

Chapter 2

On the p-part of the Birch–Swinnerton-Dyer conjecture for elliptic curves with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$

2.1 The p-part of the Birch–Swinnerton-Dyer Conjecture.

Let $\lambda > 1$ be an integer and define $E(\lambda) : y^2 = 4x^3 - 3^3\lambda$. Let us assume that $L\left(E(\lambda), 1\right) \neq 0$, so that $E(\lambda)(\mathbb{Q})$ and $Ш\left(E(\lambda)\right)$ are finite. Let $\omega = \frac{-1+\sqrt{-3}}{2}$, a cube root of unity. In this short section, we will compute the Tamagawa factors c_q for the primes q of bad reduction for $E(\lambda)$, and $\mathrm{ord}_p(E(\lambda)(\mathbb{Q}))$ for $p = 2$ or 3 according as $E(\lambda)$ is a quadratic or cubic twist of $E = X_0(27)$.

First, we consider the case when $\lambda = D^3$, for $D > 1$ a square-free integer, so that $E(D^3)$ is a quadratic twist of E. The primes of bad reduction for $E(D^3)$ are 3 and the primes dividing D, since the discriminant of $E(D^3)$ is $-27D^6$.

Lemma 2.1.1. *Let $D > 1$ be a square-free product of primes coprime to 6 which split in $\mathbb{Q}(\omega, \sqrt[3]{2})$. Then*

$$\mathrm{ord}_2\left(\frac{\prod\limits_{q\ bad} c_q}{\#(E(D^3)(\mathbb{Q}))^2}\right) = 2k(D),$$

where $k(D)$ denotes the number of prime factors of D.

Proof. We will work with the form $y^2 = x^3 - 2^4 3^3 D^3$ which is isomorphic to $E(D^3)$. With the usual notation for Tate's algorithm, we have $a_1 = a_3 = a_2 = a_4 = 0$, $a_6 = -2^4 3^3 D^3$, $b_4 = b_8 = 0$ and $b_6 = -2^6 3^3 D^3$. For a bad prime q, we have $q \mid a_1, a_2$, $q^2 \mid a_3, a_4$ and $q^3 \mid a_6$. Let P_q be the polynomial

$$P_q(T) = T^3 + \frac{a_6}{q^3}.$$

Then for $q = 3$, we have $P_3'(T) = 3T^2 \equiv 0 \bmod 3$ so $P_3(T)$ has a triple root in $\mathbb{Z}/3\mathbb{Z}$. Therefore, $c_3 = 3$ and $\operatorname{ord}_2(c_3) = 0$. If q is a prime factor of D, then $(P_q(T), P_q'(T)) = (T^3 + \frac{a_6}{q^3}, 3T^2) = 1$ in $\mathbb{Z}/q\mathbb{Z}[T]$, since $3 \nmid D$. So $P_q(T)$ has 3 distinct roots in $\mathbb{Z}/q\mathbb{Z}$. Hence, $c_q = 4$ and $\operatorname{ord}_2(c_q) = 2$.

Also, $E(D^3)[2^\infty](\mathbb{Q}) = \{\mathcal{O}\}$ since the equation $4x^3 - 3^3 D^3 = 0$ clearly has no rational solution. □

Thus (1.0.2) indeed predicts

$$\begin{aligned}\operatorname{ord}_2\left(L^{(\mathrm{alg})}\left(E(D^3),1\right)\right) &= \operatorname{ord}_2\left((\text{Ш}\left(E(D^3)\right)[2^\infty]\right) + 2k(D)\\ &\geqslant 2k(D).\end{aligned}$$

Next, we consider the case when $\lambda = D^2$, for $D > 1$ a cube-free integer, so that $E(D^2)$ is a cubic twist of E. We remark that $E(D^2)$ is isomorphic to the curve $x^3 + y^3 = D$ which is a cubic twist of the Fermat curve $x^3 + y^3 = 1$. The primes of bad reduction for $E(D^2)$ are again 3 and the primes dividing D, since the discriminant of $E(D^2)$ is $-27D^4$.

Lemma 2.1.2. *Let $D > 1$ be an odd, cube-free integer such that $D \equiv 1 \bmod 9$ and D is a product of primes congruent to 1 modulo 3. Then*

$$\operatorname{ord}_3\left(\frac{\prod\limits_{q\ bad} c_q}{\#(E(D^2)(\mathbb{Q}))^2}\right) = k(D) + 1,$$

where $k(D)$ is the number of distinct prime factors of D.

Proof. We will work with the form $y^2 = x^3 - 2^4 3^3 D^2$ which is isomorphic to $E(D^2)$. With the usual notation for Tate's algorithm, we have $a_1 = a_3 = a_2 = a_4 = 0$, $a_6 = -2^4 3^3 D^2$, $b_4 = b_8 = 0$ and $b_6 = -2^6 3^3 D^2$. Let q be a prime of bad reduction for E. If q is a prime factor of D, then we have $q \mid a_1, a_2$, $q^2 \mid a_3, a_4$ and $q^3 \nmid a_6$ hence the type is IV (see [22, p. 49]) and $c_q = 3$ or 1. However, the polynomial $T^2 + \frac{2^4 3^3 D^2}{q^2}$ has roots in $\mathbb{Z}/q\mathbb{Z}$ since $\left(\frac{-3}{q}\right) = (-1)^{q-1}\left(\frac{q}{3}\right) = 1$ and so $-\frac{2^4 3^3 D^2}{q^2}$ is a square mod q. It follows that $c_q = 3$ and $\mathrm{ord}_3(c_q) = 1$. Otherwise, $q = 3$ and we have $3 \mid a_1, a_2$, $3^2 \mid a_3, a_4$ and $3^3 \nmid a_6$. Let P_3 be the polynomial

$$P_3(T) = T^3 + \frac{a_6}{3^3}.$$

Then $P_3'(T) = 3T^2 \equiv 0 \bmod 3$ so $P_3(T)$ has a triple root in $\mathbb{Z}/3\mathbb{Z}$. After the change of variables $x = X + 3D$ the triple root is 0, and we have $a_1 = a_3 = 0$, $a_2 = 3^2 D$, $a_4 = 3^3 D^2$, $a_6 = 3^3 D^2 (D - 2^4) \equiv 3 \bmod 9$. So $Y^2 - \frac{a_6}{3^4} = Y^2 - \frac{D^2(D-2^4)}{3} \equiv Y^2 - 1 \equiv 0 \bmod 3$ has distinct roots in $\mathbb{Z}/3\mathbb{Z}$. Hence the type is IV* (see [22, p. 51]) and $c_3 = 3$, so that $\mathrm{ord}_3(c_3) = 1$.

Furthermore, by [20, Exercise 10.19], we have $E(D^2)(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}\}$ for $D > 1$. □

Thus (1.0.2) predicts

$$\begin{aligned}\mathrm{ord}_3\left(L^{(\mathrm{alg})}\left(E(D^2), 1\right)\right) &\geqslant \mathrm{ord}_3\left((\text{Ш}\left(E(D^2)\right)[3^\infty]\right) + k(D) + 1 \\ &\geqslant k(D) + 1.\end{aligned}$$

2.2 Quadratic Twists.

Let $K = \mathbb{Q}(\sqrt{-3})$, and write $\boldsymbol{\mu}_K$ for the group of roots of unity in K. We fix once and for all an embedding of K into $\mathbb{C}$. In general, if λ is a non-zero element of $\mathcal{O}_K$ which is prime to $\#(\boldsymbol{\mu}_K) = 6$, we let $\psi_\lambda := \psi_{E(\lambda)/K}$ be the Grössencharacter of $E(\lambda)$ over K with conductor $\mathfrak{f}$, and let $\mathfrak{g}$ denote some integral multiple of $\mathfrak{f}$. Let S be the set of primes of K dividing $\mathfrak{g}$. We consider the (usually) imprimitive Hecke L-series

$$L_S(\overline{\psi}_\lambda, s) = \sum_{(\mathfrak{a},\mathfrak{g})=1} \frac{\overline{\psi}_\lambda(\mathfrak{a})}{(\mathrm{N}\mathfrak{a})^{\mathrm{s}}}$$

of $\overline{\psi}_\lambda$ (the complex conjugate of ψ_λ). It can be defined by the Euler product

$$L_S(\overline{\psi}_\lambda, s) = \prod_{(v,\mathfrak{g})=1}\left(1 - \frac{\overline{\psi}_\lambda(v)}{(\mathrm{N}v)^s}\right)^{-1},$$

and if we replace $\mathfrak{g}$ by $\mathfrak{f}$ in the definition, we obtain the primitive Hecke L-function $L(\overline{\psi}_\lambda, s)$. In particular, we have

$$L(E(\lambda), 1) = L(\overline{\psi}_\lambda, 1).$$

Recall that for any complex lattice L and $z, s \in \mathbb{C}$, we can define the Kronecker–Eisenstein series

$$H_1(z, s, L) := \sum_{w \in L} \frac{\overline{z} + \overline{w}}{|z + w|^{2s}},$$

where the sum in taken over all $w \in L$, except $-z$ if $z \in L$. This series converges for Re(s) $> \frac{3}{2}$, and it has an analytic continuation to the whole complex s-plane [10, Theorem 1.1]. The non-holomorphic Eisenstein series $\mathcal{E}_1^*(z, L)$ is defined by

$$\mathcal{E}_1^*(z, L) := H_1(z, 1, L).$$

Let $\Omega_\lambda = \frac{\Omega}{\sqrt[6]{\lambda}} \in \mathbb{C}^\times$, where $\sqrt[6]{\lambda}$ denotes the real root and Ω is the least positive real period of the Néron differential of any global Weierstrass minimal equation for E. We write $\mathcal{L}_\lambda$ for the period lattice of the curve $E(\lambda)$ over $\mathbb{C}$, and write $\mathcal{L}$ for that of E.

Since $\mathfrak{g}$ is a multiple of $\mathfrak{f}$, it follows from [7, Lemma 3] that $K(E(\lambda)_\mathfrak{g})$, the extension of K obtained by adjoining the coordinates of all $\mathfrak{g}$-division points of $E(\lambda)$ to K, is isomorphic to $K(\mathfrak{g})$, the ray class field of K modulo $\mathfrak{g}$. We fix, once and for all, a set $\mathcal{B}$ of integral ideals of K prime to $\mathfrak{g}$ such that

$$\mathrm{Gal}(K(\mathfrak{g})/K) = \{\sigma_\mathfrak{b} \ : \ \mathfrak{b} \in \mathcal{B}\},$$

where the Artin symbol $\sigma_\mathfrak{b} = (\mathfrak{b}, K(\mathfrak{g})/K)$ of $\mathfrak{b}$ runs over $\mathrm{Gal}\,(K(\mathfrak{g})/K)$ precisely once as $\mathfrak{b}$ runs over $\mathcal{B}$. Fix a generator g of $\mathfrak{g}$, so that $\mathfrak{g} = g\mathcal{O}_K$. The next result is due to Goldstein and Schappacher [10, Proposition 5.5].

Lemma 2.2.1. *For all non-zero $\lambda \in \mathcal{O}_K$, we have*

$$L_S(\overline{\psi}_\lambda, s) = \frac{|\Omega_\lambda/g|^{2s}}{\overline{\Omega_\lambda/g}} \sum_{\mathfrak{b} \in \mathcal{B}} H_1\left(\psi_\lambda(\mathfrak{b})\frac{\Omega_\lambda}{g}, s, \mathcal{L}_\lambda\right).$$

Proof. The Artin map gives an isomorphism

$$\left(\mathcal{O}_K/\mathfrak{g}\right)^\times / \widetilde{\boldsymbol{\mu}}_K \xrightarrow{\sim} \mathrm{Gal}\left(K\left(E(\lambda)_\mathfrak{g}\right)/K\right)$$

where $\widetilde{\boldsymbol{\mu}}_K$ denotes the image of the group $\boldsymbol{\mu}_K$ under reduction modulo $\mathfrak{g}$. Moreover, it is clear from the choice of λ that the map from $\boldsymbol{\mu}_K$ to $\widetilde{\boldsymbol{\mu}}_K$ is an isomorphism. Hence, the principal ideal $(\psi_\lambda(\mathfrak{b})+a)$ runs over all integral ideals of K prime to $\mathfrak{g}$ precisely once as $\mathfrak{b}$ runs over $\mathcal{B}$ and a runs over $\mathfrak{g}$. It follows that

$$L_S(\overline{\psi}_\lambda, s) = \sum_{\mathfrak{b}\in\mathcal{B}}\sum_{a\in\mathfrak{g}} \frac{\overline{\psi}_\lambda((\psi_\lambda(\mathfrak{b})+a))}{|\psi_\lambda(\mathfrak{b})+a|^{2s}}.$$

Note that since $a \in \mathfrak{g}$, we can write

$$\psi_\lambda(\mathfrak{b}) + a = (\psi_\lambda(\mathfrak{b}))(1 + a/\psi_\lambda(\mathfrak{b})) = \mathfrak{b}(1 + a/\psi_\lambda(\mathfrak{b}))$$

where $\mathrm{ord}_v(a/\psi_\lambda(\mathfrak{b})) \geqslant \mathrm{ord}_v(\mathfrak{f})$ for each prime $v \mid \mathfrak{f}$, so that

$$\psi_\lambda(\psi_\lambda(\mathfrak{b}) + a) = \psi_\lambda(\mathfrak{b})(1 + a/\psi_\lambda(\mathfrak{b})) = \psi_\lambda(\mathfrak{b}) + a.$$

Hence

$$L_S(\overline{\psi}_\lambda, s) = \sum_{\mathfrak{b}\in\mathcal{B}}\sum_{a\in\mathfrak{g}} \frac{\overline{\psi_\lambda(\mathfrak{b})+a}}{|\psi_\lambda(\mathfrak{b})+a|^{2s}} = \sum_{\mathfrak{b}\in\mathcal{B}} H\left(\psi_\lambda(\mathfrak{b}), s, \mathfrak{g}\right).$$

We can renormalise the right hand side to obtain the result. □

The following is a well-known fact from, for example, [10, Theorem 2.1].

Fact 2.2.2. *For all* $\mathfrak{b} \in \mathcal{B}$*, we have*

$$\mathcal{E}_1^*\left(\frac{\Omega_\lambda}{g}, \mathcal{L}_\lambda\right) \in K(\mathfrak{g})$$

and

$$\mathcal{E}_1^*\left(\frac{\Omega_\lambda}{g}, \mathcal{L}_\lambda\right)^{\sigma_\mathfrak{b}} = \mathcal{E}_1^*\left(\frac{\psi(\mathfrak{b})\Omega_\lambda}{g}, \mathcal{L}_\lambda\right). \tag{2.2.1}$$

Now, we concentrate on the case where $E(\lambda)$ is a quadratic twist of E.

Definition 2.2.3. We say a rational prime p is a special split prime if p splits completely in $L = K(x(E[4]))$, the field obtained by adjoining to K the x-coordinates of all non-zero points in $E[4]$.

In addition, it can be shown that a rational prime p is a special split prime if and only if it splits in K, and $\psi(\mathfrak{p}) \equiv \pm 1 \bmod 4$ for both of the primes $\mathfrak{p}$ of K above p. Moreover, $L = K(\boldsymbol{\mu}_4, \sqrt[3]{2})$ (see Lemma A.1 of Appendix A).

For the remainder of this section, we assume that $D \in \mathcal{O}_K$ is such that $D \equiv 1 \bmod 3$ and $(D) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ is a square-free product of prime ideals $\mathfrak{p}_j$ of K above special split primes. In addition, we pick the sign π_j of the generator of $\mathfrak{p}_j$ so that $\pi_j \equiv 1 \bmod 4$, and set $D = \pi_1 \cdots \pi_n$ and $S = \{\pi_1, \ldots, \pi_n\}$. The sign will not matter since we are most interested in the case when D is an integer. Given $\alpha = (\alpha_1, \ldots \alpha_n)$ with $\alpha_j \in \{0, 1\}$ for all $j = 1, \ldots, n$, let $D_\alpha \in K$ be of the form $D_\alpha = \pi_1^{\alpha_1} \cdots \pi_n^{\alpha_n}$. Note that for any integers $k_j \geqslant 0$ and $D_{\alpha'} = \pi_1^{\alpha_1+2k_1} \cdots \pi_n^{\alpha_n+2k_n}$, we have

$$E(D_\alpha^3) \cong E(D_{\alpha'}^3)$$

over K, hence we may consider $\alpha = (\alpha_1, \ldots, \alpha_n) \in \{0, 1\}^n$ as an element of $(\mathbb{Z}/2\mathbb{Z})^n$. Given $\alpha \in (\mathbb{Z}/2\mathbb{Z})^n$, let n_α be the number of primes dividing D_α and define $S_\alpha = \{\pi_j : \pi_j \mid D_\alpha\}$.

Let $C(A/\mathbb{Q})$ be the conductor of an elliptic curve A over $\mathbb{Q}$. Recall that if $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \otimes_{\mathbb{Z}} \mathbb{Q} = K$, an imaginary quadratic field, we have

$$C(A/\mathbb{Q}) = \mathrm{N}_{K/\mathbb{Q}}\mathfrak{f}_A \cdot d_K, \tag{2.2.2}$$

where $\mathfrak{f}_A$ is the conductor of $\psi_{A/K}$ and d_K is the absolute value of the discriminant of $K/\mathbb{Q}$. In particular, $C(E/\mathbb{Q}) = 27$, and so the conductor of ψ is $3\mathcal{O}_K$. It can be verified using this result and Tate's algorithm that the conductor of ψ_{D^3} is $\mathfrak{f} = 3D\mathcal{O}_K$. It follows that $K\left(E(D^3)_{\mathfrak{f}}\right)$ is isomorphic to $K(\mathfrak{f})$, the ray class field of K modulo $\mathfrak{f}$. Hence the Artin map gives an isomorphism

$$\left(\mathcal{O}_K/3D\mathcal{O}_K\right)^\times / \widetilde{\boldsymbol{\mu}}_6 \xrightarrow{\sim} \mathrm{Gal}\left(K\left(E(D^3)_{\mathfrak{f}}\right)/K\right)$$

where $\widetilde{\boldsymbol{\mu}}_6$ denotes the image of $\boldsymbol{\mu}_K = \boldsymbol{\mu}_6$ under reduction modulo $\mathfrak{f}$. Note that since 3 and D are coprime and 3 ramifies in K, we have an exact sequence

$$0 \to \left(\mathcal{O}_K/D\mathcal{O}_K\right)^\times \to \left(\mathcal{O}_K/3D\mathcal{O}_K\right)^\times / \widetilde{\boldsymbol{\mu}}_6 \to \left(\mathcal{O}_K/3\mathcal{O}_K\right)^\times / \boldsymbol{\mu}_6 \to 0,$$

so that $\left(\mathcal{O}_K/3D\mathcal{O}_K\right)^\times / \widetilde{\boldsymbol{\mu}}_6 \cong \left(\mathcal{O}_K/D\mathcal{O}_K\right)^\times$.

Setting $s = 1$ and $g = 3D$ in Lemma 2.2.1 and applying (2.2.1) immediately yields:

Corollary 2.2.4. *For any $\alpha \in (\mathbb{Z}/2\mathbb{Z})^n$, we have*

$$\frac{3D}{\Omega_{D_\alpha^3}} L_S(\overline{\psi}_{D_\alpha^3}, 1) = \mathrm{Tr}_{K(\mathfrak{f})/K}\left(\mathcal{E}_1^*\left(\frac{\Omega_{D_\alpha^3}}{3D}, \mathcal{L}_{D_\alpha^3}\right)\right).$$

We wish to find $\mathrm{ord}_2\left(L^{(\mathrm{alg})}(\overline{\psi}_{D^3}, 1)\right)$. In order to do this, we consider the following sum of imprimitive Hecke L-series.

Definition 2.2.5. Let

$$\Phi_{D^3} = \sum_{\alpha\in(\mathbb{Z}/2\mathbb{Z})^n} \frac{L_S(\overline{\psi}_{D^3_\alpha}, 1)}{\Omega.}$$

Using Corollary 2.2.4, we can write this sum in the following way.

Theorem 2.2.6. *We have*

$$\Phi_{D^3} = 2^n \mathrm{Tr}_{K(\mathfrak{f})/\mathcal{J}}\left(\frac{1}{3D}\mathcal{E}_1^*\left(\frac{\Omega}{3D}, \mathcal{L}\right)\right),$$

where $\mathcal{J} = \mathbb{Q}\left(\sqrt{-3}, \sqrt{\pi_1}, \dots, \sqrt{\pi_n}\right)$.

Proof. We have for any $\alpha \in (\mathbb{Z}/2\mathbb{Z})^n$,

$$\frac{L_S(\overline{\psi}_{D^3_\alpha}, 1)}{\Omega_{D^3_\alpha}} = \frac{1}{3D}\sum_{\mathfrak{b}\in\mathcal{B}} \mathcal{E}_1^*\left(\frac{\Omega_{D^3_\alpha}}{3D}, \mathcal{L}_{D^3_\alpha}\right)^{\sigma_\mathfrak{b}}$$

and $\Omega_{D^3_\alpha} = \frac{1}{D_\alpha^{1/2}}\Omega$, so

$$\frac{L_S(\overline{\psi}_{D^3_\alpha}, 1)}{\Omega} = \frac{1}{3D}\sum_{\mathfrak{b}\in\mathcal{B}} (D^3_\alpha)^{\frac{\sigma_\mathfrak{b}-1}{6}} \mathcal{E}_1^*\left(\frac{\Omega}{3D}, \mathcal{L}\right)^{\sigma_\mathfrak{b}} \tag{2.2.3}$$

and

$$(D^3_\alpha)^{\frac{\sigma_\mathfrak{b}-1}{6}} = \left(\frac{D_\alpha}{\mathfrak{b}}\right)_2 \in \{\pm 1\},$$

where $\left(\frac{-}{\ }\right)_2$ denotes the quadratic residue symbol. Let $\epsilon_2(\cdot, \mathfrak{b}) : (\mathbb{Z}/2\mathbb{Z})^n \to \{\pm1\}$ be the 1-dimensional character defined by $\epsilon_2(\alpha, \mathfrak{b}) = \left(\frac{D_\alpha}{\mathfrak{b}}\right)_2$. Since any 1-dimensional character is irreducible, considering its inner product with the trivial character gives

$$\sum_{\alpha\in(\mathbb{Z}/2\mathbb{Z})^n} \epsilon_2(\alpha, \mathfrak{b}) = \begin{cases} 2^n & \text{if } \left(\frac{D_\alpha}{\mathfrak{b}}\right)_2 = 1 \text{ for all } \alpha \in (\mathbb{Z}/2\mathbb{Z})^n \\ 0 & \text{otherwise.} \end{cases}$$

Note that $\left(\frac{D_\alpha}{\mathfrak{b}}\right)_2 = 1$ for all $\alpha \in (\mathbb{Z}/2\mathbb{Z})^n$ if and only if $\left(\frac{\pi_j}{\mathfrak{b}}\right)_2 = 1$ for all $j = 1, \dots, n$. The result now follows by noting that $\left(\frac{\pi_j}{\mathfrak{b}}\right)_2 = 1$ for all $j = 1, \dots, n$ if and only if $\sigma_\mathfrak{b} \in \mathrm{Gal}(K(\mathfrak{f})/\mathcal{J})$ where $\mathcal{J} = \mathbb{Q}\left(\sqrt{-3}, \sqrt{\pi_1}, \dots, \sqrt{\pi_n}\right)$. □

We now make an explicit choice of $\mathcal{B}$.

Definition 2.2.7. Let $\mathcal{C}$ be a set of elements of $\mathcal{O}_K$ such that $c \in \mathcal{C}$ implies $-c \in \mathcal{C}$ and $c \bmod D$ runs over $(\mathcal{O}_K/D\mathcal{O}_K)^\times$ precisely once. Note that this is possible since $(2, D) = 1$ by hypothesis. Furthermore, since $\mathrm{Gal}(K(\mathfrak{f})/K)$ is isomorphic to $(\mathcal{O}_K/D\mathcal{O}_K)^\times$, the Artin symbol $(c, K(\mathfrak{f})/K)$ runs over $\mathrm{Gal}(K(\mathfrak{f})/K)$ precisely once as c varies in $\mathcal{C}$. In addition, we define

$$\mathcal{B} = \{(3c + D) \ : \ c \in \mathcal{C}\}$$

so that $3c + D \equiv 1 \bmod 3\mathcal{O}_K$ for all $c \in \mathcal{C}$ since $D \equiv 1 \bmod 3$ by assumption. In particular, if $\mathfrak{b} = (3c + D)$ then we have $\psi(\mathfrak{b}) = 3c + D$ since the conductor of ψ is $3\mathcal{O}_K$. Finally, let

$$V = \{c \in \mathcal{C} \ : \left(\frac{\pi_j}{\mathfrak{b}}\right)_2 = 1 \ \text{ for all } j = 1, \dots, n, \ \text{where } \mathfrak{b} = (3c + D)\},$$

where $\left(\frac{\cdot}{\cdot}\right)_2$ denotes the quadratic residue symbol.

Note that if $c \in V$ implies $-c \in V$ since

$$\begin{aligned} \left(\frac{\pi_j}{\mathfrak{b}}\right)_2 &= \left(\frac{3c + D}{\pi_j}\right)_2 && \text{(since } \pi_j \equiv 1 \bmod 4) \\ &= \left(\frac{3c}{\pi_j}\right)_2 \\ &= \left(\frac{-3c}{\pi_j}\right)_2 && \text{(since } \left(\tfrac{-1}{\pi_j}\right)_2 = 1). \end{aligned}$$

It is clear that we can also write Theorem 2.2.6 in the following way.

Corollary 2.2.8. *We have*

$$\Phi_{D^3} = 2^n \sum_{c \in V} \frac{1}{3D} \mathcal{E}_1^* \left(\frac{c\Omega}{D} + \frac{\Omega}{3}, \mathcal{L}\right).$$

Using the relation between the Eisenstein series and the Weierstrass $\wp$-function, we can show:

Theorem 2.2.9. *We have*

$$\sum_{c \in V} \mathcal{E}_1^* \left(\frac{c\Omega}{D} + \frac{\Omega}{3}, \mathcal{L}\right) = \frac{1}{2} \left(\sum_{c \in V} \frac{9}{3 - \wp\left(\frac{c\Omega}{D}, \mathcal{L}\right)}\right) - \#(V).$$

Proof. Let

$$s_2(\mathcal{L}) = \lim_{\substack{s\to 0\\ s>0}} \sum_{w\in\mathcal{L}\setminus\{0\}} w^{-2}|w|^{-2s}.$$

Then by [10, Proposition 1.5], we have

$$\mathcal{E}_1^*(z,\mathcal{L}) = \zeta(z,\mathcal{L}) - zs_2(\mathcal{L}) - \overline{z}A(\mathcal{L})^{-1}.$$

Here, $\zeta(z,\mathcal{L})$ is the Weierstrass zeta function of $\mathcal{L}$ and $A(\mathcal{L}) := \frac{\overline{u}v-u\overline{v}}{2\pi i}$ where (u,v) is a base of $\mathcal{L}$ over $\mathbb{Z}$ satisfying $\mathrm{Im}(v/u)>0$. Thus we have $A(\mathcal{L}) = \frac{\Omega^2(\omega-\overline{\omega})}{2\pi i} = \frac{\sqrt{3}\Omega^2}{2\pi}$, and we can see that $s_2(\mathcal{L})=0$ on noting that $\omega\in\mathcal{L}$ which gives $\omega^{-2}s_2(\mathcal{L}) = s_2(\mathcal{L})$. Hence

$$\mathcal{E}_1^*(z,\mathcal{L}) = \zeta(z,\mathcal{L}) - \frac{2\pi\overline{z}}{\sqrt{3}\Omega^2}.$$

Recall also that for $z_1, z_2\in\mathbb{C}$, we have an addition formula:

$$\zeta(z_1+z_2,\mathcal{L}) = \zeta(z_1,\mathcal{L}) + \zeta(z_2,\mathcal{L}) + \frac{1}{2}\frac{\wp'(z_1,\mathcal{L})-\wp'(z_2,\mathcal{L})}{\wp(z_1,\mathcal{L})-\wp(z_2,\mathcal{L})}.$$

Applying this with $z_1 = \frac{\Omega}{3}$, $z_2 = \frac{c\Omega}{D}$, we get

$$\begin{aligned}\sum_{c\in V}\mathcal{E}_1^*\left(\frac{c\Omega}{D}+\frac{\Omega}{3},\mathcal{L}\right) &= \sum_{c\in V}\left(\zeta\left(\frac{c\Omega}{D}+\frac{\Omega}{3},\mathcal{L}\right) - \left(\frac{\overline{c}\Omega}{\overline{D}}+\frac{\Omega}{3}\right)\frac{2\pi}{\sqrt{3}\Omega^2}\right)\\ &= \sum_{c\in V}\left(\zeta\left(\frac{\Omega}{3},\mathcal{L}\right)+\zeta\left(\frac{c\Omega}{D},\mathcal{L}\right)+\frac{1}{2}\frac{\wp'(\frac{\Omega}{3},\mathcal{L})-\wp'(\frac{c\Omega}{D},\mathcal{L})}{\wp(\frac{\Omega}{3},\mathcal{L})-\wp(\frac{c\Omega}{D},\mathcal{L})} - \left(\frac{\overline{c}\Omega}{\overline{D}}+\frac{\Omega}{3}\right)\frac{2\pi}{\sqrt{3}\Omega^2}\right).\end{aligned}$$

Next, we use the key property that, if $c\in V$, then also $-c\in V$. Since $\zeta(z,\mathcal{L})$ and $\wp'(z,\mathcal{L})$ are odd functions, and $\wp(z,\mathcal{L})$ is an even function, it follows that

$$\sum_{c\in V}\mathcal{E}_1^*\left(\frac{c\Omega}{D}+\frac{\Omega}{3},\mathcal{L}\right) = \left(\sum_{c\in V}\frac{1}{2}\frac{\wp'\left(\frac{\Omega}{3},\mathcal{L}\right)}{\wp\left(\frac{\Omega}{3},\mathcal{L}\right)-\wp\left(\frac{c\Omega}{D},\mathcal{L}\right)}\right) + \#(V)\left(\zeta\left(\frac{\Omega}{3},\mathcal{L}\right) - \frac{2\pi}{3\sqrt{3}\Omega}\right).$$

By applying formulae (3.2) and (3.3) of [21, p. 126], we obtain

$$\zeta(z+1,\mathcal{O}_K) = \zeta(z,\mathcal{O}_K) + \frac{2\pi}{\sqrt{3}},\quad \zeta(z+\omega,\mathcal{O}_K) = \zeta(z,\mathcal{O}_K) + \frac{2\pi}{\sqrt{3}}\overline{\omega}. \tag{2.2.4}$$

Letting $z = -\frac{1}{3}$ in (2.2.4) gives

$$\zeta\left(\frac{2}{3},\mathcal{O}_K\right) + \zeta\left(\frac{1}{3},\mathcal{O}_K\right) = \frac{2\pi}{\sqrt{3}}.$$

But we have $\zeta\left(\Omega z, \mathcal{L}\right) = \frac{1}{\Omega}\zeta\left(z, \mathcal{O}_K\right)$, so

$$\zeta\left(\frac{2\Omega}{3}, \mathcal{L}\right) + \zeta\left(\frac{\Omega}{3}, \mathcal{L}\right) = \frac{2\pi}{\sqrt{3}\Omega}. \tag{2.2.5}$$

On the other hand, we have

$$\zeta(2z, \mathcal{L}) = 2\zeta(z, \mathcal{L}) + \frac{\wp''(z, \mathcal{L})}{2\wp'(z, \mathcal{L})},$$

and by differentiating the equation $\wp'(z, \mathcal{L})^2 = 4\wp(z, \mathcal{L})^3 - 3^3$, we get $\wp''(z, \mathcal{L}) = 6\wp(z, \mathcal{L})^2$. Also, by computation we get

$$\wp\left(\frac{\Omega}{3}, \mathcal{L}\right) = 3, \quad \wp'\left(\frac{\Omega}{3}, \mathcal{L}\right) = 9,$$

thus

$$\zeta\left(\frac{2\Omega}{3}, \mathcal{L}\right) - 2\zeta\left(\frac{\Omega}{3}, \mathcal{L}\right) = \frac{\wp''\left(\frac{\Omega}{3}, \mathcal{L}\right)}{2\wp'\left(\frac{\Omega}{3}, \mathcal{L}\right)} = \frac{6\wp^2\left(\frac{\Omega}{3}, \mathcal{L}\right)}{2\wp'\left(\frac{\Omega}{3}, \mathcal{L}\right)} = 3. \tag{2.2.6}$$

Now, solving (2.2.5) and (2.2.6) gives

$$\zeta\left(\frac{\Omega}{3}, \mathcal{L}\right) = \frac{2\pi}{3\sqrt{3}\Omega} - 1.$$

Hence

$$\sum_{c\in V} \mathcal{E}_1^*\left(\frac{c\Omega}{D} + \frac{\Omega}{3}, \mathcal{L}\right) = \left(\sum_{c\in V} \frac{1}{2} \frac{\wp'\left(\frac{\Omega}{3}, \mathcal{L}\right)}{\wp\left(\frac{\Omega}{3}, \mathcal{L}\right) - \wp\left(\frac{c\Omega}{D}, \mathcal{L}\right)}\right) - \#(V).$$

Substituting the values $\wp\left(\frac{\Omega}{3}, \mathcal{L}\right) = 3$ and $\wp'\left(\frac{\Omega}{3}, \mathcal{L}\right) = 9$ again gives the result. □

Now we prove the following integrality result of the Eisenstein series.

Corollary 2.2.10. *For $n \geqslant 1$, we have*

$$\operatorname{ord}_2\left(\sum_{c\in V} \mathcal{E}_1^*\left(\frac{c\Omega}{D} + \frac{\Omega}{3}, \mathcal{L}\right)\right) \geqslant 0.$$

Proof. Given $c \in V$, let P be the point on $E : y^2 = 4x^3 - 3^3$ given by

$$x(P) = \wp\left(\frac{c\Omega}{D}, \mathcal{L}\right), \quad y(P) = \wp'\left(\frac{c\Omega}{D}, \mathcal{L}\right)$$

and define

$$\mathscr{M}(c,D)=\frac{9}{3-x(P)}.$$

Recall that E has minimal Weierstrass form

$$E:Y^2+Y=X^3-7$$

which has discriminant 3^9, so E has good reduction at 2 over K. This means that $\mathrm{ord}_2(X(P))\geqslant 0$ since P is a torsion point on E of order prime to 2. Further, $x=X$ in the change of coordinates which gives the minimal Weierstrass form, and so we have

$$\mathscr{M}(c,D)=\frac{9}{3-X(P)}.$$

We claim that $\mathrm{ord}_2(3-X(P))=0$. Suppose for a contradiction that $\mathrm{ord}_2(3-X(P))>0$. Then let $Q=(3,4)$ be the point on E which we know is a 3-torsion, so that we have $\mathrm{ord}_2(X(Q)-X(P))>0$. Hence, under reduction modulo 2, we would have $X(\widetilde{Q})=X(\widetilde{P})$ where $\tilde{}$ denotes reduction modulo 2. Then we have $\widetilde{P}=\pm\widetilde{Q}$, so either $P-Q$ or $P+Q$ is in the kernel of the reduction map, so it must correspond to an element in the formal group of E at 2, and therefore its order must be a power of 2. But this is not possible since P has order D and Q has order 3, both of which are coprime to 2. Hence

$$\begin{aligned}\mathrm{ord}_2(\mathscr{M}(c,D))&=\mathrm{ord}_2(9)-\mathrm{ord}_2(3-X(P))\\&=0.\end{aligned}$$

But $\mathscr{M}(c,D)=\mathscr{M}(-c,D)$ since $\wp(z)$ is an even function and $\#(V)$ is even, so

$$\mathrm{ord}_2(\sum_{c\in V}\mathscr{M}(c,D))\geqslant 1.$$

It follows that

$$\begin{aligned}\mathrm{ord}_2\left(\sum_{c\in V}\mathcal{E}_1^*\left(\frac{c\Omega}{D}+\frac{\Omega}{3},\mathcal{L}\right)\right)&=\min\left(\mathrm{ord}_2\left(\frac{1}{2}\sum_{c\in V}\mathscr{M}(c,D)\right),\mathrm{ord}_2\left(\#(V)\right)\right)\\&\geqslant 0\end{aligned}$$

as required. □

Remark 2.2.11. For $n = 0$ (i.e. for E), a computation using Magma gives

$$L^{(\mathrm{alg})}(\overline{\psi}, 1) = \frac{1}{3}.$$

Thus we have proved:

Theorem 2.2.12. *Let $D \in \mathcal{O}_K$ be as above and let n be the number of primes in $\mathcal{O}_K$ dividing D. Then we have*

$$\mathrm{ord}_2(\Phi_{D^3}) \geqslant n.$$

Finally, we are ready to prove the first main result:

Theorem 2.2.13. *Let $D \in \mathcal{O}_K$ be as above and let n be the number of primes in $\mathcal{O}_K$ dividing D. Then*

$$\mathrm{ord}_2\left(L^{(alg)}(\overline{\psi}_{D^3}, 1)\right) \geqslant n.$$

Proof. We prove this by induction on n. Write $D = D_\alpha$, and given $\alpha, \beta \in (\mathbb{Z}/2\mathbb{Z})^n$, we write $\beta < \alpha$ if $D_\beta \mid D_\alpha$ but $D_\beta \neq D_\alpha$. If $n_\alpha = 1$, $S_\alpha = \{\pi_1\}$ say, then

$$\Phi_{\pi_1^3} = \frac{L_{S_\alpha}(\overline{\psi}, 1)}{\Omega} + \frac{L(\overline{\psi}_{\pi_1^3}, 1)}{\Omega}.$$

By Theorem 2.2.12, we know that $\mathrm{ord}_2(\Phi_{\pi_1^3}) \geqslant 1$. Now,

$$\begin{aligned} \frac{L_{S_\alpha}(\overline{\psi}, 1)}{\Omega} &= \left(1 - \frac{\overline{\psi}((\pi_1))}{\pi_1\overline{\pi}_1}\right) \frac{L(\overline{\psi}, 1)}{\Omega} \\ &= \left(\frac{\pi_1 \pm 1}{\pi_1}\right) \frac{1}{3} \end{aligned}$$

since $\psi((\pi_1)) = \pm\pi_1$ and by Remark 2.2.11 we have $\frac{L(\overline{\psi},1)}{\Omega} = \frac{1}{3}$. But $\mathrm{ord}_2\left(\frac{\pi_1 \pm 1}{\pi_1}\right) \geqslant 1$, hence

$$\mathrm{ord}_2\left(\frac{L(\overline{\psi}_{\pi_1^3}, 1)}{\Omega}\right) \geqslant 1 = n_\alpha.$$

Now suppose $n_\alpha > 1$ and our result holds for $0 < \beta < \alpha$. Again,

$$\Phi_{D_\alpha^3} = \frac{L_{S_\alpha}(\overline{\psi}, 1)}{\Omega} + \sum_{0<\beta<\alpha} \frac{L_{S_\alpha}(\overline{\psi}_{D_\beta^3}, 1)}{\Omega} + \frac{L_{S_\alpha}(\overline{\psi}_{D_\alpha^3}, 1)}{\Omega},$$

where the last term is primitive. We know by Theorem 2.2.12 that $\mathrm{ord}_2(\Phi_{D^3_\alpha}) \geqslant n_\alpha$. Now

$$\begin{aligned}\frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega} &= \prod_{\pi\in S_\alpha}\left(1-\frac{\overline{\psi}((\pi))}{\pi\overline{\pi}}\right)\frac{L(\overline{\psi},1)}{\Omega}\\ &= \prod_{\pi\in S_\alpha}\left(\frac{\pi\pm 1}{\pi}\right)\frac{1}{3}\end{aligned}$$

where $\mathrm{ord}_2\left(\frac{\pi\pm1}{\pi}\right) \geqslant 1$ for each $\pi\in S_\alpha$. Hence

$$\begin{aligned}\mathrm{ord}_2\left(\frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega}\right) &\geqslant \#(S_\alpha)\\ &\geqslant n_\alpha.\end{aligned}$$

Also for $0<\beta<\alpha$,

$$\frac{L_{S_\alpha}(\overline{\psi}_{D^3_\beta},1)}{\Omega} = \prod_{\pi\in S_\alpha\backslash S_\beta}\left(1-\frac{\overline{\psi}_{D^3_\beta}((\pi))}{\pi\overline{\pi}}\right)\frac{L(\overline{\psi}_{D^3_\beta},1)}{\Omega}.$$

We have $\psi_{D^3_\beta}((\pi)) = \left(\frac{D_\beta}{\pi}\right)^3_6\psi((\pi)) = \pm\pi$. Hence

$$\begin{aligned}\mathrm{ord}_2\left(\prod_{\pi\in S_\alpha\backslash S_\beta}\left(1-\frac{\overline{\psi}_{D^3_\beta}((\pi))}{\pi\overline{\pi}}\right)\right) &= \mathrm{ord}_2\left(\prod_{\pi\in S_\alpha\backslash S_\beta}\left(\frac{\pi\pm1}{\pi}\right)\right)\\ &\geqslant \#(S_\alpha\backslash S_\beta)\\ &= n_\alpha - n_\beta.\end{aligned}$$

Furthermore, by the induction hypothesis, $\mathrm{ord}_2\left(\frac{L(\overline{\psi}_{D^3_\beta},1)}{\Omega}\right) \geqslant n_\beta$. Thus

$$\begin{aligned}\mathrm{ord}_2\left(\frac{L_{S_\alpha}(\overline{\psi}_{D^3_\beta},1)}{\Omega}\right) &\geqslant (n_\alpha-n_\beta)+n_\beta\\ &= n_\alpha,\end{aligned}$$

and so

$$\mathrm{ord}_2\left(\sum_{0<\beta<\alpha}\frac{L_{S_\alpha}(\overline{\psi}_{D^3_\beta},1)}{\Omega}\right) \geqslant n_\alpha.$$

It follows that

$$\mathrm{ord}_2\left(\frac{L(\overline{\psi}_{D_\alpha^3},1)}{\Omega}\right) \geqslant n_\alpha$$

as required. □

Recalling $L(E(\lambda),1) = L(\overline{\psi}_\lambda,1)$, the following is an immediate consequence.

Theorem 2.2.14. *Let $D > 1$ be an integer which is a product of $k(D)$ distinct special split primes. Then*

$$\mathrm{ord}_2\left(L^{(alg)}(E(D^3),1)\right) \geqslant 2k(D).$$

Remark 2.2.15. The bound obtained in Theorem 2.2.14 is sharp. For example, let π be the prime $13+12\omega$ and let $D = \mathrm{N}(\pi) = 157$, which is a rational prime. Then $L^{(\mathrm{alg})}(E(D^3),1) = 12$ so $\mathrm{ord}_2\left(L^{(\mathrm{alg})}(E(D^3),1)\right) = 2$, as required. More numerical examples can be found in Appendix B.

2.3 Cubic Twists.

Now we look at the cubic twists of E, i.e. the curves of the form

$$E(D^2) : y^2 = 4x^3 - 3^3D^2$$

for a cube-free integer D. This is isomorphic to the curve

$$Y^2 + DY = X^3 - 7D^2$$

via the change of variables $X = x$ and $Y = 2y+D$. Let ψ_{D^2} denote the Grössencharacter of $E(D^2)/K$.

Definition 2.3.1. We say a prime π of K is *cubic-special* if it splits completely in the field $K(E[27])$, but does not split completely in the strictly larger field $K(E[27])((1-\omega)^{1/9})$.

The following characterisation of cubic-special primes will be useful, in particular in proving Corollary A.5 of Appendix A.

Lemma 2.3.2. *A prime π of K is cubic special if and only if $\pi \equiv 1 \bmod 27$ and 9 divides the order of $1-\omega$ in $(\mathcal{O}_K/\pi\mathcal{O}_K)^\times$. The set consisting of such primes has density $\frac{2}{3}$ in the set of primes of K congruent to 1 modulo 27. In particular, there are infinitely many such primes.*

Proof. First, we note that $K(E[27])$ is equal to the ray class field $K(27)$ of K modulo 27 by [7, Lemma 3]. Since $\mathbb{Q}(\boldsymbol{\mu}_{27}) \subset K(27)$, it follows that $K(27)\left((1-\omega)^{\frac{1}{9}}\right)/K(27)$ is a Galois extension. Also $K(27)\left((1-\omega)^{\frac{1}{9}}\right)/K$ is not an abelian extension, since its subextension $K\left((1-\omega)^{\frac{1}{9}}\right)/K$ is not Galois. In addition, $K(27)\left((1-\omega)^{\frac{1}{9}}\right)/K(27)$ is a degree 3 extension since we showed that $\left(\frac{1-\omega}{\pi}\right)_3 = 1$, i.e. $(1-\omega)^{\frac{1}{3}} \in K(27)$. Let H denote the Galois group of this degree 3 extension. Furthermore, let G denote the Galois group $\mathrm{Gal}\left(K(27)\left((1-\omega)^{\frac{1}{9}}\right)/K\right)$, and let $\mathrm{Frob}_\pi \in G$ denote the Frobenius at π. Then $\mathrm{Frob}_\pi|_{K(27)} = id$ in H if and only if $\psi_{E(\pi^2)/K}((\pi)) \equiv 1 \bmod 27$. If we take a prime π such that $\mathrm{Frob}_\pi \in H\backslash\{id\}$, then $(1-\omega)$ is not a ninth power modulo π in $K(27)\left((1-\omega)^{\frac{1}{9}}\right)$, and it follows that the order of $1-\omega$ must be divisible by 9 since 27 divides $\mathrm{N}(\pi) - 1 = |\left(\mathcal{O}_K/\pi\mathcal{O}_K\right)^\times|$. By the Čebotarev density theorem, the density of such primes is $\frac{2}{3}$. □

From now on, let us assume that each prime π of K dividing D is cubic-special. Note that if p is a rational prime such that $p \equiv 1 \bmod 3$, then p always splits in K since we can write $p = a^2 - ab + b^2 = (a+b\omega)(a+b\overline{\omega})$ for some integers a and b. In addition, if $p \equiv 1 \bmod 27$, it can easily be shown that we can assume $b \equiv 0 \bmod 27$ and $a \equiv 1 \bmod 27$ using symmetry in a and b and change of sign of a. Hence we can write $p = \pi\overline{\pi}$ with $\pi \in \mathcal{O}_K$ and $\pi \equiv 1 \bmod 27$.

Before we begin, it will be useful to find a model for our curve $E : Y^2 + Y = X^3 - 7$ where E has good reduction at 3. Let $u = \frac{\sqrt{\alpha}}{\beta^2}$ where $\alpha = \frac{27+3\sqrt{-3}}{2}$, $\beta = \sqrt[3]{\frac{1-3\sqrt{-3}}{2}}$, and let $r = -\frac{3}{2}\sqrt[3]{\frac{-13-3\sqrt{-3}}{2}}$. Then the change of variables $x = u^2X + r$, $y = 2u^3Y$, gives an equation for E with good reduction at 3 (see Proposition A.2 of Appendix A).

Given $\alpha = (\alpha_1, \dots \alpha_n)$ with $\alpha_j \in \{0,1,2\}$ for all $j = 1, \dots, n$, let D_α be an element of K of the form $D_\alpha = \pi_1^{\alpha_1} \cdots \pi_n^{\alpha_n}$ where π_j are distinct cubic-special primes. Similarly to the quadratic twist case, we may consider $\alpha = (\alpha_1, \dots, \alpha_n) \in \{0,1,2\}^n$ as an element of $(\mathbb{Z}/3\mathbb{Z})^n$. Given $\alpha \in (\mathbb{Z}/3\mathbb{Z})^n$, let n_α be the number of distinct primes of K dividing D_α and define $S_\alpha = \{\pi_j : \pi_j \mid D_\alpha\}$. Pick $\alpha \in (\mathbb{Z}/3\mathbb{Z})^n$ such that $n_\alpha = n$, and set $D = D_\alpha$ and $S = \{\pi_1, \dots \pi_n\}$. We will study the following sum of imprimitive Hecke L-functions (see Definition 2.2.5).

Definition 2.3.3. Given D as above, let

$$\Phi_{D^2} = \sum_{\alpha \in (\mathbb{Z}/3\mathbb{Z})^n} \frac{L_S(\overline{\psi}_{D_\alpha^2}, 1)}{\Omega}.$$

Let $\mathfrak{f}$ be the conductor of the Grössencharacter ψ_{D^2}. Then again, a computation using Tate's algorithm shows that $\mathfrak{f} = 3D\mathcal{O}_K$. Also, the Artin map gives an isomorphism between $\mathrm{Gal}(K(\mathfrak{f})/K)$ and $(\mathcal{O}_K/3D\mathcal{O}_K)^\times/\widetilde{\boldsymbol{\mu}}_6$, which is isomorphic to $(\mathcal{O}_K/D\mathcal{O}_K)^\times$ since $(3,D)=1$ and 3 ramifies in K. Now let $\mathcal{C}$ be a set of elements of $\mathcal{O}_K$ such that $c\in\mathcal{C}$ implies ωc, $\omega^2 c\in\mathcal{C}$ and $c \bmod D$ runs over $(\mathcal{O}_K/D\mathcal{O}_K)^\times$ precisely once. This is possible since 3 and D are coprime by assumption. Then let

$$\mathcal{B}=\{(3c+D)\ :\ c\in\mathcal{C}\}$$

so that $3c+D\equiv 1 \bmod 3\mathcal{O}_K$, where $3\mathcal{O}_K$ is the conductor of ψ. In particular, if $\mathfrak{b}=(3c+D)\in\mathcal{B}$ then we have $\psi(\mathfrak{b})=3c+D$.

