The Birch and Swinnerton-Dyer conjecture for $\mathbb{Q}$-curves

Yu Zhao

Doctor of Philosophy

Department of Mathematics and Statistics

McGill University

Montreal,Quebec

March 13, 2011

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements of the degree of Doctor of Philosophy

Abstract

Let $N \equiv 1 (\mathrm{mod}\ 4)$ be a positive integer and let χ be the single even primitive quadratic Dirichlet character on $(\mathbb{Z}/N\mathbb{Z})^{\times}$. Let $f \in S_2(\Gamma_0(N), \chi)$ be a newform with nebentypus χ. By the Shimura construction, f corresponds to an abelian variety A_f defined over $\mathbb{Q}$ whose dimension is $[K_f : \mathbb{Q}]$ where K_f is the number field associated with f. When $\dim A_f = 2$, the Fricke involution w_N acts on A_f and is defined over $\mathbb{Q}(\sqrt{N})$, inducing a decomposition

$$A_f \sim E \times E,$$

where $E/\mathbb{Q}(\sqrt{N})$ is an elliptic curve which is isogenous to its Galois conjugate over $\mathbb{Q}(\sqrt{N})$. Such an E is called a $\mathbb{Q}$-curve (completely) defined over $\mathbb{Q}(\sqrt{N})$.

The main result of this thesis is the proof of a Kolyvagin-like result for $\mathbb{Q}$-curves defined over $\mathbb{Q}(\sqrt{N})$ of perfect square conductor (including trivial conductor) over that field. Such a setting lies beyond the scope of the general results of Zhang [Zh1] because of the absence of a Shimura curve parametrization for E. This thesis also describes an explicit construction of Heegner points on E in a setting which so far has not yet studied in the literature and provides numerical examples. In turn, these computations yield numerical evidence for a conjectural connection, which we propose in this thesis, between the Heegner points we construct and the ATR points obtained by Darmon-Logan in [DL].

Abrégé

Soit $N \equiv 1 (\mathrm{mod}\ 4)$ un entier positive et soit χ l'unique caractère de Dirichlet primitif pair quadratique sur $(\mathbb{Z}/N\mathbb{Z})^\times$. Soit $f \in S_2(\Gamma_0(N), \chi)$ une newform. Par la construction de Shimura, f correspond à une variété abélienne A_f définie sur $\mathbb{Q}$ dont la dimension est $[K_f : \mathbb{Q}]$ où K_f est le corps de nombres associé à f. Quand $\dim(A_f) = 2$, l'involution Frick donne la décomposition

$$A_f \sim E \times E,$$

où $E/\mathbb{Q}(\sqrt{N})$ est une courbe elliptique qui est isogène à son conjugué Galoisien sur $\mathbb{Q}(\sqrt{N})$. On dit que E est une $\mathbb{Q}$-courbe (complètement) définie sur $\mathbb{Q}(\sqrt{N})$.

Le résultat principal de cette thèse est la démontration d'un résultat dans le style de Kolyvagin pour les $\mathbb{Q}$-courbes définies sur $\mathbb{Q}(\sqrt{N})$ de conducteur un carré parfait (ce qui comprend le conducteur trivial) sur ce corps. Le résultat général de Zhang [Zh1] ne s'applique pas directement à cette situation en raison de l'absence d'une paramétrisation de E par une courbe de Shimura sur $\mathbb{Q}(\sqrt{N})$. Cette thèse décrit également la construction explicite de certains points de Heegner dans un cadre qui, jusqu'ici, n'étai pas disponible dans la littérature, et en fournit quelques exemples numériques. Ces calculs confirment conjecture, énoncée dans cette thèse, sur le rapport les points de Heegner que nous construisons et les points de ATR obtenus par Darmon-Logan [DL].

Acknowledgements

First of all, I would like to give my sincere thanks to Prof. Henri Darmon, one of my supervisors. He not only provided me an interesting problem for my PhD thesis but also encouraged me when I needed help from him. His way of thinking about mathematics had a deep impact on me. Such impact will certainly persist in my future academic career.

I also give my thanks to Prof. Victor Rotger, my co-supervisor. I discussed many details with him. Such discussions were very helpful for my thesis. Both of my two supervisors took their unique roles to guide me to finish my thesis. They also used their precious time to correct my English and French.

I would also like to thank to my M.Sc. advisor Prof. Eyal Goren. Not only did he give me the opportunity to study mathematics, but he taught me an incredible amount of mathematics during my first several years at McGill.

There are also many other people I would like to acknowledge for their support over the last years. Besides the staff in the department, I owe much to friendly fellow graduate students and postdocs. I also give my thanks to professors in other Montreal universities who taught mathematics to me. Among them, my special thanks go to Prof. Adrian Iovita who also influenced me a lot in number theory.

Last but not least, I express my indebtedness here to my wife for years of patience and support. This work is dedicated to her.

TABLE OF CONTENTS

Chapter 1
Introduction

1.1 The Birch and Swinnerton-Dyer conjecture

Let E be an elliptic curve defined over a number field F. The Mordell-Weil theorem tells us that the abelian group $E(F)$ of F-rational points on E is finitely generated. The $\mathbb{Z}$-rank of its non-torsion part is called the (*arithmetic*) *rank* of E over F. While it is often easy to compute the torsion subgroup of $E(F)$, the rank of $E(F)$ is poorly understood.

Naturally enough, analytic tools should also be considered involving the Hasse-Weil function $L(E/F, s)$. Although the original definition of $L(E/F, s)$ as an Euler product only converges to an analytic function when $\mathrm{Re}(s) > 3/2$, it is conjectured that $L(E/F, s)$ admits analytic continuation to the entire complex plane and satisfies a functional equation relating its values at s and $2 - s$. Hence the central point is $s = 1$. The celebrated conjecture [BSD] of Birch and Swinnerton-Dyer (BSD, for short) links the arithmetic rank of E with the order of vanishing of $L(E/F, s)$ at $s = 1$, which is called the *analytic rank* of E, predicting that the two ranks are equal.

This prediction is sometimes called the *weak form of the BSD conjecture*. The *strong form of the BSD conjecture* suggests in addition a precise formula for the leading term of the Taylor expansion of $L(E/F, s)$ at $s = 1$, involving the orders of the Tate-Shafarevic group $Ш(E/F)$ and the torsion group $E_{\mathrm{tor}}(F)$ of E ([Dar, §1.4],[Lan2, III §5]).

The BSD conjecture also generalizes to higher-dimensional abelian varieties A/F defined over a number field and predicts a similar conjectural description of the leading term of the Taylor expansion of the L-function of A at $s = 1$ ([Lan2, III §5]). Unfortunately, even in the simplest settings, not much is known about the BSD conjecture.

For an elliptic curve E over $\mathbb{Q}$, Gross and Zagier ([GZ]) proved under the assumption of modularity on E (which was later removed thanks to the work of Wiles, Taylor and their collaborators) a formula relating $L'(E/\mathbb{Q}, 1)$ to the Néron-Tate height of a Heegner point on E. Combined with Kolyvagin's machinery of Euler systems([Kol1], [Kol2], [Kol3]), this could be used to prove that the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ is finite and to show the BSD conjecture for $E/\mathbb{Q}$ whenever $\mathrm{ord}_{s=1}L(E/\mathbb{Q}, s) \leq 1$.

1.2 Generalization of Gross-Zagier-Kolyvagin theorem

Various generalizations have been achieved after the work of Gross, Zagier and Kolyvagin. Among them, a notable progress is the generalization obtained by Zhang ([Zh1]) to elliptic curves E defined over a totally real field F satisfying the so-called *Jacquet-Langlands hypothesis*, whose precise formulation is given in section 6.3.1. This hypothesis implies the existence of a Shimura curve X and a non-constant morphism $\varphi : X \longrightarrow E$, both defined over F. The natural supply of CM points existing on X can be used to construct Heegner points on E.

Zhang's proof heavily depends on the parametrization of E by the Shimura curve X. However, the Jacquet-Langlands hypothesis does not always hold. The simplest case where the hypothesis fails arises when the elliptic curve E is defined over a real quadratic field F and has everwhere good reduction. In this case, no Shimura or modular curve together with a non-constant morphism to E/F seems to be available in general.

1.3 $\mathbb{Q}$-curves

An exception to the previous statement is provided by the family of $\mathbb{Q}$-*curves* over totally real fields. By definition a $\mathbb{Q}$-curve E (completely defined) over a number field F is an elliptic curve E defined over F which is isogenous over F to all its Galois conjugates. Due to the work of Ribet [Rib5] and the proof of Serre's conjecture ([KW]), it is now known that all $\mathbb{Q}$-curves are modular in the sense that, for some integer $N \geq 1$, there is a non-constant morphism over F:

$$X_1(N)_F \to E\,, \tag{1.1}$$

where $X_1(N)/\mathbb{Q}$ stands for the classical modular curve of level N associated to the congruence subgroup $\Gamma_1(N)$ and $X_1(N)_F := X_1(N) \times \mathrm{Spec}(F)$.

The existence of (1.1) raises the hope of proving a Kolyvagin-like result for $\mathbb{Q}$-curves, or at least for some reasonable subset of $\mathbb{Q}$-curves.

1.4 Original contributions

Let $N > 1$ be a square-free odd positive integer and let χ be the single even non-trivial primitive quadratic character on $(\mathbb{Z}/N\mathbb{Z})^\times$. Let $f \in S_2(\Gamma_0(N), \chi)$ be a new form. Assume the associated number field of f is an imaginary quadratic field. Then Shimura's construction ([Shi1], [Shi2, Chapter 7]) shows that f corresponds to an elliptic $\mathbb{Q}$-curve E (completely) defined over $F = \mathbb{Q}(\sqrt{N})$. Since $\mathrm{ord}_{s=1} L(E/F, s)$ is even, we instead choose a quadratic ATR extension M/F and consider the twist E_M of E with respect to M/F; the sign of the L-function of E_M is now -1 and it makes sense to wonder about the existence of a natural supply of Heegner points on it. The reader is referred to section 6.4 for details including precise definitions of the above terms. Together with Darmon and Rotger, we obtain the following result ([DRZ]):

Theorem 1.4.1. *Let E/F be a $\mathbb{Q}$-curve defined over a real quadratic field F with perfect square conductor. Let M/F be an ATR extension. If $L'(E_M/F, 1) \neq 0$, then $E_M(F)$ has rank 1 and $Ш(E_M/F)$ is finite.*

1.5 Contribution of Authors

This thesis is partly based on the article [DRZ] co-authored with Prof. Henri Darmon and Prof. Victor Rotger, to which the latter made a substantial contribution. All three authors were equal partners in this collaboration and the order in which their names appear follows the common mathematical usage of listing authors alphabetically.

1.6 Structure of the thesis

Together with the introduction, this thesis consists of nine chapters.

- Chapter 2 introduces the background of newforms with nebentypus.
- Chapter 3 and Chapter 4 introduce the main objects studied in this thesis. Chapter 3 describes the Shimura construction of the abelian variety A_f up to isogeny associated with a newform $f \in S_2(\Gamma_0(N), \chi)$. Chapter 4 describes the decomposition of A_f over $\overline{\mathbb{Q}}$, which in some cases leads naturally to $\mathbb{Q}$-curves.
- Chapter 5 studies curve $X_\chi(N)$ when χ is a quadratic character. We pay particular attention to modular parametrizations of elliptic $\mathbb{Q}$-curves (completely) defined over a quadratic field afforded by curve $X_\chi(N)$, which lead to the construction of Heegner points on them.
- Chapter 6 discusses the Birch and Swinnerton-Dyer conjecture in some detail and reviews the known cases of this conjecture.
- Chapter 7 contains the proof of the main result of this thesis.

- Chapter 8 and 9 describe the explicit construction of Heegner points and provide numerical examples. These computations are also used to compare our Heegner points to those constructed by the method of Damon and Logan in [DL] by means of ATR cycles on Hilbert modular surfaces.
- Chapter 10 describes a more explicit proof of the main result (to be more precise, Theorem 7.2.5) by directly using Kolyvagin's Euler system.

Chapter 2
Modular forms with non-trivial nebentypus

We define the following standard notations:

- $\mathcal{H}$ denotes the complex upper half plane:

$$\mathcal{H} := \{z \in \mathbb{C} \,\big|\, \mathrm{Im}(z) > 0\},$$

  and $\mathcal{H}^*$ is defined as

$$\mathcal{H}^* := \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}.$$

- Let $N \geq 1$ be an integer. Define the congruence subgroups $\Gamma_0(N)$ and $\Gamma_1(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ to be

$$\Gamma_0(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \,\big|\, c \equiv 0 (\mathrm{mod}\ N) \right\},$$
$$\Gamma_1(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N) \,\big|\, a \equiv d \equiv 1 (\mathrm{mod}\ N) \right\}.$$

- For any positive integer $k > 1$, denote by $S_k(\Gamma_1(N))$ the complex vector space of cusp forms of weight k on $\Gamma_1(N)$.

2.1 Modular forms with nebetypus

For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ and $f \in S_k(\Gamma_1(N))$, the standard "$|_\gamma$" operator

$$f \mapsto f\big|_\gamma \tag{2.1}$$

is an endomorphism which depends only on $d \,(\mathrm{mod}\ N)$ and hence induces a linear action of $(\mathbb{Z}/N\mathbb{Z})^*$ on $S_2(\Gamma_1(N))$. The operator defined in (2.1) is called the *diamond*

operator and is denoted by $\langle d\rangle$. The theory of group representations yields a natural decomposition:

$$S_k(\Gamma_1(N)) = \bigoplus_{\chi} S_k(\Gamma_0(N), \chi),$$

where χ runs through all Dirichlet characters $(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}$ and $S_k(\Gamma_0(N), \chi)$ is defined as:

$$S_k(\Gamma_0(N), \chi) := \left\{ f \in S_k(\Gamma_1(N)) \,\middle|\, \langle d\rangle f = \chi(d) f, \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

The character χ here is called the *nebentypus* of f. It is easy to see that $S_k(\Gamma_0(N), \chi) = 0$ if k is even and χ is an odd character or k is odd and χ is an even character.

2.2 Hecke operators

Besides the diamond operators, there are Hecke operators T_n for integers $n \geq 1$ acting on the above spaces of modular forms. For any congruence subgroups Γ_1 and Γ_2 of $\mathrm{SL}_2(\mathbb{Z})$ and $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$, define a linear transformation $S_k(\Gamma_1) \to S_k(\Gamma_2)$ by

$$f|\Gamma_1 \gamma \Gamma_2 := \sum_j f|\beta_j \,,$$

where $\Gamma_1 \gamma \Gamma_2 = \sqcup_j \Gamma_1 \beta_j$. For any $f \in S_2(\Gamma_0(N), \chi)$ and any prime p, the Hecke operator T_p is defined in terms of these transformations as

$$T_p f := f|\Gamma_1(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma_1(N).$$

If the Fourier expansion of $f \in S_2(\Gamma_0(N), \chi)$ at ∞ is given by

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \text{ where } q = e^{2\pi i z}, \tag{2.2}$$

then

$$(T_p f)(z) = \sum_{n=1}^{\infty} (a_{np} + \chi(p) p a_{n/p}) q^n, \text{ where } a_{n/p} = 0 \text{ if } p \nmid n.$$

For a composite integer n, the Hecke operator T_n is defined in terms of the Hecke operators T_p and diamond operators: for details, we refer the reader to [Dia, Chapter 5].

Cusp forms in $S_2(\Gamma_1(N))$ may arise from lower levels dividing N. Indeed, if M divides N, the space $S_2(\Gamma_1(M))$ is contained in $S_2(\Gamma_1(N))$ in several natural ways besides the natural inclusion $S_2(\Gamma_1(M)) \subset S_2(\Gamma_1(N))$. Indeed, let d be any divisor of N/M, and define the operator $[d]$ for any $f \in S_2(\Gamma_1(M))$ by

$$f|[d](z) := df(dz), \quad \forall z \in \mathcal{H}.$$

Then the map $[d]$ is injective and takes $S_2(\Gamma_1(M))$ to $S_2(\Gamma_1(N))$. Now for any positive divisor d of N, define ι_d to be:

$$\iota_d : S_2(\Gamma_1(N/d) \times S_2(\Gamma_1(N/d) \to S_2(\Gamma_1(N)), \quad (f, g) \mapsto f + g|[d].$$

Define the subspace $S_2(\Gamma_1(N))^{\text{old}}$ of oldforms at level N to be

$$S_2(\Gamma_1(N))^{\text{old}} := \sum_{\text{prime } p|N} \iota_p(S_2(\Gamma_1(N/p)) \times S_2(\Gamma_1(N/p))).$$

The subspace $S_2(\Gamma_1(N))^{\text{new}}$ of newforms at level N is defined as the orthogonal complement of $S_2(\Gamma_1(N))^{\text{old}}$ with respect to the Petersson inner product. It can be shown that both subspaces are preserved by the diamond operators and Hecke operators.

Let $f \in S_2(\Gamma_1(N))^{\text{new}}$ be an eigenform for the Hecke operators T_n and diamond operators $\langle d \rangle$ with $(d, N) = 1$. If we write down the Fourier expansion of f as in (2.2), it can be proved that $a_1 \neq 0$. Hence we can normalize it so that $a_1 = 1$; such f is called a (normalized) *newform*. In the subspace $S_2(\Gamma_1(N))^{\text{new}}$, the well-known multiplicity one theorem says the set of newforms in $S_2(\Gamma_1(N))^{\text{new}}$ is an

orthogonal basis of this space and each newform lies in a subspace $S_2(\Gamma_0(N), \chi)$ for some nebentypus χ.

Let $f \in S_2(\Gamma_0(N), \chi)$ be a newform with Fourier expansion (2.2) at ∞. For any prime $p \nmid N$, let T_p^* be the adjoint of T_p with respect to the Petersson inner product. It is known that

$$T_p^* = \langle p \rangle^{-1} T_p = \chi(p)^{-1} T_p \ . \tag{2.3}$$

Hence

$$T_p^*(f) = \overline{a}_p f = \chi(p)^{-1} a_p f,$$

i.e.

$$a_p = \chi(p)\overline{a}_p, \tag{2.4}$$

where the bar denotes the usual complex conjugation.

Corollary 2.2.1. *Let $f \in S_2(\Gamma_0(N), \chi)$ be a newform with Fourier expansion* (2.2)*. If χ is the trivial character, then $a_p \in \mathbb{R}$ for all primes $p \nmid N$. If χ is an even quadratic character, then for any prime $p \nmid N$,*

$$a_p \in \mathbb{R} \text{ if } \chi(p) = 1;$$

$$a_p \in i \cdot \mathbb{R} \text{ if } \chi(p) = -1.$$

Proof. Obvious from (2.4) □

Let K_f be the field generated over $\mathbb{Q}$ by all the values $\chi(p)$ and a_p for a newform $f \in S_2(\Gamma_0(N), \chi)$. It is a well-known result that K_f is a number field and K_f can actually be generated by finitely many a_p's over $\mathbb{Q}$. Let σ be any embedding of K_f into $\mathbb{C}$. Define f^σ to be:

$$f^\sigma := \sum_{n=1}^{\infty} \sigma(a_n) q^n.$$

Then it is easy to prove that f^σ belongs to $S_2(\Gamma_0(N), \sigma\chi)$ and

$$T_p f^\sigma = \sigma(a_p) f^\sigma$$

for all primes p. Shimura ([Shi1, Proposition 1.3]) also proves the following result about K_f:

Proposition 2.2.2 (Shimura)**.** *If χ is non-trivial, then K_f is a CM field.*

Chapter 3
Shimura's construction

Let $f \in S_2(\Gamma_0(N), \chi)$ be a newform. Shimura ([Shi2, Chapter 7]) constructs an abelian variety A_f associated with f of dimension $\dim(A_f) = [K_f : \mathbb{Q}]$. This chapter briefly describes the construction. We follow [CoRu, Chapter 5].

3.1 Hecke operators, revisited

In this section we describe Hecke operators from another point of view.

Let p be a prime number such that $p \nmid N$. Define $\Gamma_1(N,p) := \Gamma_1(N) \cap \Gamma_0(p)$ and

$$Y_1(N,p)^{\mathrm{an}} := \Gamma_1(N,p)\backslash\mathcal{H}$$

$$X_1(N,p)^{\mathrm{an}} := \Gamma_1(N,p)\backslash\mathcal{H}^*.$$

Here $Y_1(N,p)^{\mathrm{an}}$ can be identified with the set of isomorphism classes

$$\{(E,P,G)\}/\cong,$$

where E is an elliptic curve over $\mathbb{C}$, P is a point in E of exact order N and G is a subgroup of E of order p, via the assignment

$$z \mapsto (\mathbb{C}/[1,z], \frac{1}{N}, \langle\frac{1}{p}\rangle).$$

Here $(E,P,G) \cong (E_1,P_1,G_1)$ if and only if there exists an isomorphism $\tau : E \to E_1$ such that $\tau(P) = P_1$ and $\tau(G) = G_1$.

There are two analytic maps:

$$\pi_1 : X_1(N,P)^{\mathrm{an}} \to X_1(N)^{\mathrm{an}}, \quad (E,P,G) \mapsto (E,P);$$
$$\pi_2 : X_1(N,P)^{\mathrm{an}} \to X_1(N)^{\mathrm{an}}, \quad (E,P,G) \mapsto (E/G, P \,(\mathrm{mod}\ G)).$$

Hence one has the correspondence:

$$\begin{array}{ccc} & X_1(N,p)^{\mathrm{an}} & \\ {\scriptstyle \pi_1}\swarrow & & \searrow{\scriptstyle \pi_2} \\ X_1(N)^{\mathrm{an}} & & X_1(N)^{\mathrm{an}} \end{array} \tag{3.1}$$

In the language of action of matrices on $\mathcal{H}$, π_1 is the map:

$$\Gamma_1(N,p)\backslash\mathcal{H} \to \Gamma_1(N)\backslash\mathcal{H}, \quad z \mapsto z,\ \forall z \in \mathcal{H},$$

and π_2 is the composition of the following two maps:

$$\Gamma_1(N,p)\backslash\mathcal{H} \to \gamma_p\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_1(N,p)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\gamma_p^{-1}\backslash\mathcal{H} \to \Gamma_1(N)\backslash\mathcal{H},$$

where $\gamma_p \in \mathrm{SL}_2(\mathbb{Z})$ and $\gamma_p \equiv \left(\begin{smallmatrix} p^{-1} & * \\ 0 & p \end{smallmatrix}\right)(\mathrm{mod}\ N)$. Note $\Gamma_1(N,p)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} \subset \Gamma_1(N)$ and $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$, hence $\gamma_p\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_1(N,p)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\gamma_p^{-1} \subset \Gamma_1(N)$. The action of γ_p on $\mathcal{H}$ induces a map $\langle p\rangle$:

$$Y_1(N)^{\mathrm{an}} \to Y_1(N)^{\mathrm{an}}, \quad (E,Q) \mapsto (E,pQ),$$

where Q is a point on elliptic curve E over $\mathbb{C}$ with exact order N. $\langle p\rangle$, π_1 and π_2 give us two endomorphisms on $H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}})$, where $\underline{\mathbb{Z}}$ is the constant scheme associated with $\mathbb{Z}$:

$$\langle p\rangle^* : H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}}) \to H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}}),$$
$$T_p^* = (\pi_1)_*(\pi_2)^* : H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}}) \to H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}}).$$

Let ζ_N be a primitive N-th root of unity in $\mathbb{C}$. Define the map ω_{ζ_N} as:

$$\omega_{\zeta_N} : Y_1(N)^{\mathrm{an}} \to Y_1(N)^{\mathrm{an}}, \quad (E,P) \mapsto (E,Q),\ \forall (E,P) \in Y_1(N)^{\mathrm{an}},$$

where Q is a point in $E(\mathbb{C})$ with exact order N such that the Weil paring

$$\langle P, Q\rangle_{\mathrm{Weil}} = \zeta_N.$$

Then ω_{ζ_N} gives an analytic map $X_1(N)^{\mathrm{an}} \to X_1(N)^{\mathrm{an}}$. Choose $\zeta_N = e^{2\pi i/N}$, then ω_{ζ_N} is induced by $z \to Hz$ on $\mathcal{H}$, where $H = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ and it will be denoted by ω_N. The involution ω_N also induces

$$\omega_N^* : H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}}) \to H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}}).$$

The Hodge decomposition gives isomorphisms

$$\begin{aligned} H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathbb{C} &\cong H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{C}}) \\ &\cong H^0(X_1(N)^{\mathrm{an}}, \Omega^1_{X_1(N)^{\mathrm{an}}}) \oplus H^0(X_1(N)^{\mathrm{an}}, \overline{\Omega}^1_{X_1(N)^{\mathrm{an}}}). \end{aligned}$$

If one uses the canonical identification $S_2(\Gamma_1(N)) \cong H^0(X_1(N)^{\mathrm{an}}, \Omega^1_{X_1(N)^{\mathrm{an}}})$, one can show ([CoRu, Chapter 5]) that $\langle p\rangle^* \otimes 1$ corresponds to $\langle p\rangle \oplus \overline{\langle p\rangle}$, $T_p^* \otimes 1$ corresponds to $T_p \oplus \overline{T}_p$ and $\omega_N^* \otimes 1$ to $\omega_N \oplus \overline{\omega}_N$.

3.2 Algebraic modular forms

It is well known that for any compact Riemann surface X,

$$H^1(X, \mathcal{O}_X^*) \cong \mathrm{Pic}_X \text{ and } H^2(X, \mathcal{O}_X) \cong \mathbb{Z},$$

where Pic_X is the Picard group of X. Hence from the short exact sequence

$$0 \to \underline{\mathbb{Z}} \to \mathcal{O}_X \xrightarrow{e^{2\pi i(\cdot)}} \mathcal{O}_X^* \to 1,$$

one obtains the long exact sequence

$$0 \to H^1(X, \underline{\mathbb{Z}}) \to H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X^*) \cong \mathrm{Pic}_X \to H^2(X, \mathcal{O}_X) \cong \mathbb{Z}. \qquad (3.2)$$

As it is shown in [Har, Appendix §5], (3.2) leads to the following identification:

$$\mathrm{Pic}_X^0 \cong H^1(X, \mathcal{O}_X)/H^1(X, \underline{\mathbb{Z}}). \qquad (3.3)$$

Let $f : X \to Y$ be a finite map between two compact Riemann surfaces. Then there is a trace map

$$f_* \mathcal{O}_X \to \mathcal{O}_Y$$

which is compatible with the trace map

$$f_* \underline{\mathbb{Z}} \to \underline{\mathbb{Z}}.$$

This trace map induces:

$$f_* : H^1(X, \mathcal{O}_X) \cong H^1(Y, f_* \mathcal{O}_X) \to H^1(Y, \mathcal{O}_Y).$$

In addition, there are also compatible pullbacks:

$$f^* \mathcal{O}_Y \cong \mathcal{O}_X \text{ and } f^* \underline{\mathbb{Z}} \cong \underline{\mathbb{Z}}$$

and

$$f^* : H^1(Y, \mathcal{O}_Y) \to H^1(X, f^* \mathcal{O}_Y) \cong H^1(X, \mathcal{O}_X).$$

Hence f induces two commutative diagrams:

$$\begin{array}{ccc} H^1(Y, \mathcal{O}_Y) & \xrightarrow{f^*} & H^1(X, \mathcal{O}_X) \\ \uparrow & & \uparrow \\ H^1(Y, \underline{\mathbb{Z}}) & \xrightarrow{f^*} & H^1(X, \underline{\mathbb{Z}}) \end{array} \qquad \begin{array}{ccc} H^1(X, \mathcal{O}_X) & \xrightarrow{f_*} & H^1(Y, \mathcal{O}_Y) \\ \uparrow & & \uparrow \\ H^1(X, \underline{\mathbb{Z}}) & \xrightarrow{f_*} & H^1(Y, \underline{\mathbb{Z}}) \end{array}$$

Therefore, from (3.3), we conclude that f induces maps:

$$f^* : \mathrm{Pic}^0_Y \to \mathrm{Pic}^0_X, \qquad f_* : \mathrm{Pic}^0_X \to \mathrm{Pic}^0_Y.$$

Using the isomorphism $\mathrm{Pic}^0_X \cong J(X)$, the Jacobian of X, f^* and f_* are the standard pullback and forward maps between the Jacobians of X and Y, one map being dual to another.

Note also that (3.1) gives rise to two operations on $J_1(N)$:

$$(T_p)_* := (\pi_2)_* \circ (\pi_1)^*; \; (T_p)^* := (\pi_1)_* \circ (\pi_2)^*.$$

From (3.3) and the fact $H^1(X, \underline{G}) \cong G^{2g}$ for any abelian group G, where g is the genus of X, the Tate module([CoRu, p. 210–211])

$$V_\ell(N) := V_\ell(J_1(N)) = \varprojlim_n H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}/\ell^n\mathbb{Z}}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}_\ell}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

has $\mathbb{Q}_\ell$-dimension $2g$. Here ℓ is any prime number not dividing N.

