Specialization of Heegner points
and applications

Santiago Molina
Matemàtica aplicada IV
Universitat Politècnica de Catalunya

May 10, 2012
Contents

Introduction 5

1 Shimura curves and Heegner points 13
   1.1 Quaternion algebras and oriented Eichler orders . . . . . . . . . . . . . . . . . . 13
   1.2 Optimal embeddings . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 16
   1.3 Shimura curves and their moduli interpretation . . . . . . . . . . . . . . . . . . 19
   1.4 Heegner points . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 22

2 Ribet’s bimodules and reduction of Shimura curves 27
   2.1 Bimodules: Ribet’s work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 27
       2.1.1 Admissible bimodules . . . . . . . . . . . . . . . . . . . . . . . . . . . . 27
       2.1.2 $p$-divisible groups and Dieudonné modules . . . . . . . . . . . . . . . 30
       2.1.3 Supersingular surfaces and bimodules . . . . . . . . . . . . . . . . . . . 31
   2.2 Čerednik-Drinfeld’s special fiber . . . . . . . . . . . . . . . . . . . . . . . . . . 34
   2.3 Deligne-Rapoport-Buzzard special fiber . . . . . . . . . . . . . . . . . . . . . . . 36
       2.3.1 Supersingular points on smooth fibers . . . . . . . . . . . . . . . . . . . 36
       2.3.2 Deligne-Rapoport-Buzzard special fiber . . . . . . . . . . . . . . . . . . 36
   2.4 Specialization of points in a Shimura curve . . . . . . . . . . . . . . . . . . . . 37

3 Specialization of Heegner points 39
   3.1 Supersingular specialization of Heegner points . . . . . . . . . . . . . . . . . . . 39
       3.1.1 Computable description of the map $\phi_P$ . . . . . . . . . . . . . . . . 40
       3.1.2 The action of $\text{Pic}(R)$ . . . . . . . . . . . . . . . . . . . . . . . . 42
       3.1.3 Atkin-Lehner involutions . . . . . . . . . . . . . . . . . . . . . . . . . . 45
   3.2 Generalized bimodules . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 46
   3.3 Čerednik-Drinfeld’s special fiber . . . . . . . . . . . . . . . . . . . . . . . . . . 48
       3.3.1 Heegner points and the singular locus . . . . . . . . . . . . . . . . . . . 49
       3.3.2 Heegner points and the smooth locus . . . . . . . . . . . . . . . . . . . 50
   3.4 Supersingular vs. ordinary good reduction . . . . . . . . . . . . . . . . . . . . . 52
   3.5 Deligne-Rapoport-Buzzard special fiber . . . . . . . . . . . . . . . . . . . . . . . 54
       3.5.1 Heegner points and the smooth locus . . . . . . . . . . . . . . . . . . . 54
       3.5.2 Heegner points and the singular locus . . . . . . . . . . . . . . . . . . . 55
   3.6 Numerical example . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 55
## Contents

4 Equations of hyperelliptic Shimura curves 57  
4.1 Semi-stable hyperelliptic curves ........................................... 57  
4.2 Hyperelliptic Shimura curves ................................................. 60  
4.3 Algorithm to compute equations .............................................. 64  
4.4 Case $D = 3 \cdot 13$ .............................................................. 66  
4.5 Case $D = 5 \cdot 11$ ............................................................... 71  
4.6 Atkin-Lehner quotients ......................................................... 72  
4.6.1 Quotient of the special fiber ............................................... 72  
4.6.2 Weierstrass points, leading coefficients and fields of definition ... 73  
4.6.3 Example ................................................................. 74  
4.6.4 Results ................................................................. 76  

5 Further applications 77  
5.1 Equidistribution ................................................................. 77  
5.1.1 Gross formulas and special values of $L$-functions ...................... 78  
5.1.2 Subconvexity problem and equidistribution ............................. 79  
5.2 Group of automorphisms of a Shimura curve ............................. 82  
5.3 Groups of connected components and BSD ................................ 84  
5.3.1 Group of connected components ......................................... 84  
5.3.2 Specialization of Heegner points on the group of connected components 88  
5.3.3 Heegner points and special values of $L$-functions ..................... 90  
5.3.4 The conjecture of Birch and Swinnerton-Dyer for analytic rank 0 .... 92  

Appendix: Moduli interpretations of Shimura curves 97
Introduction

Let $\mathbb{Q}$ denote the field of rational numbers and fix throughout an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

Let $B$ be a quaternion algebra over $\mathbb{Q}$ and let $D \geq 1$ denote its reduced discriminant. Let $N \geq 1$ be a positive integer, coprime to $D$, and let $\text{Pic}(D, N)$ denote the set of isomorphism classes of oriented Eichler orders of level $N$ in $B$ (cf. §1.1 for precise definitions). If $B$ is indefinite, i.e., $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})$, then $D$ is the (square-free) product of an even number of primes and $\text{Pic}(D, N)$ is trivial for any $N$; otherwise, we say $B$ is definite and $\text{Pic}(D, N)$ is a finite set whose cardinality $h(D, N)$ is often referred to as the class number of any fixed oriented Eichler order $\mathcal{O}$ of level $N$.

If $B$ is indefinite, let $X_0((D, N))/\mathbb{Q}$ denote Shimura’s canonical model [66] of the coarse moduli space of abelian surfaces with multiplication by an Eichler order $\mathcal{O}$ of level $N$ in $B$. It follows from the work of various mathematicians, including Deligne and Rapoport, Buzzard, Morita, Čerednik and Drinfeld, that there exists a proper integral model $X_0(D, N)$ of $X_0(D, N)$ over $\text{Spec}(\mathbb{Z})$, which suitably extends the moduli interpretation to arbitrary base schemes (cf. [13], [54]). It turns out that $\mathcal{X}_0(D, N)$ has good reduction at $p$ if and only if $p \nmid DN$. When $p$ is fixed in the context and no confusion can arise, we shall write $\tilde{X}_0(D, N)$ for its special fiber at $p$.

Points in $X_0(D, N)(\mathbb{C})$ whose underlying abelian surface $A$ has complex multiplication are called CM or Heegner points in the literature. In this case, the subring of endomorphisms of $A$ that commute with the quaternionic multiplications is isomorphic to an order $\mathcal{R}$ in some imaginary quadratic field $K$. We say that $A$ has complex multiplication by $\mathcal{R}$ and write $\text{CM}(\mathcal{R}) \subset X_0(D, N)(K^{ab})$ for the (finite) set of such points. The coordinates of these points are shown to lie in the maximal abelian extension of $K$ thanks to the work of Shimura and Taniyama.

This manuscript focuses on the study of the specialization of Heegner points of $X_0(D, N)$ in the special fiber of $\mathcal{X}_0(D, N)$ at a prime $p$ of either bad or good reduction by means of Ribet’s theory of bimodules, and to arithmetical and computational applications.

To put our work in a wider context, let us remark that the impact of the theory of Heegner points on Shimura curves in many areas of number theory and arithmetic geometry is enormous. Just to name some of the most relevant, class field theory and the Birch and Swinnerton-Dyer conjecture have benefited greatly from this theory.

As for the former is concerned, coordinates of Heegner points in $\text{CM}(\mathcal{R})$ generate the ring class field of $\mathcal{R}$ over $K$. In the line of Kronecker’s youth-dream, the combination of this fact together with the effective knowledge of the field of modular functions of classical modular curves $X_0(N) := X_0(1, N)$ in terms of their Fourier expansions around cusps, makes it possible to compute such class fields explicitly. Extensions of this to the case of division quaternion algebras (i.e. $D > 1$) turns out to be one of the deepest open problems in the theory of Shimura
curves. We refer the interested reader to [3], [5] and [4] for progress in this direction in the case $D = 6$.

As for the latter, Heegner points, together with modularity, are the fundamental ingredients in the most important results towards the Birch and Swinnerton-Dyer conjecture that have been established so far. Indeed, the most convincing theoretical evidence of the truth of this conjecture is the theorem of Kolyvagin and Gross-Zagier, which shows that the rank $r(E)$ of the Mordell-Weil group of an elliptic curve $E_{/\mathbb{Q}}$ coincides with the order of vanishing $r_{an}(E)$ of the $L$-series $L(E, s)$ at $s = 1$, provided $r_{an}(E) \leq 1$. More precisely, the theorem of Wiles [76] and his collaborators, combined with the Jacquet-Langlands correspondence, shows that there exists a surjective modular parametrization

$$\pi : J_0(D, N) \rightarrow E \quad (0.0.1)$$

for any factorization $\text{cond}(E) = DN$ of the conductor of $E$ into relatively prime positive integers $D, N$ such that $D \geq 1$ is, as above, the square-free product of an even number of primes. Here $J_0(D, N)$ stands for the Jacobian of $X_0(D, N)$.

Fixing one such parametrization, e.g. $D = 1, N = \text{cond}(E)$ (though any other choice, if there is any, also works for this matter), and choosing a suitable imaginary quadratic field $K$ such that $r_{an}(E \times K) = 1$ and $\text{CM}(R) \subset X_0(D, N)(K^{ab})$ is a non-empty set for each order $R$ of $K$ of conductor $c \geq 1$, $(c, DN) = 1$, the work [40] and [41] shows that the images by $\pi$ of divisors supported on $\text{CM}(R)$ can be used to construct an Euler system of cohomology classes on $E$ satisfying suitable norm-compatibility properties; combing this with [33], one shows that the point $P_K \in E(K)$ obtained by tracing down to $K$ any of these divisors generates $E(K)$ up to torsion. Little further work yields the result alluded above as the the theorem of Kolyvagin and Gross-Zagier.

Besides the obvious theoretical interest of (0.0.1), there is one computational issue about it that we also find interesting: when the discriminant $D$ in the factorization $\text{cond}(E) = DN$ is chosen to be $D = 1$, the Fourier expansion of the weight two modular newform $f_E \in S_2(\Gamma_0(N))$ attached to $E$ allows again the explicit computation of Heegner points on $E(K^{ab})$. This feature is not available when $D > 1$ and recent work of Darmon [18] suggests an alternative, explicit way of computing these points which exploits the Čerednik-Drinfeld uniformization of the Shimura curve $X_0(D, N)$ at primes $p | D$. The theory of Čerednik-Drinfeld [16], [21] shall also be central for the purposes of this thesis.

This is not the only instance in which a well-established result for classical modular curves, whose proof is based on the presence of cuspidal points, admits no straight-forward generalization to Shimura curves attached to a quaternion algebra of discriminant $D > 1$.

Let us point out here some of such open questions which we find of great interest and pose as challenges for the interested reader. As we will describe in detail in Chapters 5 and 6 devoted to applications, our results represent an attempt to make progress in some of them. We also hope that the technical core of this thesis, to be found in Chapter 4, may be useful in approaching some of the other problems that remain untouched in this manuscript.

**Open problems:**

(i) Computation of equations of the canonical model of a Shimura curve over $\mathbb{Q}$ and of its modular functions and forms. See [28], [68], [2] for a satisfactory answer in the classical case.

(ii) Determination of the group of automorphisms of $X_0(D, N)$. See [55], [39], [26] for a complete answer in the classical case.
(iii) Let $A$ be an abelian surface with quaternionic multiplication over a number field $F$. Are there infinitely many supersingular prime ideals $\varphi$ of $F$ at which $A$ has supersingular reduction? See [25] for an answer to this problem when $D = 1$ and $F$ is totally real.

(iv) Say that a point on $X_0(D, N)$ is trivial if it is either a cusp or a Heegner point and write $X_0(D, N)^{triv}(\overline{\mathbb{Q}})$ for the set of such points. Let $d \geq 1$ be a positive integer. Is it true that $X_0(D, N)(L) = X_0(D, N)^{triv}(\overline{\mathbb{Q}}) \cap X_0(D, N)(L)$ for all $D, N$ with $DN$ large enough and any number field $L$ of degree at most $d$? See [52], [58], [9] for the classical case.

Let us describe now the contents of this manuscript. The sets $CM(R)$ of Heegner points in $X_0(D, N)$ can be described purely in algebraic terms as a set of conjugacy classes of optimal embeddings; recall that a ring monomorphism $\varphi : R \hookrightarrow O$ is said to be optimal whenever $\varphi(K) \cap O = \varphi(R)$. The main aim of this monograph is to exploit this algebraic description in order to determine the specialization of Heegner points in $CM(R)$ at special fibers of $X_0(D, N)$, paying particular attention to singular fibers.

In order to explain our main results in some detail, let $p \mid DN$ be a prime of bad reduction of $X_0(D, N)$ and let $\tilde{X}_0(D, N)$ denote the (singular) special fiber of $X_0(D, N)$ at $p$. As we shall show (cf. Theorem 3.3.2, Theorem 3.5.1), there is a simple criterion for deciding whether a Heegner point $P \in CM(R)$ specializes to either the smooth or singular locus of $\tilde{X}_0(D, N)$. More precisely, it is known (though perhaps not so well-documented in the literature) that each of the sets $S$ of

- Singular points of $\tilde{X}_0(D, N)$ for $p \parallel DN$,
- Irreducible components of $\tilde{X}_0(D, N)$ for $p \parallel DN$,
- Supersingular points of $\tilde{X}_0(D, N)$ for $p \nmid DN$

are in one-to-one correspondence with either one or two copies of $Pic(d, n)$ for certain $d = d_S(p, D, N)$ and $n = n_S(p, D, N)$ (cf. §2.2, 2.3.2 and 2.3.1 for precise statements).

In each of the three cases above, we will show that under appropriate behavior of $p$ in $R \subset K$ (that we make explicit in §3.3, 3.4, 3.5, respectively -see also the table below), Heegner points $P \in CM(R)$ specialize to elements of $S$ (with the obvious meaning in each case).

For any order $\hat{O}$ in a (either definite or indefinite) quaternion algebra, let $CM_{\hat{O}}(R)$ denote the set of optimal embeddings $\varphi : R \hookrightarrow \hat{O}$ up to conjugation by elements of $\hat{O}^\times$. Define

$$CM_{d,n}(R) = \sqcup_{\hat{O}} CM_{\hat{O}}(R),$$

where $\hat{O}$ runs over a set of representatives of $Pic(d, n)$. Notice that there exists a natural forgetful projection $\pi : CM_{d,n}(R) \to Pic(d, n)$ that maps a conjugacy class of optimal embeddings $\varphi : R \hookrightarrow \hat{O}$ to the isomorphism class of its target $\hat{O}$.

As mentioned above, the set $CM(R) \subset X_0(D, N)(K^{ab})$ is in bijective correspondence with $CM_{D,N}(R)$. Thus the specialization of $CM(R)$ to elements of $S$ yields a natural map

$$CM_{D,N}(R) \to \bigcup_{i=1}^{t} Pic(d, n). \quad (0.0.2)$$
Our first observation is that, although the construction of this map is of geometric nature, both the source and the target are pure algebraic objects. Hence, one could ask whether there is a pure algebraic description of the arrow itself.

One of the aims of this note is to exploit Ribet’s theory of bimodules in order to show that this is indeed the case, and that in fact (0.0.2) can be refined as follows: there exists a map \( \phi : \text{CM}_{D,N}(R) \rightarrow \bigsqcup_{i=1}^t \text{CM}_{d,n}(R) \) which is equivariant for the actions of \( \text{Pic}(R) \) and of the Atkin-Lehner groups (see Chapter 1 for precise descriptions of these actions) and makes the diagram

\[
\begin{array}{ccc}
\text{CM}_{D,N}(R) & \xrightarrow{\phi} & \bigsqcup_{i=1}^t \text{CM}_{d,n}(R) \\
& \searrow \pi \swarrow & \\
& \bigsqcup_{i=1}^t \text{Pic}(d,n) & 
\end{array}
\]

commutative (see (3.3.15), (3.3.18), (3.4.20), (3.5.21) and (3.5.22)). Moreover, we show that when \( N \) is square free, the maps \( \phi \) are bijections.

As we explain in Chapter 3, the most natural construction of the map \( \phi \) is again geometrical, but can also be recovered in pure algebraic terms. For the convenience of the reader, we summarize our main results, proved in Chapter 3, in the following table. (Here, the maps \( \phi_s \) and \( \phi_c \) stands for the map \( \phi \) when refers to singular specialization or image on the set of irreducible components, respectively)

<table>
<thead>
<tr>
<th>Condition on ( p )</th>
<th>S=Irreducible components</th>
<th>( \phi_c )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p \mid D )</td>
<td>\bigsqcup_{i=1}^t \text{Pic}(\frac{D}{p}, N) )</td>
<td>\text{CM}<em>{D,N}(R) \rightarrow \bigsqcup</em>{i=1}^t \text{CM}_{\frac{D}{p},N}(R)</td>
</tr>
<tr>
<td>( p \parallel N )</td>
<td>\bigsqcup_{i=1}^t \text{Pic}(D_i, \frac{N}{p}) )</td>
<td>\text{CM}<em>{D,N}(R) \rightarrow \bigsqcup</em>{i=1}^t \text{CM}_{D_i,N}(R)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Condition on ( p )</th>
<th>S=Singular Points</th>
<th>( \phi_s )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p \mid D )</td>
<td>\text{Pic}(\frac{D}{p}, Np) )</td>
<td>\text{CM}<em>{D,N}(R) \rightarrow \text{CM}</em>{\frac{D}{p},Np}(R)</td>
</tr>
<tr>
<td>( p \parallel N )</td>
<td>\text{Pic}(Dp, \frac{N}{p}) )</td>
<td>\text{CM}<em>{D,N}(R) \rightarrow \text{CM}</em>{Dp,N}(R)</td>
</tr>
</tbody>
</table>

The results of Chapter 3 are the technical core of this manuscript, and provide a tool for understanding the interplay between Heegner points and the special fibers of a Shimura curve \( X_0(D,N) \). As already remarked, we hope this can serve as a tool for tackling some of the problems listed before.

The main application that we offer here is developed in Chapter 4 and concerns the computational problem of writing down explicit equations of the canonical model of \( X_0(D,N) \) when \( D > 1 \), as posed in (i).

Ihara [36] was probably one of the first to express an interest on this problem, and already found an equation for the genus 0 curve \( X_0(6,1) \), while challenged to find others. Since then, several authors have contributed to this question (Kurihara [43], Jordan [38], Elkies [27], Clark and Voight [75] for genus 0 or/and 1, González and Rotger [30], [29] for genus 1 and 2).

Elkies computes equations for the list of Shimura curves that he deals with using their hyperbolic (rather than the non-Archimedean uniformizations at primes dividing the discriminant) uniformizations. His method has the advantage that allows the identification of Heegner points in the equation, but is limited to very small discriminants \( D \) and levels \( N \).
The methods of González and Rotger are heavily based on Čerednik-Drinfeld’s theory for the special fiber at $p \mid D$ and the arithmetic properties of Heegner points. It allows to work with larger $D$ and $N$ but is again subjected to severe restrictions: the genus must be at most 2 and, in the hyperelliptic case, the curve must be bielliptic. In addition, this method does not allow to locate Heegner points in the given model of the curve. Our first application is in the line of [29] but removing such strong restrictions.

More precisely, we shall introduce an algorithm that computes equations for hyperelliptic Shimura curves with good reduction at 2. For the sake of simplicity we restrict ourselves to the case $N = 1$ and write $X_0^D = X_0(D, 1)$, although we believe that the procedure can be easily generalized to the case of arbitrary square-free $N$. Polynomials defining equations of hyperelliptic curves are closely related to their set of Weierstrass points. The set of Weierstrass points $WP(X_0^D)$ of a hyperelliptic Shimura curve $X_0^D$ turns out to be a disjoint union of Heegner points:

$$WP(X_0^D) = \bigsqcup_i \text{CM}(R_i),$$

for suitable orders $R_i$ in imaginary quadratic fields. As a consequence, $X_0^D$ admits an equation of the form

$$y^2 = \prod_i p_i(x), \quad (0.0.4)$$

where $p_i(x)$ is a polynomial attached to each set of Heegner points $\text{CM}(R_i)$.

Let $X_0^D = X_0(D, 1)$ denote Morita’s integral model of $X_0^D$. Over $\mathbb{Z}[1/2]$, $X_0^D$ will also be defined by an equation of the form (0.0.4). As we shall explain in detail, the specialization of Weierstrass points at the special fiber of $X_0^D$ at a prime $p$ can be exploited in order to compute the $p$-adic valuation of the discriminants $\text{disc}(p_i)$ and resultants $\text{Res}(p_1, p_j)$ of the above polynomials. We will make use of the theory of specialization of Heegner points introduced above in order to obtain such information.

Moreover, by means of the classical theory of complex multiplication we can also compute the splitting fields of each $p_i$. Exploiting the theory developed by Gross-Zagier in [33] we can further compute the leading coefficients of each $p_i$, once we have fixed a pair of Heegner points at infinity.

As a combination of all this data, we are able to compute an explicit model (0.0.4) for $X_0^D$. The only algorithmic limitation of this method relies on the fact that it exploits certain instructions which are currently implemented (e.g. in MAGMA) only for small degree field extensions. As long as the genus increases, the degrees of the fields involved in the computation become so large that make it impossible to proceed with the algorithm.

In order to deal with this computational limitation, we shall explain how to adapt the algorithm to quotients of Shimura curves by Atkin-Lehner involutions. It turns out that the degrees of the fields involved in the computation in this case are smaller and, consequently, we expect to compute more examples.

Finally, we devote Chapter 5 to explain three further applications of the results obtained in Chapter 3. The first two are given in the short sections §5.1 and §5.2, and are just direct consequences of our work combined with results of other people.

The aim of the more elaborated third application, offered in §5.3, is giving a proof of the main theorems of Bertolini-Darmon [8] and Longo-Vigni [50] on special values of L-functions and the Birch and Swinnerton-Dyer conjecture for analytic rank 0 that, borrowing greatly
from theirs, makes use of a different family of Heegner points. Although the material of §5.3 is not to be considered a new contribution to the subject, we hope that the new approach we suggest may be useful for proving similar results in scenarios where nothing has been proved so far. We expect to pursue this line of research in the future.

Let us describe these three applications in more detail.

In §5.1 we explore the distribution of the sets of Heegner points \( \text{CM}(R) \) into the set \( S \) of either singular points, irreducible components or supersingular points of the fiber \( \tilde{X}_0(D, N) \) as \( \text{disc}(K) \) tends to infinity. As remarked above, the specialization of Heegner points yields one-to-one correspondences between \( \text{CM}(R) \) and sets of optimal embeddings \( \bigsqcup_{i=1}^{l} \text{CM}_{d,n}(R) \) (see the table above). Moreover, composing with the previously mentioned projection \( \pi : \text{CM}_{d,n}(R) \to \text{Pic}(d, n) \), we are able to characterize the element in \( S \) where the Heegner point is located. Recent results of P. Michel [53] on the equidistribution of the sets \( \text{CM}_{d,n}(R) \) among \( \text{Pic}(d, n) \) automatically provide that, in each of the three cases, the sets \( \text{CM}(R) \) are equidistributed among the sets \( S \).

In §5.2 we explain how the ideas of Chapter 3 can be used to obtain new results regarding problem (ii) above. In §1 we introduced the group \( W(D, N) \) of Atkin-Lehner involutions of a Shimura curve \( X_0(D, N) \), which is a finite subgroup of \( \text{Aut}(X_0(D, N)) \). In fact, when the genus \( g(X_0(D, N)) \geq 2 \) and \( N \) is square-free, it is conjectured that \( \text{Aut}(X_0(D, N)) = W(D, N) \) except for finitely many values of \( (D, N) \). In [42], Kontogeorgis and Rotger deal with this conjecture and they are able to prove it for many values of \( D \) and \( N \). Their methods exploit Čerednik-Drinfeld’s description of the special fiber of \( X_0(D, N) \) at primes \( p \mid D \) and the action of \( W(D, N) \) on their set of irreducible components and singular points. In §5.2 we add a new ingredient by relating the action of \( \text{Aut}(X_0(D, N)) \) with the specialization of Heegner points. This allows us to prove that \( \text{Aut}(X_0(D, N)) = W(D, N) \) in cases where the techniques of [42] were not able to conclude; we illustrate it with the case \( D = 667, N = 1 \).

In order to describe the material of §5.3, let \( f \in S_2(\Gamma_0(M))^{\text{new}} \) be a normalized newform of weight 2 and level \( M \geq 1 \). Assume \( M \) admits a factorization \( M = d \cdot n \) into coprime integers \( d \) and \( n \) where \( d \) is the square-free product of an odd number of primes none of which splits in \( K \), and none of the prime factors of \( n \) is inert in \( K \).

A formula of Gross (see Theorem 5.1.1) relates the image of the embeddings in \( \text{CM}_{d,n}(R) \) through the forgetful map \( \pi : \text{CM}_{d,n}(R) \to \text{Pic}(d, n) \) to the special value \( L(f/K, \chi, 1) \) of the \( L \)-function of \( f \) over \( K \) twisted by a finite character \( \chi \).