Let m be such that $\boldsymbol{\mu}_m\subset K$. For $a\in K^*$ and $\mathfrak{b}$ an ideal of K coprime to m and a, we write $\left(\frac{a}{\mathfrak{b}}\right)_m$ for the m-th power residue symbol defined by the equation

$$(\sqrt[m]{a})^{\sigma_{\mathfrak{b}}}=\left(\frac{a}{\mathfrak{b}}\right)_m\sqrt[m]{a},$$

where $\sigma_{\mathfrak{b}}=(\mathfrak{b},K(\sqrt[m]{a})/K)\in\mathrm{Gal}\,(K(\sqrt[m]{a})/K)$ denotes the Artin symbol of $\mathfrak{b}$. Also, for any $a,b\in K^*$, we define

$$\left(\frac{a}{b}\right)_m=\prod_v\left(\frac{a}{v}\right)_m^{v(b)},$$

where v runs through all primes of K coprime to a. Recall also that for a prime π of K and $c\in(\mathcal{O}_K/\pi\mathcal{O}_K)^\times$, we have Euler's criterion

$$\left(\frac{c}{\pi}\right)_m\equiv c^{\frac{\mathrm{N}(\pi)-1}{m}} \bmod \pi.$$

Definition 2.3.4. Let

$$V=\{c\in\mathcal{C}\ :\left(\frac{\pi_j}{\mathfrak{b}}\right)_3=1\ \text{ for all } j=1,\dots,n, \text{ where } \mathfrak{b}=(3c+D)\}.$$

Recall that we have $\left(\frac{1-\omega}{\pi_j}\right)_3=\left(\frac{1-\omega^2}{\pi_j}\right)_3=\omega^m$ and $\left(\frac{\omega}{\pi_j}\right)_3=\omega^{-m-n}$ where $m,n\in\mathbb{Z}$ are such that $\pi_j=1+3(m+n\omega)$ (see [1, p. 354]). Hence for $c\in V$ we have

$$\begin{aligned}\left(\frac{\pi_j}{\mathfrak{b}}\right)_3&=\left(\frac{3c+D}{\pi_j}\right)_3 && \text{(since } \pi_j\equiv\mathfrak{b}\equiv 1 \bmod 3\text{, see [1, p. 354])}\\ &=\left(\frac{3c}{\pi_j}\right)_3\\ &=\left(\frac{c}{\pi_j}\right)_3 && \text{(since } \pi_j\equiv 1 \bmod 9\text{, we have } \left(\frac{1-\omega}{\pi_j}\right)_3=\left(\frac{1-\omega^2}{\pi_j}\right)_3=1).\end{aligned}$$

Furthermore, by assumption on π_j, we have $m+n\equiv 0 \bmod 3$ so $\left(\frac{\omega}{\pi_j}\right)_3 = 1$. Hence $\left(\frac{c}{\pi_j}\right)_3 = \left(\frac{\omega c}{\pi_j}\right)_3 = \left(\frac{\omega^2 c}{\pi_j}\right)_3$. So $c \in V$ implies ωc, $\omega^2 c \in V$.

It is also easy to check that

$$\mathcal{L}_{D^2} = \frac{\Omega}{\sqrt[3]{D}}\mathcal{O}_K.$$

Theorem 2.3.5. *We have*

$$\Phi_{D^2} = 3^n \sum_{c\in V} \frac{1}{3D}\mathcal{E}_1^*\left(\frac{c\Omega}{D}+\frac{\Omega}{3},\mathcal{L}\right).$$

Proof. It is clear that Lemma 2.2.1, Fact 2.2.2 and Corollary 2.2.4 still apply. Thus, for any $\alpha \in (\mathbb{Z}/3\mathbb{Z})^n$,

$$\frac{L_S(\overline{\psi}_{D_\alpha^2},1)}{\Omega_{D_\alpha^2}} = \frac{1}{3D}\sum_{\mathfrak{b}\in\mathcal{B}} \mathcal{E}_1^*\left(\frac{\Omega_{D_\alpha^2}}{3D},\mathcal{L}_{D_\alpha^2}\right)^{\sigma_\mathfrak{b}}$$

and $\Omega_{D_\alpha^2} = \frac{1}{D_\alpha^{1/3}}\Omega$, so

$$\frac{L_S(\overline{\psi}_{D_\alpha^2},1)}{\Omega} = \frac{1}{3D}\sum_{\mathfrak{b}\in\mathcal{B}} (D_\alpha^2)^{\frac{\sigma_\mathfrak{b}-1}{6}}\mathcal{E}_1^*\left(\frac{\Omega}{3D},\mathcal{L}\right)^{\sigma_\mathfrak{b}} \tag{2.3.1}$$

and

$$(D_\alpha^2)^{\frac{\sigma_\mathfrak{b}-1}{6}} = \left(\frac{D_\alpha}{\mathfrak{b}}\right)_3 \in \boldsymbol{\mu}_3.$$

We have a character $\epsilon_3(\cdot,\mathfrak{b}) : (\mathbb{Z}/3\mathbb{Z})^n \to \boldsymbol{\mu}_3$ defined by $\epsilon_3(\alpha,\mathfrak{b}) = \left(\frac{D_\alpha}{\mathfrak{b}}\right)_3$. This is a 1-dimensional character, and since any 1-dimensional character is irreducible, considering its inner product with the trivial character gives

$$\sum_{\alpha\in(\mathbb{Z}/3\mathbb{Z})^n} \epsilon_3(\alpha,\mathfrak{b}) = \begin{cases} 3^n & \text{if } \left(\frac{D_\alpha}{\mathfrak{b}}\right)_3 = 1 \quad \text{for all } \alpha \in (\mathbb{Z}/3\mathbb{Z})^n \\ 0 & \text{otherwise.}\end{cases}$$

Note that $\left(\frac{D_\alpha}{\mathfrak{b}}\right)_3 = 1$ for all $\alpha \in (\mathbb{Z}/3\mathbb{Z})^n$ if and only if $\left(\frac{\pi_j}{\mathfrak{b}}\right)_3 = 1$ for all $j = 1,\ldots,n$. It follows that

$$\Phi_{D_\alpha^2} = 3^n \sum_{c\in V}\frac{1}{3D}\mathcal{E}_1^*\left(\frac{\Omega}{3D},\mathcal{L}\right)^{\sigma_\mathfrak{b}},$$

where $\mathfrak{b} = 3c + D$. Again, applying equation (2.2.1) gives the result. □

As in Theorem 2.2.9, we have

Theorem 2.3.6.

$$\sum_{c\in V} \mathcal{E}_1^*\left(\frac{c\Omega}{D}+\frac{\Omega}{3},\mathcal{L}\right)=\frac{1}{2}\left(\sum_{c\in V}\frac{9-\wp'\left(\frac{c\Omega}{D},\mathcal{L}\right)}{3-\wp\left(\frac{c\Omega}{D},\mathcal{L}\right)}\right)-\#(V).$$

Proof. The proof is almost identical to the proof of Theorem 2.2.9, since the addition formula for $\zeta(z,\mathcal{L})$ implies $\zeta\left(\frac{c\Omega}{D},\mathcal{L}\right)+\zeta\left(\frac{\omega c\Omega}{D},\mathcal{L}\right)+\zeta\left(\frac{\omega^2 c\Omega}{D},\mathcal{L}\right)=0$, and we have $c+\omega c+\omega^2 c=0$ for any $c\in V$. □

This gives:

Corollary 2.3.7. *For $n\geqslant 1$, we have*

$$\operatorname{ord}_3\left(\sum_{c\in V}\mathcal{E}_1^*\left(\frac{c\Omega}{D}+\frac{\Omega}{3},\mathcal{L}\right)\right)\geqslant 1.$$

Before we prove this, let us prove:

Proposition 2.3.8. $\operatorname{ord}_3(\#(V))\geqslant 2$.

Proof. Given $\alpha_i\in\{0,1,2\}$ for $i=1,\dots,n$, let

$$V_{(\alpha_1,\dots\alpha_n)}=\left\{c\in\mathcal{C}:\left(\frac{c}{\pi_i}\right)=\omega^{\alpha_i}\ \text{ for all } i\in\{1,\dots n\}\right\},$$

so that now we have $V=V_{(0,\dots,0)}$. Given any $(\alpha_1,\dots,\alpha_n)$, if we can find $b\in\mathcal{C}$ such that $\left(\frac{b}{\pi_i}\right)=\omega^{\alpha_i}$, then clearly we can write

$$\begin{aligned}V_{(\alpha_1,\dots\alpha_n)}&=bV\\&=\{bc:c\in V\}\end{aligned}$$

and if there is no such b, then $V_{(\alpha_1,\dots\alpha_n)}=\varnothing$. Also, we have

$$\mathcal{C}=\bigcup_{(\alpha_1,\dots,\alpha_n)\in\{0,1,2\}^n}V_{(\alpha_1,\dots,\alpha_n)},$$

so

$$\#(\mathcal{C})=k\#(V)$$

for some positive integer $k\leqslant 3^n$, so that $\operatorname{ord}_3(k)\leqslant n$. On the other hand, $\operatorname{ord}_3\left(\#(\mathcal{C})\right)=\operatorname{ord}_3\left((\mathrm{N}(\pi_1)-1)\cdots(\mathrm{N}(\pi_\mathrm{n})-1)\right)\geqslant 3n$. Hence, $\operatorname{ord}_3(\#(V))\geqslant 3n-n=2n\geqslant 2$ for $n\geqslant 1$, so $9\mid\#(V)$ as required. □

Now we are ready to prove Corollary 2.3.7.

Proof. (of Corollary 2.3.7) Let P be the point on $E : y^2 = 4x^3 - 3^3$ given by

$$x(P) = \wp\left(\frac{c\Omega}{D}, \mathcal{L}\right), \quad y(P) = \wp'\left(\frac{c\Omega}{D}, \mathcal{L}\right),$$

and define

$$\mathscr{M}(c, D) = \frac{9 - y(P)}{3 - x(P)}.$$

Now, write V as a union $H \cup \omega H \cup \omega^2 H$ for some set H. Then

$$\sum_{c\in V} \mathscr{M}(c, D) = \sum_{c\in H} \frac{9 - \wp'\left(\frac{c\Omega}{D}, \mathcal{L}\right)}{3 - \wp\left(\frac{c\Omega}{D}, \mathcal{L}\right)} + \frac{9 - \wp'\left(\frac{\omega c\Omega}{D}, \mathcal{L}\right)}{3 - \wp\left(\frac{\omega c\Omega}{D}, \mathcal{L}\right)} + \frac{9 - \wp'\left(\frac{\omega^2 c\Omega}{D}, \mathcal{L}\right)}{3 - \wp\left(\frac{\omega^2 c\Omega}{D}, \mathcal{L}\right)}.$$

Recall that E has complex multiplication by ω via $\omega(x, y) = (\omega x, y)$, so $\wp'(\frac{\omega^i c\Omega}{D}, \mathcal{L}) = \wp'(\frac{c\Omega}{D}, \mathcal{L})$ for $i = 0, 1, 2$. Moreover, $\mathcal{L} = \omega\mathcal{L}$ so $\wp\left(\frac{\omega^i c\Omega}{D}, \mathcal{L}\right) = \wp\left(\frac{\omega^i c\Omega}{D}, \omega^i\mathcal{L}\right)$, and $\wp$ is homogeneous of degree -2 so this simplifies to

$$\sum_{c\in V} \mathscr{M}(c, D) = \sum_{c\in H} \frac{3^5 - 3^3 y(P)}{3^3 - x(P)^3}.$$

To determine $\mathrm{ord}_3(x(P))$ and $\mathrm{ord}_3(y(P))$, recall that the change of variables $x = u^2 X + r$, $y = 2u^3 Y$ where $r = -\frac{3}{2}\sqrt[3]{\frac{-13-3\sqrt{-3}}{2}}$ gives us a model of E having good reduction at 3 (see Proposition A.2 of Appendix A). In terms of X and Y, we have

$$\sum_{c\in V} \mathscr{M}(c, D) = \sum_{c\in H} \frac{3^5 - 2\cdot 3^3 u^3 Y(P)}{3^3 - r^3 - u^6 X(P)^3 - 3u^4 r X(P)^2 - 3u^2 r^2 X(P)}.$$

Now, P is a torsion of point of E of order prime to 3 and E has good reduction at 3 so $\mathrm{ord}_3(X(P)), \mathrm{ord}_3(Y(P)) \geqslant 0$. If $\mathrm{ord}_3(Y(P)) > 0$, P reduces to a 2-torsion after reduction modulo 3, but P is a D-torsion and reduction modulo 3 is injective, hence we must have $\mathrm{ord}_3(Y(P)) = 0$. Now, $\mathrm{ord}_3(3^3 - r^3) = \mathrm{ord}_3(3^3(1 - s^3))$, where $r = 3s$.

Also,

$$\begin{aligned}1 - s^3 &= 1 + \left(\frac{1}{2}\sqrt[3]{\frac{-13-3\sqrt{-3}}{2}}\right)^3\\ &= \frac{3-3\sqrt{-3}}{16},\end{aligned}$$

so $\operatorname{ord}_3(1-s^3) = 1$. In addition, we have $\operatorname{ord}_3(u) = \frac{3}{4}$ and $\operatorname{ord}_3(r) = 1$. Therefore, $\operatorname{ord}_3\left(u^6X(P)^3 + 3u^4rX(P)^2 + 3u^2r^2X(P)\right) > 4 = \operatorname{ord}_3(3^3 - r^3)$. It follows that

$$\begin{aligned}\operatorname{ord}_3\left(\sum_{c\in V}\mathscr{M}(c,D)\right) &\geqslant \operatorname{ord}_3(3^5) - \operatorname{ord}_3(3^3-r^3)\\ &= 1.\end{aligned}$$

On the other hand, by Proposition 2.3.8, we have $9 \mid \#(V)$. Hence,

$$\begin{aligned}\operatorname{ord}_3\left(\sum_{c\in V}\mathcal{E}_1^*\left(\frac{c\Omega}{D}+\frac{\Omega}{3},\mathcal{L}\right)\right) &= \min\left(\operatorname{ord}_3\left(\frac{1}{2}\sum_{c\in V}\mathscr{M}(c,D)\right),\operatorname{ord}_3(\#(V))\right)\\ &= 1\end{aligned}$$

as required. □

Recall from Remark 2.2.11 that $\frac{L(\overline{\psi},1)}{\Omega} = \frac{1}{3}$. It follows from Theorem 2.3.5 and Corollary 2.3.7 that

Theorem 2.3.9. *Let be a cube-free product of cubic special primes, and let n be the number of distinct prime factors of D in K. Then*

$$\operatorname{ord}_3(\Phi_{D^2}) \geqslant n.$$

We can generalise Definition 2.3.3 as follows.

Definition 2.3.10. Given a character $\chi : (\mathbb{Z}/3\mathbb{Z})^n \to \mathbb{C}^\times$, define

$$\Phi_{D^2}^{(\chi)} = \sum_{\alpha\in(\mathbb{Z}/3\mathbb{Z})^n}\chi(\alpha)\frac{L_{S_\alpha}(\overline{\psi}_{D_\alpha^2},1)}{\Omega}.$$

Using essentially the same arguments that are used to prove Theorem 2.3.9, we can show:

Lemma 2.3.11. *For any character $\chi : (\mathbb{Z}/3\mathbb{Z})^n \to \mathbb{C}^\times$, we have*

$$\mathrm{ord}_3(\Phi_{D^2}^{(\chi)}) \geqslant n.$$

Proof. By equation (2.3.1), we have

$$\chi(\alpha)\frac{L_S(\overline{\psi}_{D_\alpha^2}, 1)}{\Omega} = \frac{1}{3D}\sum_{\mathfrak{b}\in\mathcal{B}} \chi(\alpha)\left(\frac{D_\alpha}{\mathfrak{b}}\right)_3 \mathcal{E}_1^*\left(\frac{\Omega}{3D}, \mathcal{L}\right)^{\sigma_{\mathfrak{b}}}.$$

Also, by the law of cubic reciprocity, we have

$$\left(\frac{D_\alpha}{3c + D_\alpha}\right)_3 = \left(\frac{3c + D_\alpha}{D_\alpha}\right)_3 = \left(\frac{3c}{D_\alpha}\right)_3 = \left(\frac{c}{D_\alpha}\right)_3.$$

Let $n = n_\alpha$. Then we have a 1-dimensional character $\epsilon_3^{(\chi)}(\cdot, c) : (\mathbb{Z}/3\mathbb{Z})^n \to \boldsymbol{\mu}_3$ defined by $\epsilon_3^{(\chi)}(\alpha, c) = \chi(\alpha)\left(\frac{c}{D_\alpha}\right)_3$. Now, considering its inner product with the trivial character gives

$$\sum_{\alpha\in(\mathbb{Z}/3\mathbb{Z})^n} \epsilon_3^{(\chi)}(\alpha, c) = \begin{cases} 3^n & \text{if } c \in V^{(\chi)} \\ 0 & \text{otherwise,} \end{cases}$$

where $V^{(\chi)} = \{c \in \mathcal{C} \ : \left(\frac{c}{D_\alpha}\right)_3 = \chi(\alpha)^2 \text{ for all } \alpha \in (\mathbb{Z}/3\mathbb{Z})^n\}$. Thus

$$\Phi_{D^2}^{(\chi)} = 3^n \sum_{c\in V^{(\chi)}} \frac{1}{3D}\mathcal{E}_1^*\left(\frac{c\Omega}{D} + \frac{\Omega}{3}, \mathcal{L}\right).$$

Recall that for any prime π_j dividing D_α, we have $\left(\frac{\omega}{\pi_j}\right)_3 = 1$. Hence

$$\left(\frac{c}{D_\alpha}\right)_3 = \left(\frac{\omega c}{D_\alpha}\right)_3 = \left(\frac{\omega^2 c}{D_\alpha}\right)_3,$$

so $c \in V^{(\chi)}$ implies wc, $\omega^2 c \in V^{(\chi)}$. Also, the proof of Proposition 2.3.8 shows that $V^{(\chi)} = V_{(\alpha_1,\ldots,\alpha_n)}$ where $\alpha_i \in \{0, 1, 2\}$ is such that $\chi(e_i) = \omega^{\alpha_i}$, where $e_i \in (\mathbb{Z}/3\mathbb{Z})^n$ has 1 in the i-th entry and 0 elsewhere. Hence, $\#(V) = \#(V^{(\chi)})$ or $\#(V^{(\chi)}) = 0$, so in either case we have $9 \mid \#(V^{(\chi)})$. So we can apply the proofs of Theorem 2.3.6 and Corollary 2.3.7, and obtain

$$\mathrm{ord}_3\left(\sum_{c\in V^{(\chi)}} \mathcal{E}_1^*\left(\frac{c\Omega}{D} + \frac{\Omega}{3}, \mathcal{L}\right)\right) \geqslant 1,$$

so the result follows.

□

Remark 2.3.12. We note that the assumption $\mathrm{ord}_3(\pi - 1) \geqslant 2$ for any prime factors π of D is essential. If we take $\pi = 55 + 33\omega$ and $S = \{\pi\}$, then $\mathrm{ord}_3(\pi - 1) = \frac{3}{2}$ and $\mathrm{N}(\pi) \equiv 1 \bmod 27$. Then we have $\mathrm{ord}_3\left(\frac{L_S(\overline{\psi},1)}{\Omega}\right) = \frac{1}{2}$, but a computation shows $\frac{L(\overline{\psi}_{\pi^2},1)\sqrt[3]{\pi}}{\Omega} = 3$ and $\frac{L(\overline{\psi}_{\pi^4},1)\sqrt[3]{\pi^2}}{\Omega} = 289$, so that $\mathrm{ord}_3(\Phi_{\pi^2}) = 0$. Note also that we used $\pi \equiv 1 \bmod 9$ when showing $\left(\frac{3}{\pi}\right)_3 = 1$, which is not true when $\mathrm{ord}_3(\pi - 1) = \frac{3}{2}$.

Since we required that $\mathrm{ord}_3(\pi - 1) \geqslant 3$ and that 9 divides the order of $1 - \omega$ in $(\mathcal{O}_K/\pi\mathcal{O}_K)^\times$ for any prime π of K dividing D, we can improve the bound in Lemma 2.3.11 slightly by a similar proof. This can be found in Corollary A.5, Appendix A, and we will only use this in the case $n = 1$. We are ready to prove the second main result:

Theorem 2.3.13. *We have*

$$\mathrm{ord}_3\left(\frac{L(\overline{\psi}_{D^2},1)}{\Omega}\right) \geqslant \frac{1}{2}(n+1).$$

Proof. We prove this by induction on n. First, write $\alpha = (\alpha_1, \ldots, \alpha_n)$ for the element in $(\mathbb{Z}/3\mathbb{Z})^n$ with $D = D_\alpha$. Given $\beta, \gamma \in (\mathbb{Z}/3\mathbb{Z})^n$, we write $\beta < \gamma$ if $D_\beta \mid D_\gamma$ but $D_\beta \neq D_\gamma$. Let $n_\alpha = 1$ and $S_\alpha = \{\pi_1\}$, say. Then we consider

$$\Phi_{\pi_1^2} = \frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega} + \frac{L_{S_\alpha}(\overline{\psi}_{\pi_1^2},1)}{\Omega} + \frac{L_{S_\alpha}(\overline{\psi}_{\pi_1^4},1)}{\Omega},$$

where the last two terms are primitive. Also,

$$\begin{aligned}\frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega} &= \left(1 - \frac{\overline{\psi}((\pi_1))}{\pi_1\overline{\pi_1}}\right)\frac{L(\overline{\psi},1)}{\Omega}\\ &= \left(\frac{\pi_1 - 1}{\pi_1}\right)\frac{1}{3}\end{aligned}$$

and $\pi_1 \equiv 1 \bmod 9$. Hence $\mathrm{ord}_3\left(\frac{\pi_1-1}{\pi_1}\right) \geqslant 2$, and

$$\mathrm{ord}_3\left(\frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega}\right) \geqslant 2 - 1 = 1.$$

Now let $\chi_1 : \mathbb{Z}/3\mathbb{Z} \to \boldsymbol{\mu}_3$ be the character defined by $1 \mapsto \omega$ and let $\chi_2 : \mathbb{Z}/3\mathbb{Z} \to \boldsymbol{\mu}_3$ be the character defined by $1 \mapsto \omega^2$. Then we have

$$\Phi_{\pi_1^2}^{(\chi_i)} = \frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega} + \omega^i\frac{L_{S_\alpha}(\overline{\psi}_{\pi_1^2},1)}{\Omega} + \omega^{2i}\frac{L_{S_\alpha}(\overline{\psi}_{\pi_1^4},1)}{\Omega},$$

for $i = 1, 2$. Hence we obtain

$$\Phi_{\pi_1^2} - \omega\Phi_{\pi_1^2}^{(\chi_1)} = (1-\omega)\frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega} + (1-\omega^2)\frac{L_{S_\alpha}(\overline{\psi}_{\pi_1^2},1)}{\Omega}.$$

We know that $\mathrm{ord}_3(\Phi_{\pi_1^2} - \omega\Phi_{\pi_1^2}^{(\chi_1)}) \geqslant \frac{5}{4}$ (see Corollary A.5 of Appendix A), and we also checked that $\mathrm{ord}_3\left(\frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega}\right) \geqslant 1$, so $\mathrm{ord}_3\left((1-\omega)\left(\frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega}\right)\right) \geqslant \frac{3}{2}$. It follows that

$$\mathrm{ord}_3\left((1-\omega^2)\left(\frac{L_{S_\alpha}(\overline{\psi}_{\pi_1^2},1)}{\Omega}\right)\right) \geqslant \frac{5}{4},$$

that is,

$$\mathrm{ord}_3\left(\frac{L_{S_\alpha}(\overline{\psi}_{\pi_1^2},1)}{\Omega}\right) \geqslant \frac{3}{4}.$$

But $\frac{L_{S_\alpha}(\overline{\psi}_{\pi_1^2},1)\sqrt[3]{\pi_1^2}}{\Omega} \in K$ so $\mathrm{ord}_3\left(\frac{L_{S_\alpha}(\overline{\psi}_{\pi_1^2},1)}{\Omega}\right)$ must be an integer multiple of $\frac{1}{2}$. Hence

$$\mathrm{ord}_3\left(\frac{L_{S_\alpha}(\overline{\psi}_{\pi_1^2},1)}{\Omega}\right) \geqslant 1 = \frac{1}{2}(n_\alpha + 1)$$

as required.

Now suppose the result holds for all $n_\beta < n_\alpha$, where $\beta < \alpha$. We have

$$\Phi_{D_\alpha^2} = \frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega} + \sum_{n_\beta < n_\alpha}\frac{L_{S_\alpha}(\overline{\psi}_{D_\beta^2},1)}{\Omega} + \sum_{n_\gamma = n_\alpha}\frac{L_{S_\alpha}(\overline{\psi}_{D_\gamma^2},1)}{\Omega}$$

where the terms in the last summand are primitive.

We know that

$$\begin{aligned}\frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega} &= \prod_{\pi\in S_\alpha}\left(1 - \frac{\overline{\psi}((\pi))}{\pi\overline{\pi}}\right)\frac{L(\overline{\psi},1)}{\Omega}\\ &= \prod_{\pi\in S_\alpha}\left(\frac{\pi-1}{\pi}\right)\frac{1}{3}\end{aligned}$$

and $\pi \equiv 1 \bmod 27$, so $\mathrm{ord}_3\left(\frac{L_{S_\alpha}(\overline{\psi},1)}{\Omega}\right) \geqslant 3n_\alpha - 1$. Next, for $n_\beta < n_\alpha$, we have

$$\frac{L_{S_\alpha}(\overline{\psi}_{D_\beta^2},1)}{\Omega} = \prod_{\pi\in S_\alpha\setminus S_\beta}\left(1 - \frac{\overline{\psi}_{D_\beta^2}((\pi))}{\pi\overline{\pi}}\right)\frac{L(\overline{\psi}_{D_\beta^2},1)}{\Omega}$$

and $\psi_{D_\beta^2}((\pi)) = \left(\frac{D_\beta}{\pi}\right)_3 \pi = \omega^i \pi$, $i \in \{0,1,2\}$. Furthermore, by the induction hypothesis, $\mathrm{ord}_3\left(\frac{L(\overline{\psi}_{D_\beta^2},1)}{\Omega}\right) \geqslant \frac{1}{2}(n_\beta + 1)$. It follows that

$$\begin{aligned}\mathrm{ord}_3\left(\sum_{n_\beta < n_\alpha} \frac{L_{S_\alpha}(\overline{\psi}_{D_\beta^2},1)}{\Omega}\right) &\geqslant \frac{1}{2}(n_\alpha - n_\beta) + \frac{1}{2}(n_\beta + 1)\\ &= \frac{1}{2}(n_\alpha + 1).\end{aligned}$$

We also know by Lemma 2.3.11 that $\mathrm{ord}_3(\Phi_{D_\alpha^2}^{(\chi)}) \geqslant n_\alpha$ for any character $\chi : (\mathbb{Z}/3\mathbb{Z})^n \to \boldsymbol{\mu}_3$.

To find $\mathrm{ord}_3\left(\frac{L(\overline{\psi}_{D_\gamma^2},1)}{\Omega}\right)$ for $\gamma = (\gamma_1, \ldots, \gamma_n) \in (\mathbb{Z}/3\mathbb{Z})^n$ with $n_\gamma = n_\alpha$, suppose first that $\gamma \neq (2, \ldots, 2)$, so there exists $j \in \{1, \ldots n\}$ with $\gamma_j = 1$. Without loss of generality, we may assume $j = 1$. Let $\chi_1 : (\mathbb{Z}/3\mathbb{Z})^n = \langle g_1, \ldots, g_n \rangle \to \boldsymbol{\mu}_3$ be the character defined by $\chi_1(g_1) = \omega$ and $\chi_1(g_j) = 1$ for $j = 2, \ldots, n$, and let $\chi_2 : (\mathbb{Z}/3\mathbb{Z})^n = \langle g_1, \ldots, g_n \rangle \to \boldsymbol{\mu}_3$ be the character defined by $\chi_2(g_1) = \omega^2$ and $\chi_2(g_j) = 1$ for $j = 2, \ldots, n$. Then, by writing out $\Phi_{D_\alpha} - \omega\Phi_{D_\alpha}^{(\chi_1)}$ explicitly, we see that $\mathrm{ord}_3\left(\sum_{\substack{n_\gamma < n_\alpha\\ \gamma_j = 1}} \frac{L(\overline{\psi}_{D_\gamma^2},1)}{\Omega}\right) \geqslant \frac{1}{2}(n_\alpha + 1)$ for any $j = 1, \ldots, n$, and similarly $\mathrm{ord}_3\left(\sum_{\substack{n_\gamma < n_\alpha\\ \gamma_j = 2}} \frac{L(\overline{\psi}_{D_\gamma^2},1)}{\Omega}\right) \geqslant \frac{1}{2}(n_\alpha + 1)$ for any $j = 1, \ldots, n$.

Now let χ_2 be the character defined by $g_1 \mapsto \omega$, $g_2 \mapsto \omega$ and $g_j \mapsto 1$ for $j \neq 1, 2$, and let χ_3 be the character defined by $g_1 \mapsto \omega^2$, $g_2 \mapsto \omega$ and $g_j \mapsto 1$ for $j \neq 1, 2$. Then an easy calculation gives

$$\begin{aligned}(\Phi_{D_\alpha}^{(\chi_2)} - \omega\Phi_{D_\alpha}^{(\chi_3)}) - (\Phi_{D_\alpha} - \omega\Phi_{D_\alpha}^{(\chi_1)}) = 3\omega &\sum_{\substack{n_\beta < n_\alpha\\ \beta_1 = 0, \beta_2 = 1}} \frac{L_{S_\alpha}(\overline{\psi}_{D_\beta^2},1)}{\Omega} - 3 \sum_{\substack{n_\beta < n_\alpha\\ \beta_1 = 0, \beta_2 = 2}} \frac{L_{S_\alpha}(\overline{\psi}_{D_\beta^2},1)}{\Omega}\\ - 3 &\sum_{\substack{n_\beta < n_\alpha\\ \beta_1 = 1, \beta_2 = 0}} \frac{L_{S_\alpha}(\overline{\psi}_{D_\beta^2},1)}{\Omega} + 3\omega^2 \sum_{\substack{n_\beta < n_\alpha\\ \beta_1 = 1, \beta_2 = 1}} \frac{L_{S_\alpha}(\overline{\psi}_{D_\beta^2},1)}{\Omega}\\ + 3\omega^2 &\sum_{\substack{n_\gamma = n_\alpha\\ \gamma_1 = 1, \gamma_2 = 1}} \frac{L(\overline{\psi}_{D_\gamma^2},1)}{\Omega}.\end{aligned}$$

So we have

$$\operatorname{ord}_3\left(\sum_{\substack{n_\gamma=n_\alpha\\ \gamma_1=1,\gamma_2=1}}\frac{L(\overline{\psi}_{D_\gamma^2},1)}{\Omega}\right)\geqslant\frac{1}{2}(n_\alpha+1).$$

Similarly, we can show

$$\operatorname{ord}_3\left(\sum_{\substack{n_\gamma=n_\alpha\\ \gamma_i=e_i,\gamma_j=e_j}}\frac{L(\overline{\psi}_{D_\gamma^2},1)}{\Omega}\right)\geqslant\frac{1}{2}(n_\alpha+1)$$

for any $e_i, e_j \in \{1,2\}$ with $i \neq j$. Now we claim the following:

Lemma 2.3.14. *Let $\gamma \in (\mathbb{Z}/3\mathbb{Z})^n$ be such that $n_\gamma = n_\alpha$. Then for any $J \subset \{1,\dots,n\}$ and any $e_j \in \{1,2\}$ for $j \in J$, we have*

$$\operatorname{ord}_3\left(\sum_{\substack{\gamma_j=e_j\\ j\in J}}\frac{L(\overline{\psi}_{D_\gamma^2},1)}{\Omega}\right)\geqslant M,$$

where $M \in \mathbb{Q}$ is such that $\operatorname{ord}_3\left(\sum_{\substack{\gamma\in(\mathbb{Z}/3\mathbb{Z})^n\\ n_\gamma=n_\alpha}}\frac{L(\overline{\psi}_{D_\gamma^2},1)}{\Omega}\right)\geqslant M.$

Proof. We prove this by induction on $|J|$. The cases $|J| = 1,2$ were established above. Given $J \subset \{1,\dots,n\}$ and $e_j \in \{1,2\}$ for $j \in J$, let X_J denote the sum

$$X_J := \sum_{\substack{\gamma_j=e_j\\ j\in J}}\frac{L(\overline{\psi}_{D_\gamma^2},1)}{\Omega}.$$

Now suppose the lemma is true for any $J \subset \{1,\dots,n\}$ with $|J| = k > 1$. Then let $|J| = k+1$, and without loss of generality, we may assume $J = \{1,\dots,k+1\}$. Pick $e_j \in \{1,2\}$ for $j \in J$. Then by the induction hypothesis, $\operatorname{ord}_3(X_{\{1,\dots,k\}}) \geqslant M$ and $\operatorname{ord}_3(X_{\{2,\dots,k+1\}}) \geqslant M$. Now,

$$\begin{aligned}X_{\{1,\dots,k\}}-X_{\{2,\dots k+1\}} &= \sum_{\substack{\gamma_j=\epsilon_j j\in\{2,\dots k\}\\ \gamma_1=e_1,\gamma_{k+1}\neq e_{k+1}}}\frac{L(\overline{\psi}_{D_\gamma^2},1)}{\Omega}-\sum_{\substack{\gamma_j=\epsilon_j j\in\{2,\dots k\}\\ \gamma_1\neq e_1,\gamma_{k+1}=e_{k+1}}}\frac{L(\overline{\psi}_{D_\gamma^2},1)}{\Omega}\\ &= A-B,\end{aligned}$$

say. Now, $A+B+X_J = X_{\{2,\ldots,k\}}$ so $\mathrm{ord}_3(A+B+X_J) \geqslant M$. On the other hand, $X_{\{1,\ldots k\}} + X_{\{2,\ldots k+1\}} = A+B+2X_J$ so $\mathrm{ord}_3(A+B+2X_J) \geqslant M$. It follows that $\mathrm{ord}_3(X_J) \geqslant M$ as required. □

Hence applying the above lemma with $J = \{1,\ldots,n\}$, we see that for any $\gamma \in (\mathbb{Z}/3\mathbb{Z})^n$ and $n_\gamma = n_\alpha$, we have

$$\mathrm{ord}_3\left(\frac{L(\overline{\psi}_{D^2_\gamma},1)}{\Omega}\right) \geqslant \frac{1}{2}(n_\alpha+1)$$

and the result follows. □

The following is an immediate consequence of Theorem 2.3.13.

Theorem 2.3.15. *Let $D>1$ be an integer which is a cube-free product of cubic-special primes. Then*

$$\mathrm{ord}_3\left(L^{(alg)}\left(E(D^2),1\right)\right) \geqslant k(D)+1,$$

where $k(D)$ is the number of distinct rational prime factors of D.

Proof. The number of distinct primes in K dividing D is twice the number of distinct rational primes dividing D, so by Theorem 2.3.13,

$$\mathrm{ord}_3\left(L^{(\mathrm{alg})}\left(\overline{\psi}_{D^2},1\right)\right) \geqslant \frac{1}{2}(2(k(D)+1)) = k(D)+\frac{1}{2}.$$

But we know $L^{(\mathrm{alg})}\left(\overline{\psi}_{D^2},1\right) \in \mathbb{Q}$, so $\mathrm{ord}_3\left(L^{(\mathrm{alg})}\left(\overline{\psi}_{D^2},1\right)\right) \geqslant k(D)+1$ as required. □

Remark 2.3.16. The bound in Theorem 2.3.15 is sharp. For example, let $\pi = 28+27\omega$ and let $D = \mathrm{N}(\pi) = 757$, which is a rational prime. Then we have $L^{(\mathrm{alg})}(E(D^2),1) = 9$ so $\mathrm{ord}_3\left(L^{(\mathrm{alg})}(E(D^2),1)\right) = 2$.

In fact, the numerical examples listed in Appendix B suggest that Theorem 2.3.15 is true whenever $D>1$ is an odd integer congruent to 1 modulo 9 whose prime factors are congruent to 1 modulo 3. Finally, we note that the condition $D \equiv 1 \bmod 9$ is not sufficient. Indeed, for $D = 55$ we have $L^{(\mathrm{alg})}(E(D^2),1) = 3$.

Chapter 3

Descent Theory

3.1 Introduction

Take q to be any prime number with $q \equiv 7 \bmod 8$. Let $K = \mathbb{Q}(\sqrt{-q})$, and fix an embedding $K \hookrightarrow \mathbb{C}$. Let E be an elliptic curve over $\mathbb{C}$ with $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}$, the ring of integers of K. Since K has prime discriminant, the class number, which we denote by h, is odd. In the case $q = 7$, we can take E to be any quadratic twist of the elliptic curve $A = X_0(49)$ with equation

$$A : y^2 + xy = x^3 - x^2 - 2x - 1.$$

In this case, we have the following result due to Gonzalez-Avilés and Rubin, using Iwasawa theory.

Theorem 3.1.1. *Let E be a quadratic twist of the elliptic curve $A = X_0(49)$. If $L(E/\mathbb{Q}, 1) \neq 0$, then the full Birch–Swinnerton-Dyer conjecture holds for E.*

The proof relies heavily on the fact that 2 is a potentially ordinary prime for E. This is the only family of quadratic twists of elliptic curves with complex multiplication defined over $\mathbb{Q}$ for which 2 is a potentially ordinary prime, since $q = 7$ is the only case in which K has class number one. In general, the theory of complex multiplication tells us that the modular invariant $j(\mathcal{O})$ is a real number which satisfies an irreducible equation of degree h over K, and the Hilbert class field H of K is given by $H = K(j(\mathcal{O}))$. Given a rational prime p, the theory of complex multiplication tells us that E has potentially good ordinary reduction at all primes of H above p if and only if p splits in K.

Definition 3.1.2. We say a prime number p satisfies the *good ordinary hypothesis for E* if E has good ordinary reduction at all primes of H above p, and p splits in K.

From now on, let p be a prime number satisfying the good ordinary hypothesis for E, and write $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$. We also define

$$J = H \cap \mathbb{R} = \mathbb{Q}(j(\mathcal{O})),$$

which satisfies $[H : J] = 2$. Then for any prime number q with $q \equiv 7 \bmod 8$, Gross showed that there exists an elliptic curve $A(q)$ which is defined over J with $\mathrm{End}_H(E) = \mathcal{O}$, such that in the simplest case $q = 7$ we have $A(7) = X_0(49)$. We define $A(q)$ by constructing a Grössencharacter ψ_q of H. Let $\mathfrak{a}$ be an integral ideal of H. Define ψ_q to be the unique Grössencharacter with conductor $(\sqrt{-q})$ such that, if $\mathfrak{a}$ is an integral ideal of H with $(\mathfrak{a}, q) = 1$, then

$$\psi_q(\mathfrak{a}) = \alpha,$$

where α is the unique generator of the principal ideal $\mathrm{N}_{H/K}(\mathfrak{a})$ which is a square in $\mathcal{O}/\sqrt{-q}\mathcal{O}$. In particular, we have

$$\sigma(\psi_q) = \psi_q \text{ for all } \sigma \in \mathrm{Gal}(H/\mathbb{Q}).$$

This defines an isogeny class of elliptic curves defined over H with Grössencharacter ψ_q, j-invariant equal to $j(\mathcal{O})$ and complex multiplication by $\mathcal{O}$. The following theorem of Gross shows that we can pick out a special curve $A(q)$ in this isogeny class.

Theorem 3.1.3. *There exist a unique elliptic curve $A(q)$ defined over J with Grössencharacter $\psi_{A(q)/H} = \psi_q$ such that $\mathrm{End}_H(A(q)) = \mathcal{O}$, $j(A(q)) = j(\mathcal{O})$ and the minimal discriminant ideal is equal to $(-q^3)$.*

We will see in Lemma 3.1.9 that $A(q)$ is isogeneous to its conjugates $A(q)^\sigma$ with $\sigma \in \mathrm{Aut}(H)$, hence it is a $\mathbb{Q}$-curve.

In addition, Gross found an explicit equation for $A(q)$ over J. Let us consider a generalised Weierstrass equation of $A(q)$ of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in H$. Let $\Delta(A(q))$ denote the discriminant for this equation. We will show that we can have $a_i \in J$ with $\Delta(A(q)) = -q^3$. In order to do this, given an integral ideal $\mathfrak{a}$ of $\mathcal{O}$, let $\sigma_{\mathfrak{a}}$ denote the image of $\mathfrak{a}$ via the Artin isomorphism from the ideal class group of K to $\mathrm{Gal}(H/K)$, and let $\lambda(\mathfrak{a})$ denote the unique isogeny from $A(q)$ to

$B = A(q)^{\sigma_{\mathfrak{a}}}$ of degree $\mathrm{N}\mathfrak{a}$ defined over H, characterised by

$$\lambda(\mathfrak{a})(\mathfrak{u}) = \sigma_{\mathfrak{a}}(\mathfrak{u})$$

for any $\mathfrak{u} \in A(q)[\mathfrak{c}]$ with $(\mathfrak{c}, \mathfrak{a}) = 1$. Let x', y' be the coordinates of any generalised Weierstrass equation for B, and let $\Delta(B)$ be the discriminant of this equation. We write

$$\omega_{A(q)} = \frac{dx}{2y + a_1 x + a_3}, \quad \omega_B = \frac{dx'}{2y' + a_1' x' + a_3'}$$

for the Néron differentials. Then we see that the value $\Lambda(\mathfrak{a}) \in H^\times$ defined by

$$\lambda(\mathfrak{a})^*(\omega_B) = \Lambda(\mathfrak{a})\omega_{A(q)}$$

is such that $\Delta(B)\Lambda(\mathfrak{a})^{12}$ is independent of the choice of Weierstrass equation for B. Further, it is shown in [3, Appendix, Theorem 8] that there exists a unique $c_{A(q)}(\mathfrak{a}) \in H^\times$ such that $c_{A(q)}(\mathfrak{a})$ gives a canonical 12th root in H of

$$\frac{\Delta(A(q))^{\deg \lambda(\mathfrak{a})}}{\Delta(B)\Lambda(\mathfrak{a})^{12}} = \frac{\Delta(A(q))^{\mathrm{N}\mathfrak{a}-1}}{\Lambda(\mathfrak{a})^{12}}.$$

Taking appropriate values for $\mathfrak{a}$, we see in particular that $\Delta(A(q))$ has a 6th root in H. Now, recall that

$$j(A) = \frac{c_4^3}{\Delta(A(q))} = 1728 + \frac{c_6^2}{\Delta(A(q))},$$

where $c_4, c_6 \in H$ are the values defined in [13, §1]. This shows that $j(A(q))$ has a cube root in H and $j(A(q)) - 1728$ has a square root in H. Note that the only roots of unity in H are ± 1, so $j(A(q))$ in fact has a cube root in J. Now we have the following.

Theorem 3.1.4. *The curve $A(q)$ has a model over J*

$$y^2 = x^3 + \frac{mq}{2^4 \cdot 3}x - \frac{nq^2}{2^5 \cdot 3^3} \quad \textit{where} \tag{3.1.1}$$
$$m^3 = j(A(q)) \quad \textit{and} \quad n^2 = \frac{j(A(q)) - 1728}{-q},$$

with discriminant equal to $-q^3$. Here, we take the positive square root for n.

Proof. The arguments above show that $m \in J$, and $n \in H$ since we also have $\sqrt{-q} \in K \subset H$. But $j(A(q)) - 1728$ and $-q$ are both negative, so $n \in J$ as well. An easy computation then shows that indeed the curve defined by equation (3.1.1) has discriminant $-q^3$ and j–invariant equal to $j(A(q))$. Now, [14, Proposition 3.5] shows that there is an isomorphism over J from this curve to $A(q)$. This concludes the proof of the theorem. □

The coefficients of the (3.1.1) are integral in J, expect perhaps at 2 and 3. It is not known in general how to write a global minimal equation for $A(q)$ over$J$ explicitly for $q > 7$, although Gross has shown that it exists over J (see [14, Proposition 3.2]).

A classical 2-descent shows that, for $A(7) = X_0(49)$, we have

$$A(7)(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}, \;\; A(7)(K) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \;\; Ш(A(7)/\mathbb{Q})(2) = 0.$$

Gross generalised this result to show that, for all $q \equiv 7 \bmod 8$, we have [13, Theorem 22.4.1]:

$$A(q)(J) = \mathbb{Z}/2\mathbb{Z}, \;\; A(q)(H) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \;\; Ш(A(q)/J)(2) = 0.$$

There is one additional property of the curves $A(q)$ which is important in carrying out arguments of Iwasawa theory for them. Let $A(q)_{\mathrm{tor}}$ denote the torsion subgroup of $A(q)(\overline{J})$. It is clear from the theory of complex multiplication that $H(A(q)_{\mathrm{tor}})$ is an abelian extension of H. We have the following stronger result:

Theorem 3.1.5. *The field $H(A(q)_{tor})$ is an abelian extension of K.*

Proof. Let $\varphi_{A(q)}$ be a Grössencharacter of K with conductor $(\sqrt{-q})$ such that, if $\mathfrak{b}$ is an integral ideal of K with $(\mathfrak{b}, q) = 1$,

$$\varphi_{A(q)}(\mathfrak{b}) = \beta$$

where $\beta^h = \alpha$ is in K^*, $(\alpha) = \mathfrak{b}^h$ and α is a square mod $\sqrt{-q}$. Then $\varphi_{A(q)}$ satisfies

$$\psi_{A(q)/H} = \varphi_{A(q)} \circ \mathrm{N}_{H/K}.$$

A theorem of Shimura [19, Theorem 7.44] states that the existence of such a Grössencharacter $\varphi_{A(q)}$ is equivalent to $H(A(q)_{\mathrm{tor}})$ being an abelian extension of K. □

In what follows, we want to consider the arithmetic of the Birch–Swinnerton-Dyer conjecture for as large class as possible of quadratic twists of the curve $A(q)$ defined over J. In addition, it will be vital that such a quadratic twist E is such that $H(E_{\mathrm{tor}})/K$ is an abelian extention. From now on, assume E is a quadratic twist of $A(q)$ by a quadratic extension of H of the form $H(\sqrt{\lambda})$, where λ is some non-zero element of K and the discriminant of $H(\sqrt{\lambda})/H$ is prime to $2q$. Thus, in particular, E has good ordinary reduction at the primes of H above 2. We will show that under this condition, the extension $H(E_{\mathrm{tor}})/K$ is abelian.

Theorem 3.1.6. *We have*

$$\psi_{E/H} = \varphi_K \circ \mathrm{N}_{H/K},$$

where φ_K is a Grössencharacter of K.

Proof. We have remarked that $\psi_{A(q)/H} = \varphi_{A(q)} \circ \mathrm{N}_{H/K}$. Now, E is a twist of $A(q)$ by a quadratic extension $\mathcal{M}$ of H which we assumed to be of the form HM where M is a quadratic extension of K. Let $\chi_{\mathcal{M}}$ (resp. χ_M) be the quadratic character of H (resp. K) defining $\mathcal{M}$ (resp M). Then we have $\chi_{\mathcal{M}} = \chi_M \circ \mathrm{N}_{H/K}$ by class field theory. Now, since $\mathcal{M}/H$ has discriminant prime to p, we have $\psi_{E/H} = \psi_{A(q)/H}\chi_{\mathcal{M}}$. It follows that we can take $\varphi_K = \varphi_{A(q)}\chi_M$. □

Applying [19, Theorem 7.44] to the above theorem, we immediately obtain:

Corollary 3.1.7. *The field $H(E_{tor})$ is abelian over K.*

Write G for the Galois group of H over K and $\mathfrak{g}$ for the conductor of φ_K.

Lemma 3.1.8. *For all $a \in K$ with $(a, \mathfrak{g}) = 1$, we have*

$$\varphi_K(\overline{a}) = \overline{\varphi}_K(a).$$

Proof. Since E is defined over J, we have $\psi_{E/H} = \rho \circ \psi_{E/H} \circ \rho^{-1}$, where ρ denotes complex conjugation. This gives $(\rho \circ \varphi_K \circ \rho^{-1}) \circ \mathrm{N}_{H/K} = \varphi_K \circ \mathrm{N}_{H/K}$, and $\rho \circ \varphi_K \circ \rho^{-1} = \varphi_K \cdot \sigma$ for some $\sigma \in G$. Since $\sigma(\overline{a}) = \overline{\sigma}(a)$ for any σ, we have $\rho \circ \sigma \circ \rho^{-1} = \sigma$, and thus conjugating φ_K by ρ twice gives $\varphi_K = \varphi_K \cdot \sigma^2$. This gives $\sigma^2 = 1$, and finally $\sigma = 1$ since $[H : K]$ is odd by assumption. □

Lemma 3.1.9. *E is isogeneous over H to all of its conjugates under G.*

Proof. Suppose $\sigma \in G$. Then the Grössencharacter of E^σ over H is $\psi_{E/H} \circ \sigma^{-1}$. But, since $\psi_{E/H} = \varphi_K \circ \mathrm{N}_{H/K}$, we see that $\psi_{E/H} = \psi_{E^\sigma/H}$. Hence, E and E^σ have isomorphic Galois representations on their Tate modules, and so, they are isogenous over H by Faltings' theorem [9, Corollary 3]. □

In particular, this shows that $A(q)$ is isogeneous to all of its conjugates under $\mathrm{Gal}(H/\mathbb{Q})$, since it is defined over J, the fixed field of H under complex conjugation

$\rho \in \mathrm{Gal}(H/\mathbb{Q})$. Given an ideal $\mathfrak{b}$ of $\mathcal{O}$ prime to the conductor $\mathfrak{g}$ of the Grössencharacter φ_K, let $\sigma_{\mathfrak{b}}$ prime to $\mathfrak{g}$, let $\sigma_{\mathfrak{b}}$ be the Artin symbol of $\mathfrak{b}$ in H/K. Then in view of Lemma 3.1.9, there exists a unique H-isogeny

$$\lambda_{E^\sigma}(\mathfrak{b}) : E^\sigma \to E^{\sigma\sigma_{\mathfrak{b}}}$$

whose kernel is $E^\sigma_{\mathfrak{b}}$. This is obtained by restricting the Serre–Tate character of the abelian variety B/K [18, Theorem 10], which is the restriction of scalars of E from H to K. See [13] for more detailed account.

3.2 Descent theory over H

Recall that p is a prime satisfying the good ordinary hypothesis for E. We write $p\mathcal{O} = \mathfrak{p}\mathfrak{p}^*$, and write π for the element in $\mathcal{O}$ with $\mathfrak{p}^h = \pi\mathcal{O}$, where $h = [H : K]$. We first discuss descent theory for E over H. We need the following notation. If α is any non-zero element in $\mathcal{O}$, we write $E_\alpha = \ker\left(E(\overline{H}) \xrightarrow{[\alpha]} E(\overline{H})\right)$ for the kernel of the multiplication-by-α map $[\alpha]$. Similarly, if $\mathfrak{a}$ is any non-zero ideal of $\mathcal{O}$, we write

$$E_{\mathfrak{a}} = \bigcap_{\alpha \in \mathfrak{a}\setminus\{0\}} E_\alpha.$$

As $\mathcal{O}$-modules, we have $E_\alpha = \mathcal{O}/\alpha\mathcal{O}$ and $E_{\mathfrak{a}} = \mathcal{O}/\mathfrak{a}$. Let P denotes the set of primes of H lying above $\mathfrak{p}$. If v is any place of H, we write H_v for the completion of H at v, and write $\mathcal{O}_v$ for its ring of integers.

