2-Selmer groups and Heegner points on elliptic curves

The Harvard community has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th>Citation</th>
<th>Li, Chao. 2015. 2-Selmer groups and Heegner points on elliptic curves. Doctoral dissertation, Harvard University, Graduate School of Arts &amp; Sciences.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessed</td>
<td>September 23, 2017 1:12:12 AM EDT</td>
</tr>
<tr>
<td>Citable Link</td>
<td><a href="http://nrs.harvard.edu/urn-3:HUL.InstRepos:17464036">http://nrs.harvard.edu/urn-3:HUL.InstRepos:17464036</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at <a href="http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA">http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA</a></td>
</tr>
</tbody>
</table>

(Article begins on next page)
2-Selmer groups and Heegner points on elliptic curves

A dissertation presented

by

Chao Li

to

The Department of Mathematics

in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy
in the subject of
Mathematics

Harvard University
Cambridge, Massachusetts

April 2015
2-Selmer groups and Heegner points on elliptic curves

Abstract

This thesis studies several aspects of the arithmetic of elliptic curves. In particular, we explore the prediction of the Birch and Swinnerton-Dyer conjecture when the 2-Selmer group has rank one.

For certain elliptic curves $E/\mathbb{Q} : y^2 = F(x)$ with additive reduction at 2, we determine their 2-Selmer ranks in terms of the 2-rank of the class group of the cubic field $L = \mathbb{Q}[x]/F(x)$. We then interpret this result as a mod 2 congruence between the Hasse-Weil $L$-function of $E$ and a degree two Artin $L$-function associated to the cubic field $L$.

When the class number of $L$ is odd, the Birch and Swinnerton-Dyer conjecture predicts that $E$ should have rank one over $\mathbb{Q}(i)$. To construct such a point on $E$, we study Heegner points on Shimura curves with non-maximal level at a prime $p$ ramified in the quaternion algebra (in the special case when $p = 2$). These curves have a $p$-adic uniformization by a tame étale covering of Drinfeld’s $p$-adic half-plane. We use the covering to describe the geometry of their reduction mod $p$ and compute the Néron model of their Jacobians.

For certain elliptic curves $E/\mathbb{Q}$ with good or multiplicative reduction at 2, we study their 2-Selmer groups over imaginary quadratic fields using the method of level raising of modular forms mod $p = 2$. We prove a parity result (predicted by the Birch and Swinnerton-Dyer conjecture) for 2-Selmer ranks. We also show that there is an obstruction for lowering the 2-Selmer ranks, revealing a different phenomenon compared to odd $p$. 
Contents

1 Introduction ......................................................... 1
  1.1 The Birch and Swinnerton-Dyer conjecture .................. 1
  1.2 \( p \)-Selmer groups ...................................... 3
  1.3 Heegner points ........................................... 5
  1.4 2-Selmer groups and 2-class groups ..................... 6
  1.5 Heegner points and bad reduction of Shimura curves at \( p \) when \( p^2 \mid N \) ... 8
  1.6 Level raising and rank lowering ......................... 10
  1.7 Obstruction for rank lowering ........................... 11

2 2-Selmer groups and 2-class groups ................................. 13
  2.1 2-Selmer groups .......................................... 15
  2.2 Kummer maps ............................................. 16
  2.3 Local conditions ........................................ 19
  2.4 2-class groups of cubic fields .......................... 22

3 Artin \( L \)-functions ............................................. 25
  3.1 Artin representations and class numbers ............... 26
  3.2 The determinant and conductor .......................... 27
  3.3 Weight one newforms .................................... 30
  3.4 Examples ................................................ 32
4 Heegner points on elliptic curves of conductor $4D$

4.1 Root numbers ........................................... 41
4.2 Explicit Jacquet–Langlands correspondence .................................. 43
4.3 Shimura curves and Heegner points ........................................ 46

5 Reduction of Shimura curves at $p$ when $p^2 || N$

5.1 Motivation ............................................ 52
5.2 Néron models of Jacobians ...................................... 55
5.3 The Cerednik–Drinfeld Theorem .................................. 57
5.4 Néron models for Shimura curves with maximal level at $p$ ............ 59
5.5 The first Drinfeld cover .................................... 59
5.6 Néron models for Shimura curves with non-maximal level at $p$ ....... 61
5.7 Component groups ....................................... 66

6 Level raising mod 2 and obstruction for rank lowering

6.1 Level raising mod 2 .................................... 70
6.2 Selmer groups and sign changing ..................................... 72
6.3 Local conditions ....................................... 75
6.4 Parity of 2-Selmer ranks ..................................... 82
6.5 Obstruction for rank lowering ..................................... 88
Acknowledgements

I would like to express my deepest gratitude to my advisor Benedict Gross, whose knowledge, passion and enthusiasm have been a great inspiration for me during the entirety of graduate school. No words can describe how amazing this experience was. Besides his countless mathematical insights, one thing he taught me is how finding nontrivial examples can help in understanding theorems better – even one’s own theorems – which is hopefully reflected in the appearance of many examples in this thesis.

This thesis also owes debts to Wei Zhang, who was always kind enough to answer my questions and generous to share his ideas. In particular, I am grateful to him for sending me [Zha14] while it was still in preprint form: it inspired Chapter 6 of this thesis and the follow-up work [LL15].

Special thanks to Jeremy Teitelbaum for inviting me to UConn and answering my questions regarding [Tei90]; and to Mark Kisin and Barry Mazur for being part of my thesis defense committee and for helpful conversations and advice.

While working on the thesis, I benefited from conversations and correspondences with many people on material related to what is finally presented here: George Boxer, Kestutis Cesnavicius, Brian Conrad, Henri Darmon, Bas Edixhoven, Noam Elkies, Daniel Kriz, Bao Le Hung, Qing Liu, Yifeng Liu, Anand Patel, Keerthi Madapusi Pera, Bjorn Poonen, Kartik Prasanna, Joseph Rabinoff, Ken Ribet, Arul Shankar, Junecue Suh, Haoran Wang, Jared Weinstein, Jiangwei Xue and Show-Wu Zhang. I would like to thank them for their interest and help. The examples in this thesis are computed using Sage ([S+13]) and Magma ([BCP97]).

The Harvard Math Department has been a perfect place to study and work. I would like to thank the staff members, especially Susan Gilbert, for working so hard to make graduate students’ lives easier. I treasure the learning experience and friendship with many fellow students: Nasko, Omar, Jason, George, Gabriel, Kestutis, Carl, Jessica, Erick, Bao,
Eric, Ananth, Koji, Yunqing, Ryosuke, Cheng-Chiang, Pei-Yu, Matthew, Jerry, Jie, Rong, Yihang... Special thanks go to Chen-Yu Chi for teaching me a lot during my first year – I will not forget those nights accompanied by Chen-Yu’s pipa playing from his office.

My love goes to Charmaine, whom I was lucky to meet and who inevitably changed my life ever since. I am grateful to my parents for their unconditional support through the years. This thesis is dedicated to them.
To my parents

Fusen Li

and

Xiaoping Mao
Chapter 1

Introduction

1.1 The Birch and Swinnerton-Dyer conjecture

Given an elliptic curve $E$ defined over $\mathbb{Q}$, the rational points $E(\mathbb{Q})$ form a finitely generated abelian group by the Mordell–Weil theorem. It is a central question in number theory to understand the rank of $E(\mathbb{Q})$, known as the algebraic rank

$$r_{\text{alg}}(E/\mathbb{Q}) := \text{rk} E(\mathbb{Q}).$$

Another important invariant of $E$ is the analytic rank

$$r_{\text{an}}(E/\mathbb{Q}) := \text{ord}_{s=1} L(E/\mathbb{Q}, s),$$

defined as the order of vanishing of its $L$-function $L(E/\mathbb{Q}, s)$ (an analytic object) at the central point $s = 1$. The remarkable Birch and Swinnerton-Dyer conjecture asserts that the algebraic rank is equal to the analytic rank. It furthermore predicts a precise formula (the BSD formula) for the leading coefficient of the Taylor expansion of $L(E/\mathbb{Q}, s)$ at $s = 1$ in terms of various important arithmetic invariants of $E$. More precisely, we have
1.1. The Birch and Swinnerton-Dyer conjecture

**Conjecture 1.1** (Birch and Swinnerton-Dyer). Let $E/\mathbb{Q}$ be an elliptic curve. Then

(1) (Rank conjecture)

$$r_{\text{alg}}(E/\mathbb{Q}) = r_{\text{an}}(E/\mathbb{Q}).$$

(2) (BSD formula)

$$\frac{L^{(r)}(E/\mathbb{Q}, 1)}{r! \Omega(E/\mathbb{Q}) R(E/\mathbb{Q})} = \frac{\prod_p c_p(E/\mathbb{Q}) \cdot |\Sha(E/\mathbb{Q})|}{|E(\mathbb{Q})_{\text{tor}}|^2}. $$

Here $r = r_{\text{an}}(E/\mathbb{Q})$ is the analytic rank, $\Omega(E/\mathbb{Q})$ is the real period, $R(E/\mathbb{Q})$ is the regulator, $c_p(E/\mathbb{Q})$ is the local Tamagawa number (equal to one for almost all primes $p$), $\Sha(E/\mathbb{Q})$ is the Tate–Shafarevich group (finite under the Tate–Shafarevich conjecture), and $E(\mathbb{Q})_{\text{tor}}$ is the torsion subgroup of $E(\mathbb{Q})$. (See [Gro11] for the definitions.)

The best general result on the BSD conjecture so far is the following theorem.

**Theorem 1.2** (Gross–Zagier [GZ86], Kolyvagin [Kol90]). When $r_{\text{an}} \leq 1$, the rank conjecture holds.

Moreover, in this case both sides of the BSD formula are positive rational numbers. To prove that this is indeed an equality of two positive rational numbers, it suffices to prove this is an equality up to a $p$-adic unit, for each prime $p$. This is known as the $p$-part of the BSD formula, for which much progress has been made.

**Theorem 1.3** (Skinner–Urban [SU14], Kato [Kat04]). When $r_{\text{an}} = 0$ and certain technical assumptions are satisfied, the $p$-part of the BSD formula holds for $p \geq 3$.

**Theorem 1.4** (Wei Zhang [Zha14]). When $r_{\text{an}} = 1$ and certain technical assumptions are satisfied, the $p$-part of the BSD formula holds for $p \geq 5$.

On the other hand, very little is known for $p = 2$. Although the case $p = 2$ is often avoided in number theory due to technical complications, the $2$-part of the BSD formula is
in fact the most interesting case: for example, one observes from computational data (e.g., [Cre97, Table 4]) that the rational number appearing in the BSD formula usually consists of only small prime factors, and most frequently, the factor 2. We remark that this phenomenon is also expected from heuristics concerning the distribution of \(\Sha\) ([Del01, BKL+13]).

The theme of this thesis is to study various predictions of the BSD conjecture via the study of 2-Selmer groups and Heegner points.

Remark 1.5. We do not attempt to specify the technical assumptions in Theorem 1.3 and 1.4 here, but only mention that these assumptions in particular imply that \(E(\mathbb{Q})[p] = 0\) and some of its local Tamagawa numbers are coprime to \(p\). For simplicity, in this introduction we assume that \(E(\mathbb{Q})[p] = 0\) and all its local Tamagawa numbers are coprime to \(p\). Therefore the right hand side of the \(p\)-part of the BSD formula simplifies to \(|\Sha(E/\mathbb{Q})[p^\infty]|\), the order of the \(p\)-primary part of the Tate–Shafarevich group. We will impose these simplifying assumptions for \(p = 2\) as well, thus our main theorems are proved for elliptic curves with no rational 2-torsion and for which all local Tamagawa numbers are odd.

1.2 \(p\)-Selmer groups

Recall that the \(p\)-Selmer group \(\text{Sel}_p(E/\mathbb{Q})\) is a subspace of the Galois cohomology group \(H^1(\mathbb{Q}, E[p])\), cut out by local conditions coming from local points \(E(\mathbb{Q}_v)\) for each place \(v\) of \(\mathbb{Q}\). Namely, it sits in the pull-back diagram

\[
\begin{array}{c}
\text{Sel}_p(E/\mathbb{Q}) \rightarrow H^1(\mathbb{Q}, E[p]) \\
\prod_v E(\mathbb{Q}_v)/pE(\mathbb{Q}_v) \rightarrow \prod_v H^1(\mathbb{Q}_v, E[p]).
\end{array}
\]
1.2. $p$-Selmer groups

The Tate–Shafarevich group is defined to be

$$\sha(E/\mathbb{Q}) = \ker \left( H^1(\mathbb{Q}, E[p]) \to \prod_v H^1(\mathbb{Q}_v, E[p]) \right),$$

where $v$ runs over all places of $\mathbb{Q}$. We have the $p$-descent exact sequence

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \text{Sel}_p(E/\mathbb{Q}) \to \sha(E/\mathbb{Q})[p] \to 0.$$ 

The fundamental result that $\text{Sel}_p(E/\mathbb{Q})$ is finite is one of the key steps in the proof of the Mordell–Weil theorem.

Let $s_p(E/\mathbb{Q}) := \dim_{\mathbb{F}_p} \text{Sel}_p(E/\mathbb{Q})$ be the $p$-Selmer rank of $E/\mathbb{Q}$. Then

$$s_p(E/\mathbb{Q}) - r_{\text{alg}}(E/\mathbb{Q}) = \dim_{\mathbb{F}_p} \sha(E/\mathbb{Q})[p] \geq 0.$$ 

Due to the Cassels–Tate pairing, the finiteness of the $p$-primary part $\sha(E/\mathbb{Q})[p^\infty]$ would imply that $\sha(E/\mathbb{Q})[p]$ has even $\mathbb{F}_p$-dimension, hence $s_p(E/\mathbb{Q})$ and $r_{\text{alg}}(E/\mathbb{Q})$ have the same parity. In particular, the finiteness of $\sha(E/\mathbb{Q})[p^\infty]$ would imply the following conjecture, which we call the $p$-Selmer rank one conjecture.

**Conjecture 1.6 ($p$-Selmer rank one conjecture).** If $s_p(E/\mathbb{Q}) = 1$, then $r_{\text{alg}}(E/\mathbb{Q}) = 1$.

Progress towards this conjecture has only been made very recently.

**Theorem 1.7** (Zhang [Zha14], Skinner–Zhang [SZ14]). When $p \geq 5$ and certain technical assumptions are satisfied, Conjecture 1.6 holds.

Theorem 1.7 is a key ingredient in the following breakthrough:

**Theorem 1.8** (Bhargava–Skinner–Zhang [BSZ14]). The rank conjecture holds for at least 66% of all elliptic curves over $\mathbb{Q}$, when ordered by naive height.
1.3. Heegner points

Again, very little about Conjecture 1.6 is known for $p = 2$, though the 2-Selmer group is the easiest to compute in practice and provides as of now the best tool for computing $E(Q)$.

1.3 Heegner points

Though the statement in Conjecture 1.6 is purely algebraic, the proof of Theorem 1.7 indeed uses $L$-functions in an essential way, via their algebraic incarnation as Heegner points.

When $r_{an} = 1$, Theorem 1.2 not only shows that $r_{alg} = 1$ but actually constructs a point of infinite order on $E$. Suppose $E/Q$ has conductor $N$. We say an imaginary quadratic field $K$ satisfies the Heegner hypothesis if $p$ is split in $K$ for any $p|N$. When $K$ satisfies the Heegner hypothesis, the theory of complex multiplication ensures the existence of algebraic points $y_K \in E(K)$, known as Heegner points (see [Gro84]). The celebrated Gross–Zagier formula relates the Néron–Tate height of Heegner points to the first derivative of $L(E/K, s)$ at $s = 1$ and establishes the equivalence

$$y_K \text{ is of infinite order } \iff r_{an}(E/K) = 1.$$ 

Under the simplifying assumptions in Remark 1.5, it follows from the Gross–Zagier formula that the $p$-part of the BSD formula for $E/K$ is equivalent to saying that the equality

$$|\Pi(E/K)| = |E(K) : \mathbb{Z}y_K|^2$$

holds up to a $p$-adic unit (we assume the discriminant $d_K \neq -3, -4$ for simplicity). In the $p$-Selmer rank one case, $\Pi(E/K)[p]$ should be trivial and thus we can rephrase the $p$-part of the BSD formula in terms of the $p$-divisibility of Heegner points.

**Conjecture 1.9** ($p$-indivisibility conjecture). If $s_p(E/K) = 1$, then $y_K \not\in pE(K)$. 

Notice that if \( y_K \not\in pE(K) \), then by the assumption in Remark 1.5 that \( E \) has no rational \( p \)-torsion, we know that \( y_K \) is of infinite order. Hence we have the following implications

\[
y_K \not\in pE(K) \implies r_{an}(E/K) = 1 \implies r_{alg}(E/K) = 1.
\]

Thus

\[
p\text{-indivisibility conjecture} \implies \begin{cases} p\text{-Selmer rank one conjecture for } E/K, \\ p\text{-part of BSD for } E/K. \end{cases}
\]

Theorems 1.7 and 1.4 are indeed proved via proving the \( p \)-indivisibility Conjecture 1.9 for \( p \geq 5 \).

**Remark 1.10.** Once more, very little is known about Conjecture 1.9 for \( p = 2 \). Y. Tian [Tia14] proved it for many quadratic twists of the congruent number curve \( y^2 = x^3 - x \) using an induction argument. In a forthcoming joint work with D. Kriz, we prove Conjecture 1.9 for many quadratic twists of some general classes of elliptic curves, using a different strategy based on the \( p \)-adic Waldspurger formula of Bertolini–Darmon–Prasanna [BDP13] and Liu–Zhang–Zhang [LZZ14] for \( p = 2 \).

### 1.4 2-Selmer groups and 2-class groups

Now we turn to the main results of this thesis. Let \( E/\mathbb{Q} \) be an elliptic curve of conductor \( N \). Recall that the \( L \)-function \( L(E/\mathbb{Q}, s) \) satisfies a functional equation relating its values at \( s \) and \( 2 - s \). Let \( \Lambda(E/\mathbb{Q}, s) = (2\pi)^{-s}\Gamma(s)L(E/\mathbb{Q}, s) \) be the complete \( L \)-function. Then

\[
\Lambda(E/\mathbb{Q}, s) = \pm N^{1-s} \cdot \Lambda(E/\mathbb{Q}, 2-s),
\]

where the sign of the functional equation \( \pm \) is known as the **root number** of \( E/\mathbb{Q} \), denoted by \( \varepsilon(E/\mathbb{Q}) \in \{\pm 1\} \). The BSD conjecture implies that the root number determines the parity
1.4. 2-Selmer groups and 2-class groups

of the algebra rank: $E$ has even (resp. odd) algebraic rank if and only if $\varepsilon(E/Q) = +1$ (resp. $-1$).

Let $F(x) \in \mathbb{Z}[x]$ be an irreducible monic cubic polynomial with negative and square-free discriminant $-D$. Let $E$ be given by the Weierstrass equation $y^2 = F(x)$. In Chapter 2, we determine the 2-Selmer rank $s_2(E/Q)$ in terms of the 2-part of the ideal class group of the cubic field $L = \mathbb{Q}(x)/F(x)$ and the root number $\varepsilon(E/Q)$.

**Theorem 1.11** (Theorem 2.12). Let $\text{Cl}(L)$ be the ideal class group of the cubic field $L = \mathbb{Q}[x]/F(x)$. Let $k = \dim_{\mathbb{F}_2} \text{Cl}(L)[2]$. Then

$$s_2(E/Q) = k \text{ or } k + 1,$$

depending on whether the root number $\varepsilon(E/Q) = (-1)^k$ or $(-1)^{k+1}$. In particular, if the class number $h_L$ of $L$ is odd (i.e., $k = 0$), then

$$s_2(E/Q) = 0 \text{ or } 1,$$

depending on whether $\varepsilon(E/Q) = +1$ or $-1$.

As explained in Chapter 3, the mod 2 Galois representation $\bar{\rho} = \bar{\rho}_{E,2} : G_\mathbb{Q} \to \text{GL}_2(\mathbb{F}_2) \cong S_3$ can also be viewed as a 2-dimensional irreducible Artin representation $\sigma$ via an embedding $S_3 \hookrightarrow \text{GL}_2(\mathbb{C})$. This Artin representation $\sigma$ has dihedral image and thus is induced from the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. Then $\sigma$ is associated to a weight one newform with nebentypus the quadratic character $\varepsilon_K$, which is a Hecke theta series associated to $K$. On the other hand, there is a weight two newform $f$ with trivial nebentypus associated to the elliptic curve $E$ by the modularity theorem ([Wil95, TW95, BCDT01]). By construction we have a congruence $f \equiv h \pmod{2}$ (see Corollary 3.10). We provide several explicit examples in Section 3.4.

Under the BSD conjecture, Theorem 1.11 can be interpreted as a mod 2 congruence
between (suitably defined algebraic parts of) the special values of $L$-functions of these two modular forms (of different weights!):

- the $2$-part of $L(f, 1)$ or $L'(f, 1)$ (depending on the sign) is related to $s_2(E/Q)$ by BSD;
- the $2$-part of $L(h, 1)$ is related to the $2$-part of the ideal class group $Cl(L)$ by the class number formula (Corollary 3.5).

We depict this as follows.

$$
\begin{array}{ccc}
E & \sigma & . \\
\downarrow & \downarrow & \downarrow \\
f & \equiv & h \pmod{2} \\
& \downarrow & \\
L(f, 1) \text{ or } L'(f, 1) & \equiv & L(h, 1) \pmod{2}
\end{array}
$$

1.5 Heegner points and bad reduction of Shimura curves at $p$ when $p^2 \mid \mid N$

By Theorem 1.11, when the class number of $L$ is odd and $\varepsilon(E/Q) = -1$, the $p$-Selmer rank one Conjecture 1.6 predicts that $r_{alg}(E/Q) = 1$. In Chapter 4, we impose an additional assumption on the reduction type at $2$ of the elliptic curve considered in Theorem 1.11. Then $E$ has conductor $N = 4D$ and admits a parametrization by a Shimura curve $X$ associated to the quaternion order of reduced discriminant $4D$,

$$Z + Zi + Zj + Zij, \quad i^2 = -1, j^2 = D, ij = -ji.$$ 

Using Heegner points $y_K$ on $X$ associated to $K = \mathbb{Q}(i)$ and an explicit description of the Jacquet–Langlands correspondence, we construct a canonical point $P \in E(\mathbb{Q}(i))$, which lies in $E(\mathbb{Q})$ when $\varepsilon(E/Q) = -1$ (Theorem 4.15).
1.5. Heegner points and bad reduction of Shimura curves at $p$ when $p^2 || N$

**Remark 1.12.** One naturally expects that $P$ is of infinite order. To study the 2-divisibility of $P \in E(\mathbb{Q}(i))$, one can first study the 2-divisibility of a Heegner divisor $d \in J_X(\mathbb{Q}(i))$ constructed from $y_K$, where $J_X$ is the Jacobian of $X$, and then study its image under the projections $J_X \to E$. The first step is more accessible since it only involves the arithmetic of the Shimura curve $X$ itself. The second step is more difficult as we know very little about the maps $J_X \to E$, which should encode the information about the class number of cubic fields in a mysterious way. We hope to return to the second step in the future.

More generally, for any prime $p$, to study the $p$-divisibility of Heegner points on certain elliptic curves of conductor $N$ (when $p^2 || N$), we are led to study the mod $p$ reduction of a Shimura curve $X$ of the following type in Chapter 5. Let $B$ be an indefinite rational quaternion algebra ramified at $p$. Let $\mathcal{O}_p$ be the maximal order in $B_p$ with uniformizer $\pi$. Then the level of $X$ at $p$ is given by the compact open subgroup $R_p^\times \subseteq B_p^\times$, where $R_p \subseteq \mathcal{O}_p$ is the unique suborder of index $p$, that is,

$$R_p = \{ x \in \mathcal{O}_p : x \mod \pi \mathcal{O}_p \in \mathbb{F}_p \subseteq \mathbb{F}_p^2 = \mathcal{O}_p/\pi \mathcal{O}_p \}.$$

These curves have a $p$-adic uniformization by a *tame* étale covering $\Omega_1$ of Drinfeld’s $p$-adic half-plane $\Omega$. We use the covering to describe the geometry of $X \mod p$ and compute the Néron model $\mathcal{J}_X$ of $J_X$ over $\mathbb{Z}_p$. Let $Y$ be the Shimura curve with the same tame level (i.e., the level away from $p$) as $X$ but with the level at $p$ replaced by $\mathcal{O}_p^\times$. Then $X \to Y$ is a finite cover of degree $p + 1$.

**Theorem 1.13** (Theorem 5.16). Let $\mathcal{J}_X$ (resp. $\mathcal{J}_Y$) be the Néron model of $J_X$ (resp. $J_Y$) over $\mathbb{Z}_p$. Suppose the tame level is small enough. Then the identity component of the special fiber of the Néron models are given by

$$\mathcal{J}_{Y,F_p}^0 \cong T, \quad \mathcal{J}_{X,F_p}^0 \cong U \times T$$

9
respectively. Here $T$ is a torus of dimension equal to the genus $g(Y)$ of $Y$ and $U$ is a vector group (i.e., a product of $\mathbb{G}_a$’s) of dimension $g(X) - g(Y)$.