In §5.3 we relate our results on the specialization of Heegner points to Gross’s formula. Namely, degree-zero linear combinations of points in \( \text{CM}(R) \) yield points on the Néron model \( \mathcal{J} \) of the Jacobian of \( X_0(D, N) \) over \( K_p \) which can be projected to the group \( \Phi \) of connected components of \( \mathcal{J} \). We are able to compute the position of the image of such Heegner divisors in \( \Phi \), exploiting the work of Edixhoven in [22]. Via Gross’s formula, we relate this image to the special value \( L(f/K, \chi, 1) \). This yields a proof of the Birch and Swinnerton-Dyer conjecture in the case of analytic rank zero, alternative to the one given by Bertolini and Darmon in [8] or by Longo and Vigni in [50].

For the convenience of the reader, we conclude this introduction describing the structure of this manuscript. In Chapter 1 we recall the basic facts about quaternion algebras and Eichler orders, optimal embeddings of orders in imaginary quadratic fields, Shimura curves and Heegner points. We refer to [1] for a more detailed introduction to this topics.

In Chapter 2 we introduce Ribet’s work [61] on abelian surfaces and bimodules, which
yields a description of the special fibers of $\mathcal{X}_0(D,N)$ at a given prime. We put special emphasis to the sets of irreducible components and of singular points of $\tilde{\mathcal{X}}_0(D,N)$ for primes of bad reduction, and to the set of supersingular points of $\tilde{\mathcal{X}}_0(D,N)$ for primes of good reduction.

For primes of bad reduction, we devote §2.2 to recall the basic properties of Čerednik-Drinfeld’s special fiber at $p | D$, and §2.3 to Deligne-Rapoport-Buzzard’s special fiber at $q \parallel N$. Finally, §2.4.9 is devoted to the specialization map of a Shimura curve in terms of its moduli interpretation.

We refer to Chapter 3 for the main bulk of theoretical results on the specialization of Heegner points. We shall explore each of the singular special fibers, devoting §3.3 to Čerednik-Drinfeld’s special fiber and §3.5 to Deligne-Rapoport-Buzzard’s, having as goal the construction of the maps $\phi$ of the table above and their behavior under the actions of $\text{Pic}(R)$ and of the Atkin-Lehner group.

The aim of Chapter 4 is showing how our previous results can be applied in order to find explicit equations of certain Shimura curves. We will focus our attention to the case in which the curve is hyperelliptic. However, since the material developed in Chapter 3 is available for all Shimura curves, we hope that it can be useful as well for other cases. In §4.3 we conclude with an algorithm that computes an equation of any hyperelliptic Shimura curve under certain geometrical and computational restrictions. We devote §4.4 and §4.5 to exhibit two examples of its implementation. Finally, in §4.6 we explain how to adapt the algorithm to quotients of Shimura curves by Atkin-Lehner involutions and in §4.6.4 we present a list of equations of Shimura curves and Atkin-Lehner quotients obtained by this method. These equations were unknown until now and had been conjectured by Kurihara in [44].

Finally, the three sections of Chapter 5 are devoted to the further applications described before.

Agraïments.

Agraïxo profundament als meus directors de tesi Josep González i Víctor Rotger pel seu guiatge i suport al llarg del desenvolupament d’aquest treball. Sempre apreciaré que m’hagin introduït a aquesta meravellosa àrea de les matemàtiques.

Faig extensiu l’agraïment a tots els components del Seminari de Teoria de Nombres de Barcelona per la seva valiosa ajuda durant aquests anys i en especial als meus companys becaris als que ara considero com amics. D’entre aquests, faig un especial esment a Xevi Guitart i Francesc Fité per haver llegit detingudament diverses parts de la tesi i donar alguns comentaris molt útils.

Dono les gràcies al professors Massimo Bertolini, Matteo Longo, Qing Liu, Bas Edixhoven, Ariel Martín Pacetti i John Voight per les seues converses i discussions enriquidores.

Agraeixo la generosa ajuda i hospitalitat rebuda del Centre de Recerca Matemàtica de Bellaterra (Barcelona) durant els darrers mesos del meu treball.

També voldria agrair l’Escola Tècnica Superior d’Enginyeria de Vilanova i la Geltrú (ET-SEVG) i la Facultat de Matemàtiques Estadística (FME) de la UPC per la seva càlida hospitalitat durant diversos periodes des de 2005 fins 2010.

Finalment, aquesta tesi no l’hauria pogut realitzar sense els meravellosos moments que he compartit amb la meva família no matemàtica i amics, especialment amb la meva xicota Elisenda Farré que m’ha donat suport malgrat que, degut a aquest treball, no l’he dedicat tot el temps que es mereix.
Chapter 1

Shimura curves and Heegner points

1.1 Quaternion algebras and oriented Eichler orders

Let $F$ be a field.

Definition 1.1.1. A quaternion algebra $B$ over $F$ is a central simple algebra over $F$ of rank$_F(B) = 4$.

Assume the characteristic of $F$ is not 2. Quaternion algebras can be classically described and constructed as follows. Let $K$ be a quadratic separable algebra over the field $F$, let $\sigma$ denote the non trivial involution on $K$ over $F$ and let $m \in F^\star$ be any non zero element. Then, the algebra $B = K \oplus eK$ with $e^2 = m$ and $e \cdot x = x^{\sigma}e$ for any $x \in K$; is a quaternion algebra over $F$. As it is shown in [74], any quaternion algebra over $F$ is of this form.

The following theorem, known as the Skolem-Noether Theorem, characterizes the group of automorphisms of a quaternion algebra.

Theorem 1.1.2 (Skolem-Noether). [74, Chp. I, Theorem 2.1] Let $B$ be a quaternion algebra over $F$. Then, any automorphism $\varphi : B \rightarrow B$ of $F$-algebras is inner: there exists $\gamma \in B^\times$ such that $\varphi(\beta) = \gamma \beta \gamma^{-1}$ for all $\beta \in B$.

The algebra $B$ comes equipped with an anti-involuting conjugation map $\beta \mapsto \overline{\beta}$ such that, when restricted to a quadratic extension $F(\beta)$, $\beta \in B^\times \setminus F^\times$, is the nontrivial automorphism of $F(\beta)/F$. More explicitly, if $\beta = x + ey \in K \oplus eK$, then $\overline{\beta} = x^{\sigma} - ey$. Elements $\beta \in B$ are roots of the quadratic polynomial $x^2 + Tr(\beta)x + N(\beta)$, where

$$Tr(\beta) = \beta + \overline{\beta}$$

and

$$N(\beta) = \beta \cdot \overline{\beta}$$

denote the reduced trace and the reduced norm of $\beta \in B$, respectively.

Let $Q$ denote the field of rational numbers. For any place $v$ of $Q$, let $Q_v$ denote the completion of $Q$ respect to $v$. Regardless $v$ is archimedean or non-archimedean, there exists exactly two isomorphism classes of quaternion algebras over the local field $Q_v$: the split algebra $M_2(Q_v)$ and a division algebra, that we will denote by $\mathbb{H}_v$. Indeed, isomorphism
classes of central simple algebras over a number field $F$ are classified by the Brauer group $H^2(\text{Gal}(\bar{F}/F), \bar{F}^\times) = \text{Br}(F)$ of $F$, and quaternion algebras correspond to the 2-torsion subgroup $\text{Br}(F)[2]$. If $F = \mathbb{Q}_v$, we have $\text{Br}(\mathbb{Q}_v) = \mathbb{Q}/\mathbb{Z}$ if $v$ is non-archimedean, $\text{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ if $v = \infty$. In any case, it follows that $\text{Br}(\mathbb{Q}_v)[2] = \mathbb{Z}/2\mathbb{Z}$. Notice that if $v = \infty$, $\mathbb{Q}_\infty = \mathbb{R}$, $\mathbb{H}_\infty$ is the classical skew-field of Hamilton’s quaternions. A place $v$ of $\mathbb{Q}$ is said to ramify in $B$ if $B \otimes \mathbb{Q}_v = \mathbb{H}_v$ is the nonsplit algebra over $\mathbb{Q}_v$.

It is a classical theorem of Hasse that there is a finite and even number of places $v$ on $\mathbb{Q}$ that ramify in $B$. As a matter of fact, the classical exact sequence of Brauer groups (cf. [73, §11]),

$$0 \to \text{Br}(\mathbb{Q}) \to \prod_v \text{Br}(\mathbb{Q}_v) \xrightarrow{\sum} \mathbb{Q}/\mathbb{Z} \to 0,$$

yields an exact sequence of 2-elementary groups:

$$0 \to \text{Br}(\mathbb{Q})[2] \to \prod_v \text{Br}(\mathbb{Q}_v)[2] \xrightarrow{\sum} \mathbb{Z}/2\mathbb{Z} \to 0.$$

Hence, given a finite even number of places $S$, there exists a unique isomorphism class of quaternion algebras $B/\mathbb{Q}$ ramified exactly at the places of $S$.

**Definition 1.1.3.** The ramified set $S_B$ of a quaternion algebra $B$ over $\mathbb{Q}$ is the set of places $v$ where $B_v$ is ramified. The discriminant $D$ of $B$ is $D = \prod p$, where the product runs over the set of the finite places in $S_B$.

Note that the discriminant $D$ of $B$ characterizes the isomorphism class of quaternion algebras $B/\mathbb{Q}$ ramified exactly at the places of $S$.

**Definition 1.1.4.** An element $\beta \in B$ is integral if $\text{Tr}(\beta), N(\beta) \in \mathbb{Z}$.

Unlike number fields or local fields, the set of integral elements of $B$ is not a ring anymore.

**Definition 1.1.5.** An order $\mathcal{O} \subset B$ over $\mathbb{Z}$ is a ring of integral elements in $B$ which is finitely generated as $\mathbb{Z}$-module and such that $\mathcal{O} \otimes \mathbb{Z} \mathbb{Q} = B$. It is a maximal order if it is not properly contained in any other order.

Let us agree to say that two orders $\mathcal{O}$ and $\mathcal{O}'$ of $B$ are conjugate if $\mathcal{O} = \gamma \mathcal{O}' \gamma^{-1}$ for some $\gamma \in B^\times$.

Maximal orders in quaternion algebras are in general not unique, often not even up to conjugation by elements of $B^\times$. However, it follows from [74] that there is finite number of conjugacy classes of maximal orders in $B$.

**Definition 1.1.6.** An ideal of $B$ is a finitely generated $\mathbb{Z}$-module $\mathcal{I}$ with $\mathcal{I} \otimes \mathbb{Z} \mathbb{Q} = B$. The right order of $\mathcal{I}$ is defined to be $\mathcal{O}^r(\mathcal{I}) = \{ \beta \in B : \mathcal{I} \beta \subseteq \mathcal{I} \}$. Similarly, we define the left order $\mathcal{O}^l(\mathcal{I})$ of $\mathcal{I}$. 

CHAPTER 1. SHIMURA CURVES AND HEEGNER POINTS

Given a general $\mathbb{Z}$-module $\mathcal{M}$ with a well defined left action of $B$, let $\mathcal{O}^r(\mathcal{M})$ denote its right order. Similarly, for any $\mathbb{Z}$-module with a well defined right action of $B$, $\mathcal{O}^l(\mathcal{M})$ stands for its left order.

Let $\mathcal{O}$ be an order in $B$. A left ideal (respectively right ideal) of $\mathcal{O}$ is an ideal of $B$ such that $\mathcal{O}^r(\mathcal{I}) = \mathcal{O}$ (respectively $\mathcal{O}^l(\mathcal{I}) = \mathcal{O}$). The inverse ideal of an $\mathcal{O}$-left ideal $\mathcal{I}$ is defined to be $\mathcal{I}^{-1} = \{\beta \in B : \mathcal{I}\beta \subseteq \mathcal{I}\}$. It is a right $\mathcal{O}$-ideal such that $\mathcal{O}^r(\mathcal{I}) \subseteq \mathcal{O}^l(\mathcal{I}^{-1})$.

**Definition 1.1.7.** Two $\mathcal{O}$-left ideals $\mathcal{I}$ and $\mathcal{J}$ are equivalent if and only if there exists $\beta \in B$ such that $\mathcal{I} = \mathcal{J}\beta$. We denote by $\operatorname{Pic}_{\ell}(\mathcal{O})$ the set of equivalence classes of $\mathcal{O}$-left ideals. We define analogously the equivalence class of a $\mathcal{O}$-right ideal and the set $\operatorname{Pic}_r(\mathcal{O})$.

By [74, Chp.I, Lemme 4.9] the map $\mathcal{I} \mapsto \mathcal{I}^{-1}$ establishes a bijection between classes of $\mathcal{O}$-left ideals and classes of $\mathcal{O}$-right ideals. Thus $\operatorname{Pic}_r(\mathcal{O}) \simeq \operatorname{Pic}_l(\mathcal{O})$.

We proceed to define a particular type of orders that play an essential roll on the construction of Shimura curves.

**Definition 1.1.8.** An order $\mathcal{O}$ in $B$ over $Z$ is an Eichler order if it is the intersection of two maximal orders. Its index $N$ in any of the two maximal orders is called the level of $\mathcal{O}$.

Let $D$ be the discriminant of $B$. By [74, Lemme II.1.5], there exists a unique maximal order in $B_p$ if $p \mid D$. Hence for any Eichler order $\mathcal{O}$ in $B$ of level $N$, we have that $(D, N) = 1$.

Throughout, for any module $M$ over $Z$ and for any prime $p$ we shall write $M_p = M \otimes \mathbb{Z}_p$. Similarly, for any homomorphism $\chi: M \rightarrow N$ of modules over $Z$, we shall write $\chi_p: M_p \rightarrow N_p$ for the natural homomorphism obtained by extension of scalars. We shall also write $\hat{Z}$ to denote the profinite completion of $Z$, and $M = M \otimes \hat{Z}$.

An order is called Gorenstein if every left $\mathcal{O}$-module $\mathcal{M}$ such that $\mathcal{O}^r(\mathcal{M}) = \mathcal{O}$ is projective (i.e. locally free of rank 1) (cf. [14]). As discussed in [37], all Eichler orders over $Z$ are Gorenstein. This implies that every left $\mathcal{O}$-ideal is locally principal. Hence, the set of left $\mathcal{O}_p$-ideals is identified with the coset $\mathcal{O}_p^\times \setminus B_p^\times$ and, therefore, the set of left ideals of $\mathcal{O}$ is identified with the coset $\mathcal{O}^\times \setminus B^\times$. Finally, the set of classes of left $\mathcal{O}$-ideals $\operatorname{Pic}^\ell(\mathcal{O})$ is in turn described as the double coset $\mathcal{O}^\times \setminus B^\times / B^\times$.

**Proposition 1.1.9.** [74, Chp.III, Theorem 5.4 and Corollary 5.7 bis] Let $\mathcal{O}$ be an Eichler order. Then $\operatorname{Pic}^\ell(\mathcal{O})$ is finite. Moreover, if $B$ is indefinite then $\# \operatorname{Pic}^\ell(\mathcal{O}) = 1$.

Let $\mathcal{O}$ be an Eichler order of level $N$ in a quaternion algebra $B$ over $\mathbb{Q}$ of discriminant $D$. An orientation on $\mathcal{O}$ is a collection of choices, one for each prime $p \mid DN$: a choice of a homomorphism $\alpha_p: \mathcal{O} \rightarrow \mathbb{F}_p^2$ for each prime $p \mid D$, and a choice of a local maximal order $\mathcal{O}_p$ containing $\mathcal{O}_p$ for each $p \mid N$. One says that two oriented Eichler orders $\mathcal{O}, \mathcal{O}'$ are isomorphic whenever there exists an automorphism $\beta$ of $B$ with $\beta(\mathcal{O}) = \mathcal{O}'$ such that $\alpha_p = \alpha_p' \circ \beta$ for all $p \mid D$ and $\chi_p(\mathcal{O}_p) = \mathcal{O}_p'$ for all $p \mid N$.

**Definition 1.1.10.** Let $\mathcal{E}(D, N)$ stand for the set of oriented Eichler orders of level $N$ in $B$. Let $\operatorname{Pic}(D, N)$ denote the set of isomorphism classes of orders in $\mathcal{E}(D, N)$.

Fix an oriented Eichler order $\mathcal{O}$ in $\mathcal{E}(D, N)$. For a left $\mathcal{O}$-ideal $\mathcal{I}$ in $B$, the right order $\mathcal{O}^r(\mathcal{I})$ is also an Eichler order of level $N$ (cf.[74, Chp.III, §5]). Moreover, we can equip $\mathcal{O}^r(\mathcal{I})$ with the following local orientations at $p \mid DN$. Since $\mathcal{I}$ is locally principal, we may write $\mathcal{I}_p = \mathcal{O}_p\alpha_p$ for some $\alpha_p \in B_p$, so that $\mathcal{O}_p^\prime = \alpha_p^{-1}\mathcal{O}_p\alpha_p$. For $p \mid D$, define $\alpha_p(\alpha_p^{-1}x\alpha_p) = \alpha_p(x)$. For $p \mid N$, define $\hat{\alpha}_p = \alpha_p^{-1}\hat{\mathcal{O}}\alpha_p$. 
Definition 1.1.11. We denote by $\mathcal{I} \ast \mathcal{O} \in \mathcal{E}(D, N)$ the order $\mathcal{O}'(\mathcal{I})$ equipped with such orientations.

Notice that it coincides with the left order of $\mathcal{I}^{-1}$ equipped with the orientations analogously defined for right $\mathcal{O}$-ideals

Proposition 1.1.12. [6] Fix $\mathcal{O} \in \mathcal{E}(D, N)$. The map $\mathcal{I} \mapsto \mathcal{I} \ast \mathcal{O}$ establishes a bijection between:

$$\text{Pic}_r(\mathcal{O}) \simeq \text{Pic}(D, N).$$

1.2 Optimal embeddings

Let $K/\mathbb{Q}$ be an imaginary quadratic field. Let $R_K$ denote its integer ring. An order $R$ in $K$ is a subring of $R_K$ of rank 2 over $\mathbb{Z}$, such that $K = R \otimes \mathbb{Z} \mathbb{Q}$. Let $\text{Pic}(R)$ denote the group of fractional projective ideals of $R$ modulo principal ideals and let $h(R) = \# \text{Pic}(R)$ denote the class number of $R$. We will simply write $\text{Pic}(K)$ instead of $\text{Pic}(R_K)$ and $h(K)$ instead of $h(R_K)$.

Writing $R_K = \mathbb{Z} \oplus \alpha \mathbb{Z}$ with $\alpha \in K$, any order of $K$ is of the form $R = \mathbb{Z} \oplus c\alpha \mathbb{Z}$, where $c \in \mathbb{Z}$, $c \geq 1$. The integer $c = c(R)$ is called the conductor of $R$ and the order $R$ is completely determined by it.

Definition 1.2.1. For any $\mathbb{Z}$-algebra $\mathcal{D}$, write $\mathcal{D}^0 = \mathcal{D} \otimes \mathbb{Z} \mathbb{Q}$ and say that an embedding $\varphi: \mathcal{D}_1 \to \mathcal{D}_2$ of $\mathbb{Z}$-algebras is optimal if $\varphi(\mathcal{D}_1^0) \cap \mathcal{D}_2 = \varphi(\mathcal{D}_1^0)$ in $\mathcal{D}_2^0$.

In this section we shall consider optimal embeddings $\varphi: R \to O$, where $R$ is an order in the imaginary quadratic field $K$ and $O \in \mathcal{E}(D, N)$. Two optimal embeddings $\varphi, \psi: R \to O$ are conjugated if there exist $\beta \in B^\times$ such that $\varphi(x) = \beta \psi(x)\beta^{-1}$. Let $\text{CM}_O(R)$ denote the set of optimal embeddings $\varphi: R \to O$, up to conjugation by $B^\times$. Define

$$\text{CM}_{D,N}(R) = \bigsqcup \text{CM}_O(R),$$

where $O \in \mathcal{E}(D, N)$ runs over a set of representatives of $\text{Pic}(D, N)$. Write

$$\pi: \text{CM}_{D,N}(R) \to \text{Pic}(D, N) \quad (1.2.1)$$

for the natural forgetful projection which maps a conjugacy class of optimal embeddings $\varphi: R \to O$ to the isomorphism class of its target $O$.

Any $\varphi \in \text{CM}_{D,N}(R)$ induces an embedding $\varphi \in \text{Hom}(K, B)$ given by extension of scalars and well-defined up to conjugation by $B^\times$. Moreover, if we fix $O \in \mathcal{E}(D, N)$, by means of $\pi$ and the natural bijection $\text{Pic}(D, N) \cong \text{Pic}(O) = \hat{O}^\times \setminus \hat{B}^\times / B^\times$ we obtain a map

$$\text{CM}_{D,N}(R) \to \hat{O}^\times \setminus \hat{B}^\times \times \text{Hom}(K, B) / B^\times, \quad (1.2.2)$$

that clearly turns out to be injective.

For any embedding $(\varphi: K \to B) \in \text{Hom}(K, B)$, the set

$$\varphi(K)_- = \{ \alpha \in B, \text{ s.t. } \alpha \varphi(x) = \varphi(x^\sigma)\alpha, \text{ for all } x \in K \},$$

where $\sigma \in \text{Gal}(K/\mathbb{Q})$ is the non-trivial automorphism, is called the quaternionic complement of its image $\varphi(K)$. As shown in §1.1, it is a $K$-vector space of dimension 1. We sometimes
refer the element of a basis as a \textit{quaternionic complement of} $\varphi$. It is an element $j \in B$ such that $j^2 \in \mathbb{Q}^\times$ and $j \varphi(x) = \varphi(x \sigma)j$, for all $x \in K$.

Since $B$ is the direct sum of the image $\varphi(K)$ and its quaternionic complement, $B$ acquires structure of right $K$-algebra of dimension 2 by means of $\varphi \in \text{Hom}(K, B)$. Write $B \simeq K \oplus jK$ for such $K$-algebra structure with $j^2 = m \in \mathbb{Q}^\times$. The left action of $B$ on itself as a $K$-algebra provides an embedding

$$B \simeq K \oplus jK \hookrightarrow \mathbb{M}_2(K)$$

$$a + jb \mapsto \begin{pmatrix} a & mb^\sigma \\ b & a^\sigma \end{pmatrix}.$$  \hspace{1cm} (1.2.3)

Such embedding, in turn, provides an isomorphism

$$B \otimes_{\mathbb{Q}} K \overset{\simeq}{\longrightarrow} \mathbb{M}_2(K)$$

$$(a + jb) \otimes c \mapsto \begin{pmatrix} ac & mb^\sigma c \\ bc & a^\sigma c \end{pmatrix}. \hspace{1cm} (1.2.4)$$

\textbf{Remark 1.2.2.} Notice that the action of $1 \otimes K$ on $B$ is given by right multiplication by $K$, while the action of $\varphi(K) \otimes 1$ is given by left multiplication by $K$.

Let $\mathcal{O} \in \mathcal{E}(D, N)$ and let $\varphi : R \hookrightarrow \mathcal{O}$ be an optimal embedding. Via $\varphi$, we may regard $\mathcal{O}$ as a locally free right $R$-module of rank 2. Together with the decomposition $B \simeq K \oplus jK$ induced by $\varphi : K \hookrightarrow B$, we have

$$\mathcal{O} \simeq R \oplus eI.$$  \hspace{1cm} (1.2.5)

for some $e \in B$ and some locally free $R$-ideal $I$ in $K$. Notice that the element $e \in B$ may not be a quaternionic complement of $\varphi$. We shall use these decompositions for future computations since they characterize explicitly the optimal embedding $\varphi$.

Two local optimal embeddings $\phi_p, \varphi_p : R_p \hookrightarrow \mathcal{O}_p$ are said to be equivalent, denoted $\varphi_p \sim_p \phi_p$, if there exists $\lambda \in \mathcal{O}_p^\times$ such that $\phi_p = \lambda \varphi_p \lambda^{-1}$. Let us denote by $m_p$ the number of equivalence classes of such local embeddings. We say that two global optimal embeddings $\phi, \varphi : R \hookrightarrow \mathcal{O}$ are locally equivalent if $\varphi_p \sim_p \phi_p$ for all primes $p$.

\textbf{Proposition 1.2.3.} \cite[Chp. II, Theorem 3.1, Theorem 3.2]{74} \textit{Let} $(\frac{K}{p})$ \textit{be the Kronecker symbol. Let} $(\frac{R}{p})$ \textit{be the Eichler symbol:}

$$
\left( \frac{R}{p} \right) = \begin{cases} 
\left( \frac{K}{p} \right) & \text{if } c(R_p) = 1 \\
1 & \text{otherwise}.
\end{cases}
$$

Then,

- If $p \mid D$, then $m_p = \left( 1 - \left( \frac{R}{p} \right) \right) \in \{0, 1, 2\}$.
- If $p \parallel N$, then $m_p = \left( 1 + \left( \frac{R}{p} \right) \right) \in \{0, 1, 2\}$.
- If $p \mid N$ and $(\frac{K}{p}) = -1$, then $m_p = 0$. 