Before proceeding to study descent over various extensions of H, we make an observation that in the case $q = 7$, we have $H = K$, so that for every place v of H where E has good reduction, the formal group $\widehat{E}$ of E at v is a Lubin–Tate group of E over H_v. However, if $q > 7$, this is no longer true because $\psi_{E/H}(v)$ will no longer be a local parameter of H_v is general. We first briefly discuss how one handles with this situation.

Let v be any place of H lying above a prime w of K such that E has good reduction at v, and let $\sigma_v \in G$ be the Frobenius at v. Let $\lambda_E(v)$ denote the unique isogeny

$$\lambda_E(v) : E \to E^{\sigma_v},$$

induced by the isogeny $\lambda_E(w)$. We remark that the isogeny $\lambda_E(v)$ is defined by the same formulae which define the isogeny $\lambda(v) : A \to A^{\sigma_{\mathfrak{v}}}$. To see this, recall the notations in the proof of Theorem 3.1.6 and let τ be the nontrivial element of $\mathrm{Gal}(\mathcal{M}/H)$. Then

$E(H)$ is isomorphic to the -1 eigenspace for the action of $\mathrm{Gal}(\mathcal{M}/H)$ on $A(\mathcal{M})$, i.e. the points on $A(\mathcal{M})$ on which τ acts as -1. But we have $\lambda(v)(-P) = -\lambda(v)(P)$ since isogeny preserves the group law, and also we clearly have $\chi_{\mathcal{M}}(\tau) = -1$. Hence $\lambda(v)$ is independent of twist by $\chi_{\mathcal{M}}$.

This induces a homomorphism

$$\widehat{\lambda}_E(v) : \widehat{E} \to \widehat{E}^{\sigma_v},$$

of formal groups of the curves E and E^{σ_v} at v, defined over the ring of integers $\mathcal{O}_v$ of H_v. Thus, we can view $\widehat{\lambda}_E(v)$ as an element of $\mathcal{O}_v[[t]]$ satisfying

$$\widehat{\lambda}_E(v)(t) \equiv \Lambda(v)t \bmod \text{degree } 2, \;\; \widehat{\lambda}_E(v) \equiv t^q \bmod v,$$

where $\Lambda(v)$ is an element of $\mathcal{O}_v$ and q denotes the cardinality of the residue field of the restriction w of v to K. Now, we can apply σ_v^i for $i = 1, \ldots, f_v$, where f_v denotes the residue degree of v in H/K, to $\lambda_E(v)$ and $\widehat{\lambda}_E(v)$. Then we see that

$$\mathrm{N}_{H_v/K_w}\Lambda(v) = \psi_{E/H}(v),$$

since $\prod_{i=1}^{f_v} \sigma_v^i \lambda_E(v)$ is the unique element of $\mathrm{End}_H(E) = \mathcal{O}$ which reduces modulo v to the Frobenius endomorphism at v. Thus $\widehat{E}$ is not itself a Lubin–Tate group, but $\widehat{E}$ together with the homomorphism $\widehat{\lambda}_E(v) : \widehat{E} \to \widehat{E}^{\sigma_v}$ is a relative Lubin–Tate group, which was studied by de Shalit in [8, I §1]. The theory of Lubin–Tate groups generalises to relative Lubin–Tate groups, and in particular, we have the following:

Theorem 3.2.1. *Let v be any place of H where E has good reduction, and let w be its restriction to K. Then for any $n \geqslant 1$, the extension $H_v(E_{w^n})/H_v$ is totally ramified, and its Galois group is isormphic to $(\mathcal{O}/w^n)^\times$.*

Now, E has good ordinary reduction at the primes of H above $\mathfrak{p}$. We define $F_n = H(E_{\mathfrak{p}^n})$, and $F = F_2$ or F_1, according as $p = 2$ or $p > 2$. Set

$$F_\infty = H(E_{\mathfrak{p}^\infty}), \quad \mathfrak{H} = \mathrm{Gal}(F_\infty/H).$$

Then by Theorem 3.2.1, we have a character $\chi_{\mathfrak{p}} : \mathfrak{H} \to \mathcal{O}_{\mathfrak{p}}^\times = \mathbb{Z}_p^\times$ giving the action of $\mathfrak{H}$ on $E_{\mathfrak{p}^\infty}$, which is an isomorphism. We write $\mathfrak{H} = \Delta \times \Gamma$, where $\Delta = \mathrm{Gal}\,(F/H)$, is cyclic of order 2 or $p-1$ according as $p = 2$ or $p > 2$ by Theorem 3.2.1 and $\Gamma = \mathrm{Gal}\,(F_\infty/F)$ is isomorphic to $\mathbb{Z}_p$.

Theorem 3.2.2. *E has good reduction everywhere over F.*

Proof. Let $\varepsilon_{E/H}$ (resp. $\varepsilon_{E/F}$) be the Serre–Tate homomorphisms attached to E over H (resp. F). Thus $\varepsilon_{E/F} = \varepsilon_{E/H} \circ \mathrm{N}_{F/H}$, where $N_{F/H} : \mathbb{A}_F^\times \to \mathbb{A}_H^\times$ is the norm map from the idèle group of F to the idèle group of H. Now, E has good reduction at all places of F above p by hypothesis. Let v be any place of F which does not lie above p, and let U_v be the units of the ring of integers of the completion of F at v. Then by [18, §7, Corollary 1] E will have good reduction at v if and only if $\varepsilon_{E/F}(U_v) = 1$. Let w be the restriction of v to H. Then

$$\varepsilon_{E/F}(U_v) = \varepsilon_{E/H}(\mathrm{N}_{F_v/H_w} U_v).$$

Let $\xi_H : \mathbb{A}_H^\times \to \mathrm{Gal}(H^{\mathrm{ab}}/H)$ denote Artin's global recipricity map. Then, by class field theory, $\xi_H(\mathrm{N}_{F_v/H_w} U_v)$ fixes F. Hence our lemma will follow from the following lemma. □

Lemma 3.2.3. *If x is a unit in the ring of integers U_w of H_w and $\xi_H(x)$ fixes F, then $\varepsilon_{E/H}(x) = 1$.*

Proof. By local class field theory, $\xi_H(U_w)$ is the inertia subgroup of w in $\mathrm{Gal}(H^{\mathrm{ab}}/H)$. Since E has potential good reduction at w, it follows that $\chi_{\mathfrak{p}}(\xi_H(x))$ is a root of unity in $\mathcal{O}_{\mathfrak{p}}^\times$ for all x in U_w by the criterion of Néron–Ogg–Shafarevich. On the other hand, for all x in $\mathbb{A}_H^\times$ which fix F, we must have $\chi_{\mathfrak{p}}(\xi_H(x))$ belongs to $1 + \mathfrak{p}^i$ where $i = 2$ if $p = 2$ and $i = 1$ otherwise. But $1 + \mathfrak{p}^i$ contains no root of unity other than 1. Hence we have $\chi_{\mathfrak{p}}(\xi_H(x)) = 1$ when x lies in U_w. But $\varepsilon_{E/H}(x) = \chi_{\mathfrak{p}}(\xi_H(x))$, completing the proof. □

For each $n \geqslant 1$, we introduce the following Selmer groups:

$$\mathrm{Sel}_{\pi^n}(E/H) = \ker\left(H^1(H, E_{\pi^n}) \to \prod_v (H^1(H_v, E))_{\pi^n}\right)$$
$$\mathrm{Sel}'_{\pi^n}(E/H) = \ker\left(H^1(H, E_{\pi^n}) \to \prod_{v \notin P} (H^1(H_v, E))_{\pi^n}\right).$$

We define

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(E/H) = \varinjlim \mathrm{Sel}_{\pi^n}(E/H)$$
$$\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/H) = \varinjlim \mathrm{Sel}'_{\pi^n}(E/H),$$

where the inductive limits are taken with respect to the inclusions $E_{\pi^n} \to E_{\pi^{n+1}}$.

We also let $T = P \cup B$ where B denotes the set of primes of H where E has bad reduction, and similarly define

$$\mathrm{Sel}^{(T)}_{\pi^n}(E/H) = \ker\left(H^1(H, E_{\pi^n}) \to \prod_{v \notin T}(H^1(H_v, E))_{\pi^n}\right)$$

$$\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H) = \varinjlim \mathrm{Sel}^{(T)}_{\pi^n}(E/H).$$

Lemma 3.2.4. *If $v \in T$, then $\#(H^1(H_v, E)(\mathfrak{p})) = \#(E_{\mathfrak{p}^{*\infty}}(H_v))$, and:*

(i) If $v \in B$, $\#(H^1(H_v, E)(\mathfrak{p})) = 2$ or 1, according as $p = 2$ or $p > 2$.

(ii) If $v \in P$, then $\#(H^1(H_v, E)(\mathfrak{p})) = \left|\left(1 - \frac{\psi_{E/H}(v)}{\mathrm{N}v}\right)\right|_{\mathfrak{p}}^{-1}$.

Proof. By Tate local duality, the dual of the discrete group $H^1(H_v, E)$ is $E(H_v)$, and this induces the duality between $H^1(H_v, E)_{\pi^n}$ and $E(H_v)/\pi^{*n}E(H_v)$ for any positive integer n. On the other hand, let l be the prime number below v. Then by [20, V.II 6.3], $E(H_v)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_v, +)$. Hence we have $E(H_v) = E(H_v)_{\mathrm{tor}} \oplus \mathbb{Z}_l^{[H_v:\mathbb{Q}_l]}$, and $v \nmid \pi^*$ so $E(H_v)/\pi^{*n}E(H_v) \simeq E_{\pi^{*n}}(H_v)$. Taking the inductive limit proves the first statement.

Assume first that $v \in B$. Let m be such that $E_{\mathfrak{p}^\infty}(H_v) = E_{\mathfrak{p}^m}$. In particular, $H_v = H_v(E_{\mathfrak{p}^m})$, so v splits completely in $H(E_{\mathfrak{p}^m})/H$. But Theorem 3.2.2 tells us that v ramifies in F/H, since the reduction type is stable under unramified field extensions [20][§5, Proposition 5.4]. It follows that $m \leqslant 0$ (resp. $m \leqslant 1$) if $p > 2$ (resp. $p = 2$). Hence if $p > 2$, we have $m = 0$, and in the case $p = 2$, we also have $E_{\mathfrak{p}} = E_{\mathfrak{p}}(H) \subset E_{\mathfrak{p}}(H_v)$ so $m \geqslant 1$, proving $m = 1$ in this case.

Now assume $v \in P$. Then π^{*n} is an automorphism of the formal group of E at v, and reduction modulo v induces an isomorphism

$$\varprojlim E(H_v)/\pi^{*n}E(H_v) \cong \widetilde{E}(k_v)(p),$$

where $\widetilde{E}/k_v$ denotes the reduction of E modulo v. Now, $\psi_{E/H}(v)$ is the unique element of $\mathcal{O}$ whose reduction modulo v is the Frobenius endomorphism of $\widetilde{E}$. Hence

$$\#(\widetilde{E}(k_v)) = (\psi_{E/H}(v) - 1)(\overline{\psi}_{E/H}(v) - 1),$$

where $\overline{\psi}_{E/H}$ denotes the complex conjugate of $\psi_{E/H}$. But $\psi_{E/H} - 1$ is a unit at $\mathfrak{p}$ since $(\psi_{E/H}(v)) = \mathfrak{p}^{f_v}$, where $f_v = [k_v : \mathbb{F}_p]$. Thus

$$\mathrm{ord}_p(\#(\widetilde{E}(k_v))) = \mathrm{ord}_{\mathfrak{p}}(\overline{\psi}_{E/H}(v) - 1).$$

The result follows by dividing this through by $\overline{\psi}_{E/H}(v)$ and noting $\mathrm{N}v = \psi_{E/H}(v)\overline{\psi}_{E/H}(v)$. □

We have an exact sequence

$$0 \to \mathrm{Sel}_{\mathfrak{p}^\infty}(E/H) \to \mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H) \xrightarrow{\varphi} \prod_{v \in T} H^1(H_v, E)(\mathfrak{p}). \tag{3.2.1}$$

Thus we have shown the following.

Corollary 3.2.5. $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/H)$ *is finite if and only if* $\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)$ *is finite.*

From now on, we make the following assumptions.

Assumption. $L(E/H, 1) \neq 0$ and $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/H)$ is finite.

The second assumtion will be guaranteed by the first when combined with the main conjecture for E/H, which we will discuss in Chapter 7. Note also that the finiteness of $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/H)$ implies the finiteness of $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/H)$.

Lemma 3.2.6. *For any $n \geqslant 1$, we have*

$$\#(\mathrm{Sel}_{\pi^n}(E/H)) = \begin{cases} \#(E_{\mathfrak{p}})\#(\text{Ш}(E/H))_{\pi^n} & \textit{if } p = 2 \\ \#(\text{Ш}(E/H))_{\pi^n} & \textit{if } p > 2. \end{cases}$$

Proof. We show This follows immediately from the exact sequence

$$0 \to E(H)/\pi^n E(H) \to \mathrm{Sel}_{\pi^n}(E/H) \to \text{Ш}(E/H)_{\pi^n} \to 0 \tag{3.2.2}$$

and the fact that $E_{\mathfrak{p}^\infty}(H) = E_{\mathfrak{p}}$ if $p = 2$ and $E_{\mathfrak{p}^\infty}(H)$ is trivial if $p > 2$ which follows from the fact that Δ has order 2 when $p = 2$ and $\Delta = (\mathcal{O}/\mathfrak{p})^\times$ when $p > 2$. □

Proposition 3.2.7.

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(E/H) = \text{Ш}(E/H)(\mathfrak{p})$$

Proof. By passing (3.2.2) to the direct limit, we find the exact sequence

$$0 \to E(H) \otimes (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \to \mathrm{Sel}_{\mathfrak{p}^\infty}(E/H) \to \text{Ш}(E/H)(\mathfrak{p}) \to 0,$$

where $E(H) \otimes (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}})$ is equal to the direct sum of rank$(E(H))$ copies of $K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}$. But $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/H)$ is assumed to be finite so $E(H)$ is finite, so the direct sum is equal to zero. □

Hence it follows from (3.2.1) that

$$\#(\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)) = \#(\text{Ш}(E/H)(\mathfrak{p}))\#(\operatorname{im}\varphi).$$

Now,

$$\#(\operatorname{im}\varphi) = \#(\prod_{v\in T} H^1(H_v, E)(\mathfrak{p}))/\#(\operatorname{coker}\varphi),$$

and we calculated $\#(H^1(H_v, E)(\mathfrak{p}))$ for $v \in T$ in Lemma 3.2.4.

Lemma 3.2.8.

$$\#(\operatorname{coker}\varphi) = \#(E_{\mathfrak{p}^{*\infty}}(H)),$$

which is equal to 2 *if* $p = 2$ *and* 1 *if* $p > 2$.

Proof. By Corollary 3 on p.123 of [16], coker φ is isomorphic to the dual of $\mathrm{Sel}_{\pi^{*\infty}}(E/H)$, which we denote by $\mathfrak{S}_{\pi^{*\infty}}(E/H)$. Now, by passing (3.2.2) to the projective limit, we find $\mathfrak{S}_{\pi^{*\infty}}(E/H)$ fits in the exact sequece

$$0 \to E(H) \otimes \mathcal{O}_{\mathfrak{p}^*} \to \mathfrak{S}_{\pi^{*\infty}}(E/H) \to T_{\mathfrak{p}^*}(\text{Ш}(E/H)) \to 0,$$

where $T_{\mathfrak{p}^*}(\text{Ш}(E/H))$ is the projective limit of $\text{Ш}(E/H)_{\pi^{*n}}$. Since $\text{Ш}(E/H)$ is assumed to be finite, this is equal to zero. Also, $E(H) \otimes \mathcal{O}_{\mathfrak{p}^*}$ is equal to the direct sum of rank$(E(H))$ copies of $\mathcal{O}_{\mathfrak{p}^*}$ and the finite group $E_{\mathfrak{p}^{*\infty}}(H)$. But $E(H)$ is assumed to be finite, hence $E(H) \otimes \mathcal{O}_{\mathfrak{p}^*}$ is equal to $E_{\mathfrak{p}^{*\infty}}(H)$. The rest is clear since $E_{\mathfrak{p}^{*\infty}}(H) = E_{\mathfrak{p}^*}$ if $p = 2$ and trivial if $p > 2$. □

Theorem 3.2.9. *We have*

(i) If $p = 2$, *then*

$$\#(\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)) = 2^{b-1} \cdot \prod_{v\in P} \left|\left(1 - \frac{\psi_{E/H}(v)}{\mathrm{N}v}\right)\right|_{\mathfrak{p}}^{-1} \cdot \#(\text{Ш}(E/H)(\mathfrak{p})),$$

where $b = \#(B)$

(ii) if $p > 2$, *then*

$$\#(\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)) = \prod_{v\in P} \left|\left(1 - \frac{\psi_{E/H}(v)}{\mathrm{N}v}\right)\right|_{\mathfrak{p}}^{-1} \cdot \#(\text{Ш}(E/H)(\mathfrak{p})).$$

Proof. By Lemma 3.2.4, we have

$$\#(\prod_{v\in T} H^1(H_v,E)(\mathfrak{p})) = \begin{cases} 2^b \cdot \prod_{v\in P} \left|\left(1-\frac{\psi_{E/H}(v)}{\mathrm{N}v}\right)\right|_{\mathfrak{p}}^{-1} & \text{if } p=2 \\ \prod_{v\in P} \left|\left(1-\frac{\psi_{E/H}(v)}{\mathrm{N}v}\right)\right|_{\mathfrak{p}}^{-1} & \text{if } p>2. \end{cases}$$

In addition, by Lemma 3.2.8

$$\#(\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)) = \#(\text{Ш}(E/H)(\mathfrak{p}))\cdot\#(\prod_{v\in T} H^1(H_v,E)(\mathfrak{p}))/\#(E_{\mathfrak{p}^*\infty}(H)),$$

and $\#(E_{\mathfrak{p}^*})$ is equal to 2 if $p=2$ and 1 if $p>2$. Hence the result follows. □

3.3 Descent theory over extensions of H

We set

$$F = \begin{cases} H(E_{\mathfrak{p}^2}) & \text{if } p=2 \\ H(E_{\mathfrak{p}}) & \text{if } p>2. \end{cases}$$

Recall that $F_\infty = H(E_{\mathfrak{p}^\infty})$ and

$$\mathfrak{H} = \mathrm{Gal}(F_\infty/H).$$

Recall also that we have an isomorphism $\chi_{\mathfrak{p}} : \mathfrak{H} \to \mathcal{O}_{\mathfrak{p}}^\times = \mathbb{Z}_p^\times$ giving the action of $\mathfrak{H}$ on $E_{\mathfrak{p}^\infty}$, and $\mathfrak{H} = \Delta\times\Gamma$, where $\Delta = \mathrm{Gal}\,(F/H)$, is cyclic of order 2 or $p-1$ according as $p=2$ or $p>2$, and $\Gamma = \mathrm{Gal}\,(F_\infty/F)$ is isomorphic to $\mathbb{Z}_p$.

Write P_F for the set of primes of F above $\mathfrak{p}$, and define

$$\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F) = \ker\left(H^1(F,E_{\mathfrak{p}^\infty}) \to \prod_{v\notin P_F} H^1(F_v,E)\right).$$

Consider the exact sequence

$$0\to H^1(\Delta, E_{\mathfrak{p}^\infty}(F)) \xrightarrow{\mathrm{inf}} H^1(H,E_{\mathfrak{p}^\infty}) \xrightarrow{\mathrm{res}} H^1(F,E_{\mathfrak{p}^\infty})^\Delta,$$

and also write res for the same map restricted to $\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H) \subset H^1(H,E_{\mathfrak{p}^\infty})$.

Theorem 3.3.1. *(i) If $p>2$, we have $\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H) = \mathrm{Sel}'_{\mathfrak{p}^\infty}(E/H)$, and the restriction map gives an isomorphism*

$$\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H) = \mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^\Delta.$$

(ii) If $p = 2$, *the restriction map satisfies* $\mathrm{res}(\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)) \subset \mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^\Delta$, *and we have an exact sequence*

$$0 \to H^1(\Delta, E_{\mathfrak{p}^\infty}(F)) \to \mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H) \xrightarrow{\mathrm{res}} \mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^\Delta \to 0.$$

Proof. The proof of Theorem 3.3.1 is easy for $p > 2$, hence we shall omit the details in this case. Now assume that $p = 2$. Then the following lemma shows that res surjects onto $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^\Delta$. Recall first that the action of Δ on $H^1(\mathrm{Gal}(\overline{F}/F), E_{\mathfrak{p}^\infty})$ is given by inner automorphisms, i.e., given $\tau \in \Delta$, $\xi \in H^1(\mathrm{Gal}(\overline{F}/F), E_{\mathfrak{p}^\infty})$, $\sigma \in \mathrm{Gal}(\overline{F}/F)$ and any cocycle f representing ξ, we have

$$\tau \cdot f(\sigma) = \tau f(\tau^{-1} \cdot \sigma) = \overline{\tau} f(\overline{\tau}^{-1} \sigma \overline{\tau}),$$

where $\overline{\tau}$ is a lift of τ in $\mathrm{Gal}(\overline{F}/F)$. The next result a modification of [11, Lemma2.3.5], which was left incomplete, because the fact that the cohomology class is invariant does not mean that one can choose a cocycle which is invariant under the action of Δ. This problem has been fixed in the following proof.

Lemma 3.3.2. *Let* $p = 2$. *Then we have* $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^\Delta \subset \mathrm{res}(H^1(H, E_{\mathfrak{p}^\infty}))$.

Proof. Choose a prime $\mathfrak{q} \in B$, and fix a prime $\mathfrak{Q}$ of $\overline{F}$ above $\mathfrak{q}$. Let $I_\mathfrak{q} \subset \mathrm{Gal}(\overline{F}/H)$ be the corresponding inertia subgroup. Let τ denote the unique element of $\mathfrak{H}$ which acts as multiplication by -1 on $E_{\mathfrak{p}^\infty}$. Then τ has order 2 and its restriction to H generates Δ. Also $\mathfrak{q}$ ramifies in F/H so τ generates the inertia group of $\mathfrak{q}$ in F/H, hence we can find a lifting $\overline{\tau}$ of τ in $I_\mathfrak{q}$. Then $\overline{\tau}^2$ restricted to F is $\tau^2 = \mathrm{id}$, so $\overline{\tau}^2 \in \mathrm{Gal}(\overline{F}/F) \cap I_\mathfrak{q}$. Furthermore, we know that every $\xi_\mathfrak{p} \in \mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^\Delta$ is unramified at $\mathfrak{q}$ since $\mathfrak{q} \nmid \mathfrak{p}$. Hence $\xi_\mathfrak{p} \in \ker(H^1(\mathrm{Gal}(\overline{F}/F), E_{\mathfrak{p}^\infty}) \to H^1(\mathrm{Gal}(\overline{F}/F) \cap I_\mathfrak{q}, E_{\mathfrak{p}^\infty}))$, i.e. $g(\overline{\tau}^2) = 0$ for any 1-cocycle g representing $\xi_\mathfrak{p}$.

Given $x \in E_{\mathfrak{p}^\infty}$, let $d(x)$ denote the 1-coboundary on $\mathrm{Gal}(\overline{F}/H)$ defined by $d(x)(\sigma) = (\sigma - 1)x$. Then we have $\tau \cdot d(x) = d(\overline{\tau}(x)) = d(-x) = -d(x)$ (for any $\sigma \in \mathrm{Gal}(\overline{F}/H)$, we have $\tau \cdot d(x)(\sigma) = \overline{\tau}(\overline{\tau}^{-1}\sigma\overline{\tau} - 1)x = (\sigma - 1)\overline{\tau}(x)$). Let $\xi_\mathfrak{p} \in H^1(F, E_{\mathfrak{p}^\infty})^\Delta$ and pick a 1-cocycle g representing $\xi_\mathfrak{p}$. Then since $\xi_\mathfrak{p}$ is Δ-invariant, we have $(1 - \tau) \cdot g = d(x)$ for some $x \in E_{\mathfrak{p}^\infty}$. Now we take $y \in E_{\mathfrak{p}^\infty}$ such that $2y = x$ and define $f = g - d(y)$, then

$$\begin{aligned}(1 - \tau) \cdot f &= (g - d(y)) - \tau \cdot (g - d(y)) \\ &= g - d(y) - (g - d(x)) + \tau \cdot d(y) \\ &= g - d(y) - (g - d(x)) - d(y)\end{aligned}$$

since $\tau \cdot d(y) = -d(y)$ from above, and $(1-\tau)\cdot g = d(x)$ implies $\tau \cdot g = g - d(x)$. Therefore, we have $(1-\tau)\cdot f = d(x) - 2d(y) = 0$, hence we can pick f as the cocycle representing $\xi_{\mathfrak{p}}$ and f is invariant under the action of Δ.

It is clear that every element of $\mathrm{Gal}(\overline{F}/H)$ can be written in the form $\sigma\overline{\tau}^i$ with $\sigma \in \mathrm{Gal}(\overline{F}/F)$ and $i \in \{0,1\}$. We now define the map

$$h : \mathrm{Gal}(\overline{F}/H) \to E_{p^\infty}$$

by $h(\sigma\overline{\tau}^i) = f(\sigma)$, and claim that this is an element of $H^1(H, E_{\mathfrak{p}^\infty})$ which maps to $\xi_{\mathfrak{p}}$ under res. This map is well-defined, since $h(\overline{\tau}^i) = 0$ for all $i \geqslant 0$. Indeed, it is clear that $h(\overline{\tau}^i) = f(\mathrm{id}) = 0$ for $i \in \{0,1\}$ since H is a 1-cocycle, hence it suffices to show $h(\overline{\tau}^2) = f(\overline{\tau}^2) = 0$, which we proved earlier. To see that h is a 1-cocycle, take $\rho_1 = \sigma_1\overline{\tau}^{i_1}$, $\rho_2 = \sigma_2\overline{\tau}^{i_2} \in \mathrm{Gal}(\overline{F}/H)$. We need to show $h(\rho_1\rho_2) = h(\rho_1) + \rho_1 h(\rho_2)$. Since $\mathrm{Gal}(\overline{F}/F)$ is a normal subgroup of $\mathrm{Gal}(\overline{F}/H)$, we can find an element $\sigma_2' \in \mathrm{Gal}(\overline{F}/F)$ such that $\overline{\tau}^{i_1}\sigma_2 = \sigma_2'\overline{\tau}^{i_1}$. Then $h(\rho_1\rho_2) = h(\sigma_1\sigma_2'\overline{\tau}^{i_1+i_2}) = f(\sigma_1\sigma_2') = f(\sigma_1) + \sigma_1 f(\sigma_2')$, where the last equality follows from the fact that f is a 1-cocycle. Also, $h(\rho_1) + \rho_1 h(\rho_2) = f(\sigma_1) + \sigma_1\overline{\tau}^{i_1} f(\sigma_2)$, and since f is Δ-invariant, we have $\tau \cdot f = f$, and Δ acts by inner-automorphism so $\tau \cdot f(\sigma) = \tau f(\tau^{-1}\sigma) = \overline{\tau} f(\overline{\tau}^{-1}\sigma\overline{\tau})$. Therefore, $\overline{\tau}^{i_1} f(\sigma_2) = f(\overline{\tau}^{i_1}\sigma_2\overline{\tau}^{-i_1}) = f(\sigma_2'\overline{\tau}^{i_1}\overline{\tau}^{-i_1}) = f(\sigma_2')$. Hence $f(\sigma_1) + \sigma_1\overline{\tau}^{i_1} f(\sigma_2) = f(\sigma_1) + \sigma_1 f(\sigma_2')$, as required. Finally, $\mathrm{res}(h(\sigma\overline{\tau}^i)) = h(\sigma) = f(\sigma)$, so indeed $\mathrm{res}(h) = f$. □

We now finish the proof of Theorem 3.3.1. Recall that for a group profinite group $\mathcal{G}$ and a $\mathcal{G}$-module A, $\hat{H}^0(\mathcal{G}, A)$ is the modified 0-th cohomology group defined to be equal to $A^{\mathcal{G}}/N_{\mathcal{G}}A$ where $N_{\mathcal{G}} : A \to A,\ \ a \mapsto \sum_{\sigma\in G} \sigma a$ denotes the norm map. In addition, if G is cyclic and A is finite, then we have $H^1(\mathcal{G}, A) = \hat{H}^0(\mathcal{G}, A)$ since the Herbrand quotient is equal to 1. Hence, in order to work out the order of $H^1(\mathcal{G}, A)$, we will calculate the order of $A^{\mathcal{G}}/N_{\mathcal{G}}A$ instead. First, we have $H^1(\Delta, E_{\mathfrak{p}^\infty}(F)) = H^1(\Delta, E_{\mathfrak{p}^2}) = \hat{H}^0(\Delta, E_{\mathfrak{p}^2})$ because $\Delta = \mathrm{Gal}(F/H)$ is cyclic of order 2 by Theorem 3.2.1 and $F = H(E_{\mathfrak{p}^2})$. We have $E_{\mathfrak{p}^2}^{\Delta} = E_{\mathfrak{p}}$. Now $\Delta = \{1, \delta\}$ where δ acts as -1 on $E_{\mathfrak{p}^2}$, so we have $N_\Delta(P) = P + (-1)P = \mathcal{O}$ for all $P \in E_{\mathfrak{p}^2}$. Hence $|H^1(\Delta, E_{\mathfrak{p}^2})| = |E_{\mathfrak{p}}| = 2$.

The fact that $H^1(\Delta, E_{\mathfrak{p}^2})$ injects into $\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)$ follows from the fact that

$$H^1(\mathrm{Gal}(F_{\mathfrak{Q}}/H_{\mathfrak{q}}), E) = 0 \tag{3.3.1}$$

for any prime $q \notin B$ and any prime $\mathfrak{Q}$ of F above $\mathfrak{q}$. This is because E has good reduction at $\mathfrak{q}$ and $F_{\mathfrak{Q}}/H_{\mathfrak{q}}$ is unramified, which implies that $N_{F_{\mathfrak{Q}}/H_{\mathfrak{q}}}$ is surjective. Hence it remains to show $\mathrm{res}(\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)) = \mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^{\Delta}$. Given any prime $\mathfrak{Q}$ of F and prime $\mathfrak{q}$ of H lying below $\mathfrak{Q}$, we have the commutative diagram

$$\begin{tikzcd}
H^1(H, E_{\mathfrak{p}^\infty}) \arrow[r, "\lambda_{\mathfrak{q}}"] \arrow[d, "\mathrm{res}"] & H^1(H_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty} \arrow[d, "\mathrm{res}_{\mathfrak{Q}}"] \\
H^1(F, E_{\mathfrak{p}^\infty})^{\Delta} \arrow[r, "\lambda_{\mathfrak{Q}}"] & H^1(F_{\mathfrak{Q}}, E)^{\Delta}_{\mathfrak{p}^\infty}.
\end{tikzcd}$$

To show $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^{\Delta} \subset \mathrm{res}(\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H))$, take any $x \in \mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^{\Delta}$. Then since $H^1(H, E_{\mathfrak{p}^\infty}) \xrightarrow{\mathrm{res}} \mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^{\Delta}$ is surjective by Lemma 3.3.2, there exists $a \in H^1(H, E_{\mathfrak{p}^\infty})$ with $x = \mathrm{res}(a)$. Then for any prime $\mathfrak{q} \notin B$ of H and a prime $\mathfrak{Q}$ of F above $\mathfrak{q}$, we have

$$\mathrm{res}_{\mathfrak{Q}}(\lambda_{\mathfrak{q}}(a)) = \lambda_{\mathfrak{Q}}(x) = 0,$$

since $x \in \mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^{\Delta} \subset \ker \lambda_{\mathfrak{Q}}$. But $\mathrm{res}_{\mathfrak{Q}}$ is injective by (4.1.8), so $\lambda_{\mathfrak{q}}(a) = 0$. Hence $a \in \mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)$, and $x \in \mathrm{res}(\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H))$ as required. To show the other inclusion, it suffices to show that for any prime $\mathfrak{q} \nmid \mathfrak{p}$ of H and $\mathfrak{Q}$ of F lying above $\mathfrak{q}$ we have $\mathrm{res}(\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)) \subset \ker \lambda_{\mathfrak{Q}}$. First let $\mathfrak{Q}$ be a prime of F lying above $\mathfrak{q} \in B$. Then we have shown that $H^1(F_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty} = E_{\mathfrak{p}}$ in Lemma 3.2.4, and furthermore, we have $H^1(\Delta_{\mathfrak{Q}}, E)_{\mathfrak{p}^\infty} \simeq H^1(\Delta_{\mathfrak{Q}}, E_{\mathfrak{p}^\infty})$ since $E(F_{\mathfrak{Q}}) = E(F_{\mathfrak{Q}})_{\mathfrak{p}^\infty} \oplus A$ for a $\mathfrak{p}$-divisible group A. So $H^1(\Delta_{\mathfrak{Q}}, E)_{\mathfrak{p}^\infty} = E_{\mathfrak{p}}$ since $\Delta_{\mathfrak{Q}} = \Delta$ for such $\mathfrak{Q}$. Hence $\mathrm{res}_{\mathfrak{Q}}$ is the zero map. But given any $a \in \mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)$, the above diagram commutes so

$$\lambda_{\mathfrak{Q}}(\mathrm{res}(a)) = \mathrm{res}_{\mathfrak{Q}}(\lambda_{\mathfrak{q}}(a)) = 0, \tag{3.3.2}$$

giving $\mathrm{res}(\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)) \in \ker \lambda_{\mathfrak{Q}}$ as required. Finally, let $\mathfrak{Q}$ be a prime of F lying above $\mathfrak{q} \notin B$. Then $\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H) \subset \ker \lambda_{\mathfrak{q}}$, so for $a \in \mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)$ (4.2.2) holds again, and so $\mathrm{res}(\mathrm{Sel}^{(T)}_{\mathfrak{p}^\infty}(E/H)) \subset \ker \lambda_{\mathfrak{Q}}$. This completes the proof of Theorem 3.3.1. □

The following is an immediate consequence of Theorem 3.3.1.

Corollary 3.3.3. $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^{\Delta}$ *is finite if and only if* $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/H)$ *is.*

Assuming p satisfies the good ordinary hypothesis for E, we have

$$\#(H^1(\Delta, E_{\mathfrak{p}^\infty}(F))) = 1 \text{ or } 2,$$

depending as $p > 2$ or $p = 2$. Hence combining Theorem 3.2.9 and Theorem 3.3.1, we obtain:

Theorem 3.3.4. *Let p be a prime satisfying the good ordinary hypothesis for E. Then* $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^{\Delta}$ *is finite if and only if* $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/H)$ *is finite. Moreover, if we assume that $E(H)$ and* $\text{Ш}(E/H)(p)$ *are finite, then we have:*

(i) If $p > 2$, then

$$\#(\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^\Delta) = \prod_{v\in P}\left|\left(1-\frac{\psi_{E/H}(v)}{\mathrm{N}v}\right)\right|_{\mathfrak{p}}^{-1}\cdot\#(\text{Ш}(E/H)(\mathfrak{p}))$$

(ii) If $p = 2$, then

$$\#(\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^\Delta) = 2^{b-2}\prod_{v\in P}\left|\left(1-\frac{\psi_{E/H}(v)}{\mathrm{N}v}\right)\right|_{\mathfrak{p}}^{-1}\cdot\#(\text{Ш}(E/H)(\mathfrak{p})),$$

where $b = \#(B)$.

We define the $\mathfrak{p}^\infty$-Selmer group $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty)$ by

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty) = \ker\left(H^1(F_\infty, E_{\mathfrak{p}^\infty}) \to \prod_w H^1(F_{\infty,w}, E)\right).$$

We also define modified Selmer group

$$\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F_\infty) = \ker\left(H^1(F_\infty, E_{\mathfrak{p}^\infty}) \to \prod_{w\nmid\mathfrak{p}} H^1(F_{\infty,w}, E)\right).$$

The next result is [2, Lemma 8].

Theorem 3.3.5. *We have* $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty) = \mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F_\infty)$.

Proof. It suffices to show that $H^1(F_{\infty,\mathfrak{P}}, E)(\mathfrak{p})$ is trivial any place $\mathfrak{P}$ of F_∞ above $\mathfrak{p}$. Let $F_{n,\mathfrak{P}_n}$ denote the completion of F_n at the prime $\mathfrak{P}_n$ of F_n lying below $\mathfrak{P}$. Then we have $\cup_{n\geqslant 0}F_{n,\mathfrak{P}_n} = F_{\infty,\mathfrak{P}}$, so $H^1(F_{\infty,\mathfrak{P}}, E) = \varinjlim H^1(F_{n,\mathfrak{P}_n}, E)$ where the limit is taken with respect to the restriction. Recall that π is an element of $\mathcal{O}$ satisfying $(\pi) = \mathfrak{p}^h$. Let n be of the form $n'h$ with $n' \geqslant 0$. By Tate's local duality, the Pontryagin dual of $H^1(F_{n,\mathfrak{P}_n}, E)(\mathfrak{p})$ is equal to

$$\overline{E}(F_{n,\mathfrak{P}_n}) = \varprojlim E(F_{n,\mathfrak{P}_n})/\pi^{*m}E(F_{n,\mathfrak{P}_n}),$$

where the limit is taken with respect to the norm map. Note that $\mathfrak{P}_n$ lies above $\mathfrak{p}$ and $\mathfrak{p} \neq \mathfrak{p}^*$, so π^{*m} is an automorphism of the group $E_1(F_{n,\mathfrak{P}_n})$ of $F_{n,\mathfrak{P}_n}$-rational points in the kernel of reduction modulo $\mathfrak{P}_n$. Thus reduction modulo $\mathfrak{P}_n$ induces an isomorphism $E(F_{n,\mathfrak{P}_n})/\pi^{*m}E(F_{n,\mathfrak{P}_n}) \cong \widetilde{E}(\widetilde{F_{n,\mathfrak{P}_n}})/\pi^{*m}\widetilde{E}(\widetilde{F_{n,\mathfrak{P}_n}})$, where $\widetilde{F_{n,\mathfrak{P}_n}}$ denotes the residue field of $F_{n,\mathfrak{P}_n}$ at $\mathfrak{P}_n$. Thus we have $\overline{E}(F_{n,\mathfrak{P}_n}) \simeq \widetilde{E}(\widetilde{F_{n,\mathfrak{P}_n}})(p) \simeq E_{\mathfrak{p}^{*\infty}}(F_{n,\mathfrak{P}_n})$. This is a finite group of bounded order, since $\mathfrak{P}$ is totally ramified in $F_{\infty,\mathfrak{P}}/F_{n,\mathfrak{P}_n}$, so the residue field $\widetilde{F_{n,\mathfrak{P}_n}}$ is finite. So there exists m and n_0 such that $\widetilde{E}(\widetilde{F_{n,\mathfrak{P}_n}}) = E_{\mathfrak{p}^{*m}}$ for all $n \geqslant n_0$. Take $(P_n) \in \varprojlim \overline{E}(F_{n,\mathfrak{P}_n})$. Then $P_{n_0} = [\pi^{*m}]P_{n_0+m} = \mathcal{O}$, so in fact $(P_n) = 0$. Therefore $\varprojlim \overline{E}(F_{n,\mathfrak{P}_n})$ is trivial, and it immediately follows that $H^1(F_{\infty,\mathfrak{P}}, E)(\mathfrak{p})$ is trivial. □

Write $X(F_\infty) = \mathrm{Gal}(M(F_\infty)/F_\infty)$, where $M(F_\infty)$ is the maximal abelian p-extension of F_∞ unramified outside the primes of F_∞ above $\mathfrak{p}$. Note that, by maximality, $M(F_\infty)$ is Galois over H, and we can define an action of $\mathfrak{H} = \mathrm{Gal}(F_\infty/H)$ on $X(F_\infty)$ by

$$g \cdot x = \widetilde{g} x \widetilde{g}^{-1},$$

where $\widetilde{g}$ denotes any lifting of g in $\mathfrak{H}$ to an element of $\mathrm{Gal}(M(F_\infty)/H)$. Let

$$\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\Gamma/U]$$

be the Iwasawa algebra of Γ. The continuous action of Γ on $X(F_\infty)$ extends to an action of $\Lambda(\Gamma)$. The following classical result is well-known granted that E has good reduction everywhere over F_∞, and is omitted (see Theorem 9, Theorem 12 and Lemma 13 of [2]).

Theorem 3.3.6. *We have*

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty) = \mathrm{Hom}(X(F_\infty), E_{\mathfrak{p}^\infty}).$$

Furthermore, $X(F_\infty)$ is a finitely generated torsion $\Lambda(\Gamma)$-module, and the restriction map gives an isomorphism

$$\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F) \xrightarrow{\sim} \mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty)^\Gamma.$$

We wish to find a criterion for when $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^\Delta$ is finite, and to compute its order when it is finite. We will study this in more detail in Chapter 7 in order to state the main conjecture for E/H. Before we do this, we will construct in the next chapter the $\mathfrak{p}$-adic L-functions which appear in the statement of the main conjectures.

Chapter 4

Construction of the $\mathfrak{p}$-adic L-functions

4.1 Construction of the $\mathfrak{p}$-adic L-function for F_∞/F

We now construct the $\mathfrak{p}$-adic L-functions attached to E/H, which we shall subsequently need to formulate the main conjectures. We will follow the ideas in [4], however, we will also deal with the case $p = 2$, which cannot be found in literature.

Fix once and for all an embedding of H into $\mathbb{C}$. Write x, y for the coordinates of E/H. We fix a generalised global minimal Weierstrass equation for E over H, which exists by [14, Proposition 3.2], to be

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4.1.1}$$

Recall that G denotes the Galois group of H over K. Then applying $\sigma \in G$ to (4.1.1) gives a generalised global minimal Weierstrass equation for E^σ/H. Let

$$\omega^\sigma = \frac{dx}{2y + a_1^\sigma x + a_3^\sigma}$$

be the Néron differentials on E^σ, and note that the discriminant of this equation $\Delta(E^\sigma)$ is equal to $(\Delta(E))^\sigma = \Delta(E)$. Let $\mathfrak{g}$ denote the conductor of φ_K, so that $(\mathfrak{g}, 2p) = 1$, and let $\mathfrak{f} = \mathfrak{g}^h$, so that $\mathfrak{f}$ is principal. Let L (resp. L_σ) be the period lattice of the Neron differential on our global minimal Weierstrass equation for E (resp. E^σ). Then there exists $\Omega_\infty \in \mathbb{C}^\times$ such that $L = \Omega_\infty\mathcal{O}$. The uniformisation $\Phi : \mathbb{C}/L \xrightarrow{\sim} E(\mathbb{C})$ is accomplished through

$$\Phi(z, L_\sigma) = \left(\wp(z, L_\sigma) - \frac{((a_1^\sigma)^2 + 4a_2^\sigma)}{12}, \frac{1}{2}\left(\wp'(z, L_\sigma) - a_1^\sigma\left(\wp(z, L_\sigma) - \frac{((a_1^\sigma)^2 + 4a_2^\sigma)}{12}\right) - a_3^\sigma\right)\right).$$

Given a principal ideal $\mathfrak{a} = (\alpha)$ with $\alpha \in \mathcal{O}$ and $(\mathfrak{a}, 6\mathfrak{f}) = 1$, define

$$R_\mathfrak{a}(P) := c_E(\mathfrak{a}) \prod_U (x(P) - x(U))^{-1},$$

where U runs over any set of representatives of $E_\mathfrak{a} \backslash \{\mathcal{O}\}$ modulo $\{\pm 1\}$, and $c_E(\mathfrak{a})$ is an element of H whose 12-th power is equal to $\Delta(E)^{\mathrm{N}\mathfrak{a}-1}/\Lambda(\mathfrak{a})^{12}$, where $\Lambda(\mathfrak{a}) \in H^\times$ satisfies

$$\lambda_E(\mathfrak{a})^*(\omega^{\sigma_\mathfrak{a}}) = \Lambda(\mathfrak{a})\omega.$$

Thus $R_\mathfrak{a}(P)$ is a rational function on E with coefficients in H. Let us write P for the generic point on E^σ with coordinates (x, y). Applying $\sigma \in G$ to the coefficients of $R_\mathfrak{a}(P)$, we obtain a rational function $R_\mathfrak{a}^\sigma(P)$ on the curve E^σ/H.

Proposition 4.1.1. *Let $\mathfrak{b}$ be an integral ideal of K with $(\mathfrak{b}, \mathfrak{a}) = 1$. Then we have*

$$R_\mathfrak{a}^{\sigma\sigma_\mathfrak{b}}(\lambda_{E^\sigma}(\mathfrak{b})(P)) = \prod_{R \in E_\mathfrak{b}^\sigma} R_\mathfrak{a}^\sigma(P \oplus R).$$

Proof. Recall that the kernel of $\lambda_{E^\sigma}(\mathfrak{b})$ is $E_\mathfrak{b}^\sigma$, and $\lambda_{E^\sigma}(\mathfrak{b})$ is injective on $E_\mathfrak{a}^\sigma$ since $(\mathfrak{b}, \mathfrak{a}) = 1$. Hence, the left hand side and the right hand side of the above equation have the same divisor, and

$$\frac{R_\mathfrak{a}^{\sigma\sigma_\mathfrak{b}}(\lambda_{E^\sigma}(\mathfrak{b})(P))}{\prod_{R \in E_\mathfrak{b}^\sigma} R_\mathfrak{a}^\sigma(P \oplus R)}$$

is a non-zero element of H. It can be shown, thanks to the unique scaling factor $c_E(\mathfrak{a})$ in our definition of the rational functions, that this constant is equal to 1. See [3, Appendix, Theorem 4] for details. □

We fix a generator f of the ideal $\mathfrak{f}$, and define $Q = \Phi(\Omega_\infty/f, L)$ so that Q is a primitive f-division point on E. We then define

$$\mathfrak{R}_\mathfrak{a}(P) = \prod_{\tau \in \mathrm{Gal}(H(E_\mathfrak{f})/H)} R_\mathfrak{a}(P \oplus Q^\tau),$$

where $\oplus$ denotes the addition on E. Thus $\mathfrak{R}_{\mathfrak{a}}(P)$ is also a rational function on E over H. Similarly, we define

$$\mathfrak{R}_{\mathfrak{a}}^{\sigma}(P) = \prod_{\tau \in \mathrm{Gal}(H(E_{\mathfrak{f}})/H)} R_{\mathfrak{a}}^{\sigma}(P \oplus (Q^\sigma)^\tau),$$

a rational function on E^σ over H. Hence, defining

$$\Psi_{\mathfrak{a}}^{\sigma}(P) = \mathfrak{R}_{\mathfrak{a}}^{\sigma}(P)^{\mathrm{N}\mathfrak{p}} / \mathfrak{R}_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{p}}}(\lambda_{E^\sigma}(\mathfrak{p})(P)),$$

it follows that

$$\prod_{R \in E_{\mathfrak{p}}^{\sigma}} \Psi_{\mathfrak{a}}^{\sigma}(P \oplus R) = 1. \tag{4.1.2}$$

Now, we fix an embedding $i_v : \overline{K} \to \overline{K}_{\mathfrak{p}}$, and we let v denote the prime of H above $\mathfrak{p}$ determined by i_v. We write $\mathcal{O}_v$ for the ring of integers of H_v.

Recall that $t = -\frac{x}{y}$ is a parameter for this formal group.

Lemma 4.1.2. *Let $B_{\mathfrak{a}}^{\sigma}(t)$ denote the t-expansions of $\mathfrak{R}_{\mathfrak{a}}^{\sigma}(P)$. Then $B_{\mathfrak{a}}^{\sigma}(t)$ is a unit in $\mathcal{O}_v[[t]]$.*

Proof. We claim that, if V denotes any of the points $(Q^\sigma)^\tau$, then

$$x(P \oplus V) - x(U),$$

where U is any non-zero element of $E_{\mathfrak{a}}^{\sigma}$, has a t-series expansion which is a unit in $\mathcal{O}_{\mathfrak{B}}[[t]]$, where $\mathfrak{B}$ denotes any prime of $H(U,V)$ above v, and $\mathcal{O}_{\mathfrak{B}}$ is the ring of integers of the completion of $H(U,V)$ at this prime. Indeed, we have explicitly

$$x(P \oplus V) - x(U) = D(P,V)^2 + a_1^\sigma D(P,V) - a_2^\sigma - x(P) - x(V) - x(U),$$

where

$$D(P,V) = \frac{y(P) - y(V)}{x(P) - x(V)}.$$

Note that $x(V)$, $y(V)$ are integral at $\mathfrak{B}$ because $(\mathfrak{f}, p) = 1$ by assumption. Similarly, the expansions of $x(P)$ and $y(P)$ as power series in t begin

$$x(P) = \frac{1}{t^2} - \frac{a_1^\sigma}{t} - a_2^\sigma + \cdots, \quad y(P) = -\frac{1}{t^3} + \frac{a_1^\sigma}{t^2} + \frac{a_2^\sigma}{t} + \cdots,$$

where the coefficients of all the higher order terms lie in $\mathcal{O}_{\mathfrak{B}}$. Note that $x(U)$ is integral at primes of $H(U,V)$ above $\mathfrak{B}$ because $(\mathfrak{a}, p) = 1$. Thus we see that the coefficients of the t-series expansion of $x(P \oplus V) - x(U)$ all belong to $\mathcal{O}_{\mathfrak{B}}$. Moreover, $x(P \oplus V) - x(U)$ is holomorphic at $t = 0$, and so there are no negative powers of t in its t-series expansion. Moreover, we have

$$D(P, V) = -\frac{1}{t} - x(V)t + \cdots ,$$

so the constant term of the t-series expansion of is $x(P \oplus V) - x(U)$ is

$$x(V) - x(U).$$

We claim this must be a unit at $\mathfrak{B}$. If not, we would have $x(\widetilde{V}) = x(\widetilde{U})$, where $\widetilde{}$ denotes the reduction modulo $\mathfrak{B}$. But this would imply that $\widetilde{V} = \pm\widetilde{U}$, whence we would have one of $V \pm U$ must lie on the formal group of E^{σ} at v. But this is impossible because $(p\mathfrak{a}, \mathfrak{f}) = 1$. The assertion of the lemma now follows immediately, on noting that $c_E(\mathfrak{a})$ is a unit at v. □

From this we obtain

Corollary 4.1.3. *Let $A_{\mathfrak{a}}^{\sigma}(t)$denote the t-expansions of $\Psi_{\mathfrak{a}}^{\sigma}(P)$. Then $A_{\mathfrak{a}}^{\sigma}(t)$ belongs to $1 + \mathfrak{m}_v[[t]]$, where $\mathfrak{m}_v$ denotes the maximal ideal of $\mathcal{O}_v$.*

Proof. Write $B_{\mathfrak{a}}^{\sigma}(t) = \sum_{n=0}^{\infty} a_n t$. Thus, by the previous lemma, $a_n \in \mathcal{O}_{\mathfrak{p}}$ for all $n \geqslant 0$ and $a_0 \in \mathcal{O}_{\mathfrak{p}}^{\times}$. Now, $A_{\mathfrak{a}}^{\sigma}(t) = \frac{B_{\mathfrak{a}}^{\sigma}(t)^p}{B_{\mathfrak{a}}^{\sigma\sigma_v}\left(\widehat{\lambda}_E(v)(t)\right)}$ and recall that

$$\widehat{\lambda}_E(v)(t) \equiv t^p \bmod v.$$

Hence, we see that

$$B_{\mathfrak{a}}^{\sigma\sigma_v}\left(\widehat{\lambda}_E(v)(t)\right) = \sum_{n=0}^{\infty} a_n^{\sigma_v} (\widehat{\lambda}_E(v)(t))^n \equiv \sum_{n=0}^{\infty} a_n^p t^{pn} \bmod v.$$

On the other hand,

$$B_{\mathfrak{a}}^{\sigma}(t)^p \equiv \sum_{n=0}^{\infty} a_n^p t^{pn} \equiv \sum_{n=0}^{\infty} a_n t^{pn} \bmod v,$$

so $A_{\mathfrak{a}}^{\sigma}(t) \equiv 1 \bmod v$, as required.