Remark 1.14. We will further determine their component groups in Theorem 5.16 (3).

Remark 1.15. For the Shimura curve $Y$ with maximal level at $p$, its Néron model $\mathcal{J}_Y$ has been computed by Jordan–Livné [JL86]. Our contribution is the determination of $\mathcal{J}_X$ for the Shimura curve $X$ with deeper, but still in some sense, “tame” level at $p$. The two key ingredients are Teitelbaum’s theorem [Tei90] on the rigid geometry of $\Omega_1$ and Edixhoven’s theorem [Edi92] on the behavior of Néron models under tamely ramified extensions.

1.6 Level raising and rank lowering

In the last Chapter 6, we follow the ingenious strategy of W. Zhang for proving the $p$-indisivibility Conjecture 1.9 when $p \geq 5$ and investigate the relevant problems for $p = 2$.

Suppose we are in the situation of Conjecture 1.9. This strategy reduces the problem in rank one to rank zero via level raising, roughly consists of three steps:

A: Let $f \in S_2(N)$ be the newform associated to $E/\mathbb{Q}$. Find a congruence $f \equiv g \pmod{p}$ between $f$ and another newform $g \in S_2(Nq)$ with level raised at some prime $q$.

B: Let $A = A_g$ be the elliptic curve associated to $g$ (when $g$ does not have rational Fourier coefficients, one works with the corresponding modular abelian variety instead). Prove that one can always find $g$ in Step A such that $q$ is inert in $K$ and $s_p(A/K) = 0$.

C: Show that

$$y_K \notin pE(K_q) \iff s_p(A/K) = 0.$$ 

Step A is ensured by the level raising theorem of Ribet ([Rib90]) for any $p$.

Step B is achieved by a parity argument for $p \geq 5$, which already appeared in Gross–Parson [GP12], and by a Chebotarev density argument.
Step C can be thought of as a congruence between (suitably defined algebraic parts of) $L'(E/K)$ and $L(A/K)$:

- the $p$-part of $L'(E/K)$ is related to the $p$-divisibility of Heegner points $y_K$ by the Gross-Zagier formula;

- the $p$-part of $L(A/K)$ is related to $s_p(A/K)$ by BSD.

Its proof combines the Jochnowitz congruence established by Bertolini–Darmon [BD99] for $p \geq 5$, Gross’ explicit Waldspurger formula [Gro87], and the $p$-part of BSD formula in the case $r_{\text{an}} = 0$ due to Skinner–Urban for $p \geq 3$.

We can depict the three steps as follows.

$$
\begin{align*}
E & \downarrow \downarrow A \\
\quad & \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad 1.7 Obstruction for rank lowering  

Now we specialize the previous section to the case $p = 2$. Let $\tilde{\rho} = \tilde{\rho}_E : G_Q \to \text{Aut}(E[2]) \cong \text{GL}_2(\mathbb{F}_2)$ be the Galois representation on the 2-torsion points. The level raising theorem (Step A) in this case asserts that $q \nmid 2N$ is a level raising prime if and only if $\tilde{\rho} (\text{Frob}_q) = (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})$ or $(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})$. Under Assumption 6.1 and 6.13, we prove a parity conjecture on 2-Selmer ranks predicted by BSD (Conjecture 6.15), which allows one to raise or lower the 2-Selmer rank in a controlled way.
Theorem 1.16 (Theorem 6.27). Suppose $\bar{\rho}(\text{Frob}_q) = (\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})$. Then

$$s_2(E/K) = s_2(A/K) \pm 1.$$ 

It follows that if $s_2(E/K) = 1$, then $s_2(A/K) = 0$ or $2$. However, the Chebotarev density argument (in Step B) fails and does not show that one can always get $s_2(A/K) = 0$. In fact, we prove the following surprising obstruction for rank lowering: when $\bar{\rho}(\text{Frob}_q) = (\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})$, $s_2(A/K)$ can never be lowered to zero!

Theorem 1.17 (Theorem 6.29). Suppose $\bar{\rho}(\text{Frob}_q) = (\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})$. Then

$$s_2(E/K) = 1 \implies s_2(A/K) = 2.$$ 

Remark 1.18. Theorem 1.17 tells us that Step B of the strategy cannot naively work for $p = 2$. In joint work with B. Le Hung [LL15], we enhance Ribet’s level raising theorem to raise the level at multiple primes simultaneously, using the method of [DT94] and [All14]. With a refined control over the signs (which are not detected under the mod 2 congruence), we show that it is possible to obtain arbitrary $s_2(A/\mathbb{Q})$ via level raising mod 2. In particular, there is no obstruction for rank lowering over $\mathbb{Q}$ in contrast to the situation over $K$. The spirit of this result is similar to the work of Mazur–Rubin [MR10] on arbitrary 2-Selmer ranks in quadratic twist families. This obstruction for rank lowering is a phenomenon unique to $p = 2$, since the odd part of III never jumps under a quadratic base change! (see Example 6.30.)
Chapter 2

2-Selmer groups and 2-class groups

Let $E/\mathbb{Q}$ be an elliptic curve. We will impose the following assumptions throughout this chapter.

**Assumption 2.1.** Suppose $E$ has equation $y^2 = F(x)$, where $F(x) = x^3 + a_2x^2 + a_4x + a_6$ is an integral polynomial which

(1) is irreducible, and

(2) has negative and square-free discriminant $-D$.

Let $L = \mathbb{Q}[x]/F(x)$. Then $L$ has the following elementary properties:

(1) Since $F(x)$ is irreducible and has negative discriminant, we know that $F(x)$ has Galois group $S_3$. The field $L = \mathbb{Q}[x]/F(x)$ is a complex cubic field, i.e., $L_\infty := L \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R} \times \mathbb{C}$.

(2) Since $\text{disc } F(x) = -D$ is square-free, we know that $D \equiv 3 \pmod{4}$, $L$ has discriminant $d_L = \text{disc } F(x) = -D$, and $L$ has ring of integers $A = \mathbb{Z}[x]/F(x)$.

(3) Since $L$ has a unique real embedding, we know that the unit group $A^\times$ has rank one by Dirichlet’s unit theorem. Let $u_L$ be a fundamental unit. Then $A^\times = u_L^\mathbb{Z} \times \{\pm 1\}$. After possibly replacing $u_L$ by $-u_L$, we may assume $u_L > 0$. After possibly replacing $u_L$ by $u_L^{-1}$, we may further assume $u_L > 1$. 

13
The elliptic curve $E : y^2 = F(x)$ has the following elementary properties:

(1) Since $F(x)$ is irreducible, we have $E(\mathbb{Q})[2] = 0$.

(2) The 2-torsion field $\mathbb{Q}(E[2])$, as the Galois closure of $L$, is an $S_3$-extension over $\mathbb{Q}$.

(3) $E$ has discriminant $\Delta = -2^4 D$. Since no 12th power divides $\Delta$, the equation $y^2 = F(x)$ is minimal. It follows that $E$ has bad reduction precisely at $p \mid 2D$.

(4) For $p \mid D$, since $D$ is square-free, by comparing the power of $p$ appearing on both sides of

$$c_4^3 - c_6^2 = -2^{10} \cdot 3^3 \cdot D,$$

we see that $p \nmid c_4$. Hence $E$ has multiplicative reduction of type $I_1$ at $p \mid D$. In particular, the component group of the Néron model of $E/\mathbb{Q}_p$ is trivial.

(5) We compute that $c_4 = 16(a_2^2 - 3a_4)$, so $2 \mid c_4$ and $E$ has additive reduction at 2.

(6) Therefore the conductor of $E$ is of the form $N = 2^{2+\delta} D$ for some $\delta \geq 0$. The order of $N$ at 2 is determined by the Ogg–Saito formula ([Sil94, 11.1])

$$\text{ord}_2(N) = \text{ord}_2(\Delta) + 1 - m = 5 - m,$$  \hspace{1cm} (2.1)

where $m$ is the size of the component group of the Néron model of $E/\mathbb{Q}_2$.

Our main goal in this chapter is to relate the 2-Selmer group of $E/\mathbb{Q}$ and the 2-part of the ideal class group of the cubic field $L$, under Assumption 2.1.
2.1 2-Selmer groups

Recall that for an elliptic curve $E/\mathbb{Q}$, we have the global and local Kummer exact sequences, fitting into the following commutative diagram:

\[
\begin{array}{ccccccccc}
0 & \rightarrow & E(\mathbb{Q})/2E(\mathbb{Q}) & \delta & \rightarrow & H^1(\mathbb{Q}, E[2]) & \rightarrow & H^1(\mathbb{Q}, E)[2] & \rightarrow & 0 \\
& & \downarrow & & \downarrow \Pi_v \text{res}_v & & \downarrow & & \downarrow & \\
0 & \rightarrow & \prod_v E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) & \rightarrow & \prod_v H^1(\mathbb{Q}_v, E[2]) & \rightarrow & \prod_v H^1(\mathbb{Q}_v, E)[2] & \rightarrow & 0.
\end{array}
\]

Here the vertical maps are given by the product of restriction maps over all places $v$ of $\mathbb{Q}$.

**Definition 2.2.** The 2-Selmer group

\[\text{Sel}_2(E/\mathbb{Q}) \subseteq H^1(\mathbb{Q}, E[2])\]

consists of cohomology classes whose restriction at $v$ lies in the image of the local Kummer map $\delta_v$ for every $v$:

\[\text{Sel}_2(E/\mathbb{Q}) = \{c \in H^1(\mathbb{Q}, E[2]) : \text{res}_v(c) \in \text{im}(\delta_v)\}.\]

Colloquially, the 2-Selmer group is cut out by the **local conditions**

\[\text{im}(\delta_v) \subseteq H^1(\mathbb{Q}_v, E[2])\]

coming from local points for all $v$. By definition, we have an injection

\[E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \text{Sel}_2(E/\mathbb{Q}).\]

The 2-Selmer group, due to its local nature, is easier to understand and the 2-Selmer rank
2.2. Kummer maps

$s_2(E/Q) := \text{dim}_F \text{Sel}_2(E/Q)$ provides an upper bound for the rank of $E(Q)$.

2.2 Kummer maps

Our first goal is to give an explicit description of the global and local Kummer maps in terms of the cubic field $L$.

**Lemma 2.3.** We have an exact sequence of finite group schemes over $\mathbb{Q}$,

$$1 \rightarrow E[2] \rightarrow \text{Res}_{L/\mathbb{Q}} \mu_2 \xrightarrow{N} \mu_2 \rightarrow 1,$$

where $N$ is induced by the norm map from $L$ to $\mathbb{Q}$. We have an isomorphism

$$H^1(\mathbb{Q}, E[2]) \cong (L^\times/(L^\times)^2)_{N=\square}. \quad (2.2)$$

Here $(L^\times/(L^\times)^2)_{N=\square}$ consists of all classes in $L^\times/(L^\times)^2$ with square norms to $\mathbb{Q}^\times$.

**Proof.** It suffices to check that we have an exact sequence of $G_{\mathbb{Q}}$-modules on the level of $\overline{\mathbb{Q}}$-points. Suppose $F(x)$ has the three roots $x_1, x_2, x_3 \in \overline{\mathbb{Q}}$. Then the $\overline{\mathbb{Q}}$-points of $E[2]$ consist of $P_i = (x_i, 0), (i = 1, 2, 3)$ and $\infty$. The Galois group $G_{\mathbb{Q}}$ acts trivially on $\infty$ and permutes the three points $P_i$ via its $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$-action on $x_i$. Also, the group of $\overline{\mathbb{Q}}$-points of $\text{Res}_{L/\mathbb{Q}} \mu_2$ is isomorphic to $\mu_2 \times \mu_2 \times \mu_2$, where the three factors are indexed by the three roots $x_i$ and the Galois action permutes the three factors in the same way. The norm map simply multiplies the three factors and respects the $G_{\mathbb{Q}}$-action. One sees that the map

$$\infty \mapsto (1,1,1), \quad P_1 \mapsto (1,-1,-1), \quad P_2 \mapsto (-1,1,-1), \quad P_3 \mapsto (-1,-1,1)$$

gives an injective homomorphism of $G_{\mathbb{Q}}$-modules $E[2] \rightarrow \text{Res}_{L/\mathbb{Q}} \mu_2$. Moreover, its image is exactly the kernel of the norm map. This finishes the proof of the first part.
2.2. Kummer maps

Taking the long exact sequence in Galois cohomology, we obtain

\[ H^0(\mathbb{Q}, \text{Res}_{L/\mathbb{Q}} \mu_2) \xrightarrow{\text{N}} H^0(\mathbb{Q}, \mu_2) \to H^1(\mathbb{Q}, E[2]) \to H^1(\mathbb{Q}, \text{Res}_{L/\mathbb{Q}} \mu_2) \xrightarrow{\text{N}} H^1(\mathbb{Q}, \mu_2). \]

Since \( H^0(\mathbb{Q}, \text{Res}_{L/\mathbb{Q}} \mu_2) = \mu_2(L) = \{\pm 1\}, \ H^0(\mathbb{Q}, \mu_2) = \mu_2(\mathbb{Q}) = \{\pm 1\} \) and \( L/\mathbb{Q} \) has odd degree, we know that the first map is surjective. By Kummer theory, we know that

\[ H^1(\mathbb{Q}, \text{Res}_{L/\mathbb{Q}} \mu_2) \cong L^\times/(L^\times)^2, \quad H^1(\mathbb{Q}, \mu_2) \cong \mathbb{Q}^\times/(\mathbb{Q}^\times)^2. \]

Therefore

\[ H^1(\mathbb{Q}, E[2]) = \ker(N : L^\times/(L^\times)^2 \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2) = (L^\times/(L^\times)^2)_{N=0}. \]

This finishes the proof of the second part. \( \Box \)

**Proposition 2.4.** Under the isomorphism (2.2), the global Kummer map \( \delta \) can be described as

\[ \delta : E(\mathbb{Q})/2E(\mathbb{Q}) \to (L^\times/(L^\times)^2)_{N=0}, \quad P \mapsto x(P) - \beta, \]

where \( x(P) \) is the \( x \)-coordinate of \( P \) and \( \beta \) is the image of \( x \) in \( L = \mathbb{Q}[x]/F(x) \).

**Proof.** Let \( e_2 : E[2] \times E[2] \to \mu_2 \) be the Weil pairing. Then we see that the homomorphism \( E[2] \to \text{Res}_{L/\mathbb{Q}} \mu_2 \) in Lemma 2.3 is also given by

\[ P \mapsto (e_2(P, P_1), e_2(P, P_2), e_2(P, P_3)). \]

The rational function \( f_i = x - x_i \) has the divisor \( (f_i) = 2P_i - 2\infty \) (\( i = 1, 2, 3 \)) and there exists some rational function \( g_i \) (over \( \overline{\mathbb{Q}} \)) such that \( f_i \circ [2] = g_i^2 \) (see [Sil09, III.8]). The Weil pairing \( e_2 \) is then given by

\[ e_2(P, P_i) = \frac{g_i(X + P)}{g_i(X)}, \]

17
2.2. Kummer maps

where \(X \in E(\overline{\mathbb{Q}})\) is any point such that \(g(X + P)\) and \(g(X)\) are both defined and nonzero. For \(P \in E(\mathbb{Q})\), we choose \(Q \in E(\overline{\mathbb{Q}})\) such that \([2]Q = P\). Then \(\delta(P)\) corresponds to the cocycle \(\{\sigma \mapsto Q^\sigma - Q\} \in H^1(\mathbb{Q}, E[2])\). Taking \(P = Q^\sigma - Q\) and \(X = Q\), we know that

\[
e_2(Q^\sigma - Q, P_i) = \frac{g_i(Q)^\sigma}{g_i(Q)}, \tag{2.3}
\]

By the identification \(H^1(\mathbb{Q}, \text{Res}_{L/\mathbb{Q}} \mu_2) \cong (L^\times/(L^\times)^2)_{N=\Box}\) coming from Kummer theory, Equation (2.3) implies that

\[
\delta(P) \equiv g_i(Q)^2 \mod (L^\times)^2
\]

under the embedding \(L \hookrightarrow \mathbb{Q}\) associated to \(x_i\). But by the construction of \(g_i\), we have \(g_i(Q)^2 = f_i(P) = x(P) - x_i\). Hence

\[
\delta(P) \equiv x(P) - x_i \mod (L^\times)^2
\]

under the embedding \(L \hookrightarrow \mathbb{Q}\) associated to \(x_i\), which finishes the proof. \(\square\)

Base changing to \(\mathbb{Q}_v\) in Lemma 2.3 and Proposition 2.4, we obtain the analogous explicit description of the local Kummer maps \(\delta_v\).

**Proposition 2.5.** The local Kummer maps for \(E\) are given by

\[
\delta_v : E(\mathbb{Q}_v)[2] \to H^1(\mathbb{Q}_v, E[2]) \cong (L_v^\times/(L_v^\times)^2)_{N=\Box}, \quad P \mapsto x(P) - \beta,
\]

where \(\beta\) is the image of \(x\) in \(L_v = \mathbb{Q}_v[x]/F(x)\).

**Remark 2.6.** Even though \(E(\mathbb{Q})[2] = 0\), it is possible that \(E(\mathbb{Q}_v)[2] \neq 0\). For a nonzero point \(P \in E(\mathbb{Q}_v)[2]\), the expression \(x(P) - \beta\) does not lie in \(L_v^\times\) and it should be interpreted using the group structure: write \(P = P_1 - P_2\) as the difference of two points \(P_1, P_2 \in E(\mathbb{Q}_v)\).
2.3. Local conditions

which are not 2-torsion, then \( \delta_v(P) = (x(P_1) - \beta)/(x(P_2) - \beta) \).

2.3 Local conditions

Our next goal is to describe explicitly the local condition \( \text{im}(\delta_v) \) for each place \( v \).

Lemma 2.7. Let \( p \) be a prime. Then the valuation of \( \delta_p(P) \) is even for any \( P \in E(\mathbb{Q}_p) \), namely,

\[
\delta_p(P) \in (A_p^\times/(A_p^\times)^2)_{N=\Box},
\]

where \( A = \mathbb{Z}[x]/F(x) \) is the ring of integers of \( L \) and \( A_p = A \otimes \mathbb{Z}_p \).

Proof. Let \( P \in E(\mathbb{Q}_p) \) and write \( x = x(P) \) for short.

First consider the case \( p \nmid D \). So \( p \) is unramified in \( L \). There are three cases:

1. \( L_p \cong \mathbb{Q}_p^3 \) is the unramified cubic extension of \( \mathbb{Q}_p \). From \( y^2 = F(x) \), we know that 2 ord\(_p\)(y) = 3 ord\(_p\)(x - \beta), hence ord\(_p\)(x - \beta) is even.

2. \( L_p \cong \mathbb{Q}_p^3 \times \mathbb{Q}_p \), where \( \mathbb{Q}_p^3 \) is the unramified quadratic extension of \( \mathbb{Q}_p \). Write \( \beta = (\gamma, c) \), then \( \gamma \not\equiv c \mod p \), ord\(_p\)(\( \gamma \)) = 0 and ord\(_p\)(c) \( \geq 0 \). From \( y^2 = F(x) \), we know that 2 ord\(_p\)(y) = ord\(_p\)(x - \gamma) + ord\(_p\)(x - c). There are two cases:

   • If ord\(_p\)(x) < 0, then ord\(_p\)(x - \gamma) = ord\(_p\)(x - c) = ord\(_p\)(x). Therefore 2 ord\(_p\)(y) = 3 ord\(_p\)(x), hence ord\(_p\)(x - \gamma) = ord\(_p\)(x - c) = ord\(_p\)(x) are all even.

   • If ord\(_p\)(x) \( \geq 0 \), then ord\(_p\)(x - \gamma) = 0. So ord\(_p\)(x - c) = 2 ord\(_p\)(y) is even.

3. \( L_p \cong \mathbb{Q}_p \times \mathbb{Q}_p \times \mathbb{Q}_p \). Write \( \beta = (c_1, c_2, c_3) \). Then \( c_i \not\equiv c_j \mod p \) whenever \( i \neq j \).

   Similarly, there are two cases:

   • If ord\(_p\)(x) < 0, then ord\(_p\)(x - c_i) = ord\(_p\)(x). Therefore 2 ord\(_p\)(y) = 3 ord\(_p\)(x), hence ord\(_p\)(x - c_i) = ord\(_p\)(x) are all even.
2.3. Local conditions

- If $\text{ord}_p(x) \geq 0$, then $\text{ord}_p(x - c_i) \geq 0$. Since $c_i \not\equiv c_j \pmod{p}$, at least two of the $\text{ord}_p(x - c_i)$’s are zeros. Thus $2 \text{ord}_p(y) = \text{ord}_p(x - c_1) + \text{ord}_p(x - c_2) + \text{ord}_p(x - c_3)$ implies the third one must have even valuation as well.

Now consider the case $p \mid D$. So $p$ is ramified in $L$. Since $D$ is square-free, we know that $L_p \cong K_p \times \mathbb{Q}_p$, where $K_p$ is a ramified quadratic extension of $\mathbb{Q}_p$. Denote by $\mathfrak{p}$ the prime for $K_p$ and write $\beta = (\gamma, c)$. Then $\gamma \not\equiv c \pmod{p}$, $\text{ord}_p(\gamma) > 0$ and $\text{ord}_p(c) \geq 0$. From $y^2 = F(x)$, we know that $2 \text{ord}_p(y) = \text{ord}_p(x - \gamma) + \text{ord}_p(x - c)$. We argue similarly:

- If $\text{ord}_p(x) < 0$, then $\text{ord}_p(x - \gamma) = 2 \text{ord}_p(x)$ and $\text{ord}_p(x - c) = \text{ord}_p(x)$. Hence $\text{ord}_p(x)$ is even, therefore both $\text{ord}_p(x - \gamma)$ and $\text{ord}_p(x - c)$ are even.

- If $\text{ord}_p(x) \geq 0$, then $\text{ord}_p(x - \gamma) \geq 0$ and $\text{ord}_p(x - c) \geq 0$. Since $\gamma \not\equiv c \pmod{p}$, at least one of $\text{ord}_p(x - \gamma)$ and $\text{ord}_p(x - c)$ is zero. Hence both of them are even. \(\square\)

**Remark 2.8.** When $p \neq 2$, Lemma 2.7 can be proved by a more “pure thought” argument: since the component group of Néron model of $E/\mathbb{Q}_p$ is trivial, the local condition at $p$ corresponds to the unramified cohomology $H^1_{ur}(\mathbb{Q}_p, E[2])$ ([GP12, Lemma 6]), which consists of the units $(A_p^\times / (A_p^\times)^2)_{N=\square}$ under the isomorphism (2.2). Here we preferred the above direct computational proof using the explicit description of $\delta_p$ in Proposition 2.5, which depends on less machinery and also treats the case $p = 2$.

**Proposition 2.9.** We have

1. For $v = \infty$, both $E(\mathbb{R})/2E(\mathbb{R})$ and $(L_\infty^\times / (L_\infty^\times)^2)_{N=\square}$ are trivial. In particular, the local condition $\text{im}(\delta_\infty)$ is trivial.

2. For $v = p > 2$, the local condition $\text{im}(\delta_p) = (A_p^\times / (A_p^\times)^2)_{N=\square}$.

3. For $v = p = 2$, the local condition $\text{im}(\delta_2)$ has index 2 in $(A_2^\times / (A_2^\times)^2)_{N=\square}$ and contains all units $\equiv 1 \pmod{4}$. 