Clearly $V_\ell(N)$ has two $T_1(N)$ actions via $()_*$ or $()^*$-actions. This module is also equipped with the Weil pairing

$$\langle\, , \rangle_\ell : V_\ell(N) \otimes V_\ell(N) \to \mathbb{Q}_\ell(1)$$

which arises via the cup product

$$H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}_\ell}) \otimes_{\mathbb{Z}} H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}_\ell}) \xrightarrow{\cup} H^2(X_1(N)^{\mathrm{an}}, \underline{\mathbb{Z}_\ell}) \cong \mathbb{Z}_\ell \xrightarrow[\cong]{1 \mapsto e^{2\pi i/\ell^n}} \varprojlim_n \mu_{\ell^n}.$$

One can prove the following result ([CoRu, Corollary 5.9]):

Proposition 3.2.1. *The $\mathbb{Q}_\ell \otimes_{\mathbb{Z}} T_1(N)$-module $V_\ell(N)$ is free of rank two for either action. Moreover, $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} T_1(N), \mathbb{Q})$ is free of rank one over $\mathbb{Q} \otimes T_1(N)$.*

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. From the above proposition, one obtains a 2-dimensional representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(V_\ell(N)) \cong \mathrm{GL}_2(\mathbb{Q}_\ell \otimes_{\mathbb{Z}} T_1(N)).$$

Proposition 3.2.2. *For either action $()_*$ or $()^*$, ρ is continuous and unramified at any prime $p \nmid N\ell$ and in this case, under the $()_*$-action, the characteristic polynomial of $\rho(\mathrm{Frob}_p)$ is*

$$x^2 - (T_p)_* x + p\langle p\rangle_*.$$

Let $f \in S_2(N,\chi)$ be a newform and let I_f be the kernel of the group homomorphism

$$T_1(N) \to K_f, \quad T \mapsto a_1(Tf).$$

Define the abelian variety $A_f := J_1(N)/I_f J_1(N)$ where we regard $T_1(N)$ acting on $J_1(N)$ via the $()_*$-action. Then one has the exact sequence of abelian varieties

$$0 \to I_f J_1(N) \to J_1(N) \to A_f \to 0,$$

which in turn implies that the following sequence is exact:

$$V_\ell(I_f J_1(N)) = I_f V_\ell(J_1(N)) \to V_\ell(J_1(N)) \to V_\ell(A_f) \to 0.$$

Note that the algebra $K_f \cong T_1(N)/I_f \otimes_{\mathbb{Z}} \mathbb{Q}$ acts on A_f, by descending the action of the Hecke algebra $T_1(N)$ on $J_1(N)$. Hence

Theorem 3.2.3. *$V_\ell(A_f)$ is free of rank 2 over $\mathbb{Q}_\ell \otimes_{\mathbb{Z}} T_1(N)/I_f \cong \mathbb{Q}_\ell \otimes_{\mathbb{Q}} K_f$ and so the dimension of A_f is $[K_f : \mathbb{Q}]$. For any prime number $p \nmid N\ell$, the Frobenius element Frob_p has characteristic polynomial*

$$x^2 - (1 \otimes a_p(f))x + 1 \otimes p\chi(p).$$

Theorem 3.2.3 actually means that there exists a Galois representation

$$\rho_\ell : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_\ell \otimes_{\mathbb{Q}} K_f) \tag{3.4}$$

which is unramified at each prime $p \nmid \ell N$ and the trace and the norm of the image of the Frobenius element Frob_p with respect to such p are a_p and $p\chi(p)$ respectively.

On the other hand,

$$\mathbb{Q}_\ell \otimes_{\mathbb{Q}} K_f \cong \prod_{\lambda|\ell} (K_f)_\lambda$$

and this corresponds to the decomposition

$$V_\ell(A_f) \cong \prod_{\lambda|\ell} V_\ell(A_f)_\lambda \ .$$

Using the fact that $V_\ell(A_f)_\lambda$ is simple over $(K_f)_\lambda[G_{\mathbb{Q}}]$ ([Rib3, Theorem 2.3]) and the action of $G_{\mathbb{Q}}$ on $V_\ell(A_f)_\lambda$ is non-abelian ([Rib3, Proposition 4.1]), one can prove ([Rib4, Proposition 4.1]) that

$$\mathrm{End}_{G_{\mathbb{Q}}} V_\ell(A_f) \cong K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell. \tag{3.5}$$

From the injection

$$\mathrm{End}_{\mathbb{Q}}(A_f) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{G_{\mathbb{Q}}} V_\ell(A_f),$$

one derives the following result ([Rib4, Corollary 4.2]):

Proposition 3.2.4. $\mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q} \cong K_f$.

In particular, one concludes that A_f is simple over $\mathbb{Q}$. However, the simplicity of A_f over $\mathbb{Q}$ does not imply that A_f is absolutely simple. That is, A_f may split up to isogenies over $\overline{\mathbb{Q}}$. This is indeed what will occur in the setting of the $\mathbb{Q}$-curves which will be introduced in the next chapter.

Chapter 4
$\mathbb{Q}$-curves

Let $f \in S_2(\Gamma_0(N), \chi)$ be a newform of nebentypus χ. Chapter 3 introduced the Shimura construction to associate to f an abelian variety A_f over $\mathbb{Q}$ with the property that $\mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q} \cong K_f$. As pointed out in chapter 3, although A_f is simple over $\mathbb{Q}$, it may fail to be so over $\overline{\mathbb{Q}}$. This chapter will discuss the decomposition of A_f over $\overline{\mathbb{Q}}$ up to isogeny.

4.1 GL_2-type abelian varieties

In the literature there are several slightly different definitions of what it means for an abelian variety to be *of* GL_2*-type*. We take the one below.

Definition 4.1.1. *An abelian variety A defined over $\mathbb{Q}$ is said to be of GL_2-type if $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ contains a number field of degree equal to $\dim(A)$.*

If K is a number field equipped with an injection:

$$K \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q},$$

then K acts $\mathbb{Q}$-linearly on the cotangent space of $A/\mathbb{Q}$ whose dimension is $d = \dim(A)$. It follows that K is isomorphic to a commutative subring of $M_d(\mathbb{Q})$ and therefore $\dim(A) \geq [K : \mathbb{Q}]$. The GL_2-type abelian varieties are those for which K reaches the maximum degree.

Let A be an abelian variety of GL_2-type over $\mathbb{Q}$ and let $K \subset \mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ be a number field embedded in its endomorphism algebra of degree $[K : \mathbb{Q}] = \dim(A)$. Let

L/K be a finite field extension of degree m. Then one can always find an embedding $L \hookrightarrow M_m(K)$, the algebra of $m \times m$ matrices over K after fixing a K-basis of L/K. It is easy to see that $M_m(K)$ acts naturally on $B := \underbrace{A \times \cdots A}_{m}$. Hence there is a natural embedding $L \hookrightarrow \mathrm{End}_{\mathbb{Q}}(B) \otimes \mathbb{Q}$ and consequently B is also of GL_2-type.

Definition 4.1.2. *An abelian variety A of GL_2-type over $\mathbb{Q}$ is said to be primitive if A is not isogenous over $\mathbb{Q}$ to any abelian variety obtained by the construction above.*

Ribet ([Rib5, Theorem 2.1]) proves the following result about the primitivity of an abelian variety of GL_2-type:

Proposition 4.1.3. *Let A be an abelian variety of GL_2-type over $\mathbb{Q}$. Then the following conditions are equivalent:*

- *$A/\mathbb{Q}$ is primitive.*
- *$A/\mathbb{Q}$ is simple.*
- *$\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ is a number field with degree equal to the dimension of A.*

Due to the above proposition, by the definition of GL_2-type and the Shimura construction introduced in Chapter 3, for any newform $f \in S_2(\Gamma_0(N), \chi)$, the associated abelian variety A_f is of primitive GL_2-type.

Hereafter, we will only discuss abelian varieties of primitive GL_2-type and the word "primitive" will be dropped.

A remarkable result ([Rib5, §1]) about abelian varieties of GL_2-type is that, up to isogenies, they all can be obtained by means of the Shimura construction. Ribet's proof is based on Serre's conjecture which is proved in [KW]:

Theorem 4.1.4 (Ribet)**.** *Every abelian variety of GL_2-type is isogenous over $\mathbb{Q}$ to the abelian variety A_f associated with a newform $f \in S_2(\Gamma_0(N), \chi)$ by the Shimura construction for some level N and nebentypus χ.*

4.2 Decomposition over $\overline{\mathbb{Q}}$

As pointed out above, for any newform $f \in S_2(\Gamma_0(N), \chi)$, although the associated abelian variety A_f is defined over $\mathbb{Q}$ and is $\mathbb{Q}$-simple, it does not need to be $\overline{\mathbb{Q}}$-simple in general, i.e. A_f may be isogenous to a non-trivial product of $\overline{\mathbb{Q}}$-simple abelian varieties.

According to Shimura ([Shi1, §1]), one says an abelian variety A is of *CM-type* if it is isogenous to a product of abelian varieties $A_1 \times A_2 \times \cdots \times A_n$ such that for each A_i, $\mathrm{End}(A_i) \otimes \mathbb{Q}$ is isomorphic to a CM-field of degree $2 \cdot \dim(A_i)$.

In the case where $A_f/\overline{\mathbb{Q}}$ contains an abelian subvariety of CM-type, Shimura ([Shi1, Proposition 1.6]) proves that $A/\overline{\mathbb{Q}}$ is isogenous to a power of some CM elliptic curve.

If $A_f/\overline{\mathbb{Q}}$ does not contain a subvariety of CM-type, Ribet ([Rib5, §5]) proves the following result:

Proposition 4.2.1. *If $A_f/\overline{\mathbb{Q}}$ does not contain a subvariety of CM-type, then the center of $\mathbb{Q} \otimes \mathrm{End}_{\overline{\mathbb{Q}}}(A)$ is the subfield F of K_f generated over $\mathbb{Q}$ by numbers $a_p^2/\chi(p)$ for prime $p \nmid N$. The algebra $\mathbb{Q} \otimes \mathrm{End}_{\overline{\mathbb{Q}}}(A)$ is isomorphic to $M_n(D)$, where $D = F$ or a quaternion division algebra over F. Moreover F is totally real and K_f/F is abelian.*

The above proposition leads to the following result about the decomposition of A_f over $\overline{\mathbb{Q}}$:

Corollary 4.2.2. *With notations as in Proposition* 4.2.1*,*

$$A_f/\overline{\mathbb{Q}} \sim B^n, \tag{4.1}$$

and $B \sim B^g$ for any $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and

$$\dim(B) = \sqrt{\dim_F(D)}[F : \mathbb{Q}]. \tag{4.2}$$

Moreover,

$$\mathrm{End}_{\overline{\mathbb{Q}}}(B) \otimes \mathbb{Q} \cong D.$$

4.3 Fields of definition of isogonies

We can also ask about fields of definition of *all* isogenies between B and its Galois conjugates. Using notations above, it is well-knowm that for any $\sigma \in \mathrm{Gal}(K_f/F)$, there is a unique Dirichlet character χ_σ on $(\mathbb{Z}/N\mathbb{Z})^\times$ such that $f^\sigma = f \otimes \chi_\sigma$. Each χ_σ can be considered as a group homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$ after identifying $(\mathbb{Z}/N\mathbb{Z})^\times$ with the multiplicative group of N-th roots of unity. Define $L := \overline{\mathbb{Q}}^{\cap \ker(\chi_\sigma)}$, where χ_σ runs through all elements σ in $\mathrm{Gal}(K_f/F)$. One has the following result ([GL, Proposition 2.1]):

Proposition 4.3.1. *L is the smallest field where all endomorphisms of A_f are defined. In particular*

$$A_f \sim_L B^n.$$

If $n = \dim(A_f)$, then B is an elliptic curve which is L-isogenous to each of its Galois conjugates over $\mathbb{Q}$. In this case B is called a $\mathbb{Q}$-*curve* (*completely defined over L*).

One calls a number field F a *field of type* $(2, 2, \ldots, 2)$ if F is the composition of some quadratic fields.

Corollary 4.3.2. *Using the notations as in Proposition* 4.2.1 *and Corollary* 4.2.2 *, if* $\dim(B) = 1$ *in* (4.1) *and χ is a quadratic character, then*

$$F = D = \mathbb{Q}$$

and K_f is a field of type $(2, 2, \ldots, 2)$.

Proof. Since the dimension of B is one, by (4.2) in Corollary 4.2.2, one must have $F = D = \mathbb{Q}$. Consequently, since χ is a quadratic character and by Proposition

4.2.1 F is generated over $\mathbb{Q}$ by numbers $a_p^2/\chi(p)$, K_f is necessarily a field of type $(2, 2, \ldots, 2)$. □

Denote by $\mathcal{C}_L(B)$ the conductor of B/L. González-Jiménez and Guitart prove the following result about $\mathcal{C}_L(B)$ ([GG, Proposition 4]):

Proposition 4.3.3. *Let $\hat{G}_{L/\mathbb{Q}}$ be the set of all characters of* $\mathrm{Gal}(L/\mathbb{Q})$. *For any $\varepsilon \in \hat{G}_{L/\mathbb{Q}}$, denote by N_ε and c_ε the level of $f \otimes \varepsilon$ and the conductor of ε respectively. Denote by v_p the discrete valuation at a prime number p. Then*

$$v_p(\mathrm{Nm}_{L/\mathbb{Q}}(\mathcal{C}_L(B))) + 2\dim(B) \sum_{\varepsilon \in \hat{G}_{L/\mathbb{Q}}} v_q(c_\varepsilon) = \dim(B) \sum_{\varepsilon \in \hat{G}_{L/\mathbb{Q}}} v_p(N_\varepsilon) \tag{4.3}$$

Using the conductor-discriminant theorem, one derives the following

Corollary 4.3.4. *Suppose either N is odd and the order of χ is less than or equal to 2 or N is square free, then*

$$\mathcal{C}_L(B)\mathfrak{f}_L^{\dim B} = N^{\dim B}, \tag{4.4}$$

where $\mathfrak{f}_L$ is the conductor of the abelian exension $L/\mathbb{Q}$.

Chapter 5
The theory of complex multiplication

The theory of complex multiplication leads to the explicit construction of abelian extensions of a quadratic imaginary field. Lang's book [Lan1] and Darmon's book [Dar, Chapter 3] are good references for this theory. We will use this theory to study the field $\mathbb{C}(X_\chi(N))$ of meromorphic functions of $X_\chi(N)$.

5.1 The function field of $X_\chi(N)$

As before, our assumption is that N is an odd square free positive integer and χ is a quadratic even character with conductor N. For simplicity, here we assume N is also a prime number. But the results obtained here are clearly valid for any square free odd integers N. Define

$$\Gamma_\chi := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N) \,\middle|\, \chi(a) = 1 \right\}$$

and

$$X_\chi(N) := \Gamma_\chi(N) \backslash \mathcal{H}^*.$$

Clearly $[\Gamma_0(N) : \Gamma_\chi(N)] = 2$ and $\Gamma_0(N)$ has the coset representatives $\Gamma_\chi(N)$ and $\gamma\Gamma_\chi(N)$ in $\Gamma_\chi(N)$, where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ is any matrix such that $\chi(d) = -1$.

Theorem 5.1.1. *The field $\mathbb{C}(X_\chi(N))$ of meromorphic functions on $X_\chi(N)$ is:*

$$\mathbb{C}(X_\chi(N)) = \mathbb{C}(j, f_\chi).$$

Here

$$f_\chi : \mathcal{H} \longrightarrow \mathbb{C},\ f_\chi(\tau) = \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} f_v(\tau), \tag{5.1}$$

where

$$f_v(\tau) = \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau(\frac{v}{N}), \tag{5.2}$$

and $\wp_\tau$ is the Weierstrass $\wp$ function with respect to the lattice generated by 1 and τ over $\mathbb{Z}$.

Proof. Each f_v is a meromorphic in $\mathcal{H}^*$. We will first prove $f_\chi(\tau)$ is invariant under $\Gamma_\chi(N)$. For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_\chi(N)$,

$$\begin{aligned} f_\chi(\gamma\tau) &= \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \frac{g_2(\gamma\tau)}{g_3(\gamma\tau)} \wp_{\gamma\tau}(\frac{v}{N}) = \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau(\frac{vc\tau + vd}{N}) \\ &= \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau(\frac{vd}{N}) \qquad (c \equiv 0 (\text{mod } N)) \\ &= \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau(\frac{v}{N}). \qquad (\chi(vd) = 1 \text{ and } v_1 d \equiv v_2 d (\text{mod } N) \text{ iff } v_1 \equiv v_2 (\text{mod } N)) \end{aligned}$$

Hence $f_\chi \in \mathbb{C}(X_\chi(N))$ and so we have the following relation:

$$\mathbb{C}(X(1)) = \mathbb{C}(j) \subset \mathbb{C}(j, f_\chi) \subset \mathbb{C}(X_\chi(N)) \subset \mathbb{C}(X(N)).$$

The extension $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ is a Galois extension with Galois group $G \cong \mathrm{SL}_2(\mathbb{Z})/(\pm I)\Gamma(N)$ and so $\mathbb{C}(X(N))/\mathbb{C}(X_\chi(N))$ is clearly a Galois extension with Galois group $G_\chi \cong \Gamma_\chi(N)/(\pm I)\Gamma(N)$.

For any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, from the same calculation as above, we have

$$f_\chi(\gamma\tau) = \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \frac{g_2(\gamma\tau)}{g_3(\gamma\tau)} \wp_{\gamma\tau}(\frac{v}{N}) = \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau(\frac{vc\tau + vd}{N}). \tag{5.3}$$

For any integers c and d, we have the following result:

$$\lim_{\mathrm{Im}(\tau)\to\infty} \wp_\tau\Big(\frac{c\tau+d}{N}\Big) = \begin{cases} -\frac{\pi^2}{3}, & N \nmid c \\ -\frac{\pi^2}{3} + N^2 \sum_{l=-\infty}^{\infty} \frac{1}{(d+lN)^2}, & N \mid c. \end{cases}$$

Since $f_\chi \in \mathbb{C}(X(N))$, we can evaluate f_χ at the cusp ∞ with respect to $\Gamma(N)$:

$$\begin{aligned} f_\chi(\infty) = \lim_{\mathrm{Im}(\tau)\to\infty} f_\chi(\tau) &= \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \lim_{\mathrm{Im}(\tau)\to\infty} \frac{g_2(\tau)}{g_3(\tau)} \wp_\tau\Big(\frac{v}{N}\Big) \\ &= \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \frac{\frac{4}{3}\pi^4}{\frac{8}{27}\pi^6}\Big(-\frac{\pi^2}{3} + N^2 \sum_{l=-\infty}^{\infty} \frac{1}{(v+lN)^2}\Big) \\ &= \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \Big(-\frac{3}{2} + \frac{9N^2}{2\pi^2} \sum_{l=-\infty}^{\infty} \frac{1}{(v+lN)^2}\Big), \end{aligned}$$

and for any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) - \Gamma_\chi(N)$, from (5.3),

$$\begin{aligned} f_\chi(\gamma\infty) &= \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \frac{g_2(\infty)}{g_3(\infty)} \lim_{\mathrm{Im}(\tau)\to\infty} \wp_\tau\Big(\frac{vc\tau+vd}{N}\Big) \\ &= \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \frac{9}{2\pi^2} \lim_{\mathrm{Im}(\tau)\to\infty} \wp_\tau\Big(\frac{vc\tau+vd}{N}\Big). \end{aligned}$$

If γ is not in $\Gamma_0(N)$, then N does not divide c, and hence

$$f_\chi(\gamma\infty) = \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \frac{9}{2\pi^2}\Big(-\frac{\pi^2}{3}\Big) = \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} -\frac{3}{2} \neq f_\chi(\infty).$$

If γ belongs to $\Gamma_0(N) - \Gamma_\chi(N)$, then N divides c and $\chi(d) = -1$ and therefore

$$\begin{aligned} f_\chi(\gamma\infty) &= \sum_{\substack{v=1 \\ \chi(v)=1}}^{N-1} \frac{9}{2\pi^2}\Big(-\frac{\pi^2}{3} + N^2 \sum_{l=-\infty}^{\infty} \frac{1}{(vd+lN)^2}\Big) \\ &= \sum_{\substack{v=1 \\ \chi(v)=-1}}^{N-1} \Big(-\frac{3}{2} + \frac{9N^2}{2\pi^2} \sum_{l=-\infty}^{\infty} \frac{1}{(v+lN)^2}\Big) \end{aligned} \tag{5.4}$$

$$\neq f_\chi(\infty).$$

The last inequality holds because of the following argument: for any integer $1 \leq v \leq N-1$, we have

$$\sum_{l=-\infty}^{\infty} \frac{1}{(v+lN)^2} = \sum_{l=0}^{\infty} \frac{1}{(v+lN)^2} + \sum_{l=0}^{\infty} \frac{1}{(lN+(N-v))^2}. \tag{5.5}$$

Because $\chi(-1)=1$, it is easy to see that $\chi(v)=1$ (respectively -1) if and only if $\chi(N-v)=1$ (respectively -1). Therefore from (5.5) and the fact $2 \mid (N-1)$,

$$\begin{aligned}\sum_{\substack{v=1\\ \chi(v)=-1}}^{N-1} \sum_{l=-\infty}^{\infty} \frac{1}{(v+lN)^2} &= \sum_{\substack{v=1\\ \chi(v)=-1}}^{N-1} \Big(\sum_{l=0}^{\infty} \frac{1}{(v+lN)^2} + \sum_{l=0}^{\infty} \frac{1}{(lN+(N-v))^2} \Big) \\ &= 2 \sum_{\substack{v=1\\ \chi(v)=-1}}^{N-1} \sum_{l=0}^{\infty} \frac{1}{(v+lN)^2},\end{aligned}$$

and similarly,

$$\begin{aligned}\sum_{\substack{v=1\\ \chi(v)=1}}^{N-1} \sum_{l=-\infty}^{\infty} \frac{1}{(v+lN)^2} &= \sum_{\substack{v=1\\ \chi(v)=1}}^{N-1} \Big(\sum_{l=0}^{\infty} \frac{1}{(v+lN)^2} + \sum_{l=0}^{\infty} \frac{1}{(lN+(N-v))^2} \Big) \\ &= 2 \sum_{\substack{v=1\\ \chi(v)=1}}^{N-1} \sum_{l=0}^{\infty} \frac{1}{(v+lN)^2}.\end{aligned}$$

In order to prove the inequality of (5.4), it is enough to prove

$$\sum_{\substack{v=1\\ \chi(v)=1}}^{N-1} \sum_{l=0}^{\infty} \frac{1}{(v+lN)^2} - \sum_{\substack{v=1\\ \chi(v)=-1}}^{N-1} \sum_{l=0}^{\infty} \frac{1}{(v+lN)^2} \neq 0 \tag{5.6}$$

i.e.

$$L(2,\chi) \neq 0. \tag{5.7}$$

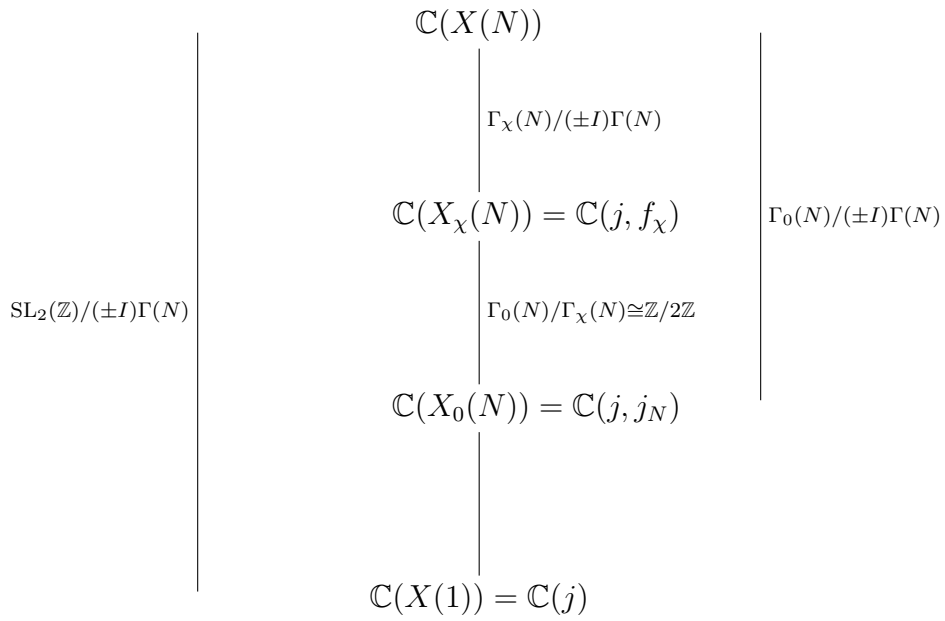
The inequality (5.7) holds because $s=2$ is within the region of absolute convergence of $L(s,\chi)$.

So an element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ can not fix the field $\mathbb{C}(j, f_\chi)$ if γ does not belong to $\Gamma_\chi(N)$. This implies:

$$\mathbb{C}(j, f_\chi) = \mathbb{C}(X_\chi(N)).$$

□

It is a well-known fact (e.g. [Kna, §11]) that the field of meromorphic functions of $X_0(N)$ and $X(1)$ are $\mathbb{C}(j, j_N)$ and $\mathbb{C}(j)$ respectively, where $j_N(\tau) = j(N\tau)$ for any $\tau \in \mathcal{H}$. Hence we have the following field tower:



(5.8)

The modular equation of f_χ over j can be computed by means of the following result ([Sch, Chapter VI]):

Theorem 5.1.2. *Let $\Gamma' \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup of level N with $-I \in \Gamma'$ and let $\gamma_1, \gamma_2, \ldots \gamma_n$ be coset representatives of Γ' in $\mathrm{SL}_2(\mathbb{Z})$, where $n = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma']$. Denote by $X'(N)$ the compact Riemann surface $\Gamma'\backslash\mathcal{H}^*$. Suppose $f \in \mathbb{C}(X'(N))$ generates $\mathbb{C}(X'(N))$ over $\mathbb{C}(j)$, then the polynomial*

$$\phi_N(x) = \prod_{v=1}^{n}(x - f \circ \gamma_v)$$

is irreducible in $\mathbb{C}(j)[x]$.

In the case of $\mathbb{C}(j, f_\chi)$, the irreducible polynomial $\phi_{\chi,N}$ in $\mathbb{C}(j)[x]$ is:

$$\phi_{\chi,N} = \prod_{v=1}^{n}(x - f_\chi \circ \gamma_v),$$

where $n = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_\chi(N)]$ and $\gamma_1, \ldots, \gamma_n$ are coset representatives of $\Gamma_\chi(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. Now we will determine such a set of representatives:

A set of left coset representatives of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ is:

$$\Big\{I, \left(\begin{smallmatrix} -s & -1 \\ 1 & 0 \end{smallmatrix}\right) \,|\, s = 0, 1, 2, \ldots, N-1\Big\}.$$

Also a set of coset representatives of $\Gamma_\chi(N)$ in Γ_0 is $\{I, \gamma_0\}$ for any fixed $\gamma_0 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ such that $\chi(d) = -1$. Hence we obtain a set A_χ of left coset representatives of $\mathrm{SL}_2(\mathbb{Z})$ in $\Gamma_\chi(N)$ as follows:

$$A_\chi = \Big\{I, \gamma_0, \left(\begin{smallmatrix} -s & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} -s & -1 \\ 1 & 0 \end{smallmatrix}\right)\gamma_0 \,|\, s = 0, 1, 2, \ldots, N-1\Big\}.$$

On the other hand, modular curves $X(1), X_1(N), X_\chi(N)$ and $X_0(N)$ are all defined over $\mathbb{Q}$. So actually $\phi_{\chi,N}(x)$ is an irreducible polynomial in $\mathbb{Q}(j)[x]$ and if we eliminate the denominators of all coefficients in $\phi_{\chi,N}$, we obtain an irreducible polynomial $\phi'_{\chi,N}$ in $\mathbb{Z}[j][x]$ where f_χ is a root.

5.2 The theory of complex multiplication

For any point $\tau \in \mathcal{H}$, define the *order* $\mathcal{O}_\tau$ associated with τ to be:

$$\mathcal{O}_\tau := \big\{\gamma \in M_2(\mathbb{Z}) \,\big|\, \det\gamma \neq 0,\ \gamma\tau = \tau\big\} \cup \big\{\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)\big\}$$

We can assign to each $0 \neq \gamma \in \mathcal{O}_\tau$ a complex number z_γ by the rule:

$$\gamma \begin{pmatrix} \tau \\ 1 \end{pmatrix} = z_\gamma \begin{pmatrix} \tau \\ 1 \end{pmatrix}.$$

This allows to regard $\mathcal{O}_\tau$ as a discrete subring of $\mathbb{C}$, which is isomorphic to the endomorphism ring of the elliptic curve $A_\tau := \mathbb{C}/\langle 1, \tau\rangle$.

The theory of complex multiplication in this setting can be stated as follows ([Dar, Theorem 3.5]):

Theorem 5.2.1. *Let $K \subset \mathbb{C}$ be a quadratic imaginary field and let τ be any point in $\mathcal{H} \cap K$. Then $K(j(\tau))$ is the ring class field H of K associated to the order $\mathcal{O}_\tau$.*

Using the notations in the above theorem, both $j(\tau)$ and $j_N(\tau)$ lie in the ring class field associated with the order $\mathcal{O}_\tau \cap \mathcal{O}_{N\tau}$. Hence we deduce from (5.8) the following result:

Proposition 5.2.2. *Let $\mathcal{O}_\tau$ and $\mathcal{O}_{N\tau} \subset K$ denote the order associated with τ and $N\tau$, respectively. Then $K(j(\tau), f_\chi(\tau))$ is a quadratic extension of the ring class field of the order $\mathcal{O}_\tau \cap \mathcal{O}_{N\tau}$.*

Let c denote the conductor of the order $\mathcal{O}_\tau \cap \mathcal{O}_{N\tau}$ and let H_c denote the corresponding ring class field. Class field theory also tells us that $K(j(\tau), f_\chi(\tau))$, which will be denoted also by $H_{c,\chi}$, is in the composite field of H_c and the ray class field of K modulo N.

Suppose first that N is inert or ramified in K. Then, except for those primes in K dividing c, there is a single prime in K ramified in $H_{c,\chi}$: the one dividing N.

Assume now that N is split in K, i.e. $N = \mathfrak{P}\overline{\mathfrak{P}}$. We need to know which primes dividing N ramify in $H_{c,\chi}$.

Let $(E, \langle Q\rangle)$ be a point on $X_0(N)$, where E is an elliptic curve defined over $\mathbb{C}$ and Q is an N-torsion point in E which generates an abelian group of order N.

Note that $X_\chi(N) \to X_0(N)$ is a finite map of degree 2; the pre-image of $(E, \langle Q\rangle)$ in $X_\chi(N)$ consists generically of two points which may be denoted as $(E, \langle Q\rangle_+^\times)$ and $(E, \langle Q\rangle_-^\times)$, where $\langle Q\rangle_+^\times$ and $\langle Q\rangle_-^\times$ are defined by

$$\langle Q\rangle_\pm^\times = \left\{ n \cdot Q \,\middle|\, n \in (\mathbb{Z}/N\mathbb{Z})^\times \text{ such that } \chi(n) = \pm 1 \right\}.$$

For any point $\tau \in \mathcal{H} \cap K$, let E_τ be the elliptic curve $\mathbb{C}/\langle 1, \tau \rangle$ with CM by some order $\mathcal{O}$ in K and let $E_\tau[\mathfrak{P}]$ denote the $\mathfrak{P}$-torsion subgroup of E_τ, i.e. $(\mathfrak{P} \cap \mathcal{O})^{-1}\langle 1, \tau \rangle / \langle 1, \tau \rangle$. It is well-known that the action of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ on $E_\tau[\mathfrak{P}]$ is unramified outside prime $\mathfrak{P}$.