□

Lemma 4.1.4. *Define $C_{\mathfrak{a}}^{\sigma}(t)$ by*

$$C_{\mathfrak{a}}^{\sigma}(t) := \frac{1}{p} \log A_{\mathfrak{a}}^{\sigma}(t).$$

Then $C^\sigma_{\mathfrak{a}}(t) \in \mathcal{O}_{\mathfrak{p}}[[t]]$, *and*

$$\sum_{\omega \in \mathcal{D}_{\sigma,p}} C^\sigma_{\mathfrak{a}}(t[+]\omega) = 0, \tag{4.1.3}$$

where $\mathcal{D}_{\sigma,p}$ *denotes the group of p-division points on the formal group* $\widehat{E}^\sigma$ *at a place* v *of* H *lying above* $\mathfrak{p}$ *and* $[+]$ *denotes the group law on* $\widehat{E}^\sigma$. *This group can be identified with* $E^\sigma_{\mathfrak{p}}$.

Proof. We have

$$C^\sigma_{\mathfrak{a}}(t) = \frac{1}{p}\sum_{n \geqslant 1} \frac{(-1)^{n-1}(A^\sigma_{\mathfrak{a}}(t)-1)^n}{n}.$$

The first claim is now clear from the previous lemma as $n \geqslant \mathrm{ord}_{\mathfrak{p}}(n)+1$ for $n \geqslant 1$. The final equation then follows from (4.1.2). □

Let $\mathscr{I}$ be the ring of integers of the completion of the maximal unramified extension $K^{\mathrm{ur}}_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$. By [8, Proposition 1.6], we have an isomorphism

$$\delta_{\sigma,v} : \widehat{\mathbb{G}}_m \xrightarrow{\sim} \widehat{E}^\sigma$$

defined over $\mathscr{I}$, where $\widehat{\mathbb{G}}_m$ denotes the formal multiplicative group and $\widehat{E}^\sigma$ denotes the formal group of E^σ at v. Define $J^\sigma_{\mathfrak{a}}(W) = C^\sigma_{\mathfrak{a}} \circ \delta_{\sigma,v}(W) \in \mathscr{I}[[W]]$.

Definition 4.1.5. Let $\mu_{\mathfrak{a},\sigma}$ be the $\mathscr{I}$-valued measure on $\mathbb{Z}_p$ determined by $J^\sigma_{\mathfrak{a}}(W)$, i.e.

$$J^\sigma_{\mathfrak{a}}(W) = \int_{\mathbb{Z}_p} (1+W)^x d\mu_{\mathfrak{a},\sigma}(x). \tag{4.1.4}$$

We claim that the measure $\mu_{\mathfrak{a},\sigma}$ is supported on $\mathbb{Z}_p^\times$. Indeed, let $\Lambda_{\mathscr{I}}(\mathbb{Z}_p)$ (resp. $\Lambda_{\mathscr{I}}(\mathbb{Z}_p^\times)$ be the ring of $\mathscr{I}$-valued measures on $\mathbb{Z}_p$ (resp. $\mathbb{Z}_p^\times$). Then we have an inclusion $\iota : \Lambda_{\mathscr{I}}(\mathbb{Z}_p^\times) \hookrightarrow \Lambda_{\mathscr{I}}(\mathbb{Z}_p)$ given by extending the measures on $\mathbb{Z}_p$ to $\mathbb{Z}_p^\times$ by zero. Let μ be a measure in $\Lambda_{\mathscr{I}}(\mathbb{Z}_p)$, and let $f_\mu(W) \in \mathscr{I}[[W]]$ be the corresponding power series given by the isomorphism $\Lambda_{\mathscr{I}}(\mathbb{Z}_p) \cong \mathscr{I}[[W]]$. Then it is well-known (see [8, I.3.3] for more details) that μ belongs to $\iota\left(\Lambda_{\mathscr{I}}(\mathbb{Z}_p^\times)\right)$ if and only if f_μ satisfies the equation

$$\sum_{\zeta \in \boldsymbol{\mu}_p} f_\mu(\zeta(1+W)-1) = 0.$$

It follows from (4.1.3) that this is satisfied by $J^\sigma_{\mathfrak{a}}$.

We know that, writing also $\mu_{\mathfrak{a},\sigma}$ for the corresponding measure in $\Lambda_{\mathscr{I}}(\mathfrak{H})$, we have

$$\int_{\mathfrak{H}} \chi^k_{\mathfrak{p}} d\mu_{\mathfrak{a},\sigma} = \int_{\mathbb{Z}_p} x^k d\mu_{\mathfrak{a},\sigma} = D^k J^\sigma_{\mathfrak{a}}(W)|_{W=0}, \tag{4.1.5}$$

where $D = (1+W)\frac{d}{dW}$. We have an isomorphism $\hat{\mathbb{G}}_m \xrightarrow{\sim} \hat{\mathbb{G}}_a$ given by $W \mapsto e^z - 1$. Hence we see immediately that $D = \frac{d}{dz}$. Moreover, we have $\delta_{\sigma,v}(W) = \Omega_{\sigma,v}W + \cdots$, so for any integer $k \geqslant 1$, we have

$$D^k J^\sigma_{\mathfrak{a}}(W)|_{W=0} = \left(\frac{d}{dz}\right)^k J^\sigma_{\mathfrak{a}}(e^z-1)|_{z=0} = \frac{1}{p}\Omega^k_{\sigma,v}\left(\frac{d}{dz}\right)^k \log\left(\Psi^\sigma_{\mathfrak{a}}(\Phi(z,L_\sigma))\right)|_{z=0}. \tag{4.1.6}$$

Lemma 4.1.6. *We have $\Omega_{\sigma,v} = \Lambda(\mathfrak{s})\Omega_v$, where $\Omega_v \in \mathscr{I}^\times$ is the coefficient of W in the formal power series $t = \delta_v(W)$, with $\delta_v : \widehat{\mathbb{G}}_m \xrightarrow{\sim} \widehat{E}$ is an isomorphism defined over $\mathscr{I}$.*

Proof. We have $\lambda_E(\mathfrak{s})^*(\omega^\sigma) = \Lambda(\mathfrak{s})\omega$ by definition, so that $\lambda_E(\mathfrak{s})\left(\Phi(z,L)\right) = \Phi(\Lambda(\mathfrak{s})z, L_\sigma)$. Hence, writing $\exp(z,L_\sigma)$ for the formal power series in z obtained by expressing $t = -x/y$ in terms of z using the isomorphism $\Phi(z,L_\sigma)$ for E^σ, we also have $\lambda_E(\exp(z,L)) = \exp(\Lambda(\mathfrak{s})z, L_\sigma))$. Now, regarding z as the parameter of the formal additive group, $\exp(z,L_\sigma)$ is the exponential map of $\widehat{E}^\sigma$. It then follows by the uniqueness of the exponential maps for the formal groups that

$$\delta_{\sigma,v}(e^{z/\Omega_{\sigma,v}} - 1) = \exp(z, L_\sigma).$$

On the other hand, we have $\delta_{\sigma,v} = \widehat{\lambda}_E(\mathfrak{s}) \circ \delta_v(W)$, where $\widehat{\lambda}_E(\mathfrak{s}) : \widehat{E} \to \widehat{E}^\sigma$ is the isomorphism over H_v of formal groups induced by $\lambda_E(\mathfrak{s})$. Hence we have

$$\delta_{\sigma,v}(e^z - 1) = \exp(\Lambda(\mathfrak{s})\Omega_v z, L_\sigma).$$

The assertion follows by comparing the coefficients of z in the above equations. □

Proposition 4.1.7. *Let $\mathfrak{s}$ be an integral ideal of K prime to $\mathfrak{f}$ such that $\sigma_{\mathfrak{s}} = \sigma$. Then for any integer $k \geqslant 1$, $k \equiv 1 \bmod \#(\Delta)$, we have*

$$\frac{d}{dz}\log \mathfrak{R}^\sigma_{\mathfrak{a}}(\Phi(z,L_\sigma)) = \sum_{k=1}^{\infty}(-1)^k \frac{\varphi^k_K(\mathfrak{s})f^k}{\Lambda(\mathfrak{s})^k\Omega^k_\infty}\left(\mathrm{N}\,\mathfrak{a} - \varphi^k_K(\mathfrak{a})\right) L(\overline{\varphi}^k_K, \sigma, k) z^{k-1}.$$

In particular, we have

$$\left(\frac{d}{dz}\right)^k \log \mathfrak{R}^\sigma_{\mathfrak{a}}(\Phi(z,L_\sigma))|_{z=0} = (-1)^k(k-1)!\frac{\varphi^k_K(\mathfrak{s})f^k}{\Lambda(\mathfrak{s})^k\Omega^k_\infty}\left(\mathrm{N}\,\mathfrak{a} - \varphi^k_K(\mathfrak{a})\right) L(\overline{\varphi}^k_K, \sigma, k).$$

Proof. Let $\mathfrak{L}$ be a complex lattice. We will modify the Weierstrass σ-function slightly, and define

$$\Theta(z,\mathfrak{L}) = \exp\left\{-s_2(\mathfrak{L})\frac{z^2}{2}\right\}\sigma(z,\mathfrak{L}).$$

Recall that for any integer $k \geqslant 1$, we can define the Kronecker–Eisenstein series

$$H_k(z,s,\mathfrak{L}) := \sum_{w\in\mathfrak{L}} \frac{(\overline{z}+\overline{w})^k}{|z+w|^{2s}},$$

where the sum in taken over all $w \in \mathfrak{L}$, except $-z$ if $z \in \mathfrak{L}$. This series converges for $\mathrm{Re(s)} > \frac{\mathrm{k}}{2}+1$, and it has an analytic continuation to the whole complex s-plane. The non-holomorphic Eisenstein series $\mathcal{E}_k^*(z,\mathfrak{L})$ is defined by

$$\mathcal{E}_k^*(z,L) := H_k(z,k,\mathfrak{L}).$$

Furthermore, it is well-known that (see [10, Corollary 1.7] for a proof and the definition of $A(\mathfrak{L})$) for any $z_0 \in \mathbb{C}\backslash\mathfrak{L}$, we have

$$\frac{d}{dz}\log\Theta(z+z_0) = \overline{z}_0 A(\mathfrak{L})^{-1} + \sum_{k=1}^{\infty}(-1)^{k-1}\mathcal{E}_k^*(z_0,\mathfrak{L})z^{k-1}. \tag{4.1.7}$$

By [10, Theorem 1.9], for any principal integral ideal $\mathfrak{a} = (\alpha)$ with $(\mathfrak{a}, 6\mathfrak{f}) = 1$, we have

$$\frac{\Theta^2(z,L_\sigma)^{\mathrm{N}\,\mathfrak{a}}}{\Theta^2(z,\alpha^{-1}L_\sigma)} = \prod_{\substack{w\in\alpha^{-1}L_\sigma/L_\sigma \\ w\neq 0}} (\wp(z,L_\sigma)-\wp(w,L_\sigma))^{-1},$$

so we can write

$$R_{\mathfrak{a}}^\sigma(\Phi(z,L_\sigma))^2 = c_E(\mathfrak{a})^2\frac{\Theta^2(z,L_\sigma)^{\mathrm{N}\,\mathfrak{a}}}{\Theta^2(z,\alpha^{-1}L_\sigma)},$$

since the product in the definition of $R_{\mathfrak{a}}^\sigma$ was over the representatives of $E_{\mathfrak{a}}\backslash\{\mathcal{O}\}$ modulo $\{\pm 1\}$, and $x(\ominus P) = x(P)$ for any P. Let $\rho = \Omega_\infty/f$ so that our choice of Q^σ is given by $\Phi(\Lambda(\mathfrak{s})\rho, L_\sigma)$. Moreover, let $\mathcal{B}$ be a set of integral ideals of K prime to $\mathfrak{f}$ such that

$$\mathrm{Gal}(H(E_{\mathfrak{f}})/K) = \{(\mathfrak{b}, H(E_{\mathfrak{f}})/K), \mathfrak{b}\in\mathcal{B}\},$$

where $(\mathfrak{b}, H(E_{\mathfrak{f}})/K)$ denotes the Artin symbol of $\mathfrak{b}$ for $H(E_{\mathfrak{f}})/K$. Hence, we have

$$\mathfrak{R}_{\mathfrak{a}}^\sigma(\Phi(z,L_\sigma)) = \prod_{\mathfrak{b}\in\mathcal{B}} R_{\mathfrak{a}}^\sigma\left(\Phi(z+\varphi_K(\mathfrak{b})\Lambda(\mathfrak{s})\rho, L_\sigma)\right).$$

Noting that $A(\alpha^{-1}L_\sigma) = \mathrm{N}\alpha^{-1}A(L_\sigma)$ and that $\mathcal{E}_k^*$ is homogeneous of degree $-k$, we obtain

$$\frac{d}{dz}\log \mathfrak{R}_{\mathfrak{a}}^{\sigma}(\Phi(z,L_\sigma)) = \sum_{k=1}^{\infty}(-1)^k \sum_{\mathfrak{b}\in\mathcal{B}} \left(\mathrm{N}\mathfrak{a}\mathcal{E}_k^*(\varphi_K(\mathfrak{b})\Lambda(\mathfrak{s})\rho, L_\sigma) - \alpha^k\mathcal{E}_k^*(\varphi_K(\mathfrak{b})\alpha\Lambda(\mathfrak{s})\rho, L_\sigma)\right) z^{k-1}.$$

By [10, Proposition 5.5], we have

$$\frac{\varphi_K^k(\mathfrak{s})}{\mathrm{N}\mathfrak{s}^{k-s}}\frac{(\overline{\Lambda(\mathfrak{s})\rho})^k}{|\Lambda(\mathfrak{s})\rho|^{2s}}L(\overline{\varphi}_K^k,\sigma,s) = \sum_{\mathfrak{b}\in\mathcal{B}} H_k(\varphi_K(\mathfrak{b})\Lambda(\mathfrak{s})\rho,0,s,L_\sigma),$$

and similarly,

$$\frac{\varphi_K^k(\mathfrak{s}\mathfrak{a})}{\mathrm{N}(\mathfrak{s}\mathfrak{a})^{k-s}}\frac{(\overline{\Lambda(\mathfrak{s})\alpha\rho})^k}{|\Lambda(\mathfrak{s})\alpha\rho|^{2s}}L(\overline{\varphi}_K^k,\sigma\sigma_{\mathfrak{a}},s) = \sum_{\mathfrak{b}\in\mathcal{B}} H_k(\varphi_K(\mathfrak{b})\Lambda(\mathfrak{s})\alpha\rho,0,s,L_\sigma).$$

Putting $s=k$, we obtain

$$\frac{d}{dz}\log \mathfrak{R}_{\mathfrak{a}}^{\sigma}(\Phi(z,L_\sigma)) = \sum_{k=1}^{\infty}(-1)^k\varphi_K^k(\mathfrak{s})\Lambda(\mathfrak{s})^{-k}f^k\Omega_\infty^{-k}\left(\mathrm{N}\mathfrak{a}L(\overline{\varphi}_K^k,\sigma,k) - \varphi_K^k(\mathfrak{a})L(\overline{\varphi}_K^k,\sigma\sigma_{\mathfrak{a}},k)\right) z^{k-1}.$$

The result now follows on noting that $\sigma_{\mathfrak{a}}=1$ because $\mathfrak{a}=(\alpha)$ is principal. □

Let us remark that Proposition 4.1.7 is true for all integers $k \geqslant 1$. However, the Hecke L-function will no longer be primitive when k is even, for example, if $k \equiv 0 \bmod \#(\Delta)$, because in this case the conductor of φ_K^k is (1). Thus we shall first concentrate on the case $k \equiv 1 \bmod \#(\Delta)$ but the arguments extend readily to k ranging over any fixed residue class modulo $\#(\Delta)$.

Lemma 4.1.8. *For any positive integer $k \equiv 1 \bmod \#(\Delta)$, we have*

$$\Lambda(\mathfrak{s})^{-k}\Omega_v^{-k}\int_{\mathfrak{H}}\chi_{\mathfrak{p}}^k d\mu_{\mathfrak{a},\sigma} = -(k-1)!\frac{\varphi_K^k(\mathfrak{s})f^k}{\Lambda(\mathfrak{s})^k\Omega_\infty^k}\left(\mathrm{N}\,\mathfrak{a} - \varphi_K^k(\mathfrak{a})\right)\left(L(\overline{\varphi}_K^k,\sigma,k) - \frac{\overline{\varphi}_K^k(\mathfrak{p})}{\mathrm{N}\mathfrak{p}}L(\overline{\varphi}_K^k,\sigma\sigma_{\mathfrak{p}},k)\right).$$

Proof. We have $\lambda_E(\mathfrak{p})\Phi(z,L_\sigma) = \Phi(\Lambda(\mathfrak{p})^\sigma z, L_{\sigma\sigma_{\mathfrak{p}}})$ and $\Lambda(\mathfrak{s}\mathfrak{p}) = \Lambda(\mathfrak{s})\Lambda(\mathfrak{p})^\sigma$, so

$$\left(\frac{d}{dz}\right)^k \log \mathfrak{R}_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{p}}}(\lambda_E(\mathfrak{p})\Phi(z,L_\sigma))|_{z=0} = -(k-1)!\frac{\varphi_K^k(\mathfrak{s}\mathfrak{p})f^k}{\Lambda(\mathfrak{s})^k\Omega_\infty^k}\left(\mathrm{N}\,\mathfrak{a} - \varphi_K^k(\mathfrak{a})\right)L(\overline{\varphi}_K^k,\sigma\sigma_{\mathfrak{p}},k)).$$

Therefore,

$$\left(\frac{d}{dz}\right)^k \log \Psi_{\mathfrak{a}}^{\sigma}(\Phi(z,L_\sigma))|_{z=0} = -c_k(\mathfrak{a})(k-1)!\frac{\varphi_K^k(\mathfrak{s})f^k\mathrm{N}\mathfrak{p}}{\Lambda(\mathfrak{s})^k\Omega_\infty^k}\left(L(\overline{\varphi}_K^k,\sigma,k) - \frac{\overline{\varphi}_K^k(\mathfrak{p})}{\mathrm{N}\mathfrak{p}}L(\overline{\varphi}_K^k,\sigma\sigma_{\mathfrak{p}},k)\right), \tag{4.1.8}$$

where $c_k(\mathfrak{a}) = \mathrm{N}\mathfrak{a} - \varphi_K^k(\mathfrak{a})$. Combining (4.1.5), (4.1.6), (4.1.8) and the fact that $\Omega_{\sigma,v} = \Lambda(\mathfrak{s})\Omega_v$ by Lemma 4.1.6, the proof of Proposition 4.1.8 is complete. □

Let

$$D_{\mathfrak{a},\sigma}(k) = \varphi_K(\mathfrak{s})^{-k} \int_{\mathfrak{H}} \chi_{\mathfrak{p}}^k d\mu_{\mathfrak{a},\sigma},$$

and define

$$G^* = \mathrm{Hom}(G, \mathbb{C}_p^\times),$$

where $G = \mathrm{Gal}(H/K)$ as before. Then for each $\chi \in G^*$, define

$$D_{\mathfrak{a}}(\chi, k) = \sum_{\sigma\in G} \chi(\sigma) D_{\mathfrak{a},\sigma}(k).$$

It is easy to see that

$$D_{\mathfrak{a}}(\chi, k) = c_k(\mathfrak{a})(k-1)! f^k \frac{\Lambda(\mathfrak{s})^k \Omega_v^k}{\Lambda(\mathfrak{s})^k \Omega_\infty^k} \sum_{\sigma\in G} \chi(\sigma) L(\overline{\varphi}_K^k, \sigma, k) \left(1 - \frac{\varphi_K^k(\mathfrak{p})\chi^{-1}(\sigma_{\mathfrak{p}})}{\mathrm{N}\mathfrak{p}}\right).$$

We let $\mathcal{C}$ denotes a set of integral ideals representing of the ideal class group of K with $(\mathfrak{c}, \mathfrak{p}\mathfrak{f}) = 1$ for any $\mathfrak{c} \in \mathcal{C}$, and set $\Omega_\infty(E/H) = \prod_{\mathfrak{c}\in\mathcal{C}} \Lambda(\mathfrak{c})\Omega_\infty$ and $\Omega_{\mathfrak{p}}(E/H) = \prod_{\mathfrak{c}\in\mathcal{C}} \Lambda(\mathfrak{c})\Omega_v$. Recalling

$$L(\overline{\psi}_{E/H}^k, k) = \prod_{\chi\in G^*} \sum_{\sigma\in G} \chi(\sigma) L(\overline{\varphi}_K^k, \sigma, k)$$

and the factorisation of primes of K in H given by class field theory, we immediately obtain the following.

Lemma 4.1.9. *For any positive integer $k \equiv 1 \bmod \#(\Delta)$, we have*

$$\prod_{\chi\in G^*} D_{\mathfrak{a}}(\chi, k) = c_k(\mathfrak{a})^h \left((k-1)!\right)^h f^{kh} \Omega_{\mathfrak{p}}(E/H)^k \Omega_\infty(E/H)^{-k} L(\overline{\psi}_{E/H}^k, k) \cdot \prod_{w|\mathfrak{p}} \left(1 - \frac{\psi_{E/H}^k(w)}{\mathrm{N}w}\right).$$

Define $\mathfrak{G} = \mathrm{Gal}(F_\infty/K)$. Write $\mu_{\mathfrak{a}}$ for the measure on $\mathfrak{G}$ satisfying

$$\int_{\mathfrak{G}} \chi_{\mathfrak{p}}^k d\mu_{\mathfrak{a}} := \prod_{\chi\in G^*} \int_{\mathfrak{G}^\chi} \chi\chi_{\mathfrak{p}}^k d(\mu_{\mathfrak{a}})^\chi = \prod_{\chi\in G^*} \sum_{\sigma\in G} \chi(\sigma)\varphi_K(\mathfrak{s})^{-k} \int_{\mathfrak{H}} \chi_{\mathfrak{p}}^k d\mu_{\mathfrak{a},\sigma}.$$

Thus

Lemma 4.1.10. *There exists a measure $\mu_{\mathfrak{a}}$ in $\Lambda_{\mathscr{I}}(\mathfrak{G})$ such that for all $k \geqslant 1$, $k \equiv 1 \bmod \#(\Delta)$, we have*

$$\Omega_{\mathfrak{p}}(E/H)^{-k}\int_{\mathfrak{G}}\chi_{\mathfrak{p}}^{k}d\mu_{\mathfrak{a}} = c_k(\mathfrak{a})^h\left((k-1)!\right)^h f^{kh}\Omega_\infty(E/H)^{-k}L(\overline{\psi}_{E/H}^{k},k)\cdot\prod_{w|\mathfrak{p}}\left(1-\frac{\psi_{E/H}^{k}(w)}{\mathrm{N}w}\right).$$

Note that, on the right hand side the equation in Lemma 4.1.10, the only dependence on $\mathfrak{a}$ occurs in the factor $c_k(\mathfrak{a})^h$. We remove this factor in the next theorem.

Theorem 4.1.11. *There exists a unique measure $\mu_E \in \Lambda_{\mathscr{I}}(\mathfrak{G})$ such that, for all integers $k \geqslant 1$ with $k \equiv 1 \bmod \#(\Delta)$, we have*

$$\Omega_{\mathfrak{p}}(E/H)^{-k}\int_{\mathfrak{G}}\chi_{\mathfrak{p}}^{k}d\mu_{E} = \left((k-1)!\right)^h f^{kh}\Omega_\infty(E/H)^{-k}L(\overline{\psi}_{E/H}^{k},k)\cdot\prod_{w|\mathfrak{p}}\left(1-\frac{\psi_{E/H}^{k}(w)}{\mathrm{N}w}\right).$$

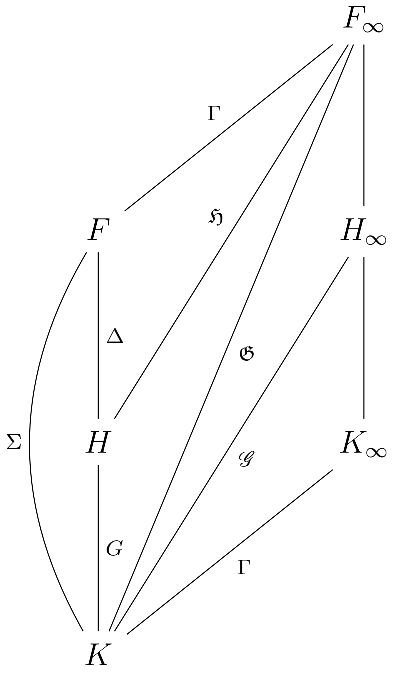
Proof. Given an integral ideal $\mathfrak{a}$ with $(\mathfrak{a}, 6\mathfrak{p}\mathfrak{f}) = 1$, let $\theta_{\mathfrak{a}}$ be the measure satisfying

$$\int_{\mathfrak{G}}\chi_{\mathfrak{p}}^{k}d\theta_{\mathfrak{a}} = c_k(\mathfrak{a})^h.$$

Then $\mu_E = \mu_{\mathfrak{a}}/\theta_{\mathfrak{a}}$ is independent of $\mathfrak{a}$. In order to show that this is an integral measure, it suffices to show that for some $\mathfrak{a}$, $c_k(\mathfrak{a})^h$ is a unit in $\mathscr{I}$. Pick $\mathfrak{a} = (\alpha)$ with $(\mathfrak{a},\mathfrak{p}) = 1$ such that $\alpha \equiv 1 \bmod \mathfrak{f}$ and $\alpha \not\equiv 1 \bmod \mathfrak{p}^*$. This is possible since we have $\mathfrak{p}^* \nmid \mathfrak{f}$ by hypothesis. Then $\varphi_K(\mathfrak{a}) = \alpha$, $\sigma_{\mathfrak{a}} = 1$, and $c_1(\mathfrak{a})^h = \alpha^h(\alpha^* - 1)^h$ is a unit in $\mathcal{O}_{\mathfrak{p}}$. This shows that there is a unit in $\mathscr{I}[[\mathfrak{G}]]$ whose values at k with $k \equiv 1 \bmod \#(\Delta)$ is equal to $c_k(\mathfrak{a})^h$.

□

Theorem 4.1.11 asserts the existence of a good $\mathfrak{p}$-adic L-function. Now, let us assume $(p,h) = 1$. Define $\Sigma = \mathrm{Gal}(F_\infty/K_\infty)$ where K_∞ is the maximal $\mathbb{Z}_p$-extension of K inside F_∞, so that $\Sigma \simeq \Delta \times G$. Furthermore, identify Γ with $\mathrm{Gal}(K_\infty/K)$. Let $H_\infty = HK_\infty$ and K_∞ is the unique $\mathbb{Z}_p$-extension of K unramified outside $\mathfrak{p}$, and define $\mathscr{G} = \mathrm{Gal}(H_\infty/K)$.



Given $\theta \in \Sigma^*$, let $\Lambda_{\mathscr{I}}(\mathfrak{G})^\theta$ denote the largest submodule of $\Lambda_{\mathscr{I}}(\mathfrak{G})$ on which Σ acts via θ. If $p > 2$, then $\#(\Sigma)$ is prime to p, so the idempotent $e_\theta = \frac{1}{\#(\Sigma)} \sum_{\tau\in\Sigma} \theta^{-1}(\tau)\tau$ lie inside $\Lambda_{\mathscr{I}}(\mathfrak{G})$. Thus we can decompose $\Lambda_{\mathscr{I}}(\mathfrak{G}) = \mathscr{I}[[\mathfrak{G}]] = \mathscr{I}[\Sigma][[\Gamma]]$ in the form

$$\Lambda_{\mathscr{I}}(\mathfrak{G}) = \oplus_{\theta\in\Sigma^*} e_\theta \Lambda_{\mathscr{I}}(\Gamma).$$

Therefore, we can write any $\mu \in \Lambda_{\mathscr{I}}(\mathfrak{G})$ as a sum of the form

$$\mu = \oplus_{\theta\in\Sigma^*} e_\theta \mu^\theta,$$

where μ^θ is an element of $\Lambda_{\mathscr{I}}(\Gamma)$.

If $p = 2$, $\#(\Delta) = 2$ is not coprime to p. In this case, let δ denote the non-trivial element of Δ. We have $\Lambda_{\mathscr{I}}(\mathfrak{G}) = \mathscr{I}[\Delta][[\mathscr{G}]]$. We claim $(1-\delta)\mathscr{I}[\Delta] = (1-\delta)\mathscr{I}$. Indeed, let $a_1 + a_\delta\delta \in \mathscr{I}[\Delta]$. Then $(1-\delta)(a_1 + a_\delta\delta) = (1-\delta)(a_1 - a_\delta) \in (1-\delta)\mathscr{I}$. Hence $(1-\delta)\mathscr{I}[\Delta] \subset (1-\delta)\mathscr{I}$, and the other inclusion is clear. It follows that $(1-\delta)\Lambda_{\mathscr{I}}(\mathfrak{G}) = (1-\delta)\Lambda_{\mathscr{I}}(\mathscr{G})$. Hence, given $\mu \in \Lambda_{\mathscr{I}}(\mathfrak{G})$, there exists unique $\mu^- \in \Lambda_{\mathscr{I}}(\mathscr{G})$ satisfying $(1-\delta)\mu = (1-\delta)\mu^-$. Similarly, we have $(1+\delta)\Lambda_{\mathscr{I}}(\mathfrak{G}) = (1+\delta)\Lambda_{\mathscr{I}}(\mathscr{G})$, so given $\mu \in \Lambda_{\mathscr{I}}(\mathfrak{G})$ there exists $\mu^+ \in \Lambda_{\mathscr{I}}(\mathscr{G})$ such that $(1+\delta)\mu = (1+\delta)\mu^+$. Furthermore, we have

$$\mu = \frac{1}{2}\left((1-\delta)\mu^- + (1+\delta)\mu^+\right).$$

Finally, since $(p, h) = 1$ by assumption, we can further decompose μ^- and μ^+ as elements in $\oplus_{\chi \in G^*} e_\chi \Lambda_{\mathscr{I}}(\Gamma)$.

For $k \equiv 1 \bmod \#(\Delta)$, we have $\chi_{\mathfrak{p}}^k(1+\delta) = 0$ and $\chi_{\mathfrak{p}}^k(1-\delta) = 2$. Thus, we obtain

$$\mu_E = \frac{1}{2}(1-\delta)\mu_E^-$$

interpolating the values of $L(\overline{\psi}_{E/H}^k, k)$ for $k \equiv 1 \bmod \#(\Delta)$ from the above construction.

Finally, we remark that our methods readily give an analogue of Theorem 4.1.11 for the $\mathfrak{p}$-adic interpolation of $L(\overline{\psi}_{E/H}^k, k)$ when k ranges over any fixed residue class modulo $\#(\Delta)$. However, the Hecke L-function will no longer be primitive when k is even, and in particular, when $k \equiv 0 \bmod \#(\Delta)$, because in this case the conductor of φ_K^k is (1). Let S denote the set of primes of H dividing $\mathfrak{f}$. Then Theorem 4.1.11 gives the imprimitive Hecke L-function $L_S(\overline{\psi}_{E/H}^k, k) = L(\overline{\psi}_{E/H}^k, k) \cdot \prod_{v \in S}\left(1 - \frac{\overline{\psi}_{E/H}^k(v)}{\mathrm{N}v^k}\right)$ on the complex side.

The aim of the next section will be to obtain a $\mathfrak{p}$-adic L-function which interpolates the values of the $L(\overline{\psi}_{E/H}^k, k)$ for k even. This will give rise to the $\mathfrak{p}$-adic L-function for H_∞/H for all p, and as we shall see in Chapter 7, will be an essential ingredient for the main conjecture for E/H for $p = 2$.

4.2 Construction of the $\mathfrak{p}$-adic L-function for H_∞/H

Let us now look at the case when k is even, so that the conductor of φ_K^k is (1). We write P_n^σ for a primitive $\mathfrak{p}^n$-division point of E^σ. Note that $R_{\mathfrak{a}}^\sigma(P)$ has a zero of order $\mathrm{N}\mathfrak{a} - 1$ at $P = \mathcal{O}$, and $R_{\mathfrak{a}}^\sigma(P_n^\sigma)$ is not a unit. To get rid of this zero at $P = \mathcal{O}$, define the index set

$$I = \{(\mathfrak{a}_i, n_i),\ \ i = 1, \dots, r,\ \mathfrak{a}_i = (\alpha_i) \subset \mathcal{O}, (\mathfrak{a}_i, 6\mathfrak{p}) = 1, n_i \in \mathbb{Z} \text{ with } \sum_{i=1}^r n_i(\mathrm{N}\mathfrak{a}_i - 1) = 0\}.$$

Given $\mathcal{D} = (\mathfrak{a}_i, n_i) \in I$, define

$$R_{\mathcal{D}}^\sigma(P_n^\sigma) = \prod_{i=1}^r R_{\mathfrak{a}_i}^\sigma(P_n^\sigma)^{n_i}.$$

Then $R_{\mathcal{D}}^\sigma(P)$ has no zero at $P = \mathcal{O}$, and $R_{\mathcal{D}}^\sigma(P_n)$ is a unit, as we will see in Corollary 4.3.7.

Definition 4.2.1. $G_k(L) = \sum\limits_{w \in L\setminus\{0\}} \frac{1}{w^k}$ for $k \geqslant 3$,

$$G_2(L) = \lim_{s \to 0+} \sum_{w \in L\setminus\{0\}} w^{-2}|w|^{-2s},$$

and $G_1(L) = 0$.

Proposition 4.2.2. *Let $\mathfrak{s}$ be an integral ideal of K prime to $\mathfrak{f}$ such that $\sigma_{\mathfrak{s}} = \sigma$. Then for any $\mathcal{D} = (\mathfrak{a}_i, n_i) \in I$ and $k \geqslant 2$ an even integer, we have*

$$\frac{d}{dz} \log R^\sigma_{\mathcal{D}}(P) = \sum_{i=1}^{r} \sum_{\substack{k=2 \\ k \text{ even}}}^{\infty} -n_i \frac{\varphi_K^k(\mathfrak{s})}{\Lambda(\mathfrak{s})^k \Omega_\infty^k} \left(\mathrm{N}\,\mathfrak{a}_i - \varphi_K^k(\mathfrak{a}_i)\right) L(\overline{\varphi}_K^k, \sigma, k))z^{k-1}.$$

In particular, we have

$$\left(\frac{d}{dz}\right)^k \log R^\sigma_{\mathcal{D}}(P)|_{z=0} = \sum_{i=1}^{r} -n_i(k-1)! \frac{\varphi_K^k(\mathfrak{s})}{\Lambda(\mathfrak{s})^k \Omega_\infty^k} \left(\mathrm{N}\,\mathfrak{a}_i - \varphi_K^k(\mathfrak{a}_i)\right) L(\overline{\varphi}_K^k, \sigma, k)).$$

Proof. We modify the usual σ-function slightly, and define

$$\Theta(z, L) = \exp\left\{-s_2(L)\frac{z^2}{2}\right\} \sigma(z, L).$$

Then for any integral ideal $\mathfrak{a} = (\alpha)$ with $(\mathfrak{a}, 6\mathfrak{f}) = 1$, we have

$$\frac{\Theta^2(z, L_\sigma)^{\mathrm{N}\,\mathfrak{a}}}{\Theta^2(z, \alpha^{-1}L_\sigma)} = \prod_{\substack{w \in \alpha^{-1}L_\sigma/L_\sigma \\ w \neq 0}} (\wp(z, L_\sigma) - \wp(w, L_\sigma))^{-1},$$

so we can write

$$R^\sigma_{\mathfrak{a}}(\Phi(z, L_\sigma))^2 = c_E(\mathfrak{a})^2 \frac{\Theta^2(z, L_\sigma)^{\mathrm{N}\,\mathfrak{a}}}{\Theta^2(z, \alpha^{-1}L_\sigma)},$$

since the product in the definition of $R^\sigma_{\mathfrak{a}}$ was over the representatives of $E_{\mathfrak{a}}\setminus\{\mathcal{O}\}$ modulo $\{\pm 1\}$, and $x(\ominus P) = x(P)$ for any P. Hence,

$$R^\sigma_{\mathcal{D}}(\Phi(z, L_\sigma))^2 = \prod_{i=1}^{r} \left(c_E(\mathfrak{a}_i)^2 \frac{\Theta^2(z, L_\sigma)^{\mathrm{N}\,\mathfrak{a}_i}}{\Theta^2(z, \alpha_i^{-1}L_\sigma)}\right)^{n_i}.$$

Now, (4.1.7) gives

$$\frac{d}{dz} \log \Theta(z, L_\sigma) = \sum_{k=1}^{\infty} (-1)^{k-1} G_k(L_\sigma) z^{k-1}$$

and $G_k(L_\sigma) = 0$ for k odd. Therefore,

$$\begin{aligned}\frac{d}{dz}\log R^\sigma_{\mathcal{D}}(\Phi(z, L_\sigma)) &= \sum_{i=1}^{r}\sum_{\substack{k\geqslant 2\\ k \text{ even}}} -n_i(\mathrm{N}\,\mathfrak{a}_i G_k(L_\sigma) - G_k(\alpha_i^{-1}L_\sigma))z^{k-1}\\ &= \sum_{i=1}^{r}\sum_{\substack{k\geqslant 2\\ k \text{ even}}} -n_i(\mathrm{N}\,\mathfrak{a}_i - \alpha_i^k)G_k(L_\sigma)z^{k-1}\end{aligned}$$

by the homogeneity of G_k.

Let $\mathfrak{b}$ be an ideal of K. Setting $k = s$, $\mathfrak{g} = (1)$ and $\rho = \Omega_\infty$ in [10, Proposition 5.5], we obtain that the partial Hecke L-function $L(\overline{\varphi}^k_K, \sigma_\mathfrak{b}, k)$ is identically equal to

$$G_k(L_{\sigma_\mathfrak{b}}) = \frac{\varphi^k_K(\mathfrak{b})}{\Lambda(\mathfrak{b})^k\Omega^k_\infty}L(\overline{\varphi}^k_K, \sigma_\mathfrak{b}, k).$$

Hence, setting $\mathfrak{b} = \mathfrak{s}$, we obtain

$$\begin{aligned}(\mathrm{N}\,\mathfrak{a}_i - \alpha_i^k)G_k(L_\sigma) &= \mathrm{N}\,\mathfrak{a}_i\frac{\varphi^k_K(\mathfrak{s})}{\Lambda(\mathfrak{s})\Omega^k_\infty}L(\overline{\varphi}^k_K, \sigma, k) - \frac{\varphi^k_K(\mathfrak{s}\mathfrak{a}_i)}{\Lambda(\mathfrak{s})\Omega^k_\infty}L(\overline{\varphi}^k_K, \sigma, k)\\ &= \frac{\varphi^k_K(\mathfrak{s})}{\Lambda(\mathfrak{s})^k\Omega^k_\infty}\left(\mathrm{N}\,\mathfrak{a}_i - \alpha_i^k\right)L(\overline{\varphi}^k_K, \sigma, k).\end{aligned}$$

This completes the proof of the proposition. □

Define

$$\Psi^\sigma_{\mathcal{D}}(P) = \frac{R^\sigma_{\mathcal{D}}(P)^{\mathrm{N}\mathfrak{p}}}{R^{\sigma\sigma_\mathfrak{p}}_{\mathcal{D}}(\lambda_{E^\sigma}(\mathfrak{p})(P))}.$$

Then we have

$$\prod_{R\in E^\sigma_\mathfrak{p}}\Psi^\sigma_{\mathcal{D}}(P\oplus R) = 1. \tag{4.2.1}$$

Let $A^\sigma_{\mathcal{D}}(t)$ be the development as a power series in t of the rational function $\Psi^\sigma_{\mathcal{D}}(P)$. Then as before, $A^\sigma_{\mathcal{D}}(t) \in 1 + \mathfrak{P}\mathcal{O}_\mathfrak{P}[[t]]$, and so $C^\sigma_{\mathcal{D}}(t) = \frac{1}{\mathrm{N}\mathfrak{p}}\log A^\sigma_{\mathcal{D}}(t) \in \mathcal{O}_\mathfrak{P}[[t]]$. Let $J^\sigma_{\mathcal{D}}(W) = C^\sigma_{\mathcal{D}}\circ\delta_{\sigma,v}(W) \in \mathscr{I}[[W]]$. Let $\mu_{\mathcal{D},\sigma}$ be the $\mathscr{I}$-valued measure on $\mathbb{Z}_p$ determined by $J^\sigma_{\mathcal{D}}(W)$. Then $\mu_{\mathcal{D},\sigma}$ is supported on $\mathbb{Z}_p^\times$, and writing also $\mu_{\mathcal{D},\sigma}$ for the corresponding measure on $\Lambda_{\mathscr{I}}(\mathfrak{H})$, we have

$$\int_\mathfrak{H}\chi^k_\mathfrak{p}d\mu_{\mathcal{D},\sigma} = \int_{\mathbb{Z}_p}x^k d\mu_{\mathcal{D},\sigma} = D^k J^\sigma_{\mathcal{D}}(W)|_{W=0}, \tag{4.2.2}$$

where $D = (1+W)\frac{d}{dW}$. We have an isomorphism $\hat{\mathbb{G}}_m \xrightarrow{\sim} \hat{\mathbb{G}}_a$ given by $W \mapsto e^z - 1$, hence we see immediately that $D = \frac{d}{dz}$. Moreover, we have $\delta_{\sigma,v}(W) = \Omega_{\sigma,v}W + \cdots$, so

$$D^k J^\sigma_{\mathcal{D}}(W)|_{W=0} = \left(\frac{d}{dz}\right)^k (J^\sigma_{\mathcal{D}}(e^z-1))|_{z=0} = \frac{1}{\mathrm{N}\mathfrak{p}}\Omega^k_{\sigma,v}\left(\frac{d}{dz}\right)^k \log \Psi^\sigma_{\mathcal{D}}(\Phi(z,L_\sigma))|_{z=0}. \tag{4.2.3}$$

Lemma 4.2.3. *For an even integer $k \geqslant 2$, we have*

$$\Lambda(\mathfrak{s})^{-k}{\Omega_v}^{-k}\int_{\mathfrak{H}} \chi^k_{\mathfrak{p}} d\mu_{\mathcal{D},\sigma} = \\ \sum_{i=1}^r -n_i(k-1)!\varphi^k_K(\mathfrak{s})\Lambda(\mathfrak{s})^{-k}\Omega^{-k}_\infty c_k(\mathfrak{a}_i)\left(L(\overline{\varphi}^k_K,\sigma,k) - \frac{\varphi^k_K(\mathfrak{p})}{\mathrm{N}\mathfrak{p}}L(\overline{\varphi}^k_K,\sigma\sigma_{\mathfrak{p}},k)\right),$$

where we recall that $c_k(\mathfrak{a}_i) = \mathrm{N}\mathfrak{a}_i - \alpha^k_i$.

Proof. We have $\lambda_E(\mathfrak{p})\Phi(z,L_\sigma) = \Phi(\Lambda(\mathfrak{p})^\sigma z, L_{\sigma\sigma_{\mathfrak{p}}})$ and $\Lambda(\mathfrak{s}\mathfrak{p}) = \Lambda(\mathfrak{s})\Lambda(\mathfrak{p})^\sigma$, so

$$\left(\frac{d}{dz}\right)^k \log R^{\sigma\sigma_{\mathfrak{p}}}_{\mathcal{D}}(\lambda_E(\mathfrak{p})\Phi(z,L_\sigma))|_{z=0} = \sum_{i=1}^r -n_i(k-1)!\frac{\varphi^k_K(\mathfrak{s}\mathfrak{p})}{\Lambda(\mathfrak{s})^k\Omega^k_\infty}c_k(\mathfrak{a}_i)L(\overline{\varphi}^k_K,\sigma\sigma_{\mathfrak{p}},k).$$

Therefore,

$$\left(\frac{d}{dz}\right)^k \log \Psi^\sigma_{\mathcal{D}}(\Phi(z,L_\sigma))|_{z=0} = \tag{4.2.4}\\ \sum_{i=1}^r -n_i(k-1)!\frac{\varphi^k_K(\mathfrak{s})\mathrm{N}\mathfrak{p}}{\Lambda(\mathfrak{s})^k\Omega^k_\infty}c_k(\mathfrak{a}_i)\left(L(\overline{\varphi}^k_K,\sigma,k) - \frac{\varphi^k_K(\mathfrak{p})}{\mathrm{N}\mathfrak{p}}L(\overline{\varphi}^k_K,\sigma\sigma_{\mathfrak{p}},k)\right).$$

Combining (4.2.2), (4.2.3) and (4.2.4), the proof of the proposition is complete. □

Let

$$D_{\mathcal{D},\sigma}(k) = \varphi_K(\mathfrak{s})^{-k}\int_{\mathfrak{H}} \chi^k_{\mathfrak{p}} d\mu_{\mathcal{D},\sigma},$$

and put for each $\chi \in G^*$,

$$D_{\mathcal{D}}(\chi,k) = \sum_{\sigma\in G}\chi(\sigma)D_{\mathcal{D},\sigma}(k).$$

Defining

$$M(\chi,k) = \sum_{\sigma\in G}\chi(\sigma)L(\overline{\varphi}^k_K,\sigma,k)\frac{\Lambda(\mathfrak{s})^k\Omega^k_v}{\Lambda(\mathfrak{s})^k\Omega^k_\infty},$$

we conclude immediately that

$$D_{\mathcal{D}}(\chi, k) = c_k(\mathcal{D})(k-1)!M(\chi, k)\left(1 - \frac{\varphi_K^k(\mathfrak{p})\chi^{-1}(\sigma_{\mathfrak{p}})}{\mathrm{N}\mathfrak{p}}\right),$$

where $c_k(\mathcal{D}) = \sum_{i=1}^{r} -n_i c_k(\mathfrak{a}_i)$. Let $\mathcal{C}$ denotes a set of integral ideals representing of the ideal class group of K with $(\mathfrak{c}, \mathfrak{p}\mathfrak{f}) = 1$ for any $\mathfrak{c} \in \mathcal{C}$, and set $\Omega_\infty(E/H) = \prod_{\mathfrak{c}\in\mathcal{C}} \Lambda(\mathfrak{c})\Omega_\infty$ and $\Omega_{\mathfrak{p}}(E/H) = \prod_{\mathfrak{c}\in\mathcal{C}} \Lambda(\mathfrak{c})\Omega_v$. Taking the product over $\chi \in G^*$, we obtain

Lemma 4.2.4. *For any even integer $k \geqslant 2$, we have*

$$\prod_{\chi\in G^*} D_{\mathcal{D}}(\chi, k) = c_k(\mathcal{D})^h \left((k-1)!\right)^h \Omega_{\mathfrak{p}}(E/H)^k \Omega_\infty(E/H)^{-k} L(\overline{\psi}_{E/H}^k, k) \cdot \prod_{w|\mathfrak{p}} \left(1 - \frac{\psi_{E/H}^k(w)}{\mathrm{N}w}\right).$$

Lemma 4.2.5. *There exists a measure $\nu_{\mathcal{D}}$ in $\Lambda_{\mathscr{I}}(\mathfrak{G})$ such that for all $k \geqslant 1$, $k \equiv 0 \bmod \#(\Delta)$, we have*

$$\Omega_{\mathfrak{p}}(E/H)^{-k} \int_{\mathfrak{G}} \chi_{\mathfrak{p}}^k d\nu_{\mathcal{D}} = c_k(\mathcal{D})^h \left((k-1)!\right)^h \Omega_\infty(E/H)^{-k} L(\overline{\psi}_{E/H}^k, k) \cdot \prod_{w|\mathfrak{p}} \left(1 - \frac{\psi_{E/H}^k(w)}{\mathrm{N}w}\right).$$

Note that, since $k \equiv 0 \bmod \#(\Delta)$, we have $\chi_{\mathfrak{p}}^k(\tau) = 1$ for any $\tau \in \Delta$. Hence, we can naturally consider $\nu_{\mathcal{D}}$ as an element of $\Lambda_{\mathscr{I}}(\mathscr{G})$. Again, the only dependence of $\nu_{\mathcal{D}}$ on $\mathcal{D}$ occurs in the factor $c_k(\mathcal{D})^h$. We claim that we can remove this factor and obtain a pseudo-measure which is independent of $\mathcal{D}$.

Lemma 4.2.6. *There exists $\mathcal{D} \in I$ and $\theta_{\mathcal{D}} \in \Lambda_{\mathscr{I}}(\mathscr{G})$ such that $\theta_{\mathcal{D}}|_\Gamma$ generates the augmentation ideal of $\Lambda_{\mathscr{I}}(\Gamma) \subset \Lambda_{\mathscr{I}}(\mathscr{G})$ and*

$$\int_{\mathscr{G}} \chi_{\mathfrak{p}}^k d\theta_{\mathcal{D}} = c_k(\mathcal{D})^h.$$

for all $k \geqslant 1$.