20
Proof. For \( v = \infty \), since \( L_\infty \cong \mathbb{R} \times \mathbb{C} \), we know that

\[
(L_\infty^\times/(L_\infty^\times)^2)_{N=\Box} = (\mathbb{R}^\times/(\mathbb{R}^\times)^2)_{N=\Box} = \{1\}.
\]

For \( v = p \), we know from Lemma 2.7 that \( \text{im}(\delta_p) \subseteq (A_p^\times/(A_p^\times)^2)_{N=\Box} \). Since the norm map is surjective on the units, we know that

\[
\#(A_p^\times/(A_p^\times)^2)_{N=\Box} = \#Z_p^\times/(Z_p^\times)^2.
\]

Notice that \( \#Z_p^\times/(Z_p^\times)^2 \) is \( 2^2 \) or \( 2 \) depending on whether \( p = 2 \) or not. If \( L_p \) is a product of \( k \) fields (\( k = 1, 2, 3 \)), then \( \#A_p^\times/(A_p^\times)^2 \) is \( 2^{k+3} \) or \( 2^k \) depending on whether \( p = 2 \) or not. It follows that

\[
\#(A_p^\times/(A_p^\times)^2)_{N=\Box} = \begin{cases} 
2^{k-1}, & p \neq 2, \\
2^{k+1}, & p = 2.
\end{cases}
\]

Since \( E(\mathbb{Q}_p) \) has a finite index subgroup isomorphic to \( \mathbb{Z}_p \), we know that

\[
\#E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) = \begin{cases} 
#E(\mathbb{Q}_p)[2], & p \neq 2, \\
2 \cdot #E(\mathbb{Q}_p)[2], & p = 2.
\end{cases}
\]

All claims except the last one then follow because \( #E(\mathbb{Q}_p)[2] \) is the same as \( 1 \) plus the number of \( \mathbb{Q}_p \)-rational solutions of \( F(x) = 0 \), which is \( 2^{k-1} \) in all cases. To see the last claim that \( \text{im}(\delta_2) \) contains all the units \( \equiv 1 \) (mod 4), let us consider a point \( P \in \hat{E}(2\mathbb{Z}_2) \), where \( \hat{E} \) is the formal group of \( E \) over \( \mathbb{Q}_2 \) given by the minimal equation. For a general elliptic curve \( E \) with minimal equation

\[
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,
\]

All claims except the last one then follow because \( #E(\mathbb{Q}_p)[2] \) is the same as \( 1 \) plus the number of \( \mathbb{Q}_p \)-rational solutions of \( F(x) = 0 \), which is \( 2^{k-1} \) in all cases. To see the last claim that \( \text{im}(\delta_2) \) contains all the units \( \equiv 1 \) (mod 4), let us consider a point \( P \in \hat{E}(2\mathbb{Z}_2) \), where \( \hat{E} \) is the formal group of \( E \) over \( \mathbb{Q}_2 \) given by the minimal equation. For a general elliptic curve \( E \) with minimal equation

\[
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,
\]

21
the general formula ([Sil94, IV.1]) reads

\[ x(P) = z^{-2} - a_1 z^{-1} - a_2 - a_3 z + O(z^2), \]

where \( z = -x/y \) is the parameter for the formal group. In our case \( a_1 = 0 \), therefore

\[ \delta_2(P) = x(P) - \beta = z^{-2} - a_2 - \beta + O(z) \equiv 1 - (a_2 + \beta)z^2 + O(z^3) \equiv 1 - (a_2 + \beta)z^2 \pmod{(L_2^\times)^2}, \tag{2.4} \]

where the last equality is because \( z \in 2\mathbb{Z}_2 \) and the units \( \equiv 1 \pmod{8} \) are squares. Since \( F(x) \mod 2 \) cannot be a product of three distinct linear factors in \( \mathbb{F}_2[x] \), we know that 2 does not split in \( L \). Now one can then check directly that im(\( \delta_2 \)) contains the units \( \equiv 1 \pmod{4} \) with square norm in the remaining two cases:

- If \( L_2 = \mathbb{Q}_8 \), then all units \( \equiv 1 \pmod{4} \) with square norms are actually squares. So the claim that im(\( \sigma_2 \)) contains all such units is trivial.

- If \( L_2 = \mathbb{Q}_4 \times \mathbb{Q}_2 \), then any class \((\alpha, a) \equiv 1 \pmod{4} \) with square norm is represented by \((\alpha, \sqrt[4]{\alpha})\) with \( \alpha \equiv 1 \pmod{4} \). There is a unique nontrivial class of units \( \alpha \equiv 1 \pmod{4} \) modulo squares, represented by \( 1 + 4\gamma \) if we write \( \beta = (\gamma, c) \). It follows from (2.4) that im(\( \delta_2 \)) contains this class. \( \square \)

### 2.4 2-class groups of cubic fields

Combining all the local conditions gives us both upper and lower bounds for the 2-Selmer group.

**Lemma 2.10.** Let

\[ M_1 = \{ \alpha \in L^\times/(L^\times)^2 : L(\sqrt[4]{\alpha})/L \text{ is unramified} \}, \]

22
2.4. 2-class groups of cubic fields

and

\[ M_2 = \{ \alpha \in L^\times / (L^\times)^2 : \alpha > 0, (\alpha) = I^2, I \subseteq L \text{ a fractional ideal} \} \]

be subgroups of \((L^\times / (L^\times)^2)_{\mathbb{N} = \mathbb{Q}}\). Then under the isomorphism (2.2), we have

\[ M_1 \subseteq \text{Sel}_2(E/\mathbb{Q}) \subseteq M_2. \]

Proof. Elements of \(M_2\) clearly have square norms since \(N\alpha = N(I)^2\). If \(\alpha \in \text{Sel}_2(E/\mathbb{Q})\), then by Proposition 2.9, \(\alpha > 0\) and \(\alpha\) has even valuation at all finite places. The latter implies that there exists a fractional ideal \(I\) such that \((\alpha) = I^2\). Thus \(\alpha \in M_2\).

Let \(\alpha \in L^\times / (L^\times)^2\). For \(p\) odd, \(L_p(\sqrt{\alpha})/L_p\) is unramified if and only if \(\alpha\) has even valuation. For \(p = 2\), \(L_2(\sqrt{\alpha})/L_2\) is unramified if and only if \(\alpha\) has even valuation and is represented by a unit \(\equiv 1 \pmod{4}\). From this description we see that \(M_1 \subseteq M_2\) and elements \(M_1\) have square norm. It also follows from this description and Proposition 2.9 that \(M_1 \subseteq \text{Sel}_2(E/\mathbb{Q})\). \(\square\)

Class field theory supplies information about the two groups \(M_1\) and \(M_2\).

Lemma 2.11. Let \(\text{Cl}(L)\) be the ideal class group of the cubic field \(L = \mathbb{Q}[x]/F(x)\). Let \(k = \dim_{\mathbb{F}_2} \text{Cl}(L)[2]\). Then \(M_1\) (resp. \(M_2\)) is an elementary 2-group of size \(2^k\) (resp. \(2^{k+1}\)).

Proof. Kummer theory tells us that

\[ M_1 \cong \text{Hom}(\text{Gal}(M/L), \mu_2), \]

where \(M\) is obtained by adjoining the square roots of all \(\alpha \in M_1\) to \(L\), which is the maximal unramified extension of \(L\) of exponent 2. By class field theory, we have

\[ \text{Gal}(M/L) \cong \text{Cl}(L)[2]. \]

Since \(#(\text{Cl}(L)/2\text{Cl}(L)) = #\text{Cl}(L)[2]\), \(M_1\) is an elementary 2-group of size \(2^k\).
Suppose $\alpha \in M_2$ such that $(\alpha) = I^2$. Then the assignment $\alpha \mapsto I$ gives a well defined map

$$M_2 \to \text{Cl}(L)[2].$$

This map is clearly surjective and its kernel is given by the positive units

$$\{\alpha \in A^\times/(A^\times)^2 : \alpha > 0\} = u_L^2/u_L^{2\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}.$$ 

Since $\# \text{Cl}(L)[2] = 2^k$, we know that $M_2$ is an elementary 2-group of size $2^{k+1}$. \qedhere

Now we are ready to prove the main theorem of this chapter.

**Theorem 2.12.** Let $\text{Cl}(L)$ be the ideal class group of the cubic field $L = \mathbb{Q}[x]/F(x)$. Let $k = \dim_{\mathbb{Z}_2} \text{Cl}(L)/2 \text{Cl}(L)$. Then

$$s_2(E/\mathbb{Q}) = k \text{ or } k + 1,$$

depending on whether the root number $\varepsilon(E/\mathbb{Q}) = (-1)^k$ or $(-1)^{k+1}$. In particular, if the class number $h_L$ of $L$ is odd (i.e., $k = 0$), then

$$s_2(E/\mathbb{Q}) = 0 \text{ or } 1,$$

depending on whether $\varepsilon(E/\mathbb{Q}) = +1$ or $-1$.

**Proof.** It follows from Lemma 2.10 and 2.11 that $s_2(E/\mathbb{Q}) = k$ or $k + 1$. By [Mon96, Theorem 1.5], the parity of $s_2(E/\mathbb{Q})$ is determined by the root number $\varepsilon(E/\mathbb{Q})$, that is,

$$( -1)^{s_2(E/\mathbb{Q})} = \varepsilon(E/\mathbb{Q}).$$

The desired result then follows. \qed
Chapter 3

Artin $L$-functions

In this chapter, we explain how Theorem 2.12, under the BSD conjecture, can be interpreted as a mod 2 congruence between the weight 2 newform $f \in S_2(N)$ associated to $E/\mathbb{Q}$ and a weight 1 newform $h$ associated to a certain 2-dimensional Artin representation $\sigma$.

Let $E/\mathbb{Q}$ be an elliptic curve. Let $\bar{\rho}: G_{\mathbb{Q}} \to \text{Aut}(E[2]) \cong \text{GL}_2(\mathbb{F}_2) = S_3$ be its mod 2 Galois representation. We will impose the following assumptions throughout this chapter.

**Assumption 3.1.**

1. $\bar{\rho}$ is surjective.
2. $E$ has negative discriminant $\Delta$.

**Remark 3.2.** $\bar{\rho}$ is surjective if and only if the 2-torsion field $\mathbb{Q}(E[2])$ is an $S_3$-extension over $\mathbb{Q}$. When $E: y^2 = F(x)$ is defined by a cubic polynomial $F(x) \in \mathbb{Q}[x]$, this happens if and only if $F(x)$ has Galois group $S_3$. In particular, Assumption 2.1 implies Assumption 3.1.
3.1 Artin representations and class numbers

Definition 3.3. Let $V$ be the unique 2-dimensional complex representation of $\text{GL}_2(\mathbb{F}_2) = S_3$. We define a complex representation $\sigma$ to be the composition

$$\sigma : G_{\mathbb{Q}} \xrightarrow{\bar{\rho}} \text{GL}_2(\mathbb{F}_2) \hookrightarrow \text{GL}(V) \cong \text{GL}_2(\mathbb{C}).$$

The kernel of $\sigma$ cuts out the $S_3$-extension $\mathbb{Q}(E[2])/\mathbb{Q}$, the Galois closure of the cubic field $L = \mathbb{Q}[x]/F(x)$. We write $G = \text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$ for short.

Let $L(\sigma,s)$ be the Artin $L$-function of $\sigma$ (for background on Artin $L$-functions, see [Tat11]). It has holomorphic continuation to $\mathbb{C}$ and satisfies a functional equation relating its values at $s$ and $1-s$. Since $\sigma$ is self-dual of orthogonal type (its image can be conjugated into $O_2(\mathbb{R})$), the sign of its functional equation is always $+1$ ([FQ73]). More precisely, let

$$\Lambda(\sigma,s) = ((2\pi)^{-s}\Gamma(s))^{\dim \sigma}L(\sigma,s)$$

be the complete $L$-function, then

$$\Lambda(\sigma,s) = N(\sigma)^{1/2-s}\Lambda(\sigma,1-s),$$

where $N(\sigma)$ is the Artin conductor of $\sigma$, a positive integer measuring the ramification of $\sigma$.

Proposition 3.4. Let $\zeta_{\mathbb{Q}}(s)$ be the Riemann zeta function and $\zeta_L(s)$ be the Dedekind zeta function of the cubic field $L$. Then

$$\zeta_{\mathbb{Q}}(s) \cdot L(\sigma,s) = \zeta_L(s).$$

In particular,

$$N(\sigma) = |d_L|,$$
3.2. The determinant and conductor

where \(d_L\) is the discriminant of \(L\).

Proof. Let \(H \subseteq G \cong S_3\) be a subgroup of order two. Then \(L \cong \mathbb{Q}(E[2])^H\). From the basic property of the Artin \(L\)-function of an induced representation, we know that \(\zeta_L(s) = L(\text{Ind}_H^G 1_H, s)\). Since \(\text{Ind}_H^G 1_H = 1_G \oplus \sigma\), we have \(\zeta_L(s) = L(1_G, s)L(\sigma, s) = \zeta_Q(s)L(\sigma, s)\).

The claim that \(N(\sigma) = d_L\) then follows from the conductor-discriminant formula. \(\square\)

Corollary 3.5. \(L(\sigma, s)\) has a simple zero at \(s = 0\) and

\[
L(\sigma, 1) = \frac{2\pi h_L \log u_L}{|d_L|^{1/2}}, \quad L'(\sigma, 0) = h_L \log u_L.
\]

Here \(u_L > 1\) is a fundamental unit of \(L\).

Proof. By the class number formula, for any number field \(K\), \(\zeta_K(s)\) has a simple pole at \(s = 1\) with residue \(\frac{2\pi(2\pi)^{s-1}h_K R_K}{w_K|d_K|^{1/2}}\) and has a zero of order \(r_1 + r_2 - 1\) with leading coefficient \(-\frac{h_K R_K}{w_K}\). In particular,

(1) \(\zeta_Q(s)\) has a simple pole at \(s = 1\) with residue 1 and has value \(\zeta_Q(0) = -\frac{1}{2}\);

(2) \(\zeta_L(s)\) has a simple pole at \(s = 1\) with residue \(\frac{2\pi h_L \log u_L}{|d_L|^{1/2}}\) and a simple zero at \(s = 0\) with leading coefficient \(-\frac{h_L \log u_L}{2}\).

The corollary then follows from Proposition 3.4. \(\square\)

3.2 The determinant and conductor

Proposition 3.6. \(\det \sigma = \varepsilon_K\), where \(\varepsilon_K\) is the quadratic character associated to \(K = \mathbb{Q}(\sqrt{\Delta})\). In particular, \(\sigma\) is an odd irreducible Artin representation.

Proof. Since \(\sigma\) has \(S_3\)-image, it is induced from a cubic character \(\chi : G_K \to \mathbb{C}^\times\), where \(K\) is the quadratic field corresponding to the sign representation

\[
G \cong S_3 \to \{\pm 1\}.
\]
3.2. The determinant and conductor

The unique quadratic subfield of \( \mathbb{Q}(E[2]) \) is \( K = \mathbb{Q}(\sqrt{\Delta}) \), where \( \Delta \) is the discriminant of \( E/\mathbb{Q} \) ([Ser72, p. 305]). By the general formula for the determinant of an induced representation, we have

\[
\det \sigma = \det(\text{Ind}^{G_K}_{G_G} \chi) = \varepsilon_K \cdot \chi_Q,
\]

where \( \chi_Q : G^{ab}_Q \rightarrow G^{ab}_K \xrightarrow{\chi} \mathbb{C}^\times \) is the transfer of \( \chi \). Since \( G^{ab} = \text{Gal}(K/\mathbb{Q}) \), it follows that \( \chi_Q \) is trivial. Since we assumed that \( \Delta < 0 \), we know that \( K \) is imaginary and \( \det \sigma = \varepsilon_K \) is \(-1\) on the class of complex conjugation, i.e., \( \sigma \) is odd.

By the general conductor formula for induced representations, we also have

**Proposition 3.7.** \( N(\sigma) = |d_K| \cdot N(\chi) \), where \( N(\chi) \) is the Artin conductor of \( \chi \).

We now further determine the Artin conductor \( N(\sigma) \) in terms of the Serre conductor \( N(\bar{\rho}) \) of the mod 2 representation \( \bar{\rho} \).

**Proposition 3.8.** We have \( N(\sigma) = N(\bar{\rho}), 4N(\bar{\rho}), \) or \( 8N(\bar{\rho}) \). Moreover,

1. If \( E \) has good supersingular reduction at 2, then \( N(\sigma) = 4N(\bar{\rho}) \).

2. If \( E \) has good ordinary reduction at 2, then \( N(\sigma) = N(\bar{\rho}) \) or \( 4N(\bar{\rho}) \) depending on whether 2 is unramified in \( K = \mathbb{Q}(\sqrt{\Delta}) \) or not.

3. If \( E \) has multiplicative reduction at 2, then the even part of \( N(\sigma) \) is equal to the even part of \( d_K \).

4. If \( E \) has additive reduction at 2 and satisfies Assumption 2.1, then \( N(\sigma) = N(\bar{\rho}) = D \).

**Proof.** By definition, the odd parts of \( N(\sigma) \) and \( N(\bar{\rho}) \) coincide and it remains to determine the even part of \( N(\sigma) \). Let \( D \subseteq G \cong S_3 \) be the decomposition group at 2 and \( I < D \) be the inertia subgroup at 2. We have following cases:

1. If \( D = S_3 \) or is of order 3, then \( I \) is either trivial or of order 3.
3.3. The determinant and conductor

(2) If $D$ is of order 2, then $I$ is either trivial or of order 2.

(3) If $D$ trivial, then $I$ is trivial.

We can determine the even part of $N(\sigma)$ depending on $I$:

(1) If $I$ is trivial, then $\sigma$ is unramified at 2 and $N(\sigma) = N(\bar{\rho})$.

(2) If $I$ is of order 3, then $\sigma$ is tamely ramified at 2, $V^I = 0$ and hence $N(\sigma) = 4N(\bar{\rho})$.

(3) If $I$ is of order 2, then the even part of $N(\sigma) = |d_L|$ (by Proposition 3.4) is equal to the discriminant of a ramified quadratic extension of $\mathbb{Q}_2$, which is either 4 or 8, hence $N(\sigma) = 4N(\bar{\rho})$ or $8N(\bar{\rho})$.

(4) When $I$ is trivial or of order 2, the even part of $N(\sigma) = d_L$ is equal to the even part of $d_K$. Moreover, $I$ is of order 2 if and only if 2 is ramified in $K = \mathbb{Q}(\sqrt{\Delta})$.

Now we can conclude:

(1) If $E$ has good supersingular reduction at 2, then $\sigma|_D$ is irreducible ([Ser72, p.275, Prop.12]), hence $I$ is of order 3 and $N(\sigma) = 4N(\bar{\rho})$.

(2) If $E$ has good ordinary reduction at 2, then the image of $\sigma|_D$ is contained in the Borel subgroup of $GL_2(\mathbb{F}_2)$, which has order 2. Hence $I$ is either trivial or order 2. Since $E$ has good reduction at 2, we know that $2 \nmid \Delta$, hence the 2-part of $d_K$ is 0 or 4, depending whether 2 is ramified in $K$ or not.

(3) If $E$ has multiplicative reduction at 2, then the image of $\sigma|_D$ is also contained in the Borel subgroup of $GL_2(\mathbb{F}_2)$, which has order 2. Hence $I$ is either trivial or order 2.

(4) If $E$ has additive reduction at 2 and satisfies Assumption 2.1, we have $d_L = -D$ is odd, hence $L/\mathbb{Q}$ is unramified at 2 and $N(\sigma) = N(\bar{\rho}) = |d_L| = D$. \qed
3.3 Weight one newforms

Write $L(\sigma, s) = \sum_{n \geq 1} b_n n^{-s}$. Then $b_p = \text{Tr}(\sigma(Frob_p))$ for any $p \nmid N(\sigma)$. In particular, $b_p$ takes values $2, 0, -1$ when $Frob_p \in G \cong S_3$ is of order $1, 2, 3$ respectively. The determination of $\det \sigma$ and $N(\sigma)$ in Proposition 3.6 and 3.8 is even more interesting in view of the following

**Theorem 3.9.** The formal series $h(z) = \sum_{n \geq 1} b_n q^n$ is the $q$-expansion of a weight one newform of level $N(\sigma)$ and nebentypus $\det \sigma = \varepsilon_K$.

**Proof.** This is a special case of Langlands–Weil for 2-dimensional odd irreducible Artin representations with solvable image (see [Ser77, Theorem 1]). The construction in our dihedral case was due to Hecke. Let $\psi : \mathbb{A}_K^\times \to \mathbb{C}^\times$ be the Hecke character associated to the cubic character $\chi : G_K \to \mathbb{C}^\times$ (recall that $\sigma = \text{Ind}_{G_K}^{G_Q} \chi$). Then the Hecke theta series associated to $\psi$,

$$\tilde{h}(z) := \sum_{a \subseteq \mathcal{O}_K} \psi(a) q^{N(a)},$$

where the sum runs over all integral ideals, is a weight one newform with nebentypus $\varepsilon_K$ and level $|d_K| \cdot N(\psi)$, which is equal to $N(\sigma)$ by Proposition 3.7 (see [Miy89, 4.8.2] for a proof using Weil’s converse theorem). Let $\tilde{b}_p$ be the $p$-th Fourier coefficient of $\tilde{h}(z)$, then $\tilde{b}_p = \sum_{N(p) = p} \psi(p)$. We easily see that for $p \nmid N(\sigma)$,

$$\tilde{b}_p = \begin{cases} 2, & \text{if } p = \mathfrak{p} \mathfrak{p} \text{ is split in } K, \psi(p) = 1, \\ 0, & \text{if } p \text{ is inert in } K, \\ -1, & \text{if } p = \mathfrak{p} \mathfrak{p} \text{ is split in } K, \psi(p) = \text{a primitive 3rd root of unity}. \end{cases}$$

By class field theory, the three cases exactly correspond to $Frob_p \in G \cong S_3$ having order $1, 2$ and $3$. It follows that $\tilde{b}_p = \text{Tr}(\sigma(Frob_p)) = b_p$ for $p \nmid N(\sigma)$ and thus $\tilde{h}(z) = h(z)$ is the desired weight one newform associated to the Artin representation $\sigma$. \hfill $\Box$

30
Corollary 3.10. Let \( f = \sum_{n \geq 1} a_n q^n \in S_2(N) \) be the weight 2 newform of level \( N \) and trivial nebentypus associated to the elliptic curve \( E \). Then for any prime \( p \neq 2 \),

\[
a_p \equiv b_p \pmod{2}.
\]

Moreover, we can determine the parity of \( a_2 \) and \( b_2 \) as follows.

1. If \( E \) has good supersingular reduction at 2, then \( a_2 \equiv 0 \) (mod 2), \( b_2 = 0 \).

2. If \( E \) has good ordinary reduction at 2, then \( a_2 \equiv 1 \) (mod 2). In this case, if 2 is ramified in \( K \), then \( b_2 = 1 \); otherwise \( b_2 = 0 \) or 2.

3. If \( E \) has multiplicative reduction at 2, then \( a_2 = \pm 1 \). In this case, if 2 is ramified in \( K \), then \( b_2 = 1 \); otherwise \( b_2 = 0 \) or 2.

4. If \( E \) has additive reduction and satisfies Assumption 2.1, then \( a_2 = 0 \). In this case, if 2 is inert in the cubic field \( L \), then \( b_2 = -1 \); otherwise \( b_2 = 0 \).

Proof. The mod 2 congruence follows by construction. All claims about \( a_2 \) are also clear.

To prove the claims about \( b_2 = \text{Tr}(\sigma(Frob_2)|V_I) \), where \( I \) is the inertia subgroup at 2, we proceed case by case as in the proof of Proposition 3.8.

1. If \( E \) has good supersingular reduction, then \( I \) has order 3. Hence \( V_I = 0 \) and \( b_2 = 0 \).

2. If \( E \) has good ordinary or multiplicative reduction. Then \( I \) is either of order 2 or trivial, depending on whether 2 is ramified in \( K \) or not. If \( I \) is order 2, then \( V_I \) is 1-dimensional and the action of \( \text{Frob}_2 \) is trivial, thus \( b_2 = 1 \). If \( I \) is trivial, then \( V_I = V \) and the action of \( \text{Frob}_2 \) is either of order 2 or trivial, thus \( b_2 = 0 \) or 2.

3. If \( E \) has additive reduction and satisfies Assumption 2.1, then \( I \) is trivial and \( V_I = V \).

Since \( F(x) \pmod{2} \) cannot be a product of three distinct linear factors in \( \mathbb{F}_2[x] \), we know that 2 does not split in \( L \). If 2 is inert in \( L \), then \( \text{Frob}_2 \) is of order 3 and \( b_2 = -1 \); otherwise \( \text{Frob}_2 \) is of order 2 and \( b_2 = 0 \).
To summarize, we obtain a congruence between a weight two newform and a weight one newform

\[ f \equiv h \pmod{2}, \]

in the sense that all (except possibly for \( p = 2 \)) of their Hecke eigenvalues are congruent mod 2. As explained in the introduction, under the BSD conjecture, Theorem 2.12 can be interpreted as a mod 2 congruence between the special values of the \( L \)-functions \( L(f, s) = L(E, s) \) and \( L(h, s) = L(\sigma, s) \).

Remark 3.11. We find this mod 2 congruence rather unusual: \( L(E, s) \) is of symplectic type with the sign of the functional equation \( \pm 1 \) whereas the Artin \( L \)-function \( L(\sigma, s) \) is of orthogonal type with the sign of the functional equation always +1. Congruences of this type mod \( p > 2 \) would force the signs to be the same. As Mazur pointed out to us, this may suggest something much more general with intersections mod 2 of 2-adic eigenvarieties of different (symplectic versus orthogonal) reductive groups.

Also, the point \( s = 1 \) is the central critical point for \( L(E, s) \) but there is no critical point for \( L(\sigma, s) \) in the sense of Deligne. We hope to formulate this type of mod 2 congruence between \( L \)-functions more precisely in the future.

3.4 Examples

We end our discussion on 2-Selmer groups and class numbers with several explicit examples.

Example 3.12 (cf. [Ser77, 7.3]). Consider the elliptic curve

\[ E = 92a1 : y^2 = F(x) = x^3 + x^2 + 2x + 1. \]

The polynomial \( F(x) \) is irreducible and has square-free and negative discriminant \(-D = -23\) and thus Assumption 2.1 holds. The elliptic curve \( E \) has discriminant \( \Delta = -2^4 \cdot 23 \),

\[ \Delta = -2^4 \cdot 23, \]
3.4. Examples

conductor \( N = 2^2 \cdot 23 \). The cubic field

\[
L = \mathbb{Q}[x]/(x^3 + x^2 + 2x + 1)
\]

has discriminant \( d_L = -23 \), hence the Artin representation \( \sigma \) has conductor \( N(\sigma) = 23 \).