On the other hand $(E_\tau, E_\tau[\mathfrak{P}]) \in X_0(N)(H_{c_0})$ for some ring class field H_{c_0} of K associated to an order in K of conductor, say, c_0. For any point $P \in E_\tau[\mathfrak{P}]$, the point (E_τ, P) belongs to $X_1(N)(H_{c_0,\mathfrak{P}})$, where $H_{c_0,\mathfrak{P}}$ is the composite of H_{c_0} and the ray class field of K modulo $\mathfrak{P}$. Since $X_\chi(N)$ lies between $X_0(N)$ and $X_1(N)$, one has the following result, which strengthens Proposition 5.2.2:

Theorem 5.2.3. *Keep the same notations as above.*

(i) $K(j(\tau), f_\chi(\tau))/K$ *is an abelian extension which is an extension of degree* 2 *over the ring class field* H_c *of order* $\mathcal{O}_\tau \cap \mathcal{O}_{N\tau}$ *with conductor* c.

(ii) Suppose N *is prime to* c *and is split in* K *with* $N = \mathfrak{P}\overline{\mathfrak{P}}$ *for some prime ideal* $\mathfrak{P}$ *and suppose the point* $(E_\tau, \langle \frac{1}{N} \rangle) \in X_0(N)$ *can be written as* $(E_{\tau'}, E_{\tau'}[\mathfrak{P}])$ *(respectively* $(E_{\tau'}, E_{\tau'}[\overline{\mathfrak{P}}])$*) for some* $\tau' \in \mathcal{H} \cap K$. *Then* $K(j(\tau), f_\chi(\tau))/K$ *lies in the composite of* H_c *and the ray class field of* K *modulo* $\mathfrak{P}$ *(respectively modulo* $\overline{\mathfrak{P}}$*). So* $K(j(\tau), f_\chi(\tau))/K$ *is ramified over primes in* K *dividing* c *and the prime* $\mathfrak{P}$ *(respectively* $\overline{\mathfrak{P}}$*).*

Remark. In the above theorem, since one of the primes in K dividing N must be ramified, the point $(E_\tau, \langle \frac{1}{N} \rangle)$ must be represented as $(E_{\tau'}, E_{\tau'}[\mathfrak{P}])$ or $(E_{\tau'}, E_{\tau'}[\overline{\mathfrak{P}}])$ for some $\tau' \in \mathcal{H}$.

Chapter 6
The Birch and Swinnerton-Dyer conjecture

In this chapter we introduce (in somewhat more detail than we did in the Introduction) the Birch and Swinnerton-Dyer (BSD) conjecture, which is one of the central problems in the study of elliptic curves. We also describe some known cases of the conjecture, focusing on those which are most relevant to the setting on which we focus in this manuscript.

6.1 The Birch and Swinnerton-Dyer conjecture

For an elliptic curve E defined over a number field F, the well-known Mordell-Weil theorem asserts that the group $E(F)$ of F-points on E is finitely generated, i.e.

$$E(F) \cong E(F)_{\mathrm{tor}} \oplus \mathbb{Z}^r \tag{6.1}$$

for some integer $r \geq 0$, where $E(F)_{\mathrm{tor}}$ is the finite subgroup of torsion points over F. In general $E(F)_{\mathrm{tor}}$ can be determined efficiently. This is because for any given prime $\mathfrak{p}$ of F over which E has good reduction, if we let $\tilde{E}/\mathbb{F}_{\mathfrak{p}}$ denote the special fiber of the Néron model of E over the integer ring of the completion of F at $\mathfrak{p}$, the reduction map

$$E(F)[m] \to \tilde{E}(\mathbb{F}_{\mathfrak{p}})$$

turns out to be a monomorphism for any integer $m \nmid \mathrm{char}(\mathbb{F}_{\mathfrak{p}})$; in practice, by utilizing several primes of F of different residual characteristic, this often allows the calculation of the whole torsion subgroup of $E(F)$.

On the other hand, the invariant r in (6.1), called the (*arithmetic*) *rank* of $E(F)$, is much more mysterious. There are very few general facts known about r, and many fundamental questions remain completely open. For example, if we fix a number field F, we ignore whether there exist elliptic curves over F with arbitrarily large rank. It is also unknown whether there exists an effective algorithm to determine r for a given elliptic curve. However, there are many fascinating conjectures on the rank of E which, if true, describe a pretty satisfactory picture about its behavior. Among them, the Birch and Swinnerton-Dyer (BSD) conjecture is the most important one.

Conjecture 6.1.1 (Birch, Swinnerton-Dyer)**.** *Let E be an elliptic curve defined over a number field F and denote by $L(E/F, s)$ the L-function of E/F. Then*

$$\mathrm{rank}(E(F)) = \mathrm{ord}_{s=1} L(E/F, s) \tag{6.2}$$

Hasse's bound on the number of points on elliptic curves over finite fields implies that $L(E/F, s)$ converges to an analytic function on the right half-plane $\mathrm{Re}(s) > \frac{3}{2}$. However, it is conjectured that $L(E/F, s)$ admits analytic continuation to the entire complex plane and has a functional equation relating its values at s and $2 - s$. It is the first part of this expectation which gives sense to the right hand side of (6.2).

So far, the full proof of (6.2) seems to have a long way to go. However, many partial results have been obtained when $\mathrm{ord}_{s=1} L(E/F, s) \leq 1$.

6.2 The BSD conjecture for $E/\mathbb{Q}$

The first breakthroughs on the BSD conjecture focused on elliptic curves over $\mathbb{Q}$ ([GZ], [Kol1]):

Theorem 6.2.1 (Gross-Zagier-Kolyvagin)**.** *Let E be an elliptic curve over $\mathbb{Q}$. If $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$, then (6.2) holds and $Ш(E/\mathbb{Q})$ is finite.*

The proof consists of the following key steps:

1. It is proved in [Wi], [TW] and [BCDT] that for any elliptic curve $E/\mathbb{Q}$ of conductor N, there is a newform $f \in S_2(\Gamma_0(N))$ such that

$$L(E/\mathbb{Q}, s) = L(f, s). \tag{6.3}$$

An important consequence is that $L(E/\mathbb{Q}, s)$ has analytic continuation to the entire complex plane and hence $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$ is well-defined.

2. For any newform $f \in S_2(\Gamma_0(N))$ with rational Fourier coefficients in its q-expansion at ∞, the Eichler-Shimura construction associates an elliptic curve $E_f/\mathbb{Q}$ of conductor N such that

$$L(E_f/\mathbb{Q}, s) = L(f, s). \tag{6.4}$$

Geometrically, the Eichler-Shimura construction provides a non-constant morphism:

$$J_0(N) \to E_f.$$

Because of (6.3) and (6.4) and Falting's proof of the Tate conjecture on abelian varieties over number fields, E_f is isogenous to E, hence we obtain a non-constant morphism:

$$\varphi_E : X_0(N) \to J_0(N) \to E, \tag{6.5}$$

where the morphism $X_0(N) \to J_0(N)$ is the Abel-Jacobi map.

3. Let K be an imaginary quadratic field with discriminant prime to N. One says K satisfies the *Heegner hypothesis* relative to N if $\mathcal{O}_K$ has a cyclic ideal $\mathcal{N}$, i.e. $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. When K satisfies the Heegner hypothesis, the functional equation of $L(E/K, s)$ has sign -1 and therefore $L(E/K, s)$ vanishes at $s = 1$ ([Dar, §3.6]).

Definition 6.2.2. *Let A be an elliptic curve with CM by an order $\mathcal{O}_c$ in K with conductor c. The point $(A, A[\mathcal{N}])$ (i.e. $(A \to A/A[\mathcal{N}])$) is called a Heegner point with CM by $\mathcal{O}_c$.*

By the theory of complex multiplication, a Heegner point P_c with CM by $\mathcal{O}_c$ is defined over the ring class field H_c of K associated with $\mathcal{O}_c$. Take the trace from H_1 to K, one can construct a point $P_K = \mathrm{Tr}_{H_1/K}(P_1)$ which is in $E(K)$. The point P_K is also called the Heegner point on E with respect to K.

4. Based on the above results, Gross and Zagier prove ([GZ]) the following result:

Theorem 6.2.3 (Gross-Zagier)**.** *For any imaginary quadratic field K satisfying the Heegner hypothesis,*

$$L'(E/K, 1) = \alpha\langle f, f\rangle\langle P_K, P_K\rangle, \tag{6.6}$$

for some $\alpha \in \mathbb{Q}^\times$, where $f \in S_2(\Gamma_0(N))$ is the newform associated with E and $\langle f, f\rangle$ and $\langle P_K, P_K\rangle$ are the Petersson inner product and the Néron-Tate height respectively.

5. Heegner points also satisfy a norm compatibility which is used by Kolyvagin to construct his Euler system to bound the p-Selmer group of E, yielding the following result([Kol1]:

Theorem 6.2.4 (Kolyvagin)**.** *Suppose P_K is non-torsion. Then the rank of $E(K)$ is one and Ш(E/K) is finite.*

6. To deduce the result on the BSD conjecture for $E/\mathbb{Q}$ when $L(E/\mathbb{Q}, s)$ has a simple zero at $s = 1$ (which also implies $\mathrm{sign}(E, \mathbb{Q}) = -1$), one proceeds as follows:

- $L(E/K, s) = L(E/\mathbb{Q}, s)L(E^{\chi_K}/\mathbb{Q}, s) = L(f, s)L(f, \chi_K, s)$, where E^{χ_K} is the twist of E by K.
- (Waldspurger, Murty-Murty) There is an imaginary quadratic field K satisfying the Heegner hypothesis relative to N and such that $L(f, \chi_K, 1) \neq 0$.
- If $L'(E/\mathbb{Q}, 1) \neq 0$, it can be shown that P_K belongs to $E(\mathbb{Q})$ (up to torsion points in $E(K)$) thanks to the following elementary result:

  Proposition 6.2.5. *Let $\tau \in \mathrm{Gal}(H/\mathbb{Q})$ be a reflection. Then*

$$\tau P_n \equiv -\mathrm{sign}(E, \mathbb{Q})\sigma P_n \pmod{E(H)_{\mathrm{tor}}}$$

for some $\sigma \in \mathrm{Gal}(H/K)$.

To extend these results on elliptic curves defined over $\mathbb{Q}$ to more general number fields, it is natural to seek a suitable non-constant map:

$$? \to E;$$

where ? is some geometric object which should be related to modular forms (or automorphic forms in a more general sense) in some way.

6.3 Zhang's result

So far little progress has been made for elliptic curves defined over number fields having complex embeddings. But for elliptic curves defined over totally real fields, Zhang ([Zh1]) generalizes to a large extent the result of Gross-Zagier-Kolyvagin.

Definition 6.3.1 (Jacquet-Langlands hypothesis)**.** *Let F be a totally real field and E/F be an elliptic curve. One says E/F satisfies the Jacquet-Langlands hypothesis if either $[F:\mathbb{Q}]$ is odd or there is a prime $\mathfrak{p}$ in F at which the automorphic form on $\mathrm{GL}_2(\mathbb{A}_F)$ attached to E is not in the principal series.*

Let K/F be a CM field. Under the Jacquet-Langlands hypothesis and the modularity of E/F, Zhang proves there exists a non-constant morphism

$$\varphi_E : \mathrm{Jac}(X) \to E \tag{6.7}$$

where X is a Shimura curve attached to an order in a quaternion algebra over F which splits at exactly one archimedean place of F, and morphism φ_E is also defined over F. The condition that the automorphic form $\pi = \otimes \pi_v$ attached to E be a principal series representation at a place v of F is satisfied precisely when E acquires good reduction over an abelian extension of F_v. For $v \nmid 2$, the meanings of various conditions on the local representations π_v in terms of the behaviour of E over F_v are summarised in the table below.

π_v	E/F_v	$\mathrm{ord}_v(\mathfrak{N})$
Unramified principal series	Good reduction over F_v	0
Principal series	Good reduction over an abelian extension of F_v	even
Steinberg	Potentially multiplicative reduction over F_v	1 or 2
Supercuspidal	Otherwise	≥ 2

Please refer to [Ge, p. 73], [Pa], [Ro, Proposition 2], [Ro2, Proposition 2 and 3] for proofs of these statements. (Note that, although in the the latter article the ground field is assumed to be $F = \mathbb{Q}$, the results remain valid for arbitrary F as the questions at issue are purely local). See [Pa] for the behaviour at places v above 2.

Building on (6.7) and applying the same ideas as in [GZ] and [Kol1], Zhang proves the following result ([Zh1, Theorem A]):

Theorem 6.3.2 (Zhang)**.** *Let F be a totally real field and E/F be an elliptic curve satisfying hypothesis (JL). If $\mathrm{ord}_{s=1}L(E/F,s) \leq 1$, then*

$$\mathrm{rank}(E(F)) = \mathrm{ord}_{s=1}L(E/F,s)$$

and Ш(E/F) is finite.

6.4 Failure of the Jacquet-Langlands hypothesis

For an elliptic curve E over a totally real field, the Jacquet-Langlands hypothesis does not always hold. When the Jacquet-Langlands hypothesis fails, the degree of $F/\mathbb{Q}$ is even and the conductor of E/F is a perfect square in F. The simplest examples are elliptic curves defined over real quadratic fields with everywhere good reduction. Such curves do exist (cf. [Cas], [Co] and [Cre] or the discussion in section 8.2 of the thesis).

When the analytic rank of E/F is 0, Longo [Lo] proves the BSD conjecture without assuming the Jacquet-Langlands hypothesis:

Theorem 6.4.1 (Longo)**.** *Let E be an elliptic curve defined over a totally real field F. If $L(E/F,1) \neq 0$, then $E(F)$ and $Ш(E/F)$ are finite.*

The proof of Longo's result uses the theory of congruence between modular forms to realize the Galois representation $E[p^n]$ in the p^n-torsion subgroup of the Jacobian of a Shimura curve X_n whose level depends on n. The Euler system of CM points on X_n is used to build p^n-torsion cohomology classes to bound the p^n-Selmer group of E/F following the method of Kolyvagin and consequently obtain the finiteness of $E(F)$ and $Ш(E/F)$.

When $\mathrm{ord}_{s=1}L(E/F,s) = 1$ and the Jacquet-Langlands hypothesis fails to hold, the problem of generalizing Zhang's theorem is still open.

To describe the situation in detail, let F be a real quadratic field and let E/F be an elliptic curve with everywhere good reduction. Let us also assume that E/F is modular so that the order of vanishing of $L(E/F,s)$ at $s=1$ is defined. Let M/F be a quadratic extension and denote by E_M/F the twist of E with respect to M/F. In this case, the sign of the functional equation of $L(E_M/F,s)$ is controlled by the two infinite places and it can be shown that:

$$\mathrm{ord}_{s=1}L(E_M/F,s) \equiv \begin{cases} 0 \pmod 2, \text{ when } M \text{ is CM or totally real} \\ 1 \pmod 2, \text{otherwise.} \end{cases} \tag{6.8}$$

Since Longo's theorem can be applied when $L(E_M/F,1) \neq 0$, only the case where M/F is neither CM nor totally real needs to be considered. Such M has only one complex place and is called an ATR (**A**lmost **T**otally **R**eal) extension, following the terminology of [Dar, §7.6].

The following conjecture lies apparently just beyond the reach of known techniques:

Conjecture 6.4.2. *Let M/F be an ATR extension. Denote by E_M the twist of E with respect to M/F. If $L'(E_M/F, 1) \neq 0$, then E_M/F has rank 1 and $Ш(E_M/F)$ is finite.*

The reason is that without the Jacquet-Langlands hypothesis, in general no modular curve or Shimura curve having a non-constant morphism to E_M is available to construct a global point in $E_M(F)$.

An important exception to this statement is provided by $\mathbb{Q}$-curves (completely) defined over F.

Chapter 7
The BSD conjecture for $\mathbb{Q}$-curves defined over real quadratic fields

Let E be an elliptic curve defined over a quadratic field F which is isogenous over F to its Galois conjugate. Such a curve is called a $\mathbb{Q}$-curve (completely) defined over F, and comes from the Shimura construction according to the work of Ribet and Serre's conjecture. In this chapter, we will prove the BSD conjecture for certain quadratic twists of E having analytic rank 1.

7.1 $\mathbb{Q}$-curves over real quadratic fields

As discussed in chapter 4, there is a positive integer N, an even Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$ and a pair f and f' of newforms in $S_2(\Gamma_\chi(N))$, such that

$$L(E/F) = L(f, s)L(f', s), \tag{7.1}$$

and there is a modular parametrization defined over F:

$$\pi_E : X_\chi(N)_F \to E. \tag{7.2}$$

We assume that N is a square-free positive odd integer, χ is a Dirichlet character of conductor N and F is a quadratic field.

Let K_f be the number field generated by the Fourier coefficients of f. It is either $\mathbb{Q}$ or a quadratic field. When $K_f = \mathbb{Q}$, the elliptic curve E is isogenous to the base change of an elliptic curve defined over $\mathbb{Q}$ and (6.2) can be shown thanks to the work of Gross, Zagier and Kolyvagin. We now assume that K_f is not equal to $\mathbb{Q}$ and hence that $K_f/\mathbb{Q}$ is a quadratic extension. Denote by σ the non-trivial element in

$\mathrm{Gal}(K_f/\mathbb{Q})$. Note that

$$f' = f^\sigma.$$

The Shimura construction gives an abelian variety A_f over $\mathbb{Q}$ associated with f.

Let τ be the unique non-trivial element in $\mathrm{Gal}(F/\mathbb{Q})$. Then there is an isogeny over F:

$$A/F \sim E \times E^\tau.$$

Denote by $\mathcal{C}_F(E)$ the conductor of E/F. The main result of [GG] shows $\mathcal{C}_F(E)$ is generated by a rational integer over $\mathcal{O}_F$, and is given by

$$\mathcal{C}_F(E)\mathfrak{f}_F = (N), \tag{7.3}$$

where $\mathfrak{f}_F$ is the conductor of F.

Suppose χ is trivial. Then K_f is real and F can be either real or imaginary. Both can happen, see [Rib5, §7]. In this case, [KL] proves (6.2) is true if $\mathrm{ord}_{s=1}L(f,s) \leq 1$.

Hence now suppose χ is non-trivial. Now K_f is an imaginary quadratic field because of (2.4). Serre proves ([Rib5, §7]) that F must be real and [Rib5] also shows $F = \overline{\mathbb{Q}}^{\ker\chi}$. Under the assumption that the even quadratic Dirichlet character on $(\mathbb{Z}/N\mathbb{Z})^\times$ is primitive, it is easy to see that $F = \mathbb{Q}(\sqrt{N})$.

Let w_N be the Fricke involution on $X_\chi(N)$ defined as $\tau \mapsto -\frac{1}{N\tau}$ when $X_\chi(N)(\mathbb{C})$ is regarded as a Riemann surface $\Gamma_\chi(N)\backslash\mathcal{H}^*$. The Fricke involution w_N induces an action on the Jacobian $J_\chi(N)$ of $X_\chi(N)$ which leaves A_f stable. When regarded as an endomorphism of $J_\chi(N)$, w_N is defined over $\mathbb{Q}(\sqrt{N})$. It can be proved ([Shi1, (2.2)], [Shi2, Theorem 7.16]) that there exists an isogeny:

$$A_f \sim (1+w_N)A_f \times (1-w_N)A_f, \tag{7.4}$$

where the isogeny is defined over F. Both factors on the right-hand side have dimension one and are conjugate one another over F. Without loss of generality, we

can assume $E = (1 + w_N)A_f$.

7.2 Main result

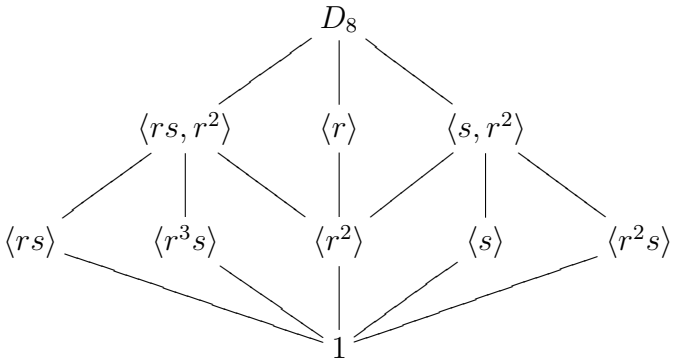
Suppose E is a $\mathbb{Q}$-curve over F of perfect square conductor $\mathfrak{N}$. The main result to be proved is the following:

Theorem 7.2.1. *Let M be an ATR extension of the real quadratic field F. Let E_M be the twist of E with respect to M/F. If $L'(E_M/F, s) \neq 0$, then $E_M(F)$ has rank one and $Ш(E_M/F)$ is finite.*

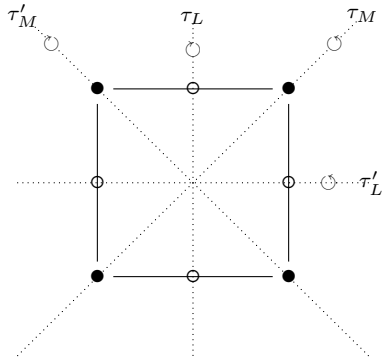
Notice that $M/\mathbb{Q}$ is not a Galois extension. Let M' be its Galois conjugate over $\mathbb{Q}$. Then the Galois closure of M is $\mathcal{M} = MM'$. It is easy to see that $\mathrm{Gal}(\mathcal{M}/\mathbb{Q}) \cong D_8$, the dihedral group of order 8, which can be expressed as

$$D_8 = \langle r, s \,\big|\, r^4 = s^2 = 1, sr = r^{-1}s \rangle.$$

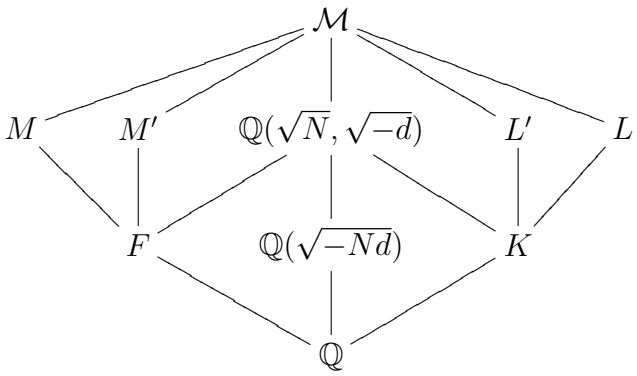
The lattice of subgroups of D_8 is given by



which can also be seen as the symmetric operations on a square:



and the corresponding tower of field extensions is



(7.5)

where

$$M = \mathcal{M}^{\tau_M},\ M' = \mathcal{M}^{\tau'_M},\ L = \mathcal{M}^{\tau_L},\ L' = \mathcal{M}^{\tau'_L}.$$

The fixed fields of the two Klein-4 groups give quadratic extensions F and K of $\mathbb{Q}$. Denote by χ_F and χ_K the corresponding Dirichlet characters with respect to $F/\mathbb{Q}$ and $K/\mathbb{Q}$ respectively. Since M/F is an ATR extension, it is easy to see that the following lemma holds:

Lemma 7.2.2. *The quadratic extension $K/\mathbb{Q}$ is imaginary.*

Extensions M and M' over F correspond to two Galois characters

$$\chi_M, \chi'_M : G_F \to \{\pm 1\}.$$

Similarly, extensions L and L' over K correspond to two Galois characters

$$\chi_L, \chi'_L : G_K \to \{\pm 1\}.$$

Using class field theory, these four characters can also be viewed as Hecke characters on $\mathbb{A}_F^\times$ and $\mathbb{A}_K^\times$ respectively. One has the following properties of these characters:

Proposition 7.2.3. (1) *The characters χ_M, χ'_M, χ_L and χ'_L have the following relations:*

$$\chi_M \chi'_M = \chi_K \circ \mathrm{Nm}_{\mathbb{A}_F^\times} \text{ and } \chi_L \chi'_L = \chi_F \circ \mathrm{Nm}_{\mathbb{A}_K^\times}, \tag{7.6}$$

where $\mathrm{Nm}_{\mathbb{A}_F^\times} : \mathbb{A}_F^\times \to \mathbb{A}_\mathbb{Q}^\times$ and $\mathrm{Nm}_{\mathbb{A}_K^\times} : \mathbb{A}_K^\times \to \mathbb{A}_\mathbb{Q}^\times$ are the norms on idèles.

(2) *The central character of χ_M and χ'_M is χ_K, and χ_F is the central character of χ_L and χ'_L.*

(3)

$$\mathrm{Ind}_F^\mathbb{Q} \chi_M = \mathrm{Ind}_F^\mathbb{Q} \chi'_M = \mathrm{Ind}_K^\mathbb{Q} \chi_L = \mathrm{Ind}_K^\mathbb{Q} \chi'_L. \tag{7.7}$$

Proof. The proof of (7.7) is easy: they are all two-dimensional representation of D_8, which has a single irreducible two-dimensional representation.

The proof of (7.6) is an application of class field theory and Kummer theory. Hecke characters can be viewed as characters on ideals. Note M, M', L and L' are Kummer extensions over F and K respectively. M and M' can be written as $\mathbb{Q}(\sqrt{\alpha})$ and $\mathbb{Q}(\sqrt{\alpha'})$ respectively, where α' is the Galois conjugate of α. Clearly $\alpha\alpha'$ is the discriminant of K up to a square factor. Denote by $\left(\frac{\cdot}{\cdot}\right)_2$ the second high power residue symbol. For any prime $\mathfrak{p}$ in F which is unramified in both M and M',

$$\chi_M \chi'_M(\mathfrak{p}) = \left(\frac{\alpha}{\mathfrak{p}}\right)_2 \left(\frac{\alpha'}{\mathfrak{p}}\right)_2 = \left(\frac{\alpha\alpha'}{\mathfrak{p}}\right)_2 = \chi_K(\mathrm{Nm}_{F/\mathbb{Q}}(\mathfrak{p})).$$

A similar argument can be applied to χ_L and χ'_L.

As for part (2), (7.6) implies that the central character of L restricted to the group of norms from K is equal to χ_F. Class field theory implies that this central

character differs from χ_F by a power of χ_K. But the central character of χ_L cannot be $\chi_F\chi_K$ since this is an odd Dirichlet character and the central character of a finite order Hecke character of an imaginary quadratic field is necessarily even, because the map from the group of components of $\mathbb{R}^\times$ to the group of components of $\mathbb{C}^\times$ is trivial. □

Lemma 7.2.4. *The field K in* (7.5) *satisfies the Heegner Hypothesis.*

Proof. Staring at the field tower (7.5), it follows from the relation of relative discriminants ([Neu, Corollary (2.10)]) that

$$\mathrm{disc}(M/\mathbb{Q}) = \mathrm{Nm}_{F/\mathbb{Q}}(\mathrm{disc}(M/F)) \cdot \mathrm{disc}(F)^2$$
$$\mathrm{disc}(L/\mathbb{Q}) = \mathrm{Nm}_{K/\mathbb{Q}}(\mathrm{disc}(L/K)) \cdot \mathrm{disc}(L)^2.$$

From relation (7.6), one has

$$\mathrm{disc}(M/\mathbb{Q}) \cdot \mathrm{disc}(K) = \mathrm{disc}(F) \cdot \mathrm{disc}(L/\mathbb{Q}).$$

Hence

$$\mathrm{disc}(F) \cdot \mathrm{Nm}_{F/\mathbb{Q}}(\mathrm{disc}(M/F)) = \mathrm{disc}(K) \cdot \mathrm{Nm}_{K/\mathbb{Q}}(\mathrm{disc}(L/K)). \tag{7.8}$$

Define

$$\mathcal{N}_{\mathrm{split}} = \left(\frac{N}{\gcd(N, \mathrm{disc}(K))}, \mathrm{disc}(L/K)\right), \mathcal{N}_{\mathrm{ram}} = \left(\gcd(N, \mathrm{disc}(K)), \sqrt{\mathrm{disc}(K)}\right)$$

Then from (7.8), $\mathcal{N} := \mathcal{N}_{\mathrm{split}} \cdot \mathcal{N}_{\mathrm{ram}}$ has norm N with desired property. □

Another key ingredient to prove Theorem 7.2.1 is the following result of Tian, Yuan, Zhang and Zhang ([YZZ], [Zh2]).

Theorem 7.2.5 (Tian-Yuan-Zhang-Zhang)**.** *Let K be an imaginary field satisfying Heegner hypothesis and $\chi_K : \mathbb{A}_K^\times \to \mathbb{C}^\times$ be a finite Hecke character of K such that*

$$\chi_K\big|_{\mathbb{A}_\mathbb{Q}^\times} \cdot \chi = 1,$$

where χ is the nebentypus of f. Then

- *The order of vanishing of the L-function $L(f/K, \chi_K, s)$ at $s = 1$ is odd.*
- *If $L'(f/K, \chi_K, s) \neq 0$, then $(A(K^{\mathrm{ab}}) \otimes \mathbb{C})^{\chi_K}$ has rank one over $K_f \otimes_{\mathbb{Q}} \mathbb{C}$ and $Ш(A/K^{\mathrm{ab}})^{\chi_K}$ is finite, where K^{ab} is the maximal abelian extension of K.*

Proof (of Theorem 7.2.1). By (7.1) and Artin's formalism,

$$L(E_M/F, s) = L(E, \chi_M, s) = L(f \otimes \chi_M/F, s) = L(f \otimes \mathrm{Ind}_F^{\mathbb{Q}} \chi_M, s).$$

From (7.7),

$$L(f \otimes \mathrm{Ind}_F^{\mathbb{Q}} \chi_M, s) = L(f \otimes \mathrm{Ind}_K^{\mathbb{Q}} \chi_L, s) = L(f/K, \chi_L, s).$$

Hence

$$L'(E_M/F, 1) = L'(f \otimes \chi_L/K, 1) = L'(f^\sigma/K, \chi_L, 1) \neq 0.$$

The last inequality holds because of $L'(E_M/F, 1) \neq 0$ by assumption. This implies the L-function

$$L(A/K, \chi_L, s) = L(f \otimes \chi_L/K, s) L(f^\sigma \otimes \chi_L/K, s)$$

vanishes at $s = 1$ to order $2 = [K_f : \mathbb{Q}]$. Hence by Theorem 7.2.5, the rank of $A(L)^-$ is two, where $A(L)^-$ denotes the subgroup of $A(L)$ of points whose trace to K is trivial. Hence the Galois representation $\mathrm{Ind}_K^{\mathbb{Q}} \chi_L$ occurs in $A(\overline{\mathbb{Q}}) \otimes \mathbb{C}$ with multiplicity 2. Hence again from (7.7),

$$\mathrm{rank}(A(M)^-) = 2.$$

Since $F \subset M$ and A is isogenous to E^2 over F, it follows that

$$\mathrm{rank}(E(M)^-) = \mathrm{rank}(E_M(F)) = 1.$$

Similarly, $Ш(E_M/F)$ is finite. □

Chapter 8
Heegner points on Shimura's elliptic curves

The crucial ingredient in the proof of the Theorem 7.2.1 is the use of Heegner points (via the Theorem 7.2.5). In this chapter, we will construct explicitly the Heegner points via the modularity (7.2).