Proof. Choose $\alpha \in \mathcal{O}_K$ so that $\alpha \equiv 1 \bmod \mathfrak{p}^{m+1}$, $\alpha \equiv 1 + p^m \bmod \mathfrak{p}^{*m+1}$ where $m = 1$ or 2 according as $p > 2$ or $p = 2$, and define $\mathfrak{a} = (\alpha)$. Take $\mathfrak{a}_1 = \mathfrak{a}$, $\mathfrak{a}_2 = \overline{\mathfrak{a}}$, $n_1 = 1$, $n_2 = -1$. Then $(\{\mathfrak{a}_1, \mathfrak{a}_2\}, \{n_1, n_2\}) \in I$. Write $\sigma_{\mathfrak{a}}$ for the Artin symbol $(\mathfrak{a}, H_\infty/K)$ of $\mathfrak{a}$ for the extension H_∞/K. Note that $(\mathfrak{a}, H/K) = 1$ since $\mathfrak{a}$ is principal, so that we can consider $\sigma_{\mathfrak{a}}$ as an element of Γ.

We will show that the measure

$$\begin{aligned}\theta_{\mathcal{D}} &= -(\mathrm{N}\,\mathfrak{a} - \sigma_{\mathfrak{a}} - (\mathrm{N}\,\overline{\mathfrak{a}} - \sigma_{\overline{\mathfrak{a}}})) \\ &= \sigma_{\mathfrak{a}} - \sigma_{\overline{\mathfrak{a}}},\end{aligned}$$

has the desired property. Indeed, we have $\chi_{\mathfrak{p}}^k(\theta_{\mathcal{D}}) = c_k(\mathcal{D})^h$, so it remains to show that $\theta_{\mathcal{D}}|_\Gamma$ generates the augmentation ideal of $\mathscr{I}[[\Gamma]]$. In order to do this, let us fix a topological generator of γ of Γ, and write $\sigma_{\mathfrak{a}}|_\Gamma = \gamma^a$, $\sigma_{\overline{\mathfrak{a}}} = \gamma^b$ where $a, b \in \mathbb{Z}_p$. It suffices to show that $\theta_{\mathcal{D}}|_\Gamma = (1-\gamma)\cdot u$ for $u \in \mathbb{Z}_p[[\Gamma]]^\times$. Now, we have $\Gamma \simeq \mathbb{Z}_p$ and $\frac{1}{p^m}\log : 1 + p^m\mathbb{Z}_p \to \mathbb{Z}_p$ sending $1 + p^m x \mapsto \sum_{i=1}^{\infty}(-1)^{i-1}\left(\frac{x}{n}\right)^i$ is an isomorphism. Hence $\mathfrak{p}^{m+1} \mid \alpha - 1$ implies $a \equiv 0 \bmod p$, and α^* generates $1 + p^m\mathcal{O}_{\mathfrak{p}}$ so $b \not\equiv 0 \bmod p$. Now,

$$\begin{aligned}\sigma_{\mathfrak{a}}|_\Gamma - \sigma_{\overline{\mathfrak{a}}}|_\Gamma &= \gamma^a - \gamma^b \\ &= \gamma^a(1-\gamma^{b-a}),\end{aligned}$$

where clearly γ^a is a unit, and also $b - a \not\equiv 0 \bmod p$ so $1 - \gamma^{b-a}$ is a product of $(1-\gamma)$ and a unit, as required □

We define

$$\nu_{\mathfrak{p}} = \nu_{\mathcal{D}}/\theta_{\mathcal{D}}. \tag{4.2.5}$$

This is a pseudo-measure, since $(1-\gamma)\cdot\frac{1}{\theta_{\mathcal{D}}} = (1-\gamma)\cdot\frac{1}{(1-\gamma)u}$ where u is a unit by the proof of Lemma 4.2.6.

The following is an immediate consequence of Lemma 4.2.5 and Lemma 4.2.6.

Theorem 4.2.7. *There exists a unique element $\nu_{\mathfrak{p}}$ belonging to the quotient field $\Lambda_{\mathscr{I}}(\mathscr{G})$ such that, for all integers $k \geqslant 1$ with $k \equiv 0 \bmod \#(\Delta)$, we have*

$$\Omega_{\mathfrak{p}}(E/H)^{-k}\int_{\mathscr{G}}\chi_{\mathfrak{p}}^k d\nu_{\mathfrak{p}} = ((k-1)!)^h\,\Omega_\infty(E/H)^{-k}L(\overline{\psi}_{E/H}^k, k)\prod_{v\in P}\left(1 - \frac{\psi_{E/H}^k(v)}{\mathrm{N}v}\right).$$

Furthermore, the denominator of $\nu_{\mathfrak{p}}$ is given by $\gamma - 1$, so that $(\gamma-1)\nu_{\mathfrak{p}} \in \Lambda_{\mathscr{I}}(\mathscr{G})$.

Recall from Section 4.1 that we can decompose $\nu_{\mathfrak{p}}$ as a sum of elements in $e_\chi\Lambda_{\mathscr{I}}(\Gamma)$ if we in addition assume that $(p, h) = 1$. Given $\chi \in G^*$, let $\nu_{\mathfrak{p}}^\chi \in \Lambda_{\mathscr{I}}(\Gamma)$ denote the χ-part of $\nu_{\mathfrak{p}}$ in the decomposition. Then we have shown that $\nu_{\mathfrak{p}}^\chi \in \Lambda_{\mathscr{I}}(\Gamma)$ for every $\chi \neq 1$, and $(\gamma-1)\nu_{\mathfrak{p}}^\chi \in \Lambda_{\mathscr{I}}(\Gamma)$ for $\chi = 1$. Thus, identifying $\Lambda_{\mathscr{I}}(\Gamma)$ with $\mathscr{I}[[T]]$ via the map sending γ to $1+T$, we have $\nu_{\mathfrak{p}}^\chi \in \mathscr{I}[[T]]/T$ when χ is trivial. The pseudo-measure $\nu_{\mathfrak{p}}$ will be used for the main conjecture of H_∞/H.

Finally, we define the $\mathfrak{p}$-adic L-function attached to E/H. In Section 4.1 we showed that the $\mathfrak{p}$-adic L-function $\mu_E \in \Lambda_{\mathscr{I}}(\mathfrak{G})$ interpolates that values of $L(\overline{\psi}^k_{E/H}, k)$ when k is odd, and of $L_S(\overline{\psi}^k_{E/H}, k)$ when k is even, where S is the set of primes of H dividing $\mathfrak{f}$. Furthermore, our methods readily give an analogue of Theorem 4.2.7 to obtain $\nu_{\mathfrak{p}}$ which takes the value 0 at $\chi^k_{\mathfrak{p}}$ for k odd and interpolates the values of $L(\overline{\psi}^k_{E/H}, k)$ for k even.

Define $\boldsymbol{\Psi}_{\mathfrak{p}} = \mu_E + \nu_{\mathfrak{p}}$, where we consider $\nu_{\mathfrak{p}}$ as an element of $\Lambda_{\mathscr{I}}(\mathfrak{G})$. Explicitely, for $p = 2$ we can write

$$\boldsymbol{\Psi}_{\mathfrak{p}} = \frac{1}{2}\left((1-\delta)\mu_E^- + (1+\delta)\nu_{\mathfrak{p}}\right) \in \Lambda_{\mathscr{I}}(\mathfrak{G}).$$

Then $\boldsymbol{\Psi}_{\mathfrak{p}}$ interpolates the values of $L(\overline{\psi}^k_{E/H}, k)$ for k ranging over all the residue classes modulo $\#(\Delta)$ in the following way.

Theorem 4.2.8. *Given a positive integer k, we have*

$$\Omega_{\mathfrak{p}}(E/H)^{-k}\int_{\mathfrak{G}} \chi^k_{\mathfrak{p}} d\boldsymbol{\Psi}_{\mathfrak{p}} = \begin{cases} L(\overline{\psi}^k_{E/H}, k)\left(1 + f^{kh}\prod_{v\in S}\left(1 - \frac{\overline{\psi}^k_{E/H}(v)}{\mathrm{N}v^k}\right)\right)A(k) & \textit{if } k \textit{ is even} \\ L(\overline{\psi}^k_{E/H}, k) f^{kh} A(k) & \textit{if } k \textit{ is odd,} \end{cases}$$

where $A(k) = ((k-1)!)^h\, \Omega_\infty(E/H)^{-k}\prod_{w|\mathfrak{p}}\left(1 - \frac{\psi^k_{E/H}(w)}{\mathrm{N}w}\right)$.

4.3 Elliptic Units

In this section, we will show that

Theorem 4.3.1. *Suppose $\mathfrak{b}$ is a non-trivial ideal of $\mathcal{O}$ such that $(\mathfrak{b}, \mathfrak{a}) = 1$, and let P be a primitive $\mathfrak{b}$-division point of E^σ. Then $R^\sigma_{\mathfrak{a}}(P) \in K(\mathfrak{b})$.*

Proof. Recall that $R^\sigma_{\mathfrak{a}}$ is defined over H, so that it belongs to the function field $H(E^\sigma)$. Let x be any element of $\mathcal{O}$ satisfying $x \equiv 1 \bmod \mathfrak{b}$. These Artin symbols $\tau = (x, K^{\mathrm{ab}}/K)$ generate $\mathrm{Gal}(K^{\mathrm{ab}}/K(\mathfrak{b}))$. Moreover, it satisfies

$$R^\sigma_{\mathfrak{a}}(P)^\tau = R^{\sigma\sigma_x}_{\mathfrak{a}}(\lambda_{E^\sigma}(x)P) = R^\sigma_{\mathfrak{a}}(P),$$

giving $R^\sigma_{\mathfrak{a}}(P) \in K(\mathfrak{b})$, as required. □

Proposition 4.3.2. *Suppose $\mathfrak{m}$ is an ideal of $\mathcal{O}$ prime to $\mathfrak{a}\mathfrak{f}$, $P \in E^\sigma_{\mathfrak{m}}$ is a primitive $\mathfrak{m}$-division point of E^σ and $\mathfrak{r}$ is a prime ideal of K dividing $\mathfrak{m}$, say $\mathfrak{m} = \mathfrak{m}'\mathfrak{r}$. Then*

$$\mathrm{N}_{K(\mathfrak{m})/K(\mathfrak{m}')}R_{\mathfrak{a}}^{\sigma}(P) = \begin{cases} R_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{r}}}\left(\lambda_{E^\sigma}(\mathfrak{r})(P)\right)^{1-\mathrm{Frob}_{\mathfrak{r}}^{-1}} & \textit{if } \mathfrak{r} \nmid \mathfrak{m}' \\ R_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{r}}}\left(\lambda_{E^\sigma}(\mathfrak{r})(P)\right) & \textit{if } \mathfrak{r} \mid \mathfrak{m}'. \end{cases}$$

where Frob$_{\mathfrak{r}}$ *denotes the Frobenius of* $\mathfrak{r}$ *in* $\mathrm{Gal}(K(\mathfrak{m}')/K)$*, and* $\mathrm{N}_{K(\mathfrak{m})/K(\mathfrak{m}')}$ *denotes the norm map from* $K(\mathfrak{m})$ *to* $K(\mathfrak{m}')$*.*

Proof. Since the reduction mod $\mathfrak{m}$ map $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{m})^\times$ is injective, the kernel of the map

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

is isomorphic to the multiplicative group $1+\mathfrak{m}'(\mathcal{O}/\mathfrak{m})$. Thus, we have an isomorphism

$$\tau : 1+\mathfrak{m}'(\mathcal{O}/\mathfrak{m}) \xrightarrow{\sim} \mathrm{Gal}(K(\mathfrak{m})/K(\mathfrak{m}'))$$

by class field theory. Note that $\mathrm{Gal}(K(\mathfrak{m})/K(\mathfrak{m}'))$ has size $\mathrm{N}\mathfrak{q}-1$ or $\mathrm{N}\mathfrak{q}$ according as $\mathfrak{r}\nmid\mathfrak{m}'$ or $\mathfrak{r}\mid\mathfrak{m}'$, and the conjugates of P over $\mathrm{Gal}(K(\mathfrak{m})/K(\mathfrak{m}'))$ are given by

$$\{(P)^\tau : \tau \in \mathrm{Gal}(K(\mathfrak{m})/K(\mathfrak{m}'))\} = \begin{cases} \{P+Q : Q \in E_{\mathfrak{q}}^{\sigma}, P+Q \notin E_{\mathfrak{m}'}^{\sigma}\} & \text{if } \mathfrak{r}\nmid\mathfrak{m}' \\ \{P+Q : Q\in E_{\mathfrak{q}}^{\sigma}\} & \text{if } \mathfrak{r}\mid\mathfrak{m}'. \end{cases}$$

Hence, if r $\mid \mathfrak{m}'$, we have

$$\mathrm{N}_{K(\mathfrak{m})/K(\mathfrak{m}')}R_{\mathfrak{a}}^{\sigma}(P) = \prod_{Q\in E_{\mathfrak{r}}^{\sigma}} \left(R_{\mathfrak{a}}^{\sigma}(P+Q)\right)$$

and the right hand side is equal to $R_{\mathfrak{a}}^{\sigma\sigma_\pi}\left(\lambda_{E^\sigma}(\mathfrak{r})(P)\right)$ by Proposition 4.1.1. On the other hand, if $\mathfrak{r}\nmid\mathfrak{m}'$, we have

$$R_{\mathfrak{a}}^{\sigma}(P+Q_0)\mathrm{N}_{K(\mathfrak{m})/K(\mathfrak{m}')}R_{\mathfrak{a}}^{\sigma}(P) = \prod_{Q\in E_{\mathfrak{r}}^{\sigma}} \left(R_{\mathfrak{a}}^{\sigma}(P+Q)\right),$$

where $Q_0 \in E_{\mathfrak{r}}^{\sigma}$ satisfies $P+Q_0 \in E_{\mathfrak{m}'}^{\sigma}$. The rest follows on noting that

$$R_{\mathfrak{a}}^{\sigma}(P+Q)^{\mathrm{Frob}_{\mathfrak{r}}} = R_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{r}}}(\lambda_{E^\sigma}(\mathfrak{r})(P)+\lambda_{E^\sigma}(\mathfrak{r})(Q)) = R_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{r}}}(\lambda_{E^\sigma}(\mathfrak{r})(P)).$$

□

Definition 4.3.3. For $n \geqslant 1$, let $P_n^\sigma = \Phi(\rho, L_\sigma)$ be a primitive $\mathfrak{p}^n$-division point on E^σ satisfying $\lambda_{E^\sigma}(\mathfrak{p})P_n^\sigma = P_{n-1}^{\sigma\sigma_{\mathfrak{p}}}$. Given an integral ideal $\mathfrak{b}$ of K prime to $\mathfrak{a}$, the image of P_n^σ under the Artin symbol of $\mathfrak{b}$ for $H(E_{\mathfrak{p}^n})/K$ is $\lambda_{E^\sigma}(\mathfrak{b})(P_n^\sigma)$, so a choice of $(P_n^\sigma)^{\sigma_{\mathfrak{b}}}$

for the Artin symbol of $\sigma_{\mathfrak{b}}$ of $\mathfrak{b}$ for H/K is given by

$$(P_n^\sigma)^{\sigma_{\mathfrak{b}}} = \Phi(\Lambda(\mathfrak{b})^\sigma \rho, L_{\sigma\sigma_{\mathfrak{b}}}),$$

which is a point on $E^{\sigma\sigma_{\mathfrak{b}}}$.

Lemma 4.3.4. *Suppose $\mathfrak{q}$ is any prime with $(\mathfrak{q}, \mathfrak{a}) = 1$ and Q_m is a primitive $\mathfrak{q}^m$-division point on E^σ. Let $R \in E_{\mathfrak{b}}^\sigma$ for some $\mathfrak{b}$ with $(\mathfrak{b}, \mathfrak{a}\mathfrak{q}) = 1$. For any integer $m \geqslant 2 + e$, we have*

$$\mathrm{N}_{H(E_{\mathfrak{p}^m\mathfrak{b}})/H(E_{\mathfrak{p}^{m-1}\mathfrak{b}})} R_{\mathfrak{a}}^\sigma(Q_m \oplus R) = R_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{q}}}(\lambda_{E^\sigma}(\mathfrak{q})(Q_m) \oplus R^{\sigma_{\mathfrak{q}}}),$$

where $\sigma_{\mathfrak{q}} = (\mathfrak{q}, H/K)$ denotes the Artin symbol of $\mathfrak{q}$ for the extension H/K.

In particular, in the case $\mathfrak{q} = \mathfrak{p}$, we have

$$\mathrm{N}_{H(E_{\mathfrak{p}^m\mathfrak{b}})/H(E_{\mathfrak{p}^{m-1}\mathfrak{b}})} R_{\mathfrak{a}}^\sigma(P_m^\sigma \oplus R) = R_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{p}}}(P_{m-1}^{\sigma\sigma_{\mathfrak{p}}} \oplus R^{\sigma_{\mathfrak{p}}}),$$

where $\sigma_{\mathfrak{p}} = (\mathfrak{p}, H/K)$ denotes the Artin symbol of $\mathfrak{p}$ for the extension H/K.

Proof. Since $m \geqslant 2 + e$, the conjugates of Q_m over $H(E_{\mathfrak{q}^{m-1}})$ are $Q_m \oplus S$ where S runs over $E_{\mathfrak{q}}^\sigma$ by Lubin–Tate theory. Now, we have $H(E_{\mathfrak{q}^m\mathfrak{b}}) = H(E_{\mathfrak{q}^{m-1}\mathfrak{b}})H(E_{\mathfrak{q}^m})$ and $H(E_{\mathfrak{q}^{m-1}\mathfrak{b}}) \cap H(E_{\mathfrak{q}^m}) = H(E_{\mathfrak{q}^{m-1}})$. Hence the conjugates of $Q_m \oplus R$ over $H(E_{\mathfrak{q}^{m-1}\mathfrak{b}})$ are $Q_m \oplus R \oplus S$ where S runs over $E_{\mathfrak{q}}^\sigma$. Hence, we have

$$\begin{aligned}\mathrm{N}_{H(E_{\mathfrak{q}^m\mathfrak{b}})/H(E_{\mathfrak{q}^{m-1}\mathfrak{b}})} R_{\mathfrak{a}}^\sigma(P_m^\sigma \oplus R) &= \prod_{S \in E_{\mathfrak{q}}^\sigma} R_{\mathfrak{a}}^\sigma(Q_m \oplus R \oplus S) \\ &= R_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{q}}}(\lambda_{E^\sigma}(\mathfrak{q})\,(Q_m) \oplus \lambda_{E^\sigma}(\mathfrak{q})(R))\end{aligned}$$

by Proposition 4.1.1. Since $\lambda_{E^\sigma}(\mathfrak{q})(R) = R^{\sigma_{\mathfrak{q}}}$ for $R \in E_{\mathfrak{b}}^\sigma$, the first statement is now clear. The second statement follows since $\lambda_{E^\sigma}(\mathfrak{p})(P_m^\sigma) = P_{m-1}^{\sigma\sigma_{\mathfrak{q}}}$ by definition. □

Corollary 4.3.5. *For any integer $m \geqslant 2$, we have*

$$\mathrm{N}_{F_m/F_{m-1}} R_{\mathfrak{a}}^\sigma(P_m^\sigma) = R_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{p}}}(P_{m-1}^{\sigma\sigma_{\mathfrak{p}}}),$$

where $\sigma_{\mathfrak{p}} = (\mathfrak{p}, H/K)$ denotes the Artin symbol of $\mathfrak{p}$ for the extension H/K.

Proof. Write $\Phi(v, L_\sigma) = P_m^\sigma$. The conjugates $\Phi(v, L_\sigma)^\tau$ of $\Phi(v, L_\sigma)$ as τ runs over $\mathrm{Gal}(F_{mh}/F_{(m-1)h})$ are $\Phi(v + u, L_\sigma)$ for $\Phi(u, L_\sigma) \in E_{\mathfrak{p}}^\sigma$. Hence

$$\mathrm{N}_{m,n} R_{\mathfrak{a}}^\sigma(\Phi(v, L_\sigma)) = \prod_{u \in \mathfrak{p}^{-1}L_\sigma/L_\sigma} R_{\mathfrak{a}}^\sigma(\Phi(v + u, L_\sigma)).$$

But by Proposition 4.1.1, the right hand side is equal to $R_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{p}}}(\lambda_{E^\sigma}(\mathfrak{p})(\Phi(v, L_\sigma))) = R_{\mathfrak{a}}^{\sigma\sigma_{\mathfrak{p}}}\left(\Phi(\Lambda(\mathfrak{p})^\sigma v, L_{\sigma\sigma_{\mathfrak{p}}}))\right)$, and $\Phi(\Lambda(\mathfrak{p})^\sigma v, L_{\sigma\sigma_{\mathfrak{p}}}))$ is a primitive $\mathfrak{p}^{m-1}$ torsion point of $E^{\sigma\sigma_{\mathfrak{p}}}$. Hence $\Phi(\Lambda(\mathfrak{p})^\sigma v, L_{\sigma\sigma_{\mathfrak{p}}})) = P_{m-1}^{\sigma\sigma_{\mathfrak{p}}}$ by the choice of $\mathfrak{p}$-power torsion points specified in Definition 4.3.3. □

Let L be an arbitrary finite extension of K. We say that $a \in L$ is a *universal norm* from $L(E_{\mathfrak{p}^\infty})$ if it is a norm from $L(E_{\mathfrak{p}^n})$ for every $n \geqslant 0$. The following is well-known (see [3, Lemma 5]).

Lemma 4.3.6. *Let L be a finite extension of K, and $a \in L^\times$ a universal norm from $L(E_{\mathfrak{p}^\infty})$. Then every prime which divides a lies above $\mathfrak{p}$.*

Corollary 4.3.7. *$\mathfrak{R}_{\mathfrak{a}}^\sigma(P_n^\sigma)$ and $R_{\mathcal{D}}^\sigma(P_n^\sigma)$ are global units.*

Proof. It is clear from the definition of $\mathfrak{R}_{\mathfrak{a}}^\sigma(P_n^\sigma)$ that it suffices to show $R_{\mathfrak{a}}(P_n \oplus R)$ is a unit for any primitive f-division point R on E. By Lemma 4.3.4, the sequence $R_{\mathfrak{a}}(P_m \oplus Q)$ $(m = 1, 2, \ldots)$ is norm compatible in the tower $H(E_{\mathfrak{p}^\infty\mathfrak{f}})$ over $H(E_{\mathfrak{p}^e\mathfrak{f}})$. It follows that $R_{\mathfrak{a}}(P_n \oplus R)$ is a universal norm from $H(E_{\mathfrak{p}^\infty\mathfrak{f}}) = L(E_{\mathfrak{p}^\infty})$, where $L = H(E_{\mathfrak{f}})$. Thus by Lemma 4.3.6, every prime occurring in the factorisation of $R_{\mathfrak{a}}(P_n \oplus R)$ lies above $\mathfrak{p}$. However, we can pick any prime $\mathfrak{q}$ dividing $\mathfrak{f}$, then $\mathfrak{q} \neq \mathfrak{p}$ and we can apply the same argument by writing $P_n \oplus Q$ as a sum of a $\mathfrak{q}$-power division point and a point $W \in E_{\mathfrak{b}}$ with $(\mathfrak{b}, \mathfrak{q}) = 1$. Thus $\mathfrak{R}_{\mathfrak{a}}^\sigma(P_n^\sigma)$ is a unit.

Next, we note that if $\mathcal{D} = (\mathfrak{a}_i, n_i)$, then $R_{\mathfrak{a}_i}^\sigma(P_n^\sigma)$ is a unit outside $\mathfrak{p}$ again by Lemma 4.3.6 because $R_{\mathfrak{a}_i}^\sigma(P_m^\sigma)$ $(m = 1, 2, \ldots)$ is norm compatible in the tower F_∞ over F by Corollary 4.3.5. If $\mathfrak{P} \mid \mathfrak{p}$ is a prime of F_n, we have $\mathrm{ord}_{\mathfrak{P}}(x(P_n^\sigma)) < 0$ but $\mathrm{ord}_{\mathfrak{P}}(x(U)) \geqslant 0$ for any $U \in E_{\mathfrak{a}}^\sigma \backslash \{\mathcal{O}\}$, giving

$$\mathrm{ord}_{\mathfrak{P}}(x(P_n^\sigma) - x(U)) = \mathrm{ord}_{\mathfrak{P}}(x(P_n^\sigma)).$$

Recalling that $\mathrm{ord}_{\mathfrak{P}}(c_E(\mathfrak{a})) = 0$, we have

$$\mathrm{ord}_{\mathfrak{P}}(R_{\mathfrak{a}_i}^\sigma(P_n^\sigma)) = \frac{1}{2}(\mathrm{N}\mathfrak{a}_i - 1)\,\mathrm{ord}_{\mathfrak{P}}(x(P_n^\sigma)),$$

because $(E_{\mathfrak{a}}^\sigma \backslash \{\mathcal{O}\})/\{\pm 1\}$ has order $\frac{1}{2}(\mathrm{N}\mathfrak{a}_i - 1)$. Hence

$$\mathrm{ord}_{\mathfrak{P}}(R_{\mathcal{D}}^\sigma(P_n^\sigma)) = \frac{1}{2}\,\mathrm{ord}_{\mathfrak{P}}(x(P_n^\sigma)) \sum_i n_i(\mathrm{N}\mathfrak{a}_i - 1) = 0,$$

since $\sum_i n_i(\mathrm{N}\mathfrak{a}_i - 1) = 0$ by the definition of $\mathcal{D}$. It follows that $R_{\mathcal{D}}^\sigma(P_n^\sigma)$ is a unit. This completes the proof of Corollary 4.3.7.

□

Definition 4.3.8. Let $H_n = F_n \cap H_\infty$. Let U_{H_n} denote the group of semi-local units of $H_n \otimes_K K_\mathfrak{p} = \oplus_{\mathfrak{P}|\mathfrak{p}} H_{n,\mathfrak{P}}$ which are congruent to 1 modulo the primes above $\mathfrak{p}$. We denote by U_{H_∞} the projective limit of the groups U_{H_n} with respect to the norm maps. We define the group of elliptic units $\mathcal{C}_{H_n}$ to be the group generated by $R_\mathcal{D}^\sigma(P_n^\sigma)$ for all $\sigma \in G$, where P_n^σ is a primitive $\mathfrak{p}^n$-division point on E^σ, as $\mathcal{D}$ runs over the index set I. Note also that the roots of unity in H_n are just $\{\pm 1\}$. We let $\bar{\mathcal{C}}_{H_n}$ denote the closure of $\mathcal{C}_{H_n}$ in U_{H_n}, and define

$$\bar{\mathcal{C}}_{H_\infty} = \varprojlim \bar{\mathcal{C}}_{H_n} \subset U_{H_\infty}$$

where the inverse limit is taken with respect to the norm maps.

Similarly, let U_{F_n} denote the group of semi-local units of $F_n \otimes_K K_\mathfrak{p} = \oplus_{\mathfrak{P}|\mathfrak{p}} F_{n,\mathfrak{P}}$ which are congruent to 1 modulo the primes above $\mathfrak{p}$, and denote by U_{F_∞} the projective limit of the groups U_{F_n} with respect to the norm maps. Let $\mathcal{C}_{F_n}$ denote the group generated by $w_n := \mathfrak{R}_\mathfrak{a}^\sigma(P_n^\sigma)$ for all $\sigma \in G$, $\bar{\mathcal{C}}_{F_n}$ the closure of $\mathcal{C}_{F_n}$ in U_{F_n}, and write

$$\bar{\mathcal{C}}_{F_\infty} = \varprojlim \bar{\mathcal{C}}_{F_n} \subset U_{F_\infty}.$$

Proposition 4.3.9. *For all positive integers $m \geqslant n$, we have*

$$\mathrm{N}_{H_m/H_n} \bar{\mathcal{C}}_{H_m} = \bar{\mathcal{C}}_{H_n},$$

where N_{H_m/H_n} denotes the norm map from H_m to H_n.

Proof. By Corollary 4.3.5, we have $\mathrm{N}_{H_m/H_n} R_\mathcal{D}^\sigma(P_m^\sigma) = R_\mathcal{D}^{\sigma\sigma_\pi^{m-n}}(P_n^{\sigma\sigma_\pi^{m-n}})$. Hence we have

$$\mathrm{N}_{H_m/H_n} \mathcal{C}_{H_m} = \mathcal{C}_{H_n}$$

modulo roots of unity in H_n, which is just $\{\pm 1\}$. But -1 is not a universal norm, so this completes the proof of the proposition. □

Given $\mathfrak{u} = (u_n) \in U_{F_\infty}$, let $g_\mathfrak{u}(W) \in \mathcal{O}_H \otimes_\mathcal{O} \mathcal{O}_\mathfrak{p}[[W]]$ denote the Coleman power series of $\mathfrak{u}$ (see [8, Theorem 2.2] for more details). We write

$$\widetilde{\log}\, g_\mathfrak{u}(W) = \log\, g_\mathfrak{u} - \frac{1}{p} \sum_{\omega \in \mathcal{D}_{\sigma,\mathfrak{p}}} g_\mathfrak{u}(W[+]\omega),$$

where we recall that $\mathcal{D}_{\sigma,\mathfrak{p}} = \hat{E}^{\sigma}_{\mathfrak{p}}$ can be identified with $E^{\sigma}_{\mathfrak{p}}$. It is well-known [8, Lemma I.3.3] that $\widetilde{\log}\, g_{\mathfrak{u}}(W)$ has integral coefficients. Define

$$i : U_{F_\infty} \to \Lambda_{\mathscr{I}}(\mathfrak{G})$$

by

$$\mathfrak{u} \mapsto \mu_{\mathfrak{u}} := \prod_{\chi \in G^*} \sum_{\sigma \in G} \chi(\sigma)\varphi_K(\mathfrak{s})^{-k}\mu_{\mathfrak{u},\sigma},$$

where $\mu_{\mathfrak{u},\sigma}$ is the measure satisfying

$$\widetilde{\log}\, g_{\mathfrak{u}} \circ \delta_{\sigma,v}(W) = \int_{\mathfrak{H}} (1+W)^{\chi_{\mathfrak{p}}(\tau)} d\mu_{\mathfrak{u},\sigma}(\tau). \tag{4.3.1}$$

Let $\mathfrak{u}_{\mathfrak{a}} = (\mathfrak{R}^{\sigma}_{\mathfrak{a}}(P^{\sigma}_{n})) \in \bar{\mathcal{C}}_{F_\infty}$. Then by construction, $\widetilde{\log}\, g_{\mathfrak{u}_{\mathfrak{a}}} = C^{\sigma}_{\mathfrak{a}}$ where $C^{\sigma}_{\mathfrak{a}}$ is defined in Lemma 4.1.4, and thus $i(\mathfrak{u}_{\mathfrak{a}}) = \mu_{\mathfrak{a}} = \prod_{\chi \in G^*} \sum_{\sigma \in G} \chi(\sigma)\varphi_K(\mathfrak{s})^{-k}\mu_{\mathfrak{a},\sigma}$. Similarly, letting $\mathfrak{u}_{\mathcal{D}} = (R^{\sigma}_{\mathcal{D}}(P^{\sigma}_{n})) \in \bar{\mathcal{C}}_{H_\infty}$, we have $i(\mathfrak{u}_{\mathcal{D}}) = \nu_{\mathcal{D}}$.

Proposition 4.3.10. *The homomorphism*

$$i : U_{F_\infty} \to \Lambda_{\mathscr{I}}(\mathfrak{G}).$$

is an injective pseudo-isomorphism.

Proof. Let $\mathfrak{P}$ be any prime of F_∞ above $\mathfrak{p}$, and let $\Phi_\infty = \cup \Phi_n$ where Φ_n denotes the completion of F_n at $\mathfrak{P}$. Let K_∞ denote the unique $\mathbb{Z}_p$-extension of K unramified outside $\mathfrak{p}$, and let $K_{\infty,\mathfrak{P}}$ denote its completion at $\mathfrak{P}$. We will show that $|\mu_{p^\infty}(\Phi_\infty)|$ is finite by class field theory. To see this, note that $K_{\mathfrak{p}} = \mathbb{Q}_p$ since p splits in K. Then the kernel of the local Artin map

$$(\cdot, K_{\mathfrak{p}}(\mu_{p^\infty})/K_{\mathfrak{p}}) : (K_{\mathfrak{p}})^\times \to \mathrm{Gal}(K_{\mathfrak{p}}(\mu_{p^\infty})/K_{\mathfrak{p}})$$

is the free group $\langle p \rangle$ generated by p (see Prop 1.8 of [Neu]). Assume, on the contrary, that all p-power roots of unity are contained in Φ_∞. Then the kernel of the local Artin map

$$(\cdot, \Phi_\infty/K_{\mathfrak{p}}) : (K_{\mathfrak{p}})^\times \to \mathrm{Gal}(\Phi_\infty/K_{\mathfrak{p}})$$

is a subgroup of $\langle p \rangle$ of finite index. Denote by $K_{\mathfrak{p}^*}$ the completion of K at $\mathfrak{p}^*$ and let $K_{\infty,\mathfrak{P}^*}$ be the completion K_∞ at $\mathfrak{P}^*$. Let $\Phi'_\infty = \cup \Phi'_n$ where Φ'_n denotes the completion of F_n at $\mathfrak{P}^*$. Then $K_{\infty,\mathfrak{P}^*}/K_{\mathfrak{p}^*}$ is an infinite unramified extension isomorphic to $\mathbb{Z}_p$ which is topologically generated by $(p, K_{\infty,\mathfrak{P}^*}/K_{\mathfrak{p}^*})$. By the product formula. we have

$(p, K_{\infty,\mathfrak{P}^*}/K_{\mathfrak{p}^*})|_{K_\infty} = (p^{-1}, K_{\infty,\mathfrak{P}}/K_{\mathfrak{p}})|_{K_\infty}$, since K_∞/K is unramified outside $\mathfrak{p}$. Hence we have $(p^n, \Phi_\infty/K_{\mathfrak{p}}) \neq 1$ for all nonzero integer n. This shows that $(\cdot, \Phi_\infty/K_{\mathfrak{p}})$ is injective, which is absurd. Hence $|\mu_{p^\infty}(\Phi_\infty)|$ is finite as claimed. Now it follows from [8, §I, Theorem 3.7] that the cokernel of i is finite. Also i is injective because given $\mathfrak{u} \in U_{F_\infty}$, $\mathfrak{u} \neq 1$, the corresponding $g_{\mathfrak{u}}$ is non-constant and it satisfies (4.3.1). Hence i is an injective pseudo-isomorphism. □

Lemma 4.3.11. *We have*

$$i(\bar{\mathcal{C}}_{F_\infty}) = J \cdot \mu_E,$$

where J is the annihilator of $\mu_{p^\infty}(F_\infty)$ in $\mathbb{Z}_p[[\mathfrak{G}]]$.

Proof. Recall that $i(\mathfrak{u}_{\mathfrak{a}}) = \mu_{\mathfrak{a}} = \theta_{\mathfrak{a}} \cdot \mu_E$, where μ_E, $\theta_{\mathfrak{a}}$ are defined after Theorem 4.1.11. Hence we just need to show that $J \cdot \Lambda_{\mathscr{I}}(\mathfrak{G})$ is generated by $\theta_{\mathfrak{a}}$, $(\mathfrak{a}, 6\mathfrak{p}\mathfrak{f}) = 1$. For this, it is enough to check that these elements generate a dense subset. Define a positive integer N by $\mu(F_n) = \mu_N$, where we know $\mu_{p^n} \subset \mu_N$ by the Weil-pairing. Let

$$\chi_{\text{cyc}} : \text{Gal}(\overline{K}/K) \to (\mathbb{Z}/N\mathbb{Z})^\times$$

denote the cyclotomic character, defined by $\sigma(\zeta) = \zeta^{\chi_{\text{cyc}}(\sigma)}$ for all $\sigma \in \text{Gal}(\overline{K}/K)$ and $\zeta \in \mu_N$. Write $\mathfrak{G}_n$ for the group $\text{Gal}(F_n/K)$. Then the annihilator of $\mu(F_n)$ as a $\mathbb{Z}/N\mathbb{Z}[\mathfrak{G}_n]$-module is generated by

$$\sigma|_{\mathfrak{G}_n} - \chi_{\text{cyc}}(\sigma)$$

where σ runs over $\text{Gal}(\overline{K}/K)$. To see this, note that every element of $\mathbb{Z}/N\mathbb{Z}[\mathfrak{G}_n]$ is a finite sum, and it is clear that $\sigma|_{\mathfrak{G}_n} - \chi_{\text{cyc}}(\sigma)$ is in the annihilator for every $\sigma \in \text{Gal}(\overline{K}/K)$, so we can take away appropriate multiples of elements of the form $\sigma|_{\mathfrak{G}_n} - \chi_{\text{cyc}}(\sigma)$ until we are left with a constant in $\mathbb{Z}/N\mathbb{Z}$, and that constant must be zero since it annihilates μ_N. Now, we will show that the annihilator as a $\mathbb{Z}[\mathfrak{G}_n]$-module is generated by

$$N\mathbb{Z} + \langle \sigma - N_\sigma \rangle_{\sigma \in \mathfrak{G}_n},$$

where $N_\sigma \in \mathbb{Z}$ is such that $\chi_{\text{cyc}}(\sigma) \equiv N_\sigma \bmod N$. To see this, given an element in the annihilator, it is a finite sum so we can eliminate the terms involving the elements of $\mathfrak{G}_n$ by taking away the terms of the form $\sigma - N_\sigma$. Then we are left with an integer, which should be divisible by N. We claim that we can get N as well. By the Čebotarev density theorem, there exists an ideal $\mathfrak{a}$ of $\mathcal{O}$ such that $\sigma = \sigma_{\mathfrak{a}} \in \mathfrak{G}_n$, and then $N_\alpha = \mathrm{N}\,\mathfrak{a}$ satisfies $\chi_{\text{cyc}}(\sigma_{\mathfrak{a}}) \equiv \mathrm{N}\mathfrak{a} \bmod N$. Hence, it is enough to show that hcf$\{\mathrm{N}\mathfrak{q}-1 : \mathfrak{q}$ is a prime which splits in $F_n\} = N$, because $\sigma_\mathfrak{q} = 1$ for a prime $\mathfrak{q}$ if it splits in F_n, so that we can get N as a combination of elements in $\langle \sigma - N_\sigma\rangle_{\sigma\in\mathfrak{G}_n}$. Given a prime $\mathfrak{q}$ which splits in F_n, we have $\mathrm{N}\mathfrak{q}-1 = NM$ for some integer M. By Galois theory, we have $\mathrm{Gal}(F_n(\mu_{NM})/F_n) = \mathrm{Gal}(K(\mu_{NM})/K(\mu_N)) \simeq (1+N\mathbb{Z}/1+NM\mathbb{Z})^\times$. Thus by the Čebotarev density theorem, we can pick another prime $\mathfrak{q}'$ of F_n which is mapped to $1+N$ and fixes μ_M. This shows that we have $\mathrm{hcf}(\mathrm{N}\mathfrak{q}-1, \mathrm{N}\mathfrak{q}'-1) = N$, as required. Hence the annihilator in $\mathbb{Z}[\mathfrak{G}_n]$ is generated by $N\mathbb{Z} + \langle \sigma_\mathfrak{a} - \mathrm{N}\mathfrak{a}\rangle_{(\mathfrak{a},6\mathfrak{p}\mathfrak{f})=1}$. But $\cup_n\mathbb{Z}[\mathfrak{G}_n]$ is dense in $\mathbb{Z}_p[[\mathfrak{G}]]$ and $\cap_n N\mathbb{Z} + \langle \sigma_\mathfrak{a} - \mathrm{N}\mathfrak{a}\rangle_{(\mathfrak{a},6\mathfrak{p}\mathfrak{f})=1} = \langle \sigma_\mathfrak{a} - \mathrm{N}\mathfrak{a}\rangle_{(\mathfrak{a},6\mathfrak{p}\mathfrak{f})=1}$, so the result follows.

□

4.4 Statement of the Main Conjecture for H_∞/H

From now on, we always assume that $(p,h)=1$, where h denotes the class number of K. Recall that K_∞ denote the unique $\mathbb{Z}_p$-extension of K unramified outside $\mathfrak{p}$, and H_∞ denotes the composite field HK_∞. Then H_∞ is a subfield of F_∞ such that H_∞/H is a $\mathbb{Z}_p$-extension, and it is clear that $H_\infty = F_\infty^\Delta$. The fact that $(p,h)=1$ implies that H_∞/H is totally ramified at all primes above $\mathfrak{p}$, since K_∞/K is totally ramified at all primes above $\mathfrak{p}$. Furthermore, for each $n \geqslant 0$, the classical theory of complex multiplication shows that $H(E_{\mathfrak{p}^n})$ contains the field $HK(\mathfrak{p}^n)$ where $K(\mathfrak{p}^n)$ denotes the ray class field of K modulo $\mathfrak{p}^n$. Then if $p=2$,

$$H_\infty = HK(\mathfrak{p}^\infty) = \bigcup_n HK(\mathfrak{p}^n)$$

is a $\mathbb{Z}_p$-extension of H, and write $\mathscr{G} = \mathrm{Gal}(H_\infty/K)$. We identify $\Gamma = \mathrm{Gal}(F_\infty/F)$ with $\mathrm{Gal}(H_\infty/H)$. Let $\Gamma_n = \Gamma^{p^{n-1-e}}$ where $e=0$ or 1 according as $p>2$ or $p=2$. Then $H_n = H_\infty^{\Gamma_n}$ so that $\mathrm{Gal}(F_n/F) = \mathrm{Gal}(H_n/H) = \mathbb{Z}/p^{n-1-e}\mathbb{Z}$.

Denote by $M(H_\infty)$ the maximal abelian p-extension of H_∞ unramified outside the primes above $\mathfrak{p}$, and write

$$X(H_\infty) = \mathrm{Gal}(M(H_\infty)/H_\infty).$$

For every $n \geqslant 0$, let $\mathcal{E}_{H_n}$ be the group of global units of H_n, and let U_{H_n} be the group of semi-local units of $H_n \otimes_K K_\mathfrak{p} = \oplus_{\mathfrak{P}|\mathfrak{p}} H_{n,\mathfrak{P}}$ which are congruent to 1 modulo the primes above $\mathfrak{p}$. Let $\bar{\mathcal{E}}_{H_n}$ be the closure of $\mathcal{E}_{H_n} \cap U_{H_n}$ in U_{H_n} in the p-adic topology.

Then we define

$$\bar{\mathcal{E}}_{H_\infty} = \varprojlim \bar{\mathcal{E}}_{H_n} \text{ and } U_{H_\infty} = \varprojlim U_{H_n},$$

where the inverse limits are taken with respect to the norm maps. A standard result from global class field theory says that the Artin map induces a $\mathrm{Gal}(H_n/H)$-isomorphism

$$U_{H_n}/\bar{\mathcal{E}}_{H_n} \simeq \mathrm{Gal}(M(H_n)/L(H_n)),$$

where $M(H_n)$ is the maximal abelian p-extension of H_n unramified outside of the primes above $\mathfrak{p}$, and $L(H_n)$ is the maximal unramified abelian p-extension of H_n. Hence, writing $X(H_n) = \mathrm{Gal}(M(H_n)/H_n)$, we have an exact sequence

$$0 \to U_{H_n}/\bar{\mathcal{E}}_{H_n} \to X(H_n) \to \mathrm{Gal}(L(H_n)/H_n) \to 0.$$

Taking the projective limit over n, we obtain an exact sequence

$$0 \to U_{H_\infty}/\bar{\mathcal{E}}_{H_\infty} \to X(H_\infty) \to \mathrm{Gal}(L(H_\infty)/H_\infty) \to 0, \tag{4.4.1}$$

where $L(H_\infty) = \varprojlim L(H_n)$ is the maximal unramified abelian p-extension of H_∞.

Let $A(H_n)$ denote the p-primary part of the ideal class group of H_n, and let $A(H_n)'$ be the quotient of $A(H_n)$ by subgroup generated by the classes of the primes of H_n above $\mathfrak{p}$ which lie in $A(H_n)$. So if we denote by D_n the subgroup of $X(H_n)$ generated by the decomposition group of the primes of H_n above $\mathfrak{p}$, we have an exact sequence

$$0 \to D_n \to X(H_n) \to A(H_n)' \to 0.$$

Furthermore, class field theory identifies $A(H_\infty)$ with $\mathrm{Gal}(L(H_\infty)/H_\infty)$, where $A(H_\infty)$ denotes the inductive limit of $A(H_n)$ taken with respect to the natural maps coming from the inclusion of fields. Thus we obtain the fundamental exact sequence needed for the proof of the main conjecture:

$$0 \to \bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty} \to U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty} \to X(H_\infty) \to A(H_\infty) \to 0. \tag{4.4.2}$$

Recall that $\mathscr{G} = \mathrm{Gal}(H_\infty/K)$. Then we have

$$\mathscr{G} = G \times \Gamma$$

so that characters of G are naturally be considered as characters of $\mathscr{G}$. Given a $\Lambda_{\mathscr{I}}(\mathscr{G})$-module M and $\chi \in G^*$, write M^χ for the largest submodule of M on which G

acts via χ. Since $p \nmid [H:K]$ by assumption, any $\Lambda_{\mathscr{I}}(\mathscr{G})$ module breaks up into the direct sum of its χ-components.

Lemma 4.4.1. *We have*

$$i(\bar{\mathcal{C}}_{H_\infty}) = I_{\mathscr{I}}(\mathscr{G}) \cdot \nu_{\mathfrak{p}},$$

where $I_{\mathscr{I}}(\mathscr{G})$ denotes the augmentation ideal of $\Lambda_{\mathscr{I}}(\mathscr{G})$.

Proof. Recall that $i(\mathfrak{u}_{\mathcal{D}}) = \nu_{\mathcal{D}} = \theta_{\mathcal{D}}\nu_{\mathfrak{p}}$ (see (4.2.5) and the comments before Proposition 4.3.10). Hence we just need to show that $I_{\mathscr{I}}(\mathscr{G})\Lambda_{\mathscr{I}}(\mathscr{G})$ is generated by $\theta_{\mathcal{D}}$, $\mathcal{D} \in I$. In Lemma 4.2.6, we have found $\mathcal{D} \in I$ such that $\theta_{\mathcal{D}}|_\Gamma$ generates $I_{\mathscr{I}}(\Gamma)$. It follows that for every $\chi \in G^*$, we have

$$i(\bar{\mathcal{C}}^{\chi}_{H_\infty}) = (I_{\mathscr{I}}(\mathscr{G}) \cdot \nu_{\mathfrak{p}})^{\chi}\,.$$

The result now follows since we have an isomorphism $\mathbb{Z}_p[[\mathscr{G}]] \simeq \mathbb{Z}_p[[\Gamma]][G]$ and the decomposition $I_{\mathscr{I}}(\mathscr{G}) = \oplus_{\chi\in G^*} I_{\mathscr{I}}(\mathscr{G})^{\chi}$, where $I_{\mathscr{I}}(\mathscr{G})^{\chi} = e_\chi I_{\mathscr{I}}(\Gamma)$ and $I_{\mathscr{I}}(\Gamma)$ is the augmentation ideal of $\Lambda_{\mathscr{I}}(\Gamma)$, which is generated by $\gamma - 1$. This concludes the proof of Lemma 4.4.1. □

Define $\boldsymbol{\varphi} = I_{\mathscr{I}}(\mathscr{G})\nu_{\mathfrak{p}} \subset \mathscr{I}[[\mathscr{G}]]$.

Lemma 4.4.2. *$\boldsymbol{\varphi}$ is independent of E.*

Proof. Recall that φ_K^k has conductor (1) for k even and positive integer. Thus, in view of Theorem 4.2.7, the period pair class $(\Omega_\infty(E/H), \Omega_{\mathfrak{p}}(E/H)) \in (\mathbb{C}^\times \times \mathbb{C}_p^\times)/\overline{\mathbb{Q}}^\times$ is independent of $\mathfrak{f}$, although they individually depend on $\mathfrak{f}$ and on the Weierstrass model of E (see [8, Remark II.4.12 (iv)]). Let us pick another global minimal equation for E/H, and let $\widetilde{\Omega}_\infty(E/H)$ and $\widetilde{\Omega}_{\mathfrak{p}}(E/H)$ denote the corresponding elements satisfying Theorem 4.2.7. It follows from the definition of $\Omega_{\mathfrak{p}}(E/H)$ that $\Omega_{\mathfrak{p}}(E/H)$ and $\widetilde{\Omega}_{\mathfrak{p}}(E/H)$ are units in $\mathscr{I}$, and since $\widetilde{\Omega}_\infty(E/H)$ mod $H^\times$ is independent of the specific Weierstrass model, we have $\widetilde{\Omega}_\infty(E/H) = u\Omega_\infty(E/H)$ for a global unit $u \in H^\times$. But $\mathfrak{p}$ does not divide u, so u^k for k even and positive is a unit in $\mathscr{I}[[\mathscr{G}]]$. It follows that the ideal $\boldsymbol{\varphi}$ in $\mathscr{I}[[\mathscr{G}]]$ is canonical. □

The following is an immediate consequence of the last two results.

Theorem 4.4.3. *We have an exact sequence of $\Lambda_{\mathscr{I}}(\mathscr{G})$-modules*

$$0 \to U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty} \to \Lambda_{\mathscr{I}}(\mathscr{G})/\boldsymbol{\varphi} \to D \to 0,$$

where D is finite and $I_{\mathscr{I}}(\mathscr{G})$ denotes the augmentation ideal of $\Lambda_{\mathscr{I}}(\mathscr{G})$.

We briefly recall the structure theorem for finitely generated torsion $\Lambda_{\mathscr{I}}(\mathscr{G})$-modules. Given a finitely generated torsion $\Lambda_{\mathscr{I}}(\mathscr{G})$-module M, the well-known structure theorem for finitely generated torsion $\Lambda_{\mathscr{I}}(\mathscr{G})^\chi \simeq \mathscr{I}[[T]]$-modules easily implies that there exist elements $f_1, \ldots, f_r$ of $\Lambda_{\mathscr{I}}(\mathscr{G})$ and pseudo-isomorphisms

$$\oplus_{j=1}^r \Lambda_{\mathscr{I}}(\mathscr{G})/(f_i) \to M \quad \text{and} \quad M \to \oplus_{j=1}^r \Lambda_{\mathscr{I}}(\mathscr{G})/(f_i).$$

The ideal $(\prod_{i=1}^r f_i)\Lambda_{\mathscr{I}}(\mathscr{G})$ is an invariant of M called the characteristic ideal of M, and is denoted by $\mathrm{char}(M)$. Furthermore, for every χ, we will denote by $\mathrm{char}\,(M)^\chi \subset \Lambda_{\mathscr{I}}(\mathscr{G})^\chi$ the characteristic ideal of the $\Lambda_{\mathscr{I}}(\mathscr{G})^\chi$-module M^χ.