The class number of \( L \) is 1 and we have \( s_2(E/\mathbb{Q}) = 0 \) as predicted by Theorem 2.12.

Notice that \( d_K = -23 \), so \( N(\chi) = 1 \) by Proposition 3.7, i.e., \( \chi \) is unramified. Hence the Hecke character \( \psi \) can be viewed as an order 3 character on the ideal class group \( \text{Cl}(K) \). We remark that \( K \) is the cubic field of \textit{smallest} (in the sense of the absolute value) discriminant with class number 3. The three ideal classes in \( \text{Cl}(K) \) are represented by the three integral binary quadratic forms of discriminant \( d_K = -23 \),

\[
x^2 + xy + 6y^2, \quad 2x^2 \pm xy + 3y^2,
\]

of order 1 and 3 respectively. We find that \( h(z) \) is the following simple linear combination of theta series associated to these quadratic forms:

\[
h(z) = \frac{1}{2} \left( \sum_{m,n \in \mathbb{Z}} q^{m^2+mn+6n^2} - \sum_{m,n \in \mathbb{Z}} q^{2m^2+mn+3n^2} \right)
= q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} - q^{24} + q^{25}
+ q^{26} + q^{27} - q^{29} - q^{31} + q^{39} - q^{41} - q^{46} - q^{47} + q^{48} + q^{49} - q^{50} \cdots
\]

We remark that \( \sigma \) is the irreducible 2-dimensional Artin representation of \textit{smallest} conductor ([Ser77, 8.1]). Moreover, \( h(z) \) can be written as the classical eta product:

\[
h(z) = \eta(z)\eta(23z) = q \prod_{n \geq 1} (1 - q^n)(1 - q^{23n}),
\]

33
3.4. Examples

where

\[ \eta(z) = q^{1/24} \prod_{n \geq 1} (1 - q^n) = \sum_{n \geq 1} \left( \frac{12}{n} \right) q^{n^2/24} \]

is Dedekind’s eta function.

The first few Hecke eigenvalues of the newforms \( f(z) \in S_2(92) \) and \( h(z) \in S_1(23, \varepsilon_{-23}) \) are listed in Table 3.1. We see that \( a_p \equiv b_p \pmod{2} \) for \( p \neq 2 \), \( a_2 = 0 \) and \( b_2 = -1 \) as in Corollary 3.10 (2 is inert in \( L \)).

<table>
<thead>
<tr>
<th>( p )</th>
<th>( 2 )</th>
<th>( 3 )</th>
<th>( 5 )</th>
<th>( 7 )</th>
<th>( 11 )</th>
<th>( 13 )</th>
<th>( 17 )</th>
<th>( 19 )</th>
<th>( 23 )</th>
<th>( 29 )</th>
<th>( 31 )</th>
<th>( 37 )</th>
<th>( 41 )</th>
<th>( 43 )</th>
<th>( 47 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a_p(f) )</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>-1</td>
<td>-6</td>
<td>2</td>
<td>-1</td>
<td>-3</td>
<td>5</td>
<td>8</td>
<td>3</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>( b_p(h) )</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td></td>
</tr>
</tbody>
</table>

Table 3.1: \( E = 92a1 \)

**Example 3.13.** Consider elliptic curve

\[ E = X_0(11) = 11a1 : y^2 + y = x^3 - x^2 - 10x - 20, \]

which has the *smallest* conductor 11 among all elliptic curves over \( \mathbb{Q} \). It has discriminant \( \Delta = -11 \) and has good supersingular reduction at 2. The cubic field

\[ L \cong \mathbb{Q}[x]/(x^3 - x^2 + x + 1) \]

has discriminant \( d_L = -2^2 \cdot 11 \). Hence the Artin representation \( \sigma \) has conductor \( N(\sigma) = 2^2 \cdot 11 \). The class number of \( L \) is 1 and we have \( s_2(E/\mathbb{Q}) = 0 \) as predicted by Theorem 2.12.

The ring class group of the quadratic order of discriminant \(-44\) in \( K = \mathbb{Q}(\sqrt{-11}) \) has order 3, represented by the three binary quadratic form of discriminant \(-44\),

\[ 2x^2 + 11y^2, \quad 3x^2 \pm 2xy + 4y^2 \]

of order 1 and 3 respectively. We find that \( h(z) \) is the following simple linear combination
of theta series associated to these quadratic forms:

\[ h(z) = \frac{1}{2} \left( \sum_{m,n \in \mathbb{Z}} q^{2m^2+11n^2} - \sum_{m,n \in \mathbb{Z}} q^{3m^2+2mn+4n^2} \right) \]

\[ = q - q^3 - q^5 + q^{11} - q^{23} + q^{27} - q^{31} - q^{33} - q^{37} + 2q^{47} + q^{49} + \ldots \]

Moreover, \( h(z) \) is the classical eta product

\[ h(z) = \eta(2z)\eta(22z) = q \prod_{n \geq 1} (1 - q^{2n})(1 - q^{22n}). \]

The newform \( f(z) \in S_2(11) \) is also a classical eta product

\[ f(z) = \eta^2(z)\eta^2(11z) = q \prod_{n \geq 1} (1 - q^n)^2(1 - q^{11n})^2 \]

\[ = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} \]

\[ + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 2q^{20} + 2q^{21} - 2q^{22} \]

\[ - q^{23} - 4q^{25} - 8q^{26} + 5q^{27} - 4q^{28} + 2q^{30} + 7q^{31} + 8q^{32} - q^{33} \]

\[ + 4q^{34} - 2q^{35} - 4q^{36} + 3q^{37} - 4q^{39} - 8q^{41} - 4q^{42} - 6q^{43} + 2q^{44} \]

\[ - 2q^{45} + 2q^{46} + 8q^{47} + 4q^{48} - 3q^{49} + 8q^{50} \ldots \]

The first few Hecke eigenvalues of the newforms \( f(z) \in S_2(11) \) and \( h(z) \in S_1(44, \varepsilon_{-44}) \) are listed in Table 3.2. We see that \( a_p \equiv b_p \pmod{2} \) for all \( p \) as in Corollary 3.10.

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
<th>47</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a_p(f) )</td>
<td>-2</td>
<td>-1</td>
<td>1</td>
<td>-2</td>
<td>1</td>
<td>-2</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>7</td>
<td>3</td>
<td>-8</td>
<td>-6</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>( b_p(h) )</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 3.2: \( E = 11a1 \)
Example 3.14. Consider the elliptic curve

\[ E = 26a_1 : y^2 + xy + y = x^3 - 5x - 8. \]

It has discriminant \( \Delta = -2^3 \cdot 13^3 \) and has nonsplit multiplicative reduction at 2. The cubic field

\[ L \cong \mathbb{Q}[x]/(x^3 - x - 2) \]

has discriminant \( d_L = -2^3 \cdot 13 = -104 \). Notice that \( d_K = -2^3 \cdot 13 \), so \( N(\chi) = 1 \) by Proposition 3.7, i.e., \( \chi \) is unramified. Hence \( \psi \) can be viewed as an order three character on the ideal class group \( \text{Cl}(K) \). We remark that \( K \) is the quadratic field of class number 6 with the second smallest discriminant (the smallest being \( \mathbb{Q}(\sqrt{-87}) \)). The 6 ideal classes are represented by the following 6 integral binary quadratic forms of discriminant \( d_K = -104 \),

\[ x^2 + 26y^2, \quad 2x^2 + 13y^2, \quad 3x^2 \pm 2xy + 9y^2, \quad 5x^2 \pm 4xy + 6y^2, \]

of order 1, 2, 3, 6 respectively. Since the character \( \psi \) takes value 1 on the order 1 and 2 classes and a primitive 3rd root of unity on the order 3 and 6 classes, we find that \( h(z) \) is the following simple linear combination of theta series associated to these quadratic forms:

\[
\begin{align*}
    h(z) &= \frac{1}{2} \left( \sum_{m,n \in \mathbb{Z}} q^{m^2+26n^2} + \sum_{m,n \in \mathbb{Z}} q^{2m^2+13n^2} - \sum_{m,n \in \mathbb{Z}} q^{3m^2+2mn+9n^2} - \sum_{m,n \in \mathbb{Z}} q^{5m^2+4mn+6n^2} \right) \\
    &= q + q^2 - q^3 + q^4 - q^5 - q^6 - q^7 + q^8 - q^{10} - q^{12} + q^{13} - q^{14} + q^{15} + q^{16} - q^{17} \\
    &\quad - q^{20} + q^{21} + q^{24} + q^{26} + q^{27} - q^{28} + q^{30} + 2q^{31} + q^{32} - q^{34} + q^{35} - q^{37} - q^{39} \\
    &\quad - q^{40} + q^{42} - q^{43} - q^{47} - q^{48} \ldots
\end{align*}
\]

The first few Hecke eigenvalues of the newforms \( f(z) \in S_2(26) \) and \( h(z) \in S_1(-104, \epsilon_{-104}) \)
are listed in Table 3.3. We see that \( a_p \equiv b_p \pmod{2} \) for all \( p \) as in Corollary 3.10 (2 is ramified in \( K \)).

<table>
<thead>
<tr>
<th>( p )</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
<th>47</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a_p(f) )</td>
<td>-1</td>
<td>1</td>
<td>-3</td>
<td>-1</td>
<td>6</td>
<td>1</td>
<td>-3</td>
<td>0</td>
<td>6</td>
<td>-4</td>
<td>-7</td>
<td>0</td>
<td>-1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>( b_p(h) )</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
<td></td>
</tr>
</tbody>
</table>

Table 3.3: \( E = 26a1 \)

**Example 3.15.** Consider the elliptic curve

\[
E = 1132a1 : y^2 = F(x) = x^3 + x^2 - 5x + 4.
\]

The polynomial \( F(x) \) is irreducible and has discriminant \(-D = -283\) and thus Assumption 2.1 holds. The elliptic curve \( E \) has discriminant \( \Delta = -2^4 \cdot 283 \), conductor \( N = 2^2 \cdot 283 \). The cubic field \( L = \mathbb{Q}[x]/F(x) \) has discriminant \( d_L = -283 \) and class number 2. We remark that \( L \) has the *smallest* discriminant among all class number 2 cubic fields. Theorem 2.12 predicts that \( s_2(E/\mathbb{Q}) = 1 \) or 2 according to the root number. In fact, \( \varepsilon(E/\mathbb{Q}) = +1 \), \( r_{\text{alg}}(E/\mathbb{Q}) = s_2(E/\mathbb{Q}) = 2 \) and the two points \((-1, 3)\) and \((1, -1)\) generate \( E(\mathbb{Q}) \).

**Example 3.16.** Consider the elliptic curve

\[
E = 26284a1 : y^2 = F(x) = x^3 + x^2 - 9x + 16.
\]

The polynomial \( F(x) \) is irreducible and has discriminant \(-D = -6571\) and thus Assumption 2.1 holds. The elliptic curve \( E \) has discriminant \( \Delta = -2^4 \cdot 6571 \), conductor \( N = 2^2 \cdot 6571 \). The cubic field \( L = \mathbb{Q}[x]/F(x) \) has discriminant \( d_L = -6571 \) and class group \( \text{Cl}(L) \cong (\mathbb{Z}/2\mathbb{Z})^2 \). We remark that \( L \) has the *smallest* discriminant among all cubic fields with class group \((\mathbb{Z}/2\mathbb{Z})^2\). Theorem 2.12 predicts that \( s_2(E/\mathbb{Q}) = 2 \) or 3 according to the root number. In fact, \( \varepsilon(E/\mathbb{Q}) = -1 \), \( r_{\text{alg}}(E/\mathbb{Q}) = s_2(E/\mathbb{Q}) = 3 \) and the three points \((-4, 2), (-3, 5), (-1, 5)\) generate \( E(\mathbb{Q}) \).
Example 3.17. Consider the elliptic curve

\[ E : y^2 = F(x) = x^3 - 49x + 169. \]

The polynomial \( F(x) \) is irreducible and has discriminant \(-D = -37 \cdot 8123\) and thus Assumption 2.1 holds. The elliptic curve \( E \) has discriminant \( \Delta = -2^4 \cdot 37 \cdot 8123 \), conductor \( N = 1202204 = 2^2 \cdot 37 \cdot 8123 \). The cubic field \( L = \mathbb{Q}[x]/F(x) \) has discriminant \( d_L = -37 \cdot 8123 \) and class group \( \text{Cl}(L) \cong (\mathbb{Z}/2\mathbb{Z})^3 \). We remark that \( L \) has the \textit{smallest} discriminant among all cubic fields with class group \( (\mathbb{Z}/2\mathbb{Z})^3 \). Theorem 2.12 predicts that \( s_2(E/\mathbb{Q}) = 3 \) or \( 4 \) according to the root number. In fact, \( \varepsilon(E/\mathbb{Q}) = +1 \), \( r_{\text{alg}}(E/\mathbb{Q}) = s_2(E/\mathbb{Q}) = 4 \) and the four points \((-8, 7), (-7, 13), (-5, 17), (-3, 17)\) generate \( E(\mathbb{Q}) \).
Chapter 4

Heegner points on elliptic curves of conductor $4D$

We come back to the situation in Chapter 2. Throughout this chapter we will impose the following assumption.

Assumption 4.1. Suppose $E$ has equation $y^2 = F(x)$, where $F(x) = x^3 + a_2x^2 + a_4x + a_6$ is an integral polynomial which

(1) is irreducible, and

(2) has negative and square-free discriminant $-D$.

We further assume that

(3) $E/\mathbb{Q}$ has Kodaira type IV.

Remark 4.2. The additional assumption (3) that $E/\mathbb{Q}$ has Kodaira type IV means that the special fiber of the minimal regular model of $E/\mathbb{Q}$ consists of three $\mathbb{P}^1$’s intersecting at a triple point. It implies that $m = 3$ in Equation (2.1). Hence $\text{ord}_2(N) = 2$ and $E$ has the minimal possible conductor $N = 4D$. It also implies that the $j$-invariant of $E$ has positive 2-adic valuation ([Sil94, Table 4.1]). In particular, $E$ has potentially good reduction at 2.
Example 4.3. If we assume

\[
\begin{align*}
  a_6 &\equiv 1 \pmod{4}, \\
  a_4^2 &\equiv 4a_2 \pmod{8},
\end{align*}
\]

then it follows from Tate’s algorithm [Sil94, IV.9] that \(E\) has Kodaira type IV over \(\mathbb{Q}_2\). In fact, making a change of variable \(y' = y + 1\), \(x' = x\), we obtain the following equation

\[
y'^2 + 2y' = x'^3 + a_2x'^2 + a_4x' + (a_6 - 1),
\]

satisfying \(2 \mid a'_3, a'_4, a'_6\). We compute that

\[
b'_2 = 4a_2, \quad b'_4 = 2a_4, \quad b'_6 = 4a_6, \quad b'_8 = 4a_2a_6 - a'_7, \quad c'_4 = 16(a_2^2 - 3a_4).
\]

So

\[
2 \mid c'_4, \quad 2^2 \mid a'_3, \quad 2^3 \mid b'_8, \quad 2^3 \mid b'_6,
\]

and Tate’s algorithm outputs the Kodaira type IV. Moreover, the component group of the Néron model over \(\mathbb{Q}_2\) is either \(\mathbb{Z}/3\mathbb{Z}\) or \(\mu_3\). It is \(\mathbb{Z}/3\mathbb{Z}\) if and only if \(x^2 + x - (a_6 - 1)/4 \equiv 0 \pmod{2}\) has a solution, if and only if \(a_6 \equiv 1 \pmod{8}\).

As we will see, the additional assumption (3) also pins down the root number of \(E\) over the quadratic field \(\mathbb{Q}(i)\) to be \(-1\) (Proposition 4.7). Let

\[
E^*: y^2 = F^*(x) = x^3 - a_2x^2 + a_4x - a_6
\]

be the quadratic twist of \(E\) by \(\mathbb{Q}(i)\). We have

\[
\varepsilon(E/\mathbb{Q}) \cdot \varepsilon(E^*/\mathbb{Q}) = \varepsilon(E/\mathbb{Q}(i)) = -1.
\]
4.1. Root numbers

It follows that the functional equations for $L(E/Q, s)$ and $L(E^*/Q, s)$ have different signs $\varepsilon(E/Q)$ and $\varepsilon(E^*/Q)$. We denote by $E^\pm = E$ or $E^*$ so that $\varepsilon(E^\pm/Q) = \pm 1$.

Notice that $E^*$ also satisfies Assumption 2.1. Moreover, the cubic field defined by $Q[x]/F^*(x)$ is isomorphic to $L = Q[x]/F(x)$. When the class number $h_L$ is odd, the $2$-Selmer rank $s_2(E^-/Q) = 1$ by Theorem 2.12. The $p$-Selmer rank one Conjecture 1.6 then predicts that

**Conjecture 4.4.** If the class number $h_L$ is odd, then $r_{\text{alg}}(E^-/Q) = 1$.

We pursue a canonical construction of a point (conjecturally) of infinite order using Shimura curves in this chapter.

4.1 Root numbers

Our first goal is to determine the root number of $E$ over the quadratic field $Q(i)$.

**Lemma 4.5.** The field $Q_2(E[3])$ generated by 3-torsion points of $E$ is the tamely ramified $S_3$-extension $Q_2(\zeta_3, \sqrt[3]{\Delta})$.

**Proof.** The assumption of Kodaira type IV at 2 allows us to compute $Q_2(E[3])$ as follows. Since the component group of the Néron model of $E/Q_2$ is either $\mathbb{Z}/3\mathbb{Z}$ or $\mu_3$, we know that $E$ has a subgroup $\mathbb{Z}/3\mathbb{Z}$ over the unramified quadratic extension $M = Q_2(\zeta_3)$. Let $G = \text{Gal}(M(E[3])/M) \subseteq \text{GL}_2(F_3)$. Then by the Weil pairing, the inertia subgroup $I \subseteq G$ acts as a subgroup of $\{(1, 0)\} \subseteq \text{GL}_2(F_3)$, hence $I$ is either trivial or of order 3. But $Q_2(E[3])$ always contains $\sqrt[3]{\Delta}$ (see [Ser72, p. 305]), so $Q_2(E[3])/Q_2$ is ramified and $I$ is of order 3. Notice that $Q_2(\zeta_3, \sqrt[3]{\Delta})$, as the Galois closure of $Q_2(\sqrt[3]{\Delta})$, has Galois group $S_3$, so we know that $G$ cannot be cyclic of order 3 or 6. Since $I$ is normal in $G$ and $G/I$ is cyclic, it follows that $G \cong S_3$ by inspection on possible subgroups of $\text{GL}_2(F_3)$. Therefore $Q_2(E[3]) = Q_2(\zeta_3, \sqrt[3]{\Delta})$.  \[\square\]
Remark 4.6. It also follows from this lemma directly that \( \text{ord}_2(N) = 2 \), which reproves the Ogg–Saito formula in this case.

**Proposition 4.7.** The root number \( \varepsilon(E/Q(i)) \) of \( E/Q(i) \) is \(-1\).

**Proof.** Recall that the root number is the product of local root numbers over all places \( v \)

\[ \varepsilon(E/Q(i)) = \prod_v \varepsilon_v(E/Q(i)). \]

We compute all the local root numbers (cf. [Dok13, 3.4]) as follows.

1. The local root number of an elliptic curve is always \(-1\) at an infinite place.
2. For \( p \notin 2 \mathcal{D} \), the elliptic curve \( E \) has good reduction at \( p \) and thus \( \varepsilon_p(E/Q(i)) = +1 \).
3. For \( p | D \), the elliptic curve \( E \) has multiplicative reduction at \( p \).
   - When \( p \) lies above \( p \equiv 3 \mod 4 \), \( \mathbb{Q}(i)_p \) is the unramified quadratic extension of \( \mathbb{Q}_p \) and thus \( E \) has split multiplicative reduction at \( p \). Therefore \( \varepsilon_p(E/Q(i)) = -1 \). Because \( D \equiv 3 \mod 4 \) is square-free, there are an odd number of primes \( p | D \) lying above \( p \equiv 3 \mod 4 \). Hence the product over all \( p \) above \( p \equiv 3 \mod 4 \) is \(-1\).
   - When \( p \) lies above \( p \equiv 1 \mod 4 \), \( E \) may have split or nonsplit multiplicative reduction at \( p \). But since \( p = pp' \) splits as two primes in \( \mathbb{Q}(i) \) and \( \varepsilon_p(E/Q(i)) = \varepsilon_{p'}(E/Q(i)) \), we know that the product over all \( p \) above \( p \equiv 1 \mod 4 \) is \(+1\).
4. When \( p | 2 \), we know the 3-torsion points \( E[3] \) generate a \( S_3 \)-extension over the wildly ramified quadratic extension \( \mathbb{Q}(i)_p = \mathbb{Q}_2(i) \) by Lemma 4.5. The local root number is \(-1\) in this case by [DD08, Remark 5].

Combining all the local results gives the desired root number \( \varepsilon(E/Q(i)) = -1 \). \( \square \)
4.2 Explicit Jacquet–Langlands correspondence

By the modularity theorem, there is an automorphic representation $\pi = \hat{\otimes}_v \pi_v$ of $\text{GL}_2(\mathbb{A})$ associated to the elliptic curve $E$, where $\mathbb{A}$ is the ring of adeles of $\mathbb{Q}$. It can be characterized as follows:

1. $\pi$ has trivial central character.
2. $\pi_\infty$ is a discrete series with Harish-Chandra parameter $\frac{1}{2}$ (corresponding to weight 2 modular forms).
3. For $p \nmid 2D$, $\pi_p$ is unramified. Its Satake parameter has characteristic polynomial $X^2 - a_p X + p$, where $a_p = p + 1 - \#E(F_p)$.
4. For $p \mid D$, $\pi_p$ is the Steinberg representation or the unramified quadratic twist of the Steinberg representation, depending on whether $\varepsilon_p(E/\mathbb{Q}) = -1$ or $\varepsilon_p(E/\mathbb{Q}) = +1$.
5. For $p = 2$, $\pi_2$ has conductor 2 (since $\text{ord}_2(N) = 2$). It cannot be a tamely ramified principal series or a tamely ramified twist of the Steinberg representation, since there are no tamely ramified characters of $\mathbb{Q}_2^\times$! Therefore $\pi_2$ is a depth zero supercuspidal representation, which is compactly induced from $\text{PGL}_2(\mathbb{Z}_2)$ using the unique discrete series representation of $\text{PGL}_2(\mathbb{F}_2) \cong S_3$, the sign character $S_3 \to \{\pm 1\}$.

Let $B = (-1, D)_\mathbb{Q}$ be the rational quaternion algebra

$$\mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \quad i^2 = -1, j^2 = D, ij = -ji.$$  

Then $B$ is split at $\infty$ and is ramified at primes in

$$\Sigma = \{2\} \cup \{p \mid D : p \equiv 3 \pmod{4}\}.$$
4.2. Explicit Jacquet–Langlands correspondence

Notice that $\Sigma$ has even cardinality since $D \equiv 3 \pmod{4}$. Let

$$R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij \subseteq B.$$  (4.1)

Then $R$ is an order of reduced discriminant $4D$. We now give a description of the local orders $R_p = R \otimes \mathbb{Z}_p$ and the normalizers of $R_p^\times$.

**Proposition 4.8.** Let $W_p = N_{B_p^\times}(R_p^\times)/R_p^\times \mathbb{Q}_p^\times$, where $N_G(H)$ denotes the normalizer of $H$ in $G$. Then

$$W_p \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & p \mid D, \\ S_3, & p = 2, \\ \{1\}, & \text{otherwise}. \end{cases}$$

**Proof.** We have the following cases:

- For $p \mid 2D$, $B_p$ is isomorphic to the matrix algebra $M_2(\mathbb{Q}_p)$ and $R_p$ is a maximal order $M_2(\mathbb{Z}_p)$ (up to conjugation). Hence $N_{B_p^\times}(R_p^\times) = \text{GL}_2(\mathbb{Z}_p) \cdot \mathbb{Q}_p^\times = R_p^\times \cdot \mathbb{Q}_p^\times$ and $W_p$ is trivial.

- For $p \mid 2D$, $p \not\in \Sigma$, $B_p$ is isomorphic to $M_2(\mathbb{Q}_p)$ and $R_p$ is an order of reduced discriminant $p\mathbb{Z}_p$, which is $\left( \begin{array}{cc} \mathbb{Z}_p & \mathbb{Z}_p \\ p\mathbb{Z}_p & p\mathbb{Z}_p \end{array} \right)$ (up to conjugation). Therefore $R_p^\times$ is the standard Iwahori subgroup of $\text{GL}_2(\mathbb{Q}_p)$ and $N_{B_p^\times}(R_p^\times)/R_p^\times \mathbb{Q}_p^\times \cong \mathbb{Z}/2\mathbb{Z}$ generated by the element $\left( \begin{array}{cc} 0 & 1 \\ p & 0 \end{array} \right)$.