---

CHAPTER 1. SHIMURA CURVES AND HEEGNER POINTS 17
We proceed now to describe an action of $\text{Pic}(R)$ on the set $\text{CM}_{D,N}(R)$ of optimal embeddings. Let $\varphi \in \text{CM}_\mathcal{O}(R) \subseteq \text{CM}_{D,N}(R)$ be an optimal embedding and let $[J] \in \text{Pic}(R)$, represented by an ideal $J$. Consider the left $\mathcal{O}$-ideal $\mathcal{O}_\varphi(J)$. Write $[J]*\mathcal{O}$ for the right order $\mathcal{O}_\varphi(J)*\mathcal{O} \in \mathcal{E}(D,N)$ defined as in §1.1, and let us denote by $[J]*\varphi \in \text{CM}_{[J]*\mathcal{O}}(R)$ the natural optimal embedding
\[ R \mapsto \{ x \in B, : \mathcal{O}_\varphi(J)x \subseteq \mathcal{O}_\varphi(J) \}. \] (1.2.6)

**Proposition 1.2.4** (Trace formula). [74, Chp. III, Theorem 5.11] The embedding $[J]*\varphi$ defined above does not depend on the choice of the representative $J$ of $[J]$ and it defines an action of $\text{Pic}(R)$ on $\text{CM}_{D,N}(R)$. Moreover, such action is faithful and preserves local equivalence. In fact,
\[ \# \text{CM}_{D,N}(R) = h(R) \prod_{p|DN} m_p, \] (1.2.7)
where $h(R) = \# \text{Pic}(R)$ is the class number of $R$.

**Corollary 1.2.5.** If $DN$ is square-free, then
\[ \# \text{CM}_{D,N}(R) = h(R) \prod_{p|D} \left( 1 - \left( \frac{R}{p} \right) \right) \cdot \prod_{p|N} \left( 1 + \left( \frac{R}{p} \right) \right). \]

For each $p^n \parallel DN$, there is also an Atkin-Lehner involution $\omega_p^n$ acting on $\text{CM}_{D,N}(R)$, which can be described as follows: Let $\mathcal{O} \in \mathcal{E}(D,N)$ and assume that $p^n \parallel DN$. As shown in [74, Chp.II, §1 and 2], the normalizer
\[ N(\mathcal{O}_p) = \{ \beta \in B_p : \beta \mathcal{O}_p \beta^{-1} \subseteq \mathcal{O}_p \} \]
is generated by $\mathcal{O}_p^\times \mathcal{O}_p^\times$ and an element $\alpha_p$ of norm $p^n$. Since any left $\mathcal{O}_p$-ideal is principal, there is a unique two-sided $\mathcal{O}_p$-ideal of norm $p^n$. This implies that there is a unique two-sided ideal $\mathfrak{P}_\mathcal{O}$ of $\mathcal{O}$ of norm $p^n$. Notice that $\mathfrak{P}_\mathcal{O}*\mathcal{O}$ equals $\mathcal{O}$ as orders in $B$, but they are endowed with possibly different local orientations. Given $\varphi \in \text{CM}_\mathcal{O}(R) \subseteq \text{CM}_{D,N}(R)$, $\omega_p$ maps $\varphi$ to the optimal embedding $\omega_p^n(\varphi) : R \mapsto \mathfrak{P}_\mathcal{O}*\mathcal{O}$, where $\omega_p^n(\varphi)$ is simply $\varphi$ as ring homomorphism. Since $\alpha_p^2 = p^n$, we have that $\mathfrak{P}_\mathcal{O}*\mathcal{O} \ast (\mathfrak{P}_\mathcal{O} * \mathcal{O}) = \mathcal{O}$. Thus $\omega_p$ is a well defined involution on $\text{CM}_{D,N}(R)$.

In the particular case $p \parallel DN$ and $m_p = 2$, the involution $\omega_p$ switches the two local equivalence classes at $p$.

For any $m \parallel DN$ we denote by $\omega_m$ the composition $\omega_m = \prod_{p^n \parallel m} \omega_p^n$. The set $W(D,N) = \{ \omega_m : m \parallel DN \}$ is an abelian 2-group, called the Atkin-Lehner group. Note that $\omega_m \omega_n = \omega_{nm/(m,n)^2}$ for all $m, n \parallel DN$.

Attached to the order $R$, we set
\[ D(R) = \prod_{p | D, m_p = 2} p, \quad N(R) = \prod_{p^n \parallel N, m_p = 2} p \]
and
\[ W_{D,N}(R) = \{ \omega_m \in W(D,N) : m \parallel D(R)N(R) \}. \]

Suppose that $N$ is square free. The following result is a direct consequence of Proposition 1.2.4, formula (1.2.7), the fact that $\text{Pic}(R)$ acts faithfully on $\text{CM}_{D,N}(R)$ by preserving local equivalences, and Atkin-Lehner involutions $\omega_p \in W_{D,N}(R)$ switch local equivalence classes at $p$. 
Corollary 1.2.6. Assume $N$ is square free. Then the group $W_{D,N}(R) \times \text{Pic}(R)$ acts freely and transitively on the set $\text{CM}_{D,N}(R)$.

1.3 Shimura curves and their moduli interpretation

Assume throughout the rest of the chapter that $B$ is an indefinite quaternion algebra over $\mathbb{Q}$. Let $D$ denote the reduced discriminant of $B$, let $N$ be an integer relatively prime to $D$ and let $\mathcal{O} \in \mathcal{E}(D,N)$ be an Eichler order of level $N$ in $B$. By Proposition 1.1.9, $\# \text{Pic}(D,N) = 1$ and there is a unique Eichler order of level $N$ up to conjugation.

Set

$$\mathbb{P} = \mathbb{P}_1(\mathbb{C}) - \mathbb{P}_1(\mathbb{R}) = \mathbb{C} - \mathbb{R}.$$  

Since $B$ splits at $\infty$, we can fix an isomorphism

$$\phi_\infty : B_\infty \rightarrow M_2(\mathbb{R})$$  

(1.3.8)

that identifies $B_\infty^\times$ with $\text{GL}_2(\mathbb{R})$; let $B^\times$ act on $\mathbb{P}$ via the natural action of $\text{GL}_2(\mathbb{R})$ on $\mathbb{P}$ by fractional linear transformations:

$$\text{GL}_2(\mathbb{R}) \times \mathbb{P} \rightarrow \mathbb{P}, \quad \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix}, z \right) \mapsto \frac{az + b}{cz + d}.$$  

Definition 1.3.1. The open Shimura curve of level $N$ and discriminant $D$ is the double coset space

$$Y_0(D,N) = \tilde{\mathcal{O}}^\times \backslash (\tilde{B}^\times \times \mathbb{P}) / B^\times,$$

turned with the natural topology induced by the product topology.

Since $\text{Pic}(D,N) \simeq \text{Pic}^f(\mathcal{O}) \simeq \tilde{\mathcal{O}}^\times \backslash \tilde{B}^\times / B^\times = \{|\mathcal{O}|\}$, for all $(b,z) \in \tilde{B}^\times \times \mathbb{P}$ there exists $z' \in \mathbb{P}$ such that $\tilde{\mathcal{O}}^\times (b,z)B^\times = \tilde{\mathcal{O}}^\times (1,z')B^\times$. Moreover, $\tilde{\mathcal{O}}^\times (1,z)B^\times = \tilde{\mathcal{O}}^\times (1,z')B^\times$ if and only if $\mathcal{O}^\times z = \mathcal{O}^\times z'$. In conclusion, if we denote by $\Gamma_0^\pm(D,N) = \phi_\infty(\mathcal{O}^\times)$, which is a discrete subgroup of $\text{GL}_2(\mathbb{R})$, then

$$Y_0(D,N) = \Gamma_0^\pm(D,N) \backslash \mathbb{P} = \Gamma_0(D,N) \backslash \mathfrak{H},$$

where $\mathfrak{H}$ is the classical upper half plane and $\Gamma_0(D,N)$ is the subgroup of matrices in $\Gamma_0^\pm(D,N)$ of determinant 1. This gives an analytic description of the curve $Y_0(D,N)$ as a Riemann surface. If $B = M_2(\mathbb{Q})$ is the usual matrix algebra (so that $D = 1$), curve $Y_0(1,N)$ is the classical open modular curve of level $N$ which can be compactified by adjoining a finite set of cusps. It is customary to write $X_0(N) := X_0(1,N)$ for the resulting compact Riemann surface. If $B$ is a division algebra (i.e., $D \neq 1$), then $Y_0(D,N)$ is already compact and we write $X_0(D,N) = Y_0(D,N)$.

Theorem 1.3.2. [66, Main Theorem I] The Riemann surface $X_0(D,N)$ admits a canonical complete non-singular algebraic model defined over $\mathbb{Q}$.

We refer to the rational model of the above theorem as Shimura’s canonical model and, by a standard abuse of notation, we continue to denote it by $X_0(D,N)/\mathbb{Q}$. To be precise, Shimura’s theorem asserts that there is an embedding of complex analytical varieties

$$j_{D,N} : X_0(D,N) \hookrightarrow \mathbb{P}^N_\mathbb{C}$$  

(1.3.9)
of the Riemann surface $X_0(D,N)$ into some complex projective space $\mathbb{P}^N_C$, $N \geq 1$, such that the image $j_{D,N}(X_0(D,N))$ admits a canonical smooth projective model over $\mathbb{Q}$. We indulge in the abuse of keeping the notation $X_0(D,N)$ for such a model.

**Remark 1.3.3.** We observe that $\mathbb{P}$ can be identified with the set of $\mathbb{R}$-algebra homomorphisms $\text{Hom}(\mathbb{C}, B_{\infty})$ in a natural way. Any $f \in \text{Hom}(\mathbb{C}, B_{\infty})$ gives rise to a group action of $\mathbb{C} \times$ on $\mathbb{P}$. There are exactly two fixed points $P^+$ and $P^-$ in $\mathbb{P}$ for such action. Let $P^+$ be the unique fixed point such that, for all $z \in \mathbb{C}$, $f(z) \left( \begin{array}{c} P^+ \\ 1 \end{array} \right) = z \left( \begin{array}{c} P^+ \\ 1 \end{array} \right)$ (respectively $f(z) \left( \begin{array}{c} P^- \\ 1 \end{array} \right) = \bar{z} \left( \begin{array}{c} P^- \\ 1 \end{array} \right)$).

This sets up a bijection

$$\text{Hom}(\mathbb{C}, B_{\infty}) \xrightarrow{\sim} \mathbb{P}$$

$$f \mapsto P^+.$$

Notice that $B^\times$ acts on $\text{Hom}(\mathbb{C}, B_{\infty})$ via conjugation.

Let us introduce now the moduli interpretation of Shimura curves $X_0(D,N)$.

**Definition 1.3.4.** By an abelian surface with quaternionic multiplication (QM) by $\mathcal{O}$ over a field $K$, we mean a pair $(A,i)$ where

i) $A/K$ is an abelian surface.

ii) $i : \mathcal{O} \hookrightarrow \text{End}(A)$ is an optimal embedding.

**Remark 1.3.5.** The optimality condition $i(B) \cap \text{End}(A) = i(\mathcal{O})$ is always satisfied when $\mathcal{O}$ is maximal.

**Definition 1.3.6.** Let $(A,i)$ be an abelian surface with QM by $\mathcal{O}$. Its ring of endomorphisms is

$$\text{End}(A,i) = \{ \phi \in \text{End}(A) : \phi \circ i(\alpha) = i(\alpha) \circ \phi \text{ for all } \alpha \in \mathcal{O} \}.$$ 

**Definition 1.3.7.** An isomorphism between abelian surfaces $(A,i)$ and $(A_0,i_0)$ with QM by $\mathcal{O}$ is an isomorphism $\phi : A \to A_0$ such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\phi} & A_0 \\ \downarrow{i(\beta)} & & \downarrow{i_0(\beta)} \\ A & \xrightarrow{\phi} & A_0 \end{array}$$

is commutative for all $\beta \in \mathcal{O}$.

Throughout, we shall denote by $[A,i]$ the isomorphism class of $(A,i)$.

Let $\phi_\infty$ be the fixed isomorphism of (1.3.8). Let $\tau \in \mathbb{P}$ and let $J \in \hat{\mathcal{O}}^\times \setminus \hat{B}^\times$ be a left $\mathcal{O}$-ideal. By means of $\phi_\infty$, we can identify $J$ as a $\mathcal{O}$-submodule in $M_2(\mathbb{R})$. Write $v_\tau = \left( \begin{array}{c} \tau \\ 1 \end{array} \right) \in \mathbb{C}^2$ and set $\Lambda_\tau = Jv_\tau$. Since $J \otimes \mathbb{R} = M_2(\mathbb{R})$ and $\tau \notin \mathbb{R}$, $\Lambda_\tau$ is a lattice in $\mathbb{C}^2$ endowed with a natural action of $\mathcal{O}$. The complex torus $\mathbb{C}^2/\Lambda_\tau$ admits natural polarizations, thus it defines an algebraic abelian surface $A_\tau$. Due to the fact that

$$\text{End}(A_\tau) = \{ \gamma \in M_2(\mathbb{C}) : \gamma \Lambda_\tau \subseteq \Lambda_\tau \},$$
there is a natural embedding \( i_r : \mathcal{O} \hookrightarrow \text{End}(A_r) \). Moreover, \( \mathcal{O} = \{ \beta \in B : \beta \Lambda_r \subseteq \Lambda_r \} \) by construction, hence the embedding \( i_r \) is optimal. We conclude that the pair \((A_r, i_r)\) defines an abelian surface with QM by \( \mathcal{O} \) over \( \mathbb{C} \).

Notice that, since \( \Lambda_r \) is a lattice in \( \mathbb{C}^2 \),

\[
B_{\infty}v_r = \Lambda_r \otimes \mathbb{R} \cong \mathbb{C}^2.
\]

This allows to endow \( B_{\infty} \) with a structure of right \( \mathbb{C} \)-vector space of dimension 2. Exploring the \( \mathbb{C} \)-vector subspace generated by \( 1 \in B_{\infty} \) one obtains a \( \mathbb{R} \)-algebra homomorphism \((f_r : \mathbb{C} \hookrightarrow B_{\infty}) \in \text{Hom}(\mathbb{C}, B_{\infty})\). More explicitly, we have that

\[
\Lambda_r \otimes \mathbb{R} \cong B_{\infty}v_r.
\]

Hence, the isomorphism \( B_{\infty} \cong \mathbb{C}^2 \) sends \( 1 \in B_{\infty} \) to \( v_r \), and the \( \mathbb{C} \)-vector subspace generated by \( 1 \in B_{\infty} \) corresponds to

\[
\mathbb{C}v_r \cong \{ \gamma \in B_{\infty} : \gamma v_r = zv_r \text{ for certain } z \in \mathbb{C} \} \subset B_{\infty}.
\]

This implies that \( f_r(z) \) is the unique matrix in \( B_{\infty} \) with eigenvector \( v_r \) and eigenvalue \( z \). Consequently, via the one-to-one correspondence \( \text{Hom}(\mathbb{C}, B_{\infty}) \xrightarrow{\sim} \mathbb{P} \) of Remark 1.3.3, \( f_r \) is sent to \( \tau \).

Reciprocally, let \((A, i)\) be an abelian surface with QM by \( \mathcal{O} \) over \( \mathbb{C} \). The embedding \( i \) equips \( H_1(A, \mathbb{Z}) \) with a structure of projective left \( \mathcal{O} \)-module of rank 1. Once fixed an isomorphism \( H_1(A, \mathbb{R}) \cong B_{\infty} \), the analytic structure of \( A \) yields an isomorphism \( H_1(A, \mathbb{R}) \cong \mathbb{C}^2 \) which, in turn, provides \( B_{\infty} \) with a structure of right \( \mathbb{C} \)-algebra, giving rise to an embedding \( f \in \text{Hom}(\mathbb{C}, B_{\infty}) \). Upon the identification \( B_{\infty} \cong H_1(A, \mathbb{R}) \), we may choose an isomorphism \( H_1(A, \mathbb{Q}) \cong B \). Thus \( H_1(A, \mathbb{Z}) \) can be regarded as a left \( \mathcal{O} \)-ideal \( H \) inside \( B \). Recall that the set of left \( \mathcal{O} \)-ideals inside \( B \) is in one-to-one correspondence with the set \( \hat{\mathcal{O}}^x \setminus \hat{B}^x \), hence every abelian surface \((A, i)\) with QM by \( \mathcal{O} \) provides an element \([\lfloor H \rfloor, f] \in \hat{\mathcal{O}}^x \setminus \hat{B}^x \times \mathbb{P} / B^x = Y_0(D, N) \) establishes a one-to-one correspondence

\[
Y_0(D, N) \overset{\sim}{\leftrightarrow} \left\{ \begin{array}{c}
\text{Abelian surfaces } (A, i)/\mathbb{C} \text{ with } \\
\text{quaternionic multiplication by } \mathcal{O}
\end{array} \right\} / \cong
\]

where the inverse map is given by \([J, \tau] \in \hat{\mathcal{O}}^x \setminus \hat{B}^x \times \mathbb{P} / B^x \mapsto [A_r, i_r] \).

The above discussion shows that the non-cuspidal \( \mathbb{C} \)-valued points of \( X_0(D, N) \) classify isomorphism classes of abelian surfaces with QM by \( \mathcal{O} \). Moreover, the Riemann surface \( X_0(D, N) \) comes equipped with a canonical model defined over \( \mathbb{Q} \). One can ask thus whether such canonical model solves a moduli problem in the category of \( \mathbb{Q} \)-schemes.

Extending the definition to arbitrary \( \mathbb{Q} \)-schemes \( S/\mathbb{Q} \), an abelian surface with QM by \( \mathcal{O} \) over \( S/\mathbb{Q} \) is a pair \((A, i)\) where

i) \( A/S \) is an abelian scheme of relative dimension 2 over \( S \).

ii) \( i : \mathcal{O} \hookrightarrow \text{End}_S(A) \) is an optimal embedding.

Analogously, an isomorphism between abelian surfaces \((A, i)/S, (A_0, i_0)/S\) is an isomorphism \( \varphi : A/S \to A_0/S \) of abelian schemes such that \( \varphi \circ i(\beta) = i_0(\beta) \circ \varphi \), for all \( \beta \in \mathcal{O} \).
Theorem 1.3.8. [13] Shimura’s canonical model $X_0(D,N)/\mathbb{Q}$ is the coarse moduli scheme associated to the moduli problem of classifying isomorphism classes of abelian surfaces with QM by $\mathcal{O}$ over an arbitrary $\mathbb{Q}$-scheme.

We will often describe points of the Shimura curve $X_0(D,N)$ by writing down the isomorphism class $P = [A,i] \in X_0(D,N)$ of the abelian surfaces with QM represented by them.

Remark 1.3.9. In most of the literature, the moduli problem claim to be solved by the Shimura curve $X_0(D,N)/\mathbb{Q}$ is that of classifying quadruples $(A, i, P, C)$ where $A/S$ is as above, $i : \mathcal{O}_0 \to \text{End}_S(A)$ is an embedding of a maximal order $\mathcal{O}_0$, $P$ is a compatible polarization and $C$ is a $\Gamma_0(N)$-structure (cf. [63] and Appendix A for precise definitions). By e.g. [64], there is a unique compatible polarization for any given triple $(A, i, C)$, hence one can remove polarizations from such moduli interpretation. The proof that both moduli problems are actually equivalent is sketched in Appendix A for the convenience of the reader.

By an isogeny between abelian surfaces $(A', i')$ and $(A, i)$ with QM by $\mathcal{O}$ we mean an isogeny $\lambda : A \to A'$ making, for all $\alpha \in \mathcal{O}$, the following diagram commutative:

$$
\begin{array}{ccc}
A & \xrightarrow{\lambda} & A' \\
\downarrow{i(\alpha)} & & \downarrow{i'(\alpha)} \\
A & \xrightarrow{\lambda} & A'.
\end{array}
$$

Write $\{A, i\}$ for the isogeny class of $[A, i]$.

Lemma 1.3.10. Let $I$ be a left $\mathcal{O}$-ideal, let $\tau \in \mathbb{P}$ and let $P = [A, i]$ be the point in $X(D,N)(\mathbb{C})$ represented by $(I, \tau)$. Then $\{A, i\} = j_{D,N}((\hat{\mathcal{O}}^\times \backslash \hat{B}^\times /\mathbb{Q}^\times \times \{\tau\})/B^\times) \subseteq X(D,N)(\mathbb{C})$.

Proof. First of all, we claim that there is a one-to-one correspondence between the isogenies $(A', i') \to (A, i)$ of degree $n^2$ and left ideals of $\mathcal{O}$ of norm $n$. Indeed, if we write $A \simeq \mathbb{C}^2/H_1(A, \mathbb{Z})$ and $A' \simeq \mathbb{C}^2/H_1(A', \mathbb{Z})$, giving an isogeny $A' \to A$ is equivalent to giving an inclusion $H_1(A', \mathbb{Z}) \subseteq H_1(A, \mathbb{Z}) \simeq \mathcal{O}$. The condition on the isogeny to be compatible with the action of $\mathcal{O}$ translates into the condition on $H_1(A', \mathbb{Z})$ to be a left $\mathcal{O}$-ideal. In addition, if the degree of the isogeny is $n^2$, then $\#\mathcal{O}/H_1(A', \mathbb{Z}) = n^2$ and therefore the norm of the $\mathcal{O}$-ideal $H_1(A', \mathbb{Z})$ is equal to $n$. This proves the claim.

Now, we observe that ideals of the form $k\mathcal{O}$ for some $k \in \mathbb{Z}$ give rise to isogenies $(A', i') \to (A, i)$ with $(A', i') \simeq (A, i)$, because they correspond to the isogenies ‘multiplication’ by $k$ in $(A, i)$. Since $\hat{\mathcal{O}}^\times \backslash \hat{B}^\times /\mathbb{Q}^\times$ is the set of all left ideals not contained in any proper ideal of the form $k\mathcal{O}$ with $k \in \mathbb{Z}$, we deduce that the orbit $(\hat{\mathcal{O}}^\times \backslash \hat{B}^\times /\mathbb{Q}^\times \times \{\tau\})/B^\times$ contains a representative for each $(A', i')$ which is isogenous to $(A, i)$.

1.4 Heegner points

Let $K$ be an imaginary quadratic field. There is a natural map from

$$
\text{Hom}(K, B) \to \text{Hom}(\mathbb{C}, B_\infty) \simeq \mathbb{P}
$$

given by extension of scalars. We say that a point $P \in X_0(D,N)(\mathbb{C})$ is a Heegner point associated to $K$ if $P \in j_{D,N}(\hat{\mathcal{O}}^\times \backslash \hat{B}^\times \times \mathbb{P}/B^\times)$ is the image of an element

$$
(g \times f) \in \hat{\mathcal{O}}^\times \backslash \hat{B}^\times \times \text{Hom}(K, B)/B^\times
$$


by the natural inclusion of $\text{Hom}(K,B)$ into $\mathbb{P}$ described in Remark 1.3.3.

Let $R$ be an order (not necessarily maximal) in $K$ and recall the natural injective map

$$\text{CM}_{D,N}(R) \hookrightarrow \hat{O}^x \backslash \hat{B}^x \times \text{Hom}(K,B)/B^x$$

of (1.2.2). We say that a point $P \in X_0(D,N)(\mathbb{C})$ is a Heegner point associated to $R$ if $P \in Y_0(D,N)$ is the image of an element $\varphi \in \text{CM}_{D,N}(R)$. We shall denote by $\text{CM}(R)$ the set of such Heegner points. By the theory of complex multiplication (cf. Theorem 1.4.2), we actually have $\text{CM}(R) \subset X_0(D,N)(K^{ab})$, where $K^{ab}/K$ is the maximal abelian extension of $K$. We shall denote the one-to-one correspondence between the set $\text{CM}(R)$ of Heegner points and the set $\text{CM}_{D,N}(R)$ of optimal embeddings by:

$$\varphi : \text{CM}(R) \xrightarrow{\sim} \text{CM}_{D,N}(R)$$

(1.4.10)

**Remark 1.4.1.** Recall that, if $p \mid DN$, the double coset $\mathcal{O}_p^x \backslash \mathcal{N}(\mathcal{O}_p)/\mathcal{Q}_p^x$ has exactly two elements. Since $\mathbb{Q}^x \hat{\mathbb{Z}}^x = \hat{\mathbb{Q}}^x$, because $h(\mathbb{Q}) = 1$, it follows that

$$\hat{O}^x \backslash \hat{B}^x / \mathbb{Q}^x = \hat{O}^x \backslash \hat{B}^x / \hat{\mathbb{Q}}^x = \prod_p \mathcal{O}_p^x \backslash \mathcal{B}_p^x / \mathcal{Q}_p^x.$$  

Thus

$$Y_0(D,N) = \hat{O}^x \backslash \hat{B}^x \times \mathbb{P} / B^x = (\prod_p \mathcal{O}_p^x \backslash \mathcal{B}_p^x / \mathcal{Q}_p^x) \times \mathbb{P} / B^x.$$  

There is also a natural action of the Atkin-Lehner group

$$W(D,N) = \prod_{p \mid DN} \mathcal{O}_p^x \backslash \mathcal{N}(\mathcal{O}_p)/\mathcal{Q}_p^x$$

on $Y_0(D,N)$ given by right multiplication on each double coset $\mathcal{O}_p^x \backslash \mathcal{B}_p^x / \mathcal{Q}_p^x$. Each automorphism $\omega_n \in W(D,N)$ is an involution on $Y_0(D,N)$ that can be extended to the whole $X_0(D,N)$. Moreover, for all $P = [A,i] \in Y_0(D,N)$ and all $\omega_n \in W(D,N)$,

$$\omega_n(P) = [A',i'] \in \{A,i\},$$

by Lemma 1.3.10. It is easy to check that for every $P \in \text{CM}(R)$,

$$\varphi(\omega_n(P)) = \omega_n(\varphi(P)),$$

where the action of $\omega_n$ on $\text{CM}_{D,N}(R)$ is the usual one described in §1.2.