Corollary 4.4.4. *For every $\chi \in G^*$, we have*

$$\mathrm{char}\left(U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}\right)^\chi = \boldsymbol{\varphi}^\chi.$$

We are now ready to state the main conjecture for H_∞/H, which will be proven in Chapter 6.

Theorem 4.4.5. *[Main Conjecture for H_∞/H] For every $\chi \in G^*$, we have*

$$\mathrm{char}\,(X(H_\infty))^\chi = \boldsymbol{\varphi}^\chi.$$

Before we move on, we will verify that Theorem 4.4.5 holds for $p = 2$ and $E = X_0(49)$, which is equal to the case $E = A(q)$ with $q = 7$. In this case, we have $M(H_\infty) = H_\infty$, because the maximal abelian extension of K in $M(H_\infty)$ coincides with the union $\cup_n K(\mathfrak{p}^n)$ of ray class fields K modulo $\mathfrak{p}^n$. Thus $X(H_\infty) = 0$, and it follows that Theorem 4.4.5 holds if and only if $\boldsymbol{\varphi}$ is a unit. By Theorem 4.2.7, this holds if and only if $(\chi_{\mathfrak{p}}(\gamma)^2 - 1)L(\overline{\psi}^2_{E/H}, 2)/\Omega_\infty(E/H)^2$ is a unit at $\mathfrak{p}$. This is true, because we can compute with Magma that $L(\overline{\psi}^2_{E/H}, 2)/\Omega_\infty(E/H)^2 = \frac{1}{8}$, and the fact that γ is a topological generator of $\Gamma \simeq 1 + 4\mathcal{O}_{\mathfrak{p}}$ gives that $\mathrm{ord}_{\mathfrak{p}}\,(\chi_{\mathfrak{p}}(\gamma)^2 - 1) = 3$, as required.

Chapter 5

Euler systems

5.1 Euler Systems of the Elliptic Units

In this section, we will treat the Iwasawa modules occurring in the fundamental exact sequence 4.4.2 as $\Lambda(\mathscr{G}) = \mathbb{Z}_p[[\mathscr{G}]]$-modules. They are finitely generated and torsion as $\mathbb{Z}_p[[\mathscr{G}]]$-modules. Given a finitely generated torsion $\mathbb{Z}_p[[\mathscr{G}]]$-module M, write $\mathrm{char}_\Lambda(M)$ for the characteristic ideal of M given by the structure theorem for finitely generated torsion $\Lambda(\mathscr{G})^\chi \simeq \mathbb{Z}_p[[\Gamma]]$-modules, and $\mathrm{char}_\Lambda(M)^\chi$ for the characteristic ideal of M^χ as a $\Lambda(\mathscr{G})^\chi$-module. The aim of this chapter is to define and study Euler systems of the elliptic units $\bar{\mathcal{C}}_{H_\infty}$, defined in Chapter 4, for the tower H_∞/H. The method of Euler systems we follow is due to Rubin [17, Chapter 1]. When combined with an application of Čebotarev density theorem, the results in this chapter enables us to prove a divisibility relation analogous to [17, Theorem 8.3]:

$$\mathrm{char}_\Lambda(A(H_\infty)) \text{ divides } p^k \mathrm{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}),$$

for an integer $k \geqslant 0$ ($k = 0$ when $p > 2$). This is proven in Chapter 6.

Let $\mathscr{G}_n = \mathrm{Gal}(H_n/K)$. Let $\Lambda_n = \mathbb{Z}_p[\mathscr{G}_n]$ and define

$$\Lambda(\mathscr{G}) = \mathbb{Z}_p[[\mathscr{G}]] = \varprojlim \mathbb{Z}_p[\mathscr{G}_n],$$

the Iwasawa algebra of $\mathscr{G}$. Since $\#(G)$ is prime to p, the group Λ_n is semisimple, i.e.,

$$\Lambda_n = \oplus_{\chi \in G^*} \Lambda_n^\chi,$$

where each summand Λ_n^χ corresponding to χ is isomorphic to $\mathbb{Z}_p[\mathrm{Gal}(H_n/H)]$, and

$$\Lambda(\mathscr{G}) = \oplus_{\chi \in G^*} \Lambda(\mathscr{G})^\chi,$$

where each $\Lambda(\mathscr{G})^\chi$ is isomorphic to $\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(H_n/H)]$.

Lemma 5.1.1. *Suppose $\lambda \in \Lambda_n$ and $m \geqslant 1$. Then $\lambda\Lambda_n/\lambda^m\Lambda_n$ is finite.*

Proof. We show that $\lambda\Lambda_n^\chi/\lambda^m\Lambda_n^\chi$ is finite for every $\chi \in G^*$. Write $\widehat{\mathscr{G}}_n^\chi = \{\rho : \mathscr{G}_n^\chi \to \boldsymbol{\mu}_{p^n}\}$ for the character group of $\mathscr{G}_n^\chi$. Every $\rho \in \widehat{\mathscr{G}}_n^\chi$ extends by linearity to a ring homomorphism from Λ_n^χ to $\mathbb{Z}_p[\boldsymbol{\mu}_{p^n}]$. Given $\lambda \in \Lambda_n^\chi$, we can define

$$\mathcal{Z}(\lambda) = \{\rho \in \widehat{\mathscr{G}}_n^\chi : \rho(\lambda) = 0\}.$$

Then clearly $\mathcal{Z}(\lambda) = \mathcal{Z}(\lambda^m)$ and

$$\mathrm{rank}_{\mathbb{Z}_p}(\Lambda_n^\chi/\lambda\Lambda_n^\chi) = \#\mathcal{Z}(\lambda)$$

and so

$$\mathrm{rank}_{\mathbb{Z}_p}(\Lambda_n^\chi/\lambda^m\Lambda_n^\chi) = \#\mathcal{Z}(\lambda^m) = \#\mathcal{Z}(\lambda),$$

giving

$$\mathrm{rank}_{\mathbb{Z}_p}(\lambda\Lambda_n^\chi/\lambda^m\Lambda_n^\chi) = 0,$$

as required. □

Fix a positive integer $l > 1$. Let $\mathcal{I}_\ell$ be the set of squarefree ideals of $\mathcal{O}_K$ which are divisible only by primes $\mathfrak{q}$ of K such that

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

(ii) $\mathrm{N}\,\mathfrak{q} \equiv 1 \bmod p^{\ell+e}$, where $e = 0$ or 1 according as p is odd or even.

Recall that $K(\mathfrak{q})$ denotes the ray class field of K modulo $\mathfrak{q}$. In the following lemma, we define the field $H_n(\mathfrak{q})$.

Lemma 5.1.2. *Given a prime $\mathfrak{q} \in \mathcal{I}_\ell$, we have a unique (cyclic) extension $H_n(\mathfrak{q})$ of H_n of degree p^ℓ inside $H_nK(\mathfrak{q})$. Furthermore, $H_n(\mathfrak{q})/H_n$ is totally ramified at the primes above $\mathfrak{q}$, and unramified everywhere else.*

Proof. Since $\mathfrak{q}$ is unramified in H_n/K, we have $K(\mathfrak{q}) \cap H_n = H \cap H_n = H$. Hence, we have

$$\mathrm{Gal}(H_nK(\mathfrak{q})/H_n) = \mathrm{Gal}(K(\mathfrak{q})/H),$$

which isomorphic to $(\mathcal{O}/\mathfrak{q}\mathcal{O})^\times/\#(\widetilde{\boldsymbol{\mu}}_K)$ via the Artin map, where $\widetilde{\boldsymbol{\mu}}_K$ denotes the image of $\boldsymbol{\mu}_K$ under reduction modulo $\mathfrak{q}$. Since $(\mathfrak{q}, 2) = 1$, the reduction modulo $\mathfrak{q}$ map is injective, and this is cyclic of order $(\mathrm{N}\mathfrak{q} - 1)/(\#(\boldsymbol{\mu}_K))$ where $\#(\boldsymbol{\mu}_K) = 2$. Hence it has a unique subgroup of order p^ℓ since $\mathrm{N}\mathfrak{q} \equiv 1 \bmod p^{\ell+e}$, where $e = 0$ or 1 according as $p > 2$ or $p = 2$. Furthermore, $H_nK(\mathfrak{q})/H_n$ is totally ramified at the primes above $\mathfrak{q}$ and unramified everywhere else, so the assertions of the lemma follow. □

Lemma 5.1.3. *Let*

$$r : H_n^\times/(H_n^\times)^{p^\ell} \to H_n(\boldsymbol{\mu}_{p^{\ell+e}})^\times/(H_n(\boldsymbol{\mu}_{p^{\ell+e}})^\times)^{p^\ell},$$

be the natural map, where $e = 0$ or 1 according as $p > 2$ or $p = 2$. Then r is injective if $p > 2$, and $4 \ker r = 0$ if $p = 2$.

Proof. We have $H_n^\times/(H_n^\times)^{p^\ell} \simeq H^1(\overline{H_n}/H_n, \boldsymbol{\mu}_{p^\ell})$ and $H_n(\boldsymbol{\mu}_{p^{\ell+e}})^\times/(H_n(\boldsymbol{\mu}_{p^{\ell+e}})^\times)^{p^\ell} \simeq H^1(\overline{H_n(\boldsymbol{\mu}_{p^{\ell+e}})}/H_n(\boldsymbol{\mu}_{p^{\ell+e}}), \boldsymbol{\mu}_{p^\ell})$ by Hilbert 90. Hence $\ker r = H^1(\mathrm{Gal}(H_n(\boldsymbol{\mu}_{p^{\ell+e}})/H_n), \boldsymbol{\mu}_{p^\ell})$. Also, $H_\infty \cap K(\boldsymbol{\mu}_{p^\infty}) = K$ because $\mathfrak{p}$ and $\mathfrak{p}^*$ are totally ramified in $K(\boldsymbol{\mu}_{p^\infty})/K$, but H_∞/K is unramified outside $\mathfrak{p}$. It follows that $H_\infty \cap \mathbb{Q}(\boldsymbol{\mu}_{p^\infty}) = \mathbb{Q}$, and

$$\mathrm{Gal}(H_n(\boldsymbol{\mu}_{p^{\ell+e}})/H_n) = (\mathbb{Z}/p^{\ell+e})^\times \simeq \Delta \times \mathbb{Z}/p^{\ell-1}\mathbb{Z}.$$

Here, $\Delta = \mathrm{Gal}(H_n(\boldsymbol{\mu}_{p^{1+e}})/H_n)$ is cyclic of order $p - 1$ or p according as p is odd or even, and $\mathrm{Gal}(H_n(\boldsymbol{\mu}_{p^{\ell+e}})/H_n(\boldsymbol{\mu}_{p^{1+e}})) \simeq \mathbb{Z}/p^{\ell-1}\mathbb{Z}$. So if $p > 2$, $\mathrm{Gal}(H_n(\boldsymbol{\mu}_{p^{\ell+e}})/H_n)$ is cyclic and we have $\ker r = 0$, as required. If $p = 2$, taking the inflation-restriction sequence gives

$$0 \to H^1(\Delta, \boldsymbol{\mu}_4) \to \ker r \to H^1(\mathrm{Gal}(H_n(\boldsymbol{\mu}_{2^{\ell+1}})/H_n(\boldsymbol{\mu}_4))\,\boldsymbol{\mu}_{2^\ell}),$$

and $H^1(\Delta, \boldsymbol{\mu}_4) = H^1(\mathrm{Gal}(H_n(\boldsymbol{\mu}_{2^{\ell+1}})/H_n(\boldsymbol{\mu}_4), \boldsymbol{\mu}_{2^\ell}) = \mathbb{Z}/2\mathbb{Z}$. Hence $|\ker r| \mid 4$, and the result follows. □

For $n \geqslant 1$, recall that $\Gamma_n = \Gamma^{p^n-1-e}$ where $e = 0$ or $e = 1$ according as $p > 2$ or $p = 2$. Define $I(H_n)$ to be kernel of the restriction map $\Lambda(\mathscr{G}) \to \Lambda_n$, i.e., the ideal of $\Lambda(\mathscr{G})$ generated by $\{\sigma - 1 : \sigma \in \Gamma_n\}$. Given a $\Lambda(\mathscr{G})$-module Y, define

$$Y^{\Gamma_n} = \{y \in Y : \sigma y = y \text{ for all } \sigma \in \Gamma_n\}.$$

Lemma 5.1.4. *Given an exact sequence of $\Lambda(\mathscr{G})$-modules*

$$0 \to Y \to Z \to W \to 0,$$

we have an exact sequence

$$0 \to Y^{\Gamma_n} \to Z^{\Gamma_n} \to W^{\Gamma_n} \to Y/I(H_n)Y \to Z/I(H_n)Z \to W/I(H_n)W \to 0.$$

Proof. Pick a topological generator γ of $\mathrm{Gal}(H_\infty/H_n)$ and consider multiplication by $\gamma - 1$ maps on Y, Z and W respectively. The lemma now follows easily by applying the snake lemma. □

Theorem 5.1.5. *$X(H_\infty)$ is a finitely generated torsion $\Lambda(\mathscr{G})$-module, and it has no non-zero finite submodule. Furthermore, $X(H_\infty)/I(H_n)X(H_\infty)$ is finite for any n.*

Proof. The first statement follows from [2, Lemma 13, Lemma 14]. Iwasawa theory shows that $I(H_n)X(H_\infty) = \mathrm{Gal}(M(H_\infty)/M(H_n))$, because $M(H_n)$ is the largest abelian extension of H_n inside $M(H_\infty)$. Hence we have an exact sequence

$$0 \to X(H_\infty)/I(H_n)X(H_\infty) \to X(H_n) \to \mathrm{Gal}(H_\infty/H_n) \to 0, \tag{5.1.1}$$

where $X(H_n) = \mathrm{Gal}(M(H_n)/H_n)$. Clearly the $\mathbb{Z}_p$-rank of $\mathrm{Gal}(H_\infty/H_n)$ is 1. We will show that the same is true for $X(H_n)$. Let $[\mathcal{F} : \mathbb{Q}] = r_1 + 2r_2$ is a number field, where r_1 is the number of real embeddings of $\mathcal{F}$ and r_2 is the number of pairs of complex embeddings. The $\mathbb{Z}$-rank of the global units $\mathcal{E}_\mathcal{F}$ of $\mathcal{F}$ is $r_1 + r_2 - 1$ by Dirichlet's unit theorem. Let $U_\mathcal{F} = \prod_{v|p} U_v$ where v is a prime of $\mathcal{F}$ above p and U_v denotes the groups of local units at v congruent to 1 modulo v. Then the $\mathbb{Z}_p$-submodule $\bar{\mathcal{E}}_\mathcal{F}$ of $U_\mathcal{F}$ generated by the image of $\mathcal{E}_\mathcal{F}$ in $U_\mathcal{F}$ has $\mathbb{Z}_p$-rank $r_1 + r_2 - 1 - v_\mathcal{F}$ for some integer $v_\mathcal{F} \geqslant 0$. The $\mathfrak{p}$-adic analogue of Leopoldt's conjecture says $v_\mathcal{F} = 0$, and this is known to hold for abelian extensions of $\mathbb{Q}$. In particular, this holds for $\mathcal{F} = H_n$, and thus $\mathrm{rank}_{\mathbb{Z}_p}(U_{H_n}/\bar{\mathcal{E}}_{H_n}) = 1$. On the other hand, we have

$$\mathrm{rank}_{\mathbb{Z}_p}(X(H_n)) = \mathrm{rank}_{\mathbb{Z}_p}(U_{H_n}/\bar{\mathcal{E}}_{H_n}).$$

by class field theory, so $\mathrm{rank}_{\mathbb{Z}_p}(X(H_n)) = 1$ as required. □

Recall that $A(H_n)$ denotes the p-primary part of the ideal class group of H_n, and $A(H_\infty) = \varinjlim A(H_n)$ where the inductive limit is taken with respect to the natural maps coming from the inclusion of fields.

Theorem 5.1.6. $\mathrm{char}_\Lambda(A(H_\infty))$ *is prime to $I(H_n)$.*

Proof. $A(H_\infty)$ is a quotient of $X(H_\infty)$, so $A(H_\infty)/I(H_n)A(H_\infty)$ is a quotient of $X(H_\infty)/I(H_n)X(H_\infty)$. Since the latter is finite by Theorem 5.1.5, we also have that $A(H_\infty)/I(H_n)A(H_\infty)$ is finite and so $\mathrm{char}_\Lambda\left(A(H_\infty)/I(H_n)A(H_\infty)\right) = 0$, as required. □

Theorem 5.1.7. *Let $\pi_U : U_{H_\infty}/I(H_n)U_{H_\infty} \to U_{H_n}$ denote the map induced by the projection map. Then*

$$I(D_\mathfrak{p}) \ker \pi_U = I(D_\mathfrak{p}) \operatorname{coker} \pi_U = 0,$$

where $D_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} D_\mathfrak{P}$ denotes the group generated by the decomposition groups $D_\mathfrak{P}$ of $\mathfrak{P}$ in H_∞/H.

Proof. See [17, Theorem 5.1]. □

Let

$$\pi_\mathcal{E} : \bar{\mathcal{E}}_{H_\infty}/I(H_n)\bar{\mathcal{E}}_{H_\infty} \to \bar{\mathcal{E}}_{H_n} \quad \text{and} \quad \pi_\mathcal{C} : \bar{\mathcal{C}}_{H_\infty}/I(H_n)\bar{\mathcal{C}}_{H_\infty} \to \bar{\mathcal{C}}_{H_n}$$

denote the maps induced by projection maps.

Theorem 5.1.8. *(i) $I(D_\mathfrak{p}) \ker \pi_\mathcal{E} = 0$, where $D_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} D_\mathfrak{P}$ and $D_\mathfrak{P}$ denotes the decomposition group of $\mathfrak{P}$ in H_∞/H.*

(ii) There exists an ideal $\mathcal{B}$ of finite index in $\Lambda(\mathscr{G})$ such that

$$I(D_\mathfrak{p})\mathcal{B} \operatorname{coker} \pi_\mathcal{E} = 0.$$

Proof. Recall that $U_{H_\infty}/\bar{\mathcal{E}}_{H_\infty} \subset X(H_\infty)$ by (4.4.1) and $X(H_\infty)/I(H_n)X(H_\infty)$ is finite by Theorem 5.1.5. Thus $X(H_\infty)^{\Gamma_n}$ is a finite submodule of $X(H_\infty)$, and therefore is equal to zero by Theorem 5.1.5. It follows that $\left(U_{H_\infty}/\bar{\mathcal{E}}_{H_\infty}\right)^{\Gamma_n} = 0$. For ease of notation, given a $\Lambda(\mathscr{G})$-module Y, let $Y(n)$ denote the quotient $Y/I(H_n)Y$ and let π_Y denote the map $Y(n) \to Y^{\Gamma_n}$ induced by the projection map. Consider the diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \bar{\mathcal{E}}_{H_\infty}(n) \arrow[r] \arrow[d, "\pi_\mathcal{E}"'] & U_{H_\infty}(n) \arrow[r] \arrow[d, "\pi_U"] & \left(U_{H_\infty}/\bar{\mathcal{E}}_{H_\infty}\right)(n) \arrow[r] \arrow[d, "\pi_{U/\mathcal{E}}"'] & 0 \\
0 \arrow[r] & \bar{\mathcal{E}}_{H_n} \arrow[r] & U_{H_n} \arrow[r] & U_{H_n}/\bar{\mathcal{E}}_{H_n} \arrow[r] & 0.
\end{tikzcd} \tag{5.1.2}$$

Applying the snake lemma to (5.1.2) gives

$$0 \to \ker \pi_\mathcal{E} \to \ker \pi_U \to \ker \pi_{U/\mathcal{E}} \to \operatorname{coker} \pi_\mathcal{E} \to \operatorname{coker} \pi_U \to \operatorname{coker} \pi_{U/\mathcal{E}} \to 0, \quad (5.1.3)$$

and, in particular, an injection $\ker \pi_{\mathcal{E}} \to \ker \pi_U$, so assertion (i) follows from Theorem 5.1.7.

To prove assertion (ii), consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & A(H_\infty)^{\Gamma_n} \arrow[r] & \left(U_{H_\infty}/\bar{\mathcal{E}}_{H_\infty}\right)(n) \arrow[r] \arrow[d, "\pi_{U/\mathcal{E}}"] & \left(U_{H_\infty}/\bar{\mathcal{E}}_{H_\infty}\right)(n) \arrow[d, "\pi_X"'] \\
 & 0 \arrow[r] & U_{H_n}/\bar{\mathcal{E}}_{H_n} \arrow[r] & X(H_n),
\end{tikzcd} \tag{5.1.4}$$

where we applied Lemma 6.2.1 to (4.4.1) and used the fact that $X(H_\infty)^{\Gamma_n} = 0$ to obtain the first row. We have $\ker \pi_X = 0$ by (5.1). Hence $A(H_\infty)^{\Gamma_n} \simeq \ker \pi_{U/\mathcal{E}}$. Note that $A(H_\infty)^{\Gamma_n}$ is finite, since $A(H_\infty)/I(H_n)A(H_\infty)$ is finite. It then follows from Theorem 5.1.7 and (5.1.3) that

$$I(D_{\mathfrak{p}})\mathcal{B} \operatorname{coker} \pi_{\mathcal{E}} = 0,$$

where $\mathcal{B}$ is the annihilator of the maximal finite submodule of $A(H_\infty)$ in $\Lambda(\mathscr{G})$. This completes the proof of Theorem 5.1.8. □

Theorem 5.1.9. $\operatorname{rank}_{\Lambda(\mathscr{G})}(\bar{\mathcal{C}}_{H_\infty}) = 1$ *and* $\operatorname{coker}(\pi_{\mathcal{C}}) = \ker(\pi_{\mathcal{C}}) = 0$.

Proof. By Lemma 4.4.1, there is a isomorphism of $\Lambda(\mathscr{G})$-modules

$$\bar{\mathcal{C}}_{H_\infty} \simeq I(\mathscr{G}),$$

where $I(\mathscr{G})$ is the augmentation ideal of $\Lambda(\mathscr{G})$, so the first statement follows on noting that $\operatorname{rank}_{\Lambda(\mathscr{G})}(\Lambda(\mathscr{G})/I(\mathscr{G})) = \operatorname{rank}_{\Lambda(\mathscr{G})}(\mathbb{Z}_p) = 0$. By Proposition 4.3.9, the projection map $\pi_{\mathcal{C}} : \bar{\mathcal{C}}_{H_\infty}/I(H_n)\bar{\mathcal{C}}_{H_\infty} \to \bar{\mathcal{C}}_{H_n}$ is surjective, so $\operatorname{coker} \pi_{\mathcal{C}} = 0$. Now, the first statement of the theorem gives $\bar{\mathcal{C}}_{H_\infty}/I(H_n)\bar{\mathcal{C}}_{H_\infty} \simeq \Lambda_n$. Furthermore, $\bar{\mathcal{C}}_{H_n}$ is isomorphic to a submodule Y of finite index in Λ_n. Define a map $f : \Lambda_n \to Y$ so that it commutes with the map $\pi_{\mathcal{C}}$. Then clearly $\ker \pi_{\mathcal{C}} \subset \ker f$ and $\operatorname{coker} f$ is a quotient of $\operatorname{coker} \pi_{\mathcal{C}}$, which is equal to zero. Thus $\ker f$ is finite, and hence equal to zero since Λ_n has no non-zero finite submodules. The theorem now follows. □

Corollary 5.1.10. $\operatorname{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty})$ *is prime to* $I(H_n)$.

Corollary 5.1.11. *There exists an ideal* $\mathcal{B} \subset \Lambda(\mathscr{G})$ *such that for every* $\lambda \in I(\mathscr{G})\mathscr{B}$, *there is a map* $\theta_{\lambda,n} : \bar{\mathcal{E}}_{H_n} \to \Lambda_n$ *satisfying*

$$\lambda^2 \operatorname{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty})\Lambda_n \subset \theta_{\lambda,n}(\bar{\mathcal{C}}_{H_n}).$$

Proof. Fix a map $\theta : \bar{\mathcal{E}}_{H_\infty} \to \Lambda(\mathscr{G})$ such that $\theta(\bar{\mathcal{C}}_{H_\infty}) \subset \mathrm{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty})$ and $\mathrm{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty})/\theta(\bar{\mathcal{C}}_{H_\infty})$ is finite. Let $\mathcal{B} = \mathcal{A}_1\mathcal{A}_2$ where $\mathcal{A}_1$ satisfies Theorem 5.1.8 (ii) and $\mathcal{A}_2$ is the annihilator of $\mathrm{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty})/\theta(\bar{\mathcal{C}}_{H_\infty})$. In particular, since $\lambda \in \mathcal{A}_2$, we have

$$\lambda \mathrm{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}) \subset \theta(\bar{\mathcal{C}}_{H_\infty}).$$

Write $\theta_n : \bar{\mathcal{E}}_{H_\infty}/I(H_n)\bar{\mathcal{E}}_{H_\infty} \to \Lambda_n$ denote the map induced by θ, so that we have

$$\lambda \mathrm{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty})\Lambda_n \subset \theta_n(\bar{\mathcal{C}}_{H_\infty}). \tag{5.1.5}$$

Define $\theta_{\lambda,n} : \bar{\mathcal{E}}_{H_n} \to \Lambda_n$ so that the following diagram commutes:

$$\begin{tikzcd}
\bar{\mathcal{E}}_{H_\infty}/I(H_n)\bar{\mathcal{E}}_{H_\infty} \arrow[r, "\theta_n"] \arrow[d, "\pi_{\mathcal{E}}"'] & \Lambda_n \arrow[d, "\lambda"] \\
\bar{\mathcal{E}}_{H_n} \arrow[r, "\theta_{\lambda,n}"] & \Lambda_n
\end{tikzcd}$$

This is well-defined since $\lambda \ker \pi_{\mathcal{E}} = \lambda \operatorname{coker} \pi_{\mathcal{E}} = 0$ by Theorem 5.1.8. Then we have

$$\lambda\theta_n(\bar{\mathcal{C}}_{H_\infty}) = \theta_{\lambda,n}\pi_{\mathcal{E}}(\bar{\mathcal{C}}_{H_\infty}) \subset \theta_{\lambda,n}(\bar{\mathcal{C}}_{H_n}) \tag{5.1.6}$$

because $\pi_{\mathcal{E}}(\bar{\mathcal{C}}_{H_\infty}) \subset \bar{\mathcal{C}}_{H_n}$. Combining (5.1.5) and (5.1.6) gives the result. □

Lemma 5.1.12. *Let $f_1, \ldots, f_k \in \Lambda(\mathscr{G})$ be such that we have an exact sequence*

$$0 \to \oplus_{i=1}^k \frac{\Lambda(\mathscr{G})}{\Lambda(\mathscr{G})f_i} \to A(H_\infty) \to Q \to 0$$

with Q finite. Then there exists an ideal $\mathcal{B}$ of finite index in $\Lambda(\mathscr{G})$ such that, for every $n \geqslant 2$, there exist classes $\mathfrak{c}_1, \ldots \mathfrak{c}_k \in A(H_n)$ satisfying $\mathcal{B}\mathcal{A}_i \subset f_i\Lambda_n$ for every i, where $\mathcal{A}_i \subset \Lambda_n$ is the annihilator of $\mathfrak{c}_i$ in $A(H_n)/(\mathfrak{c}_1\Lambda_n + \cdots + \Lambda_n\mathfrak{c}_{i-1})$.

Proof. See [17, Proposition 6.5]. □

If $\mathfrak{r} = \prod_{i_1}^l \mathfrak{q}_i \in \mathcal{I}_\ell$, we write $H_n(\mathfrak{r})$ for the composite $H_n(\mathfrak{q}_1)\cdots H_n(\mathfrak{q}_l)$, and we put $H_n(\mathcal{O}) = H_n$.

Definition 5.1.13. An Euler system is a collection of global units

$$\boldsymbol{\alpha} = \{\boldsymbol{\alpha}^\sigma(n, \mathfrak{r}) : \ n \geqslant 1, \ \mathfrak{r} \in \mathcal{I}_\ell, \ \sigma \in \mathrm{Gal}(H/K)\}$$

satisfying

(i) $\boldsymbol{\alpha}^{\sigma}(n,\mathfrak{r})$ is a global unit of $H_n(\mathfrak{r})$,

(ii) If $\mathfrak{q}$ is a prime such that $\mathfrak{rq} \in \mathcal{I}_\ell$, then

$$\mathrm{N}_{H_n(\mathfrak{rq})/H_n(\mathfrak{r})}(\boldsymbol{\alpha}^{\sigma}(n,\mathfrak{rq})) = \boldsymbol{\alpha}^{\sigma}(n,\mathfrak{r})^{1-\mathrm{Frob}_{\mathfrak{q}}^{-1}} \tag{5.1.7}$$

where $\mathrm{Frob}_{\mathfrak{q}}$ is the Frobenius of $\mathfrak{q}$ in $\mathrm{Gal}(H_n(\mathfrak{rq})/K)$.

(iii)

$$\mathrm{N}_{H_{n+1}(\mathfrak{r})/H_n(\mathfrak{r})}(\boldsymbol{\alpha}^{\sigma}(n+1,\mathfrak{r})) = \boldsymbol{\alpha}^{\sigma\sigma_{\mathfrak{p}}}(n,\mathfrak{r}), \tag{5.1.8}$$

where $\sigma_{\mathfrak{p}} = (\mathfrak{p}, H/K) \in \mathrm{Gal}(H/K)$.

We now show how the elliptic units give rise to an Euler system.

Lemma 5.1.14. *Let $\mathfrak{q} \in \mathcal{I}_\ell$ be a prime. Then*

(i) $K(\mathfrak{qfp}^n) = F_n(E_{\mathfrak{qf}})$.

(ii) $[H_n(E_{\mathfrak{q}}) : H_n(\mathfrak{q})] = (\mathrm{N}\mathfrak{q} - 1)/p^\ell$.

Proof. By [10, Lemma 4.7], we have

$$H(E_{\mathfrak{qfp}^n}) = K(\mathfrak{qfp}^n)$$

because the conductor $\mathfrak{g}$ of φ_K divides $\mathfrak{f}$. But $H(E_{\mathfrak{qfp}^n}) = F_n(E_{\mathfrak{qf}})$ since $(\mathfrak{p},\mathfrak{qf}) = 1$ and $F_n = H(E_{\mathfrak{p}^n})$ by definition. This proves (i). For (ii), since $\mathfrak{q}$ is a prime of good reduction for E, $\mathfrak{q}$ is totally ramified in $H_n(E_{\mathfrak{q}})/H$ and unramified in H_n/H. Thus, by Theorem 3.2.1, $\mathrm{Gal}(H_n(E_{\mathfrak{q}})/H_n) \simeq \mathrm{Gal}(H(E_{\mathfrak{q}})/H) \simeq (\mathcal{O}/\mathfrak{q})^\times$. Assertion (ii) now follows on noting that $[H_n(\mathfrak{q}) : H_n] = p^\ell$. □

Proposition 5.1.15. *If $u \in \mathcal{C}_{H_n}$, then there exists an Euler system $\{\boldsymbol{\alpha}^{\sigma}(n,\mathfrak{r}) :\ n \geqslant 1,\ \mathfrak{r} \in \mathcal{I}_\ell,\ \sigma \in \mathrm{Gal}(H/K)\}$ with $\boldsymbol{\alpha}^{\sigma}(n,1) = u$.*

Proof. It suffices to consider the case $u = R^{\sigma}_{\mathcal{D}}(P^{\sigma}_n)$. Given $\mathfrak{r} \in \mathcal{I}_\ell$, define $\alpha^{\sigma}_n(\mathfrak{r}) = R^{\sigma}_{\mathcal{D}}(\lambda_{E^\sigma}(\mathfrak{r})^{-1}(P^{\sigma}_n))$. Then clearly $\alpha^{\sigma}_n(1) = u$ and $\alpha^{\sigma}_n(\mathfrak{r})$ is a global unit in $H_n(\mathfrak{r})$. Furthermore, if $\mathfrak{q}$ is a prime in $\mathcal{I}_\ell$ and $\mathfrak{rq} \in \mathcal{I}_\ell$, then $\sigma_{\mathfrak{q}} = 1$, so by Proposition 4.3.2 we have

$$\begin{aligned} N_{H_n(\mathfrak{rq})/H_n(\mathfrak{r})}(\alpha^{\sigma}_n(\mathfrak{rq})) &= N_{H_n(\mathfrak{rq})/H_n(\mathfrak{r})}(R^{\sigma}_{\mathcal{D}}\left(\lambda_{E^\sigma}(\mathfrak{rq})^{-1}(P^{\sigma}_n)\right)) \\ &= R^{\sigma}_{\mathcal{D}}\left(\lambda_{E^\sigma}(\mathfrak{r})^{-1}(P^{\sigma}_n)\right)^{1-\mathrm{Frob}_{\mathfrak{q}}^{-1}} \\ &= \alpha^{\sigma}_n(\mathfrak{r})^{1-\mathrm{Frob}_{\mathfrak{q}}^{-1}}, \end{aligned}$$

and similarly

$$\begin{aligned}N_{H_{n+1}(\mathfrak{r})/H_n(\mathfrak{r})}(\alpha_{n+1}^{\sigma}(\mathfrak{r})) &= N_{H_{n+1}(\mathfrak{r})/H_n(\mathfrak{r})}(R_{\mathcal{D}}^{\sigma}\left(\lambda_{E^{\sigma}}(\mathfrak{r})^{-1}(P_{n+1}^{\sigma})\right)) \\ &= R_{\mathcal{D}}^{\sigma\sigma_{\mathfrak{p}}}\left(\lambda_{E^{\sigma\sigma_{\mathfrak{p}}}}(\mathfrak{r})^{-1}(\lambda_{E^{\sigma}}(\mathfrak{p})(P_{n+1}^{\sigma})\right) \\ &= R_{\mathcal{D}}^{\sigma\sigma_{\mathfrak{p}}}\left(\lambda_{E^{\sigma\sigma_{\mathfrak{p}}}}(\mathfrak{r})^{-1}(P_{n}^{\sigma\sigma_{\mathfrak{p}}})\right) \\ &= \alpha_{n}^{\sigma\sigma_{\mathfrak{p}}}(\mathfrak{r}).\end{aligned}$$

Therefore, defining $\boldsymbol{\alpha}^{\sigma}(n,\mathfrak{r}) = \alpha_n^{\sigma}(\mathfrak{r})$ gives the result. □

For every prime $\mathfrak{q} \in \mathcal{I}_{\ell}$, write $G_{\mathfrak{q}} = \mathrm{Gal}(H_n(\mathfrak{q})/H_n)$. Then $G_{\mathfrak{q}}$ is cyclic of order p^{ℓ} so we fix a generator $\tau_{\mathfrak{q}}$. Define

$$\mathcal{D}_{\mathfrak{q}} = \sum_{i=0}^{p^{\ell}-1} i\tau_{\mathfrak{q}}^{i} \in \mathbb{Z}[G_{\mathfrak{q}}]$$

and for any $\mathfrak{a} \in \mathcal{I}_{\ell}$ define

$$\mathcal{D}_{\mathfrak{a}} = \prod_{\mathfrak{q}\mid\mathfrak{a}} \mathcal{D}_{\mathfrak{q}} \in \mathbb{Z}[G_{\mathfrak{a}}].$$

where $G_{\mathfrak{a}} = \mathrm{Gal}(H_n(\mathfrak{a})/H_n) \simeq \prod_{\mathfrak{q}\mid\mathfrak{a}} G_{\mathfrak{q}}$. Also, we define

$$N_{\mathfrak{q}} = \sum_{\sigma\in G_{\mathfrak{q}}} \sigma \in \mathbb{Z}[G_{\mathfrak{q}}]$$

for any prime $\mathfrak{q} \in \mathcal{I}_{\ell}$ and set

$$N_{\mathfrak{a}} = \prod_{\mathfrak{q}\mid\mathfrak{a}} N_{\mathfrak{q}} \in \mathbb{Z}[G_{\mathfrak{a}}].$$

Proposition 5.1.16. *Suppose $\boldsymbol{\alpha} = \{\boldsymbol{\alpha}^{\sigma}(n,\mathfrak{r}) :\ n \geqslant 1,\ \mathfrak{r} \in \mathcal{I}_{\ell},\ \sigma \in \mathrm{Gal}(H/K)\}$ is an Euler system. Given $\sigma \in \mathrm{Gal}(H/K)$, there exists a canonical map*

$$\kappa_{\boldsymbol{\alpha}} : \mathcal{I}_{\ell} \to H_n^{\times}/(H_n^{\times})^{p^{\ell}}$$

such that for every $n \geqslant 1$ and $\mathfrak{r} \in \mathcal{I}_{\ell}$ we have $\kappa_{\alpha}(\mathfrak{r}) = \boldsymbol{\alpha}^{\sigma}(n,\mathfrak{r})^{\mathcal{D}_{\mathfrak{a}}} \bmod (H_n(\mathfrak{r})^{\times})^{p^{\ell}}$.

Proof. In order to prove this, we will briefly introduce an alternative definition of Euler systems. See [17, Proposition 2.2] for more details. For $n \geqslant 1$ and $\mathfrak{r} \in \mathcal{I}_{\ell}$, let $X_n(\mathfrak{r})$ be the quotient of the free $\mathbb{Z}[\mathrm{Gal}(H_n(\mathfrak{r})/K)]$-module on the indeterminates $\{x_n^{\sigma}(\mathfrak{s}) : \mathfrak{s} \mid \mathfrak{r}, \sigma \in \mathrm{Gal}(H/K)\}$ by the following relations:

(1) $x_n^{\sigma}(\mathfrak{s})^{\rho-1}$ for all $\rho \in \mathrm{Gal}(H_n(\mathfrak{r})/H_n(\mathfrak{s}))$,

(2) $x_n^\sigma(\mathfrak{q}\mathfrak{s})^{N_\mathfrak{q}} = x_n^\sigma(\mathfrak{s})^{(1-\mathrm{Frob}_\mathfrak{q}^{-1})}$ if $\mathfrak{q}\mathfrak{s} \mid \mathfrak{r}$ and $\mathfrak{q}$ is a prime in $\mathcal{I}_\ell$,

(3) $x_{n+1}^\sigma(\mathfrak{r})^{N'} = x_n^{\sigma\sigma_\mathfrak{p}}(\mathfrak{r})$ where $N' = \sum_{\tau\in\mathrm{Gal}(H_{n+1}(\mathfrak{r})/H_n(\mathfrak{r}))} \tau \in \mathbb{Z}[\mathrm{Gal}(H_{n+1}(\mathfrak{r})/H_n(\mathfrak{r}))]$ and $\sigma_\mathfrak{p} = (\mathfrak{p}, H/K) \in \mathrm{Gal}(H/K)$.

Then we can define an Euler system to be a Galois equivariant map

$$\boldsymbol{\alpha} = \{\boldsymbol{\alpha}^\sigma(n,\mathfrak{r}) :\ n \geqslant 1,\ \mathfrak{r} \in \mathcal{I}_\ell,\ \sigma \in \mathrm{Gal}(H/K)\} : \varinjlim_{n,\mathfrak{r}} X_n(\mathfrak{r}) \to \cup_{n,\mathfrak{r}} H_n(\mathfrak{r})^\times.$$

Using this map, we can define a 1-cocycle $c : G_\mathfrak{r} \to H_n(\mathfrak{r})^\times$ by

$$c(\rho) = \boldsymbol{\alpha}^\sigma\ (n,\mathfrak{r})^{(\rho-1)\mathcal{D}_\mathfrak{r}/p^\ell}$$

for $\rho \in G_\mathfrak{r}$. Since $H^1(G_\mathfrak{r}, H_n(\mathfrak{r})^\times) = 0$, there exists $\beta \in H_n(\mathfrak{r})^\times$ such that $c(\rho) = \beta^\rho/\beta$ for every $\rho \in G_\mathfrak{r}$. Then $\boldsymbol{\alpha}^\sigma(n,\mathfrak{r})^{\mathcal{D}_\mathfrak{r}}/\beta^{p^\ell} \in H_n^\times$ and we can define

$$\kappa_{\boldsymbol{\alpha}}(\mathfrak{r}) = \boldsymbol{\alpha}^\sigma(n,\mathfrak{r})^{\mathcal{D}_\mathfrak{r}}/\beta^{p^\ell} \in H_n^\times/(H_n^\times)^{p^\ell}.$$

□

5.2 An Application of the Čebotarev Density Theorem

Write $\mathscr{G}_n = \mathrm{Gal}(H_n/K)$. Fix $n \geqslant 1 + e$, and let

$$I_{H_n} = I = \oplus_\mathfrak{Q} \mathbb{Z}\mathfrak{Q}$$

denote the group of fractional ideals of H_n written additively, where the sum runs over the prime ideals of H_n. For every prime $\mathfrak{q}$ of K, let

$$I_\mathfrak{q} = \oplus_{\mathfrak{Q}|\mathfrak{q}} \mathbb{Z}\mathfrak{Q} = \mathbb{Z}[\mathscr{G}_n]\mathfrak{Q}.$$

For $y \in H_n^\times$ let $(y)_\mathfrak{q}$, $[y]$ and $[y]_\mathfrak{q}$ be the projection of the principal ideal (y) in $I_\mathfrak{q}$, $I/p^\ell I$ and $I_\mathfrak{q}/p^\ell I_\mathfrak{q}$ respectively. Note that $[y]$ and $[y]_\mathfrak{q}$ are well-defined for $y \in H_n^\times/(H_n^\times)^{p^\ell}$.

Suppose now that $\mathfrak{Q}$ is a prime of H_n lying above a prime $\mathfrak{q} \in \mathcal{I}_\ell$. Then $H_n(\mathfrak{q})/H_n$ is totally ramified at $\mathfrak{Q}$, and we let $\tilde{\mathfrak{Q}}$ be the prime of $H_n(\mathfrak{q})$ above $\mathfrak{Q}$. We have a natural isomorphism $\mathcal{O}_{H_n(\mathfrak{q})}/\tilde{\mathfrak{Q}} \simeq \mathcal{O}_{H_n}/\mathfrak{Q}$, where $\mathcal{O}_{H_n(\mathfrak{q})}$ denotes the ring of integers of $H_n(\mathfrak{q})$. Suppose $x \in H_n(\mathfrak{q})^\times$ and $\rho \in G_\mathfrak{q}$. Then $x^{1-\rho}$ mod $\tilde{\mathfrak{Q}} \in (\mathcal{O}_{H_n(\mathfrak{q})}/\tilde{\mathfrak{Q}})^\times$, where

$\mathcal{O}_{H_n(\mathfrak{q})}$ denotes the ring of integers of $H_n(\mathfrak{q})$. We let $x^{1-\rho} \bmod \mathfrak{Q}$ denote the image of $x^{1-\rho} \bmod \tilde{\mathfrak{Q}}$ in $(\mathcal{O}_{H_n}/\mathfrak{Q})^\times$. Recall that $\tau_\mathfrak{q}$ is a fixed generator of the cyclic group $G_\mathfrak{q}$, and let $\overline{x^{1-\tau_\mathfrak{q}}}$ denote the image of $x^{1-\tau_\mathfrak{q}} \bmod \mathfrak{Q}$ inside $(\mathcal{O}_{H_n}/\mathfrak{Q})^\times/((\mathcal{O}_{H_n}/\mathfrak{Q})^\times)^{p^\ell}$. Then we write $(\overline{x^{1-\tau_\mathfrak{q}}})^{1/d}$ for the unique d-th root of $\overline{x^{1-\tau_\mathfrak{q}}}$ in $(\mathcal{O}_{H_n}/\mathfrak{Q})^\times/((\mathcal{O}_{H_n}/\mathfrak{Q})^\times)^{p^\ell}$, where $d = (\mathrm{N}\mathfrak{q} - 1)/p^\ell$. Then the map

$$H_n(\mathfrak{q}) \to (\mathcal{O}_{H_n}/\mathfrak{Q})^\times/((\mathcal{O}_{H_n}/\mathfrak{Q})^\times)^{p^\ell}, \quad x \to (\overline{x^{1-\tau_\mathfrak{q}}})^{1/d}$$

is surjective, with kernel $\{x \in H_n(\mathfrak{q})^\times : \mathrm{ord}_{\tilde{\mathfrak{Q}}}(x) \equiv 0 \bmod p^\ell\}$. Let w be the image of x under this map. Then setting

$$l_\mathfrak{Q} : (\mathcal{O}_{H_n}/\mathfrak{Q})^\times/((\mathcal{O}_{H_n}/\mathfrak{Q})^\times)^{p^\ell} \xrightarrow{\sim} \mathbb{Z}/p^\ell\mathbb{Z}, \quad w \to \mathrm{ord}_{\tilde{\mathfrak{Q}}}(x) \bmod p^\ell$$

gives an isomorphism.

Now define a map

$$\varphi_\mathfrak{q} : (\mathcal{O}_{H_n}/\mathfrak{q}\mathcal{O}_{H_n})^\times/((\mathcal{O}_{H_n}/\mathfrak{q}\mathcal{O}_{H_n})^\times)^{p^\ell} \to I_\mathfrak{q}/p^\ell I_\mathfrak{q}$$

by

$$\varphi_\mathfrak{q}(w) = \sum_{\mathfrak{Q}|\mathfrak{q}} l_\mathfrak{Q}(w)\mathfrak{Q},$$

where we also write $l_\mathfrak{Q}$ for the map composed with the natural projection

$$(\mathcal{O}_{H_n}/\mathfrak{q}\mathcal{O}_{H_n})^\times/((\mathcal{O}_{H_n}/\mathfrak{q}\mathcal{O}_{H_n})^\times)^{p^\ell} \to (\mathcal{O}_{H_n}/\mathfrak{Q})^\times/((\mathcal{O}_{H_n}/\mathfrak{Q})^\times)^{p^\ell}.$$

Proposition 5.2.1. *Suppose $\boldsymbol{\alpha}$ is an Euler system, $n \geqslant 1$, $\mathfrak{r} \in \mathcal{I}_\ell$ and let $\mathfrak{q}$ be a prime of K. Then*

(i) If $\mathfrak{q} \nmid \mathfrak{r}$ then $[\kappa_{\boldsymbol{\alpha}}(\mathfrak{r})]_\mathfrak{q} = 0$.

(ii) If $\mathfrak{q} \mid \mathfrak{r}$ then $[\kappa_{\boldsymbol{\alpha}}(\mathfrak{r})]_\mathfrak{q} = \varphi_\mathfrak{q}(\mathfrak{r}/\mathfrak{q})$,

where $\kappa_{\boldsymbol{\alpha}}$ is the map defined in Proposition 5.1.16.

Proof. This again follows from the alternative definition of Euler systems. See [17, Proposition 2.4]. □

Theorem 5.2.2. *Suppose $\chi \in G^*$, $v \in \left(H_n^\times/(H_n^\times)^{p^\ell}\right)^\chi$, V is a finite Λ_n-submodule of $(H_n^\times/(H_n^\times)^{p^\ell})^\chi$ generated by v, and $\phi \in \mathrm{Hom}_{\Lambda_n}(V, \Lambda_n/p^\ell\Lambda_n)$, $\phi \neq 0$. Let $\mathfrak{c} \in p^e I(\mathscr{G})A(H_n)^\chi$, where $e = 1$ if $p = 2$ and $e = 0$ otherwise. Then there is a prime $\mathfrak{q} \in \mathcal{I}_\ell$ and a prime $\mathfrak{Q}$ of H_n above $\mathfrak{q}$ such that* *(i) the ideal class of $\mathfrak{Q}$ in $A(H_n)^\chi$ is equal to $\mathfrak{c}$,*

(ii) $[v]_{\mathfrak{q}} = 0$ and there exists $u \in (\mathbb{Z}/p^\ell\mathbb{Z})^\times$ such that $\varphi_{\mathfrak{q}}(v) = p^{3e}u\phi(v)$.

Proof. Write $H'_n = H_n(\boldsymbol{\mu}_{p^{\ell+e}})$, and $V_r = V/V \cap \ker r$, where r is the map in Lemma 5.1.3, so that $V_r = V$ if $p > 2$. Fix a primitive p^ℓ-th root of unity ζ, and let

$$\iota : \Lambda_n/p^\ell\Lambda \to \boldsymbol{\mu}_{p^\ell}$$

be the map sending $\sum a_\sigma \sigma \bmod p^\ell$ to ζ^{a_1}. We have an isomorphism

$$\mathrm{Gal}(H'_n(v^{1/p^\ell})/H'_n) \xrightarrow{\sim} \mathrm{Hom}(V_r, \boldsymbol{\mu}_{p^\ell})$$

given by Kummer theory, and $\beta := p^{3e}(\iota \circ \phi) \in p^e \,\mathrm{Hom}(V_r, \boldsymbol{\mu}_{p^\ell})$. Let b be the element of $p^e \,\mathrm{Gal}(H'_n(v^{1/p^\ell})/H'_n)$ corresponding to β via the Kummer map so that

$$\beta(v) = \frac{b(v^{1/p^\ell})}{v^{1/p^\ell}}.$$

Let L_n denote the unramified extension of H_n such that $A(H_n)^\chi = \mathrm{Gal}(L_n/H_n)$. Then we see that there exists a submodule W of V_r such that

$$\mathrm{Gal}(L'_n/L_n \cap H'_n) = \mathrm{Gal}(L'_nH'_n/H'_n) = \mathrm{Hom}(W, \boldsymbol{\mu}_{p^\ell}),$$

where $L'_n = L_n \cap H'_n(v^{1/p^\ell})$. On the other hand, $\mathrm{Gal}(H'_n/H_n)$ acts trivially on $\mathrm{Gal}(L'_nH'_n/H'_n)$ and $\boldsymbol{\mu}_{p^\infty}(H_n) = \boldsymbol{\mu}_2$, so that

$$\mathrm{Hom}(W, \boldsymbol{\mu}_{p^\ell}) = \mathrm{Hom}(W, \boldsymbol{\mu}_{p^\ell})^{\mathrm{Gal}(H'_n/H_n)} = \mathrm{Hom}(W, \boldsymbol{\mu}_2).$$

Therefore, $p^e \,\mathrm{Gal}(L'_n/L_n \cap H'_n) = 0$, and b restricted to L'_n is trivial. Furthermore, $I(\mathscr{G})$ annihilates $\mathrm{Gal}(L_n \cap H'_n/H_n)$ since H'_n is abelian over H, so we can consider $\mathfrak{c}$ as an element of $p^e \,\mathrm{Gal}(L_n/L'_n)$. Hence we can choose $\rho \in \mathrm{Gal}(L_nH'_n(v^{1/p^\ell})/H_n)$ such that $\rho|_{L_n} = \mathfrak{c}$ and $\rho|_{H'_n(v^{1/p^\ell})} = b$. By the Čebotarev density theorem, there are infinitely many prime ideals of H_n of degree one, unramified in $H'_n(v^{1/p^\ell})/K$ whose Frobenius in $\mathrm{Gal}(L_nH'_n(v^{1/p^\ell})/H_n)$ is equal to ρ. Let $\mathfrak{Q}$ be one such prime, lying above a prime $\mathfrak{q}$ of K. First, the fact that $\mathfrak{Q}$ has degree one and ρ fixes L'_n means $\mathfrak{q}$ splits completely in H'_n and thus $\mathfrak{q} \in \mathcal{I}_\ell$. Then class field theory identifies $[\mathfrak{Q}] \in A(H_n)^\chi$ with $\mathrm{Frob}_{\mathfrak{Q}} \in \mathrm{Gal}(L_n/H_n)$, so (i) follows immediately. Now, $[v]_{\mathfrak{q}} = 0$ because all primes lying above $\mathfrak{q}$ are unramified in $H'_n(v^{1/p^\ell})/H_n$, and v is a p^ℓ-th power in $H'_n(v^{1/p^\ell})$.