8.1 An explicit Heegner point construction

Using the notation in the field tower (7.5), let

$$\hat{\mathcal{O}}_K^\times := \prod_v \mathcal{O}_v^\times$$

denote the maximal compact subgroup of the group $\mathbb{A}_{K,\mathrm{fin}}^\times$ of finite idèles of K. Given a rational integer $c \geq 1$, $(c, N) = 1$, we define

$$U_c = \hat{\mathbb{Z}}^\times (1 + c\hat{\mathcal{O}}_K)\mathbb{C}^\times \subset \mathbb{A}_K^\times.$$

By class field theory, the quotient $G_c := \mathbb{A}_K^\times/(K^\times U_c)$ is identified with $\mathrm{Gal}(H_c/K)$, where H_c is the *ring class field* of K of conductor c.

As a piece of notation, we shall write H_c for the ring class field attached to the order in K of conductor $c \geq 1$ and write $K_{\mathfrak{a}}$ for the ray class field of conductor $\mathfrak{a}$.

Define

$$U_c^+ = \{\beta \in U_c \text{ such that } (\beta)_{\mathcal{N}} \in \ker(\chi) \subset (\mathbb{Z}/N\mathbb{Z})^\times\},$$

$$U_c^- = \{\beta \in U_c \text{ such that } (\beta)_{\overline{\mathcal{N}}} \in \ker(\chi) \subset (\mathbb{Z}/N\mathbb{Z})^\times\},$$

and $\tilde{U}_c = U_c^+ \cap U_c^-$. Here $(\beta)_{\mathcal{N}}$ denotes the image of the local term of the idèle β at $\mathcal{N}$ in the quotient $\mathcal{O}_{\mathcal{N}}^\times/(1+\mathcal{N}\cdot\mathcal{O}_{\mathcal{N}}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$. Similarly for $\overline{\mathcal{N}}$. This way we can regard the character χ as having source either $\mathcal{O}_{\mathcal{N}}^\times$ or $\mathcal{O}_{\overline{\mathcal{N}}}^\times$.

Set

$$\tilde{G}_c := \mathbb{A}_K^\times/(K^\times \tilde{U}_c) = \mathrm{Gal}(\tilde{H}_c/K),$$

where $\tilde{H}_c$ is a biquadratic extension of the ring class field H_c. It can be written as $\tilde{H}_c = L_c L_c'$, where L_c (resp. L_c') is the class field attached to U_c^+ (resp. U_c^-).

Theorem 8.1.1. *The relative discriminant of L/K factors as $d(L/K) = c\cdot\mathcal{N}$, where $c = 2^t c_0$ is a positive integer for some $0 \le t \le 3$ and odd square-free integer c_0 such that $L \subset L_c$ and $L' \subset L_c'$ and thus $\mathcal{M} \subset \tilde{H}_c$.*

Proof. In order to avoid the distraction from the main purpose of this section, the proof is postponed to the last section. □

We now explain how to construct a degree zero divisor on $X_\chi(N)$ defined over $\tilde{H}_c$. To do this, let A_c be an elliptic curve satisfying

$$\mathrm{End}(A_c) = \mathcal{O}_c,$$

where $\mathcal{O}_c := \mathbb{Z} + c\mathcal{O}_K$ is the order in K of conductor c. Such a curve, along with its endomorphisms, may be defined over the ring class field H_c. The module $A_c[\mathcal{N}]$ of $\mathcal{N}$-torsion points is therefore defined over H_c, yielding a point

$$P_c := [A_c, A_c[\mathcal{N}]] \in X_0(N)(H_c).$$

The action of $G_{H_c} := \mathrm{Gal}(\overline{\mathbb{Q}}/H_c)$ on the points of the group scheme $A_c[\mathcal{N}]$ gives a Galois representation

$$\rho_{\mathcal{N}} : G_{H_c} \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times.$$

The composition of $\rho_{\mathcal{N}}$ with the nebentypus character χ is a quadratic character of G_{H_c}, which cuts out the quadratic extension L_c of H_c. The point P_c lifts to two points P_c^+ and P_c^- in $X_\chi(N)(L_c)$ which are interchanged by the action of $\mathrm{Gal}(L_c/H_c)$; we do not specify the order in which these points are to be taken. Similarly, we can replace the module $A_c[\mathcal{N}]$ by $A_c[\overline{\mathcal{N}}]$, mimic the above construction and obtain points $P_c'^+$ and $P_c'^-$ defined over L_c'.

Definition 8.1.2. *Let*

$$\mathrm{CM}(c) = \bigcup \{P_c^+, P_c^-, P_c'^+, P_c'^-\} \subset X_\chi(N)(\tilde{H}_c)$$

be the set of Heegner points on $X_\chi(N)$ obtained by letting A_c run over all isomorphism classes of elliptic curves with CM by $\mathcal{O}_c$.

If we let $h(O_c)$ denote the cardinality of the group $\mathrm{Pic}(\mathcal{O}_c)$ of classes of locally free ideals of $\mathcal{O}_c$, the cardinality of $\mathrm{CM}(c)$ is $4h(\mathcal{O}_c)$. In fact, $\mathrm{CM}(c)$ is naturally the disjoint union of the two subsets $\mathrm{CM}(c) \cap X_\chi(N)(L_c)$ and $\mathrm{CM}(c) \cap X_\chi(N)(L_c')$, each of cardinality $2h(\mathcal{O}_c)$.

A Heegner point $P \in \mathrm{CM}(c)$ of conductor c may be described by a triple $([\mathfrak{a}], \mathfrak{n}, t)$, where

- $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_c)$ is the class of an invertible $\mathcal{O}_c$-module of K,
- $\mathfrak{n}$ is an integral ideal of $\mathcal{O}_c$ such that the quotient $\mathcal{O}_c/\mathfrak{n}$ is cyclic of order N,
- t is an orbit for the action of $\ker(\chi)$ of an element of order N in $\mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$.

Let $\tilde{C}$ be the quotient of the ray class group of K of conductor $c\mathcal{N}$ for which Artin's reciprocity map of global class field theory furnishes a canonical isomorphism

$$\mathrm{rec} : \tilde{C} \xrightarrow{\sim} \mathrm{Gal}(\tilde{H}_c/K).$$

Let $\mathcal{O} = \mathcal{O}_c$ denote the order of conductor c in K. There are natural exact sequences, sitting in the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(\tilde{H}_c/H_c) & \longrightarrow & \mathrm{Gal}(\tilde{H}_c/K) & \xrightarrow{\mathrm{res}_{\tilde{H}_c/H_c}} & \mathrm{Gal}(H_c/K) & \longrightarrow & 1 \\ & & \downarrow \mathrm{rec} & & \downarrow \mathrm{rec} & & \downarrow \mathrm{rec} & & \\ 1 & \longrightarrow & \langle [\beta_0], [\beta_0'] & \longrightarrow & \tilde{C} & \longrightarrow & \mathrm{Pic}(\mathcal{O}) & \longrightarrow & 1, \end{array}$$

where the vertical arrows are isomorphisms. Here, $\beta_0 \in \mathcal{O}_{\mathcal{N}}^\times$ and $\beta_0' \in \mathcal{O}_{\overline{\mathcal{N}}}^\times$ are elements such that $\chi(\beta_0) = -1$ and $\chi(\beta_0') = -1$. Artin's reciprocity map induces an isomorphism

$$\mathrm{Gal}(\tilde{H}_c/H_c) \cong \mathcal{O}_{\mathcal{N}}^\times/\ker(\chi) \times \mathcal{O}_{\overline{\mathcal{N}}}^\times/\ker(\chi) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

We thus can formally write elements of $\tilde{C}$ as classes of *enhanced ideals*, which are defined as elements of the form $\underline{\mathfrak{b}} := \beta_{\mathcal{N}}\beta_{\overline{\mathcal{N}}} \prod_{\wp \nmid N} \wp^{n_\wp}$, taken up to principal ideals (b) with $b \in K^\times$. Here $\beta_{\mathcal{N}}$ and $\beta_{\overline{\mathcal{N}}}$ belong to $K_{\mathcal{N}}^\times/\ker(\chi)$ and $K_{\overline{\mathcal{N}}}^\times/\ker(\chi)$ respectively, $\wp$ runs over all prime invertible ideals of $\mathcal{O}$ not dividing N, and the exponents $n_\wp$ are integers which are almost all zero. We say an enhanced ideal is *integral* if $\beta_{\mathcal{N}}$ and $\beta_{\overline{\mathcal{N}}}$ have representatives in $\mathcal{O}_{\mathcal{N}}^\times$ and $\mathcal{O}_{\overline{\mathcal{N}}}^\times$ respectively, and $n_\wp \geq 0$ for all $\wp$. The image of the class $\underline{\mathfrak{b}}$ in $\mathrm{Pic}(\mathcal{O})$ is simply the class of the ideal $\mathfrak{b} = \mathcal{N}^{\mathrm{ord}_{\mathcal{N}}(\beta_{\mathcal{N}})}\overline{\mathcal{N}}^{\mathrm{ord}_{\overline{\mathcal{N}}}(\beta_{\overline{\mathcal{N}}})} \prod_{\wp \nmid N} \wp^{n_\wp}$ generated by it.

By Shimura's reciprocity law (cf. e.g. [Shi2, §5.3], [Lan1, §10.2]),

$$\mathrm{rec}(\underline{\mathfrak{b}})(D) = \underline{\mathfrak{b}}^{-1} \star D \tag{8.1}$$

for all $\underline{\mathfrak{b}} \in \tilde{C}$ and all divisors $D \in J_\chi(N)(\tilde{H}_c)$ supported on $\mathrm{CM}(c)$.

On the left hand side we make use of the natural Galois action of $\mathrm{Gal}(\tilde{H}_c/K)$ on $J_\chi(N)(\tilde{H}_c)$, via Artin's reciprocity isomorphism. On the right hand side, a class

$[\underline{\mathfrak{b}}] \in \tilde{C}$ acts on $\mathrm{CM}(c)$ by the rule

$$\underline{\mathfrak{b}} \star P = ([\mathfrak{a}\mathfrak{b}^{-1}], \mathfrak{n}, \varphi_{\mathfrak{b}}(\beta_{\mathcal{N}} t)), \tag{8.2}$$

where $P = ([\mathfrak{a}], \mathfrak{n}, t) \in \mathrm{CM}(c)$, $\underline{\mathfrak{b}} = \beta_{\mathcal{N}}\beta_{\overline{\mathcal{N}}} \prod_{\wp \nmid N} \wp^{n_\wp}$ is an integral representative of its class and $\varphi_{\mathfrak{b}} : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathfrak{b}^{-1}$ is the natural projection map. Writing $P = [\tau] \in X_\chi(N)(\mathbb{C})$ for some $\tau \in \mathcal{H}$, let $\gamma_{\underline{\mathfrak{b}}} \in \mathrm{GL}_2^+(\mathbb{Q})$ be such that $\underline{\mathfrak{b}} \star P = [\gamma_{\underline{\mathfrak{b}}}\tau]$.

Besides this action, there is also the diamond involution W_χ, acting on $P = [\tau] \in X_\chi(N)(\mathbb{C})$ as $W_\chi([\tau]) = [\gamma_\chi \tau]$ and on $P = ([\mathfrak{a}], \mathfrak{n}, t) \in \mathrm{CM}(c)$ as

$$W_\chi(P) = ([\mathfrak{a}], \mathfrak{n}, dt), \quad \text{for } \gamma_\chi = \left(\begin{smallmatrix} a & b \\ Nc & d \end{smallmatrix}\right) \in \Gamma_0(N) \setminus \Gamma_\chi(N). \tag{8.3}$$

The cardinality of $\mathrm{CM}(c)$ is $4h(\mathcal{O})$ and it is acted on freely and transitively by the group $\langle W_N, W_\chi \rangle \times \tilde{C}_{\mathcal{M}}$, where we let $\tilde{C}_{\mathcal{M}} := \mathrm{rec}^{-1}(\mathrm{Gal}(\tilde{H}_c/\mathcal{M})) \subset \tilde{C}_K$. Note that the restriction map $\mathrm{res}_{\tilde{H}_c/H_c}$ induces an isomorphism $\tilde{C}_{\mathcal{M}} \cong \mathrm{Pic}(\mathcal{O}) \cong \mathrm{Gal}(H_c/K)$.

It is our aim now to define a point $P_M \in E(M)$ (and thus also, by conjugation over F, a point $P_{M'} \in E(M')$) on the elliptic curve E, rational over the ATR extension M/F. We shall construct P_M as a suitable linear combination of certain points $P_L \in A(L)$ and $P_{L'} \in A(L')$ on the abelian surface $A = \mathrm{Res}_{F/\mathbb{Q}}(E)$. These points are defined as the trace to L of the projection of $P_c^+ \in X_\chi(N)(L_c)$ (respectively of $P_c'^+ \in X_\chi(N)(L_c')$) on A.

Before doing so, we first observe that choosing $P_c^- = W_\chi(P_c^+)$ instead of P_c^+ (and similarly $P_c'^-$ instead of $P_c'^+$) is unimportant for our construction, as the next lemma shows that both lead to the same point on A up to sign and torsion. Recall the canonical projection $\pi_f : J_\chi(N) \to A$ defined over $\mathbb{Q}$, which can be composed with the natural embedding of $X_\chi(N)$ into its jacobian $J_\chi(N)$ given by the map $P \mapsto P - i\infty$. By an abuse of notation, we continue to denote by π_f this composition.

Lemma 8.1.3. *For any $P \in X_\chi(N)(\overline{\mathbb{Q}})$, the point $\pi_f(P) + \pi_f(W_\chi(P))$ belongs to $A(F)_{\mathrm{tors}}$.*

Proof. There is a natural decomposition $S_2(\Gamma_\chi(N)) = S_2(\Gamma_0(N)) \oplus S_2(\Gamma_0(N), \chi)$ corresponding to the eigenspaces of eigenvalue ± 1 with respect to the action of the involution W_χ. The rule $f(z) \mapsto f(z)dz$ yields an identification of $S_2(\Gamma_\chi(N))$ with the space of holomorphic differentials on $X_\chi(N)(\mathbb{C})$. Via this isomorphism, $\pi_f^* H^0(\Omega^1_A)$ is contained in $S_2(\Gamma_0(N), \chi)$. Consequently, $\pi_f(P - i\infty) = -\pi_f(W_\chi(P - i\infty))$ and

$$\begin{aligned}\pi_f(P) + \pi_f(W_\chi(P)) &= \pi_f(P - i\infty) + \pi_f(W_\chi(P) - i\infty) \\ &= \pi_f(P - i\infty) + \pi_f(W_\chi(P) - W_\chi(i\infty)) + \pi_f(W_\chi(i\infty) - i\infty) \\ &= \pi_f(W_\chi(i\infty) - i\infty).\end{aligned}$$

This last expression is a torsion point on $A(F)$ by the Manin-Drinfeld theorem which asserts that degree zero cuspidal divisors on a modular curve give rise to torsion elements in its Jacobian. □

We now set

$$P_L = \mathrm{Tr}_{L_c/L}(\pi_f(P_c^+)) \in A(L).$$

Note that $\tau_M(P_L)$ is either equal to $\mathrm{Tr}_{L'_c/L'}(\pi_f(P_c'^+))$ or to $\mathrm{Tr}_{L'_c/L'}(\pi_f(P_c'^-))$. Without loss of generality, assume that $\tau_M(P_L) = \mathrm{Tr}_{L'_c/L'}(\pi_f(P_c'^+))$ and denote it by P'_L.

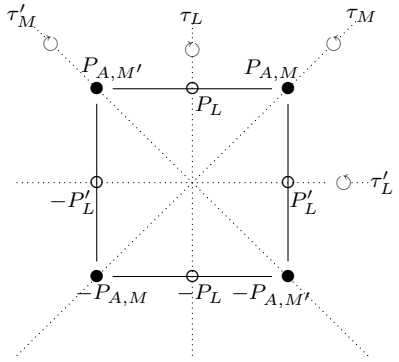
Set

$$u = \begin{cases} 2 & \text{if } K = \mathbb{Q}(\sqrt{-1}) \text{ and } c = 1; \\ 3 & \text{if } K = \mathbb{Q}(\sqrt{-3}) \text{ and } c = 1; \\ 1 & \text{otherwise,} \end{cases}$$

and define

$$P_{A,M} := \frac{1}{u}(P_L + P'_L), \qquad P_{A,M'} := \frac{1}{u}(P_L - P'_L).$$

The construction of the point $P_{A,M}$ is illustrated in the figure below.



This figure suggests –and it is indeed easy to check– that

$$P_{A,M} \in A(M), \qquad P_{A,M'} \in A(M').$$

Recall that the morphism $\varphi_F : A_F \longrightarrow E$ is defined over $F \subset M$, and therefore that the point

$$P_M := \varphi_F(P_{A,M})$$

belongs to $E(M)$. As a by-product of our explicit construction we obtain the following analytic formula for calculating the point P_M.

Theorem 8.1.4. *Let $\tau_c, \tau'_c \in \mathcal{H}$ be elements representing the Heegner points $P_c^+, P_c'^+ \in X_\chi(N)(\tilde{H}_c)$. Set*

$$z_M = \sum_{\underline{\mathfrak{b}} \in \tilde{C}_{\mathcal{M}}} \left[\int_{i\infty}^{\gamma_{\underline{\mathfrak{b}}}\tau_c} (f_E(\tau) + f_E\big|_{W_N}(\tau))\, d\tau + \int_{i\infty}^{\gamma_{\underline{\mathfrak{b}}}\tau'_c} (f_E(\tau) + f_E\big|_{W_N}(\tau))\, d\tau \right]. \quad (8.4)$$

Then $P_M = \eta(z_M)$ where η is the Weierstrass parametrization

$$\eta : \mathbb{C}/\Lambda_E \longrightarrow E(\mathbb{C}), \quad \eta(z) = (\wp(z), \wp'(z)). \quad (8.5)$$

Here, $\wp$ is the Weierstrass function associated with the lattice of periods

$$\Lambda_E := \left\{ \int_\delta (f_E + f_E\big|_{W_N}) d\tau \right\}$$

where $\delta \in H_1(X_\chi(\mathbb{C}), \mathbb{Z})$ *runs over the cycles of* $X_\chi(\mathbb{C})$ *such that* $\int_\delta (f_E - f_E\big|_{W_N}) d\tau = 0$.

8.2 Numerical examples

$\mathbb{Q}$-curves having everywhere good reduction over real quadratic fields were investigated first by Shimura and so commonly referred to as Shimura elliptic curves. Cremona provided in [Cre] the list of all primes $N \leq 1000$ for which there is a modular form $f \in S_2(\Gamma_0(N), \chi_N)$ with quadratic fourier coefficients. Here we use PARI ([PA]) to extend the data to primes $1 \leq N \leq 5000$ with $K_f = \mathbb{Q}(\sqrt{-d})$:

N	29	37	41	109	157	229	257	337	349	373	397	421
d	5	1	2	3	1	5	2	2	5	1	1	7
N	461	509	877	881	997	1069	1709	1861	2657	4481	4597	
d	5	5	1	2	3	1	5	5	2	11	1	

Furthermore, according to Cremona, Dembelé, Elkies and Pinch, there are only four primes $N = 509, 853, 929, 997$ in the range $[1, 1000]$ for which there exists a non-$\mathbb{Q}$-curve but with everywhere good reduction over $\mathbb{Q}(\sqrt{N})$.

For $N = 29, 37, 41$, since $S_2(\Gamma_0(N), \chi_N)$ is 2-dimensional, there is a unique Shimura elliptic curve defined over $F = \mathbb{Q}(\sqrt{N})$ up to isogeny over F.

The aim of this section is providing numerical examples to illustrate Theorem 8.1.1 which we have gathered by explicitly computing points P_M and for several ATR extensions M/F on each of the three elliptic curves mentioned above. The computation of Heegner points P_M was performed with the software package PARI [PA] by exploiting formula (8.4) and the material of [Shio] and [Cre, Ch. 6]. These

data will also be used to compare them with the points generated by the method proposed by Darmon and Logan [DL].

In the tables below, following almost the same notation as in [DL, §3], $M = F(\beta)$, $\beta^2 \in F$, is an ATR field extension of F of absolute discriminant $D_M = \mathrm{Nm}_{F/\mathbb{Q}}(\mathrm{disc}(M/F))$ (Note that K is used in [DL] to denote M here). We also let L/K denote the quadratic extension sitting in the Galois closure of M as in the field diagram (7.5), and set $D_K = \mathrm{disc}(K/\mathbb{Q})$ and $D_L = \mathrm{Nm}_{K/\mathbb{Q}}(\mathrm{disc}(L/K))$. Finally, $u = \beta^2$ or $4\beta^2$ depending on whether $\beta^2 \in \mathbb{Z} + \mathbb{Z}\sqrt{N}$ or not.

1. $N = 29$**.** Set $\delta = 2 + \omega = (5 + \sqrt{29})/2$. Shiota's Weierstrass equation for E_N is

$$E_{29} : y^2 + xy + \delta^2 y = x^3,$$

whose discriminant is $\Delta_{29} = -\delta^{10}$.

D_M	τ	β^2	P_M
-7	$\frac{15+\sqrt{-7}}{2\cdot 29}$	$-1+\omega$	$[2]\Big(-\frac{5}{32}\sqrt{29u}-\frac{27}{32}\sqrt{u}+\frac{53}{8}+\frac{5}{4}\sqrt{29},\ -\frac{5}{64}\sqrt{29u}-\frac{161}{48}-\frac{27}{64}\sqrt{u}-\frac{5}{8}\sqrt{29}\Big)$
-16	$\frac{5+2\sqrt{-1}}{29}$	$2+\omega$	$[2]\Big(\frac{12}{49}\sqrt{29u}+\frac{436}{49}+\frac{65}{49}\sqrt{u}+\frac{82}{49}\sqrt{29},\ \frac{464}{343}\sqrt{29u}+\frac{24587}{686}+\frac{2497}{343}\sqrt{u}+\frac{4561}{686}\sqrt{29}\Big)$
-23	$\frac{21+\sqrt{-23}}{2\cdot 29}$	$17+8\omega$	$[2]\Big(\frac{165}{23}+\frac{31}{23}\sqrt{29},\ \frac{9497}{2116}\sqrt{u}+\frac{1767}{2116}\sqrt{u}\sqrt{29}-\frac{951}{92}-\frac{177}{92}\sqrt{29}\Big)$
-35_1	$\frac{9+\sqrt{-35}}{2\cdot 29}$	$19+9\omega$	$[2]\Big(\frac{14947}{53868}\sqrt{29u}+\frac{1548911}{80802}+\frac{240995}{161604}\sqrt{u}+\frac{96439}{26934}\sqrt{29},\ \frac{74583313}{32482404}\sqrt{29u}+\frac{133892213}{10827468}\sqrt{u}+\frac{862284017}{5413734}+\frac{480249637}{16241202}\sqrt{29}\Big)$
-35_2	$\frac{9+\sqrt{-35}}{2\cdot 29}$	$4+3\omega$	$[2]\Big(-\frac{339}{5684}\sqrt{29u}+\frac{883}{2842}-\frac{1775}{5684}\sqrt{u}+\frac{209}{2842}\sqrt{29},\ -\frac{53387}{1153852}\sqrt{29u}+\frac{5737}{19894}+\frac{28899}{576926}\sqrt{29}-\frac{9991}{39788}\sqrt{u}\Big)$
-59	$\frac{17+\sqrt{-59}}{2\cdot 29}$	$61+28\omega$	$[2]\Big(\frac{5093}{52038}+\frac{135}{5782}\sqrt{29},\ \frac{35703391}{64475082}\sqrt{u}+\frac{6641449}{64475082}\sqrt{29u}-\frac{353803}{52038}-\frac{7295}{5782}\sqrt{29}\Big)$
-63	$\frac{13+3\sqrt{-7}}{58}$	3ω	$[2]\big(\frac{26327}{169}\sqrt{29u}+\frac{877497}{169}+\frac{141773}{169}\sqrt{u}+\frac{162951}{169}\sqrt{29},\ -\frac{49494863}{2197}\sqrt{29u}-\frac{3299520153}{4394}-\frac{266537981}{2197}\sqrt{u}-\frac{612705527}{4394}\sqrt{29}\big)$
-64	$\frac{10+4\sqrt{-1}}{29}$	$4+2\omega$	$[2]\Big(\frac{4169198204}{100436309}\sqrt{29u}+\frac{72319314464}{100436309}+\frac{22449388076}{100436309}\sqrt{u}+\frac{13431238560}{100436309}\sqrt{29},$ $\frac{11963390607709696}{5420447160421}\sqrt{29u}+\frac{7156690316570624}{186911971049}+\frac{2221547130507776}{186911971049}\sqrt{u}+\frac{38539928458137600}{5420447160421}\sqrt{29}\Big)$
-80	$\frac{3+2\sqrt{-5}}{29}$	$1+\omega$	$[2]\Big(\frac{75784715911}{140152297922}\sqrt{29u}+\frac{710531714168}{70076148961}+\frac{409063432719}{140152297922}\sqrt{u}+\frac{131982297126}{70076148961}\sqrt{29},$ $-\frac{13833377427880917}{37100976153613918}\sqrt{29u}-\frac{441793918069863523}{530013945051627 4}-\frac{745200169674923005}{37100976153613918}\sqrt{u}-\frac{574038958928716191}{37100976153613918}\sqrt{29}\Big)$
-91	$\frac{5+\sqrt{-91}}{229}$	$7+5\omega$	$[2]\Big(\frac{949312718319}{25098316471684}\sqrt{29u}+\frac{51776586949723}{363925588839418}+\frac{17987557631105}{363925588839418}\sqrt{29}+\frac{141288587920885}{727851177678836}\sqrt{u},$ $\frac{10194037543394049672 29}{5287287021858945214428 4}\sqrt{29u}+\frac{1247932951860721104 73}{9116012106653353817 98}+\frac{3964832398274695988 75}{2643643510929472607 2142}\sqrt{29}+\frac{1972029475618364365 95}{1823202421330670763596}\sqrt{u}\Big)$
-175	$\frac{17+5\sqrt{-7}}{58}$	$-5+5\omega$	$[2]\big(\frac{26243089}{2805005}+\frac{4996259}{2805005}\sqrt{29},-\frac{543541975531}{84037949800}\sqrt{u}-\frac{4032863103}{3361517992}\sqrt{29u}-\frac{128221313}{11220020}-\frac{24017543}{11220020}\sqrt{29}\big)$

Table 8–2: ATR extensions of $\mathbb{Q}(\sqrt{29})$ and Heegner points for $N = 29$

2. $N = 37$**.** Shiota's Weierstrass equation for E_{37} is

$$E_{37} : y^2 + y = x^3 + 2x^2 - (19 + 8\omega)x + (28 + 11\omega), \quad \text{where } \omega = \frac{1+\sqrt{37}}{2}.$$

Its discriminant is $\Delta_{37} = (5+2\omega)^6$. Note that $5+2\omega$ is a fundamental unit of F of negative norm.