Let $P = [A,i] \in X_0(D,N)(\mathbb{C})$ be a Heegner point associated to the imaginary quadratic field $K$ and let $f \in \text{Hom}(\mathbb{C}, B_\infty) \simeq \mathbb{P}$ be a representative of it in $Y_0(D,N)$. We have shown that $f : \mathbb{C} \hookrightarrow B_\infty$ arises from the analytic structure $B_\infty \simeq H_1(A, \mathbb{R}) \simeq \mathbb{C}^2$. Since $f$ is the extension of scalars of a suitable $\varphi \in \text{Hom}(K,B)$, such analytic structure is the extension of scalars of the isomorphism $H_1(A, \mathbb{Q}) \simeq B \simeq K^2$ provided by $\varphi$. We deduce that

$$\text{End}^0(A) = \{ \gamma \in M_2(\mathbb{C}) : \gamma H_1(A, \mathbb{Q}) \subset H_1(A, \mathbb{Q}) \} = \{ \gamma \in M_2(\mathbb{C}) : \gamma K^2 \subset K^2 \} = M_2(K).$$
The embedding $\varphi$ induces the isomorphism $B \otimes_{Q} K \cong M_{2}(K)$ of (1.2.4). Moreover, the monomorphism $B \hookrightarrow \text{End}^{0}(A)$ induced by $i$ is provided by the composition $B \hookrightarrow B \otimes_{Q} K \cong M_{2}(K)$. It follows that

$$\text{End}^{0}(A, i) = \{\gamma \in M_{2}(K) : \gamma i(\beta) = i(\beta)\gamma, \text{ for all } \beta \in B\} \simeq \{\beta \otimes \alpha \in B \otimes_{\mathbb{Z}} Q : \beta\beta' \otimes \alpha = \beta'\beta \otimes \alpha, \text{ for all } \beta' \in B\} = 1 \otimes K \simeq K.$$

Throughout, we shall fix the isomorphism $\psi : \text{End}^{0}(A, i) \cong K$ to be the canonical one provided by the right $K$-algebra structure of $B$ via $\varphi$. More precisely, upon the identification $B \simeq H_{1}(A, Q)$, the image $\psi(\alpha) \in K$ of any $\alpha \in \text{End}^{0}(A, i)$ satisfies

$$H_{1}(A, Q) \xrightarrow{\alpha^*} H_{1}(A, Q) \xrightarrow{\cong} B \xrightarrow{\beta} \beta \varphi(\psi(\alpha))$$

by Remark 1.2.2.

Let $P = [A, i] \in \text{CM}(R)$ and let $\varphi = \varphi(P) \in \text{Hom}(K, B)$ be an embedding associated with it. We have

$$\text{End}(A, i) = \{\alpha \in \text{End}^{0}(A, i) : \alpha^* H_{1}(A, \mathbb{Z}) \subseteq H_{1}(A, \mathbb{Z})\}.$$

Upon the above identifications $\text{End}^{0}(A) \simeq K$, $B \simeq H_{1}(A, Q)$, and regarding $H_{1}(A, \mathbb{Z})$ as a left $\mathcal{O}$-ideal in $B$ we deduce

$$\text{End}(A, i) \simeq \{\alpha \in K : H_{1}(A, \mathbb{Z}) \varphi(\alpha) \in H_{1}(A, \mathbb{Z})\} = K \cap \mathcal{O}^{*}(H_{1}(A, \mathbb{Z})) = R.$$

Indeed, this is a consequence of the optimality and due to the fact that, via the embedding $\text{CM}_{D, N}(R) \rightarrow \hat{\mathcal{O}}^{*} \backslash \hat{B}^{*} \times \text{Hom}(K, B) / B^{*}$ of (1.2.2), $\varphi(P)$ maps to the class $[H_{1}(A, \mathbb{Z}), \varphi]$.

The following theorem, known as Shimura’s reciprocity law, describes the field of definition of a Heegner point and the action of the Galois group over $K$ on it.

**Theorem 1.4.2.** [66, Main Theorem I] Let $P \in \text{CM}(R) \subset X_{0}(D, N)$.

(i) Let $H_{R}$ be the ring class field of $R$ and let $K(P)$ denote the extension of $K$ generated by the coordinates of $P$ at the model $X_{0}(D, N)/Q$, then $H_{R} = K(P)$.

(ii) (Shimura reciprocity law) Let $\text{Pic}(R) \xrightarrow{\Phi_{R}} \text{Gal}(H_{R}/K)$ be Artin’s reciprocity map of class field theory [73]. Then,

$$[J]^{-1} \ast \varphi(P) = \varphi(P^{\Phi_{R}([J])}),$$

for all $[J] \in \text{Pic}(R)$.

The theorem below determines the field of definition $\mathbb{Q}(P)$ of any $P \in \text{CM}(R)$ and describes the action of complex conjugation on $P$.

**Theorem 1.4.3.** [30, Lemma 5.10, Theorem 5.12] Assume that $DN$ is square free. Let $P \in \text{CM}(R) \subset X_{0}(D, N)(H_{R})$ for some order $R$ of conductor $c$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-c})$. Fix an embedding $H_{R} \subset \mathbb{C}$ and denote by $P \mapsto \overline{P}$ the complex conjugation on $\text{CM}(R)$. Then
Thus, for any $[a] \in \text{Pic}(R)$ such that
\[
\mathcal{P} = \omega_{m}(P^{\Phi_{R}(\mathcal{a})}),
\]
where
\[
m = \frac{DN}{\gcd(DN, c \cdot \text{disc}(K))}, \quad B \simeq \left(-s, m \cdot N_{K/Q}(a)\right).
\]

(iii) If $m \neq 1$ then $\mathbb{Q}(P) = H_{R}$. Otherwise, $[H_{R} : \mathbb{Q}(P)] = 2$ and $\mathbb{Q}(P) \subset H_{R}$ is the subfield fixed by the composition of complex conjugation with $\Phi_{R}(\mathcal{a})$.

**Remark 1.4.4.** As discussed in [30, §5], the class $[a] \in \text{Pic}(R)$ does depend on $P$. Assume that $[a] = [c]^{2}[b]$. Then exchanging $P$ with $Q = P^{\Phi_{R}(\mathcal{d})} \in \text{CM}(R)$ and $[a]$ with $[b]$ the above theorem applies. Indeed,
\[
\mathcal{Q} = P^{\Phi_{R}(\mathcal{d})} = \mathcal{P}^{\Phi_{R}(\mathcal{d})^{-1}} = \omega_{m}(P^{\Phi_{R}(\mathcal{a})})(\Phi_{R}(\mathcal{d})^{-1}) = \omega_{m}(P^{\Phi_{R}(\mathcal{b})}) = \omega_{m}(Q^{\Phi_{R}(\mathcal{b})}).
\]

Thus, for any $b$ verifying that $[a] \cdot [b]^{-1} \in \text{Pic}(R)^{2}$, there exists some $Q \in \text{CM}(R)$ such that $\mathcal{Q} = \omega_{m}(Q^{\Phi_{R}(\mathcal{b})})$.

Let $M_{R_{1}}$ be the isomorphism class of the field $\mathbb{Q}(P)$, for any $P \in \text{CM}(R_{1})$. Then $M_{R_{1}}$ is characterized by the class $\{a\} \in \text{Pic}(R)/\text{Pic}(R)^{2}$. It is clear that any ideal $b$ in $\{a\}$ satisfies the isomorphism $B \simeq \left(-D_{N_{K/Q}(b)}/\mathbb{Q}\right)$. In general, the converse is not true. However, if $[H_{R} : H_{R_{1}}]$ is odd, then $\{a\} \in \text{Pic}(R)/\text{Pic}(R)^{2}$ is uniquely determined by such isomorphism (see [30, Remark 5.11]).

For any optimal embedding $\varphi : R \hookrightarrow \mathcal{O}$, recall the decomposition $\mathcal{O} \simeq R \oplus eI$ of (1.2.5) induced by $\varphi$. The following proposition illustrates the moduli interpretation of Heegner points $P \in \text{CM}(R)$.

**Proposition 1.4.5.** Let $P = [A, i] \in \text{CM}(R)$ be a Heegner point. Let $\mathcal{O} \simeq R \oplus eI$ be the $R$-module structure induced by $\varphi(P) \in \text{CM}_{D, N}(R)$. Then $A \simeq E \oplus E_{I}$, where $E$ and $E_{I}$ are the isogenous CM elliptic curves $C/R$ and $C/I$, respectively. Moreover, $\text{End}(A)$ is the image of $\mathcal{O} \otimes_{\mathbb{Z}} R$ in $M_{2}(K) = \text{End}^{0}(A)$ via the isomorphism $B \otimes_{\mathbb{Q}} K \simeq M_{2}(K)$ of (1.2.4) provided by $\varphi(P)$, and $i$ corresponds to the natural embedding $i : \mathcal{O} \hookrightarrow \mathcal{O} \otimes_{\mathbb{Z}} R$.

**Proof.** Assume that $P \in Y_{0}(D, N)$ is the image of the class $[J, \varphi] \in \hat{O}^{\times} \backslash B^{\times} \otimes \text{Hom}(K, B)/B^{\times}$. Since $\hat{O}^{\times} \backslash B^{\times}/B^{\times} = 1$, we can assume without loss of generality that $J = \mathcal{O}$. Then the abelian surface $A/C \simeq \mathcal{O}^{2}/\mathcal{O}(\begin{pmatrix} \tau \\ 1 \end{pmatrix})$, where $\tau \in \mathbb{P}$ is such that $\varphi(\alpha)(\begin{pmatrix} \tau \\ 1 \end{pmatrix}) = \alpha(\begin{pmatrix} \tau \\ 1 \end{pmatrix})$, for all $\alpha \in K$. Write $v_{\tau} = (\begin{pmatrix} \tau \\ 1 \end{pmatrix})$. From the decomposition $\mathcal{O} \simeq \varphi(R) \oplus e\varphi(I)$ induced by $\varphi(P)$ we deduce that
\[
A \simeq \mathcal{O}^{2}/\mathcal{O}v_{\tau} \simeq \mathcal{O}^{2}/(\varphi(R) \oplus e\varphi(I))v_{\tau} = \mathcal{O}^{2}/(Rv_{\tau} \oplus Iev_{\tau}).
\]
Vectors $v_{\tau}$ and $ev_{\tau}$ must be $\mathbb{C}$-linearly independent given that $(Rv_{\tau} \oplus Iev_{\tau})$ is a lattice in $\mathbb{C}^{2}$, consequently, $A \simeq \mathcal{O}/\mathcal{R} \times \mathcal{C}/I$.

Finally, since $\text{End}^{0}(A) \simeq M_{2}(K) \simeq B \otimes_{\mathbb{Q}} K$,
\[
\text{End}(A) = \{\alpha \in \text{End}^{0}(A) : \alpha^{*}H_{1}(A, \mathcal{Z}) \subseteq H_{1}(A, \mathcal{Z})\} = \{\beta \otimes \gamma \in B \otimes_{\mathbb{Q}} K : (\beta \otimes \gamma)\mathcal{O} \subseteq \mathcal{O}\}.
\]
Moreover, due to the fact that $1 \otimes \gamma \in B \otimes_{\mathbb{Q}} K$ acts on $B \simeq H_1(A, \mathbb{Q})$ via right multiplication by $\gamma$ (cf. Remark 1.2.2), it follows that

$$\text{End}(A) = \{ \beta \otimes \gamma \in B \otimes_{\mathbb{Q}} K : \beta \mathcal{O} \gamma \subseteq \mathcal{O} \} = \mathcal{O} \otimes_{\mathbb{Z}} R.$$

□
Chapter 2

Ribet’s bimodules and reduction of Shimura curves

It follows from the work of various people, including Deligne and Rapoport, Buzzard, Morita, Čerednik and Drinfeld, that the Shimura curve $X_0(D,N)/\mathbb{Q}$ admits a proper integral model $X_0(D,N)$ over $\text{Spec}(\mathbb{Z})$, smooth over $\mathbb{Z}[1/ND]$ which suitably extends its moduli interpretation to arbitrary base schemes (cf.[54], [13]). When $p$ is a prime that divides $D$, sometimes we refer to its singular fiber $X_0(D,N) \times \text{Spec}(\mathbb{F}_p)$ as Čerednik-Drinfeld’s special fiber at $p$ ([16], [21]). If $q$ is a prime that divides $N$, we may refer to the special fiber $X_0(D,N) \times \text{Spec}(\mathbb{F}_q)$ as Deligne-Rapoport-Buzzard’s special fiber at $q$ ([19], [15]).

In this chapter we shall describe such special fibers, with special emphasis to their set of irreducible components and of singular points. In order to do so, we shall introduce Ribet’s notion of $(O,S)$-bimodule and relate it with certain supersingular points in the fiber. Finally, we shall explain how the specialization map works for an arbitrary prime $p$.

2.1 Bimodules: Ribet’s work

2.1.1 Admissible bimodules

Let $Z$ denote either $\mathbb{Z}$ or $\mathbb{Z}_p$ for some prime $p$. Let $O \subset B$ be an Eichler order and let $S \subset H$ be a maximal order, both over $Z$, in two possibly distinct quaternion algebras $B$ and $H$. By an $(O,S)$-bimodule $M$ we mean a free module of finite rank over $Z$ endowed with structures of left projective $O$-module and right (projective) $S$-module. For any $(O,S)$-bimodules $M$ and $N$, let us denote by $\text{Hom}_O^{S}(M,N)$ the set of $(O,S)$-bimodule homomorphisms from $M$ to $N$, i.e., $Z$-homomorphisms equivariant for the left action of $O$ and the right action of $S$. If $M = N$, we shall write $\text{End}_O^{S}(M)$ for $\text{Hom}_O^{S}(M,M)$.

Notice that, since $S$ is maximal, every right $S$-module $M$ verifies $O^r(M) = S$. Thus, since $S$ is Gorestein, all $S$-modules are projective. Note also that $(O,S)$-bimodules are naturally $O \otimes_S S$-modules.

Definition 2.1.1. Let $\Sigma$ denote the (possibly empty) set of prime numbers which ramify in both $O$ and $S$. For $p$ in $\Sigma$, let $\mathfrak{P}_O$ and $\mathfrak{P}_S$ denote the unique two-sided ideals of $O$ and $S$, respectively, of norm $p$. An $(O,S)$-bimodule $M$ is said to be admissible if $\mathfrak{P}_O M = M \mathfrak{P}_S$ for all $p \in \Sigma$. 

27
Remark 2.1.2. Let $\mathcal{M}$ be an $(\mathcal{O}, \mathcal{S})$-bimodule of rank $4n$ over $\mathcal{Z}$, for some $n \geq 1$. Since $\mathcal{M}$ is free over $\mathcal{Z}$, $\mathcal{M}$ is also free over $\mathcal{S}$ as right module, by [23]. Up to choosing an isomorphism between $\mathcal{M}$ and $\mathcal{S}^n$, there is a natural identification $\text{End}_\mathcal{S}(\mathcal{M}) \simeq M_n(\mathcal{S})$. Thus, giving a structure of left $\mathcal{O}$-module on $\mathcal{M}$ amounts to giving a homomorphism $f : \mathcal{O} \to M_n(\mathcal{S})$.

Since Eichler orders are Gorenstein, the $\mathcal{O}$-module $\mathcal{M}$ is projective if and only if $f$ is optimal. In particular, we conclude that the isomorphism class of an $(\mathcal{O}, \mathcal{S})$-bimodule $\mathcal{M}$ is completely determined by the $\text{GL}_n(\mathcal{S})$-conjugacy class of an optimal embedding $f : \mathcal{O} \to M_n(\mathcal{S})$. Finally, in terms of $f$, $\mathcal{M}$ is admissible if and only if $f(\mathfrak{P}_{\mathcal{O}}) = M_n(\mathfrak{P}_{\mathcal{S}})$ for all $p \in \Sigma$.

We now proceed to describe Ribet’s classification of -local and global- admissible bimodules. Let $p$ be a prime. Let $\mathcal{O}$ denote the maximal order in a quaternion division algebra $B$ over $\mathbb{Q}_p$. Let $\mathfrak{P} = \mathcal{O} \cdot \pi$ be the maximal ideal of $\mathcal{O}$ and let $\mathbb{F}_{p^n}$ be the residue field of $\mathfrak{P}$.

Theorem 2.1.3. [61, Theorem 1.2] Assume $\mathcal{Z} = \mathbb{Z}_p$, $B$ is division over $\mathbb{Q}_p$ and $\mathcal{O}$ is maximal in $B$. Let $\mathcal{M}$ be an admissible $(\mathcal{O}, \mathcal{O})$-bimodule of finite rank over $\mathbb{Z}_p$. Then

$$\mathcal{M} \cong \bigotimes_{r \text{ factors}} \mathcal{O} \times \cdots \times \bigotimes_{s \text{ factors}} \mathfrak{P} \times \cdots \times \mathfrak{P},$$

regarded as a bimodule via the natural action of $\mathcal{O}$ on $\mathcal{O}$ itself and on $\mathfrak{P}$ given by left and right multiplication. In that case, we say that a $(\mathcal{O}, \mathcal{O})$-bimodule $\mathcal{M}$ is of type $(r, s)$.

Using the above local description, Ribet classifies global bimodules of rank 8 over $\mathcal{Z}$ in terms of their algebra of endomorphisms, provided $\mathcal{O}$ is maximal. Hence, assume for the rest of this subsection that $\mathcal{Z} = \mathbb{Z}$ and, unless otherwise stated, $\mathcal{O}$ is maximal in $B$. Write $D_B = \text{disc}(B)$, $D_H = \text{disc}(H)$ for the reduced discriminants. Let $\mathcal{M}$ be an $(\mathcal{O}, \mathcal{S})$-bimodule of rank 8, set

$$D_0^M = \prod_{p \mid D_B D_H, p \notin \Sigma} \mathfrak{p}$$

and let $\mathcal{C}$ be the quaternion algebra over $\mathbb{Q}$ of reduced discriminant $D_0^M$. Note that the class of $\mathcal{C}$ in the Brauer group $\text{Br}(\mathbb{Q})$ of $\mathbb{Q}$ is the sum of the classes of the quaternion algebras $B$ and $H$.

We shall further assume for convenience that $D_0^M \neq 1$, i.e., $B \neq H$.

Proposition 2.1.4. [61, Proposition 2.1] $\text{End}_\mathcal{S}(\mathcal{M}) \otimes \mathbb{Q} \simeq \mathcal{C}$ and the ring $\text{End}_\mathcal{S}(\mathcal{M})$ is an Eichler order in $\mathcal{C}$ of level $\prod_k p_k$, where $p_k$ are the primes in $\Sigma$ such that $\mathcal{M}_{p_k}$ is of type $(1, 1)$.

Assume now that $\mathcal{O}$ and $\mathcal{S}$ are equipped with orientations. Namely, $o_p : \mathcal{O} \to \mathbb{F}_{p^2}$ and $\overline{o}_q : \mathcal{S} \to \mathbb{F}_{p^2}$, for all $p \mid D_B, q \mid D_H$. Let $\mathcal{M}$ be an $(\mathcal{O}, \mathcal{S})$-bimodule and let $p \mid D_0^M$ be such that (for example) $p \mid D_B$ and $p \nmid D_H$. Regard $\mathbb{F}_{p^2}$ as a right $\mathcal{O}$-module by means of $o_p : \mathcal{O} \to \mathbb{F}_{p^2}$, and consider the tensor product $\mathbb{F}_{p^2} \otimes_\mathcal{O} \mathcal{M}$. It is then an $(\mathbb{F}_{p^2}, \mathcal{S})$-bimodule, i.e., a left module over $\mathbb{F}_{p^2} \otimes \mathbb{Z}_p \simeq M_2(\mathbb{F}_{p^2})$. Since $\mathcal{S}$ is $\mathbb{Z}$-free of rank 8, $\mathbb{F}_{p^2} \otimes \mathcal{O} \mathcal{M}$ is a $\mathbb{F}_{p^2}$-vector space of dimension 2. Therefore, $M_2(\mathbb{F}_{p^2})$ is identified with a subalgebra of the algebra of $\mathbb{F}_{p^2}$-endomorphisms of $\mathbb{F}_{p^2} \otimes_\mathcal{O} \mathcal{M}$. Moreover, due to the fact that $\text{End}_{\mathbb{F}_{p^2}}^S(\mathbb{F}_{p^2} \otimes_\mathcal{O} \mathcal{M})$ is a set of $\mathbb{F}_{p^2}$-module endomorphisms, $\text{End}_{\mathbb{F}_{p^2}}^S(\mathbb{F}_{p^2} \otimes_\mathcal{O} \mathcal{M}) \subseteq M_2(\mathbb{F}_{p^2}) \simeq \mathbb{F}_{p^2} \otimes \mathbb{Z}_p \mathcal{S}$. We deduce then,

$$\text{End}_{\mathbb{F}_{p^2}}^S(\mathbb{F}_{p^2} \otimes_\mathcal{O} \mathcal{M}) = \{ \alpha \otimes s \in \mathbb{F}_{p^2} \otimes_\mathcal{O} \mathcal{S} : \alpha \beta \otimes s' = \beta \alpha \otimes s', \text{ for all } \beta \in \mathbb{F}_{p^2}, s' \in \mathcal{S} \} = \mathbb{F}_{p^2} \otimes 1.$$
The natural morphism \( \Lambda = \text{End}_S^D(\mathcal{M}) \to \text{End}_S^D(F_{p^2} \otimes \mathcal{O}) \) composed with the natural isomorphism \( F_{p^2} \otimes 1 \simeq F_{p^2}, \alpha \otimes 1 \mapsto \alpha \), provides an induced orientation \( \delta_p : \Lambda \to F_{p^2} \) for \( \Lambda \) at \( p \).

Analogously, we define a natural orientation for \( \Lambda \) at \( q \mid D_H, q \nmid D_B \).

Let \( N_0^\mathcal{M} \) be the product of the primes \( p \) in \( \Sigma \) such that \( \mathcal{M}_p \) is of type \((1,1)\). In order to endow \( \Lambda \) with structure of oriented Eichler order, we must define an orientation for each \( p \mid N_0^\mathcal{M} \). As above, regard \( F_{p^2} \) as a right \( \mathcal{O} \)-module by means of \( \delta_p : \mathcal{O} \to F_{p^2} \) and consider the \((F_{p^2},\mathcal{S})\)-bimodule \( \overline{\mathcal{M}} := F_{p^2} \otimes \mathcal{O} \). Since \( \mathcal{M}_p \) is of type \((1,1)\), \( \overline{\mathcal{M}} = \overline{\mathcal{M}}^{(1)} \oplus \overline{\mathcal{M}}^{(2)} \), where

\[
\overline{\mathcal{M}}^{(1)} = \{ m \in \overline{\mathcal{M}} : m \cdot s = o'(s)m, \text{ for all } s \in \mathcal{S} \},
\]

\[
\overline{\mathcal{M}}^{(2)} = \{ m \in \overline{\mathcal{M}} : m \cdot s = o'(s)^pm, \text{ for all } s \in \mathcal{S} \}.
\]

Let \( \mathcal{M}^{(1)}, \mathcal{M}^{(2)} \subset \mathcal{M} \) be the kernels of the maps \( \pi_2 : \mathcal{M} \to \overline{\mathcal{M}}^{(2)} \) and \( \pi_1 : \mathcal{M} \to \overline{\mathcal{M}}^{(1)} \), respectively. It is clear from the description above that each \( \mathcal{M}^{(i)} \) is \( \mathcal{O} \)- and \( \mathcal{S} \)-stable, hence it can be regarded as an \((\mathcal{O},\mathcal{S})\)-bimodule. Since \( \overline{\mathcal{M}}^{(1)} \) and \( \overline{\mathcal{M}}^{(2)} \) are \( F_{p^2} \)-vector spaces of dimension \( 1 \), the indexes \([\mathcal{M} : \mathcal{M}^{(i)}] = p^2\).