Also,

$$\operatorname{ord}_{\mathfrak{Q}}(p^{3e}\phi(v)\mathfrak{Q}) = 0 \Leftrightarrow p^{3e}(\iota \circ \phi(v)) = \beta(v) = 1 \Leftrightarrow \frac{b((v)^{1/p^{\ell}})}{(v)^{1/p^{\ell}}} = 1$$

$$\Leftrightarrow v \text{ is an } p^{\ell}\text{-th power modulo } \mathfrak{Q}.$$

On the other hand, we have

$$\operatorname{ord}_{\mathfrak{Q}}(\varphi_{\mathfrak{q}}(v)) = l_{\mathfrak{Q}}(v) = 0 \Leftrightarrow v \text{ is an } p^{\ell}\text{-th power modulo } \mathfrak{Q}.$$

It follows that there exists $u \in (\mathbb{Z}/p^{\ell}\mathbb{Z})^{\times}$ with $\operatorname{ord}_{\mathfrak{Q}}(\varphi_{\mathfrak{q}}(v)) = u \operatorname{ord}_{\mathfrak{Q}}(p^{3e}\phi(v)\mathfrak{Q})$, and the map sending

$$v \mapsto \varphi_{\mathfrak{q}}(v) - p^{3e}u\phi(v)\mathfrak{Q}$$

gives rise to a $\mathscr{G}_n$-equivariant injective homomorphism from V to $\oplus_{\substack{h\in\mathscr{G}_n \\ h\neq 1}}(\mathbb{Z}/p^{\ell}\mathbb{Z})\mathfrak{Q}^h$. But the latter has no non-zero $\mathscr{G}_n$-stable submodules, so

$$\varphi_{\mathfrak{q}}(v) = p^{3e}u\phi(v)\mathfrak{Q},$$

as required. □

5.3 The Inductive Argument

For $n \geqslant 1$, recall that $\Lambda_n = \mathbb{Z}_p[\mathscr{G}_n]$, where $\mathscr{G}_n = \operatorname{Gal}(H_n/K)$. If $\mathfrak{Q}$ is a prime of H_n lying above $\mathfrak{q} \in \mathcal{I}_{\ell}$, then $I_{\mathfrak{q}}$ is a free $\mathbb{Z}[\mathscr{G}_n]$-module of rank 1 generated by $\mathfrak{P}$, and we define

$$v_{\mathfrak{Q}} : H_n^{\times} \to \Lambda_n \quad \text{by} \quad v_{\mathfrak{Q}}(w)\mathfrak{Q} = (w)_{\mathfrak{q}},$$

$$\bar{v}_{\mathfrak{Q}} : H_n^{\times}/(H_n^{\times})^{p^{\ell}} \to \Lambda_n/p^{\ell}\Lambda_n \quad \text{by} \quad \bar{v}_{\mathfrak{Q}}(w)\mathfrak{Q} = [w]_{\mathfrak{q}}$$

The following lemma is an important tool in the induction argument to follow.

Lemma 5.3.1. *Suppose* $\chi \in G^*$, $v \in \left(H_n^{\times}/(H_n^{\times})^{p^{\ell}}\right)^{\chi}$, $\mathfrak{q} \in \mathcal{I}_{\ell}$ *is a prime,* $\mathfrak{Q}$ *is a prime of* H_n *lying above* $\mathfrak{q}$, S *is a set of primes of* K *not containing* $\mathfrak{q}$, *and* $f, \lambda_0, \lambda_1, \lambda_2 \in \Lambda(\mathscr{G})$, *with* $\lambda_0 = 2$ *if* $p = 2$. *Write* B_n *for the subgroup of* $A(H_n)$ *generated by the primes of* H_n *lying above the primes in* S, $\mathfrak{c}$ *for the image of* $\mathfrak{Q}$ *in* $A(H_n)^{\chi}$ *and* V *for the* Λ_n*-submodule of* $H_n^{\times}/(H_n^{\times})^{p^{\ell}}$ *generated by* v. *Suppose also that we have*

(i) $[v]_{\mathfrak{r}} = 0$ *for a prime* $\mathfrak{r}$ *of* K *not in* $S \cup \{\mathfrak{q}\}$,

(ii) the annihilator $\operatorname{Ann}(\mathfrak{c}) \subset \Lambda_n^{\chi}$ *of* $\mathfrak{c}$ *in* $A(H_n)^{\chi}/B_n^{\chi}$ *satisfies* $\lambda_1\operatorname{Ann}(\mathfrak{c}) \subset f\Lambda_n^{\chi}$,

(iii) $\#(A(H_n)^\chi) \mid p^\ell$ *and* $\bar{v}_{\mathfrak{Q}}(v)$ *divides* $(p^\ell/\#(A(H_n)^\chi))\lambda_2$ *in* $\Lambda_n^\chi/p^\ell\Lambda_n^\chi$*, and*

(iv) $f\Lambda(\mathscr{G})$ *is prime to* $I(H_n)$*.*

Then there exists a $\mathscr{G}_n$*-equivariant map* $\phi : V \to \Lambda_n/p^\ell\Lambda_n$ *satisfying*

$$f\phi(v) = \lambda_0\lambda_1\lambda_2\bar{v}_{\mathfrak{Q}}(v).$$

Proof. This is a combination of [17, Lemma 8.2] and [11, Lemma 3.8.4]. □

Fix elements $f_1, \ldots, f_k \in \Lambda(\mathscr{G})$ so that

$$0 \to \oplus_{i=1}^k \frac{\Lambda(\mathscr{G})}{\Lambda(\mathscr{G})f_i} \to A(H_\infty) \to Q \to 0$$

with Q finite. In particular,

$$\mathrm{char}_\Lambda(A(H_\infty)) = \left(\prod_{i=1}^k f_i\right)\Lambda(\mathscr{G}).$$

Theorem 5.3.2. *(i) If* $p > 2$*,* k *is as above and* $\chi \in G^*$*, we have*

$$\mathrm{char}_\Lambda(A(H_\infty)^\chi) \ \ \textit{divides} \ \ I(D_{\mathfrak{p}})^{4k+4}\mathrm{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty})^\chi,$$

where $D_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} D_{\mathfrak{P}}$ *denotes the group generated by the decomposition groups* $D_{\mathfrak{P}}$ *of* $\mathfrak{P}$ *in* H_∞/H*.*

(ii) If $p = 2$*,* k *is as above and* $\chi \in G^*$*, we have*

$$\mathrm{char}_\Lambda(A(H_\infty)^\chi) \ \ \textit{divides} \ \ 2^{6k+6}\mathrm{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty})^\chi.$$

Proof. We will prove this for $p = 2$. The case $p > 2$ is similar. Fix a generator β of $\mathrm{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty})^\chi$. Let $\mathcal{B}$ be an ideal of finite index in $\Lambda(\mathscr{G})$ satisfying the conditions in Theorem 5.1.8 (ii) and Lemma 5.1.12. Take $\lambda \in 2I(\mathscr{G})\mathcal{B}$. By Lemma 5.1.1, $\lambda\Lambda_n/\lambda^{2k}\Lambda_n$ is finite. Also, by Corollary 5.1.10, $\beta\Lambda(\mathscr{G})$ is prime to $I(H_n)$, so $\Lambda_n/\beta\Lambda_n$ is finite. It follows that $\lambda\Lambda_n/\lambda^{2k}\beta\Lambda_n$ is finite. Thus, for some $\ell \geqslant 1$, we have

$$2^\ell\lambda\Lambda_n \subset (2^{n+4k}(\#(A(H_n)^\chi))\lambda^{2k}\beta)\Lambda_n. \tag{5.3.1}$$

Now, by Corollary 5.1.11, there exists $\theta_{\lambda,n} : \bar{\mathcal{E}}_{H_n} \to \Lambda_n$ such that

$$\lambda^2\beta \in \theta_{\lambda,n}(\bar{\mathcal{C}}_{H_n}).$$

Thus, we may fix $u \in \bar{\mathcal{C}}_{H_n}$ with $\theta_{\lambda,n}(u) = \lambda^2\beta$, and also we fix $u_0 \in \mathcal{C}_{H_n}$ with

$$u \equiv u_0 \bmod (\bar{\mathcal{C}}_{H_n})^{p^\ell}.$$

By Proposition 5.1.15, we have an Euler system $\boldsymbol{\alpha}$ and $\sigma \in \mathrm{Gal}(H/K)$ with $\boldsymbol{\alpha}^\sigma(n,1) = u_0$. Let $\kappa_{\boldsymbol{\alpha}}$ be the map defined in Proposition 5.1.16, and let $\mathfrak{c}_1, \ldots, \mathfrak{c}_k \in A(H_n)$ be as given in Lemma 5.1.12. We will use induction to select primes $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_{k+1}$ of H_n lying above primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_{k+1}$ of K satisfying:

$$[\mathfrak{Q}_i] = \lambda\mathfrak{c}_i^\chi \text{ in } A(H_n)^\chi, \text{ and } \mathfrak{q}_i \in \mathcal{I}_\ell, \tag{5.3.2}$$

$$\bar{v}_{\mathfrak{Q}_1}(\kappa_{\boldsymbol{\alpha}}(\mathfrak{q}_1)^\chi) = r_1 2^4\lambda^2\beta \text{ and } f_{i-1}\bar{v}_{\mathfrak{Q}_i}(\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_i)^\chi) = r_i 2^4\lambda^2\bar{v}_{\mathfrak{Q}_{i-1}}(\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_{i-1})^\chi), \tag{5.3.3}$$

where $\mathfrak{a}_i = \mathfrak{q}_1 \cdots \mathfrak{q}_i$ and $r_i \in (\mathbb{Z}/p^\ell\mathbb{Z})^\times$.

For $i = 1$, we take $\mathfrak{c} = \lambda\mathfrak{c}_1^\chi \in 2I(\mathscr{G})A(H_n)^\chi$, $W = \left(\bar{\mathcal{E}}_{H_n}/\bar{\mathcal{E}}_{H_n} \cap (H_n^\times)^{p^\ell}\right)^\chi$, $\phi = 2\theta_{\lambda,n}$ and apply Theorem 5.2.2 and Proposition 5.2.1. Then we obtain a prime $\mathfrak{Q}_1$ of H_n such that $[\mathfrak{Q}_1] = \lambda\mathfrak{c}_1^\chi$ in $A(H_n)^\chi$ and a prime $\mathfrak{q}_1 \in \mathcal{I}_\ell$ lying below $\mathfrak{Q}_1$,

$$\begin{aligned}
[(\kappa_{\boldsymbol{\alpha}}(\mathfrak{q}_1)^\chi)]_{\mathfrak{Q}_1} &= \varphi_{\mathfrak{q}_1}(\kappa_{\boldsymbol{\alpha}}(1)^\chi) = \varphi_{\mathfrak{q}_1}(\boldsymbol{\alpha}^\sigma(n,1)^\chi) \\
&= r_1 2^3\phi(u_0)\mathfrak{Q}_1 = r_1 2^4\theta_{\lambda,n}(u_0)\mathfrak{Q}_1 = r_1 2^4\lambda^2\beta\mathfrak{Q}_1.
\end{aligned}$$

Thus, by the definition of $[\cdot]_{\mathfrak{Q}_1}$, we have

$$\bar{v}_{\mathfrak{Q}_1}\left(\kappa_{\boldsymbol{\alpha}}(\mathfrak{q}_1)^\chi\right) = r_1 2^4\lambda^2\beta,$$

which proves the first equality of (5.3.3).

Now, let $1 < i < k$ and suppose we have selected primes $\mathfrak{Q}_1, \ldots \mathfrak{Q}_i$ satisfying (5.3.2) and (5.3.3). We will define $\mathfrak{Q}_{i+1}$. Recall $\mathfrak{a}_i = \prod_{j \leqslant i}\mathfrak{q}_j$.Let V_i be the Λ_n-submodule of $H_n^\times/(H_n^\times)^{p^\ell}$ generated by $\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_i)^\chi$. We will apply Lemma 5.3.1 with $\mathfrak{Q} = \mathfrak{Q}_i$, $v = \kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_i)^\chi$, $\lambda_1 = \lambda_2 = \lambda$ and $S = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_{i-1}\}$. This is possible because conditions (i), (ii) and (iv) of Lemma 5.3.1 are satisfied thanks to Proposition 5.2.1, Lemma 5.1.12 and Theorem 5.1.6, and (iii) is satisfied because by (5.3.3), $\bar{v}_{\mathfrak{Q}_i}(\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_i)^\chi)$ divides $2^{4i}\lambda^{2i}\beta$ in $\Lambda_n^\chi/2^\ell\Lambda_n^\chi$, so by the choice of ℓ made in (5.3.1), $\bar{v}_{\mathfrak{Q}_i}(\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_i)^\chi)$ divides $\left(p^\ell/\#(A(H_n)^\chi)\right)\lambda$ in $\Lambda_n/2^\ell\Lambda_n$. Thus, we obtain a map $\phi_i : V_i \to \Lambda_n/p^\ell\Lambda_n$ such that

$$f_i\phi_i(\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_i)^\chi) = 2\lambda^2\bar{v}_{\mathfrak{Q}_i}(\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_i)^\chi). \tag{5.3.4}$$

Now, applying Theorem 5.2.2 by setting $V = V_i$, $\mathfrak{c} = \lambda\mathfrak{c}_{i+1}^{\chi}$, $\phi = \phi_i$, we obtain a prime $\mathfrak{q}_{i+1} \in \mathcal{I}_\ell$ and a prime $\mathfrak{Q}_{i+1}$ of H_n lying above it. Then (i) and (ii) of Theorem 5.2.2 gives (5.3.2) for $i+1$. Furthermore, by Proposition 5.2.1 (ii) and Theorem 5.2.2 (iii), for some $r_{i+1} \in (\mathbb{Z}/p^\ell\mathbb{Z})^\times$ we have

$$\begin{aligned} f_i[\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_{i+1})]_{\mathfrak{Q}_{i+1}} &= f_i\varphi_{\mathfrak{q}_{i+1}}(\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_i)^\chi) \\ &= r_{i+1}2^3 f_i\phi_i(\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_i)^\chi)\mathfrak{Q}_{i+1} \\ &= r_{i+1}2^4\lambda^2\bar{v}_{\mathfrak{Q}_i}(\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_i)^\chi)\mathfrak{Q}_{i+1}, \end{aligned}$$

where the last equation follows from (5.3.4). This proves (5.3.3) for $i+1$. Finally, combining (5.3.3) for $1 \leqslant i \leqslant k+1$ gives

$$\prod_{i=1}^{k} f_i\bar{v}_{\mathfrak{Q}_{k+1}}(\kappa_{\boldsymbol{\alpha}}(\mathfrak{a}_{k+1})^\chi) = r2^{4k+4}\lambda^{2k+2}\beta$$

in $\Lambda_n/p^\ell\Lambda_n$ for some $u \in (\mathbb{Z}/p^\ell\mathbb{Z})^\times$. It follows that

$$\mathrm{char}_\Lambda(A(H_\infty)) = \prod_{i=1}^{k} f_i \quad \text{divides} \quad 2^{4k+4}\lambda^{2k+2}\beta\Lambda(\mathscr{G}) = 2^{4k+4}\lambda^{2k+2}\mathrm{char}_\Lambda\left(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}\right).$$

This holds for every $\lambda \in 2I(\mathscr{G})\mathcal{B}$, so in particular, holds for λ being the greatest common divisor λ_0 of all elements in $2I(\mathscr{G})\mathcal{B}$. It is easy to show that in this case we have $\lambda_0\Lambda(\mathscr{G}) = 2I(\mathscr{G})$. This concludes the proof of Theorem 5.3.2, because $\mathrm{char}_\Lambda(A(H_\infty))$ is prime to $I(\mathscr{G})$ by Theorem 5.1.6. □

Corollary 5.3.3. *Let $p > 2$. Then*

$$\mathrm{char}_\Lambda(A(H_\infty)) \ \textit{divides}\ \mathrm{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}).$$

Proof. We have shown in Theorem 5.1.6 that $\mathrm{char}_\Lambda(A(H_\infty))$ is prime to $I(D_\mathfrak{p})$, so by Theorem 5.3.2, $\mathrm{char}_\Lambda(A(H_\infty))$ divides $\mathrm{char}_\Lambda(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty})$. □

Recall that $p \nmid [H : K]$ by assumption.

Theorem 5.3.4. *We have* $\mathrm{char}_\Lambda(X(H_\infty)) = \mathrm{char}_\Lambda\left(U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}\right)$ *if and only if* $\mathrm{char}_\Lambda(A(H_\infty)) = \mathrm{char}_\Lambda\left(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}\right)$*, and*

$$\mathrm{char}_\Lambda(X(H_\infty)) \mid 2^{e(6k+6)}\mathrm{char}_\Lambda\left(U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}\right).$$

Proof. Recall from (4.4.2) that we have an exact sequence

$$0 \to \bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty} \to U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty} \to X(H_\infty) \to A(H_\infty) \to 0,$$

and therefore $\mathrm{char}_\Lambda(A(H_\infty))\mathrm{char}_\Lambda\left(U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}\right) = \mathrm{char}_\Lambda(X(H_\infty))\mathrm{char}_\Lambda\left(\bar{\mathcal{E}}_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}\right)$. The last assertion of the theorem follows from Theorem 5.3.2 and Corollary 5.3.3. □

Chapter 6

Proof of the main conjecture for H_∞/H

6.1 The Iwasawa Invariants of $X(H_\infty)$

Recall that

$$\mathscr{G} \simeq G \times \Gamma,$$

where we identify G with $\mathrm{Gal}(H_\infty/K_\infty)$ and Γ with $\mathrm{Gal}(K_\infty/K)$. Recall that any $\Lambda_{\mathscr{I}}(\mathscr{G}) = \mathscr{I}[[\mathscr{G}]]$-module M can be decomposed into a direct sum $M = \oplus_{\chi \in G^*} M^\chi$ of its χ-components. Thus, let us consider $\mathscr{I}[[\Gamma]]$ as a $\Lambda_{\mathscr{I}}(\mathscr{G})$-module via χ. Given a finitely generated torsion $\Lambda_{\mathscr{I}}(\mathscr{G})$-module M, recall from Section 4.4 that $\mathrm{char}(M) \subset \Lambda_{\mathscr{I}}(\mathscr{G})$ denotes the characteristic ideal of M. If X is a $\Lambda(\mathscr{G})$-module and $\chi \in G^*$, we write X^χ for $(X \widehat{\otimes}_{\mathbb{Z}_p} \mathscr{I})^\chi$. This is justified because we are only interested in $\mathrm{char}(X)^\chi$, and the characteristic ideals of a Γ-module behaves well under extension of scalars. This comes from the fact that we can identify $\mathscr{I}[[\Gamma]]$ with $\mathscr{I}[[T]]$.

Recall also that any $f(T) \in \mathscr{I}[[T]]$ can be written uniquely, by the p-adic Weierstrass preparation theorem, in the form

$$f(T) = \boldsymbol{\pi}^m P(T) U(T)$$

where $\boldsymbol{\pi}$ is a uniformiser of $\mathscr{I}$, $P(T)$ is a distinguished polynomial, i.e., a monic polynomial whose coefficients are divisible by $\boldsymbol{\pi}$, and $U(T)$ is a unit in $\mathscr{I}[[T]]$. Let ϵ be the absolute ramification index of $\mathscr{I}$. The invariants

$$\mu(f) = \frac{m}{\epsilon} \quad \text{and} \quad \lambda(f) = \deg P(T)$$

are called the Iwasawa μ-invariant and λ-invariant of f, respectively. The Iwasawa invariants of $\Lambda(\mathscr{G})$-modules are defined similarly, and if $M = X\widehat{\otimes}_{\mathbb{Z}_p}\mathscr{I}$ is obtained from a $\Lambda(\mathscr{G})$-module X by extension of scalars to $\mathscr{I}$, the invariants of M coincide with those of X.

Define $f^\chi = \operatorname{char}(X(H_\infty))^\chi$ and let $g^\chi = \operatorname{char}\left(U_{H\infty}/\bar{\mathcal{C}}_{H_\infty}\right)^\chi$, and set $f = \prod f^\chi$ and $g = \prod g^\chi$. By Theorem 5.3.4, we have

Theorem 6.1.1. *$f^\chi \mid \boldsymbol{\pi}^{ek} g^\chi$ for some integer $k \geq 0$, $e = 0$ if $p > 2$ and $e = 1$ if $p = 2$.*

Thus, in order to show f^χ and g^χ define the same ideal, it remains to show that f and g the have the same Iwasawa invariants. We shall compute them separately, and show that they are equal. First, we compute at the invariants of $X(H_\infty)$ using class field theory, and in Section 6.2 we compute the invariants of $U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}$ using the analytic class number formula.

Recall from the proof of Theorem 5.1.5 that $X(H_\infty)/I(H_n)X(H_\infty)$ is equal to $\mathrm{Gal}(M(H_n)/H_\infty)$, where $M(H_n)$ is the maximal abelian p-extension of H_n which is unramified outside the primes above $\mathfrak{p}$. Thus the asymptotic formula of Iwasawa [23, Theorem 13.13] gives:

Theorem 6.1.2. *Let f be the characteristic power series for $X(H_\infty)$ as a $\mathbb{Z}_p[[\Gamma]]$-module. For sufficiently large n, we have*

$$\operatorname{ord}_p\left(\#(X(H_\infty)/I(H_n)X(H_\infty)\right) = \mu(f)p^{n-1-e} + \lambda(f)(n-1-e) + c,$$

where $\mu(f)$ and $\lambda(f)$ are the Iwasawa invariants of $X(H_\infty)$ and $c \in \mathbb{Z}$ is independent of n.

We will now compute p-adic valuation of the index $[M(H_n) : H_\infty]$ using the methods of Coates and Wiles [7], and use it to find $\operatorname{ord}_p\left(\#(X(H_\infty)/I(H_n)X(H_\infty)\right)$. We note that p is assumed to be an odd prime number in [7], but it can easily be extended to $p = 2$ in our case, because 2 splits in K and $(p, h) = 1$ by assumption.

Set $[H_n : K] = d$, which is equal to $p^{n-1-e}h$ where $e = 0$ or 1 according as p is odd or even. Let $\xi_1, \ldots \xi_d$ denote the distinct embeddings of H_n into $\mathbb{C}_p$. Since H_n is totally imaginary, $\operatorname{rank}_{\mathbb{Z}}\left(\mathcal{E}_{H_n}/(\mathcal{E}_{H_n})_{tor}\right) = d - 1$. We pick a basis $\epsilon_1, \ldots, \epsilon_{d-1}$ for $\mathcal{E}_{H_n}/(\mathcal{E}_{H_n})_{tor}$, and put $\epsilon_d = 1 + p$ or $1 + p^2$ according as p is odd or even.

Definition 6.1.3.

$$R_n = (d \log \epsilon_d)^{-1} \det\left(\log(\xi_i(\epsilon_j))\right)_{1 \leqslant i,j \leqslant d}.$$

Let C_{H_n} denote the idele class group of H_n. For each $n \geqslant 1$, let

$$Y_n = \cap_{m \geqslant n} N_{H_m/H_n} C_{H_m}$$

Let $\Phi_\mathfrak{p} = H_n \otimes_K K_\mathfrak{p}$.

Let $\mathscr{P}$ denote the set of primes of H_n lying above $\mathfrak{p}$. Let $U_{H_{n,\mathfrak{P}}}$ denote the group of units in the completion of H_n at $\mathfrak{P}$ which are congruent to 1 modulo $\mathfrak{P}$, and let $t \geqslant 0$ be such that $p^{-t}\mathcal{O}_\mathfrak{P} \subset \log U_{H_{n,\mathfrak{P}}}$ for each $\mathfrak{P} \in \mathscr{P}$.

The p-adic logarithm gives a homomorphism $\log : U_{H_{n,\mathfrak{P}}} \to H_{n,\mathfrak{P}}$ whose kernel has order $w_\mathfrak{P} = \#\boldsymbol{\mu}_{p^\infty}(H_{n,\mathfrak{P}})$. Write $\log U_{H_n} = \prod_{\mathfrak{P}\in\mathscr{P}} \log U_{H_{n,\mathfrak{P}}}$, so that we have $\log : U_{H_n} \to \Phi_\mathfrak{p}$ with kernel $w_\mathfrak{p} = \prod_{\mathfrak{P}\in\mathscr{P}} w_\mathfrak{P}$,

Lemma 6.1.4.

$$\mathrm{ord}_p\left([\prod_{\mathfrak{P}\in\mathscr{P}} p^{-t}\mathcal{O}_\mathfrak{P} : \log U_{H_n}]\right) = \mathrm{ord}_p\left(w_\mathfrak{p} \prod_{\mathfrak{P}\in\mathscr{P}} \mathrm{N}\mathfrak{P}\right) + td.$$

Proof. See [6, Lemma 7]. □

Let $V^n = 1 + \mathfrak{p}^n\mathcal{O}_\mathfrak{p}$ denote the local units of $K_\mathfrak{p}$ which are congruent to 1 modulo $\mathfrak{p}^n$, and define $D_n = V^{1+e}\bar{\mathcal{E}}_{H_n} \subset U_{H_n}$, where $e = 0$ or 1 according as $p > 2$ or $p = 2$. Furthermore, let $\Delta_{H_n/K}$ denote the discriminant of H_n/K, and pick a generator Δ_n of the ideal $\Delta_{H_n/K}\mathcal{O}_\mathfrak{p}$.

Lemma 6.1.5.

$$\mathrm{ord}_p\left([\log U_{H_n} : \log D_n]\right) = \mathrm{ord}_p\left(\frac{R_n}{\sqrt{\Delta_n}}\left(w_\mathfrak{p}\prod_{\mathfrak{P}\in\mathscr{P}} \mathrm{N}\mathfrak{P}\right)^{-1}\right) + n + 1.$$

Proof. Using methods analogous to [6, Lemma8], we can show that

$$\mathrm{ord}_p\left([\prod_{\mathfrak{P}\in\mathscr{P}} p^{-t}\mathcal{O}_\mathfrak{P} : \log D_n]\right) = \mathrm{ord}_p\left(\frac{R_n}{\sqrt{\Delta_n}}\right) + td + n - e + \mathrm{ord}_p\left(\log(1 + p^{1+e})\right), \tag{6.1.1}$$

where $e = 0$ or 1 according as $p > 2$ or $p = 2$. We have $\mathrm{ord}_p\left(\log(1 + p^{1+e})\right) = 1 + e$, so the right hand side of (6.1.1) is equal to $\mathrm{ord}_p\left(\frac{R_n}{\sqrt{\Delta_n}}\right) + td + n + 1$. The result now follows from Lemma 6.1.4. □

Corollary 6.1.6.

$$\operatorname{ord}_p\left([U_{H_n}:D_n]\right)=\operatorname{ord}_p\left(\frac{R_n}{\omega_{H_n}\sqrt{\Delta_n}}\left(\prod_{\mathfrak{P}\in\mathscr{P}}\mathrm{N}\mathfrak{P}\right)^{-1}\right)+n+1.$$

Proof. This is an immediate consequence of Lemma 6.1.5, obtained by applying the snake lemma to the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & D_n \arrow[r] \arrow[d, "\log"'] & U_{H_n} \arrow[r] \arrow[d, "\log"] & U_{H_n}/D_n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \log D_n \arrow[r] & \log U_{H_n} \arrow[r] & \log U_{H_n}/\log D_n \arrow[r] & 0.
\end{tikzcd}$$

with exact rows. □

Lemma 6.1.7.

$$\begin{aligned}Y_n\cap U_{H_n}&=\ker\left(\mathrm{N}_{\Phi_\mathfrak{p}/K_\mathfrak{p}}\,|_{U_{H_n}}\right)\\ \bar{\mathcal{E}}_{H_n}&=\ker\left(\mathrm{N}_{\Phi_\mathfrak{p}/K_\mathfrak{p}}\,|_{D_n}\right).\end{aligned}$$

Proof. See Lemma 5 and Lemma 6 of [6]. □

Lemma 6.1.8.

$$[Y_n\cap U_{H_n}:\bar{\mathcal{E}}_{H_n}]=\operatorname{ord}_p\left(\frac{R_n}{\sqrt{\Delta}_n}\prod_{\mathfrak{P}\in\mathscr{P}}(1-(\mathrm{N}\mathfrak{P})^{-1})\right)+n$$

Proof. By Lemma 6.1.7 and the definition of D_n, we have $\mathrm{N}_{\Phi_\mathfrak{p}/K_\mathfrak{p}}(D_n)=(V^{1+e})^d=(V^{1+e})^{n-e}=V^{n+1}$. Hence, applying Lemma 6.1.7 again, we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \bar{\mathcal{E}}_{H_n} \arrow[r] \arrow[d] & D_n \arrow[r, "\mathrm{N}_{\Phi_\mathfrak{p}/K_\mathfrak{p}}"] \arrow[d] & V^{n+1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Y_n\cap U_{H_n} \arrow[r] & U_{H_n} \arrow[r, "\mathrm{N}_{\Phi_\mathfrak{p}/K_\mathfrak{p}}"] & V^n \arrow[r] & 0.
\end{tikzcd}$$

Lemma 6.1.8 now follows from Lemma 6.1.7 on noting that $\operatorname{ord}_\mathfrak{p}\left(\prod_{\mathfrak{P}\in\mathscr{P}}(1-(\mathrm{N}\mathfrak{P})^{-1})\right)=\operatorname{ord}_p\left(\prod_{\mathfrak{P}\in\mathscr{P}}(\mathrm{N}\mathfrak{P})^{-1}\right)$ and $[V^n:V^{n+1}]=p$. □

Theorem 6.1.9. *Let $M(H_n)$ be the maximal abelian p-extension of H_n which is unramified outside the primes in $\mathscr{P}$. Then*

$$\operatorname{ord}_p\left([M(H_n) : H_\infty]\right) = \operatorname{ord}_p\left(\frac{h_{H_n} R_n}{\sqrt{\Delta_n}} \prod_{\mathfrak{P}\in\mathscr{P}} (1 - (\mathrm{N}\mathfrak{P})^{-1})\right) + n,$$

where h_{H_n} denotes the class number of H_n.

Proof. Let $L(H_n)$ be the maximal unramified extension of H_n in $M(H_n)$. Thus we may identify $\mathrm{Gal}(L(H_n)/H_n)$ with $A(H_n)$, the p-primary part of the ideal class group of H_n. Class field theory gives an isomorphism

$$Y_n \cap U_{H_n}/\bar{\mathcal{E}}_{H_n} \cong \mathrm{Gal}(M(H_n)/L(H_n)H_\infty).$$

Noting that $L(H_n) \cap H_\infty = H_n$ because H_∞/H_n is totally ramified at $\mathfrak{p}$, we obtain

$$0 \to Y_n \cap U_{H_n}/\bar{\mathcal{E}}_{H_n} \to \mathrm{Gal}(M(H_n)/H_\infty) \to A(H_n) \to 0.$$

The theorem now follows from Lemma 6.1.8 and the fact that $\operatorname{ord}_p\left(\#(A(H_n))\right) = \operatorname{ord}_p\left(h_{H_n}\right)$. □

Corollary 6.1.10. *Let f be the characteristic power series for $X(H_\infty)$ as a Γ-module. Then for sufficiently large n,*

$$\mu(f) \cdot p^{n-1-e}(p-1) + \lambda(f) = 1 + \operatorname{ord}_p\left(\frac{h_{H_{n+1}} R_{n+1}}{\sqrt{\Delta_{n+1}}} / \frac{h_{H_n} R_n}{\sqrt{\Delta_n}}\right),$$

where $\mu(f)$ and $\lambda(f)$ are the Iwasawa invariants of $X(H_\infty)$.

Proof. By Theorem 6.1.9, it is clear that the right hand side of the above equation is equal to $\operatorname{ord}_p\left([M(H_{n+1}) : H_\infty]/[M(H_n) : H_\infty]\right)$. Recalling that $\mathrm{Gal}(M(H_n)/H_\infty) = X(H_\infty)/I(H_n)X(H_\infty)$, Theorem 6.1.2 gives $\operatorname{ord}_p\left([M(H_{n+1}) : H_\infty]/[M(H_n) : H_\infty]\right)$ is equal to

$$(\mu(f)p^{n-e} + \lambda(f)(n-e) + c) - (\mu(f)p^{n-1-e} + \lambda(f)(n-1-e) + c) = \mu(f)p^{n-1-e}(p-1) + \lambda(f).$$

This completes the proof of the corollary. □

6.2 The Iwasawa Invariants of the $\mathfrak{p}$-adic L-function

In this section, we will compute the Iwasawa invariants of $U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}$ and show that they coinsides with those of $X(H_\infty)$ computed in Corollary 6.1.10. We will follow the methods discussed in [8, Chapter III.2]. Again, the prime p is assumed to be odd in Chapter III of [8], but the methods still holds for $p = 2$ thanks to our assumptions that p splits in K and $p \nmid [H : K]$.

Fix a generator $g \in \mathscr{I}[[\Gamma]]$ of char $\left(U_{H_\infty}/\bar{\mathcal{C}}_{H_\infty}\right)$, and let $\mu(g)$ and $\lambda(g)$ denote the Iwasawa invariants.

Lemma 6.2.1. *Recall that $\Gamma_n = \Gamma^{p^{n-1-e}}$. For any character ρ of Γ of finite order, write $l(\rho) = n - 1 - e$ if $\rho(\Gamma_n) = 1$ but $\rho(\Gamma_{n-1}) \neq 1$. Then for n sufficiently large,*

$$\operatorname{ord}_p\left(\prod_{l(\rho)=n-e} \rho(g)\right) = \mu(g) \cdot p^{n-1-e}(p-1) + \lambda(g).$$

Proof. See [8, Lemma III.2.9]. □

Given a ramified character ε of $\mathscr{G} = G \times \Gamma$, write $\varepsilon = \chi\rho$ where χ is a character of G and ρ is a character of Γ. Let $\mathfrak{f}_\varepsilon$ denote the conductor of ε, $f_\varepsilon = \mathfrak{f}_\varepsilon \cap \mathbb{Z}$, and let B_n be the collection of all ε with $\mathfrak{p}^n \mid\mid \mathfrak{f}_\varepsilon$. Then

Proposition 6.2.2. *For n sufficiently large,*

$$ord_p\left(\prod_{l(\rho)=n-e} \rho(g)\right) = 1 + \operatorname{ord}_p\left(\frac{h_{H_{n+1}}R_{n+1}}{\sqrt{\Delta_{n+1}}} \Big/ \frac{h_{H_n}R_n}{\sqrt{\Delta_n}}\right).$$

Proof. We follow the arguments in Proposition III.2.10 and 2.11 in [8]. Any $\varepsilon \in B_n$ can be written in the form $\varepsilon = \chi\rho$ where χ is a character of G and ρ is a character of Γ with $l(\rho) = n$. Let $H'_\infty = HK(\mathfrak{p}^{*\infty})$ and $S = \{s \in \mathrm{Gal}(H'_\infty H_n/K) : s|_{H'_\infty} = (\mathfrak{p}^n, H'_\infty/K)\}$. For $n \geqslant 0$, fix primitive p^n-th roots of unity ζ_n satisfying $\zeta_n^p = \zeta_{n-1}$, and define $G(\varepsilon)$ by

$$G(\varepsilon) = \frac{\rho(\mathfrak{p}^n)}{p^n} \sum_{s\in S} \chi(s)(\zeta_n^s)^{-1}.$$

Let

$$S_p(\varepsilon) = -\frac{1}{12^2 f_\varepsilon w_{\mathfrak{f}_\varepsilon}} \cdot \sum_{\mathfrak{c}\in Cl(\mathfrak{f}_\varepsilon)} \varepsilon^{-1}(\mathfrak{c}) \log\, \varphi_{\mathfrak{f}_\varepsilon}(\mathfrak{c}),$$

where $Cl(\mathfrak{f}_\varepsilon)$ denotes the ray class group modulo $\mathfrak{f}_\varepsilon$ and $\varphi_{\mathfrak{f}_\varepsilon}(\mathfrak{c})$ is Robert's invariant associated to the class $\mathfrak{c}$ (see [8, II.2.6]). Then by [8, Theorem II.5.2], we have

$$\rho(g^\chi) = \int_{\mathscr{G}_\chi} \chi\rho d\nu_{\mathfrak{p}}^\chi = \begin{cases} G(\varepsilon)S_p(\varepsilon) & \text{if } \chi \text{ is non-trivial} \\ (\rho(\gamma)-1)\,G(\varepsilon)S_p(\varepsilon) & \text{if } \chi = 1, \end{cases}$$

where γ is a topological generator of Γ and $\nu_{\mathfrak{p}}$ satisfies Theorem 4.2.7. Hence $\prod_{l(\rho)=n-e}(\rho(\gamma)-1) = \prod_{\zeta\in\boldsymbol{\mu}_{p^{n-e}}}(\zeta-1)$. Noting that $\mathrm{ord}_p\left(\prod_{\zeta\in\boldsymbol{\mu}_{p^{n-e}}}(\zeta-1)\right)) = 1$, we obtain

$$ord_p\left(\prod_{l(\rho)=n-e}\rho(g)\right) = 1 + \mathrm{ord}_p\left(\prod_{\varepsilon\in B_{n+1-e}} G(\varepsilon)S(\varepsilon)\right). \tag{6.2.1}$$

On the other hand, using the analytic class number formula for the fields H_{n+1} and H_n gives (see [8, III.2.11]):

$$\mathrm{ord}_p\left(\prod_{\varepsilon\in B_{n+1-e}} G(\varepsilon)S_p(\varepsilon)\right) = \mathrm{ord}_p\left(\frac{h_{H_{n+1}}R_{n+1}}{\sqrt{\Delta_{n+1}}}/\frac{h_{H_n}R_n}{\sqrt{\Delta_n}}\right) \tag{6.2.2}$$

Combining (6.2.1) and (6.2.2) completes the proof of Proposition 6.2.2. □

Comparing Corollary 6.1.10, Lemma 6.2.1 and Proposition 6.2.2, we conclude that f and g have the same Iwasawa invariants. As discussed at the beginning of Section 6.1, this together with the divisibility relation obtained in Theorem 5.3.4 completes the proof of the main conjecture for H_∞/H.

Chapter 7

Some Remarks on the Main Conjecture for E/H

7.1 Relation to the Main Conjecture for H_∞/H

In this section, we briefly discuss the main conjecture for E/H and its relation to the main conjecture for H_∞/H which we proved in Chapter 6. Let $M(F_\infty)$ be the maximal abelian p-extension of F_∞ which is unramified outside the primes above $\mathfrak{p}$, and put $X(F_\infty) = \mathrm{Gal}(M(F_\infty)/F_\infty)$.

Let

$$Y_\infty = \mathrm{Hom}\left(\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty)^\Delta, K_\mathfrak{p}/\mathcal{O}_\mathfrak{p}\right),$$

the Pontryagin dual of $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty)^\Delta$. We first discuss its relation to the Selmer group of E over H_∞. We note that Theorem 3.3.1 holds with H with H_n and F with F_n for all n. Thus we can take the inductive limit to obtain a surjection from $\mathrm{Sel}_{\mathfrak{p}^\infty}^{(\mathcal{T})}(E/H_\infty)$ to $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty)^\Delta$ given by the restriction map, where $\mathcal{T}$ is the set of places of H_∞ lying above $\mathfrak{p}$ and the primes of bad reduction for E. This is an isomorphism if $p > 2$, and the kernel of this map is the inductive limit of $H^1(\Delta, E_{\mathfrak{p}^2})$ if $p = 2$, which is a cyclic group of order 2.

We can further describe Y_∞ in terms of $X(F_\infty)$ as follows. Recall that $\mathfrak{H} = \mathrm{Gal}(F_\infty/H)$, which is isomorphic to $\Delta \times \Gamma$, and $\chi_\mathfrak{p} : \mathfrak{H} \to \mathcal{O}_\mathfrak{p}^\times$ is the isomorphism giving the action of $\mathfrak{H}$ on $E_{\mathfrak{p}^\infty}$. Let $\rho = \chi_\mathfrak{p}|_\Delta$, so ρ has order $p-1$ or 2, according as $p > 2$ or $p = 2$. If $p > 2$, the action of Δ on any $\mathbb{Z}_p[\Delta]$-module A is semisimple, and we have the decomposition

$$A = \oplus_{i \bmod p-1} A^{(\rho^i)},$$

where $A^{(\rho^i)} = \{a \in A : \sigma \cdot a = \rho^i(\sigma)a \text{ for all } \sigma \in \Delta\}$. If $p = 2$, no such decomposition exists. In this case, we write δ for the non-trivial element of Δ, so that $\delta \cdot z = -z$ for all $z \in E_{\mathfrak{p}^\infty}$.

Lemma 7.1.1. *(i) If $p > 2$, $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty)^\Delta = \mathrm{Hom}(X(F_\infty)^\rho, E_{\mathfrak{p}^\infty})$.*

(ii) If $p = 2$, $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty)^\Delta = \mathrm{Hom}(X(F_\infty)/(\delta+1)X(F_\infty), E_{\mathfrak{p}^\infty})$.

Proof. Part (i) follows immediately from semisimplicity, and the fact that Δ acts on $E_{\mathfrak{p}^\infty}$ via the character ρ. For (ii), note that given $f \in \mathrm{Hom}(X(F_\infty), E_{\mathfrak{p}^\infty})$, we have

$$(\delta f)(x) = \delta f(\delta^{-1}x) = -f(\delta^{-1}x) = -f(\delta x).$$

Hence, we have $\delta f = f$ if and only if $f((\delta+1)x) = 0$ for all $x \in X(F_\infty)$, and so (ii) follows. □

Let

$$T_\rho(E)^{(-1)} = \mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(E_{\mathfrak{p}^\infty}, K_\mathfrak{p}/\mathcal{O}_\mathfrak{p}),$$

a free $\mathcal{O}_\mathfrak{p}$-module of rank 1 on which $\mathfrak{H}$ acts via $\chi_\mathfrak{p}^{-1}$. Given any $\mathcal{O}_\mathfrak{p}$-module V endowed with an action of $\mathfrak{H}$, we define

$$V(-1) = V \otimes_{\mathcal{O}_\mathfrak{p}} T_\mathfrak{p}(E)^{(-1)},$$

endowed with the diagonal action of $\mathfrak{H}$, i.e. $\sigma(v \otimes t) = \sigma(v) \otimes \sigma(t)$ for any $\sigma \in \gamma G$, $v \in V$ and $t \in T_\mathfrak{p}(E)^{(-1)}$.

In view of the above lemma, we obtain

Proposition 7.1.2. *The Pontryagin dual Y_∞ of $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty)^\Delta$ is isomorphic as Γ-module to $X(F_\infty)^{(\rho)}(-1)$ if $p > 2$, and to $(X(F_\infty)/(\delta+1)X(F_\infty))(-1)$ if $p = 2$.*

In particular, we have shown that Y_∞ is a finitely generated torsion $\Lambda(\Gamma)$-module because $X(F_\infty)$ is, by the $\mathfrak{p}$-adic Leopoldt conjecture for abelian extensions of K, and

$$\mathrm{char}(Y_\infty) = \begin{cases} \mathrm{char}\left(X(F_\infty)^{(\rho)}\right) & \text{if } p > 2 \\ \mathrm{char}(X(F_\infty)/(\delta+1)X(F_\infty)) & \text{if } p = 2. \end{cases}$$

Recall that $\mathfrak{G}$ denotes the Galois group of F_∞ over K, and $\mathfrak{G} = \Sigma \times \Gamma$ where we identify Σ with $\mathrm{Gal}(F_\infty/K_\infty)$ and Γ with $\mathrm{Gal}(K_\infty/K)$. Let $\mathscr{I}'$ be the extension of $\mathscr{I}$ generated by the values of all characters χ on Σ. We have $\mathscr{I}' = \mathscr{I}$ if $p > 2$ because $p \nmid \#(\Sigma)$. If $p > 2$, given a finitely generated torsion $\Lambda(\mathfrak{G})$-module M and $\chi \in \Sigma^*$, we write M^θ for $e_\theta(M\widehat{\otimes}_{\mathbb{Z}_p}\mathscr{I})$ where e_θ is the idempotent corresponding to θ. That is, M^θ is the largest submodule of M on which Σ acts via θ. For any p, we let M_θ denote the largest quotient of $M\widehat{\otimes}_{\mathbb{Z}_p}\mathscr{I}'$ on which Σ acts through θ. If the p-torsion submodule is finite, then M_θ is pseudo-isomorphic to M^θ [8, III.1.8]. In particular, we know that this is true for $p > 2$, because the μ-invariant of $X(F_\infty)$ is zero in this case, and thus $X(F_\infty)$ is a free $\mathbb{Z}_p$-module of finite rank (see [8, Corollary III.2.12]). Let $\mathbf{\Psi}_\mathfrak{p} \in \Lambda_\mathscr{I}(\mathfrak{G})$ denotes the $\mathfrak{p}$-adic L-function attached to E/H constructed at the end of Section 4.2.

Now, let $Y(F_\infty) = \mathrm{Gal}(M(F_\infty)/F_\infty M(H_\infty))$. Furthermore, since $M(H_\infty) \cap F_\infty = H_\infty$, we can identify $X(H_\infty)$ with $\mathrm{Gal}(F_\infty M(H_\infty)/F_\infty)$, and we have an exact sequence

$$0 \to Y(F_\infty) \to X(F_\infty) \to X(H_\infty) \to 0. \tag{7.1.1}$$

We will see in Lemma 7.1.8 that $\mathrm{char}(Y(F_\infty)) = \mathrm{char}(Y_\infty)$ for all p, assuming $X(F_\infty)$ has μ-invariant equal to 0 and both $X(F_\infty)$ and $X(H_\infty)$ contain no non-zero finite Γ-submodules for $p = 2$ (automatic if $p > 2$).

Conjecture 7.1.3 (The Main Conjecture for $Y(F_\infty)$)**.** *For any character θ on Σ,*

$$\mathrm{char}\left((Y(F_\infty))_\theta\right) = (\mu_E)^\theta,$$

where μ_E is as defined in Theorem 4.1.11.

The techniques used in Chapters 5 and 6 extend to apply for $Y(F_\infty)$ without any difficulty if $p > 2$. They can also be applied to the case $p = 2$ if we assume in addition that we can prove the μ-invariant of $X(F_\infty)$ is zero.

Finally, the main conjecture for E/H says:

Conjecture 7.1.4 (The Main Conjecture for E/H)**.** *For any character θ on Σ,*

$$\mathrm{char}\left(X(F_\infty)_\theta\right) = (\mathbf{\Psi}_\mathfrak{p})^\theta,$$

where $\mathbf{\Psi}_\mathfrak{p}$ is defined at the end of section 4.2.

Clearly, we have $\mathrm{char}(X(F_\infty)) = \mathrm{char}(X(H_\infty))\mathrm{char}(Y(F_\infty))$. If $p > 2$, the main conjecture for $X(F_\infty)$ easily follows from the main conjectures for $X(H_\infty)$ and $Y(F_\infty)$, using the fact that $(\#(\Sigma), p) = 1$. Hence, in the remainder of this section, we study more closely the relation between $\mathrm{char}(X(F_\infty))$ and $\mathrm{char}(X(H_\infty))$ when $p = 2$.