- For odd $p \in \Sigma$, $B_p$ is a quaternion algebra over $\mathbb{Q}_p$ and $R_p$ is the maximal order of $B_p$. Hence $N_{B_p^\times}(R_p^\times)/R_p^\times \mathbb{Q}_p^\times \cong \mathbb{Z}/2\mathbb{Z}$ is generated by a uniformizer of $B_p$.

- For $p = 2$, since $R_2$ has reduced discriminant $4\mathbb{Z}_2$, it is the unique index 2 suborder of the maximal order $\mathcal{O}_2$ of $B_2$,

$$R_2 = \{ x \in \mathcal{O}_2 : (x \mod m_2) \in \mathbb{F}_2 \subseteq \mathbb{F}_4 = \mathcal{O}_2/m_2 \},$$
where $m_2$ is the maximal ideal of $O_2$. Then $N_{B_2^\times}(R_2^\times)/R_2^\times \mathbb{Q}_2^\times \cong B_2^\times /R_2^\times \mathbb{Q}_2^\times \cong S_3$, which is generated by the order 2 class of a uniformizer and the cyclic quotient $O_2^\times /R_2^\times \cong \mathbb{F}_2^\times /\mathbb{F}_2^\times \cong \mathbb{Z}/3\mathbb{Z}$.

Remark 4.9. Since $R_p$ is a local Eichler order of reduced discriminant $p$ for any $p \neq 2$ (for background on Eichler orders, see [AB04, 1.2]) and Eichler orders are determined by its localizations ([AB04, 1.51]), we know that there is a unique Eichler order $S$ such that

$$S_p = R_p \text{ for } p \neq 2, \quad S_2 = O_2.$$ 

Then $S$ is the unique Eichler order of reduced discriminant $2D$ containing $R$ and $R \subseteq S$ is the unique index 2 suborder, given by

$$R = \{ x \in S : (x \mod m_2) \in \mathbb{F}_2 \subseteq \mathbb{F}_4 = O_2 / m_2 \}.$$ 

The Jacquet–Langlands correspondence associates to $\pi$ an automorphic representation $\sigma = \hat{\otimes} \sigma_v$ of $\hat{B}^\times = B^\times (\mathbb{A})$ of the same conductor $4D$. We can characterize it as follows:

1. $\sigma$ has trivial central character.

2. $\sigma_\infty \cong \pi_\infty$ is a discrete series with Harish-Chandra parameter $\frac{1}{2}$ (corresponding to weight 2 modular forms).

3. For $p \nmid 2D$, we have $B_p^\times \cong \text{GL}_2(\mathbb{Q}_p)$ and $\sigma_p \cong \pi_p$ is unramified. Its Satake parameter has characteristic polynomial $X^2 - a_p X + p$, where $a_p = p + 1 - \# E(\mathbb{F}_p)$.

4. For $p \mid 2D$, $p \notin \Sigma$, we also have $B_v^\times \cong \text{GL}_2(\mathbb{Q}_v)$ and $\sigma_v \cong \pi_v$. Since $\sigma_p$ has conductor 1 and $R_p^\times$ is the standard Iwahori subgroup of $\text{GL}_2(\mathbb{Q}_p)$, the fixed space $\sigma_{pR_p}^R$ is 1-dimensional. The group $W_p$ acts on $\delta_{pR_p}^R$ via the sign or the trivial character depending on whether $\pi_p$ is the Steinberg representation or the unramified quadratic twist of the Steinberg representation.
4.3 Shimura curves and Heegner points

(5) For odd \( p \in \Sigma \), since \( \sigma_p \) has conductor 1, the fixed space \( \sigma_p^{R\hat{x}} \) is a 1-dimensional representation of \( W_p \). It is either the trivial or the sign character depending on whether \( \pi_p \) is the Steinberg representation or the unramified quadratic twist of the Steinberg representation.

(6) For \( p = 2 \), since \( \sigma_2 \) has conductor 2 (\( \text{ord}_2(N) = 2 \)), we have \( \sigma_2^{R\hat{x}} \neq 0 \). Since \( \pi_2 \) is supercuspidal, we know that \( \sigma_2 \) is the unique 2-dimensional irreducible representation of \( B_2^\times / \mathbb{Q}_2^\times \simeq S_3 \).

Let \( \hat{R}^\times = (R \otimes \hat{\mathbb{Z}})^\times \). The following proposition follows immediately from the previous local description of \( \sigma \).

**Proposition 4.10.** (1) The space of invariants \( \sigma^{R\hat{x}} \) is 2-dimensional.

(2) For \( p \mid D, W_p \cong \mathbb{Z}/2\mathbb{Z} \) acts on \( \sigma^{R\hat{x}} \) via 2 copies of the character

\[ w_p \mapsto \left( -\frac{1}{p} \right) \varepsilon_p(E/\mathbb{Q}). \]

(3) For \( p = 2 \), \( W_2 \cong S_3 \) acts on \( \sigma^{R\hat{x}} \) via the unique 2-dimensional representation of \( S_3 \).

4.3 Shimura curves and Heegner points

Let \( \mathcal{H}^\pm = \mathbb{C} - \mathbb{R} \) be the union of the upper and lower half plane. Associated to the order \( R \) we have a Shimura curve

\[ X = R^\times \backslash \mathcal{H}^\pm, \]

where \( R^\times \) acts on \( \mathcal{H}^\pm \) via an embedding \( R^\times \hookrightarrow (B \otimes \mathbb{R})^\times \cong \text{GL}_2(\mathbb{R}) \). Let \( T/\mathbb{Q} \) be the maximal torus in \( B^\times \) induced by the natural embedding \( \mathbb{Z}[i] \hookrightarrow R \) (so \( T \) is split by \( \mathbb{Q}(i) \)). Let \( M \) be the \( \text{GL}_2(\mathbb{R}) \)-conjugates of the natural homomorphism \( h_0 : T(\mathbb{R}) = \mathbb{C}^\times \hookrightarrow \text{GL}_2(\mathbb{R}) \), then \( M \cong \mathcal{H}^\pm \) and \( h_0 \) is naturally identified with \( i \in \mathcal{H}^+ \). The Shimura curve \( X \) has the
4.3. Shimura curves and Heegner points

adelic description

\[ X \cong B^\times(Q) \backslash M \times B^\times(k_f)/\hat{R}^\times. \quad (4.2) \]

It is a well-known fact due to Shimura [Shi67] that the points of \( X \) classify abelian surfaces together with endomorphisms by \( R \) and this moduli interpretation provides the Shimura curve \( X \) with a canonical smooth projective model over \( \mathbb{Q} \).

**Definition 4.11.** Let \( K/\mathbb{Q} \) be an imaginary quadratic field with an embedding \( \tau : \mathcal{O}_K \hookrightarrow \mathbb{R} \). Then the induced homomorphism \( h : (K \otimes \mathbb{R})^\times = \mathbb{C}^\times \hookrightarrow (B \otimes \mathbb{R})^\times \cong \text{GL}_2(\mathbb{R}) \) corresponds to a point \( y_K \) on \( X \), known as a Heegner point. Notice that \( y_K \) depends on the choice of the embedding \( \tau \). In terms of the moduli interpretation, \( y_K \) corresponds to an abelian surface which is isomorphic to a product of two elliptic curves with complex multiplication by \( \mathcal{O}_K \). By the theory of complex multiplication, \( y_K \) is defined over the Hilbert class field of \( K \).

We specialize to the case \( K = \mathbb{Q}(i) \) and the natural embedding

\[ \tau : \mathcal{O}_K = \mathbb{Z}[i] \hookrightarrow R = \mathbb{Z} + Zi + Zj + Zij. \]

The associated Heegner point \( y_K \) is represented by the point \([h_0, 1]\) under the double quotient (4.2) and it is \( K \)-rational since \( K \) has class number one.

The finite group \( W = \prod_{p \mid D} W_p \) acts on \( X \) as automorphisms defined over \( \mathbb{Q} \). The generator \( w_p \) of \( W_p \) for \( p \mid D \) are known as the Atkin–Lehner involution.

**Proposition 4.12.** Let \( w = \prod_{p \mid D} w_p \in W \). Then \( w(y_K) = \overline{y_K} \), the complex conjugate of \( y_K \).

**Proof.** In view of the moduli interpretation, the point \( \overline{y_K} \) corresponds to the complex conjugate embedding \( \overline{\tau} : \mathbb{Z}[i] \hookrightarrow R \) of \( \tau \). Since \( ji^{-1} = -i \), we know that conjugating \( \tau \) by \( j \in B^\times \) gives \( \overline{\tau} \) and thus \( jy_K = \overline{y_K} \). On the other hand, the reduced norm of \( j^2 \) is \(-D\), so
we see that
\[
jR_p^\times \mathbb{Q}_p^\times / R_p^\times \mathbb{Q}_p^\times = \begin{cases} w_p, & p \mid D, \\ 1, & p \nmid D. \end{cases}
\]
It follows that \( j_{y_K} = j[h_0, 1] = [h_0, w] = w(y_K) \). We conclude that \( w(y_K) = \overline{y_K} \).

**Proposition 4.13.** Each point in the set \( W(y_K) = \{ \sigma(y_K), \sigma \in W \} \) has a stabilizer of order 2 (contained in \( W \)) under the action of \( W \). In particular, \( W(y_K) \) has size \( 3 \cdot 2^\# \{ p \mid D \} \) and \( W_2(y_K) \) has size 3.

**Proof.** The stabilizer of \( y_K = [h_0, 1] \) under the action of \( B^\times \) is \( T(Q) = \mathbb{Q}(i)^\times \subseteq B^\times \). Since \( \mathbb{Q}(i) \) is unramified at \( p \neq 2 \), it follows that for \( p \neq 2 \), \( \mathbb{Q}_p(i)^\times R_p^\times / R_p^\times \mathbb{Q}_p^\times = \{ 1 \} \) and thus \( W_p \) acts on \( W(y_K) \) freely. For \( p = 2 \), \( \mathbb{Q}(i) \) is ramified at 2 and \( \mathbb{Q}_2(i)^\times R_2^\times / R_2^\times \mathbb{Q}_2^\times \cong \mathbb{Z}/2\mathbb{Z} \) is generated by the class of a uniformizer of \( \mathbb{Q}_2(i) \). So \( W_2 \) acts on \( y_K \) with a stabilizer of order 2.

Let \( D^0 \) be the free abelian group of degree 0 divisors supported on the \( K \)-rational points \( W(y_K) \). Let \( J_X = \text{Jac}(X) \) be the Jacobian of \( X \) and \( H = \text{Hom}_Q(J_X, E) \) be the group of homomorphisms (defined over \( Q \)) from \( J_X \) to \( E \), then \( W \) acts on \( J_X \) and \( H \). We will see later that \( H \) is a free abelian group of rank 2.

**Proposition 4.14.** Let \( d \in D^0 \) and \( \phi \in H \). Then \( \phi(d) \in E^-(Q) \subseteq E(Q(i)) \).

**Proof.** For any \( d \in D^0 \), it follows from Proposition 4.12 that \( wd = \overline{d} \). Therefore
\[
\overline{\phi(d)} = \phi(\overline{d}) = \phi(\sigma d) = \phi^\sigma(d) = w(\phi)(d).
\]
By Proposition 4.10, this is equal to
\[
\prod_{p \mid D} \left( \frac{-1}{p} \right) \varepsilon_p(E/Q) \cdot \phi(d).
\]
4.3. Shimura curves and Heegner points

But $\varepsilon_2(E/\mathbb{Q}) = -1$ and $\prod_{p|D} \left(\frac{-1}{p}\right) = -1$ since $D \equiv 3 \pmod{4}$, we obtain that

$$\overline{\phi(d)} = -\varepsilon(E/\mathbb{Q}) \cdot \phi(d).$$

Hence $\overline{\phi(d)} = \phi(d)$ if and only if $\varepsilon(E/\mathbb{Q}) = -1$. In other words, the image lies in $E^-(\mathbb{Q})$.

The pairing between two free abelian groups

$$\langle \ , \rangle : H \times D^0 \to E(\mathbb{Q}(i)), \quad \langle \phi, d \rangle = \phi(d)$$

is bilinear and satisfies $\langle \phi^\sigma, d \rangle = \langle \phi, \sigma d \rangle$ for any $\sigma \in W$. Hence it induces a map

$$H \otimes_{\mathbb{Z}[W]} D_2^0 \to E(\mathbb{Q}(i)),$$

whose image lies in $E^-(\mathbb{Q})$ by Proposition 4.14.

We now use the extra automorphisms in $W_2$ to produce a canonical (up to sign) rational point in $E^-(\mathbb{Q})$. Let $D_2^0 \subseteq D^0$ be the subgroup of divisors supported on the set of three points $W_2(y_K)$.

**Theorem 4.15.** $H \otimes_{\mathbb{Z}[W_2]} D_2^0$ is a free abelian group of rank one. Hence the image of the homomorphism

$$H \otimes_{\mathbb{Z}[W_2]} D_2^0 \to E^-(\mathbb{Q})$$

has rank at most one.

**Proof.** Notice that $H$ is a free abelian group and by [YZZ13, 3.2.3], we have

$$H \otimes \mathbb{C} \cong \sigma^{R^\times},$$

as $W_2 \cong S_3$-representations. We know from Proposition 4.10 that $\sigma^{R^\times}$ is the irreducible 2-dimensional representation of $S_3$, thus $H$ is a free abelian group of rank 2. There are two
possibilities for the integral $S_3$-representation $H$: it is either the $A_2$-lattice

$$A_2 = \{a_1 e_1 + a_2 e_2 + a_3 e_3 : \sum a_i = 0\} \subseteq \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$$

or its dual

$$A_2^\vee = \text{Hom}(A_2, \mathbb{Z}) = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3 / \mathbb{Z}(e_1 + e_2 + e_3),$$

where $S_3$ permutes the basis vectors $\{e_1, e_2, e_3\}$ in the natural way. On the other hand, by Proposition 4.13, $W_2(y_K)$ consists of three points. Hence as a $W_2 \cong S_3$-representation, $D_0^2$ is isomorphic to the $A_2$-lattice.

If $H = A_2^\vee$, then the natural pairing between $A_2$ and $A_2^\vee$ induces an isomorphism

$$H \otimes_{\mathbb{Z}[W_2]} D_0^2 \cong A_2 \otimes_{\mathbb{Z}[S_3]} A_2^\vee \cong \mathbb{Z}.$$ 

It remains to check that the case $H = A_2$, i.e., it remains to show that

$$A_2 \otimes_{\mathbb{Z}[S_3]} A_2 \cong \mathbb{Z}.$$ 

Since $A_2$ is freely generated by the two vectors $u = e_1 - e_2$ and $v = e_2 - e_3$, it suffices to check that $u \otimes u$, $v \otimes v$, $u \otimes v$ and $v \otimes u$ in $A_2 \otimes_{\mathbb{Z}[S_3]} A_2$ generate a free abelian group of rank one. In fact, we have

$$u \otimes u = (e_1 - e_2) \otimes (e_1 - e_3 + e_3 - e_2) = \sigma_{12}(e_1 - e_2) \otimes \sigma_{12}(e_1 - e_3) - u \otimes v = -2u \otimes v,$$

$$v \otimes v = (e_2 - e_3) \otimes (e_2 - e_3) = \sigma_{13}(e_2 - e_3) \otimes \sigma_{13}(e_2 - e_3) = u \otimes u,$$

and

$$u \otimes v = (e_1 - e_2) \otimes (e_2 - e_3) = \sigma_{13}(e_1 - e_2) \otimes \sigma_{13}(e_2 - e_3) = v \otimes u,$$
where $\sigma_{ij} \in S_3$ denotes the transposition switching $e_i$ and $e_j$. It follows that

\[ v \otimes v = u \otimes u = -2u \otimes v, \quad v \otimes u = u \otimes v, \]

and thus $A_2 \otimes_{\mathbb{Z}[S_3]} A_2$ is freely generated on one element $u \otimes v$.

Let $P \in E^-(\mathbb{Q})$ be the image of the generator (up to sign) of $H \otimes_{\mathbb{Z}[W_2]} D_0^0$. In view of Conjecture 4.4, we propose the following conjecture.

**Conjecture 4.16.** If the class number $h_L$ is odd, then $P \in E^-(\mathbb{Q})$ has infinite order.

**Example 4.17.** Consider the case $D = 11$. The Shimura curve $X$ associated to the quaternion order of discriminant 44 has genus 2. Elkies computed that $X$ has equation $-y^2 = x^6 - 7x^4 + 59x^2 + 11$ and the three elliptic points in $W_2(y_K)$ are $\infty$, $(1, 8i)$ and $(-1, 8i)$. The Jacobian $J_X$ is $(2, 2)$-isogenous to $E \times \tilde{E}$, where

\[ E = 44a1 : y^2 = x^3 + 7x^2 + 59x - 11, \quad \tilde{E} = 44a2 : y^2 = x^3 - 59x^2 - 77x - 121, \]

and the map $J_X \to E \times \tilde{E}$ is induced from the two maps

\[ X \to E, \quad (x, y) \mapsto (-x^2, y), \quad X \to \tilde{E}, \quad (x, y) \mapsto \left( -\frac{11}{x^2}, \frac{11y}{x^3} \right). \]

The two elliptic curves $E, \tilde{E}$ are 3-isogenous to each other and we see that $\text{Hom}_{\mathbb{Q}}(J_X, E)$ is indeed of rank 2. The cubic field $L$ has discriminant $-44$ and class number $h_L = 1$. The root number $\varepsilon(E/\mathbb{Q}) = +1$. The quadratic twist of $E$ by $\mathbb{Q}(i)$ has equation

\[ E^- = 176c1 : y^2 = x^3 - 7x^2 + 59x + 11. \]

As predicted by Conjecture 4.4 and 4.16, $r_{\text{alg}}(E^-/\mathbb{Q}) = 1$ and the canonical point $P = (1, 8) \in E^-(\mathbb{Q})$ we constructed is indeed a point of infinite order.
Chapter 5

Reduction of Shimura curves at $p$
when $p^2 \mid \mid N$

5.1 Motivation

To study the 2-divisibility of the point $P \in E(\mathbb{Q}(i))$ constructed in Chapter 4, one can first study the 2-divisibility of a Heegner divisor $d \in D^0_2(y_K) \subseteq J_X(\mathbb{Q}(i))$ and then study its image under the projections $J_X \to E$.

One way of studying the 2-divisibility $d \in J_X(\mathbb{Q}(i))$ is to study its reduction mod 2. Let $J_X/\mathbb{Z}_2(i)$ be the Néron model of $J_X$. We denote by $\overline{d} \in J_X(\mathbb{F}_2)$ its reduction, then

$$\overline{d} \notin 2J_X(\mathbb{F}_2) \implies d \notin 2J_X(\mathbb{Q}(i)).$$

To study the reduction $\overline{d}$, we need to first understand the structure of the special fiber of the Néron model $J_X$. For example, if $J_X_{\mathbb{F}_2} = \mathbb{G}_m^n$ is a vector group of dimension $m$ and $\overline{d} \neq 0$, then $\overline{d} \notin 2J_X(\mathbb{F}_2)$ because multiplication by 2 on any vector group over $\mathbb{F}_2$ is the zero map.

More generally, for any prime $p$, to study the $p$-divisibility of Heegner points on certain
elliptic curves of conductor $N$ (when $p^2 || N$), we are led to study the mod $p$ reduction of Shimura curves $X$ defined as follows. Let $B$ be an indefinite rational quaternion algebra ramified at $p$. Let $\mathcal{O}_p$ be the maximal order of $B_p$ with uniformizer $\pi$. Motivated by Remark 4.9, we let

$$R_p = \{ x \in \mathcal{O}_p : x \mod \pi \mathcal{O}_p \in \mathbb{F}_p \subseteq \mathbb{F}_{p^2} = \mathcal{O}_p/\pi \mathcal{O}_p \} \subseteq \mathcal{O}_p$$

be the unique suborder of index $p$.

**Definition 5.1.** Fix an open compact subgroup $U^p \subseteq B^\times(\mathbb{A}_f^p)$ (the tame level). Let $X$ be the Shimura curve with level $U^p \cdot R_p^\times$,

$$X = B^\times(\mathbb{Q})/\mathcal{H}^\pm \times B^\times(\mathbb{A}_f)/U^p \cdot R_p^\times.$$ 

Let $Y$ be the Shimura curve with the same tame level but with the level at $p$ given by the maximal open compact subgroup $\mathcal{O}_p^\times \subseteq B_p^\times$,

$$Y = B^\times(\mathbb{Q})/\mathcal{H}^\pm \times B^\times(\mathbb{A}_f)/U^p \cdot \mathcal{O}_p^\times.$$ 

Notice that $X \to Y$ is finite cover of degree $[\mathcal{O}_p^\times : R_p^\times] = [\mathbb{F}_{p^2} : \mathbb{F}_p] = p + 1$.

**Remark 5.2.** We recover the Shimura curve $X$ of level $4D$ considered in Section 4.3 by taking $p = 2$ and $U^p = R^\times(\mathbb{A}_f^p)$, where $R$ is the order of reduced discriminant $4D$ defined in (4.1).

Our goal in this chapter is to compute the special fiber of the Néron model $J_X$ over $\mathbb{Z}_p$, at least when $U^p$ is small enough (see Remark 5.3). Since Néron models are compatible with étale base change, it suffices to compute the Néron model $J_X$ over $W = W(k)$, the Witt vectors over $k = \mathbb{F}_p$. Raynaud’s theorem, which we will recall in Section 5.2, allows one to compute the Néron model of the Jacobian of a curve from a regular semistable model of the curve over $W$. 

53
5.1. Motivation

The Néron model $\mathcal{J}_Y$ for the Shimura curve $Y$ with maximal level at $p$ has been computed by [JL86]. The Shimura curve $Y$ is $p$-adically uniformized by Drinfeld’s $p$-adic half-plane $\Omega$ and admits a regular semistable model $\mathcal{Y}$ over $W$. The special fiber $\mathcal{Y}_k$ consists of $\mathbb{P}^1$’s and its dual graph $G_Y$ is a quotient of the Bruhat–Tits tree of $\text{SL}_2(\mathbb{Q}_p)$. The Néron model $\mathcal{J}_Y$ has purely toric reduction (see Theorem 5.10). The situation is comparable to the classical modular curve $X_0(p)$.

The level of the Shimura curve $X$ at $p$ is deeper and one expects that the reduction of $X$ should be worse than $Y$. Indeed $X$ no longer admits a regular semistable model over $W$. Nevertheless $X$ is still $p$-adic uniformized by a tame étale covering $\Omega_1$ of Drinfeld’s $p$-adic half-plane $\Omega$. Using Teitelbaum’s theorem [Tei90] on the rigid geometry of $\Omega_1$, we obtain a regular semistable model $\mathcal{X}$, not over $W$ but over a tamely ramified extension of $W'/W$ of degree $p + 1$. The dual graph of the special fiber $\mathcal{X}_k$ is the same as that of $\mathcal{Y}_k$ but each irreducible component becomes the Drinfeld curve

$$y^p - y = x^{p+1}$$

of genus $\frac{p(p-1)}{2} \geq 1$, rather than $\mathbb{P}^1$. We then use Edixhoven’s theorem [Edi92] on the behavior of Néron models under tamely ramified extensions to recover the Néron model $\mathcal{J}_X$ over $W$. It turns out the toric part of $\mathcal{J}_X$ coincides with that of $\mathcal{J}_Y$ but $\mathcal{J}_X$ has an extra unipotent part, which is shown to be a vector group (see Theorem 5.16).

Remark 5.3. To avoid difficulties in resolving singularities, we will assume that the tame level $U^p$ is small enough so that the relevant discrete subgroups in $B^\times(\mathbb{Q})$ and $\text{GL}_2(\mathbb{Q}_p)$ are all torsion-free. Unfortunately this assumption is not satisfied for the Shimura curve of level $4D$ considered in Section 4.3. Nevertheless, one can always achieve this neatness assumption by shrinking the tame level, e.g., by intersecting it with the principal congruence subgroup $U(M)$ (consisting of units congruent 1 mod $M$) for any $M \geq 3$ ([BC91, III.1.5]). The net effect is to replace the Shimura curves $X, Y$ with non-neat level by the two finite covers

54
5.2. Néron models of Jacobians

$X' \to X$, $Y' \to Y$ with the same covering groups, so that the Shimura curves $X'$, $Y'$ are neat. This can be depicted as follows:

\[
\begin{array}{c}
X' \downarrow^{p+1} \quad Y' \\
\downarrow \quad \downarrow \\
X \quad Y
\end{array}
\]

5.2 Néron models of Jacobians

In this section we review the necessary background on Néron models of Jacobians (see also [Maz77, Appendix] for a nice summary). Our set-up is the following.