We claim that each endomorphism ring \( \Lambda^{(i)} := \text{End}_S^D(\mathcal{M}^{(i)}) \) is an Eichler order of level \( N/p \in \Lambda^0 = \text{End}_D^H(\mathcal{M}) \).

Indeed, since \( \mathcal{M}_q = \mathcal{M}_q^{(i)} \) for all \( q \neq p \), \( \Lambda_q^{(i)} = (\text{End}_S^D(\mathcal{M}))_q = \Lambda_q \).

Moreover, \( \mathcal{O}_p \simeq \mathcal{S}_p \) and \( \mathcal{M}_p \simeq \mathcal{O}_p \times \mathcal{O}_p \), hence it follows that \( \overline{\mathcal{M}} \simeq \mathcal{S}_p \times \mathcal{O}_p \times \mathcal{O}_p \). We deduce that \( \Lambda_p^{(1)} \simeq \mathcal{O}_p \times \mathcal{O}_p \) and \( \Lambda_p^{(2)} \simeq \mathcal{O}_p \times \mathcal{O}_p \). Thus both \( \Lambda_p^{(1)} \) and \( \Lambda_p^{(2)} \) are \((\mathcal{O}_p,\mathcal{O}_p)\)-bimodules of type \((2,0)\) and \((0,2)\), respectively. Hence \( \Lambda_p^{(1)} \) and \( \Lambda_p^{(2)} \) are maximal orders by Proposition 2.1.4 and the claim follows. Finally, since \( \Lambda = \Lambda^{(1)} \cap \Lambda^{(2)} \), the choice of \( \Lambda_p^{(1)} \) provides an orientation at \( p \mid N_0^\mathcal{M} \).

We have attached to the Eichler order \( \Lambda = \text{End}_S^D(\mathcal{M}) \) orientations in a natural way. The following theorem shows that the isomorphism class of \( \mathcal{M} \) is determined by the isomorphism class of \( \Lambda \), as oriented Eichler order.

**Theorem 2.1.5.** [61, Theorem 2.4] The map \( \mathcal{M} \mapsto \text{End}_S^D(\mathcal{M}) \) induces a one-to-one correspondence between the set of isomorphism classes of admissible rank-\( 8 \) bimodules of type \((r_p,s_p)\) at \( p \in \Sigma \), and the set \( \text{Pic}(D_0^M, N_0^M) \) of isomorphism classes of oriented Eichler orders.

The following theorem generalizes Ribet’s Theorem above to \((\mathcal{O},\mathcal{S})\)-bimodules where \( \mathcal{O} \) is an Eichler order in \( B \) of level \( N \), \((N,D_B D_H) = 1\), not necessarily maximal.

**Theorem 2.1.6.** Let \( \mathcal{O} \in \mathcal{E}(D_B,N) \) and \( \mathcal{S} \in \mathcal{E}(D_H,1) \), where \((N,D_B D_H) = 1\). Then, the map \( \mathcal{M} \mapsto \text{End}_S^D(\mathcal{M}) \) induces a one-to-one correspondence between the set of isomorphism classes of admissible \((\mathcal{O},\mathcal{S})\)-bimodules \( \mathcal{M} \) of rank \( 8 \) over \( \mathcal{O} \) and of type \((r_p,s_p)\) at \( p \in \Sigma \), and the set \( \text{Pic}(D_0^M, N_0^M) \) of isomorphism classes of oriented Eichler orders.

**Proof.** For any \( p \mid N \), let \( \overline{\mathcal{O}}_p \supseteq \mathcal{O}_p \) be the maximal order provided by the orientation of \( \mathcal{O} \) at \( p \). Write \( \overline{\mathcal{O}}_p = \mathcal{O}_p \) for all \( p \nmid N \) and set \( \mathcal{O}_0 = B \cap \prod_p \overline{\mathcal{O}}_p \). Furnished with the orientations inherited from those of \( \mathcal{O} \), \( \mathcal{O}_0 \) can be regarded as an element of \( \mathcal{E}(D_B,1) \). By means of the natural embedding \( \mathcal{O} \subseteq \mathcal{O}_0 \), \( \mathcal{O}_0 \) is a natural right \( \mathcal{O} \)-module. Hence, given any \((\mathcal{O},\mathcal{S})\)-bimodule \( \mathcal{M} \), we can consider the \((\mathcal{O}_0,\mathcal{S})\)-bimodule \( \mathcal{M}_0 := \mathcal{O}_0 \otimes \mathcal{O} \mathcal{M} \). By Theorem 2.1.5, \( \Lambda_0 := \text{End}_S^D(\mathcal{M}_0) \in \mathcal{E}(D_0^M, N_0^M) \).

Since \( \mathcal{O} = \mathcal{O}_1 \cap \mathcal{O}_0 \), where \( \mathcal{O}_1 \in \mathcal{E}(D_B,1) \), we have that

\[
\text{End}_S^D(\mathcal{M}) = \Lambda_0 \cap \Lambda_1 := \text{End}_S^D(\mathcal{M}_0) \cap \text{End}_S^D(\mathcal{M}_1),
\]
where } \mathcal{M} := \mathcal{O} \otimes \mathcal{O}. \text{ Thus } \Lambda := \text{End} \mathcal{S}(\mathcal{M}) \in \mathcal{E}(D^M_0, NN^M_0), \text{ endowed with the orientations at } p \mid N \text{ given by the choice of } \Lambda_0 \text{ (Notice that, since } \mathcal{S}_p \cong M_2(\mathbb{Z}_p), (\Lambda_0)_p = (\mathcal{O}_0)_p, (\Lambda_1)_p = (\mathcal{O}_1)_p \text{ and } \Lambda_p = \mathcal{O}_p). \text{ Finally, due to the fact that the orientation } \Lambda \subset \Lambda_0 \text{ is in correspondence with the orientation } \mathcal{O} \subset \mathcal{O}_0 \text{ and the map } \mathcal{M}_0 \rightarrow \Lambda_0 \text{ defines a one-to-one correspondence between the isomorphism classes of } (\mathcal{O}_0, \mathcal{S})\text{-bimodules and } \text{Pic}(D^M_0, NN^M_0), \text{ the desired result yields.}

\section*{2.1. Bimodules: Ribet’s Work}

\subsection*{2.1.2 \textit{p}-divisible groups and Dieudonné modules}

Let } S \text{ be an } \mathbb{F}_p\text{-scheme. The \textit{absolute Frobenius} of } S \text{ is the morphism of schemes } F_S : S \rightarrow S \text{ attached to the morphism of sheaves } F_S : \mathcal{O}_S \rightarrow \mathcal{O}_S \text{ that sends every section to its } p\text{th power. For any } S\text{-scheme } \pi : X \rightarrow S \text{ we have that } F_S \circ \pi = \pi \circ F_X. \text{ We denote by } X^{(p)} = X \times_S S \text{ its pull-back by } F_S.

\[
\begin{array}{c}
X \\
\downarrow \pi \\
S \\
\downarrow F_S \\
S^{(p)}
\end{array}
\]

Since } F_S \circ \pi = \pi \circ F_X, \text{ the pair } (F_X, \pi) \text{ induces a morphism of } S\text{-schemes}

\[F_{X/S} : X \rightarrow X^{(p)}\]

called the \textit{relative Frobenius} of } X \text{ over } S \text{ (Notice that } q \circ F_{X/S} = F_X). \text{ If } S = \text{Spec}(K) \text{ where } K \text{ is a perfect field, } F_S \text{ is an isomorphism, thus } q : X^{(p)} \rightarrow X \text{ is also an isomorphism.}

Fix a base scheme } S. \text{ Let } \pi : G \rightarrow S \text{ be a commutative group scheme and let } n \in \mathbb{Z}^+. \text{ Let } G[n] \text{ denote the kernel } \text{Ker}(n_G : G \rightarrow G), \text{ where } n_G \text{ is the multiplication by } n \text{ morphism.}

\begin{definition}
Let } \mathcal{C}_S^f \text{ be the category of flat finite commutative group schemes over } S \text{ whose ranks are powers of } p. \text{ A } \text{\textit{p}-divisible group is an object in the category } \mathcal{C}_S \text{ of formal inductive limits in } \mathcal{C}_S:\n
\[G = \lim_{\rightarrow} n G_n\]

satisfying

(i) } G_n = G_{n+1}[p^n] \text{ for each } n.

(ii) } p_G \text{ is an epimorphism.}

An isogeny of } \text{\textit{p}-divisible groups } \varphi : G \rightarrow G' \text{ is an epimorphism with finite kernel.}

The relative Frobenius } F_{G_n/S} : G_n \rightarrow G_n^{(p)} \text{ induces an isogeny } F_{G/S} : G \rightarrow G^{(p)}. \text{ Its dual isogeny } V_{G/S} : G^{(p)} \rightarrow G \text{ is called the Verschiebung morphism. It satisfies } V_{G/S} \circ F_{G/S} = p_G \text{ and } F_{G/S} \circ V_{G/S} = p_G^{(p)}.

For any abelian scheme } X \text{ over } S, \text{ set}

\[X[p^\infty] = \lim_{\rightarrow} n X[p^n]\]

It is a } \mathbb{Z}_p\text{-module that clearly verifies the above conditions. It will be so called the } \text{\textit{p}-divisible group attached to } X.

Let } \varphi : X \rightarrow Y \text{ be an isogeny of } S\text{-abelian schemes. Then, it is easy to check that } \varphi \text{ induces an isogeny of } \text{\textit{p}-divisible groups } \hat{\varphi} : X[p^\infty] \rightarrow Y[p^\infty] \text{ in a natural way.}
Definition 2.1.8. Let \( K \) a perfect field of characteristic \( p \). The ring of (infinite) Witt vectors of \( K \), \( W = W(K) \), is the unique complete discrete valuation ring with maximal ideal \( (p) \) such that \( W/pW \cong K \).

There is a way to express Witt vectors as sequences in \( K \) such that, for all \( u = (u_0, u_1, \ldots) \), \( v = (v_0, v_1, \ldots) \) ∈ \( W \) (\( u_i, v_i \in K \)),

\[
    u + v = (\phi_0, \phi_1, \ldots), \quad uv = (\psi_0, \psi_1, \ldots),
\]

where \( \phi_n \) and \( \psi_n \) are polynomials in \( u_0, \ldots, u_n, v_0, \ldots, v_n \) for each \( n \). Furthermore, one can check that the absolute Frobenius of \( K \) can be uniquely lifted to an endomorphism \( \sigma \) of \( W \). Namely,

\[
    u^\sigma = (u_0^p, u_1^p, \ldots), \quad pu = (0, u_0^p, u_1^p, \ldots).
\]

Polynomials \( \phi_i, \psi_i \) define an addition and a product on the \( n \)-dimensional affine space \( \mathbb{A}_K^n \) for each \( n \). In such a way, \( \mathbb{A}_K^n \) is endowed with a ring scheme structure, denoted by \( W_n \).

The Witt scheme over \( K \) is formal ring scheme \( W := \lim_n W_n \). The multiplication map of \( W \) will be denoted by \( \mu : W \times W \to W \). Notice that the set of \( K \)-rational points of \( W \) corresponds to \( W \cong W(K) \), as a ring.

For any \( G \in \mathfrak{C}_{\text{Spec}(K)} \), write

\[
    D(G) = \text{Hom}_K(G, W).
\]

The group \( D(G) \) acquires structure of \( W \)-module by means of \( \mu \). Namely,

\[
    W \times D(G) \to D(G) \quad (a : \text{Spec}K \to W, m : G \to W) \mapsto am : G \cong \text{Spec}(K) \times G \to W \times W \overset{\mu}{\to} W.
\]

The relative Frobenius and Verschiebung of \( G \) induce \( W \)-semilinear endomorphisms \( F \) and \( V \) on \( D(G) \), respectively,

\[
    F(ax) = a^p F(x), \quad V(ax) = a^{p^{-1}} V(x) \quad \text{(for all } a \in W, x \in D(G))
\]

and \( F \circ V = V \circ F = p \cdot \text{id}_{D(G)} \).

(Notice that \( F_{G/K} : G \to G^{(p)} \) induces a \( W \)-linear map \( D(G^{(p)}) \to D(G) \), which is equivalent to a \( W \)-semilinear map \( F : D(G) \to D(G) \) above.)

Definition 2.1.9. Let \( X \) be an abelian variety of dimension \( g \) over \( K \), we denote by the Dieudonné module of \( X \) the \( W \)-module \( D = D(X[p^\infty]) \). It is a free \( W \)-module of rank \( 2g \).

Since every isogeny in \( \text{End}(X) \) induces an isogeny on \( X[p^\infty] \), the group \( \text{End}(X) \) acts on \( D \) on the right. Moreover, \( X[p^\infty] \) is furnished with a natural \( \mathbb{Z}_p \)-module structure. Hence, in fact, \( D \) has a right \( \text{End}(X) \otimes \mathbb{Z}_p \)-action.

2.1.3 Supersingular surfaces and bimodules

Let \( p \) be a prime and let \( \mathbb{F} \) be a fixed algebraic closure of \( \mathbb{F}_p \). An abelian surface \( \tilde{A}/\mathbb{F} \) is supersingular if it is isogenous to a product of supersingular elliptic curves over \( \mathbb{F} \). Given a supersingular abelian surface \( \tilde{A} \), one defines Oort’s invariant \( a(\tilde{A}) \) as follows. If \( \tilde{A} \) is isomorphic to a product of supersingular elliptic curves, set \( a(\tilde{A}) = 2 \); otherwise set \( a(\tilde{A}) = 1 \) (see [45, Chapter 1] for an alternative definition of this invariant).
Let \( B \) be an indefinite quaternion algebra over \( \mathbb{Q} \) of reduced discriminant \( D \). Let \( N \geq 1 \) be an integer such that \((N, pD) = 1\) and let \( \mathcal{O} \in \mathcal{E}(D, N) \).

In this subsection we shall consider supersingular abelian surfaces \((\tilde{A}, \tilde{i})\) with QM by \( \mathcal{O} \) over \( \mathbb{F} \). The following theorem describes those whose Oort’s invariant is 2.

**Theorem 2.1.10.** [69, Theorem 3.5] [57, Theorem 6.2] Let \( \tilde{A}/\mathbb{F} \) be a supersingular abelian surface such that \( a(\tilde{A}) = 2 \). Then \( \tilde{A} \cong \tilde{E} \times \tilde{E} \), where \( \tilde{E} \) is any fixed supersingular elliptic curve over \( \mathbb{F} \).

Assume that \((\tilde{A}, \tilde{i})\) is such that \( \tilde{A} \cong \tilde{E}^2 \) as in the above theorem. Let us denote by \( \mathcal{S} = \text{End}(\tilde{E}) \) the endomorphism ring of \( \tilde{E} \). According to a well known theorem of Deuring [20], \( \mathcal{S} \) is a maximal order in the quaternion algebra \( H = \mathcal{S} \otimes \mathbb{Q} \), which is definite of discriminant \( p \). Therefore, giving such an abelian surface \((\tilde{A}, \tilde{i})\) with QM by \( \mathcal{O} \) is equivalent to providing an optimal embedding
\[
\tilde{i} : \mathcal{O} \longrightarrow \text{M}_2(\mathcal{S}) \cong \text{End}(\tilde{A}),
\]
or, thanks to Remark 2.1.2, an \((\mathcal{O}, \mathcal{S})\)-bimodule \( \mathcal{M} \) of rank 8 over \( \mathbb{Z} \).

**Remark 2.1.11.** The maximal order \( \mathcal{S} \) comes equipped with a natural orientation at \( p \), and therefore can be regarded as an element of \( \mathcal{E}(p, 1) \). Indeed, let \( \mathcal{D}(\tilde{E}) \) be the Dieudonné module of \( \tilde{E} \), so that \( \mathcal{D}(\tilde{E}) \) is a free \( W(\mathbb{F}) \)-module of rank 2. The space \( \mathcal{D}(\tilde{E})/\mathcal{F}\mathcal{D}(\tilde{E}) \) is a \( \mathbb{F} \)-vector space of dimension 1. The functorial action of \( \mathcal{S} \) on this vector space is thus described by a character \( \kappa : \mathcal{S} \rightarrow \mathbb{F} \). Its image is necessarily the subfield \( \mathbb{F}_p^\alpha \) of \( \mathbb{F} \) of cardinality \( p^2 \). Thus \( \mathcal{S} \) is canonically oriented.

Let \( \mathcal{M} = \mathcal{M}_{(\tilde{A}, \tilde{i})} \) be the bimodule attached to a pair \((\tilde{A}, \tilde{i})\) with \( a(\tilde{A}) = 2 \) by the above construction. Then
\[
\text{End}^S(\mathcal{M}) \simeq \{ \gamma \in \text{M}_2(\mathcal{S}) \simeq \text{End}(\tilde{A}) \mid \gamma \circ \tilde{i}(\alpha) = \tilde{i}(\alpha) \circ \gamma, \text{ for all } \alpha \in \mathcal{O} \} = \text{End}(\tilde{A}, \tilde{i}). \quad (2.1.1)
\]

For any supersingular abelian surface \((\tilde{A}, \tilde{i})\) with QM by \( \mathcal{O} \), let \( \mathcal{D} \) be the Dieudonné module associated to the \( p \)-divisible group of \( \tilde{A} \). Thus \( \mathcal{D} \) is a free rank-4 module over \( W = W(\mathbb{F}) \). Recall that this module is furnished with an induced right-action of \( \mathcal{O} \). So the tensor product \( \mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p \) acts naturally on \( \mathcal{D} \) on the right.

Consider the submodules \( \mathcal{F}\mathcal{D} \) and \( \mathcal{V}\mathcal{D} \) of \( \mathcal{D} \), and denote by \((\mathcal{F}, \mathcal{V})\mathcal{D}\) their sum. These modules contain \( p\mathcal{D} = \mathcal{F}\mathcal{V}\mathcal{D} \), so the quotients \( \mathcal{D}/\mathcal{F}\mathcal{D}, \mathcal{D}/\mathcal{V}\mathcal{D}, \mathcal{D}/(\mathcal{F}, \mathcal{V})\mathcal{D} \) are naturally \( \mathbb{F} \)-vector spaces. Write \( \alpha_p \) for the usual inseparable group scheme of rank \( p \) attached to the dimension 0 algebra \( \mathbb{F}_p[x]/(x^p - 1) \).

**Lemma 2.1.12.** [61, §4] We have
\[
a(\tilde{A}) = \dim_{\mathbb{F}}(\text{Hom}(\alpha_p, \tilde{A})) = \dim_{\mathbb{F}}(\mathcal{D}/(\mathcal{F}, \mathcal{V})\mathcal{D}),
\]
\[
\dim_{\mathbb{F}}(\mathcal{D}/\mathcal{F}\mathcal{D}) = 2 \quad \dim_{\mathbb{F}}(\mathcal{D}/\mathcal{V}\mathcal{D}) = 2.
\]

At this point, let us assume that \( p \mid D \). We will give a classification of all abelian surfaces over \( \mathbb{F} \) with QM by \( \mathcal{O} \), with special emphasis on those which are supersingular and have Oort’s invariant equal to 2. If this is the case, we will give an interpretation of some attributes of the attached \((\mathcal{O}, \mathcal{S})\)-bimodule.

**Lemma 2.1.13.** [61, Lemma 4.1] Let \((\tilde{A}, \tilde{i})\) be an abelian surface with QM by \( \mathcal{O} \in \mathcal{E}(D, N) \) over \( \mathbb{F} \) and assume that \( p \mid D \). Then \( \tilde{A} \) is supersingular.
Notice that the ring $\mathcal{O}_p$ is a maximal order in a quaternion division algebra over $\mathbb{Q}_p$. Let $\mathfrak{P}$ be the maximal ideal of $\mathcal{O}_p$.

**Definition 2.1.14.** An abelian surface $(\tilde{A}, \tilde{i})$ with QM by $\mathcal{O}$ is said to be *exceptional* if the action of $\mathcal{O}_p/p\mathcal{O}_p$ on $\mathcal{D}/F\mathcal{D}$ factors through the quotient $\mathcal{O}_p/\mathfrak{P}$.

**Proposition 2.1.15.** [61, Proposition 4.2] Suppose that $(\tilde{A}, \tilde{i})$ is exceptional. Then $a(\tilde{A}) = 2$.

Recall that $\mathcal{O}_p/p\mathcal{O}_p$ is a $\mathbb{F}_{p^2}$-vector space of dimension 2. As such, there is a natural embedding $\mathbb{F}_{p^2} \rightarrow \mathcal{O}_p/p\mathcal{O}_p$. Consider the action of the submodule $\mathbb{F}_{p^2}$ of $\mathcal{O}_p/p\mathcal{O}_p$ on the 2 dimensional $\mathbb{F}$-vector space $L = \mathcal{D}/F\mathcal{D}$. Letting $\sigma$ and $\tau$ be the two embedding $\mathbb{F}_{p^2} \hookrightarrow \mathbb{F}$, we find a canonical decomposition of $\mathbb{F}$-vector spaces $L = L_\sigma \oplus L_\tau$, where

$$L_\sigma = \{ t \in L : at = \sigma(a)t \text{ for all } a \in \mathbb{F}_{p^2} \}.$$ 

And similarly for $L_\tau$. (Strictly speaking, the action of $\mathbb{F}_{p^2}$ is on the right but we write it on the left because $\mathbb{F}_{p^2}$ is commutative).

**Definition 2.1.16.** An abelian surface $(\tilde{A}, \tilde{i})$ with QM by $\mathcal{O}$ is said to be *mixed* if the two spaces $L_\sigma$ and $L_\tau$ are non-zero. An abelian surface $(\tilde{A}, \tilde{i})$ with QM is *pure of type $\sigma$* if $L_\sigma$ is 2-dimensional and $L_\tau$ is zero. Respectively, $(\tilde{A}, \tilde{i})$ is *pure of type $\tau$* if $L_\tau$ is 2-dimensional and $L_\sigma$ is zero.

**Proposition 2.1.17.** [61, Proposition 4.3] All pure abelian surfaces with QM are exceptional.

**Remark 2.1.18.** Assume that $(\tilde{A}, \tilde{i})$ is exceptional. Since $a(\tilde{A}) = 2$ we can consider its attached bimodule $\mathcal{M} = \mathcal{M}(\tilde{A}, \tilde{i})$. Let $\mathcal{D}$ be the Dieudonné module associated to the $p$-divisible group of $\tilde{A}$. The fact that $(\tilde{A}, \tilde{i})$ is exceptional implies $\mathcal{D}\mathfrak{P} = F\mathcal{D}$. The relative Frobenius $F_{\tilde{A}/\mathbb{F}}$ generates the maximal ideal $\mathfrak{P}_S$ of $\mathcal{S}$, hence we deduce that $\mathfrak{P}_S\mathcal{M} = \mathcal{M}\mathfrak{P}_S$, that is $\mathcal{M}$ is admissible.

Let $\sigma_p : \mathcal{O} \rightarrow \mathbb{F}_{p^2}$ and $\sigma'_p : \mathcal{S} \rightarrow \mathbb{F}_{p^2}$ be the orientations of $\mathcal{O}$ and $\mathcal{S}$ at $p$. Write $\mathcal{M} = \mathbb{F}_{p^2} \otimes \mathcal{O}\mathcal{M}$ and $\mathcal{M}^1 = \{ m \in \mathcal{M} : m \cdot s = \sigma'(s)m, \text{ for all } s \in \mathcal{S} \}$, $\mathcal{M}^2 = \{ m \in \mathcal{M} : m \cdot s = \sigma'(s)^p m, \text{ for all } s \in \mathcal{S} \}$, as in §2.1.1. Let $\mathcal{L} = \mathcal{D}/F\mathcal{D}$ as above. Once we identify $\mathcal{S}/\mathfrak{P}_S$ with $\mathbb{F}_{p^2} \subset \mathbb{F}$ by means of $\sigma'_p$ and assume that the composition $\mathcal{O}/\mathfrak{P}_S$ $\mathbb{F}_{p^2}$ $\subset \mathbb{F}$ correspond to $\sigma$, we easily check that

$$\text{dim}_F(\mathcal{L}_\sigma) = \text{dim}_{\mathbb{F}_{p^2}}(\mathcal{M}^1), \quad \text{dim}_F(\mathcal{L}_\tau) = \text{dim}_{\mathbb{F}_{p^2}}(\mathcal{M}^2).$$

By the discussion of §2.1.1, we deduce that $(\tilde{A}, \tilde{i})$ is mixed exceptional if and only if $\mathcal{M}$ is admissible of type $(1, 1)$. Reciprocally, $(\tilde{A}, \tilde{i})$ is pure of type $\sigma$ (respectively, of type $\tau$) if and only if $\mathcal{M}$ is admissible of type $(2, 0)$ (respectively, of type $(0, 2)$).