Lemma 7.1.5. *Let $p = 2$. Then $X(F_\infty)_\Delta = \mathrm{Gal}(L/F_\infty)$, where L is the maximal abelian extension of H_∞ contained in $M(F_\infty)$.*

Proof. By definition, $X(F_\infty)_\Delta = X(F_\infty)/(\delta-1)X(F_\infty)$ where δ is the non-trivial element of Δ. Note first that $M(F_\infty)/H_\infty$ is a Galois extension. Indeed, $\delta(M(F_\infty))$ is again an extension of F_∞ since F_∞ is Galois over H_∞, and it is clearly an abelian 2-extension over F_∞. Also the primes of $M(F_\infty)$ lying above the primes of H where E has bad reduction ramify completely in F_∞/H_∞, so $\delta(M(F_\infty))/F_\infty$ is still unramified outside the primes above $\mathfrak{p}$, hence $\delta(M(F_\infty)) = M(F_\infty)$ as required. Now, $\mathrm{Gal}(F_\infty/H_\infty)$ is generated by δ so every element of $\mathrm{Gal}(M(F_\infty)/H_\infty)$ can be expressed in the form $\gamma_\delta^a x$ for $x \in X(F_\infty)$, γ_δ a lifting of δ in $\mathrm{Gal}(M(F_\infty)/H_\infty)$ and $a \in \{0,1\}$. For any $x \in X(F_\infty)$, we have $(\delta-1)x = \gamma_\delta x \gamma_\delta^{-1} x^{-1} = [\gamma_\delta, x]$, a commutator. We claim that $(\delta-1)X(F_\infty)$ is the full commutator subgroup of $\mathrm{Gal}(M(F_\infty)/H_\infty)$. Indeed, for any two elements $\gamma_\delta^{a_1}x_1$, $\gamma_\delta^{a_2}x_2 \in \mathrm{Gal}(M(F_\infty)/H_\infty)$, a simple computation shows that we have

$$[\gamma_\delta^{a_1}x_1, \gamma_\delta^{a_2}x_2] = \delta^{a_2}(\delta^{a_1}-1)x_2 - \delta^{a_1}(\delta^{a_2}-1)x_1,$$

which clearly lies inside $(\delta-1)X(F_\infty)$ for any $a_1, a_2 \in \{0,1\}$ and $x_1, x_2 \in X(F_\infty)$. Hence if we let L be the maximal abelian extension of H_∞ contained in $M(F_\infty)$, we have

$$\mathrm{Gal}(M(F_\infty)/L) = (\delta-1)X(F_\infty),$$

and so

$$X(F_\infty)/(\delta-1)X(F_\infty) = \mathrm{Gal}(L/F_\infty)$$

as claimed. □

Proposition 7.1.6. *Let $p = 2$. If $X(H_\infty)$ is a finitely generated $\mathbb{Z}_2$-module, then so is $X(F_\infty)_\Delta$.*

Proof. By Lemma 7.1.5,

$$X(F_\infty)/(\delta-1)X(F_\infty) = \mathrm{Gal}(L/F_\infty),$$

where L denotes the maximal abelian extension of H_∞ contained in $M(F_\infty)$. Recall that $\Delta = \mathrm{Gal}(F_\infty/H_\infty)$ has order 2 and we have an exact sequence

$$0 \to \mathrm{Gal}(L/F_\infty M(H_\infty)) \to \mathrm{Gal}(L/H_\infty) \to X(H_\infty) \to 0,$$

so it remains to show that $\mathrm{Gal}(L/F_\infty M(H_\infty))$ is a finitely generated $\mathbb{Z}_2$-module. We will do this by showing that $\mathrm{Gal}(L/M(H_\infty))$ is finite, so that $\mathrm{Gal}(L/F_\infty M(H_\infty))$ is also. Since L is contained in $M(F_\infty)$, the only primes which ramify in L/H_∞ are the primes of H_∞ lying above $\mathfrak{p}$ and the primes in B_∞, where B_∞ denotes the set of primes in H_∞ lying above the primes of H where E has bad reduction. But $M(H_\infty)$ is the maximal abelian extension of H_∞ unramified outside the primes above $\mathfrak{p}$, so $\mathrm{Gal}(L/M(H_\infty))$ is generated by the inertia subgroups I_v of the primes v in B_∞ inside $\mathrm{Gal}(L/H_\infty)$. Since L/F_∞ is unramified outside $\mathfrak{p}$, I_v injects into the inertia subgroup of v in $\mathrm{Gal}(F_\infty/H_\infty)$ for any v in B_∞, which is clearly finite. □

It then follows by Nakayama's Lemma that $X(F_\infty)$ is a finitely generated $\mathbb{Z}_2$-module. Given any Δ-module A, let A^+ denote the set of all $a \in A$ such that $\delta \cdot a = a$, and similarly let A^- denote the set of all $a \in A$ such that $\delta \cdot a = -a$.

Corollary 7.1.7. *Let* $p = 2$. *Then*

$$\mathrm{char}\left(X(F_\infty)^+\right) = \mathrm{char}\left(X(H_\infty)\right).$$

Proof. By Proposition 7.1.6, $\mathrm{char}\left(\mathrm{Gal}(L/H_\infty)\right) = \mathrm{char}\left(X(H_\infty)\right)$, so $\mathrm{char}\left(X(F_\infty)_\Delta\right) = \mathrm{char}\left(X(H_\infty)\right)$. The result now follows on noting that we have an exact sequence

$$0 \to X(F_\infty)^+ \to X(F_\infty) \xrightarrow{\times\delta-1} X(F_\infty) \to X(F_\infty)/(\delta-1)X(F_\infty) \to 0,$$

where the middle map is multiplication by $\delta - 1$. □

Lemma 7.1.8. $\mathrm{char}(Y(F_\infty)) = \mathrm{char}(Y_\infty)$ *for all* p, *assuming for* $p = 2$ *that* $X(F_\infty)$ *has* μ*-invariant equal to* 0 *and both* $X(F_\infty)$ *and* $X(H_\infty)$ *contain no non-zero finite* Γ*-submodules (this is automatic if* $p > 2$*).*

Proof. We will prove this for $p = 2$, and the case $p > 2$ is similar. Since the μ-invariant is zero, the 2-torsion $X(H_\infty)_2$ of $X(H_\infty)$ is zero, and $X(H_\infty)/2X(H_\infty)$ is finite. Further, $(1+\delta)X(H_\infty) = 2X(H_\infty)$, thus it follows from the snake lemma and the fact that $(X(H_\infty))_2 = 0$ that

$$Y(F_\infty)^- = X(F_\infty)^-.$$

But $X(F_\infty)/2X(F_\infty)$ and $Y(F_\infty)/2Y(F_\infty)$ are also finite because the μ-invariant of $X(F_\infty)$ is zero, and $(X(F_\infty))_2 = (Y(F_\infty))_2 = 0$, so $2X(F_\infty) \subset X(F_\infty)^+ \oplus X(F_\infty)^-$ and $\mathrm{char}(X(F_\infty)) = \mathrm{char}(X(F_\infty)^+)\mathrm{char}(X(F_\infty)^-)$. Similarly, $\mathrm{char}(Y(F_\infty)) = \mathrm{char}(Y(F_\infty)^+)\mathrm{char}(Y(F_\infty)^-)$, and thus in view of the exact sequence (7.1.1), we obtain

$$\mathrm{char}(X(F_\infty)^+) = \mathrm{char}(X(H_\infty))\mathrm{char}(Y(F_\infty)^+).$$

It follows from Corollary 7.1.7 and the fact that $X(F_\infty)$ has no non-zero finite submodule that $Y(F_\infty)^+ = 0$. Now, the snake lemma also gives an exact sequence

$$0 \to Y(F_\infty)/(\delta+1)Y(F_\infty) \to X(F_\infty)/(\delta+1)X(F_\infty) \to X(H_\infty)/2X(H_\infty) \to 0.$$

But we have $(1+\delta)Y(F_\infty) \subset Y(F_\infty)^+ = 0$ and $X(H_\infty)/2X(H_\infty)$ is finite, so

$$\mathrm{char}(Y(F_\infty)) = \mathrm{char}(X(F_\infty)/(1+\delta)X(F_\infty)).$$

The lemma now follows from Proposition 7.1.2. □

7.2 Relation to the p-part of the Birch–Swinnerton-Dyer Conjecture

In this short section, let us assume that the main conjecture for $Y(F_\infty)$ holds. Let $f_Y(T)$ denote a generator of the characteristic ideal of $X(F_\infty)^{(\rho)}$ or $(X(F_\infty)/(\delta+1)X(F_\infty))$ according as $p > 2$ or $p = 2$, as a $\Lambda(\Gamma)$-module. Then a generator of the characteristic ideal of Y_∞ is given by $f_{Y_\infty}(\chi_\mathfrak{p}(\gamma)(1+T)-1)$, where γ is the fixed topological generator of Γ. We have the Euler characteristic formula ([5, A.2]):

Lemma 7.2.1. *$(Y_\infty)_\Gamma$ is finite if and only if $f_{Y_\infty}(\chi_\mathfrak{p}(\gamma)-1) \neq 0$. If $f_{Y_\infty}(\chi_\mathfrak{p}(\gamma)-1) \neq 0$, then Y_∞^Γ is also finite, and*

$$|f_{Y_\infty}(\chi_\mathfrak{p}(\gamma)-1)|_p^{-1} = \frac{\#\left((Y_\infty)_\Gamma\right)}{\#\left(Y_\infty^\Gamma\right)}.$$

Recalling that $(Y_\infty)_\Gamma$ is dual to $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty)^{\mathfrak{H}} = \mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^\Delta$, we conclude that $f_{Y_\infty}(\chi_\mathfrak{p}(\gamma)-1) \neq 0$ if and only if $E(H)$ and $\text{Ш}(E/H)(\mathfrak{p})$ are finite.

Let us assume that Y_∞ has no non-zero finite Γ-submodule. This is automatic for $p > 2$, because Greenberg's theorem gives that $X(F_\infty)$ has no non-zero finite Γ-submodule. If $p = 2$, $X(F_\infty)$ still has no non-zero finite Γ-submodule, but it could well be that $X(F_\infty)/(\delta+1)X(F_\infty)$ does. Finally, suppose $L(\overline{\psi}_{E/H}^k, 1) \neq 0$. Under these hypotheses, we have $|f_{Y_\infty}(\chi_\mathfrak{p}(\gamma)(1+T)-1)|_p^{-1} = \#\left((Y_\infty)_\Gamma\right)$ because Y_∞^Γ must be trivial. When combined with Theorem 3.3.4 which relates $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)^\Delta$ to $\#(\text{Ш}(E/H)(\mathfrak{p})$ and Theorem 4.1.11 which relates μ_E to $L(\overline{\psi}_{E/H}^k, 1)$, we obtain the p-part of the Birch–Swinnerton-Dyer conjecture for E/H.

A Some Proofs from Chapter 2

Here we prove some results from Chapter 2. We follow the notation in Chapter 2, so that $K = \mathbb{Q}(\sqrt{-3})$, $E = X_0(27)$ and ψ is the Grössencharacter of E over K.

Lemma A.1. *A rational prime p is a special split prime if and only if it splits in K, and $\psi(\mathfrak{p}) \equiv \pm 1 \bmod 4$ for both of the primes $\mathfrak{p}$ of K above p. Moreover, $L = K(\boldsymbol{\mu}_4, \sqrt[3]{2})$.*

Proof. Put $F = K(E[4])$, and let G denote the Galois group of F over K. Since E has good reduction at 2, the action of G on $E[4]$ defines an isomorphism

$$j : G \xrightarrow{\sim} \mathrm{Aut}_{\mathcal{O}_K}(E[4]) = (\mathcal{O}_K/4\mathcal{O}_K)^{\times}.$$

In particular, it follows that $[F : K] = 12$, since 2 is inert in K. Let τ denote the unique element of G such that $j(\tau) = -1 \bmod 4\mathcal{O}_K$. Then the field $L = K(x(E[4]))$ is the fixed field of τ, so that $[L : K] = 6$. Clearly, $K(E[2]) = K(\sqrt[3]{2})$. Also by Weil pairing, we have $\boldsymbol{\mu}_4 \subset F$. We claim that $L = K(\boldsymbol{\mu}_4, \sqrt[3]{2})$. We know that $E[2] = \{\mathcal{O}, (\frac{\sqrt[3]{2}\cdot 3}{2}, 0), (\frac{\sqrt[3]{2}\cdot 3}{2}\omega, 0), (\frac{\sqrt[3]{2}\cdot 3}{2}\omega^2, 0)\}$. Using the doubling formula, we get that the x-coordinate of a point in $E[4]\backslash E[2]$ satisfies

$$\frac{x^4 + 2\cdot 3^3 x}{4x^3 - 3^3} = \frac{\sqrt[3]{2}\cdot 3}{2}.$$

Let $x = \frac{\sqrt[3]{2}\cdot 3}{2}z$, then the equation becomes

$$z^4 - 4z^3 + 8z + 4 = (z^2 - 2z - 2)^2 = 0,$$

which has roots $z = 1 \pm \sqrt{3}$ each with multiplicity 2. Hence the x-coordinate of a point in $E[4]\backslash E[2]$ is $x = \frac{\sqrt[3]{2}\cdot 3(1\pm\sqrt{3})}{2} \in K(\boldsymbol{\mu}_4, \sqrt[3]{2})$, as required. Now let p be any prime which splits in K, and let $\mathfrak{p}$ be one of the prime ideals of K above p. Then the Frobenius automorphism of K acts on $E[4]$ by multiplication by $\psi(\mathfrak{p})$, thanks to the main theorem of complex multiplication. It follows that $\mathfrak{p}$ splits completely in F if and only if $\psi(\mathfrak{p}) \equiv 1 \bmod 4$, and $\mathfrak{p}$ splits completely in L if and only if $\psi(\mathfrak{p}) \equiv \pm 1 \bmod 4$. □

Proposition A.2. *Over the field*

$$F = K\left(\sqrt[6]{\frac{27+3\sqrt{-3}}{2}}\right),$$

there exists a change of variables $x = u^2X + r$, $y = 2u^3Y$ with $u, r \in F$ which gives the following equation for E

$$Y^2 = X^3 + \frac{(9+\sqrt{-3})}{4}X^2 + \frac{13+3\sqrt{-3}}{8}X + \frac{2+\sqrt{-3}}{8}$$

which has good reduction at 3. *Here, $u = \frac{\sqrt{\alpha}}{\beta^2}$ where $\alpha = \frac{27+3\sqrt{-3}}{2}$, $\beta = \sqrt[3]{\frac{1-3\sqrt{-3}}{2}}$ and $r = -\frac{3}{2}\sqrt[3]{\frac{-13-3\sqrt{-3}}{2}}$.*

Proof. Note that for our curve, the smallest split prime is 7. So one should try to find an explicit equation for the curve E over the field $F = K(E[2+\sqrt{-3}])$ having good reduction at 3 (see [7, Theorem 2]). The conductor of F over K is $(3(2+\sqrt{-3}))$, since the conductor of the Grössencharacter of E/K is $3\mathcal{O}_K$. Furthermore, F/K is an abelian extension of degree 6 and the group $\mu_6 \subset K$. Thus, by Kummer theory, we must have $F = K(\sqrt[6]{\alpha})$, for some $\alpha \in K^*$. The only primes of K which can ramify in F are those dividing 7, 3 and w, so the Kummer generator α must be of the form $(2+\sqrt{-3})^a \cdot (\omega - 1)^b \cdot (-\omega)^c$ where $a, b, c \in \{0, \ldots, 5\}$. Recall from the theory of complex multiplication that for a prime ideal $\mathfrak{p}$ of K prime to 3, we have $\psi_{E/K}(\mathfrak{p}) = \pi$ where π is the unique generator of $\mathfrak{p}$ which is 1 mod $3\mathcal{O}_K$. Now, suppose in addition that $\mathfrak{p}$ is prime to 7. Then F/K is unramified at $\mathfrak{p}$ so

$$\mathrm{Frob}_{\mathfrak{p}} = \psi_{E/K}(\mathfrak{p}).$$

If we pick a prime $\mathfrak{p} = (\pi)$ such that $\pi \equiv 1 \bmod 3\mathcal{O}_K$ and $\pi \equiv 1 \bmod (2+\sqrt{-3})\mathcal{O}_K$, then we have

$$(P)^{\mathrm{Frob}_{\mathfrak{p}}} = \psi_{E/K}(\mathfrak{p})(P) = \pi(P) = P$$

for $P \in E[2+\sqrt{-3}]$, since $\pi \equiv 1 \bmod (2+\sqrt{-3})\mathcal{O}_K$. So $\psi_{E/K}(\mathfrak{p})$ is the identity in the extension $K(E[2+\sqrt{-3}])/K$. On the other hand, $K(E[2+\sqrt{-3}]) = K(\sqrt[6]{\alpha})$ and we know that

$$(\sqrt[6]{\alpha})^{\mathrm{Frob}_{\mathfrak{p}}} \equiv (\sqrt[6]{\alpha})^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{p},$$

so for $\mathrm{Frob}_{\mathfrak{p}}$ to be the identity, it is necessary that

$$(\sqrt[6]{\alpha})^{\mathrm{N}(\mathfrak{p})} \equiv \sqrt[6]{\alpha} \bmod \mathfrak{p}.$$

We eliminate the possibilities for (a, b, c) by trying out some examples.

Example A.3. Let $\pi = 13 + 6\sqrt{-3}$ and $\mathfrak{p} = (\pi)$. Then $\pi \equiv 1 \bmod 3\mathcal{O}_K$, $\pi \equiv 1 \bmod (2+\sqrt{-3})\mathcal{O}_K$ and $\mathrm{N}(\mathfrak{p}) = 277$. So $(\sqrt[6]{\alpha})^{\mathrm{Frob}_\mathfrak{p}} \equiv (\sqrt[6]{\alpha})^{277} \equiv (\sqrt[6]{\alpha})\alpha^{46}$. Thus, for $\mathrm{Frob}_\mathfrak{p}$ to be the identity, we need

$$\alpha^{46} \equiv \left(2+\sqrt{-3}\right)^{46a}\left(\frac{-3+\sqrt{-3}}{2}\right)^{46b}\left(\frac{1-\sqrt{-3}}{2}\right)^{46c} \equiv 1 \bmod \mathfrak{p}.$$

But $13 + 6\sqrt{-3} \equiv 0 \bmod \mathfrak{p}$ so we can replace $\sqrt{-3}$ with $\frac{-13}{6}$ and now that we have rational numbers, we can replace mod $\mathfrak{p}$ with mod $\mathrm{N}(\mathfrak{p})$. Hence the equation becomes

$$\left(2-\frac{13}{6}\right)^{46a}\left(\frac{-3-\frac{13}{6}}{2}\right)^{46b}\left(\frac{1+\frac{13}{6}}{2}\right)^{46c} \equiv 1 \bmod 277.$$

Also, $6^{-1} \equiv -46 \bmod 277$ and $2^{-1} \equiv 139 \bmod 277$, so

$$(2+46\cdot 13)^{46a}\,(139(-3+46\cdot 13)^{46b}\,(139(1-46\cdot 13))^{46c} \equiv 1 \bmod 277,$$

that is,

$$117^a \cdot 276^b \cdot 160^c \equiv 1 \bmod 277. \tag{A.1}$$

Example A.4. Let $\pi = 1 + \frac{1+\sqrt{-3}}{2}\cdot 3(2+\sqrt{-3}) = \frac{5+9\sqrt{-3}}{2}$. Then $\pi \equiv 1 \bmod 3\mathcal{O}_K$, $\pi \equiv 1 \bmod (2+\sqrt{-3})\mathcal{O}_K$ and $\mathrm{N}(\mathfrak{p}) = 67$. So $(\sqrt[6]{\alpha})^{\mathrm{Frob}_\mathfrak{p}} \equiv (\sqrt[6]{\alpha})^{67} \equiv (\sqrt[6]{\alpha})\alpha^{11}$. Hence for $\mathrm{Frob}_\mathfrak{p}$ to be the identity, we need

$$\alpha^{11} \equiv \left(2+\sqrt{-3}\right)^{11a}\left(\frac{-3+\sqrt{-3}}{2}\right)^{11b}\left(\frac{1-\sqrt{-3}}{2}\right)^{11c} \equiv 1 \bmod \mathfrak{p}.$$

But we now have $\sqrt{-3} \equiv \frac{5}{9} \bmod \mathfrak{p}$, $9^{-1} \equiv 15 \bmod 67$ and $2^{-1} \equiv 34 \bmod 67$ so the equation becomes

$$(2+15\cdot 5)^{11a}(34(-3+15\cdot 5))^{11b}(34(1-15\cdot 5))^{11c} \equiv 1 \bmod 67$$

that is,

$$29^a \cdot 37^b \cdot 38^c \equiv 1 \bmod 67. \tag{A.2}$$

Comparing the solutions to (A.1) and (A.2) in Examples A.3 and A.4, we find that the common solutions are $(a, b, c) = (0, 0, 0), (1, 3, 2), (2, 0, 4), (3, 3, 0), (4, 0, 2)$ and $(5, 3, 4)$. However, we know that F/K is a degree 6 extension, so the only possibilities are

$(a, b, c) = (1, 3, 2)$ and $(5, 3, 4)$. But $\frac{(2+\sqrt{-3})(\omega-1)(-\omega)}{\sqrt[6]{(2+\sqrt{-3})^5(\omega-1)^3(-\omega)^4}} = \sqrt[6]{(2+\sqrt{-3})(\omega-1)^3(-\omega)^2}$, so the corresponding fields are the same. Hence

$$\begin{aligned} K(E[2+\sqrt{-3}]) &= K\left(\sqrt[6]{(2+\sqrt{-3})(\omega-1)^3(-\omega)^2}\right) \\ &= K\left(\sqrt[6]{\frac{27+3\sqrt{-3}}{2}}\right). \end{aligned}$$

Let $E : y^2 = 4x^3 - 3^3$ and $x = u^2X + r$, $y = u^3Y$. Then in terms of X, Y, we have

$$u^6Y^2 = 4u^6X^3 + 12u^4rX^2 + 12u^2r^2X + 4r^3 - 3^3$$

and $\operatorname{ord}_3\left(\sqrt[6]{\frac{27+3\sqrt{-3}}{2}}\right) = \frac{1}{4}$, so $\operatorname{ord}_3\left(\sqrt{\frac{27+3\sqrt{-3}}{2}}\right) = \frac{3}{4}$. We also have $\sqrt[3]{\alpha} = \sqrt[3]{2+\sqrt{-3}} \cdot \frac{-3+\sqrt{-3}}{2} \cdot \sqrt[3]{\left(\frac{1-\sqrt{-3}}{2}\right)^2} \in F$, so $\beta = \sqrt[3]{(2+\sqrt{-3}) \cdot \left(\frac{1-\sqrt{-3}}{2}\right)^2} = \sqrt[3]{\frac{1-3\sqrt{-3}}{2}} \in F$, so let $u = \frac{\sqrt{\alpha}}{\beta^2}$. Then $\operatorname{ord}_3(u) = \frac{3}{4}$ and $\operatorname{ord}_7(u) = -\frac{1}{12}$. If we divide the equation through by u^6, one can easily check that the discriminant of this curve is $u^{-12}\operatorname{disc}(E)$, so it is a 3-adic unit and is integral at 7. To make sure the coefficients of

$$Y^2 = 4X^3 + \frac{12r}{u^2}X^2 + \frac{12r^2}{u^4}X + \frac{4r^3 - 3^3}{u^6}$$

are integral at 3, it is sufficient that $\operatorname{ord}_3(4r^2 - 3^3) \geqslant \operatorname{ord}_3(u^6) = \frac{9}{2}$. So we need $r = 3s$ for some $s \in F$ and $\operatorname{ord}(4r^2 - 3^3) = \operatorname{ord}_3(3^3(4s^3 - 1)) \geqslant \frac{9}{2}$, so $\operatorname{ord}_3(4s^3 - 1) \geqslant \frac{3}{2}$. Now, let

$$\begin{aligned} s = -\frac{\beta^2}{2} &= -\frac{1}{2}\sqrt[3]{(2+\sqrt{-3})^2\left(\frac{1-\sqrt{-3}}{2}\right)^4} \\ &= -\frac{1}{2}\sqrt[3]{\frac{-13-3\sqrt{-3}}{2}}. \end{aligned}$$

Then

$$4s^3 - 1 = \frac{13+3\sqrt{-3}}{4} - 1 = \frac{9+3\sqrt{-3}}{4}$$

so $\operatorname{ord}_3(4s^3 - 1) = \frac{3}{2}$, as required. Now, $r = 3s = -\frac{3\beta^2}{2}$ and $u = \frac{\sqrt{\alpha}}{\beta^2}$, so

$$Y^2 = 4X^3 - \frac{18\beta^6}{\alpha}X^2 + \frac{27\beta^{12}}{\alpha^2} - \frac{27\beta^{12}(\beta^6 + 2)}{2\alpha^3}.$$

So substituting the values for α and β, we obtain an equation with coefficients in K:

$$Y^2 = 4X^3 + (9+\sqrt{-3})X^2 + \frac{13+3\sqrt{-3}}{2}X + \frac{2+\sqrt{-3}}{2}.$$

□

Corollary A.5. *For any character $\chi : (\mathbb{Z}/3\mathbb{Z})^n \to \mathbb{C}^\times$, we have*

$$\mathrm{ord}_3(\Phi_{D^2}^{(\chi)}) \geqslant n + \frac{1}{4}.$$

Proof. We will assume for simplicity that D is a prime power since we only use this Corollary in the case $n=1$. The proof for the case $n \geqslant 1$ is similar. Pick $\beta \in \mathcal{O}_K$ be such that $(1-\omega)\beta \equiv 1 \bmod D$. Let $\mathcal{C}$ be a set of elements of $\mathcal{O}_K$ such that $c \bmod D$ runs over $(\mathcal{O}_K/D\mathcal{O}_K)^\times$ precisely once and $\mathcal{C}$ can be written as a union of sets $\mathcal{C} = \bigcup_{i\in\{0,1,2\}} \omega^i\mathcal{H} \bigcup_{i\in\{0,1,2\}} \omega^i(1-\omega)\mathcal{H} \bigcup_{i\in\{0,1,2\}} \omega^i\beta\mathcal{H}$ for some set $\mathcal{H}$. This is possible since 3 and D are coprime and 9 divides the order of $1-\omega$ in $(\mathcal{O}_K/D\mathcal{O}_K)^\times$ by assumption. We will follow the notation in the proof of Lemma 2.3.11. Given $c \in V^{(\chi)}$, let P be the point on $E : y^2 = 4x^3 - 3^3$ given by $x(P) = \wp\left(\frac{c\Omega}{D}, \mathcal{L}\right), y(P) = \wp'\left(\frac{c\Omega}{D}, \mathcal{L}\right)$. Similarly let Q and R be the points given by $(x(Q), y(Q)) = \left(\wp\left(\frac{(1-\omega)c\Omega}{D}, \mathcal{L}\right), \wp'\left(\frac{(1-\omega)c\Omega}{D}, \mathcal{L}\right)\right)$ and $(x(R), y(R)) = \left(\wp\left(\frac{\beta c\Omega}{D}, \mathcal{L}\right), \wp'\left(\frac{\beta c\Omega}{D}, \mathcal{L}\right)\right)$ respectively, and define

$$\mathscr{M}(c, D) = \frac{9 - y(P)}{3 - x(P)}.$$

We can write $V^{(\chi)}$ as a union of sets

$$V^{(\chi)} = \bigcup_{i\in\{0,1,2\}} \omega^i H \bigcup_{i\in\{0,1,2\}} \omega^i(1-\omega)H \bigcup_{i\in\{0,1,2\}} \omega^i\beta H$$

for some set H, since $\left(\frac{1-\omega}{D}\right)_3 = \left(\frac{\beta}{D}\right)_3 = 1$. We wish to find $\mathrm{ord}_3\left(\sum_{c\in V^{(\chi)}} \mathscr{M}(c, D)\right)$. Recall that E has complex multiplication by ω via $\omega(x,y) = (\omega x, y)$, so $\wp'\left(\frac{\omega^i c\Omega}{D}, \mathcal{L}\right) = \wp'\left(\frac{c\Omega}{D}, \mathcal{L}\right)$. Moreover, $\mathcal{L} = \omega\mathcal{L}$ so $\wp\left(\frac{\omega^i c\Omega}{D}, \mathcal{L}\right) = \wp\left(\frac{\omega^i c\Omega}{D}, \omega^i\Lambda\right)$ for $i = 0, 1, 2$ and $\wp$ is homogeneous of degree -2 so

$$\sum_{i\in\{0,1,2\}} \frac{9-\wp'\left(\frac{w^i c\Omega}{D},\mathcal{L}\right)}{3-\wp\left(\frac{\omega^i c\Omega}{D},\mathcal{L}\right)} = \frac{9-\wp'\left(\frac{c\Omega}{D},\mathcal{L}\right)}{3-\wp\left(\frac{c\Omega}{D},\mathcal{L}\right)} + \frac{9-\wp'\left(\frac{c\Omega}{D},\mathcal{L}\right)}{3-\omega\wp\left(\frac{c\Omega}{D},\mathcal{L}\right)} + \frac{9-\wp'\left(\frac{c\Omega}{D},\mathcal{L}\right)}{3-\omega^2\wp\left(\frac{c\Omega}{D},\mathcal{L}\right)}$$
$$= \frac{3^5-3^3y(P)}{27-x(P)^3}.$$

Furthermore, using the addition formula

$$\wp(z_1+z_2,\mathcal{L}) = -\wp(z_1,\mathcal{L})-\wp(z_2,\mathcal{L})+\frac{1}{4}\left(\frac{\wp'(z_1,\mathcal{L})-\wp'(z_2,\mathcal{L})}{\wp(z_1,\mathcal{L})-\wp(z_2,\mathcal{L})}\right)^2,$$

and noting $\wp(z,\mathcal{L})$ is even and $\wp'(z,\mathcal{L})$ is odd, we get

$$\wp\left(\frac{(1-\omega)c\Omega}{D},\mathcal{L}\right) = -\wp\left(\frac{c\Omega}{D},\mathcal{L}\right)-\wp\left(\frac{-\omega c\Omega}{D},\mathcal{L}\right)+\frac{1}{4}\left(\frac{\wp'(\frac{c\Omega}{D},\mathcal{L})-\wp'(\frac{-\omega c\Omega}{D},\mathcal{L})}{\wp\left(\frac{c\Omega}{D},\mathcal{L}\right)-\wp\left(\frac{-\omega c\Omega}{D},\mathcal{L}\right)}\right)^2$$
$$= -(1+\omega)x(P)+\left(\frac{y(P)}{(1-\omega)x(P)}\right)^2.$$

Also, $\beta-\omega\beta\equiv 1 \bmod D_a$ so

$$\wp\left(\frac{c\Omega}{D},\mathcal{L}\right) = -\wp\left(\frac{\beta c\Omega}{D},\mathcal{L}\right)-\wp\left(\frac{-\omega\beta c\Omega}{D},\mathcal{L}\right)+\frac{1}{4}\left(\frac{\wp'(\frac{\beta c\Omega}{D},\mathcal{L})-\wp'(\frac{-\omega\beta c\Omega}{D},\mathcal{L})}{\wp(\frac{\beta c\Omega}{D},\mathcal{L})-\wp(\frac{-\omega\beta c\Omega}{D},\mathcal{L})}\right)^2$$
$$= -(1+\omega)x(R)+\left(\frac{y(R)}{(1-\omega)x(R)}\right)^2.$$

Therefore,

$$\sum_{c\in V^{(x)}}\mathscr{M}(c,D) = \sum_{c\in H}\sum_{i\in\{0,1,2\}} \frac{9-\wp'\left(\frac{w^i c\Omega}{D},\mathcal{L}\right)}{3-\wp\left(\frac{\omega^i c\Omega}{D},\mathcal{L}\right)} + \frac{9-\wp'\left(\frac{\omega^i(1-\omega)c\Omega}{D},\mathcal{L}\right)}{3-\wp\left(\frac{\omega^i(1-\omega)c\Omega}{D},\mathcal{L}\right)} + \frac{9-\wp'\left(\frac{w^i\beta c\Omega}{D},\mathcal{L}\right)}{3-\wp\left(\frac{\omega^i\beta c\Omega}{D},\mathcal{L}\right)},$$

and this is equal to

$$\sum_{c\in H}\frac{3^5-3^3y(P)}{27-x(P)^3}+\frac{3^5-3^3y(Q)}{27-\left(\omega^2x(P)+\left(\frac{y(P)}{(1-\omega)x(P)}\right)^2\right)^3}+\frac{3^5-3^3y(R)}{27-\left(\omega x(P)-\omega\left(\frac{y(R)}{(1-\omega)x(R)}\right)^2\right)^3}. \tag{A.3}$$

To determine $\operatorname{ord}_3\left(\frac{y(P)}{(1-\omega)x(P)}\right)$, recall from Proposition A.2 that the change of variables $x=u^2X+r$, $y=2u^3Y$ where $r=-\frac{3}{2}\sqrt[3]{\frac{-13-3\sqrt{-3}}{2}}$ gives us a model of E

having good reduction at 3. In terms of X and Y, we have

$$\frac{y(P)}{(1-\omega)x(P)} = \frac{u^3Y(P)}{(1-\omega)(u^2X(P)+r)}.$$

Now, P is a torsion of point of E of order prime to 3 and E has good reduction at 3 so $\mathrm{ord}_3(X(P)), \mathrm{ord}_3(Y(P)) \geqslant 0$. Also $\mathrm{ord}_3(u) = \frac{3}{4}$, and $\mathrm{ord}_3(r) = 1$ so

$$\mathrm{ord}_3\left(\frac{y(P)}{(1-\omega)x(P)}\right) = \frac{3}{4} + \mathrm{ord}_3(Y(P)).$$

If $\mathrm{ord}_3(Y(P)) > 0$, P reduces to a 2-torsion after reduction modulo 3, but P is a D-torsion and reduction modulo 3 is injective, hence we must have $\mathrm{ord}_3(Y(P)) = 0$. Similarly $\mathrm{ord}_3\left(\frac{y(R)}{(1-\omega)x(R)}\right) = \frac{3}{4}$. We also showed in the proof of Corollary 2.3.7 that $\mathrm{ord}_3(27 - x(P)^3) = 4$, so when we add the three terms in equation (A.3), the product of the denominators has 3-adic valuation 12. The numerator is of the form

$$\left(27 - x(P)^3\right)^2\left(3^6 - 3^3(y(P)+y(Q)+y(R))\right) + \left(\text{terms of 3-adic valuation} \geqslant \frac{27}{2}\right),$$

and $\mathrm{ord}_3(y(P)) = \frac{9}{4}$, so

$$\mathrm{ord}_3\left(\sum_{c\in V^{(x)}} \mathscr{M}(c,D)\right) \geqslant \left(8 + \frac{21}{4}\right) - 12 = \frac{5}{4}.$$

On the other hand, by the proof of Lemma 2.3.11, we have $9 \mid \#(V^{(x)})$. Thus,

$$\begin{aligned}\mathrm{ord}_3\left(\sum_{c\in V^{(x)}} \mathcal{E}_1^*\left(\frac{c\Omega}{D} + \frac{\Omega}{3}, \mathcal{L}\right)\right) &\geqslant \min\left(\mathrm{ord}_3\left(\frac{1}{2}\sum_{c\in V^{(x)}} \mathscr{M}(c,D)\right), \mathrm{ord}_3(\#(V^{(x)}))\right)\\ &\geqslant \frac{5}{4}\end{aligned}$$

as required. □

B Numerical Examples

The following examples are computed using Magma.

Quadratic Twists

Let $E(D^3): y^2 = 4x^3 - 3^3D^3$, $\omega = e^{\frac{2\pi i}{3}}$. In what follows, π denotes a prime of K congruent to 1 modulo 12. In particular, $D = \mathrm{N}\pi$ is a special split prime defined in Definition 2.2.3. We order $\pi = a + b\omega$, $a, b \in \mathbb{Z}$,by $|a|$ and then by $|b|$.

$\pi = a + b\omega$	$D = \mathrm{N}\pi$	$L^{(\mathrm{alg})}(E(D^3), 1)$
$13 + 12\omega$	157	$12 = 2^2 \cdot 3$
$13 + 24\omega$	433	$48 = 2^4 \cdot 3$
$-23 - 12\omega$	397	0
$-23 - 36\omega$	997	0
$25 + 24\omega$	601	$48 = 2^4 \cdot 3$
$25 + 36\omega$	1021	$12 = 2^2 \cdot 3$
$37 + 60\omega$	2749	$12 = 2^2 \cdot 3$
$37 + 72\omega$	3889	0
$37 + 12\omega$	1069	$12 = 2^2 \cdot 3$
$47 + 12\omega$	1789	$12 = 2^2 \cdot 3$
$47 + 24\omega$	1657	$12 = 2^2 \cdot 3$
$49 + 24\omega$	1801	$12 = 2^2 \cdot 3$
$49 + 36\omega$	1933	$48 = 2^4 \cdot 3$
$49 + 60\omega$	3061	$12 = 2^2 \cdot 3$
$49 + 72\omega$	4057	$48 = 2^4 \cdot 3$
$-59 - 12\omega$	2917	0
$-59 - 48\omega$	2953	$12 = 2^2 \cdot 3$
$-59 - 60\omega$	3541	$12 = 2^2 \cdot 3$
$-59 - 84\omega$	5581	$48 = 2^4 \cdot 3$
$61 + 24\omega$	2833	$108 = 2^2 \cdot 3^3$
$61 + 72\omega$	4513	$108 = 2^2 \cdot 3^3$
$61 + 84\omega$	5653	$12 = 2^2 \cdot 3$
$-71 - 132\omega$	13093	$12 = 2^2 \cdot 3$
$73 + 96\omega$	7537	$108 = 2^2 \cdot 3^3$
$73 + 108\omega$	9109	$48 = 2^4 \cdot 3$
$-83 - 120\omega$	11329	$59 = 2^4 \cdot 3$
$85 + 156\omega$	18301	0

$\pi = a + b\omega$	$D = \mathrm{N}\pi$	$L^{(\mathrm{alg})}(E(D^3), 1)$
$85 + 168\omega$	21169	$192 = 2^6 \cdot 3$
$-95 - 156\omega$	18541	0
$-71 - 72\omega$	5113	0
$-71 - 84\omega$	6133	$108 = 2^2 \cdot 3^3$
$73 + 12\omega$	4597	0
$73 + 24\omega$	4153	$12 = 2^2 \cdot 3$
$73 + 48\omega$	4129	$12 = 2^2 \cdot 3$
$73 + 60\omega$	4549	$48 = 2^4 \cdot 3$
$83 + 12\omega$	6037	$12 = 2^2 \cdot 3$
$-83 - 36\omega$	5197	$48 = 2^4 \cdot 3$
$-83 - 48\omega$	5209	$12 = 2^2 \cdot 3$
$85 + 48\omega$	5449	$192 = 2^6 \cdot 3$
$-95 - 24\omega$	7321	0
$-95 - 72\omega$	7369	0
$-95 - 84\omega$	8101	0
$-95 - 108\omega$	10429	$12 = 2^2 \cdot 3$
$97 + 36\omega$	7213	$12 = 2^2 \cdot 3$
$97 + 48\omega$	7057	$108 = 2^2 \cdot 3^3$
$97 + 84\omega$	8317	$12 = 2^2 \cdot 3$
$97 + 108\omega$	10597	$12 = 2^2 \cdot 3$
$97 + 132\omega$	14029	$12 = 2^2 \cdot 3$
$-107 - 60\omega$	8629	$48 = 2^4 \cdot 3$
$-107 - 72\omega$	8929	$48 = 2^4 \cdot 3$
$107 + 120\omega$	13009	$48 = 2^4 \cdot 3$
$109 + 60\omega$	8941	$12 = 2^2 \cdot 3$
$109 + 84\omega$	9781	$48 = 2^4 \cdot 3$
$109 + 144\omega$	16921	0
$109 + 156\omega$	19213	$108 = 2^2 \cdot 3^3$
$-119 - 96\omega$	11953	0
$-119 - 108\omega$	12973	$48 = 2^4 \cdot 3$
$-119 - 120\omega$	14281	$48 = 2^4 \cdot 3$
$-119 - 132\omega$	15877	$108 = 2^2 \cdot 3^3$
$-119 - 144\omega$	17761	$108 = 2^2 \cdot 3^3$
$121 + 72\omega$	11113	$12 = 2^2 \cdot 3$
$121 + 96\omega$	12241	0

$\pi = a + b\omega$	$D = \mathrm{N}\pi$	$L^{(\mathrm{alg})}(E(D^3), 1)$
$121 + 156\omega$	20101	$48 = 2^4 \cdot 3$
$121 + 180\omega$	25261	$108 = 2^2 \cdot 3^3$
$-131 - 132\omega$	17293	$12 = 2^2 \cdot 3$
$-131 - 156\omega$	21061	$12 = 2^2 \cdot 3$
$-131 - 180\omega$	25981	$108 = 2^2 \cdot 3^3$
$133 + 144\omega$	19273	$48 = 2^4 \cdot 3$
$133 + 156\omega$	21277	0
$-143 - 144\omega$	20593	$48 = 2^4 \cdot 3$
$-143 - 180\omega$	27109	$12 = 2^2 \cdot 3$
$145 + 132\omega$	19309	$108 = 2^2 \cdot 3^3$
$145 + 156\omega$	22741	0
$145 + 168\omega$	24889	$48 = 2^4 \cdot 3$
$-155 - 144\omega$	22441	$12 = 2^2 \cdot 3$
$-155 - 156\omega$	24181	$108 = 2^2 \cdot 3^3$
$-155 - 168\omega$	26209	$12 = 2^2 \cdot 3$
$157 + 144\omega$	22777	$300 = 2^2 \cdot 3 \cdot 5$
$157 + 168\omega$	26497	0
$157 + 180\omega$	28789	$12 = 2^2 \cdot 3$
$-167 - 168\omega$	28057	$300 = 2^2 \cdot 3 \cdot 5$

The following is a small sample of D divisible by two relatively small (due to computational complexity) distinct special split primes.

D	$L^{(\mathrm{alg})}(E(D^3), 1)$
$157 \cdot 601$	0
$601 \cdot 1021$	0
$157 \cdot 1021$	$192 = 2^6 \cdot 3$
$157 \cdot 1789$	0
$1021 \cdot 1789$	$1200 = 2^4 \cdot 3 \cdot 5^2$

Cubic Twists

Let $E(D^2) : y^2 = 4x^3 - 3^3 D^3$, $\omega = e^{\frac{2\pi i}{2}}$. Let D be an odd, cube-free integer such that $D \equiv 1 \bmod 9$ and D is a product of prime numbers congruent to 1 modulo 3. We first list examples where D is a prime number, $D = \mathrm{N}\pi$ and π is a prime of K. We order π by $|a|$ and then by $|b|$.

$\pi = a + b\omega$	$D = \mathrm{N}\pi$	$L^{(\mathrm{alg})}(E(D^2), 1)$
$1 + 9\omega$	73	$9 = 3^2$
$1 + 18\omega$	307	$9 = 3^2$
$1 - 27\omega$	757	$27 = 3^3$
$1 + 81\omega$	6481	$27 = 3^3$
$4 + 15\omega$	181	$9 = 3^2$
$7 + 12\omega$	109	$9 = 3^2$
$7 + 30\omega$	739	$36 = 2^2 \cdot 3^2$
$7 + 39\omega$	1297	$9 = 3^2$
$7 + 48\omega$	2017	$9 = 3^2$
$13 + 6\omega$	127	0
$13 + 15\omega$	199	$9 = 3^2$
$13 + 24\omega$	433	0
$16 + 39\omega$	1153	$9 = 3^2$
$16 + 57\omega$	2593	$36 = 2^2 \cdot 3^2$
$19 + 27\omega$	577	$9 = 3^2$
$19 + 54\omega$	2251	$36 = 2^2 \cdot 3^2$
$22 + 15\omega$	379	0
$25 + 21\omega$	541	$9 = 3^2$
$25 + 39\omega$	1171	0
$28 + 9\omega$	613	$9 = 3^2$
$28 + 45\omega$	1549	$9 = 3^2$
$31 + 6\omega$	811	$9 = 3^2$
$31 + 42\omega$	1423	$9 = 3^2$
$34 + 3\omega$	1063	0
$34 + 21\omega$	883	0
$34 + 57\omega$	2467	$36 = 2^2 \cdot 3^2$
$37 + 9\omega$	1117	$9 = 3^2$
$37 + 54\omega$	2287	$9 = 3^2$
$40 + 51\omega$	2161	$9 = 3^2$
$43 + 30\omega$	1459	0
$43 + 39\omega$	1693	$9 = 3^2$
$43 + 48\omega$	2089	0
$43 + 57\omega$	2647	0

$\pi = a + b\omega$	$D = \mathrm{N}\pi$	$L^{(\mathrm{alg})}(E(D^2), 1)$
$46 + 9\omega$	1783	$9 = 3^2$
$49 + 6\omega$	2143	$9 = 3^2$
$49 + 24\omega$	1801	0
$49 + 33\omega$	1873	$36 = 2^2 \cdot 3^2$
$49 + 51\omega$	2503	$9 = 3^2$
$49 + 60\omega$	3061	$9 = 3^2$
$52 + 21\omega$	2053	$9 = 3^2$
$-53 + 27\omega$	4969	$27 = 3^3$
$-53 - 135\omega$	13879	$9 = 3^2$
$55 + 27\omega$	2269	0
$55 + 36\omega$	2341	$36 = 2^2 \cdot 3^2$
$55 + 54\omega$	2971	$36 = 2^2 \cdot 3^2$
$58 + 15\omega$	2719	$9 = 3^2$
$58 + 33\omega$	2539	0
$-80 - 27\omega$	4969	$27 = 3^3$
$-80 - 81\omega$	6481	$27 = 3^3$
$82 - 81\omega$	19927	$243 = 3^5$
$82 + 135\omega$	13879	$9 = 3^2$
$-107 + 54\omega$	20143	$27 = 3^3$
$-107 + 135\omega$	44119	$27 = 3^3$
$109 - 81\omega$	27271	$27 = 3^3$
$136 - 81\omega$	36073	$27 = 3^3$

We list some examples where D is divisible by at least two primes which are not necessarily distinct. Again, D is an odd, cube-free integer such that $D \equiv 1 \bmod 9$ and D is a product of prime numbers congruent to 1 modulo 3.

D	$L^{(\mathrm{alg})}(E(D^2), 1)$
19^2	$9 = 3^2$
37^2	$9 = 3^2$
163^2	$9 = 3^2$
631^2	$9 = 3^2$
$7 \cdot 211$	$27 = 3^3$
$7 \cdot 2551$	$108 = 2^2 \cdot 3^3$
$7 \cdot 1381$	$27 = 3^3$

D	$L^{(\mathrm{alg})}(E(D^2),1)$
$7 \cdot 3037$	$27 = 3^3$
$19 \cdot 37$	$27 = 3^3$
$37 \cdot 163$	$27 = 3^3$
$7 \cdot 13 \cdot 19$	0
$7 \cdot 13 \cdot 19 \cdot 37$	0
$7 \cdot 13 \cdot 31 \cdot 61$	0
$109 \cdot 307$	$27 = 3^3$
$19^2 \cdot 163$	$27 = 3^3$
$19 \cdot 163^2$	$27 = 3^3$
$19 \cdot 37 \cdot 163$	0
$19^2 \cdot 37 \cdot 163$	$81 = 3^4$
$19^2 \cdot 37^2 \cdot 163$	0
$19 \cdot 37 \cdot 163^2$	$81 = 3^4$
$19 \cdot 37^2 \cdot 163^2$	0
$19^2 \cdot 37 \cdot 163^2$	$729 = 3^6$
$19^2 \cdot 37^2 \cdot 163^2$	$2916 = 2^2 \cdot 3^4$
$7 \cdot 139$	0
$79 \cdot 139$	0
$7^2 \cdot 37^2$	$27 = 3^3$
$19^2 \cdot 37^2$	$27 = 3^3$
$37^2 \cdot 163^2$	$108 = 2^2 \cdot 3^3$
$7^2 \cdot 13^2 \cdot 19^2$	$81 = 3^4$
$7^2 \cdot 13^2 \cdot 19^2 \cdot 37^2$	$972 = 2^2 \cdot 3^5$
127^2	$9 = 3^2$
157^2	0
229^2	0
307^2	$36 = 2^2 \cdot 3^2$
397^2	$144 = 2^4 \cdot 3^2$
691^2	0
$127^2 \cdot 307^2$	$432 = 2^4 \cdot 3^3$
$127 \cdot 307^2$	$54864 = 2^4 \cdot 3^3 \cdot 127$
$127^2 \cdot 307$	$8289 = 3^3 \cdot 307$
$127 \cdot 307$	0
$127^2 \cdot 397^2$	$27 = 3^3$
$307^2 \cdot 397^2$	$2187 = 3^7$

References

[1] Cassels, J. and Fröhlich, A. (2010). *Algebraic Number Theory.* London Math. Soc, second edition.

[2] Coates, J. (1983). Infinite descent on elliptic curves with complex multiplication. *Arithmetic and Geometry - Papers dedicated to I. R. Shafarevich, Progress in Math.*, 35:107–136.

[3] Coates, J. (1991). Elliptic curves with complex multiplication and iwasawa theory. *Bull. London Math. Soc.*, 23:321–350.

[4] Coates, J. and Goldstein, C. (1983). Some remarks on the main conjecture for elliptic curves with complex multiplication. *American Journal of Mathematics*, 105:337–366.

[5] Coates, J. and Sujatha, R. (2006). *Cyclotomic Fields and Zeta Values.* Springer, first edition.

[6] Coates, J. and Wiles, A. (1977a). Kummer's criterion for hurwitz numbers. *Japan Soc. for the Promotion of Science*, pages 9–23.

[7] Coates, J. and Wiles, A. (1977b). On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39:223–251.

[8] de Shalit, E. (1987). *Iwasawa Theory of Elliptic Curves with Complex Multiplication*, volume 3 of *Perspectives in Math.* Academic Press.

[9] Faltings, G. (1983). Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Invent. Math.*, 73:349–366.

[10] Goldstein, C. and Schappacher, N. (1981). Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe. *J. Reine Angew. Math.*, 327:184–218.

[11] Gonzalez-Aviles, C. (1994). *On the "2-part" of the Birch–Swinnerton-Dyer conjecture for elliptic curves with complex multiplication.* PhD thesis, Graduate School of The Ohio State University.

[12] Gross, B. and Zagier, D. (1986). Heegner points and derivatives of L-series. *Invent. Math.*, pages 225–320.

[13] Gross, B. H. (1980). Arithmetic on elliptic curves with complex multiplication. *Lecture Notes in Math.*, 776. Springer-Verlag.

[14] Gross, B. H. (1982). Minimal models for elliptic curves with complex multiplication. *Compositio Mathematica*, 45:155–164.

[15] Kolyvagin, V. A. (1988). Finiteness of e(q) and sh(e,q) for a subclass of weil curves. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 52 (3):522–540, 670–671.

[16] Perrin-Riou, B. (1984). Arithmétique des courbes elliptiques et théorie d'iwasawa. *Mémoires de la S.M.E. 2e série*, 17:1–130.

[17] Rubin, K. (1991). The "main conjectures" of iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103:25–68.

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

[19] Shimura, G. (1971). *Introduction to the arithmetic of automorphic functions.* Princeton University Press.

[20] Silverman, J. (2009). *The Arithmetic of Elliptic Curves.* Springer, second edition.

[21] Stephens, N. M. (1968). The diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 231:121–162.

[22] Tate, J. (1975). Algorithm for determining the type of a singular fiber in an elliptic pencil. *Modular Functions of One Variable IV, Lecture Notes in Math.*, 476:33–52. Springer.

[23] Washington, L. (1982). *Introduction to Cyclotomic Fields*, volume 83. Springer.

[24] Zhao, C. (2001). A criterion for elliptic curves with second lowest 2-power in l(1). *Math. Proc. Camb. Phil. Soc*, 131:385–404.

[25] Zhao, C. (2003). A criterion for elliptic curves with second lowest 2-power in l(1) (ii). *Math. Proc. Camb. Phil. Soc*, 134:407–420.