- Let $R$ be a henselian discrete valuation ring with algebraically closed residue field $k = \overline{\mathbb{F}_p}$.
- Let $K$ be the fraction field of $R$.
- Let $C/K$ be a smooth, proper, geometrically irreducible curve.
- Let $C/R$ be a regular model of $C/K$, i.e., $C$ is regular as a scheme, proper and flat over $R$, with generic fiber $C_K = C$.
- Let $J/K$ be the Jacobian of $C/K$.
- Let $J/R$ be the Néron model of $J/K$, i.e., the unique $R$-scheme which is smooth, separated, of finite type, with generic fiber $J_K = J$ and satisfies the Néron mapping property: for any smooth $R$-scheme $Y$, any $K$-morphism $Y_K \to J_K$ extends to a unique $R$-morphism $Y \to J$.
- Let $J^0$ be the identity component of the Néron model. Then its special fiber $J^0_k$ is a
smooth commutative connected algebraic group over \( k \), hence it is an extension

\[
0 \to T \times U \to J^0_k \to A \to 0
\]

of an abelian variety \( A \) by a product \( T \times U \), where \( T \) is a torus and \( U \) is a unipotent group (see [BLR90, 9.2.1, 9.2.2]).

- Let \( \Phi = J_k / J^0_k \) be the component group of (the special fiber of) the Néron model \( J \).

**Definition 5.4.** We say that \( C/R \) is **semistable** if the special fiber \( C_k \) is reduced and all its singular points are ordinary double points. If \( C/R \) is semistable, we denote by \( \mathcal{G} = \mathcal{G}(C_k) \) the **dual graph** of the special fiber \( C_k \), i.e., the vertices of \( \mathcal{G} \) are irreducible components of \( C_k \) and the edges are singular points of \( C_k \). Two vertices \( v_1, v_2 \) are connected by an edge \( e \) if and only if the two irreducible components corresponding to \( v_1, v_2 \) intersect at the singular point corresponding to \( e \).

We have the following theorem relating the Néron model \( J \) and a regular semistable model \( C \) of the curve \( C \).

**Theorem 5.5** (Raynaud). Let \( C/R \) be a regular semistable model of \( C/K \). Then

1. ([BLR90, 9.5.4]) We have an isomorphism \( \text{Pic}^0_{C/R} \cong J^0 \). Here \( \text{Pic}^0_{X/R} \) is the identity component of \( \text{Pic}_{C/R} \), classifying line bundles on \( C \) whose restriction to each irreducible component of \( C_k \) has degree 0.

2. ([BLR90, 9.2.8]) The special fiber \( J^0_k \) is a semi-abelian variety, i.e., the unipotent part \( U \) is trivial. Moreover, suppose \( C_k \) has \( n \) irreducible components \( C_i, i = 1, \ldots, n \) and let \( \tilde{C}_i \) be the normalization of \( C_i \). Then the abelian variety part \( A \) is given by

\[
A \cong \prod_{i=1}^{n} \text{Jac}(\tilde{C}_i).
\]

The dimension of the torus part \( T \) is equal to the rank of the abelian group \( H_1(\mathcal{G}, \mathbb{Z}) \).
5.3. The Cerednik–Drinfeld Theorem

(3) ([BLR90, 9.6.3]) Let \( M = (C_i \cdot C_j)_{i,j=1}^n \) be the intersection matrix of the special fiber \( C_k \).

If \( M \) has Smith normal form \( \text{diag}\{d_1, \ldots, d_{n-1}, 0\} \) (so \( d_i \mid d_{i+1} \)). Then the component group is given by

\[
\Phi \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_{n-1}\mathbb{Z}.
\]

5.3 The Cerednik–Drinfeld Theorem

Our goal in this section is to describe Cerednik–Drinfeld’s theorem on the \( p \)-adic uniformization of Shimura curves, following [BC91].

Let \( B \) be an indefinite rational quaternion algebra ramified at \( p \) and \( U \) be a compact open subgroup of \( B^\times(\mathbb{A}_f) \). The Shimura curve

\[
M_U = B^\times(\mathbb{Q})\backslash H^\pm \times B^\times(\mathbb{A}_f)/U
\]

associated to \( U \) has a canonical model over \( \mathbb{Q} \).

When \( U \) decomposes as a product \( U^p \cdot U^0_p \), where \( U^p \subseteq B^\times(\mathbb{A}_f^p) \) is small enough and \( U^0_p = \mathcal{O}_p^\times \) (i.e., the level at \( p \) is maximal), \( M \) has a flat and proper (but non-smooth) \( \mathbb{Z}_p \)-model \( \mathcal{M}_U \), representing a suitable moduli problem of abelian schemes of dimension 2 with endomorphisms by a maximal order \( \mathcal{O} \subseteq B \) ([BC91, III.3.2]). The flatness is ensured by imposing a certain special condition on the action of \( \mathbb{Z}_p^2 \subseteq \mathcal{O}_p \) on the Lie algebra of the abelian schemes in characteristic \( p \) ([BC91, III.3.7]). The properness follows from the semistable reduction theorem ([BC91, III.3.8]).

Let \( \Omega \) be Drinfeld’s \( p \)-adic half plane over \( \mathbb{Q}_p \). Denote the formal model of \( \Omega \) by \( \hat{\Omega} / \text{Spf} \mathbb{Z}_p \) ([BC91, I.3]). Its special fiber consists of \( \mathbb{P}^1 \)'s with the dual graph equal to the Bruhat–Tits tree \( T \) of \( \text{SL}_2(\mathbb{Q}_p) \). Let \( \overline{B} \) be the definite rational quaternion algebra obtained by switching the local invariants of \( B \) at \( p \) and \( \infty \). We fix isomorphisms

\[
\overline{B}^\times(\mathbb{A}_f^p) \cong B^\times(\mathbb{A}_f^p), \quad \overline{B}^\times(\mathbb{Q}_p) \cong \text{GL}_2(\mathbb{Q}_p).
\]
5.3. The Cerednik–Drinfeld Theorem

Let $W = W(k)$ be the Witt vectors over $k = \mathbb{F}_p$ and let $K = \text{Frac}(W)$.

Now we are ready to state the Cerednik–Drinfeld theorem for Shimura curves with the maximal level at $p$.

**Theorem 5.6** (Cerednik–Drinfeld, [BC91, III.5.3]). Let $\hat{\mathcal{M}}_U$ be the completion of $\mathcal{M}_U$ along its special fiber. For $U^p \subseteq B^x(A_p_f)$ small enough and $U = U^p \cdot U_0^p$, there is an isomorphism of formal schemes over $\text{Spf} \mathbb{Z}_p$,

$$\hat{\mathcal{M}}_U \cong \text{GL}_2(\mathbb{Q}_p) \backslash \left( \hat{\Omega} \times_{\text{Spf} \mathbb{Z}_p} \text{Spf} W \right) \times \mathbb{Z}_U,$$

where $\mathbb{Z}_U = U^p \setminus B^x(A_f)/B^x(\mathbb{Q})$ and $\text{GL}_2(\mathbb{Q}_p)$ acts on $W$ via $g \mapsto \text{Frob}_p^{-\text{val}(|\det(g)|)}$.

**Remark 5.7.** The quotient $\text{GL}_2(\mathbb{Q}_p) \backslash \mathbb{Z}_U$ is a finite set by strong approximation. Let $\{x_i\}$ be a set of representatives and let $\Gamma_i$ be the stabilizer of $x_i$ of the action of $\text{GL}_2(\mathbb{Q}_p)$ on $\mathbb{Z}_U$. Then $\Gamma_i$ is a discrete and cocompact subgroup of $\text{GL}_2(\mathbb{Q}_p)$ and $\hat{\mathcal{M}}_U$ is thus a disjoint union of the quotients $\Gamma_i \backslash \left( \hat{\Omega} \times \text{Spf} W \right)$. Since $U^p$ is assumed to be small enough, the action of $\Gamma_i$ on $\hat{\Omega}$ is free and therefore $\hat{\mathcal{M}}_U$ is a disjoint union of unramified twists of Mumford curves $\Gamma_i \backslash \hat{\Omega}$ ([BC91, III.5.4]).

There is a further generalization of Theorem 5.6 for non-maximal level at $p$. Recall that by Drinfeld’s theorem, $\hat{\Omega} \times \text{Spf} W$ is the moduli space of certain rigidified special formal $\mathcal{O}_p$-modules of dimension 2 and height 4 ([BC91, II.8.2]). There is a universal family of formal groups $X$ over the moduli space $\hat{\Omega} \times \text{Spf} W$. Let $\pi$ be a uniformizer of $\mathcal{O}_p$. Let $X[\pi^n]$ be the group of $\pi^n$ torsion points of $X$. It is representable by a formal group scheme, finite and locally free over $\hat{\Omega} \times \text{Spf} W$ of rank $p^{2n}$. Then the rigid analytic space $X_n$ associated to $X[\pi^n]$ is a finite étale covering of $\Omega \otimes \text{Spf} K$. Let $\Omega_n = X_n - X_{n-1}$ be the space “killed by $\pi^n$ exactly”. Then $\Omega_n$ is an étale Galois cover of $\Omega \otimes \text{Spf} K$ with Galois group $(\mathcal{O}_p/\pi^n \mathcal{O}_p)^\times$ ([BC91, II.13.2]). Now we can state the generalization of the Cerednik–Drinfeld theorem in the case when $U_p$ is not maximal.
Theorem 5.8 ([BC91, III.5.8]). For \( U = U_p \cdot U_p^m \), where \( U_p^m \) consists of units of \( \mathcal{O}_p \) that are congruent to 1 modulo the \( \pi^n \mathcal{O}_p \), there is an isomorphism of rigid analytic spaces

\[
M^\text{an}_U \cong \text{GL}_2(\mathbb{Q}_p) \backslash (\Omega_n \times Z_U).
\]

5.4 Néron models for Shimura curves with maximal level at \( p \)

Let \( W = W(k) \) be the Witt vectors over \( k = \overline{\mathbb{F}}_p \) and let \( K = \text{Frac}(W) \). By Remark 5.7, base extending to \( W \), the Shimura curve \( Y/K \) in Definition 5.4 has a regular semistable model \( \mathcal{Y}/W \) as a finite disjoint union of Mumford curves \( \Gamma \backslash \hat{\Omega} \).

Remark 5.9. To compute the Néron model \( \mathcal{J}_Y \) over \( W \), it suffices to compute the Néron model of the Jacobian of each component \( \Gamma \backslash \hat{\Omega} \). Without loss of generality, we replace \( Y \) by one of its components and assume \( Y = \Gamma \backslash \hat{\Omega} \), where \( \Gamma = \Gamma_i \) for some \( i \). This remark about irreducible components will also apply to the Shimura curve \( X \).

Theorem 5.10. Let \( \mathcal{J}_Y \) be the Néron model of \( J_Y \) over \( W \). Then \( \mathcal{J}_Y^0 \cong \textsf{T} \), where \( \textsf{T} \) is a torus. The dimension of \( \textsf{T} \) is equal to the rank of \( H_1(\Gamma \backslash \mathcal{T}, \mathbb{Z}) \), which is also equal to \( g(Y) \), the genus of \( Y \).

Proof. From the description of the special fiber of \( \hat{\Omega} \), we know that the special fiber \( \mathcal{Y}_k \) of the regular semistable model \( \mathcal{Y}/W \) of \( Y \) consists of \( \mathbb{P}^1 \)'s and the dual graph is equal to the quotient graph \( \Gamma \backslash \mathcal{T} \). The results then follow from Theorem 5.5 (2) and the fact that \( \dim \textsf{T} = \dim J_Y = g(Y) \).

5.5 The first Drinfeld cover

Teitelbaum [Tei90] discovered a rigid geometric description of \( \Omega_1 \): it is a Kummer covering over each affinoid \( U \) of \( \Omega \) corresponding to a vertex of \( \mathcal{T} \). Over \( W \), the Kummer covering is
defined by
\[ p(y^p - y)^{p-1} = x^{p^2-1}, \]
where \( y \) is a suitable local coordinate on \( U \). After adjoining a \((p+1)\)-st root of \( p \), one obtains a regular semistable model of \( \Omega_1 \): it consists of \( p-1 \) connected components and the special fiber of each component has dual graph \( \mathcal{T} \). Each vertex corresponds to a copy of the smooth projective curve (known as the Drinfeld curve)

\[ C : y^p - y = x^{p+1}. \]

An edge between two vertices corresponds to two copies of \( C \)'s intersecting at an \( \mathbb{F}_p \)-rational ordinary double point.

**Example 5.11.** For \( p = 2 \), the Shimura curve \( X \) admits a 2-adic uniformization \( X = \Gamma \backslash \Omega_1 \). The first Drinfeld cover \( \Omega_1 \) is abelian over \( \Omega \) with Galois group \( \mathbb{Z}/3\mathbb{Z} \). Over \( W(\sqrt[3]{2}) \), \( \Omega_1 \) is defined by the equation \( y^2 - y = x^3 \) over each affinoid \( U \). The special fiber of \( \Omega_1 \) thus has components isomorphic to the elliptic curve \( C : y^2 - y = x^3 \) of \( j \)-invariant 0.

In general, we have \( U_1^1 \subseteq R_1^\times \subseteq \mathcal{O}_p^\times = U_0^1 \), \( [R_1^\times : U_0^1] = p-1 \) and \( [\mathcal{O}_p^\times : R_0^\times] = p+1 \). We know that the Shimura curve \( X \) is \( p \)-adically uniformized by the unique degree \( p+1 \) subcovering of \( \Omega_1/\Omega \). Let \( W' = W(\varpi)/W \) be the tamely ramified extension of degree \( p+1 \) with \( \varpi^{p+1} = p \). Then by Teitelbaum’s theorem, the Shimura curve \( X \) admits a regular semistable model \( \mathcal{X}/W' \) whose special fiber consists of curves isomorphic to

\[ C : y^p - y = x^{p+1} \]

with the same dual graph \( \Gamma \backslash \mathcal{T} \) as that of \( \mathcal{Y}_k \).
5.6 Néron models for Shimura curves with non-maximal level at $p$

**Theorem 5.12.** Let $J'_X$ be the Néron model of $J_X$ over $W'$. Then $(J'_{X,k})^0$ is semi-abelian and fits into the exact sequence

$$0 \to T \to (J'_{X,k})^0 \to A \to 0. \quad (5.1)$$

1. The torus part $T$ is isomorphic to that of $J^0_{Y,k}$ (in Theorem 5.10), hence has dimension $g(Y)$.
2. The abelian variety part is given by

$$A \cong \text{Jac}(C)^n,$$

where $n$ is the number of irreducible components in $X_k$, which also equal to the number of irreducible components in $Y_k$.
3. The component group $\Phi'_{X}$ of $J'_{X}$ is isomorphic to the component group $\Phi_{Y}$ of $J_{Y}$.

**Proof.** The results follow from Theorem 5.5 (2-3) using the above description of a regular semistable model $X/W'$ and the fact that the dual graphs of $X_k$ and $Y_k$ are the same. \hfill $\square$

Denote $K = \text{Frac}(W)$, $K' = \text{Frac}(W')$ and $G = \text{Gal}(K'/K)$. Then the cyclic Galois group $G$ of order $p + 1$ acts on the generic fiber $J_{X,K'}$. It extends to an action on the Néron model $J'_X/W'$ by the Néron mapping property. Edixhoven’s theorem allows us to recover the special fiber of $J_X/W$ using the Néron model $J'_X/W'$ over a tamely ramified extension $W'/W$.

**Theorem 5.13** (Edixhoven, [Edi92, Theorem 4.2]). We have $J_X(k) = J'_X(W'/pW')^G$, where the symbol $(-)^G$ stands for taking $G$-invariants.
5.6. Néron models for Shimura curves with non-maximal level at $p$

To gain more information, we now describe a natural filtration on $\mathcal{J}_X'(W'/pW')$. Define

$$F^i := \ker(\mathcal{J}_X'(W'/pW') \to \mathcal{J}_X'(W'/\varpi^iW')).$$  

Then the $F^i$’s form a descending filtration

$$F^0 = \mathcal{J}_X'(W'/pW') \supseteq F^1 \supseteq F^2 \supseteq \cdots \supseteq F^{p+1} = 0.$$

We have $G$-equivariant isomorphisms (see [Edi92, 5.1])

$$F^0/F^1 \cong \mathcal{J}_X'(k), \quad F^i/F^{i+1} \cong \text{Lie } \mathcal{J}_{X,k} \otimes (\varpi W'/\varpi^2 W')^\otimes, \quad i \geq 1.$$

In particular, for $i \geq 1$, $F^i$ is a successive extension of vector groups, hence is unipotent.

**Lemma 5.14.** The group $F^2$ is a vector group.

**Proof.** Denote by $F$ the formal group over $W'$ associated to the semiabelian scheme $\mathcal{J}_X'$. Then $F^i = F(\varpi^iW'/pW')$ for $i \geq 1$. The multiplication by $p$ on $F$ is of the form

$$[p](T_1, \ldots, T_g) = (pf_1(T_1, \ldots, T_g) + h_1(T_1^p, \ldots, T_g^p), \ldots, p f_g(T_1, \ldots, T_g) + h_g(T_1^p, \ldots, T_g^p)),$$

where $g$ is the dimension of $F$ and $f_i, h_i \in W'[T_1, \ldots, T_g]$ are formal power series with no constant terms. Because $2p > p + 1$, we know that $h_i(T_1, \ldots, T_g) \in pW'$ if $T_i \in \varpi W'$. Hence $F^2 = F(\varpi^2 W'/pW')$ is indeed killed by $p$ and thus $F^2$ is a vector group. \hfill \square

**Lemma 5.15.** We have $(F^1)^G = (F^2)^G$. In particular, $(F^1)^G$ is a vector group.

**Proof.** By Teitelbaum’s description of the regular semistable model $\mathcal{X}/W'$ and Theorem 5.5 (1), we know that $G$ acts on the torus part $T$ trivially and the action of an element $\sigma \in G$...
5.6. Néron models for Shimura curves with non-maximal level at $p$

on the abelian variety part $A$ is induced by the following action on $C$,

$$x \mapsto \chi(\sigma)x, \quad y \mapsto y,$$

where $\chi(\sigma) = \sigma(\varpi)/\varpi$ is a $(p+1)$-st root of unity.

Since the order of the group $G$ is coprime to $p$ and $F^i$ is unipotent for $i \geq 1$, taking $G$-invariants gives an exact sequence

$$0 \to (F^{i+1})^G \to (F^i)^G \to (\text{Lie} J'_{X,k} \otimes (\varpi W'/\varpi^2 W')^\otimes)^G \to 0.$$

Notice that the action of $G \varpi W'/\varpi^2 W'$ is given by $\chi^{-1}$ ([Edi92, 5.2]), so we know that

$$(F^1)^G/(F^2)^G = \text{Lie} J'_{X,k}[\chi],$$

the $\chi$-isotypic component of $\text{Lie} J'_{X,k}$ as a $G$-representation. The exact sequence (5.1) gives an exact sequence of $G$-representations

$$0 \to \text{Lie} T \to \text{Lie} J'_{X,k} \to \text{Lie} A \to 0.$$

Notice that $G$ acts on $\text{Lie} T$ trivially and acts on $\text{Lie} A = \oplus^n \text{Lie Jac}(C)$ via the induced action from $C$. Because $\text{Lie Jac}(C)$ is dual to $H^0(C, \Omega^1_C)$, we can describe the $G$-action on $\text{Lie Jac}(C)$ by looking at the $G$-action on a basis of regular differentials on $C$. In fact, \{x^i y^j dx : 0 \leq i, j \leq p - 2\} is such a basis and the action of $G$ on $x^i y^j dx$ is given by $\chi^{i+1}$. Therefore as a $G$-representation,

$$H^0(C, \Omega^1_C) \cong \bigoplus_{i=1}^{p-1} (\chi^i)^{\otimes i}.$$
Taking the dual we obtain that
\[
\text{Lie} \text{Jac}(C) \cong \bigoplus_{i=2}^{p}(\chi^i)^{\otimes p+1-i}.
\]
It follows that \(\text{Lie} \mathcal{J}'_{X,k}[\chi] = 0\) and thus \((F^1)^G = (F^2)^G\). In particular, \((F^1)^G\) is a vector group by Lemma 5.14.

Now we are ready to prove our main theorem on the Néron model \(\mathcal{J}_X/W\) of \(J_X\).

**Theorem 5.16.** We have
\[
\mathcal{J}^0_{X,k} \cong U \times T.
\]

(1) The torus part \(T\) is isomorphic to that of \(\mathcal{J}^0_{Y,k}\) (in Theorem 5.10), hence has dimension \(g(Y)\).

(2) The unipotent part \(U\) is a vector group. It has dimension \(g(X) - g(Y)\), which is also equal to \(np(p-1)/2\), where \(n\) is the number of irreducible components of \(\mathcal{X}_k\) (or \(\mathcal{Y}_k\)).

(3) The component group \(\Phi_X\) sits inside an exact sequence
\[
0 \to (\mathbb{Z}/(p+1)\mathbb{Z})^{n(p-1)} \to \Phi_X \to \Phi_Y \to 0.
\]

**Proof.** By Edixhoven’s theorem 5.13, we have \(\mathcal{J}_X(k) \cong (F^0)^G\). Taking the \(G\)-invariants of the exact sequence
\[
0 \to F^1 \to F^0 \to \mathcal{J}'_{X,k} \to 0
\]
gives the exact sequence
\[
0 \to (F^1)^G \to \mathcal{J}_{X,k} \to (\mathcal{J}'_{X,k})^G \to 0,
\]
since the order of the group \(G\) is coprime to \(p\) and \(F^1\) is unipotent. By Lemma 5.15, \((F^1)^G\)
is a vector group. By Theorem 5.12, we have exact sequences

\[ 0 \to (J'_{X,k})^0 \to J'_{X,k} \to \Phi_Y \to 0, \]

and

\[ 0 \to T \to (J'_{X,k})^0 \to \text{Jac}(C)^n \to 0. \]

Since \( G \) acts on \( T \) and \( \Phi_Y \) trivially and \( \text{Jac}(C)^G \cong (\mathbb{Z}/(p+1)\mathbb{Z})^{p-1} \) (by Theorem 5.18 below) is a finite group, we know that the identity component of \( (J'_{X,k})^G \) is isomorphic to \( T \).

It follows that the component group of \( (J'_{X,k})^G \) (and hence the component group of \( J_{X,k} \)) is an extension of \( \Phi_Y \) by \( (\text{Jac}(C)^G)^n \cong (\mathbb{Z}/(p+1)\mathbb{Z})^{n(p-1)} \). It also follows that \( J_{X,k} \) has no abelian variety part. Its torus part is given by \( T \) of dimension \( g(Y) \), and its unipotent part is the vector group \( (F^1)^G \), which has dimension \( \dim J_X - \dim T = g(X) - g(Y) \). By Theorem 5.12, \( \dim J_X - \dim T \) is also equal to \( \dim \text{Jac}(C)^n \), which is \( n \cdot g(C) = np(p-1)/2 \).

All the claims then follow. \( \square \)

**Example 5.17.** In Figure 5.1, we illustrate Theorem 5.10 and 5.16 for the case \( p = 2 \). The dual graph \( \Gamma \setminus \mathcal{T} \) of \( \mathcal{Y}_k \) consist of two vertices and three edges. So \( g(Y) = 2 \).

The special fiber \( \mathcal{Y}_{\mathbb{F}_2} \) consists of two \( \mathbb{P}^1 \)'s intersecting at the three \( \mathbb{F}_2 \)-rational points. The special fiber \( X_{\mathbb{F}_2} \) consists of two elliptic curves \( y^2 - y = x^3 \) of \( j \)-invariant 0 intersecting at the three \( \mathbb{F}_2 \)-rational points. By Theorem 5.10 and 5.16, we have

\[ J^0_{\mathcal{Y},\mathbb{F}_2} \cong \mathbb{G}_m^2, \quad J^0_{X,\mathbb{F}_2} \cong \mathbb{G}_m^2 \times \mathbb{G}_a^2. \]

In particular, we have \( g(X) = 4 \). By Riemann–Hurwitz, the degree 3 covering map \( X \to Y \)
is unramified. The intersection matrix of $\mathcal{Y}_{\mathbb{F}_2}$ is given by

$$M = \begin{pmatrix} -3 & 3 \\ 3 & -3 \end{pmatrix},$$

which has Smith normal form $\text{diag}\{3, 0\}$. Hence by Theorem 5.5 (3), the component group $\Phi_Y \cong \mathbb{Z}/3\mathbb{Z}$. The component group $\Phi_X$ sits in an exact sequence

$$0 \rightarrow (\mathbb{Z}/3\mathbb{Z})^2 \rightarrow \Phi_X \rightarrow \mathbb{Z}/3\mathbb{Z} \rightarrow 0.$$

Hence $\Phi_X$ is either $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $(\mathbb{Z}/3\mathbb{Z})^3$.

### 5.7 Component groups

In this section we determine the finite group $\text{Jac}(C)^G$, which appeared in the proof of Theorem 5.16.

**Theorem 5.18.** $\text{Jac}(C)^G \cong (\mathbb{Z}/(p+1)\mathbb{Z})^{p-1}$. 
5.7. Component groups

Proof. The curve \( C : y^p - y = x^{p+1} \) is a degree \( p + 1 \) cover of \( \mathbb{P}^1 \), branched exactly at the rational points \( \mathbb{P}^1(\mathbb{F}_p) \). Moreover, the covering map is totally ramified at these branched points. Let \( P_0 = \infty \) and \( P_i = (0, y_i) \) (\( i = 1, \ldots, p, y_i \in \mathbb{F}_p \)) be the preimages of \( \mathbb{P}^1(\mathbb{F}_p) \).