The following proposition links the above definitions with the number of $\mathcal{O}$-stable subgroups of $\tilde{A}$ isomorphic to $\sigma_p$.

**Proposition 2.1.19.** [61, Proposition 4.4, Proposition 4.5, Proposition 4.6]

(i) Suppose that $(\tilde{A}, \tilde{i})$ is mixed. If $(\tilde{A}, \tilde{i})$ is exceptional, then $\tilde{A}$ has precisely two $\mathcal{O}$-stable subgroups isomorphic to $\sigma_p$. If $(\tilde{A}, \tilde{i})$ is not exceptional, then $\tilde{A}$ has precisely one such subgroup.
(ii) Suppose that \( \tilde{A}, \tilde{i} \) is pure. Then all subgroups of \( \tilde{A} \) isomorphic to \( \alpha_p \) are \( \mathcal{O} \)-stable. Moreover, such subgroups are in 1-1 correspondence with points of the 1-dimensional projective space \( \mathbb{P}(L) \), which has a canonical structure over \( \mathbb{F}_p \).

Let us consider triples \( (\tilde{A}, \tilde{i}, H) \), where \( (\tilde{A}, \tilde{i}) \) is an abelian surface with QM by \( \mathcal{O} \) and \( H \) is an \( \mathcal{O} \)-stable subgroup scheme of \( \tilde{A} \) isomorphic to \( \alpha_p \). Given such a triple \( (\tilde{A}, \tilde{i}, H) \) write \( \tilde{B} = \tilde{A}/H \) and let \( \tilde{j} : \mathcal{O} \to \text{End}(\tilde{B}) \) be the monomorphism provided by the induced action of \( \mathcal{O} \) on the quotient \( \tilde{A}/H \) (Notice that \( H \) is \( \mathcal{O} \)-stable thus any morphism \( \tilde{i}(\alpha) \), \( \alpha \in \mathcal{O} \), induces a morphism \( \tilde{j}(\alpha) \) in \( \text{End}(\tilde{A}/H) \)). We endow to the pair \( (\tilde{B}, \tilde{j}) \) with the subgroup \( I = \tilde{A}[F_{\tilde{A}/\mathbb{F}}]/H \), where \( \tilde{A}[F_{\tilde{A}/\mathbb{F}}] \) is the kernel of the relative Frobenius.

**Lemma 2.1.20.** [61, Lemma 4.8] The group \( I \) is \( \mathcal{O} \)-stable and isomorphic to \( \alpha_p \).

Let us denote by \( \Theta \) the operator constructed above that maps a triple \( (\tilde{A}, \tilde{i}, H) \) to \( (\tilde{B} = \tilde{A}/H, \tilde{j} = I = \tilde{A}[F_{\tilde{A}/\mathbb{F}}]/H) \). It is clear that it satisfies \( \Theta(\Theta(\tilde{A}, \tilde{i}, H)) = (\tilde{A}, \tilde{i}, H)(p) \).

**Theorem 2.21.** [61, Theorem 4.9] The restriction of \( \Theta \) to the set of triples \( (\tilde{A}, \tilde{i}, H) \) with \( (\tilde{A}, \tilde{i}) \) pure (respectively, mixed) induces a one-to-one correspondence between the set of isomorphism classes of such triples and the set of isomorphism classes of triples \( (\tilde{A}, \tilde{i}, H) \) with \( (\tilde{A}, \tilde{i}) \) mixed (respectively, pure).

### 2.2 Čerednik-Drinfeld’s special fiber

In this section we shall describe the special fiber \( \tilde{X}_0(D, N) = \mathcal{X}_0(D, N) \times \text{Spec}(\mathbb{F}_p) \) at \( p \mid D \) in terms of exceptional pairs. Let \( \mathcal{O} \in \mathcal{E}(D, N) \) and let \( T \) be any base scheme. An abelian surface \( (A, i) \) over \( T \) with QM by \( \mathcal{O} \) is said to be special if the map \( i \) satisfies the condition

\[
\text{Trace}_{\mathcal{O}_T}(i(\alpha) \mid \text{Lie}(A)) = \text{Tr}(\alpha) \in \mathbb{Z}
\]

for all \( \alpha \in \mathcal{O} \), where \( \text{Tr} \) is the reduced trace in \( B = \mathcal{O}^{0} \). This condition is automatically satisfied when \( D \) is invertible in \( T \) because \( B \otimes \mathcal{O}_T \) is in a matrix algebra and \( \text{Lie}(A) \) is a 2-dimensional \( \mathcal{O}_T \)-module. In characteristic \( p \mid D \) every abelian surface with QM by \( \mathcal{O} \) is supersingular by Lemma 2.1.13. We claim that \( (\tilde{A}, \tilde{i}) \) is special if and only if it is mixed. Indeed, if \( T = \text{Spec}(\mathbb{F}) \), where \( \mathbb{F} \) is a algebraic closure of \( \mathbb{F}_p \), we can identify \( \text{Lie}(\tilde{A}) \) with the 2-dimensional \( \mathbb{F} \)-vector space \( \mathcal{L} = \mathcal{D}/\mathcal{F}\mathcal{D} = \mathcal{L}_r \oplus \mathcal{L}_s \). In case \( (\tilde{A}, \tilde{i}) \) mixed, we can choose \( \{e_\sigma \in \mathcal{L}_s, e_\tau \in \mathcal{L}_r\} \) to be a basis for \( \mathcal{L} \). It is clear that \( \alpha e_\sigma \in \sigma(\alpha_p(\alpha))e_\sigma + \mathbb{F}e_\tau \), \( \alpha e_\tau \in \tau(\alpha_p(\alpha))e_\tau + \mathbb{F}e_\sigma \) for all \( \alpha \in \mathcal{O} \), where \( \alpha_p \) stands for its orientation at \( p \), hence

\[
\text{Trace}_{\mathcal{O}_T}(i(\alpha)) = \sigma(\alpha_p(\alpha)) + \tau(\alpha_p(\alpha)) = \text{Tr}(\alpha) \mod p.
\]

In case \( (\tilde{A}, \tilde{i}) \) pure we obtain \( \text{Trace}_{\mathcal{O}_T}(i(\alpha)) = 2\sigma(\alpha_p(\alpha)) \) or \( 2\tau(\alpha_p(\alpha)) \).

We can see in [54] and [13] that Morita’s integral model \( \mathcal{X}_0(D, N)/\mathbb{Z} \) is characterized as the coarse moduli space which classifies special abelian surfaces with QM by \( \mathcal{O} \). As such, points in \( \tilde{X}_0(D, N)(\mathbb{F}) \) parameterize mixed supersingular abelian surfaces \( (\tilde{A}, \tilde{i}) \) over \( \mathbb{F} \) with QM by \( \mathcal{O} \).

Assume that \( (\tilde{A}, \tilde{i}) \) is mixed non-exceptional. By Proposition 2.1.19, \( \tilde{A} \) has a unique \( \mathcal{O} \)-stable subgroup \( H \) isomorphic to \( \alpha_p \), hence it has a unique attached triple \( (\tilde{A}, \tilde{i}, H) \). By means of the map \( \Theta \) of Theorem 2.1.21, such triple maps to \( (\tilde{B}, \tilde{j}, I) \), where \( (\tilde{B}, \tilde{j}) \) is pure. Write \( S_{(\tilde{B}, \tilde{j})} \)
for the set of isomorphism classes of mixed triples $[\tilde{A}', \tilde{\gamma}', H']$ such that $\Theta(\tilde{A}', \tilde{\gamma}', H') = (\tilde{B}, \tilde{\gamma}, I')$, for a suitable subgroup scheme $I'$. By Proposition 2.1.19 and Theorem 2.1.21, $S_{(\tilde{B}, \tilde{\gamma})}$ is in one-to-one correspondence with a 1-dimensional projective space with a canonical structure over $\mathbb{F}_p$. By Proposition 2.1.19, the natural map

$$\bigcup S_{(\tilde{B}, \tilde{\gamma})} \longrightarrow \tilde{X}_0(D, N)(\mathbb{F}),$$

$$[\tilde{A}, \tilde{\gamma}, H] \longrightarrow \mathcal{P} = [\tilde{A}, \tilde{\gamma}]$$

is one-to-one except when $(\tilde{A}, \tilde{\gamma})$ is mixed exceptional, which in such case is two-to-one. The fact that triples in $S_{(\tilde{B}, \tilde{\gamma})}$ are parameterized by points in $\mathbb{P}^1(\mathbb{F})$ regards $\tilde{X}_0(D, N)(\mathbb{F})$ as an union of projective lines meeting at mixed exceptional points. Therefore, the set of irreducible components (respectively singular points) is in one-to-one correspondence with the set of isomorphism classes of pure (respectively mixed exceptional) abelian surfaces with QM by $\mathcal{O}$. By Remark 2.1.18, the isomorphism class $[\tilde{A}, \tilde{\gamma}]$ of a pure abelian surface with QM of type $\sigma$ (respectively $\tau$) is characterized by the isomorphism class of its attached $(\mathcal{O}, \mathcal{S})$-bimodule, which is admissible of type $(2, 0)$ (respectively of type $(0, 2)$) at $p$. Thus by Theorem 2.1.6, the set of irreducible components is in one-to-one correspondence with two copies of $\text{Pic}(D/p, N)$. In turn, the set of mixed exceptional abelian surfaces with quaternionic multiplication by $\mathcal{O}$ is in bijective correspondence with $\text{Pic}(D/p, Np)$ since their attached bimodules are admissible of type $(1, 1)$ at $p$.

By the work of Čerednik and Drinfeld [16] [21], the special fiber $\tilde{X}_0(D, N)$ is reduced and semi-stable, thus singular points are ordinary double points. The following theorem summarizes the above description of such fiber and gives a recipe to compute the thickness of its singular points (cf. §4.1 for precise definitions of semi-stable curve, ordinary double point and thickness).

**Theorem 2.2.1.** [22, §3][61, Theorem 5.3] Let $\tilde{X}_0(D, N)$ be the special fiber at $p \mid D$.

i) The set of singular points $\tilde{X}(D, N)_{\text{sing}}$ of $\tilde{X}_0(D, N)$ is in one-to-one correspondence with the set $\text{Pic}(\frac{D}{p}, Np)$. Moreover, if we denote by

$$\varepsilon_\sigma : \tilde{X}(D, N)_{\text{sing}} \overset{1:1}{\longrightarrow} \text{Pic}\left(\frac{D}{p}, Np\right)$$

the corresponding bijection, we have $\varepsilon_\sigma(\tilde{P}) = \text{End}(\tilde{A}, \tilde{\gamma}) = \text{End}_{\mathcal{O}}(\mathcal{M}_{(\tilde{A}, \tilde{\gamma})}) \in \text{Pic}(D/p, Np)$, for all $\tilde{P} = [\tilde{A}, \tilde{\gamma}] \in \tilde{X}(D, N)_{\text{sing}}$. In addition, the thickness of $\tilde{P}$ is given by the rule $e_{\tilde{P}} = \varepsilon_\sigma(\tilde{P})$, where $\varepsilon : \text{Pic}(\frac{D}{p}, Np) \rightarrow \mathbb{Z}$ stands for the natural map

$$\varepsilon(\mathcal{O}_i) = \#(\mathcal{O}_i^*/\{\pm 1\}), \quad \text{for all } \mathcal{O}_i \in \text{Pic}\left(\frac{D}{p}, Np\right).$$

ii) The set of irreducible components $\tilde{X}(D, N)_c$ is in one-to-one correspondence with two copies of $\text{Pic}(\frac{D}{p}, N)$. We denote by

$$\varepsilon_c : \tilde{X}(D, N)_c \overset{1:1}{\longrightarrow} \text{Pic}\left(\frac{D}{p}, N\right) \sqcup \text{Pic}\left(\frac{D}{p}, N\right)$$

the corresponding bijection. Let $\tilde{Q} = [\tilde{A}, \tilde{\gamma}] \not\in \tilde{X}_0(D, N)_{\text{sing}}$. If we write $C_{\tilde{Q}}$ for the irreducible component where $\tilde{Q}$ lies, then $\varepsilon_c(C_{\tilde{Q}}) = \text{End}(\tilde{B}, \tilde{\gamma}) = \text{End}_{\mathcal{O}}(\mathcal{M}_{(\tilde{B}, \tilde{\gamma})}) \in \text{Pic}(\frac{D}{p}, N)$.
2.3. DELIGNE-RAPOPORT-BUZZARD SPECIAL FIBER

Pic\((D/p, S)\) \cup \text{Pic}(D/p, N)\), where \(\Theta(\tilde{A}, \tilde{t}, H) = (\tilde{B}, \tilde{j}, I)\), \(H\) is the unique \(O\)-stable subgroup of \(\tilde{A}\) isomorphic to \(\alpha_p\) and \(\text{End}(\tilde{B}, \tilde{j})\) lies in the first or second copy of \(\text{Pic}(D/p, N)\) depending if \((\tilde{B}, \tilde{j})\) is pure of type \(\sigma\) or \(\tau\).

**Remark 2.2.2.** In Ribet’s original paper [61], singular points are characterized as triples \([\tilde{A}_0, \tilde{t}_0, C]\) where \((\tilde{A}_0, \tilde{t}_0)\) is an abelian surface with QM by a maximal order and \(C\) is a \(\Gamma_0(N)\)-structure. According to Appendix A, we can construct from such a triple a pair \((\tilde{A}, \tilde{t})\) with QM by \(O\) such that \(\text{End}(\tilde{A}, \tilde{t}) = \text{End}(\tilde{A}_0, \tilde{t}_0, C)\).

2.3 Deligne-Rapoport-Buzzard special fiber

In order to describe the Deligne-Rapoport-Buzzard special fiber, we must characterize the set of supersingular points in any smooth special fiber, \(\bar{X}_0(D, N) = X_0(D, N) \times \text{Spec}(\mathbb{F}_q), q \nmid DN\).

2.3.1 Supersingular points on smooth fibers

Let \(q \nmid DN\) and fix \(\mathbb{F}\) an algebraic closure of \(\mathbb{F}_q\). By the above discussion on the moduli interpretation of Morita’s integral model \(X_0(D, N)\), \(\mathbb{F}\)-rational points of \(\bar{X}_0(D, N)\) classify abelian surfaces over \(\mathbb{F}\) with QM by \(O\).

Denote by \(\bar{X}_0(D, N)\) the set of points \(P = [\tilde{A}, \tilde{t}] \in \bar{X}_0(D, N)(\mathbb{F})\) such that \((\tilde{A}, \tilde{t})\) is supersingular. By Lemma 2.1.12, if \(P = [\tilde{A}, \tilde{t}]\) lies in \(\bar{X}_0(D, N)\), we have that the Oort’s invariant \(a(\tilde{A}) = \dim_{\mathbb{F}}(\text{Hom}(\alpha_q, \tilde{A}))\). The \(\mathbb{F}\)-vector space \(\text{Hom}(\alpha_q, \tilde{A})\) is naturally a module over \(O \otimes \mathbb{F} \cong M_2(\mathbb{F})\). Its dimension \(a(\tilde{A})\) is therefore even. Since \(a(\tilde{A})\) is a priori either 1 or 2, it follows that \(a(\tilde{A}) = 2\). Hence, we can consider its attached \((O, \mathcal{S})\)-bimodule \(\mathcal{M}(\tilde{A}, \tilde{t}) = \mathcal{M}\). The isomorphism class \([\tilde{A}, \tilde{t}]\) is characterized by the isomorphism class of \(\mathcal{M}\). Thus, by Theorem 2.1.6, we have the following result:

**Proposition 2.3.1.** There is a one-to-one correspondence

\[
\varepsilon_{ss} : (\bar{X}_0(D, N))_{ss} \xleftarrow{1:1} \text{Pic}(Dq, N),
\]

given by the rule

\[
\varepsilon_{ss}(\bar{P}) = \text{End}(\tilde{A}, \tilde{t}) = \text{End}_{\mathbb{F}}(\mathcal{M}(\tilde{A}, \tilde{t})) \in \text{Pic}(Dq, N),
\]

for all \(P = [\tilde{A}, \tilde{t}] \in \bar{X}_0(D, N)\).

2.3.2 Deligne-Rapoport-Buzzard special fiber

Let \(q\) be a prime dividing exactly \(N\), fix \(\mathbb{F}\) an algebraic closure of \(\mathbb{F}_q\) and let \(\bar{X}_0(D, N)\) denote the special fiber \(X_0(D, N) \times \text{Spec}(\mathbb{F}_q)\). Recall that points in \(\bar{X}_0(D, N)(\mathbb{F})\) classify abelian surfaces over \(\mathbb{F}\) with QM by \(O\).

Let \(X_0(D, N) \Rightarrow X_0(D, N/q)\) be the two degeneracy maps described in Appendix A. Let \(\delta\) and \(\delta_\omega\) denote their specializations \(X_0(D, N) \Rightarrow \bar{X}_0(D, N/q)\) on the special fibers. Write \(\gamma\) and \(\omega_q\gamma\) for the maps \(X_0(D, N/q) \Rightarrow \bar{X}_0(D, N)\) given, in terms of the moduli interpretation described in Appendix A, by \(\gamma((\tilde{A}, \tilde{t})) = (\tilde{A}, \tilde{t}, \ker(F_{\tilde{A}/\mathbb{F}}))\) and \(\omega_q\gamma((\tilde{A}, \tilde{t})) = (\tilde{A}(q), \tilde{t}(q), \ker(V_{\tilde{A}/\mathbb{F}}))\), where \(F_{\tilde{A}/\mathbb{F}}\) and \(V_{\tilde{A}/\mathbb{F}}\) are the usual relative Frobenius and Verschiebung. It can be easily checked that \(\gamma \circ \delta = \omega_q\gamma \circ \delta_\omega = \text{Id}\) and \(\gamma \circ \delta_\omega = \omega_q\gamma \circ \delta = \omega_q\), where \(\omega_q\) is the usual Atkin-Lehner involution.
Theorem 2.3.2. [19, Theorem V.1.16][15] The maps $\gamma$ and $\omega_q$ are closed morphisms and their images are respectively the two irreducible components of $\hat{X}_0(D, N)$. These irreducible components meet transversally at the supersingular points of $\hat{X}_0(D, N/q)$.

Thus by the work of Deligne and Rapoport for $D = 1$, and Buzzard for $D > 1$, there are two irreducible components of $\hat{X}_0(D, N)$ and they are isomorphic to $\hat{X}_0(D, N/q)$. Notice that $\hat{X}_0(D, N/q)$ has good reduction at $q$, hence $\hat{X}_0(D, N/q)$ is smooth. Moreover, the two irreducible components meet transversally at the supersingular points $\hat{X}_0(D, N/p)_{ss}$. Hence, by Proposition 2.3.1, the set of singular points $\hat{X}_0(D, N)_{sing}$ of $\hat{X}_0(D, N)$ is in one-to-one correspondence with $\text{Pic}(Dq, N/q)$. We denote by

$$\varepsilon_s : \hat{X}(D, N)_{sing} \xrightarrow{1:1} \text{Pic} \left( Dq, \frac{N}{q} \right)$$

(2.3.6)

the corresponding bijection.

Let $\tilde{P} = [\tilde{A}, \tilde{i}] \in \hat{X}(D, N)_{sing}$ and let $[\tilde{A}_0, \tilde{i}, \tilde{C}]$ be the triple corresponding to $[\tilde{A}, \tilde{i}]$ by means of the other moduli interpretation given in Appendix A. Recall that $\varepsilon_s(\tilde{P}) = \text{End}_{\tilde{C}}(\mathcal{M}_{(\tilde{A}_0, \tilde{i})}) = \text{End}(\tilde{A}_0, \tilde{i})$, by Proposition 2.3.1. Since $\tilde{A}_0$ is supersingular, $\tilde{C} = \ker(F_{\tilde{A}/\tilde{F}})$, and thanks to the fact that the $F_{\tilde{A}/\tilde{F}}$ lies in the center of $\text{End}(\tilde{A}_0)$, it follows that $\text{End}(\tilde{A}_0, \tilde{i}, \tilde{C}) = \text{End}(\tilde{A}_0, \tilde{i}, \tilde{C})$. By Proposition 5.3.7, $\text{End}(\tilde{A}, \tilde{i}) = \text{End}(\tilde{A}_0, \tilde{i}, \tilde{C})$, thus we deduce that, analogously as in Theorem 2.2.1,

$$\varepsilon_s(\tilde{P}) = \text{End}(\tilde{A}_0, \tilde{i}) \in \text{Pic} \left( Dq, \frac{N}{q} \right).$$

(2.3.7)

Proposition 2.3.3. [22, §3] The thickness of $\tilde{P} \in \hat{X}(D, N)_{sing}$ is given by the rule $e_P = \varepsilon(\varepsilon_s(\tilde{P}))$, where $\varepsilon : \text{Pic}(Dq, N/q) \to \mathbb{Z}$ stands for the natural map

$$\varepsilon(O_i) = \#(O_i^*/\langle \pm 1 \rangle), \quad \text{for all } O_i \in \text{Pic} \left( Dq, \frac{N}{q} \right).$$

(2.3.8)

Notice that, in analogy with the Čerednik-Drinfeld situation, the set of irreducible components of $\hat{X}_0(D, N)$ can be identified with $\text{Pic}(D, \frac{N}{q}) \sqcup \text{Pic}(D, \frac{N}{q})$, since $\#\text{Pic}(D, \frac{N}{q}) = 1$.

2.4 Specialization of points in a Shimura curve

Let $p$ be any prime, let $\mathbb{F}$ be a fixed algebraic closure of $\mathbb{F}_p$, let $\mathbb{Z}_p$ denote the integer ring of $\overline{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}_p$) and fix an embedding $\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}$. Write $X_0(D, N) = X_0(D, N) \times \text{Spec}(\mathbb{F}_p)$ as above. Let $P \in X_0(D, N)(\overline{\mathbb{Q}})$ be a point on the Shimura curve. Since $X_0(D, N)$ is a proper $\mathbb{Z}$-scheme with generic fiber $X_0(D, N)$, there exists $\mathcal{P} \in X_0(D, N)(\mathbb{Z}_p)$ such that $\mathcal{P} \cap X_0(D, N)(\overline{\mathbb{Q}}) = P$. We denote by $\tilde{P} = \mathcal{P} \cap \hat{X}_0(D, N)(\mathbb{F})$ its specialization. We proceed to describe the specialization map

$$X_0(D, N)(\overline{\mathbb{Q}}) \ni P \quad \mapsto \quad \hat{X}_0(D, N)(\mathbb{F}), \quad \tilde{P}$$

(2.4.9)

in terms of the moduli interpretation of $X_0(D, N)$.
Let \( P = [A, i] \in X_0(D, N)(\mathbb{Q}) \) be a (non-cusp) point on the Shimura curve \( X_0(D, N) \). Pick a field of definition \( M \) of \( (A, i) \). Fix a prime \( \mathfrak{p} \) of \( M \) above \( p \) and let \( \tilde{A} \) denote the special fiber of the Néron model of \( A \) at \( \mathfrak{p} \). By [60, Theorem 3], \( A \) has potential good reduction at \( \mathfrak{p} \). Hence, after extending the field \( M \) if necessary, we obtain that \( A \) is smooth over \( \mathbb{F} \).

Since \( A \) has good reduction at \( \mathfrak{p} \), the natural morphism \( \phi : \text{End}(A) \to \text{End}(\tilde{A}) \) is injective. The composition \( \tilde{i} = \phi \circ i \) yields an optimal embedding \( \tilde{i} : \mathcal{O} \to \text{End}(\tilde{A}) \) and the isomorphism class of the pair \( (\tilde{A}, \tilde{i}) \) corresponds to the specialization \( \tilde{P} \) of the point \( P \) on the special fiber \( X_0(D, N) \).

Let us denote by \( \phi_P : \text{End}(A, i) \to \text{End}(\tilde{A}, \tilde{i}) \) the restriction of \( \phi \) to \( \text{End}(A, i) \).