D_M	τ	β^2	P_M
-3	$\frac{21+\sqrt{-3}}{2\cdot 37}$	$-3+\omega$	$[2]\Big(-\frac{4417}{1452}-\frac{243}{484}\sqrt{37}-\frac{1}{484}(83+14\sqrt{37})\sqrt{u},\ -\frac{33985}{5324}-\frac{5591}{5324}\sqrt{37}+\frac{1}{5324}(2281+376\sqrt{37})\sqrt{u}\Big)$
-7	$[2]\,\frac{17+\sqrt{-7}}{2\cdot 37}$	$1+\omega$	$[2]\big(-\frac{91}{48}-\frac{5}{16}\sqrt{37}+\frac{1}{16}(6+\sqrt{37})\sqrt{u},\ -\frac{3}{8}-\frac{1}{16}\sqrt{37}-\frac{1}{16}\big(\frac{13}{4}\sqrt{37}+\frac{79}{4}\big)\sqrt{u}\big)$
-11	$\frac{27+\sqrt{-11}}{2\cdot 37}$	$38+15\omega$	$[2]\Big(-\frac{457}{588}-\frac{27}{196}\sqrt{37}-\frac{1}{196}\big(\frac{5}{2}\sqrt{37}+\frac{27}{2}\big)\sqrt{u},\ \frac{2911}{1372}+\frac{481}{1372}\sqrt{37}+\frac{1}{1372}\big(\frac{129}{2}\sqrt{37}+\frac{775}{2}\big)\sqrt{u}\Big)$
-16	$\frac{12+2\sqrt{-1}}{37}$	$5+2\omega$	$[4]\Big(-\frac{701}{294}-\frac{39}{98}\sqrt{37}-\frac{1}{49}\big(23+3\sqrt{37}\big)\sqrt{u},\ -\frac{849}{343}-\frac{279}{686}\sqrt{37}+\frac{1}{343}\big(431+69\sqrt{37}\big)\sqrt{u}\Big)$
-48	$\frac{5+2\sqrt{-3}}{37}$	$2+\omega$	$[2]\Big(\frac{122293}{2175698}\sqrt{37}\sqrt{u}-\frac{3719909}{6527094}+\frac{761343}{2175698}\sqrt{u}-\frac{188225}{2175698}\sqrt{37},$ $-\frac{258896601}{2269253014}\sqrt{37}\sqrt{u}+\frac{9762572151}{2269253014}-\frac{1571259649}{2269253014}\sqrt{u}+\frac{800896996}{1134626507}\sqrt{37}\Big)$
-64	$\frac{13+4\sqrt{-1}}{37}$	$10+4\omega$	$[2]\Big(\frac{187}{225}\sqrt{37}\sqrt{u}+\frac{54871}{7350}+\frac{1107}{1225}\sqrt{u}+\frac{599}{490}\sqrt{37},\ -\frac{38712}{42875}\sqrt{37}\sqrt{u}-\frac{499137}{17150}-\frac{235934}{42875}\sqrt{u}-\frac{205146}{42875}\sqrt{37}\Big)$
-67	$\frac{9+\sqrt{-67}}{2\cdot 37}$	$193+76\omega$	$[2]\Big(-\frac{111}{196}\sqrt{37}\sqrt{u}+\frac{17173}{196}+\frac{2845}{196}\sqrt{37}-\frac{655}{196}\sqrt{u},\ -\frac{14753}{1372}\sqrt{37}\sqrt{u}+\frac{2041969}{1372}-\frac{89717}{1372}\sqrt{u}+\frac{335813}{1372}\sqrt{37}\Big)$
-75	$\frac{31+5\sqrt{-3}}{2\cdot 37}$	$-15+5\omega$	$[2]\Big(-\frac{569629831}{2885264648}\sqrt{37}\sqrt{u}-\frac{3466106179}{2885264648}\sqrt{u}+\frac{9086370409}{1442632324}+\frac{1642128111}{1442632324}\sqrt{37},$ $\frac{63077074474447}{5479406093016 8}\sqrt{37}\sqrt{u}-\frac{709813043287921}{27397030465084}+\frac{383672624573755}{5479406093016 8}\sqrt{u}-\frac{114454323723451}{27397030465084}\sqrt{37}\Big)$
-192	$\frac{10+4\sqrt{-3}}{37}$	$18+8\omega$	$[2]\big(\frac{1}{3}\sqrt{37}\sqrt{u}+\frac{5965}{338}+\frac{1049}{507}\sqrt{u}+\frac{1017}{338}\sqrt{37},\ \frac{21239}{6591}\sqrt{37}\sqrt{u}+\frac{543385}{4394}+\frac{129121}{6591}\sqrt{u}+\frac{89685}{4394}\sqrt{37}\big)$
-275	$\frac{13+5\sqrt{-11}}{2\cdot 37}$	$445+180\omega$	$[2]\big(\frac{997105}{238575708}\sqrt{37}\sqrt{u}+\frac{10672901 5}{34082244}+\frac{21329537}{34082244}\sqrt{37}+\frac{8788883}{238575708}\sqrt{u},$ $\frac{5183238404}{174100622913}\sqrt{37}\sqrt{u}+\frac{126328779110}{24871517559}+\frac{31211705185}{174100622913}\sqrt{u}+\frac{22765460497}{24871517559}\sqrt{37}\big)$
-448	$\frac{6+4\sqrt{-7}}{37}$	$2+2\omega$	$[2]\Big(\frac{25718964}{714877}\sqrt{37}\sqrt{u}+\frac{957496657}{1429754}+\frac{156446894}{714877}\sqrt{u}+\frac{157538925}{1429754}\sqrt{37},$ $-\frac{6872526597129}{3676612411}\sqrt{37}\sqrt{u}-\frac{6819660247093}{198735806}-\frac{1129836753745}{99367903}\sqrt{u}-\frac{41481720050853}{7353224822}\sqrt{37}\Big)$

Table 8–3: ATR extensions of $\mathbb{Q}(\sqrt{37})$ and Heegner points for $N=37$

3. $N=41$**.** Shiota's Weierstrass equation for E_{41} is

$$E_{41}: y^2 = x^3 - \frac{17}{48}x + \Big(-\frac{5}{32}+\frac{1}{27}\sqrt{41}\Big)$$

D_M	τ	β^2	P_M
-4	$\frac{9+\sqrt{-1}}{41}$	$27+10\omega$	$\frac{1}{3}\,[2]\Big(\frac{109}{256}\sqrt{41}\sqrt{u}+\frac{25}{256}+\frac{55}{768}\sqrt{41}-\frac{695}{256}\sqrt{u},\ \frac{361}{2048}\sqrt{41}\sqrt{u}-\frac{2283}{2048}\sqrt{u}-\frac{283}{2048}+\frac{121}{2048}\sqrt{41}\Big)$
-8	$\frac{11+\sqrt{-2}}{41}$	$-248+67\omega$	$[2]\Big(\frac{24}{25}\sqrt{41}\sqrt{u}+\frac{81}{100}+\frac{154}{25}\sqrt{u}+\frac{29}{150}\sqrt{41},\ -\frac{507}{250}\sqrt{41}\sqrt{u}-\frac{829}{500}-\frac{3247}{250}\sqrt{u}-\frac{149}{500}\sqrt{41}\Big)$
-20	$\frac{6+\sqrt{-5}}{41}$	$697+258\omega$	$[2]\Big(-\frac{7}{32}+\frac{17}{96}\sqrt{41},\frac{101}{128}\sqrt{u}+\frac{7}{128}\sqrt{41}\sqrt{u}\Big)$
-23	$\frac{31+\sqrt{-23}}{2\cdot 41}$	$398+144\omega$	$[2]\Big(-\frac{142}{225}\sqrt{u}+\frac{2521}{900}+\frac{98}{25}\sqrt{u}+\frac{29}{150}\sqrt{41},\ -\frac{457}{375}\sqrt{41}\sqrt{u}-\frac{7009}{1500}+\frac{27523}{3375}\sqrt{u}-\frac{12689}{13500}\sqrt{41}\Big)$
-32	$\frac{19+2\sqrt{-2}}{41}$	$1+\omega$	$[2]\Big(\frac{3}{100}\sqrt{41}\sqrt{u}+\frac{21}{100}-\frac{13}{100}\sqrt{u}+\frac{11}{150}\sqrt{41},\ \frac{9}{100}\sqrt{41}\sqrt{u}-\frac{281}{500}-\frac{139}{1000}\sqrt{u}+\frac{11}{500}\sqrt{41}\Big)$
-36	$\frac{14+3\sqrt{-1}}{41}$	$6+3\omega$	$[2]\Big(\frac{-59671}{800}+\frac{28097}{2400}\sqrt{41},\ \frac{20169873}{64000}\sqrt{u}-\frac{3150037}{64000}\sqrt{41}\sqrt{u}\Big)$
-40	$\frac{20+\sqrt{-10}}{41}$	$35+13\omega$	$[2]\Big(\frac{73}{288}+\frac{11}{288}\sqrt{41},\ \frac{3169}{6912}\sqrt{u}-\frac{485}{6912}\sqrt{41}\sqrt{u}\Big)$
-100	$\frac{4+5\sqrt{-1}}{41}$	$10+5\omega$	$[2]\Big(\frac{-291785}{3297312}+\frac{451237}{3297312}\sqrt{41},\ \frac{2630491537}{16934994432}\sqrt{u}-\frac{92418887}{5644998144}\sqrt{41}\sqrt{u}\Big)$
-115	$\frac{7+\sqrt{-115}}{2\cdot 41}$	$177+68\omega$	$[2]\Big(\frac{319}{36}+\frac{13}{9}\sqrt{41},\ \frac{473}{270}\sqrt{u}+\frac{83}{270}\sqrt{41}\sqrt{u}\Big)$
-160	$\frac{1+2\sqrt{-10}}{41}$	4ω	$[2]\Big(-\frac{977902009}{4872819200}+\frac{1700474873}{14618457600}\sqrt{41},\ -\frac{83440266352461}{481044711424000}\sqrt{u}+\frac{8695872103839}{481044711424000}\sqrt{41}\sqrt{u}\Big)$
-368	$\frac{20+2\sqrt{-23}}{41}$	$43+16\omega$	$[2]\Big(\frac{556779493}{30264200}+\frac{300543551}{90792600}\sqrt{41},\ -\frac{219324270863}{29431934500}\sqrt{u}-\frac{78994648597}{29431934500}\sqrt{41}\sqrt{u}\Big)$

Table 8–4: ATR extensions of $\mathbb{Q}(\sqrt{41})$ and Heegner points for $N=41$

8.3 The proof of Theorem 8.1.1

The aim of this section is proving Theorem 8.1.1, which was left unproved in section 8.1 and asserts that the relative discriminant of L/K factors as $d(L/K) = c \cdot \mathcal{N}$, where c is a positive integer such that $L \subset L_c$ (and similarly $L' \subset L'_c$).

Recall our assumption on $N = \mathrm{disc}(F)$ to be odd, and thus square-free. Here we shall assume for notational simplicity that $K \neq \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, so that $\mathcal{O}_K^\times = \{\pm 1\}$; we leave to the reader the task of filling the details for the two excluded fields.

Let us recall first the following classical lemma on Kummer extensions of local fields, which applies in particular to our quadratic extension L/K([Hec, §38-39], [Dab]).

Lemma 8.3.1. *Let k be a local field containing all p-th roots of unity for some prime p and let $v_k : k^\times \to \mathbb{Z}$ denote the valuation map of k, normalized so that $v_k(k^\times) = \mathbb{Z}$. Let K/k be a Kummer extension of degree p with discriminant $\mathfrak{d}_{K/k}$. Then $K = k(\sqrt[p]{\vartheta})$ for some $\vartheta \in k$ such that $v_k(\vartheta) \in \{0, 1\}$. Moreover,*

(*i*) *If $v_k(\vartheta) = 1$, $v_k(\mathfrak{d}_{K/k}) = pv_k(p) + (p-1)$.*

(*ii*) *Assume $v_k(\vartheta) = 0$. If $v_k(p) = 0$, then $v_k(\mathfrak{d}_{K/k}) = 0$. Otherwise, write $\mathfrak{p}_k$ for the unique maximal ideal in k. We have:*

  (*a*) *If equation $x^p \equiv \vartheta (\mathrm{mod}\ \mathfrak{p}_k^{pv_k(p)/(p-1)})$ can be solved in k, then $v_k(\mathfrak{d}_{K/k}) = 0$.*

  (*b*) *If not, $v_k(\mathfrak{d}_{K/k}) = pv_k(p) + (p-1)(1-\eta)$, where $\eta = \max_\ell \{0 \leq \ell < pv_k(p)/(p-1) \,\big|\, x^p \equiv \vartheta (\mathrm{mod}\ \mathfrak{p}_k^\ell)$ can be solved in $\mathcal{O}_k\}$.*

We use the above result in order to deduce several lemmas which shall allow us to reduce the proof of Proposition 8.1.1 to the case in which L/K is unramified at dyadic primes.

Lemma 8.3.2. *Let $p \nmid \mathrm{disc}(K)$ be a prime and put $p^* = 8$ if $p = 2$, $p^* = p$ if $p \equiv 1 (\mathrm{mod}\ 4)$ and $p^* = -p$ if $p \equiv -1 (\mathrm{mod}\ 4)$. Then $K(\sqrt{p^*})$ is contained in the* ring class field H_c *of K associated to the order $\mathcal{O}_c$ of conductor $c = |p^*|$.*

Proof. Suppose first that p is split in K and fix a prime $\mathfrak{p}|p$ in K. Let

$$U = K_{\mathfrak{p}}^{\times} \bigcap K^{\times} \prod_{v} \mathcal{O}_{c,v}^{\times},$$

where the intersection is computed by regarding $K_{\mathfrak{p}}^{\times}$ as a subgroup of $\prod_v K_v^{\times}$ by means of the usual embedding $x_{\mathfrak{p}} \mapsto (1, ..., 1, x_{\mathfrak{p}}, 1, ..., 1)$.

Since the map $K_{\mathfrak{p}}^{\times}/U \to \mathbb{I}_K / \left(K^{\times} \prod_v \mathcal{O}_{c,v}^{\times}\right)$ is injective by [Mil2, p. 173, Proposition 5.2], it follows that $U \subset K_{\mathfrak{p}}^{\times} \simeq \mathbb{Q}_p^{\times}$ corresponds to $H_{c,\mathfrak{P}}/K_{\mathfrak{p}}$ by local class field theory for any prime $\mathfrak{P}$ of H_c above $\mathfrak{p}$.

Write $c = p^r$ with $r = 3$ if $p = 2$, $r = 1$ if p is odd. Since $1 + p^r\mathbb{Z}_p \subseteq U$, $1 + p^{r-1}\mathbb{Z}_p \not\subset U$ by [Cox, p. 197], an easy calculation shows that

$$U = \{\frac{\alpha}{\overline{\alpha}} \,\big|\, \alpha \in V\} \cdot (1 + \mathfrak{p}^r),$$

where $V = \{\alpha \in K^{\times} \,\big|\, \mathrm{ord}_v(\alpha) = 0\ \forall v \neq \mathfrak{p}\}$. Note that $V = \{\pm\alpha_0^n, n \in \mathbb{Z}\}$ for some $\alpha_0 \in K^{\times}$ such that $\mathrm{ord}_v(\alpha_0) = 0$ for all $v \neq \mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}}(\alpha_0) = n_0 \geq 1$ is minimal. With this notation we have

$$U = \{\big(\frac{\alpha_0}{\overline{\alpha}_0}\big)^n, n \in \mathbb{Z}\} \cdot (1 + \mathfrak{p}^r). \tag{8.6}$$

Suppose now that p remains inert in $\mathcal{O}_K$. Arguing similarly as before we obtain that the open subgroup $U \subset K_p^{\times}$ corresponding to $H_{p^r,\mathfrak{P}}/K_p$ by local class field theory is $U = K_p^{\times} \cap \left(K^{\times} \prod_v \mathcal{O}_{p^r,v}^{\times}\right)$, i.e.

$$U = \{\alpha \,\big|\, \alpha \in K^{\times},\, \mathrm{ord}_v(\alpha) = 0,\, \forall v \neq p\} \cdot (1 + p^r\mathcal{O}_{K_p}) = \{(\pm\alpha_0)^n \,\big|\, n \in \mathbb{Z}\} \cdot (1 + p^r\mathcal{O}_{K_p}), \tag{8.7}$$

where $\alpha_0 \in K^\times$ is chosen such that $\mathrm{ord}_v(\alpha_0) = 0$ for all $v \neq p$ and $\mathrm{ord}_p(\alpha_0) \geq 1$ is minimal. We can thus take $\alpha_0 = p^{n_0}$ for some $n_0 \geq 1$.

Put $K' = K(\sqrt{p^*})$. Any prime $\mathfrak{p}$ in K above p ramifies in K'. Fix one such prime $\mathfrak{p}$ and put $\mathfrak{p} = \wp^2$ in K' so that $K'_\wp = K_\mathfrak{p}(\sqrt{p^*})$. By class field theory, in order to prove that $K' \subset H_c$ it is enough to show that $U \subset \mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K'^\times_\mathfrak{p})$. Since $d(K'/K) = p^*$ by Lemma 8.3.1, K' is contained in the *ray class field* K_c of conductor c of K and it thus suffices to verify that $\alpha_0\overline{\alpha}_0$ (resp. $\pm\alpha_0$) lies in $\mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K'^\times_\mathfrak{p})$ if p splits (resp. remains inert) in K.

Assume $p = 2$. Then $\pm 1, \pm 2 \in \mathrm{Nm}_{K'_\wp/K_\mathfrak{p}}(K'^\times_\wp)$ because $-1 = \mathrm{Nm}(1+\sqrt{2})$ and $-2 = \mathrm{Nm}(\sqrt{2})$. The lemma thus follows automatically if 2 is inert in K, while if 2 splits, it follows because $\alpha_0\overline{\alpha}_0$ is a power of 2, hence $\alpha_0\overline{\alpha}_0$ lies in either $\pm\mathbb{Q}_2^{\times^2}$ or $\pm 2\mathbb{Q}_2^{\times^2}$.

Assume p is odd. Then $-p^* = \mathrm{Nm}(\sqrt{p^*}) \in \mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K'^\times_\mathfrak{p})$. Suppose first p splits in K: as before, it is enough to show that $p \in \mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K'^\times)$, which we already did if $p^* = -p$. That the same holds when $p^* = p$ follows because $p \equiv 1 (\mathrm{mod}\ 4)$ implies that $-1 \in \mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K'^\times_\mathfrak{p})$. Suppose now p remains inert in K; we must show that $\pm p \in \mathrm{Nm}_{K'_\mathfrak{p}/K_\mathfrak{p}}(K'^\times_\mathfrak{p})$. If $p^* = p$ this follows by the same reason as above; if $p^* = -p$, then $p \equiv 3 \,(\mathrm{mod}\ 4)$, $K_p = \mathbb{Q}_p(\sqrt{-1})$ and thus $-1 \in K_p^{\times^2}$, which allows us to conclude. □

Note that a direct consequence of the previous lemma is that for any odd square free integer m relatively coprime with $\mathrm{disc}(K)$ either $K(\sqrt{m})$ or $K(\sqrt{-m})$ is contained in H_m.

Lemma 8.3.3. *$d(L/K) = 2^t c_0 \mathcal{N}$ for some integer $0 \leq t \leq 3$ and some positive integer $c_0 \geq 1$ relatively coprime to 2 and $\mathcal{N}$. If further 2 is ramified in K, $0 \leq t \leq 2$.*

Proof. Write $K = \mathbb{Q}(\sqrt{-d_0})$ for some square free integer $d_0 > 0$ and $L = K(\sqrt{\beta})$ for some $\beta \in \mathbb{Z} + \mathbb{Z}\sqrt{-d_0}$ and square free in K. Without loss of generality, N can

be written as $\mathcal{N}\overline{\mathcal{N}}$ where $\mathcal{N}$ divides the square free part $\mathfrak{B}$ of (β) in K and $\overline{\mathcal{N}}$ is relatively coprime to $\mathfrak{B}$.

Write $\mathfrak{B}_2$ for the largest ideal which divides $\mathfrak{B}$ and is relatively coprime to any prime of K above 2. Since $v_{K_{\mathfrak{p}'}}(2) = 0$ and $v_{K_{\mathfrak{p}'}}(\mathfrak{B}_2) = 1$ for any prime $\mathfrak{p}' \mid \mathfrak{B}_2$, Lemma 8.3.1 shows that $v_{K_{\mathfrak{p}'}}(\mathfrak{d}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}'}}) = 1$, where $\mathfrak{P}'$ is the prime in L above $\mathfrak{p}'$, thus the prime-to-2 part of $d(L/K)$ is $\mathfrak{B}_2$. Besides, $\mathfrak{B}_2 = \mathcal{N} \cdot \mathfrak{C}$ with $(\mathfrak{C}, \mathcal{N}) = 1$. Since $\mathrm{Nm}_{K/\mathbb{Q}}(\beta)/N$ is a perfect square in $\mathbb{Z}$, $\mathfrak{C}$ is principal and can be written as $\mathfrak{C} = (c_0)$ for some integer $c_0 > 0$. Hence $\mathcal{N}c_0 \mid d(L/K) \mid 2^t\mathcal{N}c_0$ for some integer $t \geq 0$.

If 2 is unramified in K we have $v_{K_{\mathfrak{p}}}(2) = 1$ for any prime $\mathfrak{p} \mid 2$ in K and it follows from Lemma 8.3.1 that $d(L/K) = \mathcal{N}c_0 2^t$ with $0 \leq t \leq 3$.

Suppose now that 2 ramifies in K with $(2) = \mathfrak{p}^2$ in K. Then, since $v_{K_{\mathfrak{p}}}(2) = 2$ and $\mathrm{Nm}_{K/\mathbb{Q}}(\beta)/N$ is a perfect square in $\mathbb{Z}$, we fall into case (ii) of Lemma 8.3.1: for any prime $\mathfrak{P}$ in L above $\mathfrak{p}$, $L_{\mathfrak{P}}$ can be written as $K_{\mathfrak{p}}(\sqrt{\vartheta})$ for some $\vartheta \in K_{\mathfrak{p}}^{\times}$ such that $v_{k_{\mathfrak{p}}}(\vartheta) = 0$. Suppose $v_{K_{\mathfrak{p}}}(\mathfrak{d}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}) \neq 0$. Then Lemma 8.3.1 (b) asserts that

$$v_{K_{\mathfrak{p}}}(\mathfrak{d}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}) = 5 - \eta,$$

where

$$\eta = \max\{0 \leq \ell < 4 \,\big|\, \exists \iota \in \mathcal{O}_{K_{\mathfrak{p}}},\, \iota^2 \equiv \vartheta (\mathrm{mod}\ \mathfrak{p}^{\ell})\}.$$

A classical result of Hilbert (cf. [HSW], [Hil]) implies that $v_{K_{\mathfrak{p}}}(\mathfrak{d}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}})$ is even. Hence $d(L/K) = \mathcal{N}2^t c_0$ with $0 \leq t \leq 2$. □

Lemma 8.3.4. *It is enough to prove Proposition* 8.1.1 *when* $d(L/K) = 2^t\mathcal{N}$ *and* $0 \leq t \leq 2$.

Proof. Lemma 8.3.3 shows in general $d(L/K) = 2^t c_0 \mathcal{N}$, where $0 \leq t \leq 3$ and $c_0 \geq 1$. Suppose first that $t = 3$, then 2 is unramified in K by the same lemma. Let $\mathfrak{P}$ and $\mathfrak{p}$ be prime ideals in L and K respectively such that $\mathfrak{P}|\mathfrak{p}|2$. Then $L_{\mathfrak{P}}$ can be written

as $K_{\mathfrak{p}}(\sqrt{\vartheta})$ for some $\vartheta \in K$ with $v_{K_{\mathfrak{p}}}(\vartheta) \in \{0,1\}$. Define $L' = K(\sqrt{\vartheta'})$, where ϑ' is defined as

$$\vartheta' = \begin{cases} \vartheta/2 & \text{if } v_{K_{\mathfrak{p}}}(\vartheta) = 1; \\ \vartheta & \text{if } v_{K_{\mathfrak{p}}}(\vartheta) = 0. \end{cases}$$

Hence $v_{K_{\mathfrak{p}}}(\vartheta') = 0$. Let $\mathfrak{P}'$ be a prime in L' above $\mathfrak{p}$. Then either case (a) or (b) of Lemma 8.3.1 applies. In case (a), $v_{K_{\mathfrak{p}}}(\mathfrak{d}_{L'_{\mathfrak{P}'}/K_{\mathfrak{p}}}) = 0$. In case (b), $v_{K_{\mathfrak{p}}}(\mathfrak{d}_{L'_{\mathfrak{P}'}/K_{\mathfrak{p}}}) = 3-\eta$, where $0 \leq \eta \leq 2$, hence $\mathfrak{p}$ is ramified in L', so residue field of $L'_{\mathfrak{P}'}$ is equal to that of $K_{\mathfrak{p}}$ and consequently $\eta \geq 1$. We conclude that $v_{K_{\mathfrak{p}}}(\mathfrak{d}_{L'_{\mathfrak{P}'}/K_{\mathfrak{p}}}) \leq 2$. By Lemma 8.3.2, $L \subset K(\sqrt{2})L' \subset H_8 L'$ with $d(L'/K) = 2^{t'} c_0 \mathcal{N}$ for some integer $0 \leq t' \leq 2$.

Suppose now $c_0 > 1$. Setting $L'' = K(\sqrt{\delta\vartheta'/c_0})$ we have $d(L''/K) = 2^{t'}\mathcal{N}$, where $\delta \in \{\pm 1\}$ such that $K(\sqrt{\delta c_0}) \subset H_{c_0}$ as described in Lemma 8.3.2. By the same lemma, $L' \subset K(\sqrt{\delta c_0})L'' \subset H_{c_0}L''$.

So $L \subset H_8 L' \subset H_8 H_{c_0} L'' = H_{8c_0} L''$ such that L''/K is a quadratic extension and $d(L''/K) = 2^{t'}\mathcal{N}$ for some integer $0 \leq t' \leq 2$. This justifies we only need to prove proposition 8.1.1 when $0 \leq t \leq 2$ and $d(L/K) = 2^t \mathcal{N}$. □

Thanks to Lemma 8.3.4 we can assume in what follows that $c_0 = 1$ and $0 \leq t \leq 2$.

Lemma 8.3.5. *There is a unique quadratic extension $\mathcal{L}_{2^t}/K_{2^t}$ contained in $K_{2^t\mathcal{N}}$ such that the set of primes in K_{2^t} which ramify in $\mathcal{L}_{2^t}$ is the set of primes above $\mathcal{N}$. We have $L \subset \mathcal{L}_{2^t}$.*

Proof. Assume first $t = 0$ or 1. Then $\mathrm{Gal}(K_{2^t\mathcal{N}}/K_{2^t}) \cong (\prod_{\mathfrak{p}|\mathcal{N}}(\mathcal{O}_K/\mathfrak{p})^\times)/\{\pm 1\} \cong (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$. This is obvious for $t = 0$, and holds for $t = 1$ because $K_2 K_{\mathcal{N}} = K_{2\mathcal{N}}$. Extension $\mathcal{L}_{2^t}/K_{2^t}$ corresponds by Galois theory to the unique primitive even quadratic Dirichlet character χ of conductor N.

Suppose now $t = 2$. Then

$$\mathrm{Gal}(K_{2^t\mathcal{N}}/K_{2^t}) \cong G := \big(\{\pm 1\} \times (\mathbb{Z}/N\mathbb{Z})^\times\big)/\{\pm \mathbb{1}\},$$

where $\mathbb{1} = (1, \mathbf{1})$ is the identity element of $\{\pm 1\} \times (\mathbb{Z}/N\mathbb{Z})^\times$. Again, any extension $\mathcal{L}_{2^t}/K_{2^t}$ as in the statement corresponds to a non-trivial character $\chi' : G \to \{\pm 1\}$ which is trivial on $\{\pm 1\} \times \{\mathbf{1}\}$ and is even and primitive on $\{1\} \times (\mathbb{Z}/N\mathbb{Z})^\times$. As above, the only such character is $\chi' = 1 \times \chi$.

Finally, note that LK_{2^t}/K_{2^t} is a quadratic extension contained in $K_{2^t\mathcal{N}}$. Since $\mathrm{disc}(LK_{2^t}/K_{2^t}) = \mathcal{N}$ it follows that $\mathcal{L}_{2^t} = LK_{2^t}$ and thus $L \subset \mathcal{L}_{2^t}$. □

Recall the quadratic extension L_c of the ring class field H_c introduced in section 8.1, over which the Heegner points P_c^+ and $P_c^- \in \mathrm{CM}(c)$ are rational. Lemma 8.3.5 reduces the proof of Proposition 8.1.1 to showing that $L_c = \mathcal{L}_c$. Since L_c was defined as the quadratic extension of H_c cut out by the kernel of the single even primitive character χ of conductor N, it suffices to show that $H_{2^t} = K_{2^t}$ for $0 \le t \le 2$.

When $t = 0$ and we obviously have $H_1 = K_1$. If $t = 1$ or 2, the ratio of the ray class number h_{2^t} by the ring class number $h(\mathcal{O}_{2^t})$ is (cf. [Mil2, p.146] for this and the remaining notations):

$$\begin{aligned}
\frac{h_{2^t}}{h(\mathcal{O}_{2^t})} &= \frac{[U : U_{2^t,1}]^{-1}\mathrm{Nm}(2^t)\prod_{\mathfrak{p}|2^t}(1 - \frac{1}{\mathrm{Nm}(\mathfrak{p})})}{\frac{2^t}{[\mathcal{O}_K^\times : \mathcal{O}_{2^t}^\times]}\prod_{p|2^t}(1 - \left(\frac{d_K}{p}\right)\frac{1}{p})} \\
&= \begin{cases}
\frac{[\mathcal{O}_K^\times : \mathcal{O}_{2^t}^\times]}{[U:U_{2^t,1}]} \cdot \frac{2^{2t}\left(1-\frac{1}{4}\right)}{2^t\left(1-\left(\frac{d_K}{2}\right)\frac{1}{2}\right)} & \text{if 2 is inert in } K, \\
\frac{[\mathcal{O}_K^\times : \mathcal{O}_{2^t}^\times]}{[U:U_{2^t,1}]} \cdot \frac{2^{2t}\left(1-\frac{1}{2}\right)^2}{2^t\left(1-\left(\frac{d_K}{2}\right)\frac{1}{2}\right)} & \text{if 2 is split in } K, \\
\frac{[\mathcal{O}_K^\times : \mathcal{O}_{2^t}^\times]}{[U:U_{2^t,1}]} \cdot \frac{2^{2t}\left(1-\frac{1}{2}\right)}{2^t} & \text{if 2 is ramified in } K.
\end{cases} \\
&= \frac{[\mathcal{O}_K^\times : \mathcal{O}_{2^t}^\times]}{[U : U_{2^t,1}]} \cdot 2^{t-1}.
\end{aligned} \tag{8.8}$$

Since $K \neq \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, $[\mathcal{O}_K^\times : \mathcal{O}_{2^t}^\times] = 1$. If $t = 1$, then $U = U_{2^t,1}$, so $K_2 = H_2$. If $t = 2$, then $[U : U_{2^t,1}] = 2$, and therefore $K_{2^2} = H_{2^2}$.

Chapter 9
Darmon-Logan's ATR cycles

As pointed out in the previous chapter, it is known there exist elliptic curves E defined over real quadratic fields F which are not $\mathbb{Q}$-curves but have everywhere good reductions. In this case there are no known methods to construct algebraic points on E. In this chapter, we will describe a conjectural construction by Darmon and Logan ([DL]).

9.1 Review of Darmon-Logan's construction

Let E be an elliptic curve over a totally real field F. Assume for simplicity that F has narrow class number 1 so that we can avoid the language of adèles (for a discussion of how this assumption can be relaxed, see [Gar]). Let σ_0 and σ_1 denote the real embeddings of F and let E_j be the base change of E to $\mathbb{R}$ via σ_j $(j = 0, 1)$.

We also assumed E/F is modular. Hence there is a Hilbert modular form G attached to E/F with parallel weight 2 on $\mathcal{H}_0 \times \mathcal{H}_1$ under the action $\mathrm{SL}_2(\mathcal{O}_F)$ embedded in $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$ via σ_0 and σ_1. It gives rise to an holomorphic 2-form on $X_F(\mathbb{C}) = \mathrm{SL}_2(\mathcal{O}_F)\backslash\mathcal{H}_0 \times \mathcal{H}_1$ by the rule

$$w_G^{\mathrm{hol}} = (2\pi i)^2 G(\tau_0, \tau_1) d\tau_0 d\tau_1.$$

Choose $\epsilon \in \mathcal{O}_F^\times$ of norm -1 such that

$$\epsilon_0 = \sigma_0(\epsilon) > 0, \quad \epsilon_1 = \sigma_1(\epsilon) < 0.$$

Define a non-holomorphic 2-form ω_G as

$$\omega_G := (2\pi i)^2(G(\tau_0,\tau_1)d\tau_0 d\tau_1 - G(\epsilon_0\tau_0,\epsilon_1\overline{\tau}_1)d\tau_0 d\overline{\tau}_1),$$

which is also invariant under $\Gamma = \mathrm{SL}_2(\mathcal{O}_F)$.