By Riemann–Roch, for any degree zero divisor \( D \) on \( C \), there exists a unique effective divisor \( E \) of minimal degree \( 0 \leq m \leq g \) such that \( D \) is linearly equivalent to \( E - mP_0 \) ([GPS02, Theorem 1]). If the divisor class \( [D] \) is \( G \)-invariant, then by minimality, \( E \) must be a linear combination of the fixed points \( P_i \). Therefore \( \text{Jac}(C)^G \) is generated by the classes \( [D_i] = [P_i - P_0] \) (\( i = 1, \ldots, p \)).

Notice that \( (p+1)[D_i] = 0 \) since it is the divisor of the function \( y - y_i \). Also notice that \( \sum_{i=1}^{p}[D_i] = 0 \) since it is the divisor of the function \( x \). In particular, for any \( i \),

\[
[P_1 + \cdots + P_{i-1} - pP_i + P_{i+1} + \cdots P_p + \infty] = \sum_{j=1}^{p}[D_j] - (p+1)[D_i] = 0.
\]

Therefore any degree zero divisor \( D \) supported on \( \{P_0, \ldots, P_p\} \) is linearly equivalent to a degree zero divisor \( D_0 \) supported on \( \{P_1, \ldots, P_p\} \). We claim that \( D \) is principal if and only if for any \( i = 1, \ldots, p \), the coefficient of \( P_i \) in \( D_0 \) is divided by \( p + 1 \). It follows from the claim that

\[
\text{Jac}(C)^G \cong \left\{ (a_1, \ldots, a_p) : a_i \in \mathbb{Z}/(p+1)\mathbb{Z}, \sum_{i=1}^{p} a_i = 0 \right\} \cong (\mathbb{Z}/(p+1)\mathbb{Z})^{p-1}.
\]

It remains to show the claim. The “only if” direction is obvious: \( D_0 = \sum a_iP_i \) is the divisor of the rational function \( \prod(y - y_i)^{a_i/(p+1)} \). For the “if” direction, we notice that \( D_0 \) is \( G \)-invariant and the function field \( k(C) \) admits a \( G \)-invariant decomposition

\[
k(C) = \bigoplus_{i=0}^{p} x^i \cdot k(y),
\]

hence \( D_0 \) is the divisor of \( x^ag(y) \) for some \( 0 \leq a \leq p \) and a rational function \( g(y) \). Write
5.7. Component groups

\[ g(y) = \prod_{i=1}^{p} (y - y_i)^{b_i}, \] then the coefficient of \( P_0 \) in \( D_0 \) is

\[ 0 = a + (p + 1) \sum_{i=1}^{p} b_i. \]

It follows that \((p + 1) | a\), which is only possible when \( a = 0 \). Thus

\[ D_0 = (p + 1) \sum_{i=1}^{p} b_i P_i, \]

as desired.

\[ \square \]

**Remark 5.19.** Let \( C \) be a smooth projective model of the affine curve defined by \( x^n = f(y) \) over an algebraically closed field \( k \) with \( \text{char}(k) \nmid n \). The cyclic group \( G = \mathbb{Z}/n\mathbb{Z} \) acts on \( C \) by \((x, y) \mapsto (\zeta_n x, y)\). The same proof shows that \( \text{Jac}(C)^G \cong (\mathbb{Z}/n\mathbb{Z})^{\deg f - 1} \) whenever \((n, \deg f) = 1 \) and \( f \) has no repeated roots over \( k \) (cf. [Zar05, 4.7]).
Chapter 6

Level raising mod 2 and obstruction for rank lowering

In this Chapter we study 2-Selmer groups using the method of level raising mod 2 (Step B of the strategy explained in the introduction).

Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N$. Let $\overline{\rho} = \overline{\rho}_{E,2} : G_{\mathbb{Q}} \to \text{Aut}(E[2]) \cong \text{GL}_2(\mathbb{F}_2)$ be the Galois representation on the 2-torsion points. By the modularity theorem, $\overline{\rho}$ comes from a weight 2 cusp newform of level $N$. We make the following mild assumptions.

**Assumption 6.1.**

1. $E$ has good or multiplicative reduction at 2 (i.e., $4 \nmid N$).
2. $\overline{\rho}$ is surjective.
3. The Serre conductor $N(\overline{\rho})$ is equal to the odd part of $N$. If $2 \mid N$, $\overline{\rho}$ is ramified at 2.
4. If $2 \nmid N$, $\overline{\rho}|_{G_{\mathbb{Q}_2}}$ is nontrivial.

**Remark 6.2.** The assumption (2) that $\overline{\rho}$ is surjective implies that the 2-torsion field $\mathbb{Q}(E[2])$ is a $\text{GL}_2(\mathbb{F}_2) \cong S_3$-extension over $\mathbb{Q}$. We change notation in this chapter and use $L$ to
denote the 2-torsion field \( \mathbb{Q}(E[2]) \), which is the Galois closure of the cubic field \( \mathbb{Q}[x]/F(x) \) that appeared in previous chapters. Then \( \text{Gal}(L/\mathbb{Q}) \cong S_3 \) acts on \( E[2] \) via the unique 2-dimensional irreducible representation. The unique quadratic subextension of \( L \) is \( \mathbb{Q}(\sqrt{\Delta}) \) (see [Ser72, p. 305]).

**Remark 6.3.** All the level-raised forms will be automatically new at \( p \mid N \) due to assumption (3). This assumption is also equivalent to saying that the component group of the Néron model of \( E \) at any \( p \mid N \) has odd order (see [GP12, Lemma 4]).

**Remark 6.4.** Notice that \( \bar{\rho}|_{G_{\mathbb{Q}^2}} \) is trivial if and only if 2 splits in \( L \), if and only if \( E \) is ordinary at 2 and 2 splits in the quadratic subfield \( \mathbb{Q}(\sqrt{\Delta}) \subseteq L \). The assumption (4) is only needed for Lemma 6.20 (4) (see Remark 6.28).

### 6.1 Level raising mod 2

Under the above assumptions, \( E[2] \) (as a \( G_{\mathbb{Q}} \)-module) together with the knowledge of reduction type at a prime \( q \) pins down the local condition defining \( \text{Sel}_2(E/K) \) at \( q \) (see Lemma 6.20 for more precise statements). We would like to keep \( E[2] \), but at a prime \( q \nmid 2N \) of choice, switch good reduction to multiplicative reduction and thus change the local condition at \( q \). For this to happen, a necessary condition is that \( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} q^* & \ast \\ 0 & 1 \end{pmatrix} \pmod{2} \) (up to conjugation). Namely, \( \bar{\rho}(\text{Frob}_q) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) or \( \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) (order 1 or 2 in \( S_3 \)).

**Definition 6.5.** We call \( q \nmid 2N \) a **level raising prime** for \( E \) if \( \text{Frob}_q \) is of order 1 or 2 acting on \( E[2] \). Notice that there are lots of level raising primes: by the Chebotarev density theorem, they make up 2/3 of all primes. If we write \( f = \sum_{n \geq 1} a_n q^n \in S_2(N) \) (normalized so that \( a_1 = 1 \)) to be the newform associated to the elliptic curve \( E \). Then by definition \( q \nmid 2N \) is a level raising prime for \( E \) if and only if \( a_q \) is even.

Ribet’s level raising theorem [Rib90, Theorem 1] ensures that this necessary condition is also sufficient.
Theorem 6.6. Let $E/\mathbb{Q}$ be an elliptic curve satisfying (1-3) of Assumption 6.1. Let $q$ be a level raising prime. Then $\bar{\rho}$ comes from a weight 2 newform of level $Nq$.

So whenever $q$ is a level raising prime, there exists a newform $g = \sum_{n \geq 1} b_n q^n \in S_2(Nq)$ of level $Nq$ such that

$$g \equiv f \pmod{2}.$$ 

More precisely, there exists a prime $\lambda | 2$ of the (totally real) Hecke field $\mathcal{F} = \mathbb{Q}(\{b_n\}_{n \geq 1})$ such that we have a congruence $b_p \equiv a_p \pmod{\lambda}$, for any $p \neq q$.

This level raised newform $g$, via the Eichler–Shimura construction, determines an abelian variety $A$ over $\mathbb{Q}$ up to isogeny, of dimension $[\mathcal{F} : \mathbb{Q}]$, with real multiplication by $\mathcal{F}$. We will choose an $A$ in this isogeny class so that $A$ admits an action by the maximal order $\mathcal{O}_\mathcal{F}$. By Assumption 6.1 (2), $A$ is unique up to a prime-to-$\lambda$ isogeny.

Let $k = \mathcal{O}_\mathcal{F}/\lambda$ be the residue field. By construction, for almost all primes $p$, $\text{Frob}_p$ has the same characteristic polynomials on the 2-dimensional $k$-vector spaces $E[2] \otimes k$ and $A[\lambda]$. Hence by Chebotarev’s density theorem and the Brauer-Nesbitt theorem we have

$$E[2] \otimes k \cong A[\lambda]$$

as $G_{\mathbb{Q}}$-representations.

Definition 6.7. We say that $A$ is obtained from $E$ via level raising at $q$ and that $A$ and $E$ are congruent mod 2.

Example 6.8. Consider $E = 11a1 = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$. It satisfies Assumption 6.1. Since $a_7 = -2$ is even, we know that $q = 7$ is a level raising prime (so are $q = 13, 17, 19$). The space of newforms of level 77 has dimension 5, which corresponds to three isogeny classes of elliptic curves (77a, 77b, 77c) and one isogeny class of abelian surfaces (77d). Among them (77a, 77b) are congruent to $E$ mod 2: i.e., obtained from $E$ via level raising at 7. Their first few Hecke eigenvalues are listed in Table 6.1.
6.2 Selmer groups and sign changing

Suppose $A$ is obtained from $E$ via level raising at a level raising prime $q$. Fix an isomorphism between $A[λ] \cong E[2] \otimes k$ and denote them by $V$. In this section we first introduce a more general notion of Selmer groups cut out by arbitrary local conditions. We then deduce a parity prediction on the 2-Selmer rank of $E/K$ and $λ$-Selmer rank of $E/K$ for certain imaginary quadratic fields $K$.

**Definition 6.9.** Let $K$ be a number field. Let $v$ be a place of $K$. We define

$$H^1_{ur}(K_v, V) := H^1(K_v^{ur}/K_v, V^I) \subseteq H^1(K_v, V)$$

consisting of classes which are split over an unramified extension of $K_v$.

**Definition 6.10.** Let $L = \{L_v\}$ be the collection of $k$-subspaces $L_v \subseteq H^1(K_v, V)$, where $v$ runs over every place of $K$. We say $L$ is a collection of local conditions if $L_v = H^1_{ur}(K_v, V)$ for almost all $v$. We define the Selmer group cut out by the local conditions $L$ to be

$$H^1_L(V) := \{ x \in H^1(K, V) : \text{res}_v(x) \in L_v, \text{for all } v \}.$$

**Definition 6.11.** We define $L_v(E)$ to be the image of the local Kummer map

$$(E(K_v)/2E(K_v)) \otimes_{F_2} k \to H^1(K_v, E[2]) \otimes k = H^1(K_v, V).$$

### Table 6.1: Level raising at 7

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>11a</td>
<td>−2</td>
<td>−1</td>
<td>1</td>
<td>−2</td>
<td>1</td>
<td>4</td>
<td>−2</td>
<td>0</td>
</tr>
<tr>
<td>77a</td>
<td>0</td>
<td>−3</td>
<td>−1</td>
<td>−1</td>
<td>−4</td>
<td>2</td>
<td>−6</td>
<td></td>
</tr>
<tr>
<td>77b</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>−1</td>
<td>−4</td>
<td>−6</td>
<td>2</td>
</tr>
</tbody>
</table>

72
Then the Selmer group cut out by the local conditions \( \mathcal{L}(E) := \{ \mathcal{L}_v(E) \} \) is

\[
H^1_{\mathcal{L}(E)}(V) = \text{Sel}_2(E/K) \otimes k.
\]

**Definition 6.12.** Similarly, we define \( \mathcal{L}_v(A) \) to be the image of the local Kummer map

\[
A(K_v) \otimes_{O_F} k \to H^1(K_v, A[\lambda]) = H^1(K_v, V).
\]

The \( \lambda \)-Selmer group of \( A \) is defined to be the Selmer group cut out by \( \mathcal{L}(A) := \{ \mathcal{L}_v(A) \} \), denoted by \( \text{Sel}_\lambda(A/K) \). For details on descent with endomorphisms, see the appendix of [GP12].

Now let \( K \) be an imaginary quadratic field satisfying the *Heegner hypothesis*: if \( p | N \) then \( p \) is split in \( K \). By Chebotarev’s density theorem, half of the level raising primes \( q \) are *inert* in \( K \). From now on we assume the following assumption.

**Assumption 6.13.**

1. \( K \) is an imaginary quadratic field satisfying the Heegner hypothesis for \( E/\mathbb{Q} \).
2. \( q \) is a level raising prime for \( E/\mathbb{Q} \), which is inert in \( K \).

**Proposition 6.14.** Assume Assumption 6.1 and 6.13. Then the newform \( f \) of level \( N \) and newform \( g \) of level \( Nq \) have opposite signs of the functional equations over \( K \),

\[
\varepsilon(f/K) = -1, \quad \varepsilon(g/K) = +1.
\]

**Proof.** For any finite place \( v \) of \( K \) not dividing the level \( N \), \( \varepsilon_v(f/K) = +1 \). For \( p | N \), \( p \) splits as \( p_1p_2 \) in \( K \) and \( \varepsilon_{p_1}(f/K) = \varepsilon_{p_2}(f/K) \), so \( \varepsilon_{p_1}(f/K) \cdot \varepsilon_{p_2}(f/K) = +1 \). It follows that

\[
\varepsilon(f/K) = \varepsilon_\infty(f/K) = -1.
\]
Since \( q \) is inert in \( K \), we have \( \varepsilon_q(g/K) = -1 \) and the same reasoning shows that \[ \varepsilon(g/K) = -\varepsilon_{\infty}(g/K) = +1, \] as desired.

By Proposition 6.14, the BSD conjecture predicts that rank \( E(K) \) and rank \( F \) \( A(K) \) have different parity. Moreover, \( \dim_{\mathbb{F}_2} \text{III}(E/K)[2] \) and \( \dim_k \text{III}(A/K)[\lambda] \) should be even. So the BSD conjecture predicts the following

**Conjecture 6.15.** Assume 6.1 and 6.13. Then

\[ s_2(E/K) := \dim_{\mathbb{F}_2} \text{Sel}_2(E/K), \quad s_2(A/K) := \dim_k \text{Sel}_\lambda(A/K) \]

have different parity.

Our next goal is to prove this parity conjecture (Theorem 6.27).

**Remark 6.16.** Over \( \mathbb{Q} \), the signs \( \varepsilon(f/Q) \) and \( \varepsilon(g/Q) \) are not necessarily opposite. For example, consider \( E = 11a_1 \) in Example 6.8. Both \( A_1 = 77a \) and \( A_2 = 77b \) are obtained from \( E \) via level raising at 7 and

\[ \varepsilon(E/Q) = +1, \quad \varepsilon(A_1/Q) = -1, \quad \varepsilon(A_2/Q) = +1. \]

Therefore level raising mod 2 does not necessarily change the signs of the functional equations over \( \mathbb{Q} \) and thus there is no parity prediction. For more refined control over the possible signs under level raising mod 2, see [LL15].

**Remark 6.17.** Notice that \( \dim_k \text{III}(A/Q)[\lambda] \) is not necessarily even when \( \dim A > 1 \): the Cassels–Tate pairing is always skew-symmetric but may fail to be alternating. So even when \( \varepsilon(g/Q) = -\varepsilon(f/Q) \), there is no parity prediction for 2-Selmer groups over \( \mathbb{Q} \). This is again a phenomenon unique to \( p = 2 \). When \( A \) has an odd degree polarization, Poonen–Stoll [PS99]
constructed an element $c \in \Sha(A/Q)[2]$ with Cassels-Tate pairing $(c, c) = 0$ or $1/2 \in \mathbb{Q}/\mathbb{Z}$, so that $(c, c)$ on $\Sha(A/Q)[2]$ is alternating if and only if $(c, c) = 0$. Notice that a quadratic base change $K/Q$ kills the later obstruction and so the parity prediction is available over $K$ (see, e.g., [Ces14, 3.6]).

6.3 Local conditions

In this section we discuss the local conditions defining the Selmer groups of $E$ and $A$.

Definition 6.18. The Weil pairing $E[2] \times E[2] \to \mu_2$ induces a perfect pairing $V \times V \to k(1)$. We identify $V \cong V^* = \text{Hom}(V, k(1))$ using this pairing. For each place $v$ of $K$, we define the cup product pairing

$$(c, c)_v : H^1(K_v, V) \times H^1(K_v, V) \to H^2(K_v, k(1)) \cong k.$$ 

This is a perfect pairing by local Tate duality. We denote the annihilator of $L_v$ by

$$L^\perp_v := \{x \in H^1(K_v, V) : (x, y)_v = 0, \text{ for all } y \in L_v\}.$$ 

Then $\dim_k L_v + \dim L^\perp_v = \dim H^1(K_v, V)$ by the non-degeneracy of $(c, c)_v$. By the local Tate duality for the elliptic curve $E$, $L_v(E)$ is equal to its own annihilator $L_v(E)^\perp$ and hence

$$\dim L_v(E) = \frac{1}{2} \dim H^1(K_v, V).$$ 

Lemma 6.19. Suppose $v \nmid 2N\infty$ is a place of a number field $K$. Then

$$\dim H^1(K_v, V) = 2 \dim H^1_{\text{ur}}(K_v, V) = 0, 2, 4,$$

if $\text{Frob}_v \in G_{K_v}$ is of order 3, 2, 1 acting on $V$ respectively.

Proof. The map $c \mapsto c(\text{Frob}_v)$ induces an isomorphism $H^1_{\text{ur}}(K_v, V) \cong V^I/(\text{Frob}_v - 1)V^I$, which has dimension $0, 1, 2$ if $\text{Frob}_v$ has order 3, 2, 1 respectively. It follows from [Mil86,
6.3. Local conditions

I.2.6] that the annihilator of $H^1_{\text{ur}}(K_v, V)$ under the local Tate pairing is equal to itself, hence $\dim H^1(K_v, V) = 2 \dim H^1_{\text{ur}}(K_v, V).$ 

Under Assumption 6.1 and 6.13, the following lemma identifies the local conditions of the abelian variety $A$ purely in terms of the Galois representation $V$, which is the key to controlling the Selmer rank under level raising.

**Lemma 6.20.** Suppose $A$ is obtained from $E$ via level raising at $q$ (we allow $A = E$ and view $q = 1$ in this case). Let $L = L(A)$ be the local conditions defining $\text{Sel}_\lambda(A/K)$. Then

1. For $v \nmid 2q\infty$, 
   $$L_v = H^1_{\text{ur}}(K_v, V).$$

2. For $v = \infty$, 
   $$L_v = H^1(K_v, V) = 0.$$

3. For $v = q$, if $\text{Frob}_q \in G_{Q_q}$ has order 2 acting on $V$, then $H^1(K_v, V)$ is 4-dimensional and 
   $$L_v = \text{im}(H^1(K_v, W) \to H^1(K_v, V))$$
   is 2-dimensional. Here $W$ is the unique $G_{Q_q}$-stable line in $V$. Moreover, 
   $$L_v \cap H^1_{\text{ur}}(K_v, V) = H^1_{\text{ur}}(K_v, W)$$
   is 1-dimensional.

4. If $E$ is good at $v|2$, then 
   $$L_v = H^1_{\text{fl}}(\text{Spec} \, O_v, E[2]) \otimes k,$$
   where $E/O_v$ is the Néron model of $E/K_v$ and $H^1_{\text{fl}}(\text{Spec} \, O_v, E[2])$ is the flat cohomology group, viewed as a subspace of $H^1_{\text{fl}}(\text{Spec} \, K_v, E[2]) = H^1(K_v, E[2]).$
(5) If \( E \) is multiplicative at \( v|2 \), then

\[
L_v = \text{im}(H^1(\mathbb{Q}_2, W) \to H^1(\mathbb{Q}_2, V)).
\]

Here \( W \) is the unique \( G_{\mathbb{Q}_2} \)-stable line in \( V \).

Proof. (1) It follows from [GP12, Lemma 6] and Remark 6.3.

(2) It is clear since \( K \) is imaginary.

(3) Our argument closely follows the proof of [GP12, Lemma 8]. Let \( A/\mathbb{Z}_q \) be the Néron model of \( A/\mathbb{Q}_q \). Let \( A^0/\mathbb{F}_q \) be the identity component of the special fiber of \( A \). Since \( A \) is an isogeny factor of the new quotient of \( J_0(Nq_1 \cdots q_m) \), it has purely toric reduction at \( q \): \( A^0/\mathbb{F}_q \) is a torus that is split over \( \mathbb{F}_{q^2} \) and it is split over \( \mathbb{F}_q \) if and only if \( \varepsilon = +1 \). By the Néron mapping property, \( \mathcal{O}_F \) acts on \( A^0 \) and makes the character group \( X^*(A^0/\mathbb{F}_q) \otimes \mathbb{Q} \) a 1-dimensional \( F \)-vector space.

Let \( T/\mathbb{Q}_q \) be the split torus with character group \( X^*(A^0/\mathbb{F}_q) \). Let \( \chi : \text{Gal}(K_q/\mathbb{Q}_q) \to \{ \pm 1 \} \) be the trivial or nontrivial quadratic character according to whether \( A^0/\mathbb{F}_p \) splits over \( \mathbb{F}_q \) or not. Let \( T(\chi)/\mathbb{Q}_q \) be the twist of \( T/\mathbb{Q}_q \) by \( \chi \). Then \( \mathcal{O}_F \) naturally acts on \( T \) (dual to the action on the character group). By the theory of \( q \)-adic uniformization, we have a \( G_{\mathbb{Q}_q} \)-equivariant exact sequence

\[
0 \to \Lambda(\chi) \to T(\chi)(\overline{\mathbb{Q}_q}) \to A(\overline{\mathbb{Q}_q}) \to 0,
\]

where \( \Lambda \) is a free \( \mathbb{Z} \)-module with \( G_{\mathbb{Q}_q} \)-action by \( \chi \). Since \( \mathcal{O}_F \) is a maximal order, \( \Lambda \) is a locally free \( \mathcal{O}_F \)-module of rank one. Consider the following commutative diagram

\[
\begin{array}{ccc}
T(\chi)(K_q) \otimes \mathcal{O}_F/\lambda & \longrightarrow & H^1(K_q, T(\chi)[\lambda]) \\
\downarrow & & \downarrow \\
A(K_q) \otimes \mathcal{O}_F/\lambda & \longrightarrow & H^1(K_q, A[\lambda]).
\end{array}
\]
6.3. Local conditions

Here the horizontal arrows are the local Kummer maps and the vertical maps are induced by the \(q\)-adic uniformization. The left vertical map is surjective since its cokernel lies in \(H^1(K_q, \Lambda) = \text{Hom}(G_{K_q}, \Lambda)\), which is zero as \(\Lambda\) is torsion-free. The top horizontal map is also surjective since its cokernel maps into \(H^1(K_q, T(\chi))\), which is zero by Hilbert 90 as \(T(\chi)\) is a split torus over \(K_q\). It follows that

\[
\mathcal{L}_q = \text{im} \left( H^1(K_q, T(\chi)[\lambda]) \to H^1(K_q, A[\lambda]) \right).
\]

Also, because \(\Lambda(\chi)\) has no \(\lambda\)-torsion, we see that \(T(\chi)[\lambda] \to A[\lambda]\) is a \(G_{Q_q}\)-equivariant injection. But since \(\text{Frob}_q \in G_{Q_q}\) is assumed to have order 2 acting on \(V = A[\lambda]\), \(V\) has a unique \(G_{Q_q}\)-stable line \(W\). Therefore

\[
\mathcal{L}_q = \text{im}(H^1(K_q, W) \to H^1(K_q, V)).
\]

Since \(q\) is inert in \(K\), we know that \(\text{Frob}_q \in G_{K_q}\) acts on \(V\) trivially. It follows from Lemma 6.19 that \(H^1(K_q, V)\) is 4-dimensional and \(H^1_{ur}(K_q, V)\) is 2-dimensional. The intersection \(\mathcal{L}_v \cap H^1_{ur}(K_q, W)\) consists of unramified homomorphisms \(\text{Gal}(K_q^{ur}/K_q) \to W\), hence is 1-dimensional.

(4) Let \(E/\mathbb{Q}_2\) be the Néron model of \(E/\mathbb{Q}\) and \(A/\mathbb{Z}_2\) be the Néron model of \(A/\mathbb{Q}_2\). We claim that \(E[2] \otimes k = A[\lambda]\) over \(\mathbb{Z}_2\) (extending the isomorphism \(E[2] \otimes k = A[\lambda]\)). The argument in [GP12] no long applies since the absolute ramification index \(e = 1 = p - 1\) in this case and the general fiber does not determine the finite flat model uniquely.