**Lemma 2.4.1.** The embeddings \( \phi \) and \( \phi_P \) are optimal locally at every prime but possibly at \( p \).

**Proof.** We first show that \( \phi_P \) is optimal for any prime \( \ell \neq p \). For this, let us identify \( \text{End}^0(A)_{\ell} \) with a subalgebra of \( \text{End}^0(\tilde{A})_{\ell} \) via \( \phi \), so that we must prove that \( \text{End}^0(A)_{\ell} \cap \text{End}(\tilde{A})_{\ell} = \text{End}(A)_{\ell} \). It is clear that \( \text{End}^0(A)_{\ell} \cap \text{End}(\tilde{A})_{\ell} \supset \text{End}(A)_{\ell} \). As for the reversed inclusion, let \( \alpha \in \text{End}^0(A)_{\ell} \cap \text{End}(\tilde{A})_{\ell} \) and let \( M \) be a field of definition of \( \alpha \). Due to good reduction, there is an isomorphism of Tate modules \( T_{\ell}(A) = T_{\ell}(\tilde{A}) \). Faltings’s theorem on Tate’s Conjecture [72, Theorem 7.7] asserts that \( \text{End}_M(A)_{\ell} = \text{End}_{G_M}(T_{\ell}(A)) \subseteq \text{End}(T_{\ell}(A)) \), where \( G_M \) stands for the absolute Galois group of \( M \) and \( \text{End}_{G_M}(T_{\ell}(A)) \) is the subgroup of \( \text{End}(T_{\ell}(A)) \) fixed by the action of \( G_M \). Since \( \alpha \in \text{End}^0_M(A)_{\ell} \), there exists \( n \in \mathbb{Z} \) such that \( n\alpha \in \text{End}_M(A)_{\ell} = \text{End}_{G_M}(T_{\ell}(A)) \). By hypothesis \( \alpha \in \text{End}_{G_M}(T_{\ell}(A)) \), hence it easily follows that \( \alpha \in \text{End}_{G_M}(T_{\ell}(A)) = \text{End}_M(A)_{\ell} \subseteq \text{End}(A)_{\ell} \).

This shows that \( \phi_{\ell} \) is optimal. One easily concludes the same for \( (\phi_P)_{\ell} \) by taking into account that \( \text{End}(A, i) = \text{End}(\tilde{A}, \tilde{i}) \cap \text{End}(A) \). \( \square \)

**Remark 2.4.2.** Notice that if \( \text{End}(A, i) \) is maximal in \( \text{End}^0(A, i) \), the embedding \( \phi_P \) is optimal. In fact, if \( \text{End}(A, i) \) is not maximal in \( \text{End}^0(A, i) \) the embedding \( \phi_P \) may not be optimal at \( p \). For example, let \( R \) be an order in an imaginary quadratic field \( K \) of conductor \( cp^r \), let \( A \cong E \times E \) where \( E \) is an elliptic curve with CM by \( R \) and let \( i : M_2(\mathbb{Z}) \to M_2(R) = \text{End}(A) \). Then \( \text{End}(A, i) \cong R \) whereas, if \( p \) is inert in \( K \), \( \text{End}(\tilde{A}, \tilde{i}) \in \mathcal{E}(p, 1) \). Thus if \( \phi_P \) were optimal, it shall provide an element of \( \text{CM}_{p,1}(R) \) which is impossible by Corollary 1.2.5.
Chapter 3

Specialization of Heegner points

In this chapter we will use the results of the previous ones to describe the specialization of the Heegner points $\text{CM}(R)$, focusing our attention on the behavior of the actions of $\text{Pic}(R)$ and the Atkin-Lehner group under the specialization map of (2.4.9).

3.1 Supersingular specialization of Heegner points

Let $R$ be an order of conductor $c$ in an imaginary quadratic field $K$. Let $P = [A,i] \in \text{CM}(R) \subset X_0(D,N)(\mathbb{Q})$ be a Heegner point. By Theorem 1.4.5, $A \cong E \times E_I$ where $E = \mathbb{C}/R, E_I = \mathbb{C}/I$ are elliptic curves with CM by $R$. Here $I$ is a projective $R$-ideal in $K$.

Assume that $p$ is coprime to $cN$ and does not split in $K$. Then $\tilde{A} \cong \tilde{E} \times \tilde{E}_I$ is a product of two supersingular elliptic curves over $\mathbb{F}$. Let $S \in \mathcal{E}(p,1)$ be the endomorphism ring of $\tilde{E}$ endowed with the natural orientation described in Remark 2.1.11. Since $a(\tilde{A}) = 2$, we can assign an $(O,S)$-bimodule $M = M_{\tilde{P}}$ to $\tilde{P} = [\tilde{A}, \tilde{i}]$ as in the previous section.

Theorem 3.1.1. For any $P \in \text{CM}(R)$ write $\varphi(P) \in \text{CM}_{D,N}(R)$ for its attached optimal embedding via (1.4.10). Then,

(a) There exists an optimal embedding $\psi_p : R \hookrightarrow S$ such that, for all $P \in \text{CM}(R)$,

$$M_{\tilde{P}} \cong O \otimes_R S,$$

where $S$ is regarded as left $R$-module via $\psi_p$ and $O$ as right $R$-module via $\varphi(P)$.

(b) Upon the identifications (2.1.1) and (3.1.1), the optimal embedding $\phi_P$ of Lemma 2.4.1 is given by the rule

$$R \quad \hookrightarrow \quad \text{End}_O^S(O \otimes_R S),$$

$$\delta \quad \mapsto \quad \phi_P(\delta) : \alpha \otimes s \mapsto \alpha(\varphi(P)(\delta)) \otimes s,$$

up to conjugation by $\text{End}_O^S(O \otimes_R S)^\times$.

Proof. As explained in §2.1.3, the isomorphism class of the bimodule $M_{\tilde{P}}$ is completely determined by the optimal embedding $\tilde{i} : O \rightarrow \text{End}(\tilde{A}) = M(2,S)$, which in turn is defined as the composition of $i$ with $\phi : \text{End}(A) \rightarrow \text{End}(\tilde{A})$.

According to Theorem 1.4.5, the endomorphism ring $\text{End}(A)$ can be identified with the image of $O \otimes_R K$ in $M_2(K)$ via the isomorphism $B \otimes_K K \cong M_2(K)$ provided by $\varphi(P)$. Such
identification is given by the following action of $O \otimes_{\mathbb{Z}} R$ on $O$, furnished with structure of right $R$-module via $\varphi(P)$,

\[
O \otimes_{\mathbb{Z}} R \times O \rightarrow O \\
(\alpha \otimes \delta, \alpha') \mapsto \alpha \alpha' \varphi(P)(\delta)
\]

The order $S = \text{End}(\tilde{E})$ acquires structure of left $R$-module by means of the natural optimal embedding $\psi_p : \text{End}(E) \simeq R \rightarrow \text{End}(\tilde{E}) \simeq S$ (here $\psi_p$ is optimal by Lemma 2.4.1). Via such $R$-module structure, we can identify $\text{End}(\tilde{A})$ with $\text{End}(A) \otimes_R S$. Thus the isomorphism $(O \otimes_{\mathbb{Z}} R) \otimes_R S \simeq M_2(S)$ will be provided by the action

\[
(O \otimes_{\mathbb{Z}} R) \otimes_R S \times O \otimes_R S \rightarrow O \otimes_R S \\
(\alpha \otimes \delta \otimes s, \alpha' \otimes s') \mapsto \alpha \alpha' \varphi(P)(\delta) \otimes ss'.
\]

This shows that $M_{\tilde{P}} \cong O \otimes_R S$.

Moreover, since the subalgebra $R \simeq \text{End}(A, i) \subset \text{End}(A) \subset \text{End}(\tilde{A})$ corresponds to the inclusion $1 \otimes R \subset O \otimes_{\mathbb{Z}} R \subset (O \otimes_{\mathbb{Z}} R) \otimes_R S$, the embedding $R \rightarrow \text{End}_{\tilde{S}}^0(O \otimes_R S)$ arising from $\phi_P : \text{End}(A, i) \rightarrow \text{End}(\tilde{A}, i)$ is given by $\phi_P(\delta)(\alpha \otimes s) = \alpha \delta \otimes s$. This endomorphism clearly commutes with both (left and right) actions of $O$ and $S$. Moreover this construction is determined up to isomorphism of $(O, S)$-bimodules, i.e. up to conjugation by $\text{End}_{\tilde{S}}^0(M_{\tilde{P}})^\times$.

**Remark 3.1.2.** The embedding $\psi_p : R \rightarrow S$ depends on the immersion $\rho : H_R \rightarrow \overline{\mathbb{Q}}_p$ chosen for the specialization. Given another optimal embedding $\psi'_p \in \text{CM}_{p,1}(R)$, there exists a different immersion $\rho' : H_R \rightarrow \overline{\mathbb{Q}}_p$ such that, specializing via $\rho'$, Theorem 3.1.1 applies with $\psi'_p$ instead of $\psi_p$. Indeed, the embedding $\psi_p$ corresponds to the inclusion $\text{End}(E) \subset \text{End}(\tilde{E})$, where $E$ is the CM elliptic curve $\mathbb{C}/R$ and $\tilde{E}$ is its specialization via $\rho$. Both, the set of immersions $H_R \rightarrow \overline{\mathbb{Q}}_p$ and $\text{CM}_{p,1}(R)$ are $\text{Pic}(R)$-torsors and the action of $\sigma \in \text{Gal}(H_R/K) \simeq \text{Pic}(R)$ turns $\psi_p$ into the embedding $\text{End}(E^\sigma) \subset \text{End}(\tilde{E}^\sigma)$, where $\tilde{E}^\sigma$ is specialized by means of $\rho$. It is clear that such an optimal embedding coincides with the one obtained specializing $E$ via $\rho' = \rho \sigma$.

### 3.1.1 Computable description of the map $\phi_P$

Since Theorem 3.1.1 describes the map $\phi_P : \text{End}(A, i) \rightarrow \text{End}(\tilde{A}, i)$ in terms of purely algebraic objects, we shall be able to compute it starting from the corresponding embedding $\varphi(P) \in \text{CM}_{D,1}(R)$ of (1.4.10). Next, we shall present an explicit description of $\phi_P$ obtained from an explicit description of $\varphi(P)$.

For any optimal embedding $(\psi : R \rightarrow O_{d,n}) \in \text{CM}_{d,n}(R)$, recall the decomposition $O_{d,n} \simeq R \oplus eI$ of (1.2.5). This decomposition determines completely $\psi$. Besides, $O_{d,n}^0$ is characterized by the presentation $O_{d,n}^0 \simeq K \oplus jK$, where $O_{d,n}^0$ is also regarded as a right $K$-vector space via $\psi$ and $jK$ is the quaternionic complement of $K \xrightarrow{\psi} O_{d,n}^0$. Recall that $j$ is determined by $j^2 \in \mathbb{Q}^\times$ and the fact that $j\psi(x) = \psi(x^\sigma)j$, for all $x \in K$.

In conclusion, in order to compute $\phi_P : R \rightarrow \Lambda$ explicitly, where $\Lambda = \text{End}(\tilde{A}, i)$, we only have to present the corresponding decompositions of $\Lambda$ and $\Lambda^0$ via $\phi_P$.

**Theorem 3.1.3.** Let $P \in \text{CM}(R)$ be a Heegner point. Let $(\psi_p : R \rightarrow S) \in \text{CM}_{p,1}(R)$ be the fixed optimal embedding of Theorem 3.1.1. Write $S^0 = H$ and let $H = K \oplus j_2 K, S \simeq R \oplus e_2 J_2,$
\( j_2^2 = m_2, e_2 = e_{2,1} + j_2 e_{2,2} \), be the presentations of \( H \) and \( S \) induced by \( \psi_p \). Analogously, let \( B = K \oplus j_1 K \) and \( \mathcal{O} \simeq R \oplus e_1 I_1 \), \( j_2^2 = m_1, e_1 = e_{1,1} + j_1 e_{1,2} \), be the presentations of \( B \) and \( \mathcal{O} \) induced by \( \varphi(P) \). Then, the optimal embedding \( \phi_P : R \hookrightarrow \Lambda \) is characterized by:

\[
\Lambda^0 = K \oplus j_3 K \quad \text{and} \quad \Lambda = R \oplus e_3 I_3,
\]

where \( j_3 \) is a quaternionic complement of \( \phi_P \) such that \( j_3^2 = m_1 \cdot m_2, e_3 = e_2,1 \cdot e_{1,1} - j_3 e_{2,2} \cdot e_{1,2} \) and

\[
I_3 = \begin{cases} 
I_2 I_1^\sigma & \text{if } e_{1,1} = 0, e_{2,1} = 0, \\
I_2 I_1^\sigma \cap \frac{1}{e_{1,1}} I_2 & \text{if } e_{1,1} \neq 0, e_{2,1} = 0, \\
(I_2 \cap \frac{1}{e_{2,1}} R) I_1^\sigma & \text{if } e_{1,1} = 0, e_{2,1} \neq 0, \\
(I_2 \cap \frac{1}{e_{2,1}} R) I_1^\sigma \cap \frac{1}{e_{1,1}} I_2 & \text{if } e_{1,1} \neq 0, e_{2,1} \neq 0.
\end{cases}
\]

**Proof.** Attached to the right \( K \)-module structure of \( B \) via \( \varphi(P) \) we have two distinguished basis, namely \((1, j_1)\) and \((1, e_1)\). We denote by \( M_{e_1} = \begin{pmatrix} 1 & e_{1,1} \\ 0 & e_{1,2} \end{pmatrix} \) the matrix attached to the change of basis.

It follows that an element \( z = x + j_1 y \in K \oplus j_1 K = B \) acts on \( K \oplus j_1 K \) via the matrix

\[
M_x = \begin{pmatrix} x & m_1 y \sigma \\ y & x \sigma \end{pmatrix} \in M_2(K).
\]

Since \( B \otimes_K H = (K \oplus j_1 K) \otimes_K H = H \oplus j_1 H \), any element \( z = x + j_1 y \in B \) acts on \( B \otimes_K H \) through the same matrix \( M_z \). Hence

\[
\Lambda^0 = \text{End}_B^H(B \otimes_K H) = \left\{ \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in M_2(H) : M_z \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) M_z \right\}.
\]

This implies that \( a = d, m_1 c = b, a \in \{ x \in H : xy = yx, \text{ for all } y \in K \} = K \) and \( b \in \{ x \in H : xy = yx, \text{ for all } y \in K \} = j_2 K \). Thus

\[
\Lambda^0 = K \oplus \begin{pmatrix} 0 & m_1 j_2 \\ j_2 & 0 \end{pmatrix} = K \oplus j_3 K, \quad j_3 = \begin{pmatrix} 0 & m_1 j_2 \\ j_2 & 0 \end{pmatrix}
\]

(3.12)

where \( j_3 \) satisfies \( x j_3 = j_3 x \sigma \) for all \( x \in K \) and \( j_3^2 = m_1 m_2 \in \mathbb{Q} \). Hence \( j_3 \) is a quaternionic complement of \( \phi_P : K \hookrightarrow \Lambda^0 \).

The \( R \)-module decomposition \( \mathcal{O} = R \oplus e_1 I_1 \) yields the \( S \)-module structure of \( \mathcal{O} \otimes_R S \), namely \( S \times (I_1 \otimes_R S) \) with basis \((1, e_1)\). We turn it into our original basis \((1, j_1)\) by means of \( M_{e_1} \). Then,

\[
\Lambda = \{ (a + j_3 b) \in \Lambda \otimes \mathbb{Q} : M_{e_1}^{-1}(a + j_3 b) M_{e_1} (S \times (I_1 \otimes_R S)) \subseteq S \times (I_1 \otimes_R S) \}.
\]

We obtain that \( M_{e_1}^{-1}(a + j_3 b) M_{e_1} = a + M_{e_1}^{-1} j_3 M_{e_1} b \) where:

\[
M_{e_1}^{-1} j_3 M_{e_1} = \begin{pmatrix} -j_2 & 0 \\ 0 & j_2 \end{pmatrix} \frac{1}{e_{1,2}^\sigma} \begin{pmatrix} e_{1,1}^\sigma & N(e_1) \\ 1 & e_{1,1} \end{pmatrix}.
\]

Hence the \( R \)-module \( \Lambda \) consists of elements \( a + j_3 b \in \Lambda^0 \) with \( a, b \in K \) such that, for all \( x \in S \) and all \( y \in (I_1 \otimes_R S) \),

\[
\begin{pmatrix} ax \\ ay \end{pmatrix} + \begin{pmatrix} -j_2 & 0 \\ 0 & j_2 \end{pmatrix} \frac{1}{e_{1,2}^\sigma} \begin{pmatrix} e_{1,1}^\sigma & N(e_1) \\ 1 & e_{1,1} \end{pmatrix} \begin{pmatrix} bx \\ by \end{pmatrix} \in S \times (I_1 \otimes_R S).
\]
We deduce that
\[
\begin{aligned}
\begin{cases}
ax - j_2 \frac{e_{1,1}^2 bx + N(e_1)by}{e_{1,2}^2} = ax + \frac{e_{2,1}(e_{1,1}^2 bx + N(e_1)by) - e_{2,1}^2 bx + N(e_1)by}{e_{1,2} \cdot e_{2,2}} \in \mathcal{S} \\
ay + j_2 \frac{bx + e_{1,1}by}{e_{1,2}^2} = ay - \frac{e_{2,1}(bx + e_{1,1}by)}{e_{1,2} \cdot e_{2,2}} + e_2 bx + e_{1,1}by \in I_1 \otimes_R \mathcal{S}.
\end{cases}
\end{aligned}
\] (3.1.3)

Set \( e_3 = e_{2,1} \cdot e_{1,1}^2 - j_3 e_{2,2} \cdot e_{1,2}^2 \). For all \( a, b \in K \), we have that \( a + j_3 b = a' + e_3 b' \), where \( a' = a + \frac{e_{2,1} e_{1,1}^2}{e_{2,2} \cdot e_{1,2}^2} b \) and \( b' = -\frac{b}{e_{2,2} \cdot e_{1,2}^2} \).

Thus the expressions of (3.1.3) become (with this new basis \( (1, e_3) \)):
\[
(a'x - e_{2,1} N(e_1) b'y) + e_2 (e_{1,1}^2 b'x + N(e_1) b'y) \in \mathcal{S}
\]
(3.1.4)
\[
(a'y + e_{2,1} \text{Tr}(e_{1,1}) b'y + e_{2,1} b'x) - e_2 (b'x + e_{1,1} b'y) \in I_1 \otimes_R \mathcal{S}.
\]
(3.1.5)

In particular, assuming \( y = 0 \) we obtain from (3.1.4) that \((a' + e_2 e_{1,1} b') x \in \mathcal{S} = R \oplus e_2 I_2\). This implies that \( a' \in R \) and \( e_{1,1} b' \in I_2 \). It follows from (3.1.5) that \((e_{2,1} - e_2) b'x \in (I_1 \otimes_R \mathcal{S})\), that is \( b'' j_2 e_{2,2} = (e_{2,1} - e_2) b' \in (I_1 \otimes_R \mathcal{S}) \). Hence \( b' \in I_1' I_2' \) where
\[
I_2' = \begin{cases}
I_2 \cap \frac{1}{e_{2,1}} R & \text{if } e_{2,1} \neq 0 \\
I_2 & \text{if } e_{2,1} = 0.
\end{cases}
\]

Assuming that \( x = 0 \), it follows from (3.1.4) that \(- (e_{2,1} - e_2) N(e_1) b'y \in \mathcal{S} \), which is deduced from \((e_{2,1} - e_2) b' \in (I_1 \otimes R \mathcal{S}) \) above and the fact that, since \( e_1 I_1 \in \mathcal{O}, N(e_1) I_1' \subseteq R \).
Moreover, by (3.1.5) we have that \((a' + e_{2,1} \text{Tr}(e_{1,1}) b' - e_2 e_{1,1} b') y \in I_1 \otimes_R \mathcal{S} \), which is again deduced from \((e_{2,1} - e_2) b' \in (I_1 \otimes_R \mathcal{S}) \) and \((a' + e_2 e_{1,1} b') x \in \mathcal{S} \), since
\[
(a' + e_{2,1} \text{Tr}(e_{1,1}) b' - e_2 e_{1,1} b') y = y (a' + e_2 e_{1,1} b') + (e_{2,1} - e_2) \text{Tr}(e_{1,1} y) b' \in I_1 \otimes_R \mathcal{S},
\]
for all \( y \in I_1 \) and \( \text{Tr}(e_{1,1} y) = \text{Tr}(e_1 y) \in I_1 \subseteq \mathbb{Z} \subseteq R \).

In conclusion, \( a' + e_3 b' \in \Lambda \) if and only if \( a' \in R \) and \( b' \in I_3 \), where
\[
I_3 = \begin{cases}
I_2' I_1' \cap \frac{1}{e_{1,1}} I_2 & \text{if } e_{1,1} \neq 0 \\
I_2' I_1' & \text{if } e_{1,1} = 0.
\end{cases}
\]
(3.1.6)

Thus \( \Lambda \simeq R \oplus e_3 I_3 \), where \( e_3 = e_{2,1} \cdot e_{1,1} - j_3 e_{2,2} \cdot e_{1,2} \), and \( j_3 \) is a quaternionic complement of \( \phi_p \), such that \( j_3^2 = m_1 m_2 \).

3.1.2 The action of \( \text{Pic}(R) \)

**Definition 3.1.4.** For an \((\mathcal{O}, \mathcal{S})\)-bimodule \( \mathcal{M} \), let

- \( \text{Pic}^\mathcal{S}_\mathcal{O}(\mathcal{M}) \) denote the set of isomorphism classes of \((\mathcal{O}, \mathcal{S})\)-bimodules that are locally isomorphic to \( \mathcal{M} \),
- \( \text{CM}_\mathcal{M}(R) \) denote the set of \( \text{End}^\mathcal{S}_\mathcal{O}(\mathcal{M})^\times \)-conjugacy classes of optimal embeddings \( \varphi : R \leftrightarrow \text{End}^\mathcal{S}_\mathcal{O}(\mathcal{M}) \),
- \( \text{CM}^\mathcal{M}_\mathcal{O}\mathcal{S}(R) = \{ (\mathcal{N}, \psi) : \mathcal{N} \in \text{Pic}^\mathcal{S}_\mathcal{O}(\mathcal{M}), \psi \in \text{CM}_\mathcal{N}(R) \} \).
Let $P = [A, i] \in \text{CM}(R)$ be a Heegner point and let $\mathcal{M}_P$ be the $(\mathcal{O}, S)$-bimodule attached to its specialization $\overline{P} = [\overline{A}, \overline{i}]$ at $p$ as described above.

By Theorem 3.1.1, the bimodule $\mathcal{M}_P$ and the $\End^S_D(\mathcal{M}_P)$-conjugacy class of $\phi_P : R \to \End^S_D(\mathcal{M}_P)$ are determined by the optimal embedding $\varphi(P) \in \text{CM}_{D,N}(R)$. Hence specialization at $p$ induces a map

$$\phi : \text{CM}_{D,N}(R) \to \bigcup_{\mathcal{M}} \text{CM}^M_{D,S}(R), \quad \varphi(P) \mapsto (\mathcal{M}_P, \phi_P), \quad (3.1.7)$$

where $\mathcal{M}$ runs over a set of representatives of local isomorphism classes of $(\mathcal{O}, S)$-bimodules arising from some $\varphi(P) \in \text{CM}_{D,N}(R)$. Note that composing $\phi$ with the natural projection

$$\pi : \bigcup_{\mathcal{M}} \text{CM}^M_{D,S}(R) \to \bigcup_{\mathcal{M}} \text{Pic}^S_D(\mathcal{M}), \quad (\mathcal{M}, \psi) \mapsto \mathcal{M}, \quad (3.1.8)$$

one obtains the map $\varphi(P) \mapsto \mathcal{M}_P$ which assigns to $\varphi(P)$ the bimodule that describes the supersingular specialization of the Heegner point associated to it.

Recall that following directly from the definition, $I \ast O$ coincides with the left order of $I^{-1} = \{ \beta \in B : I \beta \subseteq O \}$ endowed with the natural local orientations.

**Lemma 3.1.5.** There is an isomorphism of $(I \ast O, I \ast O)$-bimodules between $I \ast O$ and $I^{-1} \otimes_O I$.

**Proof.** Since $I \ast O = \{ x \in B : Ix \subseteq I \} = \{ x \in B : xI^{-1} \subseteq I^{-1} \}$, both $I \ast O$ and $I^{-1} \otimes_O I$ are $(I \ast O, I \ast O)$-bimodules with the obvious left and right $(I \ast O)$-action. Moreover, by definition,

$$I^{-1} \otimes_O I = \{ x \in B \otimes_O I = B : Ix \subseteq O \otimes_O I = I \} = I \ast O,$$

which proves the desired result. \hfill \Box

**Theorem 3.1.6.** [61, Theorem 2.3] Let $\mathcal{M}$ be an $(\mathcal{O}, S)$-bimodule and let $\Lambda = \End^S_D(\mathcal{M})$. Then the correspondence $\mathcal{N} \mapsto \text{Hom}^S_D(\mathcal{M}, \mathcal{N})$ induces a bijection between $\text{Pic}^S_D(\mathcal{M})$ and the set of isomorphism classes of locally free rank-1 right $\Lambda$-modules.