Define $\Lambda_G = \left\{ \int_\gamma \omega_G \,\middle|\, \gamma \in H_2(X_F(\mathbb{C}),\mathbb{Z}) \right\}$. Oda proposes the following conjecture [Oda]:

Conjecture 9.1.1. *The group Λ_G is a lattice in $\mathbb{C}$ and $\mathbb{C}/\Lambda_G$ is isogenous to E_0.*

Fix an ATR quadratic extension M of F, and let $\Psi : M \to M_2(F)$ be an F-algebra embedding. Then

1. Since $M \otimes_{F,v_0} \mathbb{R} \cong \mathbb{C}$, the torus $\Psi(M^\times)$ has a unique fixed point $\tau_0 \in \mathcal{H}_0$.
2. The fact that $M \otimes_{F,v_1} \mathbb{R} \cong \mathbb{R} \oplus \mathbb{R}$ shows that $\Psi(M^\times)$ has two fixed points τ_1 and τ_1' on the boundary of $\mathcal{H}_1$. Let $\Upsilon_1 \subset \mathcal{H}_1$ be the hyperbolic geodesic joining τ_1 to τ_1'.

An embedding $\Psi : M \to M_2(F)$ has a conductor, which is defined to be the $\mathcal{O}_F$-ideal c_Ψ for which

$$\Psi(M) \cap M_2(\mathcal{O}_F) = \Psi(\mathcal{O}_F + c_\Psi \mathcal{O}_M).$$

The $\mathcal{O}_F$-order $\mathcal{O}_\Psi := \mathcal{O}_F + c_\Psi\mathcal{O}_M$ is called the order associated to Ψ. It can be shown that there are finitely many distinct $\mathrm{SL}_2(\mathcal{O}_F)$-conjugacy classes of embeddings of M into $M_2(F)$ associated to a fixed order $\mathcal{O} \subset \mathcal{O}_M$, and that the Picard group (in the narrow sense) of $\mathcal{O}$ acts simply transitively on the set of such conjugacy classes of embeddings.

By the Dirichlet unit theorem, the group

$$\Gamma_\Psi := \Psi((\mathcal{O}_\Psi)^\times) \subset \mathrm{SL}_2(\mathcal{O}_F)$$

is of rank 1 and preserves the region

$$R_\Psi := \{\tau_0\} \times \Upsilon_1.$$

The ATR cycle associated to the embedding Ψ is defined to be the quotient

$$\Delta_\Psi := \Gamma_\Psi \backslash R_\Psi.$$

It can be shown that the real one-dimensional cycle Δ_ψ is null-homologous, at least after multiplying it by a suitable integer.

Choose an isogeny $\eta : \mathbb{C}/\Lambda_G \to E_0(\mathbb{C})$, and set

$$\mathrm{AJ}_G(\Delta_\Psi) := \eta\left(\int_{\tilde{\Delta}_\Psi} \omega_G\right), \qquad \text{for any } \tilde{\Delta}_\Psi \text{ with } \partial\tilde{\Delta}_\Psi = \Delta_\Psi. \tag{9.1}$$

The following conjecture lends arithmetic meaning to the Abel-Jacobi map AJ_G and to the ATR cycles Δ_Ψ.

Conjecture 9.1.2 (Darmon-Logan)**.** *The isogeny η in the definition of AJ_G can be chosen so that, for all Ψ,*

$$\mathrm{AJ}_G(\Delta_\Psi) \in E(H_{c_\Psi}),$$

where H_{c_Ψ} is the ring class field of M of conductor c_Ψ. Furthermore, if $\Psi_1, \ldots, \Psi_h$ is a complete system of representatives for the $\mathrm{SL}_2(\mathcal{O}_F)$-conjugacy classes of embeddings of M in $M_2(\mathcal{O}_F)$ of a given conductor c, then the Galois group $\mathrm{Gal}(H_c/M)$ acts (transitively) on the set $\{\mathrm{AJ}_G(\Delta_{\Psi_1}), \ldots, \mathrm{AJ}_G(\Delta_{\psi_h})\}$.

Definition 9.1.3. *Define:*

$$P_M^{\mathrm{DL}} := \mathrm{AJ}_G(\Delta_{\Psi_1}) + \cdots + \mathrm{AJ}_G(\Delta_{\Psi_h}).$$

9.2 Conjectural Relation with Heegner points

We have two constructions. The first is the one provided by the Heegner points which are subject to no conjecture but are available only for $\mathbb{Q}$-curves; the second is

the Darmon-Logan construction which is available for all elliptic curves defined over a totally real field, but which remains highly conjectural.

When we restrict our attention to $\mathbb{Q}$-curves, we make the following conjecture relating Darmon-Logan ATR points –which we denote P_M^{DL}– and the Heegner points –which we denote P_M– as M ranges over the quadratic ATR extension of F. Let τ be the non-trivial element in $\mathrm{Gal}(F/\mathbb{Q})$ and D_F the discriminant of F. Denote by $c_{E/F}$ (resp. $c_{E^\tau/F}$) either the real period or twice the real period of $E/\mathbb{R}$ (resp. of $E^\tau/\mathbb{R}$) depending on whether $E(\mathbb{R})$ (resp. $E^\tau(\mathbb{R})$) is connected or not.

Conjecture 9.2.1. *The ATR point P_M^{DL} is of infinite order if and only if P_M is of infinite order and $L(E/F,1) \neq 0$. More precisely,*

$$P_M^{\mathrm{DL}} = 2^s \ell \cdot P_M \tag{9.2}$$

where $\ell \in \mathbb{Q}^\times$ is a non-zero rational quantity which depends only on (E,F) and not on M, and satisfies

$$\ell^2 = \frac{L(E/F,1)}{\Omega_{E/F}}, \qquad \textit{with } \Omega_{E/F} = \frac{c_{E/F} \cdot c_{E^\tau/F} \cdot c_{\mathrm{fin}}}{D_F^{1/2} \cdot |E_{\mathrm{tor}}(F)|^2},$$

where c_{fin} is the local fudge factor of E/F and $s \in \mathbb{Z}$ depends on M.

9.3 Numerical evidence

In this section we provide some evidence for Conjecture 9.2.1, building on the data offered in section 8.2. Please note c_{fin} in Conjecture 9.2.1 is 1 if E/F has everywhere good reduction.

In order to compare Heegner points versus Darmon-Logan points, it is actually sufficient to compute the element $z_M^{\mathrm{DL}} \in \mathbb{C}/\Lambda_E$ which maps to P_M^{DL} under the Weierstrass uniformization. This approach has great advantage over the one that [DL] uses. This is because of the restriction of precision, the recognition of algebraicity

of P_M^{DL} in [DL] is difficult. The authors of [DL] are forced to perform an independent search for a generator of $E(M)$ which is a difficult task to check P_M^{DL} equals to up to torsion a point on $E(M)$ within the precision, whereas we can resort to an independent classical Heegner point calculation.

In the tables below, the notations are the same as those in section 8.2 and those in Conjecture 9.2.1. Note that ℓ and s uniquely determine Heegner points P_M up to sign and $E(M)_{\mathrm{tor}}$.

1. $N = 29$**.** Our calculations show that

$$\ell^2 = \frac{L(E_{29}/F, 1)}{\Omega_{E_{29}/F}} = 1$$

and that the point P_M^{DL} and s are given in the following table.

$D_M = D_K \cdot c^2$	β^2	D_L	$\lvert\mathrm{Pic}(\mathcal{O}_c)\rvert$	P_M^{DL}	s
$-7 = -7 \cdot 1$	$-1+\omega$	29	1	$(\beta^2+3,\ -\frac{5}{2}\beta^3 - 3\beta^2 - 8\beta - \frac{19}{2})$	-2
$-16 = -4 \cdot 2^2$	$2+\omega$	$2^2 \cdot 29$	1	$(\frac{\beta^2}{2},\ -\frac{5}{4}\beta^3 - \frac{11}{4}\beta^2 - \frac{\beta}{4} - \frac{1}{2})$	-2
$-23 = -23 \cdot 1$	$17+8\omega$	29	3	$(\frac{1}{8}(11\beta^2+5),\ -\frac{13}{8}\beta^3 - \beta^2 - \frac{7}{8}\beta - \frac{1}{2})$	-2
$-35_1 = -35 \cdot 1$	$19+9\omega$	29	2	$(\frac{1}{5}(2\beta^2+1),\ -\frac{59}{225}\beta^3 - \frac{43}{90}\beta^2 - \frac{89}{450}\beta - \frac{29}{90})$	-2
$-35_2 = -35 \cdot 1$	$4+3\omega$	29	2	$(-\frac{1}{15}(4\beta^2+11),\ -\frac{1}{150}(17\beta^3 + 105\beta^2 + 43\beta + 270))$	-2
$-59 = -59 \cdot 1$	$61+28\omega$	29	3	$(-\frac{1}{9},\ -\frac{11}{1512}\beta^3 - \frac{5}{56}\beta^2 - \frac{1}{1512}\beta + \frac{1}{504})$	-2
$-63 = -7 \cdot 3^2$	3ω	$3^2 \cdot 29$	4	$(\frac{7}{9}\beta^2+5,\ \frac{26}{27}\beta^3 - \frac{11}{9}\beta^2 + \frac{57}{9}\beta - 8)$	-2
$-64 = -4 \cdot 4^2$	$4+2\omega$	$2^4 \cdot 29$	2	$(-\frac{1}{4},\ -\frac{3}{8}\beta^3 - \frac{5}{4}\beta^2 - \frac{\beta}{4} - \frac{3}{8})$	-2
$-80 = -20 \cdot 2^2$	$1+\omega$	$2^2 \cdot 29$	4	$(\frac{1}{10}(43\beta^2+51),\ -\frac{517}{50}\beta^3 - \frac{93}{20}\beta^2 - \frac{1233}{100}\beta - \frac{111}{20})$	-2
$-91 = -91 \cdot 1$	$7+5\omega$	29	2	$(\frac{1}{13}(98\beta^2+387),\ -\frac{18939}{845}\beta^3 - \frac{111}{26}\beta^2 - \frac{150109}{1690}\beta - \frac{439}{26})$	-2
$-175 = -7 \cdot 5^2$	$-5+5\omega$	$5^2 \cdot 29$	6	$(-\frac{6}{50}\beta^2 - 2,\ \frac{1}{10}\beta^3 - \frac{11}{25}\beta^2 + \frac{98}{100}\beta - \frac{45}{10})$	-2

Table 9–1: ATR extensions of $\mathbb{Q}(\sqrt{29})$ and ATR points on E_{29}

2. $N = 37$. Our calculations are consistent with the fact that

$$\ell^2 = \frac{L(E_{37}/F, 1)}{\Omega_{E_{37}/F}} = 1.$$

The point P_M^{DL} and s are given in the tables below.

$D_M = D_K \cdot c^2$	β^2	D_L	$\lvert\mathrm{Pic}(\mathcal{O}_c)\rvert$	P_M^{DL}	s
$-3 = -3 \cdot 1$	$-3+\omega$	37	1	$(-\frac{2}{3}\beta - \frac{13}{3},\ -\frac{61}{18}\beta^3 - \frac{169}{9}\beta - \frac{1}{2})$	-1
$-7 = -7 \cdot 1$	$1+\omega$	37	1	$(\frac{2}{7}\beta - \frac{3}{7},\ -\frac{57}{98}\beta^3 - \frac{44}{49}\beta - \frac{1}{2})$	-1
$-11 = -11 \cdot 1$	$38+15\omega$	37	1	$(-\frac{2}{165}\beta^2 - \frac{104}{165},\ -\frac{17}{1210}\beta^3 - \frac{2}{605}\beta - \frac{1}{2})$	-1
$-16 = -4 \cdot 2^2$	$5+2\omega$	$2^2 \cdot 37$	1	$(\frac{\beta^2}{8} - \frac{5}{8},\ \frac{\beta^3}{8} - \frac{1}{2})$	-2
$-48 = -3 \cdot 4^2$	$2+\omega$	$4^2 \cdot 37$	3	$(\frac{115}{588}\beta^2 - \frac{80}{147},\ -\frac{11225}{24696}\beta^3 - \frac{1529}{6174}\beta - \frac{1}{2})$	-1
$-64 = -4 \cdot 4^2$	$10+4\omega$	$4^2 \cdot 37$	2	$(-\frac{\beta^2}{8} - \frac{3}{4},\ -\frac{\beta^3}{8} - \frac{1}{2})$	-2
$-67 = -67 \cdot 1$	$193+76\omega$	67	1	$(-1, -\frac{1}{2} + \frac{1}{2}\beta)$	-2
$-75 = -3 \cdot 5^2$	$-15+5\omega$	$5^2 \cdot 37$	3	$(\frac{196}{775}\beta^2 + \frac{136}{27}, -\frac{1559}{12150}\beta^3 - \frac{25732}{6075}\beta - 1/2)$	-1
$-192 = -3 \cdot 8^2$	$18+8\omega$	$8^2 \cdot 37$	6	$(\frac{7}{3} + \frac{7}{6}\omega, -\frac{1}{2} + \frac{1}{36}(\frac{85}{3} + \frac{14}{3}\sqrt{37})\beta)$	-2
$-275 = -11 \cdot 5^2$	$445+180\omega$	$5^2 \cdot 37$	4	$(\frac{2}{11} + \frac{4}{11}\omega, -\frac{1}{2} + \frac{1}{242}(\frac{62}{7} + \frac{9}{7}\sqrt{37})\beta)$	-2
$-448 = -7 \cdot 8^2$	$2+2\omega$	$8^2 \cdot 37$	4	$(\frac{45}{7} + \frac{39}{14}\omega, -\frac{1}{2} + \frac{1}{196}(\frac{689}{2}\sqrt{37} + \frac{4191}{2})\beta)$	-2

Table 9–2: ATR extensions of $\mathbb{Q}(\sqrt{37})$ and ATR points on E_{37}

3. $N = 41$. In their computations, Darmon and Logan used instead curve E'_{41} : $y^2 + xy = x^3 - (32+5\sqrt{41})x$. This Weierstrass equation was first found by Oort, and there is an explicit isogeny $\psi : E'_{41} \to E_{41}$ of degree 2. Following Darmon-Logan's approach, points P_M^{DL} listed below are points on E'_{41}. Since the isogeny ψ is explicit, it is an easy task to transfer them to points on E_{41}, and this is what we did in order to compare the Heegner points $P_M \in E_{41}(M)$ with points $\psi(P_M^{\mathrm{DL}}) \in E_{41}(\mathbb{C})$. In this case, calculations suggest once again that

$$\ell^2 = \frac{L(E_{41}/F, 1)}{\Omega_{E_{41}/F}} = 1.$$

The points P_M^{DL} and s are given below:

$D_M = D_K \cdot c^2$	β^2	D_L	$\lvert\mathrm{Pic}(\mathcal{O}_c)\rvert$	P_M^{DL}	s
$-4 = -4 \cdot 1$	$27+10\omega$	41	1	$(-\frac{1}{4},\ -\frac{\beta}{2} + \frac{1}{8})$	1
$-8 = -8 \cdot 1$	$-248+67\omega$	41	1	$(-\frac{1}{268}(3\beta^2 + 1481),\ \frac{1}{536}(-254\beta^3 + 3\beta^2 - 108954\beta + 1481))$	0
$-20 = -20 \cdot 1$	$697+258\omega$	41	2	$(\frac{1}{43}(\beta^2 - 9),\ \frac{1}{258}(-\beta^3 - 3\beta^2 + 181\beta + 27))$	0
$-23 = -23 \cdot 1$	$398+144\omega$	41	3	$(\frac{-71027\beta^2 - 1271153}{9884736},\ \frac{-1095348\beta^3 + 9304537\beta^2 + 16459332\beta + 166521043}{2589800832})$	0
$-32 = -8 \cdot 2^2$	$1+\omega$	$2^2 \cdot 41$	2	$(\frac{29\beta^2+49}{4},\ \frac{1}{16}(-359\beta^3 - 58\beta^2 - 611\beta - 98))$	0
$-36 = -4 \cdot 3^2$	$6+3\omega$	$3^2 \cdot 41$	4	$(-8 + 2\omega, (\frac{7}{2} - \frac{1}{2}\sqrt{41})(1 + 5\beta))$	-1
$-40 = -40 \cdot 1$	$35+13\omega$	41	2	$(9 + \frac{27}{8}\omega, -\frac{171}{32} - \frac{27}{32}\sqrt{41} + \frac{3}{32}(\frac{109}{2} + \frac{17}{2}\sqrt{41})\beta)$	-1
$-100 = -4 \cdot 5^2$	$10+5\omega$	$5^2 \cdot 41$	2	$(\frac{9}{2} + \frac{7}{4}\omega, -\frac{43}{16} - \frac{7}{16}\sqrt{41} + (\frac{3}{8}\sqrt{41} + \frac{19}{8})\beta)$	-2
$-115 = -115 \cdot 1$	$177+68\omega$	41	2	$(-\frac{31}{9} - \frac{11}{9}\omega, \frac{73}{36} + \frac{11}{36}\sqrt{41} + \frac{1}{108}(\frac{59}{5} + \frac{9}{5}\sqrt{41})\beta)$	-1
$-160 = -40 \cdot 2^2$	4ω	$2^2 \cdot 41$	4	$(32 + 12\omega, -19 - 3\sqrt{41} + (\frac{173}{2} + \frac{27}{2}\sqrt{41})\beta)$	-2
$-368 = -23 \cdot 4^2$	$43+16\omega$	$4^2 \cdot 41$	6	$(\frac{29}{4} + \frac{11}{4}\omega, -\frac{69}{16} - \frac{11}{16}\sqrt{41} + (\frac{13}{4} + \frac{1}{2}\sqrt{41})\beta)$	-2

Table 9–3: ATR extensions of $\mathbb{Q}(\sqrt{41})$ and ATR points on E'_{41}

Chapter 10
Another proof of Theorem 7.2.5

In this chapter, we use Kolyvagin's Euler system to prove Theorem 7.2.5. Besides Kolyvagin's original papers([Kol1] – [Kol3]), [Gro] illustrates Kolyvagin's main ideas quite well. [How] is a good reference to the background needed here for our purpose. Basic ideas and notations here are borrowed from [How].

10.1 Norm compatibility

Let $N > 1$ be a square-free odd integer and let χ be a primitive even quadratic character on $(\mathbb{Z}/N\mathbb{Z})^\times$. Let $f \in S_2(\Gamma_0(N), \chi)$ be a newform. Recall that f is associated with an abelian variety A_f which is $\mathbb{Q}$-simple and has dimension $[K_f : \mathbb{Q}]$. One has the following morphism defined over $\mathbb{Q}$:

$$\Phi_f : \underbrace{X_\chi(N) \overset{\iota}{\hookrightarrow} J_\chi(N) \overset{\lambda}{\to} A_f}.$$

A (coarse) moduli interpretation of $Y_\chi(N) = \Gamma_\chi(N)\backslash\mathcal{H}$ is:

$$Y_\chi(N) = \left\{(E, C_+^\times)\right\} / \sim, \tag{10.1}$$

where E is an elliptic curve, C is a cyclic subgroup in E of order N, and $C_+^\times$ is defined as one of the two orbits of $C - \{0\}$ with respect to the natural action of $(\mathbb{Z}/N\mathbb{Z})^{\times 2}$ where C is a cyclic subgroup of order N in E, i.e. fix a generator Q of C, then $C_+^\times$ is one of the following two sets:

$$\{n \cdot Q \,\big|\, \chi(n) = 1\};\ \{n \cdot Q \,\big|\, \chi(n) = -1\}.$$

The equivalence $\sim$ in (10.1) has the obvious meaning.

For any odd prime $\ell \nmid ND$, where D is the discriminant of K in the field tower (7.5), the Hecke operator T_ℓ acts on the moduli space $Y_\chi(N)$ by the rule

$$T_\ell\big((E, C_+^\times)\big) = \sum_{\substack{E \xrightarrow{\eta} E' \\ \deg \eta = \ell}} (E', {C'}_+^\times),$$

where ${C'}_+^{\ \times} = \eta(C_+^\times)$. Note we have the following field tower:

$$\begin{array}{c} \tilde{H}_{c\ell} \\ {\scriptstyle G_\ell}\big| \\ \tilde{H}_c \\ | \\ \mathcal{M} \\ | \\ K \\ | \\ \mathbb{Q} \end{array}$$

Clearly $G_\ell \cong \mathrm{Gal}(H_\ell/H_1)$ canonically. By assumption, any prime dividing N is split in K and hence N has a decomposition $N = \mathcal{N}\overline{\mathcal{N}}$. Let $C = E[\mathcal{N}]$. Choose some point $Q \in E[\mathcal{N}]$. We can assume the point $(E, \langle Q\rangle_+^\times)$ is defined over $\tilde{H}_c$ for some integer $c \geq 1$. Note the point (E, C) is defined over H_c.

Assume further that ℓ is inert in K. Then $\mathrm{Gal}(H_{c\ell}/H_c)$, which is canonically isomorphic to $\mathrm{Gal}(\tilde{H}_{c\ell}/\tilde{H}_c)$, acts transitively on the set of cyclic subgroups $M_0, M_1, \ldots, M_\ell$ of order ℓ in A. Hence

$$T_\ell\big((E, \langle Q\rangle_+^\times)\big) = \sum_{s=0}^{\ell} \big(E/M_s, \langle Q\rangle_+^\times (\mathrm{mod}\ M_s)\big) = \mathrm{Tr}_{\tilde{H}_{c\ell}/\tilde{H}_c}\big((E/M_0, \langle Q\rangle_+^\times (\mathrm{mod}\ M_0)\big).$$

Analytically, Shimura shows ([Shi3, Theorem 1]):

$$\theta(a_\ell) \circ \Phi_f = \lambda \circ T_\ell \circ \iota, \tag{10.2}$$

where θ is the ring homomorphism: $\theta : K_f \xrightarrow{\cong} \mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$. Hence we have the following result:

Proposition 10.1.1. *Let ℓ be an odd prime integer, inert in K and $\ell \nmid ND$ and $P_{c\ell}$ be a point on E defined over $\tilde{H}_{c\ell}$, then there exists a point P_c defined over $\tilde{H}_c$ on A_f such that*

$$\mathrm{Tr}_{\tilde{H}_{c\ell}/\tilde{H}_c}(P_{c\ell}) = \theta(a_\ell)P_c. \tag{10.3}$$

For each P_n defined in $\tilde{H}_{nc}$ (recall $(n, c) = 1$ and n is square free), we define $\tilde{P}_n$ as follows:

$$\tilde{P}_n = \mathrm{Tr}_{\tilde{H}_{nc}/\mathcal{M}H_n}(P_n). \tag{10.4}$$

For any prime ℓ relatively prime to nc, by the fact that $\theta(a_\ell)$ is defined over $\mathbb{Q}$ together with the formula (10.3), one has

$$\mathrm{Tr}_{\tilde{H}_{nc}/\mathcal{M}H_n} \circ \mathrm{Tr}_{\tilde{H}_{n\ell c}/\tilde{H}_{nc}}(P_{n\ell}) = \theta(a_\ell) \cdot \mathrm{Tr}_{\tilde{H}_{nc}/\mathcal{M}H_n}(P_n) = \theta(a_\ell) \cdot \tilde{P}_n.$$

The left hand side of the above equality is

$$\mathrm{Tr}_{\tilde{H}_{nc\ell}/\mathcal{M}H_n}(P_{n\ell}) = \mathrm{Tr}_{\mathcal{M}H_{n\ell}/\mathcal{M}H_n} \circ \mathrm{Tr}_{\tilde{H}_{nc\ell}/\mathcal{M}H_{n\ell}}(P_{n\ell}) = \mathrm{Tr}_{\mathcal{M}H_{n\ell}/\mathcal{M}H_n}(\tilde{P}_{n\ell}).$$

Hence $\tilde{P}_n$ enjoys similar properties as those satisfied by point P_n. One also has the following result:

Lemma 10.1.2. *For a fixed prime p and fixed integer $m > 0$, define $\mathcal{K}'_m(p)$ to be the set of primes ℓ such that*

(a) $(\ell, Np) = 1$;

(b) *ℓ is inert in K;*

(c) *ℓ splits in $F = \mathbb{Q}(\sqrt{N})$;*

(d) $\ell \equiv -1 (\mathrm{mod}\ p^m)$.

(e) $a_\ell/p^m \in \mathcal{O}_{K_f}$.

(f) *(ℓ) in K splits completely in $\mathcal{M}$.*

Then $\mathcal{K}'_m(p)$ is non-empty.

Proof. For any integer n, denote by ξ_n a primitive n-th root of unity. Take some integer $m \geq 1$. Let Υ be a polarization map $A_f \to \check{A}_f$. Then we have the Weil pairing $[\,,\,]_W : A_f[p^m] \otimes A_f[p^m] \to \mu_{p^m}$ depending on Υ, where μ_{p^m} is the multiplicative group of p^m-th roots of unity in $\overline{\mathbb{Q}}$. The kernel of the Weil paring is $\ker(\Upsilon) \cap A_f[p^m]$. Set $m_2 = \mathrm{ord}_p(|\ker(\Upsilon)|)$. By [KL, Lemma 3.1.1], there exist points $Q_1, Q_2 \in A_f[p^{m+m_2}]$ such that $[Q_1, Q_2]_W = \xi_{p^m}$. Denote by ϱ the usual complex conjugation. Choose prime ℓ such that Fr_ℓ is in the conjugacy class of ϱ. The Cheborarev theorem shows there are infinitely many such primes. Clearly ℓ is inert in K and since $\varrho\big|_F$ is the identity map, ℓ is split in F. Consider $\varrho\big|_{\mathcal{M}}$ which has order 2. Since ℓ is inert in K, (ℓ) in K must split completely in $\mathcal{M}$. Take the reduction at ℓ, $\overline{A}_f[p^{m+m_2}] \subset \overline{A}_f[\mathbb{F}_{\ell^2}]$. Then by the properties of Weil pairing,

$$[\varrho(Q_1), \varrho(Q_2)]_W = \varrho([Q_1, Q_2]_W) = \varrho(\xi_{p^m}) = \xi_{p^m}^{-1}$$

and

$$[\varrho(Q_1), \varrho(Q_2)]_W = [\overline{\varrho(Q_1)}, \overline{\varrho(Q_2)}]_W = [\mathrm{Fr}_\ell(\bar{Q}_1), \mathrm{Fr}_\ell(\bar{Q}_2)]_W = \xi_{p^m}^{\ell}.$$

Hence

$$\ell + 1 \equiv 0 (\mathrm{mod}\ p^m). \tag{10.5}$$

Since such ℓ is inert in K, (ℓ) in K is totally split in $\mathcal{M}H_c$. Let λ_1 and λ_ℓ be the primes in $\mathcal{M}H_c$ and $\mathcal{M}H_{c\ell}$ above ℓ respectively. Then the residue fields of $\mathcal{M}\tilde{H}_{\ell c}$, $\mathcal{M}\tilde{H}_c$ and K at λ_1, λ_ℓ and (ℓ) are all isomorphic to $\mathbb{F}_{\ell^2}$.

Since $\chi(-1) = 1$ and ℓ splits in F, we deduce that $\chi(\ell) = 1$(cf. e.g. [Bmp, Exercise 1.1.6]), which in turn implies that $\overline{\langle \ell \rangle}$ acts trivially on the points in $\overline{A}_f$. Therefore by Eichler-Shimura relation and (10.2), for any point $P \in \overline{A}_f[p^m]$,

$$\mathrm{Fr}_\ell^2 - \theta(a_\ell)\mathrm{Fr}_\ell + \ell = 0. \tag{10.6}$$

Since in our case Fr_ℓ^2 is the identity map, one has from (10.5), $\theta(a_\ell)\mathrm{Fr}(P) = 0$, which means $\theta(a_\ell) = 0$ on $\overline{A}_f[p^m]$ and so is on $A_f[p^m]$. Consequently $\theta(a_\ell)/p^m$ belongs to $\mathrm{End}(A_f)$, i.e. $a_\ell/p^m \in \mathcal{O}_{K_f}$. □

Fix $\ell \in \mathcal{K}_1'(p)$ which satisfies the conditions of proposition 10.1.1. Since ℓ is inert in K, (ℓ) splits completely in H_1 and each prime in H_1 above (ℓ) is totally ramified in H_ℓ. Also note (ℓ) in K splits completely in $\mathcal{M}$. Hence (ℓ) in K splits completely in $\mathcal{M}H_1$ and any prime in $\mathcal{M}H_1$ above ℓ is totally ramified in $\mathcal{M}H_\ell$. Pick up any prime λ_1 in $\mathcal{M}H_1$ above (ℓ) and any prime λ_ℓ in $\mathcal{M}H_\ell$ above λ_1. From the fact that canonically $\mathrm{Gal}(\mathcal{M}H_\ell/\mathcal{M}H_1) \cong \mathrm{Gal}(H_\ell/H_1)$, one knows that the residue field of $\mathcal{M}H_\ell$ at λ_ℓ is the same as that of $\mathcal{M}H_1$ at λ_1. Therefore, one sees that (10.3) and (10.6) imply

Corollary 10.1.3.

$$\mathrm{Tr}_{\mathcal{M}H_\ell/\mathcal{M}H_1}(\tilde{P}_\ell) \equiv (\ell+1)\tilde{P}_1 (\mathrm{mod}\ \lambda_\ell).$$

This corollary implies

Corollary 10.1.4.

$$\mathrm{Fr}_\ell(\tilde{P}_\ell (\mathrm{mod}\ \lambda_\ell)) = \tilde{P}_1 (\mathrm{mod}\ \lambda_\ell).$$

Proof. For $\ell \in \mathcal{K}_1(p)$, the Eichler-Shimura relation gives

$$T_\ell (\mathrm{mod}\ \lambda_\ell) = \mathrm{Fr}_\ell + \ell \mathrm{Fr}_\ell^{-1}.$$

Note the diamond operator is trivial here since ℓ splitting in F implies $\left(\frac{N}{\ell}\right) = 1$. Since T_ℓ is defined over $\mathbb{Q}$, the relation

$$\mathrm{Tr}_{\tilde{H}_{c\ell}/\tilde{H}_c}(P_\ell) = T_\ell(P_1)$$

implies that

$$\begin{aligned}\mathrm{Tr}_{\mathcal{M}H_\ell/\mathcal{M}H_1}(\tilde{P}_\ell) &= \mathrm{Tr}_{\mathcal{M}H_\ell/\mathcal{M}H_1} \circ \mathrm{Tr}_{\tilde{H}_{c\ell}/\mathcal{M}H_\ell}(P_\ell) \\ &= \mathrm{Tr}_{\tilde{H}_{c\ell}/\mathcal{M}H_1}(P_\ell) \\ &= \mathrm{Tr}_{\tilde{H}_c/\mathcal{M}H_1} \circ \mathrm{Tr}_{\tilde{H}_{c\ell}/\tilde{H}_c H_\ell}(P_\ell) \\ &= \mathrm{Tr}_{\tilde{H}_c/\mathcal{M}H_1} \circ T_\ell(P_1) \\ &= T_\ell \circ \mathrm{Tr}_{\tilde{H}_c/\mathcal{M}H_1}(P_1) \\ &= T_\ell(\tilde{P}_1).\end{aligned}$$

Since λ_1 in $\mathcal{M}H_1$ is totally ramified in $\mathcal{M}H_\ell$,

$$(\mathrm{Fr}_\ell + \ell \mathrm{Fr}_\ell^{-1})(\tilde{P}_1(\mathrm{mod}\ \lambda_\ell)) = (\ell+1)\tilde{P}_\ell(\mathrm{mod}\ \lambda_\ell).$$

Hence

$$(\mathrm{Fr}_\ell^2 + \ell)(\tilde{P}_1(\mathrm{mod}\ \lambda_\ell)) = (1+\ell)\mathrm{Fr}_\ell(\tilde{P}_\ell(\mathrm{mod}\ \lambda_\ell)).$$

We are done since $\mathrm{Fr}_\ell^2 = 1$ in our case. □

One has the following canonical decomposition of the Tate module at a prime integer p:

$$T_p(A_f) \cong \underset{\wp|p}{\oplus} T_\wp(A_f),$$

where $\wp$ runs through all primes in K_f dividing p. Fix such a prime $\wp$ in $\mathcal{O}_{K_f}$ above p. Let prime ℓ be an element in $\mathcal{K}'_m(p)$. The action of Frobenius $\mathrm{Fr}_\ell(\mathcal{M})$ of ℓ in $\mathcal{M}$ on $T_\wp(A_f)$ has characteristic polynomial $1 - a_\ell X + \ell X^2$. From the property of $\mathcal{K}'_m(p)$, $p^m \mid \ell + 1$ and $p^m \mid a_\ell$ in $\mathcal{O}_{K_f}$. Hence one has the following result:

Lemma 10.1.5. $\mathrm{Fr}_\ell(\mathcal{M})$ *acts trivially on* $T_\wp(A_f)/p^m T_\wp(A_f)$ *for any* $\ell \in \mathcal{K}'_m(p)$.