This can be salvaged when \(E\) is supersingular at 2. Let \(W\) be the strict henselization of \(\mathbb{Z}_2\). Let \(F\) be the fraction field of \(W\) and \(I\) be the absolute Galois group of \(F\) (i.e., the inertia subgroup at 2). Notice that \(E[2]\) is an irreducible \(F_2[I]\)-module ([Ser72, p.275, Prop.12], see also [Con97, Theorem 1.1]), hence [Ray74, 3.3.2.3^3] is applicable and it follows that \(E[2]\) has a unique finite flat model over \(W\). Since the descent datum from \(W\) down to
6.3. Local conditions

$\mathbb{Z}_2$ is determined by that of the generic fiber, $E[2]$ has a *unique* finite flat model over $\mathbb{Z}_2$ as well. Now $E[2] \otimes k$ is a direct sum of $[k : \mathbb{F}_2]$ copies of $E[2]$, by the standard 5-lemma argument ([Tat97, Prop 4.2.1]), we know that $E[2] \otimes k$ also has a unique finite flat model over $\mathbb{Z}_2$. We conclude that this unique finite flat model of $E[2] \otimes k$ must be isomorphic to $E[2] \otimes k = A[\lambda]$.

Now consider the case that $E$ is ordinary at 2. Then $E[2]$ is an extension of $\mathbb{Z}/2\mathbb{Z}$ by $\mu_2$ over $\mathbb{Z}_2$. Notice that $b_2 \equiv a_2 \not\equiv 0 \pmod{\lambda}$ by construction, so we know that $E[2] \otimes k = A[\lambda]$ is also ordinary, i.e., an extension of $\mathbb{Z}/2\mathbb{Z} \otimes k$ by $\mu_2 \otimes k$ over $\mathbb{Z}_2$. To show that $E[2] \otimes k = A[\lambda]$ has a unique finite flat model over $\mathbb{Z}_2$ that is an extension of $\mathbb{Z}/2\mathbb{Z} \otimes k$ by $\mu_2 \otimes k$. This is true because of Assumption 6.1 (4) that $G_{\mathbb{Q}_2}$ acts non-trivially on $E[2]$. In fact, the generic fiber map

$$\text{Ext}_{\mathbb{Z}_2}(\mathbb{Z}/2\mathbb{Z}, \mu_2) \to \text{Ext}_{\mathbb{Q}_2}(\mathbb{Z}/2\mathbb{Z}, \mu_2)$$

between the extension groups in the category of fppf sheaves of $\mathbb{Z}/2\mathbb{Z}$-modules can be identified with the natural map

$$H^1_{\text{fppf}}(\mathbb{Z}_2, \mu_2) \cong \mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \to H^1_{\text{fppf}}(\mathbb{Q}_2, \mu_2) \cong \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2.$$

This map is injective. As a direct sum of $[k : \mathbb{F}_2]^2$ copies of this map, it follows that

$$\text{Ext}_{\mathbb{Z}_2}(\mathbb{Z}/2\mathbb{Z} \otimes k, \mu_2 \otimes k) \to \text{Ext}_{\mathbb{Q}_2}(\mathbb{Z}/2\mathbb{Z} \otimes k, \mu_2 \otimes k)$$

is also injective, which means that the extension class of such a finite flat model $\mathcal{V}$ of $E[2] \otimes k$ is determined by the extension class of the generic fiber of $\mathcal{V}$. But $G_{\mathbb{Q}_2}$ acts non-trivially on $E[2]$, there is a unique $\mathbb{F}_2$-subspace of dimension $[k : \mathbb{F}_2]$ in $E[2] \otimes k$ with trivial $G_{\mathbb{Q}_2}$-action, so the extension class of the generic fiber of $\mathcal{V}$ is uniquely determined by $E[2] \otimes k$, as desired.

In both cases, we have $E[2] \otimes k = A[\lambda]$. Now base changing to $\mathcal{O}_e$ and applying [GP12,
Lemma 7], we know that

\[ \mathcal{L}_v = H^1_{\text{dR}}(\mathcal{O}_v, A[\lambda]) = H^1_{\text{dR}}(\mathcal{O}_v, \mathcal{E}[2]) \otimes k. \]

(5) By Assumption 6.13, \( v \) splits in \( K \) and thus \( K_v \cong \mathbb{Q}_2 \). By Assumption 6.1 (3), there exists a unique \( G_{\mathbb{Q}_2} \)-stable line \( W \) in \( V \). If \( A \) has split toric reduction at 2, the claim follows from the same argument as in (3) using the 2-adic uniformization of \( A/\mathbb{Q}_2 \). Now let us assume that \( A \) has non-split toric reduction. Since \( G_{\mathbb{Q}_2} \) acts on \( V \) nontrivially and the image of \( \bar{\rho}|_{\mathbb{Q}_2} \) has order 2, one easily sees that \( \dim H^1(\mathbb{Q}_2, V) = 4 \) by the Euler characteristic formula and

\[ \dim \text{im}(H^1(\mathbb{Q}_2, W) \to H^1(\mathbb{Q}_2, V)) = 2 \]

by the long exact sequence in Galois cohomology associated to the short exact sequence

\[ 0 \to W \to V \to W/V \to 0. \]

Since \( \mathcal{L}_2 \) is a maximal isotropic subspace of \( H^1(\mathbb{Q}_2, V) \) by local Tate duality for \( A \), we know that \( \dim \mathcal{L}_2 = 2 \), half of the dimension of \( H^1(\mathbb{Q}_2, V) \). To prove the claim, it suffices to show that \( \mathcal{L}_2 \) contains \( \text{im}(H^1(\mathbb{Q}_2, W) \to H^1(\mathbb{Q}_2, V)) \).

Let \( T \) be the split torus over \( \mathbb{Q}_2 \) with character group \( X^*(A^0/\mathbb{F}_2) \). Let \( \chi \) be the unramified quadratic character \( \chi : \text{Gal}(\mathbb{Q}_4/\mathbb{Q}_2) \to \{ \pm 1 \} \) and \( T(\chi) \) be the \( \chi \)-twist of \( T \). We have a \( G_{\mathbb{Q}_2} \)-equivariant exact sequence

\[ 0 \to \Lambda(\chi) \to T(\chi)(\overline{\mathbb{Q}_2}) \to A(\overline{\mathbb{Q}_2}) \to 0, \]

where \( \Lambda \) is a locally free \( \mathcal{O}_{\mathbb{F}} \)-module of rank one with trivial \( G_{\mathbb{Q}_2} \)-action. As in (3), consider
the following commutative diagram

\[
\begin{array}{ccc}
T(\chi)(Q_2) \otimes O_F/\lambda & \longrightarrow & H^1(Q_2, T(\chi)[\lambda]) \\
\downarrow & & \downarrow \\
A(Q_2) \otimes O_F/\lambda & \longrightarrow & H^1(Q_2, A[\lambda]).
\end{array}
\]

Since the image of the right vertical arrow is \( \text{im}(H^1(Q_2, W) \rightarrow H^1(Q_2, V)) \), we are done if the left vertical arrow is surjective, or equivalently,

\[
\ker (H^1(Q_2, \Lambda(\chi)) \rightarrow H^1(Q_2, T(\chi))) \otimes O_F/\lambda \tag{6.1}
\]

is zero. Since \( H^1(Q_4, \Lambda(\chi)) = 0 \) (\( \Lambda \) is torsion-free) and \( H^1(Q_4, T(\chi)) = 0 \) by Hilbert 90 \((T(\chi) \text{ splits over } Q_4)\), by inflation-restriction we know that

\[
H^1(Q_2, \Lambda(\chi)) = H^1(Q_4/Q_2, \Lambda(\chi)) = \Lambda/2\Lambda,
\]

and

\[
H^1(Q_2, T(\chi)) = H^1(Q_4/Q_2, T(\chi)(Q_4)) = T(Q_2)/N(T(Q_4)),
\]

where \( N : T(Q_4) \rightarrow T(Q_2) \) is the norm map. The domain and target in (6.1) are finite \( O_{F,\lambda} \)-modules of the same size because \( \Lambda \) is a locally free \( O_F \)-module of rank one. Hence it suffices to show that

\[
H^1(Q_2, \Lambda(\alpha)) \rightarrow H^1(Q_2, T(\chi))
\]

is surjective, which can be checked after tensoring with \( O_F/\lambda \), i.e.,

\[
\Lambda/\lambda \Lambda \rightarrow T(Q_2)/N(T(Q_4)) \otimes O_F/\lambda
\]

is surjective. Since these are 1-dimensional \( k \)-vector spaces, it suffices to show this last map is nonzero. We claim that for any \( a \in \Lambda - \lambda \Lambda \), we have \( a \notin N(T(Q_4)) \). This is true because
of Assumption 6.1 (3) that \( \bar{\rho} \) is ramified at 2. In fact, since \( A[\lambda] = \lambda^{-1}\Lambda/\Lambda \), we know
that \( \lambda^{-1}(a) \) generates a ramified extension of \( \mathbb{Q}_2 \). On the other hand, for any \( b \in T(\mathbb{Q}_4) \),
\( \lambda^{-1}(\mathcal{N}(b)) = \lambda'(\sqrt{\mathcal{N}(b)}) \), where \( \lambda' \) is an integral ideal of \( \mathcal{O} \) such that \( \lambda \lambda' = (2) \). Since
\( \mathbb{Q}_2(\sqrt{\mathcal{N}(b)})/\mathbb{Q}_2 \) is unramified, we know that \( \lambda^{-1}(\mathcal{N}(b)) \) generates an unramified extension of \( \mathbb{Q}_2 \). Therefore \( a \) is not of the form \( \mathcal{N}(b) \), as desired. \( \square \)

6.4 Parity of 2-Selmer ranks

Since we are working in characteristic 2, to prove the Parity Conjecture 6.15, we not only
need the local Tate pairing

\[ (\ ,\ )_v : H^1(K_v, V) \times H^1(K_v, V) \to k(1), \]

but also a quadratic form \( Q_v \) giving rise to it. To define \( Q_v \), first recall that the line bundle
\( \mathcal{L} = \mathcal{O}_E(2\infty) \) on \( E \) induces a degree 2 map

\[ E \to \mathbb{P}^1 = \mathbb{P}(H^0(E, \mathcal{L})). \]

For \( P \in E \), let \( \tau_P \) be the translation by \( P \) on \( E \). Since for \( P \in E[2] \), \( \tau_P^*\mathcal{L} \cong \mathcal{L} \), the
translation by \( E[2] \) induces an action of \( E[2] \) on \( \mathbb{P}^1 \), i.e., a homomorphism \( E[2] \to \text{PGL}_2 \).
The short exact sequence

\[ 0 \to \mathbb{G}_m \to \text{GL}_2 \to \text{PGL}_2 \to 0 \]

induces the connecting homomorphism in nonabelian Galois cohomology

\[ H^1(K, \text{PGL}_2) \to H^2(K, \mathbb{G}_m). \]
Definition 6.21. We define $Q$ to be the composition

$$Q : H^1(K, E[2]) \rightarrow H^1(K, \text{PGL}_2) \rightarrow H^2(K, \mathbb{G}_m).$$

For a place $v$ of $K$, we denote its restriction by

$$Q_v : H^1(K_v, E[2]) \rightarrow H^1(K_v, \text{PGL}_2) \rightarrow H^2(K_v, \mathbb{G}_m).$$

By local class field theory, $H^2(K_v, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}$ and so $Q_v$ takes value in $H^2(K_v, \mathbb{G}_m)[2] \cong \mathbb{Z}/2\mathbb{Z}$. By [O’N02, §4], $Q_v$ is a quadratic form and extending scalars we obtain a quadratic form

$$Q_v : H^1(K_v, V) \rightarrow k,$$

whose associated bilinear form $(x, y) \mapsto Q_v(x + y) - Q_v(x) - Q_v(y)$ is equal to $\langle , \rangle_v$ by [O’N02, 4.3].

Definition 6.22. We say a subspace $W \subseteq H^1(Q_v, V)$ is totally isotropic for $Q_v$ if $Q_v|_W = 0$. We say $W$ is maximal totally isotropic if it is totally isotropic and $W = W^\perp$.

Remark 6.23. As char($k$) = 2, the requirement $Q_v|_W = 0$ is stronger than $\langle , \rangle_v|_W = 0$. For example, for the 2-dimensional quadratic space $(k^2, Q)$ with $Q((x, y)) = xy$, the associated bilinear form is given by

$$\langle (x_1, y_1), (x_2, y_2) \rangle = x_1y_2 + x_2y_1.$$

In particular $\langle (x, y), (x, y) \rangle = 2xy = 0$ and hence all three lines in $k^2$ are maximal totally isotropic for the bilinear form $\langle , \rangle$. But only the two lines $x = 0$ and $y = 0$ are maximal totally isotropic for the quadratic form $Q$.

Remark 6.24. The local condition $L_v(E)$ is maximal totally isotropic for $Q_v$ by [PR12, Prop. 4.11] (this is also implicit in [O’N02, Prop. 2.3]).
Lemma 6.25. Suppose $\text{Frob}_q \in G_{\mathbb{Q}_q}$ has order 2 acting on $V$. Then for any place $v$ of $K$, $\mathcal{L}_v(A)$ is maximal totally isotropic for $Q_v$.

**Proof.** The claim for $v \neq q$ follows immediately from Lemma 6.20 and Remark 6.24. It remains to check the case $v = q$. We provide an explicit way to compute the image of a cocycle $c \in H^1(K_q, E[2])$ under $Q_q$. Recall that $H^1(K_q, \text{PGL}_2)$ classifies forms of $\mathbb{P}^1$, i.e., algebraic varieties $S/K_q$ which become isomorphic to $\mathbb{P}^1$ over $\overline{K_q}$. For any cocycle $c$, the corresponding form $S$ can be described as follows. As a set, $S = \mathbb{P}^1(K_q)$. The Galois action of $g \in G_{K_q}$ on $x \in S$ is given by $g.x = c(g).g(x)$. The cocycle $c$ gives the trivial class in $H^1(K_q, \text{PGL}_2)$ if and only if $S(K_q) \neq \emptyset$.

Since $\text{Frob}_q \in G_{\mathbb{Q}_q}$ has order 2 acting on $V$, we know that $E[2](\mathbb{Q}_q) \cong \mathbb{Z}/2\mathbb{Z}$. Let $P \in E[2](\mathbb{Q}_q)$ be its generator. Let $\sigma \in G_{K_q}$ be a Frobenius and let $\tau$ be a generator of the tame quotient $\text{Gal}(K_q^t/K_q^ur)$. Then by Lemma 6.20 (3), $\mathcal{L}_q(A)$ is generated by the two cocycles

$$c(\sigma) = 0, \quad c(\tau) = P$$

and

$$c'(\sigma) = P, \quad c'(\tau) = 0.$$  

For the cocycle $c$, the corresponding form $S$ has a $K_q$-rational point if and only if there exists $x \in \mathbb{P}^1(K_q^t)$ such that

$$\sigma(x) = x, \quad P.\tau(x) = x.$$  

Suppose $E$ has a Weierstrass equation $y^2 = F(x)$, where $F(x) \in \mathbb{Q}(x)$ is an irreducible cubic polynomial. Let $\alpha_1, \alpha_2, \alpha_3$ be the three roots of $F(x)$. We fix a embedding $\mathbb{K} \hookrightarrow \overline{K_q}$ and view $\alpha_i$ as elements in $\overline{K_q}$. Without loss of generality, we may assume that $\alpha_1 \in K_q$ and thus $P = (\alpha_1, 0)$. Then the action of $P$ on $\mathbb{P}^1$ is an involution that swaps $\alpha_1 \leftrightarrow \infty$, $\alpha_2 \leftrightarrow \alpha_3$. One can compute explicitly that this involution is given by the linear fractional
transformation

\[ x \mapsto \frac{\alpha_1 x + (\alpha_2 \alpha_3 - \alpha_1 \alpha_2 - \alpha_1 \alpha_3)}{x - \alpha_1}. \]

Therefore \( Q_q(c) = 0 \) if and only if there exists \( x \in \mathbb{P}^1(K_q^t) \) such that

\[ \sigma(x) = x, \quad (\tau(x) - \alpha_1)(x - \alpha_1) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3). \] (6.2)

The right hand side is the image of \( \alpha_1 - \alpha_2 \) under the norm map \( K_q^\times \to \mathbb{Q}_q^\times \), hence has even valuation. Taking \( x = \alpha_1 + \sqrt{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)} \in K_q \) we see that \( Q_q(c) = 0 \). Similarly, \( Q_q(c') = 0 \) if and only if there exists \( x \in \mathbb{P}^1(K_q^{ur}) \) such that

\[ (\sigma(x) - \alpha_1)(x - \alpha_1) = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3). \]

Taking \( x = \alpha_2 \in K_q \) we see that \( Q_q(c') = 0 \). Hence \( \mathcal{L}_q(A) \) is maximal totally isotropic for \( Q_v \).

Remark 6.26. The local condition \( \mathcal{L}_q(A) \) may fail to be maximal totally isotropic for \( Q_q \) when working over \( \mathbb{Q} \) instead of over \( K \). This is expected since there is no parity prediction over \( \mathbb{Q} \) (Remark 6.16).

Now we are ready to prove the Parity Conjecture 6.15 on the 2-Selmer ranks.

**Theorem 6.27.** Assume Assumption 6.1 and 6.13. Suppose \( \text{Frob}_q \in G_{Q_q} \) has order 2 acting on \( V \). Then

\[ s_2(E/K) = s_2(A/K) \pm 1. \]

Moreover,

\[ s_2(E/K) = s_2(A/K) - 1 \]

if and only if \( \text{res}_q(\text{Sel}_2(E/K) \otimes k) \subseteq H^1_{ur}(K_q, W) \), where \( W \) is the unique \( G_{Q_q} \)-stable line in \( V \).
6.4. Parity of 2-Selmer ranks

Proof. Define the strict local conditions $S$ by $S_v = \mathcal{L}_v(E) = \mathcal{L}_v(A)$ for $v \neq q$ and

$$S_q = \mathcal{L}_v(E) \cap \mathcal{L}_v(A) = H^1_{ur}(K_q, W)$$

(by Lemma 6.20). Similarly, define the relaxed local conditions $R$ by $R_v = \mathcal{L}_v(E) = \mathcal{L}_v(A)$ for $v \neq w$ and $R_q = S_q^\perp$. Then we have

$$H^1_S(V) \subseteq H^1_L(E)(V) \subseteq H^1_R(V), \quad H^1_S(V) \subseteq H^1_L(A)(V) \subseteq H^1_R(V).$$

Since $S^\perp = R$, we use [DDT97, Theorem 2.18] to compare the dual Selmer groups:

$$\#H^1_S(V) = \prod_v \#S_v \#H^0(K_v, V), \quad \#H^1_R(V) = \prod_v \#R_v \#H^0(K_v, V).$$

It follows that

$$\dim H^1_K(V) - \dim H^1_S(V) = \frac{1}{2}(\dim R_q - \dim S_q) = 1,$$

since $S_q$ is 1-dimensional and $R_q$ is 3-dimensional. By global class field theory, for any class $c \in H^1_R(V)$, we have

$$\sum_v Q_v(\text{res}_v(c)) = 0.$$

Since $R_q$ is totally isotropic for $Q_v$ for any $v \neq q$ by Lemma 6.25, we know that that $Q_q(\text{res}_q(c)) = 0$. In other words, the image $\text{res}_q(H^1_K(V))$ is a totally isotropic subspace for $Q_q$. On the other hand, since $R_q/S_q$ is a 2-dimensional quadratic space obtained by extending scalars from a 2-dimensional quadratic space over $\mathbb{F}_2$ and $R_q/S_q$ contains an isotropic line with respect to $Q_v$, we know that it has Arf invariant 0 and is isomorphic to $(k^2, xy)$ as a quadratic space. By Remark 6.23 we know that there are exactly two maximal totally isotropic subspaces of $R_q$ containing $S_q$, which must be $\mathcal{L}_q(E)$ and $\mathcal{L}_q(A)$. It follows that either $H^1_R(V) = H^1_L(E)(V)$ or $H^1_R(V) = H^1_L(A)(V)$. The two cases cannot
hold simultaneously since
\[ H^1_{V}(A)(V) \cap H^1_{E}(V) = H^1_{S}(V) \subsetneq H^1_{R}(V). \]

So either
\[ H^1_{V}(A)(V) = H^1_{R}(V), \quad H^1_{E}(V) = H^1_{S}(V), \]
or
\[ H^1_{E}(V) = H^1_{R}(V), \quad H^1_{V}(A)(V) = H^1_{S}(V). \]

Moreover, the first case happens if and only if \( \text{res}_q(H^1_{E}(V)) \subseteq S_q \). The desired result then follows.

\[ \square \]

Remark 6.28. The conclusion of Theorem 6.27 may fail when Assumption 6.1 (4) is not satisfied due to the uncertainty of the local condition at 2. For example, the elliptic curve

\[ E = 2351a1 : y^2 + xy + y = x^3 - 5x - 5 \]

has trivial \( \bar{\rho}_{|G_{22}} \). The elliptic curve

\[ A = 25861i1 : y^2 + xy + y = x^3 + x^2 - 17x + 30 \]

is obtained from \( E \) via level raising at \( q = 11 \). For \( K = \mathbb{Q}(\sqrt{-111}) \),

\[ r_{\text{alg}}(E/K) = s_2(E/K) = 1 \quad \text{and} \quad r_{\text{alg}}(A/K) = s_2(A/K) = 4 \]
differ by 3 (rather than 1).
6.5 Obstruction for rank lowering

It follows from Theorem 6.27 that if $s_2(E/K) = 1$, then $s_2(A/K) = 0$ or 2. However, the Chebotarev density argument for $p \geq 5$ in [Zha14] fails in this case and does not show that one can always get $s_2(A/K) = 0$. In fact, we prove the following very surprising obstruction for rank lowering: $s_2(A/K)$ can never be lowered to zero!

**Theorem 6.29.** Assume Assumption 6.1 and 6.13. Suppose $\text{Frob}_q \in G_{Q_q}$ has order 2 acting on $V$. Then

$$s_2(E/K) = 1 \implies s_2(A/K) = 2.$$ 

**Proof.** By Theorem 6.27, we need to show that $\text{res}_q(\text{Sel}_2(E/K) \otimes k) \subseteq H^1_{\text{ur}}(K_q, W)$, where $W$ is the unique $G_{Q_q}$-stable line in $V$. Notice that the action of $\text{Gal}(K/\mathbb{Q})$ on $E[2]$ induces an action on $\text{Sel}_2(E/K)$. By assumption, we have $\text{Sel}_2(E/K) \cong \mathbb{Z}/2\mathbb{Z}$. So the action of $\text{Gal}(K/\mathbb{Q})$ on $\text{Sel}_2(E/K)$ must be trivial. It follows that

$$\text{res}_q(\text{Sel}_2(E/K) \otimes k) \subseteq H^1_{\text{ur}}(K_q, V)^{\text{Gal}(K_q/\mathbb{Q}_q)} = \text{Hom}(\text{Gal}(K_q^{\text{ur}}/K_q), V)^{\text{Gal}(K_q/\mathbb{Q}_q)}$$

$$= \text{Hom}(\text{Gal}(K_q^{\text{ur}}/K_q), W) = H^1_{\text{ur}}(K_q, W),$$

as desired. □

We end with an example illustrating Theorem 6.29.

**Example 6.30.** Consider $E = X_0(11)$. In Table 6.2 we list the first few level raising primes $q$ and corresponding level raising abelian varieties $A$ ($\dim A = 1$). For each choice of $K = \mathbb{Q}(\sqrt{d_K})$, we find that $s_2(A/K) = 2$ always.

In most cases, this is explained by the fact that $r_{\text{alg}}(A/K) = 2$. In the remaining cases, there is a jump coming from the 2-part of $\text{III}$ for the base change $A/K$,

$$\dim \text{III}(A/K)[2] = 2,$$
though in all such cases the 2-part of \( \Sha \) for \( A \) and its quadratic twist \( A^K \) are both trivial,

\[
\Sha(A/\mathbb{Q})[2] = 0, \quad \Sha(A^K/\mathbb{Q})[2] = 0.
\]

This is a phenomenon unique to \( p = 2 \) because for odd \( p \) it is always true that

\[
\Sha(A/K)[p] = \Sha(A/\mathbb{Q})[p] \oplus \Sha(A^K/\mathbb{Q})[p].
\]

<table>
<thead>
<tr>
<th>( q )</th>
<th>( A )</th>
<th>( d_K )</th>
<th>( r_{\text{alg}}(A/K) )</th>
<th>( \dim \Sha(A/K)[2] )</th>
<th>( s_2(A/K) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>77a</td>
<td>-8</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>77b</td>
<td>-8</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>143a</td>
<td>-7</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>13</td>
<td>143a</td>
<td>-8</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>187a</td>
<td>-7</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>187a</td>
<td>-24</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>209a</td>
<td>-7</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>209a</td>
<td>-19</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>29</td>
<td>319a</td>
<td>-8</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>29</td>
<td>319a</td>
<td>-19</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 6.2: Obstruction for rank lowering
Bibliography


B. V. Le Hung and C. Li, Level raising mod 2 and arbitrary 2-Selmer ranks, ArXiv e-prints (January 2015), 1501.01344.