10.2 Kolyvagin system

10.2.1 Local condition

Let K be a non-archimedean local field with residue field $\mathbb{F}$ with characteristic ℓ. Let R be a complete, noetherian, local ring with finite residue field $\Bbbk$ of characteristic $p \neq \ell$.

Let T be a topological R-module with continuous G_K-action. A local condition on T over K is a choice of an R-submodule $H^1_{\mathcal{F}}(K,T)$ of $H^1(K,T)$. Suppose T is unramified with respect to the G_K action, then $H^2(K,T) = 0$ and so one has the exact sequence:

$$0 \to H^1(K^{\mathrm{ur}}/K,T) \xrightarrow{\inf} H^1(G_K,T) \to H^1(I_K,T)^{\mathrm{Gal}(K^{\mathrm{ur}}/K)} \to 0,$$

where I_K is the inertia subgroup of G_K. The group $H^1(K^{\mathrm{ur}}/K,T)$ which is considered to be a subgroup of $H^1(K,T)$ is called the unramified or finite part of $H^1(K,T)$ and is denoted by $H^1_{\mathrm{ur}}(K,T)$. The quotient $H^1(K,T)/H^1(K^{\mathrm{ur}}/K,T) \cong H^1(I_v,T)^{\mathrm{Gal}(K^{\mathrm{ur}}/K)}$ is called the singular part of $H^1(K,T)$, denoted by $H^1_s(K,T)$.

One has the following well-known result ([Rub, p. 13]):

Lemma 10.2.1. *Suppose T is of finite type R-module, the action of G_K on T is unramified and $|\mathbb{F}^\times| \cdot T = 0$, then one has the canonical isomorphisms*

$$H^1_{\mathrm{ur}}(K,T) \cong T/(\mathrm{Fr}_\ell - 1)T \tag{10.7}$$

and

$$H^1_s(K,T) \otimes \mathbb{F}^\times \cong T^{\mathrm{Fr}_\ell - 1}. \tag{10.8}$$

Suppose L/K is a totally ramified abelian extension of degree $|\mathbb{F}^\times|$. Define the *transverse condition* $H^1_{L\text{-tr}}$ to be $H^1(L/K, T^{G_L}) \subset H^1(K,T)$. The subscript L is often omitted if L/K is clear. For such L/K, the following statement holds ([MaRu, p.11]):

Lemma 10.2.2. *Let L/K be defined as above. Then*

$$H^1(K,T) \cong H^1_{\mathrm{ur}}(K,T) \oplus H^1_{\mathrm{tr}}(K,T), \tag{10.9}$$

associated with L.

10.2.2 Selmer structures

We still assume as in the previous section that T is a topological R-module. But in this section we assume that $\mathcal{J}$ is a number field, T has a continuous R-linear action of $G_{\mathcal{J}}$ on it and the action of $G_{\mathcal{J}}$ is unramified outside a finite set of primes of $\mathcal{J}$.

Definition 10.2.3. *A Selmer structure on T is a pair $(\mathscr{F}, \Sigma)$, where Σ is a finite set of places of $\mathcal{J}$ containing all archimedean places, primes at which T is ramified with respect to the action of $G_{\mathcal{J}}$ and all primes above p; and $\mathscr{F}$ is a collection of subgroups $H^1_{\mathscr{F}}(\mathcal{J}_v, T) \subset H^1(\mathcal{J}_v, T)$ such that for each place $v \notin \Sigma$, one has $H^1_{\mathscr{F}}(\mathcal{J}_v, T) = H^1(\mathcal{J}_v^{\mathrm{ur}}/\mathcal{J}_v, T)$. Here $H^1(\mathcal{J}_v^{\mathrm{ur}}/\mathcal{J}_v, T)$ is considered as a subgroup of $H^1(\mathcal{J}_v, T)$ via exact sequence of inflation and restriction maps:*

$$0 \to H^1(\mathcal{J}_v^{\mathrm{ur}}/\mathcal{J}_v, T) \xrightarrow{\inf} H^1(\mathcal{J}_v, T) \to H^1(I_v, T)^{\mathrm{Gal}(\mathcal{J}_v^{\mathrm{ur}}/\mathcal{J}_v)},$$

where I_v is the inertia subgroup of $\mathrm{Gal}(\overline{\mathcal{J}}_v/\mathcal{J}_v)$.

Lemma 10.2.4. *Suppose $\mathcal{J}$ is totally imaginary, then $H^1(\mathcal{J}_v, T) = 0$ for any archimedean place v.*

Proof. Trivial because $\mathcal{J}_v = \mathbb{C}$ now. □

Suppose T' is a submodule(resp. quotient) of T, then it is easy to see a Selmer condition on T induces a Selmer condition on T' under the natural maps of local cohomology. This is called the *propagation* of Selmer structures.

Definition 10.2.5. *The selmer module $H^1_{\mathscr{F}}(\mathcal{J}, T)$ associated with the Selmer structure $(\mathscr{F}, \Sigma)$ on R-module T is the kernel of the map:*

$$H^1(\mathcal{J}_\Sigma/\mathcal{J}, T) \xrightarrow{\oplus \mathrm{loc}_v} \sum_{v\in\Sigma} H^1(\mathcal{J}_v, T)/H^1_{\mathscr{F}}(\mathcal{J}_v, T),$$

where $\mathcal{J}_\Sigma$ is the maximal field extension of $\mathcal{J}$ unramified outside of Σ.

10.2.3 Kolyvagin system

In this section we adopt the notations used in section 10.1. Fix a prime $\ell \in \mathcal{K}'_1(p)$. Then ℓ is inert in K and totally split in $\tilde{H}_c$ hence also in $\mathcal{M}$. Any prime in $\tilde{H}_c$ above ℓ is totally ramified in $\tilde{H}_{c\ell}$. Hence there is no danger to denote by $\mathcal{M}_\ell$ the completion of $\mathcal{M}$ at any prime λ' in $\mathcal{M}$ above ℓ. Let λ_1 be a prime above λ' in $\tilde{H}_c$ and let λ_ℓ be the unique prime above λ_1 in $\tilde{H}_{c\ell}$. Recall T is a topological R-module and $\mathscr{F}$ is a Selmer structure on T.

For a fixed prime p and fixed integer $m > 0$, define $\mathcal{K}_m(p)$ to be the subset of $\mathcal{K}'_m(p)$ such that for each prime ℓ in $\mathcal{K}_m(p)$ satisfies the following extra conditions:

(*a*) $\ell \notin \{N, p\} \cup \Sigma$;

(*b*) Frobenius in $\mathcal{M}$ above ℓ acts trivially on T/p^mT.

We can see here $\mathcal{K}_m(p) \neq \emptyset$ in the case where we are interested in: let $\wp$ be any prime in K_f above p. Take $T = T_\wp(A_f)$. Then lemma 10.1.2 and 10.1.5 show $\mathcal{K}_m(p)$ is not empty. Define $\mathscr{M}_m$ to be the set of positive integers each of which is a product of distinct primes in $\mathcal{K}_m(p)$.

For each $n \in \mathscr{M}_1$, we define a new Selmer structure $\mathscr{F}(n)$ on T by

$$H^1_{\mathscr{F}(n)} = \begin{cases} H^1_{\mathrm{tr}}(\mathcal{M}_\ell, T), & \ell \mid n; \\ H^1_{\mathscr{F}}(\mathcal{M}_\ell, T), & \text{otherwise.} \end{cases}$$

For each $\ell \in \mathcal{K}_1(p)$, define $I_\ell = p^\beta R$, where β is the positive integer which is maximal under the condition $\ell \in \mathcal{K}_\beta(p)$. For $n \in \mathscr{M}_1$, Define

$$I_n = \sum_{\ell|n} I_\ell,\ \Delta_n = \underset{\ell|n}{\otimes} G_\ell.$$

So clearly T/I_nT is annihilated by both $|G_\ell|$ and $\mathrm{Fr}_\ell - 1$ on $\mathcal{M}$ for any $\ell \mid n$.

Let $I \supset I_\ell$ be any ideal in R. Then by (10.9),

$$H^1(\mathcal{M}_\ell, T/IT) \cong H^1_{\mathrm{ur}}(\mathcal{M}_\ell, T/IT) \oplus H^1_{\mathrm{tr}}(\mathcal{M}_\ell, T/IT),$$

associated with $\tilde{H}_{c\ell}$. This makes sense because $\tilde{H}_{c\ell,\lambda_\ell}/\mathcal{M}_\ell$ is a totally ramified abelian extension. By (10.8), we have the canonical isomorphisms ([Rub, §1.2]):

$$H^1_{\mathrm{ur}}(\mathcal{M}_\ell, T/IT) \cong T/IT,\ H^1_{\mathrm{tr}}(\mathcal{M}_\ell, T/IT) \otimes G_\ell \cong T/IT. \tag{10.10}$$

Consequently, one can define an isomorphism ∂_ℓ:

$$\partial_\ell :\ H^1_{\mathrm{ur}}(\mathcal{M}_\ell, T/IT) \cong H^1_{\mathrm{tr}}(\mathcal{M}_\ell, T/IT) \otimes G_\ell\,.$$

For every $n\ell \in \mathscr{M}_1$, one has the following maps

$$\begin{array}{ccc} & & H^1_{\mathscr{F}(n)}(\mathcal{M}, T/I_nT) \otimes \Delta_n \\ & & \Big\downarrow{\scriptstyle \mathrm{loc}_\ell} \\ & & H^1_{\mathrm{ur}}(\mathcal{M}_\ell, T/I_{n\ell}T) \otimes \Delta_n \\ & & \Big\downarrow{\scriptstyle \partial_\ell \otimes 1} \\ H^1_{\mathscr{F}(n\ell)}(E, T/I_{n\ell}T) \otimes \Delta_{n\ell} & \xrightarrow{\mathrm{loc}_\ell} & H^1_{\mathrm{tr}}(\mathcal{M}_\ell, T/I_{n\ell}T) \otimes \Delta_{n\ell} \end{array} \tag{10.11}$$

Definition 10.2.6. *Let $\mathcal{K}(p) \subset \mathcal{K}_1(p)$ and let $\mathscr{M}$ be the set of square free products of primes in $\mathcal{K}(p)$. A Kolyvagin system κ with respect to $(T, \mathscr{F}, \mathcal{K}(p))$ is a collection of elements*

$$\kappa_n \in H^1_{\mathscr{F}(n)}(\mathcal{M}, T/I_nT) \otimes \Delta_n$$

for each $n \in \mathscr{M}$ such that for any $n\ell \in \mathscr{M}$, κ_n and $\kappa_{n\ell}$ agree in (10.11).

10.2.4 Bounding Selmer structures

In this section, R will be the ring of integers of a non-archimedean local field $\mathcal{R}$ whose maximal ideal will be denoted by $\mathfrak{m}$ with a uniformizer ν, and T will be a free R-module of rank 2 with a continuous R-linear action of $G_{\mathcal{J}}$. Recall the finite residue field of R has characteristic p and is denoted by $\Bbbk$. Define $\mathscr{D} := \mathcal{R}/R$, $V := T \otimes_R \mathcal{R}$ and $\overline{V} := V/T$.

Let $(\mathscr{F}, \Sigma)$ be a Selmer structure on V. We can propagate this Selmer structure on T and $\overline{V}$ both of which will be denoted by $\mathscr{F}$. Consequently, the isomorphism $T/\mathfrak{m}^n \cong W[\mathfrak{m}^n]$ identifies the Selmer structure on $T/\mathfrak{m}^n$ propagated from T with the Selmer structure on $\overline{V}[\mathfrak{m}^n]$ propagated from $\overline{V}$.

We assume in this section T satisfies the following conditions:

H1 There is a Galois extension $\mathcal{J}'/\mathbb{Q}$ containing $\mathcal{J}$ such that $G_{\mathcal{J}'}$ acts trivially on T and $H^1(\mathcal{J}'(\mu_{p^\infty})/\mathcal{J}, T/\mathfrak{m}T) = 0$.

H2 $T/\mathfrak{m}T$ is an absolutely irreducible representation of $R/\mathfrak{m}[[G_{\mathcal{J}}]]$ and the action of $G_{\mathcal{J}}$ extends to an action of $G_{\mathbb{Q}}$. Furthermore, the action of complex conjugation ϱ splits $T/\mathfrak{m}T$ into two one-dimensional eigenspaces.

H3 There is a perfect, symmetric and R-bilinear pairing

$$(,)_R : T \times T \to R(1),$$

such that $(x^\sigma, y^{\varrho\sigma\varrho})_R = (x,y)_R^\sigma$ for any $x, y \in T$ and $\sigma \in G_{\mathcal{J}}$. The induced pairing

$$T/\mathfrak{m}T \times T/\mathfrak{m}T \to (R/\mathfrak{m})(1)$$

satisfies

$$(\bar{x}^\varrho, \bar{y}^\varrho)_R = (\bar{x}, \bar{y})_R^\varrho.$$

The pairing $(,)_R$ is a $G_{\mathcal{J}}$-equivariant pairing $T \times T_0 \to R(1)$, where $T_0 = T$ as R-module but with $G_{\mathcal{J}}$-action via conjugation with ϱ. We can give the similar definition of V_0 and $\bar{V}_0$. This induces an isomorphism

$$H^n(\mathcal{J}, T) \cong H^n(\mathcal{J}, T_0).$$

Locally, for any prime v in $\mathcal{J}$,

$$H^1(\mathcal{J}_{v^\varrho}, T) \cong H^1(\mathcal{J}_v, T_0).$$

Tate duality yields a perfect pairing:

$$H^1(\mathcal{J}_v, T) \times H^1(\mathcal{J}_{v^\varrho}, \bar{V}) \to \mathscr{D}, \tag{10.12}$$

and

$$H^1(\mathcal{J}_v, V) \times H^1(\mathcal{J}_{v^\varrho}, V) \to \mathcal{R}. \tag{10.13}$$

We insist here that the Selmer structure $\mathscr{F}$ on T satisfies the following assumption:

- H4 At every place v of $\mathcal{J}$, the local condition $H^1_{\mathscr{F}}(\mathcal{J}_v, V)$ and $H^1_{\mathscr{F}}(\mathcal{J}_{v^\varrho}, V)$ are exact orthogonal complements under the pairings (10.12) and (10.13).
- H5 At every prime p of $\mathbb{Q}$, the module $\oplus_{v|p} H^1_{\mathscr{F}}(\mathcal{J}_v, T/\mathfrak{m}T)$ is stable under the action of $\mathrm{Gal}(\mathcal{J}/\mathbb{Q})$.

Lemma 10.2.7. *There is an integer r and a finite R-module B such that*

$$H^1_{\mathscr{F}}(\mathcal{J}, \overline{V}) \cong \mathscr{D}^r \otimes B \otimes B.$$

Proof. Define a Selmer structure $\mathscr{F}$ on $T_0(\overline{V})$ by means of isomorphism

$$H^1(\mathcal{J}_{v^\varrho}, \overline{V}) \cong H^1(\mathcal{J}_v, T_0(\overline{V})). \tag{10.14}$$

By [Fla], there is a generalized Cassels pairing

$$H^1_{\mathscr{F}}(\mathcal{J}, \overline{V}) \times H^1_{\mathscr{F}}(\mathcal{J}, T_0(\overline{V})) \to \mathscr{D},$$

whose kernels on the left and right are exactly the submodules of R-divisible elements. The identification made via (10.14) gives a pairing:

$$H^1_{\mathscr{F}}(\mathcal{J},\overline{V})\times H^1_{\mathscr{F}}(\mathcal{J},\overline{V})\to\mathscr{D}.$$

By [Fla], the pairing is alternating. □

Before we give the proof of the main theorem of this section, we need to prove several lemmas.

Lemma 10.2.8. *$H^1(\mathcal{J},T)/H^1_{\mathscr{F}}(\mathcal{J},T)$ is torsion free as an R-module.*

Proof. By definition, $H^1_{\mathscr{F}}(\mathcal{J},T)$ is propagated from $H^1_{\mathscr{F}}(\mathcal{J},V)$ which is an $\mathcal{R}$-vector space. Suppose there are a non-zero $r\in R$ and non-zero $\alpha\in H^1(\mathcal{J},T)$ such that $r\alpha\in H^1_{\mathscr{F}}(\mathcal{J},T)$. It is enough to show $\alpha\in H^1_{\mathscr{F}}(\mathcal{J},T)$. For any prime $v\in\Sigma$, denote by $(\alpha)_v$ the local image of α in $H^1_{\mathscr{F}}(\mathcal{J}_v,T)$. Then $r(\alpha)_v$ is the local image of $r\alpha$ in $H^1_{\mathscr{F}}(\mathcal{J}_v,T)$. On the other hand, $H^1_{\mathscr{F}}(\mathcal{J}_v,T)$ is the preimage of $H^1_{\mathscr{F}}(\mathcal{J}_v,V)$ in the map $\vartheta: H^1(\mathcal{J}_v,T)\to H^1(\mathcal{J}_v,V)$. So $\vartheta(r(\alpha)_v)=r\vartheta((\alpha)_v)\in H^1(\mathcal{J}_v,V)$, which is an $\mathcal{R}$-vector space. Since $r\neq 0$, we also have $\vartheta((\alpha)_v)\in H^1(\mathcal{J}_v,V)$. Hence $\alpha\in H^1_{\mathscr{F}}(\mathcal{J},T)$. □

Theorem 10.2.9. *Suppose there is a subset $\mathcal{K}(p)\subset\mathcal{K}_1(p)$ such that $\mathcal{K}_e(p)\subset\mathcal{K}(p)$ for any big enough positive integer e. Suppose there is a collection of cohomology classes*

$$\{\kappa_n\in H^1(\mathcal{J},T/I_nT)\otimes\Delta_n\,\big|\,n\in\mathscr{M}\}$$

such that $\kappa_1\neq 0$ and there exists an integer $u\geq 0$, independent of the choice of elements in $\mathscr{M}$, such that the set of $p^u\kappa_n$ is a Kolyvagin system for $(T,\mathscr{F},\mathcal{K}(p))$. Then $\kappa_1\in H^1_{\mathscr{F}}(\mathcal{J},T)$ and $H^1_{\mathscr{F}}(\mathcal{J},T)$ is free of rank one over R.

Proof. We first deal with $n=1$. $\kappa_1\in H^1(\mathcal{J},T)$. Since $H^1(\mathcal{J},T)\cong\varprojlim_m H^1(\mathcal{J},T/\mathfrak{m}^mT)$ and $\kappa_1\neq 0$, the image of κ_1 in $H^1(\mathcal{J},T/IT)$ is non-zero for $I=p^sR$, where

s is any big enough positive integer. By assumption one can choose s such that $\mathcal{K}_{s+u}(p) \subset \mathcal{K}(p)$. Denote $\mathcal{K}_{s+u}(p)$ by $\tilde{\mathcal{K}}$ and the set of square free products of primes in $\tilde{\mathcal{K}}$ by $\tilde{\mathscr{M}}$. Let $\tilde{\kappa}_n$ be the image of κ_n in $H^1(\mathcal{J}, T/IT) \otimes \Delta_n$. First we prove that the set of $\tilde{\kappa}_n$ is a Kolyvagin system for $(T/IT, \mathscr{F}, \tilde{\mathcal{K}})$ over R/I. For $n = 1$, we need to show $\kappa_1 \in H^1_{\mathscr{F}}(\mathcal{J}, T/IT)$. Since $p^d\kappa_1 \in H^1(\mathcal{J}, T)$, by lemma 10.2.8, $\kappa_1 \in H^1_{\mathscr{F}}(\mathcal{J}, T)$. Hence $\tilde{\kappa}_1 \in H^1_{\mathscr{F}}(\mathcal{J}, T/IT)$. Now assume $n > 1$. Then I_n is generated by I^j for some positive integer j. Clearly, $s + u \leq j$. Now take $n \in \tilde{\mathscr{M}}$ and define $I' = p^{j'}R \supset I_n$, where $j' = s + u$. Multiplication by p^u on T gives a homomorphism

$$\vartheta' : H^1(\mathcal{J}, T/IT) \otimes \Delta_n \to H^1(\mathcal{J}, T/I'T) \otimes \Delta_n.$$

Clearly $\vartheta'(\tilde{\kappa}_n) = \widetilde{p^u\kappa_n} \pmod{I'}$. By assumption, $\widetilde{p^u\kappa_n} \in H^1_{\mathscr{F}(n)}(\mathcal{J}, T/I'T)$, where by abuse of notations, $\widetilde{p^u\kappa_n}$ is the image of $p^u\kappa_n$ in the composition of maps: $H^1(\mathcal{J}, T/I_nT) \otimes \Delta_n \to H^1(\mathcal{J}, T/IT) \otimes \Delta_n \to H^1(\mathcal{J}, T/I'T) \otimes \Delta_n$. Since $\mathscr{F}(n)$ is cartesian ([MaRu, p. 34]), $\tilde{\kappa}_n \in H^1_{\mathscr{F}(n)}(\mathcal{J}, T/IT) \otimes \Delta_n$. It is easy to see the set of κ_n satisfies (10.11).

By [MaRu, p. 28], for each $n \in \tilde{\mathcal{K}}$, one has the isomorphism:

$$H^1_{\mathscr{F}(n)}(\mathcal{J}, \overline{V})[I] \cong H^1_{\mathscr{F}(n)}(\mathcal{J}, T/IT) \cong (R/I)^\delta \oplus M(n)^2$$

for some finite R-module $M(n)$ and $\delta = 0$ or 1. We may assume $\tilde{\mathcal{K}} \subset \mathcal{K}_{2s+u}(p)$. Define $\mathrm{Stub}(n) := n^{\mathrm{length}_R(M(n))} \cdot H^1_{\mathscr{F}(n)}(\mathcal{J}, T/IT)$. Then for each $n \in \tilde{\mathcal{K}}$, $\tilde{\kappa}_n \in \mathrm{Stub}(n)$. In particular, Stub(1) is non-zero and M_1 has length strictly less than that of R/I. This implies $\delta = 1$ and M is finite. □

10.2.5 Kolyvagin system using Heegner points

Recall A_f is the abelian variety defined over $\mathbb{Q}$ associated with a newform $f \in \Gamma_0(N,\chi)$, where χ is a primitive even quadratic Dirichlet character. Without loss of generality, we can assume $\mathcal{O}_{K_f} \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A_f)$ via θ. We also fix an $\mathcal{O}_{K_f}$-linear polarization of A_f. Let $\wp$ be a prime in $\mathcal{O}_{K_f}$ above p. Denoted by $\mathcal{O}_\wp$ the ring of integers of $K_{f,\wp}$, where $K_{f,\wp}$ is the completion of K_f at $\wp$. Denote by $\Bbbk_\wp$ the residue field of $K_{f,\wp}$. Let Σ be a finite set of places of $\mathcal{M}$ containing the archimedean places, the primes above p and primes above $2N$. Denote by $T_\wp$ the Tate module of A_f with respect to $\wp$. Define $V_\wp = T_\wp \otimes_{\mathcal{O}_\wp} K_{f,\wp}$ and $\overline{V}_\wp = V_\wp/T_\wp \cong A_f[\wp^\infty]$. We have the following canonical isomorphism over $\mathcal{O}_{K_f}$:

$$T_p = \underset{\wp|p}{\oplus} T_\wp\,. \tag{10.15}$$

We assume prime p satisfies the following conditions

(A1) p is odd, does not divide the class number of $\mathcal{M}$, N, or the degree of the polarization of A_f.

(A2) The image of $\wp$-adic representation

$$\rho_\wp : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathcal{O}_\wp}(T_\wp(A_f)) \cong \mathrm{GL}_2(\mathcal{O}_\wp)$$

is equal to the subgroup $G_\wp$ consisting of matrices whose determinant lies in $\mathbb{Z}_p^\times \subset \mathcal{O}_\wp^\times$.

The key result here is that condition (A2) holds for almost all p ([Rib2], [Mom]).

Lemma 10.2.10. *For any p satisfying condition* (A2)*, $A_f(L)[\wp]$ is trivial for any solvable extension $L/\mathbb{Q}$.*

Proof. $G_{\mathbb{Q}}$ acts transitively on the non-zero elements of $A_f[\wp]$ and hence $A(L)[\wp]$ is trivial for any finite abelian extension L of $\mathbb{Q}$ and hence for any solvable extension $L/\mathbb{Q}$. □

Corollary 10.2.11. *For any p satisfying condition* (A2)*, $A_f(\mathcal{M})[\wp]$ is trivial.*

Our choice of polarization of A_f gives a perfect, skew-symmetric, $G_{\mathbb{Q}}$-equivariant pairing

$$T_\wp \times T_\wp \to \mathbb{Z}_p(1) \tag{10.16}$$

with self-adjoint $\mathcal{O}_{K_f}$ action. We also have the following properties:

Proposition 10.2.12.

- *$\mathcal{O}_\wp$-module $T_\wp$ is free of rank 2.*
- *The action of the complex conjugation splits $T_\wp$ into two eigenspaces each of which has rank one.*
- *There is a perfect, skew-symmetric, $\mathcal{O}_\wp$-bilinear, $G_{\mathbb{Q}}$-equivariant pairing:*

$$\langle , \rangle_\wp : T_\wp(A_f) \times T_\wp(A_f) \to \mathcal{O}_\wp(1)$$

  such that (10.16) *factors as* $\mathrm{Tr} \circ \langle , \rangle_\wp$*, where* Tr *is the twist of the trace map from $\mathcal{O}_\wp$ to $\mathbb{Z}_p$.*
- $a_\ell \in I_\ell$.

Proof. Fix a complex parametrization $\mathbb{C}^d/\Lambda \cong A_f(\mathbb{C})$. Since $[\mathcal{O}_{K,f} : \mathbb{Z}] = d$, one has

$$T_\wp \cong \Lambda \otimes_{\mathcal{O}_{K_f}} \mathcal{O}_\wp \cong (\mathcal{O}_{K_f} \oplus \mathcal{O}_{K_f}) \otimes_{\mathcal{O}_{K_f}} \mathcal{O}_\wp, \tag{10.17}$$

which is free of rank two as $\mathcal{O}_\wp$-module. Let ϖ be a generator of the inverse different of $\mathcal{O}_\wp/\mathbb{Z}_p$. Then one has the map:

$$\hbar : \mathrm{Hom}_{\mathcal{O}_\wp}(T_\wp, \mathcal{O}_\wp) \to \mathrm{Hom}_{\mathbb{Z}_p}(T_\wp, \mathbb{Z}_p),\ f \mapsto \mathrm{Tr} \circ (\varpi \cdot f).$$

From the definition of different ideals, the definition of $\hbar$ makes sense. It is easy to see from (10.17) that $\hbar$ is an isomorphism. For $s, t \in T_\wp$, define $\langle s, t \rangle_\wp$ as follows. From (10.16), one has the map:

$$T_\wp \to \mathrm{Hom}_{\mathbb{Z}_p}(T_\wp, \mathbb{Z}_p(1)).$$

So s corresponds to a function $f_s \in \mathrm{Hom}_{\mathbb{Z}_p}(T_\wp, \mathbb{Z}_p(1))$ and f_s gives a unique element $g_s \in \mathrm{Hom}_{\mathcal{O}_\wp}(T_\wp, \mathcal{O}_\wp(1))$. Define $\langle s,t\rangle_\wp = g_s(t)$, which has the required properties. As for $a_\ell \in I_\ell$, by definition, $I_\ell = p^\beta \mathcal{O}_\wp$, where β is the maximal integer such that $\ell \in \mathcal{K}_\beta(p)$. Since $\ell \in \mathcal{K}_1(p)$, $\beta \geq 1$ and $p^\beta \mid a_\ell$ in $\mathcal{O}_{K,f}$, i.e. $a_\ell = p^\beta a_0$ for some $a_0 \in \mathcal{O}_{K,f} \subset \mathcal{O}_\wp$. □

Now let $\ell \in \mathcal{K}_1(p)$ and denote $G_\ell = \mathrm{Gal}(\mathcal{M}H_\ell/\mathcal{M}H_1) \cong \mathrm{Gal}(H_\ell/H_1)$, $\mathcal{G}_\mathrm{n} = \mathrm{Gal}(\mathcal{M}H_n/\mathcal{M})$ for $n \in \mathscr{M}_1$, $\mathcal{G} = \mathrm{Gal}(\mathcal{M}H_1/\mathcal{M})$, and $n_\ell = \#G_\ell$.

Since ℓ is inert in K and $G_\ell \cong \mathrm{Gal}(H_\ell/H_1) \cong (\mathcal{O}_K/(\ell))^\times/(\mathbb{Z}/\ell\mathbb{Z})^\times$, $n_\ell = \ell + 1$. For each $n \in \mathscr{M}_1$, clearly $G_n \cong \prod_{\ell|n} G_\ell$ canonically. Therefore, there is a natural projection $\eta_n : \mathbb{Z}[\mathcal{G}_n] \to \mathbb{Z}[\mathcal{G}]$. Define $S = \sum_{\sigma\in\mathcal{G}} \sigma$. Let $\tilde{S}_n$ be an element in $\eta_n^{-1}(S)$. Since G_ℓ is a cyclic group, we can fix a generator σ_ℓ, and define:

$$S_\ell = \sum_{\sigma\in G_\ell} \sigma,\ D_\ell = \sum_{i=0}^{n_\ell - 1} i\sigma_\ell^i,\ \tilde{S}_\ell = S_\ell \tilde{S}_1,\ \tilde{D}_\ell = D_\ell \tilde{S}_n.$$

For $n \in \mathscr{M}_1$, define $D_n = \prod_{\ell|n} D_\ell$ and $\tilde{D}_n = D_n \tilde{S}_1$. Let $\tilde{P}_n \in A_f(\mathcal{M}H_n)$ be the point of level n in the Heegner system associated with $(A_f, \mathcal{M})$ as constructed before. Denote by $c(n)$ the image of $\tilde{P}_n$ of the natural map

$$\varphi_n : A_f(\mathcal{M}H_n) \to A_f(\mathcal{M}H_n) \otimes_{\mathcal{O}_{K_f}} \mathcal{O}_\wp \to H^1(\mathcal{M}H_n, T_\wp).$$

The image of $c(n)$ in the natural map $H^1(\mathcal{M}H_n, T_\wp) \to H^1(\mathcal{M}H_n, T_\wp/I_nT_\wp)$ is denoted by $\tilde{c}(n)$.

Lemma 10.2.13. *$\tilde{D}_n\tilde{c}(n)$ is fixed under the action of $\mathcal{G}_n$.*

Proof. One has

$$\begin{aligned}(\sigma_\ell - 1)D_\ell &= \sum_{i=0}^{n_\ell - 1} i\sigma_\ell^{i+1} - \sum_{i=0}^{n_\ell - 1} i\sigma_\ell^i \\ &= (n_\ell - 1) + \sum_{i=1}^{n_\ell - 1}(i-1)\sigma_\ell^i - \sum_{i=1}^{n_\ell - 1} i\sigma_\ell^i \\ &= (n_\ell - 1) - \sum_{i=1}^{n_\ell - 1}\sigma_\ell^i = n_\ell - S_\ell\,.\end{aligned}$$

Hence

$$\begin{aligned}(\sigma_\ell - 1)D_n\tilde{P}_n &= (\sigma_\ell - 1)D_\ell D_{n/\ell}\tilde{P}_n \\ &= D_{n/\ell}(n_\ell - S_\ell)\tilde{P}_n \\ &= n_\ell D_{n/\ell}\tilde{P}_n - \theta(a_\ell)D_{n/\ell}\tilde{P}_{n/\ell}.\end{aligned} \tag{10.18}$$

$\tilde{P}_n$ is mapped to an element $\varphi \in H^1(\mathcal{M}H_n, T_p)$ because $\varphi(\omega) = \omega(\alpha) - \alpha$ for any $\omega \in G_{\mathcal{M}H_n}$ and for some $\alpha = (\alpha_1, \cdots, \alpha_h, \cdots)$ such that $p^h\alpha_h = P_n$, and then is projected to an element in $H^1(\tilde{H}_{cn}, T_\wp)$ via (10.15). One has

$$\begin{aligned}\big((\sigma_\ell - 1)D_n \cdot \varphi\big)(\omega) &= [(\sigma_\ell - 1)D_\ell D_{n/\ell}]\big(\varphi\big([(\sigma_\ell - 1)D_\ell D_{n/\ell}]^{-1}\omega[(\sigma_\ell - 1)D_\ell D_{n/\ell}]\big)\big) \\ &= \omega\big([(\sigma_\ell - 1)D_\ell](D_{n/\ell})\alpha\big) - [(\sigma_\ell - 1)D_\ell](D_{n/\ell})\alpha\end{aligned}$$

From (10.18) and the fact $p \mid n_\ell$ and $a_\ell \in I_\ell \subset I_n$, one has $(\sigma_\ell - 1)D_n\varphi = 0$ when φ is considered as an element in $H^1(\tilde{H}_{cn}, T_p/I_nT_p)$. Therefore, $D_n \cdot \varphi$ is fixed by σ_ℓ, hence by G_ℓ and consequently fixed by G_n Hence from the definition of $\tilde{S}_n$ one sees $\tilde{D}_n\tilde{c}(n)$ is fixed by $\mathcal{G}_n$. □

Since $A_f(\mathcal{M}H_n)[\wp] = 0$, by the Hochschild-Serre spectral sequence, restriction gives an isomorphism

$$H^1(\mathcal{M}, T_\wp/I_nT_\wp) \xrightarrow{\cong} H^1(\mathcal{M}H_n, T_\wp/I_nT_\wp)^{\mathcal{G}_n}. \tag{10.19}$$

This isomorphism implies there is a unique element $d(n) \in H^1(\mathcal{M}, T_\wp/I_nT_\wp)$ corresponding to $D_nc(n)$. Define $\tilde{d}(n)$ to be $d(n) \otimes_{\ell|n} \sigma_\ell \in H^1(A_f, T_\wp/I_nT_\wp) \otimes \Delta_{\mathrm{n}}$.

We define the canonical Selmer structure $(\mathscr{F}_0, \Sigma)$ on V for any Galois extension J of $\mathbb{Q}$ containing $\mathcal{M}$ by taking the unramified local condition at any place v' of J not dividing p and by taking the image of the local Kummer map

$$A_f(J_{v'}) \otimes_{\mathcal{O}_{K_f}} K_f \to H^1(J_{v'}, V).$$

We also propagate $\mathscr{F}_0$ on T and $\overline{V}$ which are also denoted by $\mathscr{F}_0$. One can prove the following two results ([Rub, §1.3–1.6]).

Lemma 10.2.14. *Let J be any Galois extension of $\mathbb{Q}$ containing $\mathcal{M}$ and v' be any prime in J. Then the following sequence is exact:*

$$0 \to H^1_{\mathscr{F}_0}(J_{v'}, \overline{V}) \to H^1(J_{v'}, \overline{V}) \to H^1(J_{v'}, A_f(\bar{J}))[\wp^\infty] \to 0. \tag{10.20}$$

If $v' \nmid p$, then

$$H^1_{\mathscr{F}_0}(J_{v'}, V) = H^1_{\mathscr{F}_0}(J_{v'}, \overline{V}) = 0. \tag{10.21}$$

Consequently there is an exact sequence

$$0 \to A_f(\mathcal{M}) \otimes_{\mathcal{O}_{K_f}} \mathcal{O}_\wp \to H^1_{\mathscr{F}_0}(K_{f,\wp}/\mathcal{O}_\wp) \to H^1_{\mathscr{F}_0}(\mathcal{M}, \overline{V}) \to Ш(A_f/\mathcal{M})[\wp^\infty] \tag{10.22}$$

Lemma 10.2.15. *There exists an integer α_f in dependent of ℓ such that $\alpha \cdot d(\ell) \in H^1_{\mathscr{F}_0(\ell)}(A_f, T_\wp/I_\ell T_\wp)$.*

Proof. We can identify T/I_nT with $\overline{V}[I_n]$. Let v be any prime in $\mathcal{M}$. First assume $v \nmid np$. If v is archimedean, from lemma 10.2.4, there is nothing to prove. Now we assume v is finite. Let λ be any prime in $\mathcal{M}H_n$ above v. From (10.20) and (10.21), One has the following composition:

$$A_f(\mathcal{M}H_n) \to A_f((\mathcal{M}H_n)_\lambda) \to H^1((\mathcal{M}H_n)_\lambda, \overline{V}[I_n])$$

$$\to H^1((\mathcal{M}H_n)_\lambda, \overline{V}) \cong H^1((\mathcal{M}H_n)_\lambda, A_f)[\wp^\infty].$$

The image of $\tilde{P}_n$ in $H^1(\mathcal{M}H_n, A_f)$ is zero and hence is zero in $H^1((\mathcal{M}H_{nc})_\lambda, \overline{V})$. So the image of $\tilde{D}_n\tilde{c}_n$ under the natural map $H^1(\mathcal{M}H_{nc}, \overline{V}[I_n]) \to H^1((\mathcal{M}H_{nc})_\lambda, \overline{V})$ is trivial. From the inflation-restriction exact sequence

$$0 \to H^1((\mathcal{M}H_n)_\lambda/\mathcal{M}_v, \overline{V}[I_n]) \to H^1(\mathcal{M}_v, \overline{V}[I_n]) \to H^1((\mathcal{M}H_n)_\lambda, \overline{V}[I_n]),$$

one knows $\tilde{D}_n\tilde{c}_n$ actually lies in $H^1((\mathcal{M}H_n)_\lambda/\mathcal{M}_v, \overline{V}[I_n])$. Because v does not divide np, v is unramified in $\mathcal{M}H_n$, and therefore $(\mathcal{M}H_n)_\lambda \subset \mathcal{M}_v^{\mathrm{ur}}$. Hence we have the inflation-restriction exact sequence:

$$0 \to H^1((\mathcal{M}H_n)_\lambda, \overline{V}[I_n]) \to H^1_{\mathrm{ur}}(\mathcal{M}_v, \overline{V}[I_n]) \to H^1((\mathcal{M}H_n)_\lambda/\mathcal{M}_v, \overline{V}[I_n]).$$

Therefore, $\tilde{D}_n\tilde{c}_n$ can be regarded to be in $H^1_{\mathrm{ur}}(\mathcal{M}_v, \overline{V}[I_n])$ and so can $d(n)$ under (10.19). Let $G^0(\mathcal{A}_{f,v})$ be the group of components of the Néron model $\mathcal{A}_{f,v}$ of A_f at v. Then by [Mil1, p. 47],

$$H^1(\mathcal{M}_v^{\mathrm{ur}}/\mathcal{M}_v, A_f(\mathcal{M}_v^{\mathrm{ur}})) = H^1(\mathcal{M}_v^{\mathrm{ur}}/\mathcal{M}_v, G^0(\mathcal{A}_{f,v}).$$

Since the group of components is a finite group scheme, Tamagawa number of A_f at v is $|H^1(\mathcal{M}_v^{\mathrm{ur}}/\mathcal{M}_v, G^0(\mathcal{A}_{f,v})| = |H^1(\mathcal{M}_v^{\mathrm{ur}}/\mathcal{M}_v, A_f(\mathcal{M}_v^{\mathrm{ur}}))|$. Hence $|H^1(\mathcal{M}_v^{\mathrm{ur}}/\mathcal{M}_v, \overline{V})| = |H^1(\mathcal{M}_v^{\mathrm{ur}}/\mathcal{M}_v, A_f[\wp^\infty])|$ is the p-part $c_{v,p}$ of the Tamagawa number at v. Define

$$\alpha_f = \prod_v c_{v,p},$$

then $\alpha_f d(n)$ has trivial image in $H^1(\mathcal{M}_v, \overline{V})$. Hence by (10.21) and the definition of propagation of Selmer structures, $\alpha_f d(n)$ lines in $H^1_{\mathscr{F}_0}(\mathcal{M}_v, \overline{V}[I_n])$.

Now suppose $v|n$ and is above a prime number $\ell|n$. Let λ' be a prime in $\mathcal{M}H_\ell$ above v. It is enough to show $d(n)$ has trivial image in $H^1((\mathcal{M}H_\ell)_{\lambda'}, \overline{V}[I_n])$. Define

$$H^1((\mathcal{M}H_n)_v, \overline{V}[I_n]) = \underset{w|v}{\oplus} H^1((\mathcal{M}H_n)_w, \overline{V}[I_n]).$$

Since λ' is totally split in $\mathcal{M}H_n$, it is enough to check that the image of $\tilde{D}_n\tilde{c}_n$ in $H^1((\mathcal{M}H_n)_v, \overline{V}[I_n])$ is trivial. Since v does not divide p, the image of $\tilde{c}_n$ in $H^1((\mathcal{M}H_n)_w, \overline{V}[I_n])$ is unramified, and hence it is in $H^1_{\mathrm{ur}}((\mathcal{M}H_n)_w, \overline{V}[I_n])$. By (10.10), one has the G_n-module isomorphism

$$H^1_{\mathrm{ur}}((\mathcal{M}H_n)_w, \overline{V}[I_n]) \cong \overline{V}[I_n],$$

by evaluating the Frobenius element. Hence

$$H^1_{\mathrm{ur}}((\mathcal{M}H_n)_v, \overline{V}[I_n]) = \underset{w|v}{\oplus} \overline{V}[I_n]$$

and the action of G_n is just to permute the summands. In particular G_ℓ acts trivially since all primes in $\mathcal{M}H_{n/\ell}$ above ℓ are totally ramified in $\mathcal{M}H_n$. Hence the action of D_ℓ on $H^1_{\mathrm{ur}}((\mathcal{M}\tilde{H}_n)_v, \overline{V}[I_n])$ is just the multiplication by $(|G_\ell| \cdot (G_\ell - 1))/2 \in I_\ell \subset I_n$. This shows $\tilde{D}_n\tilde{c}_n$ is trivial in $H^1((\mathcal{M}H_n)_v, \overline{V}[I_n])$.

Suppose $v|p$. By (10.20), it is enough to show the image of $d(n)$ in the composition

$$H^1(\mathcal{M}, \overline{V}[I_n]) \to H^1(\mathcal{M}_v, \overline{V}) \to H^1(\mathcal{M}_v, A_f)$$

is trivial. Consider the commutative diagram

$$\begin{array}{ccc} H^1(\mathcal{M}_v, \overline{V}[I_n]) & \longrightarrow & \underset{w|v}{\oplus} H^1((\mathcal{M}H_n)_w, \overline{V}[I_n]) \\ \downarrow & & \downarrow \\ H^1(\mathcal{M}_v, A_f) & \longrightarrow & \underset{w|v}{\oplus} H^1((\mathcal{M}H_n)_w, A_f) \end{array} \tag{10.23}$$

Since $c(n)$ is in the image of P_n under the global Kummer map, the image of $d(n)$ in the left right corner is trivial. Since A_f has good reduction at v, [Mil1, p. 47] gives

$$H^1(\mathcal{M}_v^{\mathrm{ur}}/\mathcal{M}_v, A_f(\mathcal{M}_v^{\mathrm{ur}})) = 0.$$

Since w over v is unramified, there is the inflation-restriction exact sequence:

$$0 \to H^1((\mathcal{M}H_n)_w/\mathcal{M}_v, A_f((\mathcal{M}H_n)_w)) \to H^1(\mathcal{M}_v^{\mathrm{ur}}/\mathcal{M}_v, A_f(\mathcal{M}_v^{\mathrm{ur}})) \to H^1(\mathcal{M}_v^{\mathrm{ur}}/\tilde{H}_{nc,w}, A(\mathcal{M}_v^{\mathrm{ur}})).$$

Hence one has

$$H^1((\mathcal{M}H_n)_w/\mathcal{M}_v, A_f((\mathcal{M}H_n)_w)) = 0.$$

So from the inflation-restriction exact sequence

$$0 \to H^1((\mathcal{M}H_n)_w/\mathcal{M}_v, A_f((\mathcal{M}H_n)_w)) \to H^1(\mathcal{M}_v, A_f) \to H^1((\mathcal{M}H_n)_w, A),$$

one sees the bottom line of the diagram (10.23) is injective. Hence the image of $d(n)$ in $H^1(\mathcal{M}_v, A_f)$ is trivial. □

We also need the following result ([McC, Proposition 4.4]):

Lemma 10.2.16. *For every ℓ, there is an $\mathcal{O}_\wp$-automorphism η_ℓ such that the isomorphism:*

$$\varpi : H^1_{\mathrm{ur}}(\mathcal{M}_\ell, T_\wp/I_\ell T_\wp) \cong T_\wp/I_\ell T_\wp \xrightarrow{\eta_\ell} T_\wp/I_\ell T_\wp \cong H^1_{\mathrm{tr}}(\mathcal{M}_\ell, T_\wp/I_\ell T_\wp) \otimes \Delta_\ell$$

satisfies $\varphi(\mathrm{loc}_\ell(\alpha_f d(n))) = \mathrm{loc}_\ell(\alpha_f d(n\ell)) \otimes \sigma_\ell$ for every n such that $n\ell \in \mathscr{M}$. If $n \in \mathscr{M}$, elements in $\left\{\eta_\ell \,\middle|\, \ell | n\right\}$ commute with each other.

Now we can prove the main result of this chapter:

Theorem 10.2.17. *The $\mathcal{O}_\wp$-module $A_f(\mathcal{M}) \otimes_{\mathcal{O}_{K_f}} \mathcal{O}_\wp$ is free of rank one and the $\wp$-primary part of $Ш(A_f/\mathcal{M})$ is finite.*

Proof. For each $n \in \mathscr{M}_1$ and prime $\ell \mid n$, η_ℓ in Lemma 10.2.16 induces an automorphism on $H^1(\mathcal{M}, T/I_n T)$, which is still denoted by η_ℓ. Define η_n be the composition

of all η_ℓ for all $\ell \mid n$. The property shown in the Lemma 10.2.16 implies the collection of

$$d(n)' = \alpha_f \eta_n^{-1}(\tilde{d}(n)) \in H^1_{\mathscr{F}_0(n)}(\mathcal{M}, T_\wp/I_n T_\wp) \otimes \Delta_n$$

is a Kolyvagin system for $(T_\wp, \mathscr{F}, \mathcal{K}_1(p))$. Take $n = 1$. By convention, $G_1 = 1$ and hence $\tilde{d}(1) = d(1)$ which corresponds to

$$\tilde{D}_1 \tilde{c}(1) = D_1 \tilde{S}_1 c(1) = \sum_{\sigma \in \mathcal{G}} \varphi_1(P_1) = \varphi_1(\sum_{\sigma \in \mathcal{G}} P_1).$$

Hence it is non-zero by our assumption.

Now we only need to check (H1)-(H5) holds. By assumption, the image $G_\mathcal{M} \to \mathrm{Aut}_{\mathcal{O}_\wp}(T_\wp(A_f))$ is equal to $G_\wp$ determinant of any element of which lies in $\mathbb{Z}_p^\times$. Take $\mathcal{M}' = \mathcal{M}(A_f[\wp^\infty])$. Then $H^1(\mathcal{M}'/\mathcal{M}, A_f[\wp]) \cong H^1(G_\wp, A_f[\wp])$ from Corollary 10.2.11. By embedding $\mathbb{Z}_p^\times$ into $G_\wp$ diagonally, $\mathbb{Z}_p^\times$ can be regarded as a subgroup of $G_\wp$. Since the order of μ_{p-1} is $p-1$, which is coprime to the order of $A_f[\wp]$, $H^n(\mu_{p-1}, A_f[\wp]) = 0$ for any $n \geq 1$. Since p is odd, μ_{p-1} is not trivial, and therefore $H^0(\mu_{p-1}, A_f[\wp]) = 0$. Consequently, from the spectral sequence $H^m(\mathbb{Z}_p^\times/\mu_{p-1}, H^n(\mu_{p-1}, A_f[\wp])) \Rightarrow H^{m+n}(\mathbb{Z}_p^\times, A_f[\wp])$, one sees $H^n(\mathbb{Z}_p^\times, A_f[\wp]) = 0$ for any integer $n \geq 0$. Therefore from the spectral sequence $H^m(G_\wp/\mathbb{Z}_p^\times, H^n(\mathbb{Z}_p^\times, A_f[\wp])) \Rightarrow H^{m+n}(G_\wp, A_f[\wp])$, one sees $H^n(G_\wp, A[\wp]) = 0$ for any integer $n \geq 0$. In particular $H^1(G_\wp, A_f[\wp]) = 0$ and hence $H^1(\mathcal{M}'/M, A_f[\wp]) = 0$, i.e. (H1) holds. Proposition 10.2.12 and the fact $G_\wp$ acts transitively on non-zero elements of $A_f[\wp]$ give (H2). Using the pairing $\langle , \rangle_\wp$ in Proposition 10.2.12, define $(x, y)_\wp = \langle x, y^\varrho \rangle_\wp$. Then $(,)_\wp$ satisfies (H3). (H4) is the local Tate pairing. (H5) is trivial.

□

Bibliography

[BSD] B. J. Birch and H. P. F. S. Dyer, *Notes on elliptic curves II*, J. Reine Angew. Math. **218** (1965), 79–108. 1

[BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*. J. Amer. Math. Soc. **14** (2001), no. 4, 843–939. 37

[Bmp] D. Bump, *Automorphic forms and representations*. Cambridge University Press, 1997. 76

[Cas] W. Casselman, *On abelian varieties with many endomorphisms and a conjecture of Shimura's*, Inventiones Math. **12** (1971), 225–236. 40

[Co] S. Comalada, *Elliptic curves with trivial conductor over quadratic fields*, Pacific J. Math. **144** (1990), 237-258. 40

[CoRu] B. Conrad and K. Rubin (eds), *Arithmatic Algebraic Geometry*, Americal Mathematical Society, 2001. 13, 15, 17

[Cox] D. A. Cox, *Primes of the form* x^2+ny^2*: Fermat, class field theory, and complex multiplication.* John Wiley & Sons (1989). 62

[Cre] J. E. Cremona, *Modular symbols for* $\Gamma_1(N)$ *and elliptic curves with everywhere good reduction*, Math. Proc. Camb. Phil. Soc, **111**(1992), 199–218. 40, 58

[Dab] M. Daberkow, *On computations in Kummer extensions*. J. Symbolic Computation **31** (2001), 113–131. 61

[DL] H. Darmon and A. Logan, *Periods of Hilbert modular forms and rational points on elliptic curves*. International Math. Res. Not. **40** (2003), 2153–2180. i, iii, 5, 59, 67, 70, 71

[Dar] H. Darmon, *Rational points on modular elliptic curves*, CBMS **101**, American Mathematical Society, 2004. 1, 27, 33, 37, 41

[Dia] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics **228**, Springer-Verlag, 2005. 9

[DRZ] H. Darmon, V. Rotger, and Y. Zhao, *The Birch and Swinnerton-Dyer conjecture for* $\mathbb{Q}$*-curves and Oda's period relations.* Submitted. 3, 4

[Fla] M. Flach, *A generalisation of the Cassels-Tate pairing*, J. Reine Angew. Math. **412** (1990), 113–127. 84, 85

[Gar] J. Gärtner. *Points de Darmon et variétés de Shimura*. Thèse de Doctorat, Université Paris 7 (Jussieu) (2010). 67

[Ge] S. Gelbart. *Automorphic forms on adèle groups*. Ann. of Math. Studies **83**, Princeton Univ. Press, Princeton, NJ (1975). 40

[GG] E. González and X. Guitart, *On the modularity level of modular abelian varieties over number fields*, J. Number Theory **130** (2010), no. 7, 1560–1570. 25, 44

[GL] J. González and J.-C. Lario, *Q-curves and their Manin ideals*, Amer. J. Math**123**(2001), no.3, 475–503. 24

[Gro] B. Gross, *Kolyvagin's work on modular elliptic curves* in *L-functions and arithmetics, proceedings of the Durham symposium, July 1989*, J. Coates and M. J. Taylor (eds), Cambridge University Press, 1991. 73

[GZ] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*. Invent. Math. **84** (1986), no. 2, 225–320. 2, 36, 38, 40

[Har] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer-Verlag, 1977. 16

[Hec] E. Hecke, *Lectures on the theory of algebraic numbers.* Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen. Graduate Texts in Mathematics, 77. Springer-Verlag, New York-Berlin (1981). 61

[Hil] D. Hilbert, *Über die Theories des relativquadratischen Zahlkörpers*. Math. Ann. **51** (1899), 1–127. 64

[How] B. Howard, *Iwasawa theory of Heegner points on abelian varieties of* GL_2*-type*, Duke Math. J. **124** (2004), no.1, 1–45. 73

[HSW] J. G. Huard, B. K. Spearman, and K.S. Williams, *Integral bases for quartic fields with quadratic subfields*. J. Number Theory **51** (1995), no. 1, 87–102. 64

[KL] V. A. Kolyvagin and D. Yu. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Leningrad Math. J. **1** (1990), no. 5, 1229–1253. 44, 76

[Kol1] V. A. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $Ш(E,\mathbb{Q})$ *for a subclass of Weil curves*, Math. USSR Izvestiya **32** (1989), 523–541. 2, 36, 38, 40, 73

[Kol2] ———, *On the Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, Math. USSR Izvestiya **33** (1989), 473–499. 2

[Kol3] ———, *Euler systems* in *The Grothendieck festschrift volume II, a collection of articles written in honor of the 60th birthday of Alexander Grothendieck*, P. Cartier, L. Illusie, N. M. Katz, G. Laumon, Y. I. Manin, and K. Ribet (eds), Birkhäuser, 2007. 2, 73

[Kna] A. W. Knapp, *Elliptic curves*, Princeton University Press, 1993. 31

[KW] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture I, II.* Invent. Math. **178** (2009), no. 3, 485–504 and 505–586. 3, 22

[Lan1] S. Lang, *Elliptic functions* (*2nd ed*),Springer-Verlag, 1987. 27, 54

[Lan2] ———, *Survey of Diophantine geometry*, Springer-Verlag, 1997. 1, 2

[Lo] M. Longo, *On the Birch and Swinnerton-Dyer conjecture for modular elliptic curves over totally real fields*. Ann. Inst. Fourier (Grenoble) **56** (2006), no. 3, 689–733. 41

[MaRu] B. Mazur and K. Rubin, *Kolyvagin Systems,* Memoirs of the American Mathematical Society **799** (2004). Available online at `http://math.stanford.edu/~rubin/preprints/kolysys.pdf`. 79, 86

[McC] W. McCallum, *Kolyvagin's work on Shafarevich-Tate groups* in *L-functions and arithmetics, proceedings of the Durham symposium, July 1989*, J. Coates and M. J. Taylor (eds), Cambridge University Press, 1991. 94

[Mil1] J. S. Milne, *Arithmetic duality theorems*, Academic Press Inc., 1986. 92, 94

[Mil2] ———, *Class field theory (version 4.00)*. Available online at `http://www.jmilne.org/math`. 62, 66

[Mom] F. Momose, *On the ℓ-adic representations attached to modular forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981),89–109. 87

[Neu] J. Neukirch, *Algebraic number theory*, Springer-Verlag, 1999. 48

[Oda] T. Oda, *Periods of Hilbert modular sjrfaces*, Birkhäuser, 1982. 68

[Pa] A. Pacetti, On the change of root number under twisting and applications, available at arXiv:1010.3781. 40

[PA] PARI/GP, version `2.3.4`, Bordeaux (2008). Available at `http://pari.math.u-bordeaux.fr/`. 58

[Rib1] K. Ribet, *Galois representations attached to eigenforms with nebentypus*, Modular functions of one variable V, Lectur Notes of Mathematics **601**, *Springer-Verlag*,1977.

[Rib2] ———, *On ℓ-adic representations attached to modular forms II*, Glasgow Math. J. **27** (1985) 185–194. 87

[Rib3] ———, *Galois representation attached to eigenforms with nebentypus*, Lecture Notes in Mathematics **601**, Springer-Verlag, 1977. 19

[Rib4] ———, *Twists of modular forms and endomorphisms of abelian varieties,* Math. Ann. **253** (1980), 43–62. 19

[Rib5] ———, *Abelian varieties over $\mathbb{Q}$ and modular forms.* Algebra and topology 1992 (Taejŏn), Korea Adv. Inst. Sci. Tech., Taejŏn (1992), 53–79. 3, 22, 23, 44

[Ro] D.E. Rohrlich. *Nonvanishing of L-functions and structure of Mordell-Weil groups.* Journal für di Reine und Angewand. Math. **417** (1991), 1–26. 40

[Ro2] D.E. Rohrlich. *Variation of the root number in families of elliptic curves.* Compositio Math. **87** (1993) 119–151. 40

[Rub] K. Rubin, *Euler systems*, Annal of Math. Study **147**, Princeton University Press, 2000. 79, 82, 91

[Sch] B. Schoeneberg, *Elliptic modular functions – an introduction*, Springer-Verlag, 1974. 31

[Shi1] G. Shimura, *Class fields over real quadratic fields and Hecke operators*, Ann. of Math.**95** (1972), 130–190. 3, 11, 23, 44

[Shi2] ———, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten, Publishers and Princeton University Press, 1971. 3, 13, 44, 54

[Shi3] ———, *On the factors of the Jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), no.3, 523–544. 74

[Shio] K. Shiota, *On the explicit models of Shimura's elliptic curves*, J.Math. Soc. Japan**38** (1986), no.4, 649–659. 58

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) **141** (1995), no. 3, 553–572. 37

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. 37

[YZZ] X. Yuan, W. Zhang, and S. Zhang, *Heights of CM points I: Gross–Zagier formula*. Preprint. 48

[Zh1] S. Zhang, *Heights of Heegner points on Shimura curves.* Ann. of Math. (2) **153** (2001), no. 1, 27–147. i, iii, 2, 39, 40

[Zh2] ———, *Arithmetic of Shimura curves*. Science China Mathematics **53** (2010), 573–592. 48