The one-to-one correspondence is given by:

$$\mathcal{N} \mapsto I(\mathcal{N}) = I \otimes_\Lambda \mathcal{M} \quad (3.1.6)$$

We can define an action of $\text{Pic}(R)$ on $\text{CM}^M_{D,S}(R)$ which generalizes the one on $\text{CM}_{D,N}(R)$. Let $(\mathcal{N}, \psi : R \to \Lambda) \in \text{CM}^M_{D,S}(R)$ where $\mathcal{N} \in \text{Pic}^S_D(\mathcal{M})$ and $\Lambda = \End^S_D(\mathcal{N})$. Pick a representative $J$ of a class $[J] \in \text{Pic}(R)$. Then $\psi(J^{-1})\Lambda$ is a locally free rank-1 right $\Lambda$-module. Write $[J] \ast \mathcal{N} := \psi(J^{-1})\Lambda \otimes_\Lambda \mathcal{N} \in \text{Pic}^S_D(\mathcal{M})$ for the element in $\text{Pic}^S_D(\mathcal{M})$ corresponding to it by the correspondence of Theorem 3.1.6. Note that this construction does not depend on the representative $J$, since $[J] \ast \mathcal{N}$ only depends on the isomorphism class of the rank-1 right $\Lambda$-module $\psi(J^{-1})\Lambda$. Since $R$ acts on $\psi(J^{-1})\Lambda$, there is an action of $R$ on $\psi(J^{-1})\Lambda \otimes_\Lambda \mathcal{N}$ which commutes with the actions of both $\mathcal{O}$ and $S$. This yields a natural embedding $[J] \ast \psi : R \to \End^S_D([J] \ast \mathcal{N})$, which is optimal because

$$\{ x \in K : \psi(x)(\psi(J^{-1})\Lambda \otimes_\Lambda \mathcal{M}) \subseteq \psi(J^{-1})\Lambda \otimes_\Lambda \mathcal{N} \} = R,$$
and does not depend on the representant $J$ of $[J]$. Hence, it defines an action of $[J] \in \text{Pic}(R)$ on $(N, \psi) \in \text{CM}^M_{O,S}(R)$. Namely $[J] \ast (N, \psi) = ([J] \ast N, [J] \ast \psi) \in \text{CM}^M_{O,S}(R)$.

Given that both sets $\text{CM}_{D,N}(R)$ and $\text{CM}^M_{O,S}(R)$ are equipped with an action of $\text{Pic}(R)$, it seems reasonable to ask about the behaviour of the action of $\text{Pic}(R)$ under the map $\phi: \text{CM}_{D,N}(R) \to \bigsqcup_M \text{CM}^M_{O,S}(R)$ of (3.1.7). This is the aim of the rest of this subsection.

Recall that, $B$ being indefinite, the orders $\mathcal{O}$ and $I \ast \mathcal{O}$ are isomorphic for any locally free left $\mathcal{O}$-module $I$ of rank 1.

**Lemma 3.1.7.** Let $\mathcal{M}$ be an $(\mathcal{O}, \mathcal{S})$-bimodule and let $I$ be a locally free left-$\mathcal{O}$-module of rank 1. Then $I^{-1} \otimes_\mathcal{O} \mathcal{M}$ admits a structure of $(I \ast \mathcal{O}, \mathcal{S})$-bimodule and the isomorphism $\mathcal{O} \cong I \ast \mathcal{O}$ identifies the $(\mathcal{O}, \mathcal{S})$-bimodule $I^{-1} \otimes_\mathcal{O} \mathcal{M}$ with the $(I \ast \mathcal{O}, \mathcal{S})$-bimodule $I^{-1} \otimes_\mathcal{O} \mathcal{M}$.

*Proof.* Since $B$ is indefinite, $\text{Pic}(D, N) = 1$ and $I$ must be principal. Write $I = O\gamma$. Then $I \ast \mathcal{O} = \gamma^{-1} \mathcal{O}\gamma$ and the isomorphism $I \ast \mathcal{O} \cong \mathcal{O}$ is given by $\gamma^{-1}\alpha\gamma \mapsto \alpha$. Finally, the isomorphism of $\mathbb{Z}$-modules

$$I^{-1} \otimes_\mathcal{O} \mathcal{M} \longrightarrow \mathcal{M}$$

$$\gamma^{-1}\beta \otimes m \mapsto \beta m$$

is compatible with the isomorphism $I \ast \mathcal{O} \cong \mathcal{O}$ described above. \hfill $\square$

**Theorem 3.1.8.** The map $\phi: \text{CM}_{D,N}(R) \longrightarrow \bigsqcup_M \text{CM}^M_{O,S}(R)$ satisfies the reciprocity law

$$\phi([J] \ast \varphi) = [J]^{-1} \ast \phi(\varphi),$$

for any $\varphi: R \to \mathcal{O}$ in $\text{CM}_{D,N}(R)$ and any $[J] \in \text{Pic}(R)$.

*Proof.* The map $\phi$ is given by

$$\phi: \text{CM}_{D,N}(R) \longrightarrow \bigsqcup_M \text{CM}^M_{O,S}(R)$$

$$(\varphi: R \to \mathcal{O}) \longmapsto (\mathcal{O} \otimes_R \mathcal{S}, \phi_\varphi: R \to \text{End}^S_O(\mathcal{O} \otimes_R \mathcal{S})).$$

Let $\varphi: R \to \mathcal{O}$ denote the conjugacy class of an embedding in $\text{CM}_{D,N}(R)$ and let $[J] \in \text{Pic}(R)$. Write $[J] \ast \varphi: R \mapsto [J] \ast \mathcal{O}$ for the embedding induced by the action of $[J]$ on $\varphi$. By Lemma 3.1.5,

$$([J] \ast \mathcal{O}) \otimes_R \mathcal{S} = (\varphi(J^{-1}) \mathcal{O} \otimes_R \mathcal{O} \varphi(J)) \otimes_R \mathcal{S}.$$

Then Lemma 3.1.7 asserts that, under the isomorphism $[J] \ast \mathcal{O} \cong \mathcal{O}$, the $([J] \ast \mathcal{O}, \mathcal{S})$-bimodule $(\varphi(J^{-1}) \mathcal{O} \otimes_R \mathcal{O} \varphi(J)) \otimes_R \mathcal{S}$ is naturally identified with the $(\mathcal{O}, \mathcal{S})$-bimodule $\mathcal{O} \varphi(J) \otimes_R \mathcal{S}$. Moreover, the embedding $\phi_{[J] \ast \varphi}$ is given by

$$\begin{align*}
R & \ni \delta \mapsto \text{End}_O^S(\mathcal{O} \varphi(J) \otimes_R \mathcal{S}) \\
& \mapsto (\alpha \varphi(j) \otimes s \mapsto \alpha \varphi(j\delta) \otimes s).
\end{align*}$$

Setting $\Lambda = \text{End}_O^S(\mathcal{O} \otimes_R \mathcal{S})$, we easily obtain that

$$\mathcal{O} \varphi(J) \otimes_R \mathcal{S} = (\varphi(\varphi)(J)\Lambda \otimes (\mathcal{O} \otimes_R \mathcal{S}) = [J]^{-1} \ast (\mathcal{O} \otimes_R \mathcal{S}).$$

Finally, since the action of $\phi_{[J] \ast \varphi}(R)$ on $[J]^{-1} \ast (\mathcal{O} \otimes_R \mathcal{S})$ is given by the natural action of $R$ on $J$, we conclude that $\phi([J] \ast \varphi) = [J]^{-1} \ast \phi(\varphi)$. \hfill $\square$
Let $\mathcal{M}$ be an admissible $(\mathcal{O}, \mathcal{S})$-bimodule of rank 8. By Theorem 2.1.6, the map $\mathcal{M} \mapsto \text{End}_R(\mathcal{M})$ induces a one-to-one correspondence between the sets $\text{Pic}_0^S(\mathcal{M})$ and $\text{Pic}(D_0^M, NN_0^M)$, where $D_0^M$ and $N_0^M$ were already defined in §2.1. This implies that the set $\text{CM}_{0, \mathcal{S}}^M(R)$ can be identified with $\text{CM}_{D_0^M, NN_0^M}^M(R)$, under the above correspondence.

Both sets are endowed with an action of the group $\text{Pic}(R)$. We claim that the bijection

$$\text{CM}_{0, \mathcal{S}}^M(R) \simeq \text{CM}_{D_0^M, NN_0^M}^M(R)$$

(3.1.9)
is equivariant under this action.

Indeed for any $[J] \in \text{Pic}(R)$ and any $(\mathcal{N}, \psi : R \mapsto \text{End}_R(\mathcal{N}))$ in $\text{CM}_{0, \mathcal{S}}^M(R)$, Theorem 3.1.10 asserts that $\text{Hom}_R^S(\mathcal{N}, [J] * \mathcal{N}) = \psi(J^{-1}) \text{End}_R^S(\mathcal{N})$. Therefore

$$\text{End}_R^S([J] * \mathcal{N}) = \{ \rho \in \text{End}_R^S(\mathcal{N}) : \rho \text{Hom}_R^S(\mathcal{N}, [J] * \mathcal{N}) \subseteq \text{Hom}_R^S(\mathcal{N}, [J] * \mathcal{N}) = [J] * \text{End}_R^S(\mathcal{N})$$

which is the left Eichler order of $\psi(J^{-1}) \text{End}_R^S(\mathcal{N})$. Moreover, $[J] * \psi$ arises from the action of $R$ on $\psi(J^{-1}) \text{End}_R^S(\mathcal{N})$ via $\psi$. In conclusion, both actions coincide.

**Corollary 3.1.9.** Assume that for all $P \in \text{CM}(R)$ the bimodules $\mathcal{M}_P$ are admissible. Then the map $\phi : \text{CM}_{D,N}(R) \mapsto \bigcup_{\mathcal{M}} \text{CM}_{D_0^M, NN_0^M}^M(R)$, satisfies $\phi([J] * \varphi) = [J]^{-1} * \phi(\varphi)$, for any $\varphi : R \mapsto \mathcal{O}$ in $\text{CM}_{D,N}(R)$ and any $[J] \in \text{Pic}(R)$.

### 3.1.3 Atkin-Lehner involutions

Recall from §1.2 that the set of optimal embeddings $\text{CM}_{D,N}(R)$ is also equipped with an action of the group $W(D, N)$ of Atkin-Lehner involutions. Let $q \mid DN$, $q \neq p$ be a prime and let $n \geq 1$ be such that $q^n \nmid DN$. For any $(\mathcal{O}, \mathcal{S})$-bimodule $\mathcal{M}$, there is a natural action of $\omega_{q^n}$ on $\text{CM}_{0, \mathcal{S}}^M(R)$ as well, as we now describe.

Let $\Omega_{\mathcal{O}}$ be the single two-sided $\mathcal{O}$-ideal of norm $q^n$. Let $(\mathcal{N}, \psi : R \mapsto \text{End}_R(\mathcal{N})) \in \text{CM}_{0, \mathcal{S}}^M(R)$. Since $\Omega_{\mathcal{O}}$ is two-sided, $\text{End}_{\mathcal{O} \otimes \mathcal{O}}(\mathcal{N})$ acquires a natural structure of $(\mathcal{O}, \mathcal{S})$-bimodule.

Recall that $\mathcal{O}$ equals $\Omega_{\mathcal{O}} * \mathcal{O}$ as orders in $B$. Hence the algebra $\text{End}_R^S(\Omega_{\mathcal{O}} \otimes \mathcal{O}) \mathcal{N}$ is isomorphic to $\text{End}_R^S(\mathcal{O} \otimes \mathcal{O}) \mathcal{N} = \text{End}_R^S(\mathcal{N})$ by Lemma 3.1.7.

Moreover, the bimodule $\Omega_{\mathcal{O}} \otimes \mathcal{O} \mathcal{N}$ is locally isomorphic to $\mathcal{N}$ at all places of $\mathcal{O}$ except possibly for $q$. Since we assumed $q \neq p$, there is a single isomorphism class locally at $q$. Hence we deduce that $\Omega_{\mathcal{O}} \otimes \mathcal{O} \mathcal{N} \in \text{Pic}_0^S(\mathcal{M})$. Thus $\omega_{q^n}$ defines an involution on $\text{CM}_{0, \mathcal{S}}^M(R)$ by the rule $\omega_{q^n}(\mathcal{N}, \psi) = (\Omega_{\mathcal{O}} \otimes \mathcal{O} \mathcal{N}, \psi)$.

We now proceed to describe the behavior of the Atkin-Lehner involution $\omega_{q^n}$ under the map

$$\phi : \text{CM}_{D,N}(R) \mapsto \bigcup_{\mathcal{M}} \text{CM}_{D_0^M, NN_0^M}^M(R)$$

introduced above.

**Theorem 3.1.10.** For all $\varphi : R \mapsto \mathcal{O}$ in $\text{CM}_{D,N}(R)$,

$$\omega_{q^n}(\varphi) = \omega_{q^n}(\phi(\varphi)).$$

**Proof.** For any $\varphi \in \text{CM}_{D,N}(R)$, let $\omega_{q^n}(\varphi) : R \mapsto \Omega_{\mathcal{O}} * \mathcal{O}$ as in §1.2. Set $\phi(\varphi) = (\mathcal{O} \otimes R \mathcal{S}, \phi_\varphi)$.

As ring monomorphisms, $\varphi$ equals $\omega_{q^n}(\varphi)$. Hence, $\phi(\omega_{q^n}(\varphi)) = ((\Omega_{\mathcal{O}} * \mathcal{O}) \otimes R \mathcal{S}, \phi_\varphi)$. Applying Lemma 3.1.5, we obtain that

$$(\Omega_{\mathcal{O}} * \mathcal{O}) \otimes R \mathcal{S} = (\mathcal{O}^{-1} \otimes \Omega_{\mathcal{O}}) \otimes R \mathcal{S}.$$
3.2 Generalized bimodules

By Lemma 3.1.7, the \((\Omega_O \ast \mathcal{O}, S)\)-bimodule \((\Omega_O^{-1} \otimes \Omega_O) \otimes R S)\) corresponds to the \((\mathcal{O}, S)\)-bimodule \(\Omega_O \otimes R S = \Omega_O \otimes (\mathcal{O} \otimes R S)\). Thus we conclude that \(\phi(\omega_p^\ast(\mathcal{O})) = (\Omega_O \otimes \mathcal{O} (\mathcal{O} \otimes R S), \phi_p) = \omega_p^\ast(\phi(\mathcal{O})).\) □

Remark 3.1.11. We defined an action of \(\omega_p^\ast\) on \(\text{CM} \mathcal{M}(\mathcal{O})\) for any \((\mathcal{O}, S)\)-bimodule \(\mathcal{M}\). Returning to the situation where \(\mathcal{M}\) is admissible, one can ask if, through the correspondence \(\text{CM} \mathcal{M}(\mathcal{O}) \leftrightarrow \text{CM} \mathcal{D}^M_0, N_0 M, N(R)\) of (3.1.9), this action agrees with the Atkin-Lehner action \(\omega_p^\ast\) on \(\text{CM} \mathcal{D}^M_0, N_0 M, N(R)\).

Indeed, let \((\mathcal{N}, \psi) \in \text{CM} \mathcal{M}(\mathcal{O})\) and set \(\Lambda = \text{End}^S(\mathcal{N}) \in \text{Pic}(\mathcal{D}^M, N_0 M N).\) Since \(\omega_p^\ast(\mathcal{N}, \psi) = (\mathcal{O} \otimes \mathcal{N}, \psi)\), we only have to check that \(\Omega_{\Lambda} := \text{Hom}^S(\mathcal{N}, \mathcal{O} \otimes \mathcal{N})\) is a locally free rank-1 two-sided \(\Lambda\)-module of norm \(q^n\) in order to ensure that \(\text{End}^S(\mathcal{O} \otimes \mathcal{N}) = \Omega_{\Lambda} \ast \Lambda\).

Since \(\Omega_{\Lambda}\) is naturally a right \(\text{End}^S(\mathcal{O} \otimes \mathcal{N})\)-module and \(\Lambda\) equals \(\text{End}^S(\mathcal{O} \otimes \mathcal{N})\) as orders in \(\text{End}^S_{\mathcal{O}}(\mathcal{N})\), we conclude that \(\Omega_{\Lambda}\) is two-sided. In order to check that \(\Omega_{\Lambda}\) has norm \(q^n\), note that \(\Omega_{\Lambda}\) coincides with \(\text{Hom}^S(\mathcal{O} \otimes \mathcal{N}, (\mathcal{O} \otimes \mathcal{O} \otimes \mathcal{O}) \otimes \mathcal{N})\) as ideals on the ring \(\Lambda\).

Hence
\[
\Omega_{\Lambda}^S = \text{Hom}^S(\mathcal{O} \otimes \mathcal{N}, q^n \mathcal{N}) \cdot \text{Hom}^S(\mathcal{N}, \mathcal{O} \otimes \mathcal{N}) = \text{Hom}^S(\mathcal{N}, q^n \mathcal{N}) = q^n \Lambda.
\]

3.2 Generalized bimodules

We proceed to generalize the above results to general \((\mathcal{O}, S^{(n)})\)-bimodules, where the order \(S^{(n)}\) may not be necessarily an Eichler order. These orders \(S^{(n)}\), that are locally maximal at all primes but one, arise from certain elliptic curves over local artinian rings.

Let \(R\) be an order in \(K\) with conductor \(c\), as above. Let \(E\) be an elliptic curve with CM by \(R\), and let \(p \nmid c\) be a prime that does not split in \(K\) (thus \(E\) has supersingular specialization modulo \(p\)). Denote by \(H_R\) the ring class field of \(R\) and fix an embedding \(\mathbb{Q} \hookrightarrow \overline{\mathbb{Q}}_p\). Set \(H_R \times \mathbb{Q} / H_p, p\) be the maximal unramified extension of \(H_p\) and let \(R_p^\text{ur}\) be its ring of integers with uniformizer \(\pi\). Write \(W_n = R_p^\text{ur} / \pi^n R_p^\text{ur}\).

Due to the fact that \(E\) has potentially good reduction, after extending \(H_p^\text{ur}\) if necessary, we can choose a smooth model \(E\) of \(E\) over \(R_p^\text{ur}\). Denote by \(S^{(n)} = \text{End}_{W_n}(E)\). In particular, \(S^{(1)} = S = \text{End}(\hat{E})\) shall be regarded as an element of \(E(p, 1)\).

The monomorphism of algebras \(\psi_p : K \simeq \text{End}^0(E) \hookrightarrow \text{End}^0(\hat{E})\) yields a decomposition
\[
S^0 = S^0_+ \oplus S^0_-
\]
where \(S^0_+ = \psi(p)\) and \(S^0_\mp\) is its quaternionic complement. Since the conductor of \(R\) is prime to \(p\), the following proposition describes completely \(S^{(n)}\):

Proposition 3.2.1. [33, Proposition 3.7.3][31, Proposition 3.3]

\[
S^{(n)} = \psi(\mathcal{O}) + p^{n-1} \mathcal{S} \subseteq \mathcal{S},
\]

\[
S^{(n)} = \{ \alpha = \alpha_+ + \alpha_- \in S : d \cdot N(\alpha_-) \equiv 0 \mod p \cdot N(\mathfrak{P})^{n-1} \},
\]

where \(d\) is the discriminant of \(K\), \(\mathfrak{P} \subset R\) is the prime ideal lying above \(p\) and \(\alpha_\pm \in S^0_\pm\).

Recall that, for all \(n\), the embedding \(\psi_p : K \hookrightarrow S^0\) gives rise to an optimal embedding
\[
\psi^{(n)}_p : R \hookrightarrow S^{(n)},
\]
furnishing $S^{(n)}$ with structure of right $R$-module.

Let $P = [A, i] \in \text{CM}(R) \subset X_0(D, N)(H)$ be a Heegner point. In order to specialize $(A, i)$ over $W_n$ as in the above setting, we must consider a smooth model $\mathcal{A}$ of $A$ over $R^n_{\mathbb{Z}}$ and specialize modulo $\pi^n$. By Proposition 1.4.5, the endomorphism ring $\End(A)$ is identified with $O \otimes R$. Thus, upon this identification, $\End_{W_n}(\mathcal{A}) \simeq (O \otimes R) \otimes R S^{(n)}$. Similarly as in Theorem 3.1.1, this isomorphism is given by the natural action on the generalized $(O, S^{(n)})$-bimodule $M^{(n)}_P = O \otimes R S^{(n)}$

\[(O \otimes R) \otimes_R S^{(n)} \times O \otimes_R S^{(n)} \longrightarrow O \otimes R S^{(n)}
\]

\[\langle \alpha \otimes \delta \otimes s, \alpha' \otimes s' \rangle \longmapsto \alpha \alpha' (\varphi(P)(\delta)) \otimes ss',\]

where $S^{(n)}$ is regarded as left $R$-module via $\psi^{(n)}$ and $O$ as right $R$-module via $\varphi(P)$.

Denote by $\Lambda^{(n)}$ the commutator

\[\Lambda^{(n)} := \End_{W_n}(A, i) = \{ \lambda \in \End_{W_n}(A) : i(\alpha) \lambda = \lambda i(\alpha) \text{ for all } \alpha \in O \}.\]

Thus, it follows that

\[\Lambda^{(n)} = \{ \alpha \in (O \otimes R) \otimes_R S^{(n)} : \pi \alpha m = \alpha \pi m, \text{ for all } m \in M^{(n)}_P, \alpha \in O \} = \End_{SO}(M^{(n)}_P).\]

Let $\phi_P : \End(A, i) \hookrightarrow \End(\tilde{A}, \tilde{i})$ be the optimal embedding of Lemma 2.4.1. Since $\End_{W_n}(A, i) = \End(\tilde{A}, \tilde{i})$, the corresponding embedding

\[\phi^{(n)}_P : \End(A, i) \simeq R \hookrightarrow \End_{W_n}(A, i) = \Lambda^{(n)}, \quad (3.2.13)\]

is also optimal.

We deduce similarly that $\phi^{(n)}_P$ is given by the rule

\[R \hookrightarrow \End_{SO}(O \otimes_R S^{(n)})
\]

\[\delta \longmapsto \phi^{(n)}_P(\delta) : \alpha \otimes s \mapsto \alpha \delta \otimes s, \quad (3.2.14)\]

up to conjugation by $\End_{SO}(O \otimes_R S^{(n)})$. Moreover, upon the inclusion of algebras $\Lambda^{(n)} \subseteq \Lambda^{(m)}$, $m < n$, the restriction of $\phi^{(n)}_P$ to $\Lambda^{(n)}$ is precisely $\phi^{(n)}_P$.

**Lemma 3.2.2.** Write $\Lambda = \End(\tilde{A}, \tilde{i}) = \End_S(M^{(1)}_{P})$, then, for all $n$,

\[\Lambda^{(n)} = \{ \alpha \in \Lambda : d \cdot N(\alpha_-) \equiv 0 \mod p \cdot N(\mathfrak{P})^{n-1} \}.
\]

**Proof.** For any prime $q \neq p$ we have $S_q = S^{(n)}_q$, thus $(M^{(1)}_{P})_q = (M^{(n)}_P)_q$. It follows that if $q \neq p \Lambda^{(n)}_q = \Lambda^{(1)}_q = \Lambda_q$. Besides, $\Lambda^{(n)}_P$ corresponds to matrices in $M_2(S^{(n)}_P)$ that commute with $O_p = M_2(\mathbb{Z}_p)$, hence $\Lambda^{(n)}_P \simeq S^{(n)}_P$. Applying the description of $S^{(n)}$ above the desired result follows.

Let $P = [A, i], P' = [A', i'] \in \text{CM}(R)$ be a pair of Heegner points and assume that $[A', i']$ lies in $\{ A, i \}$, the isogeny class of $[A, i]$. By Lemma 1.3.10, both $(A, i)$ and $(A', i')$ are represented by suitable pairs $(J, \varphi), (J, \varphi) \in \hat{O}^\times \setminus \hat{B}^\times \times \text{Hom}(K, B)$. Since the identification $B \otimes Q K \simeq M_2(K) = \End(A)$ is given by means of $\varphi$ and the embeddings $\psi_p : R \hookrightarrow \Lambda$ only depend on $R$, we have a canonical isomorphism $M^{(n)}_P \simeq M^{(n)}_{P'}$.

Once we fix $M^{(n)}_P, M^{(n)}_{P'} \subset M^{(n)}_P$, the set of isogenies between $(A, i)/W_n$ and $(A', i')/W_n$, say $\text{Hom}_{W_n}(P, P') = \text{Hom}_{W_n}((A, i), (A', i'))$, is isomorphic with the set of $(O, S^{(n)})$-bimodule homomorphisms between $M^{(n)}_P$ and $M^{(n)}_{P'}$, say $\text{Hom}_{SO}(M^{(n)}_P, M^{(n)}_{P'})$. Consequently, $\text{Hom}_{W_n}(P, P')$ is a natural right $\Lambda^{(n)}$-module. Clearly, $(A, i) \simeq (A', i')$ over $W_n$ if and only if $\text{Hom}_{W_n}(P, P')$ is principal.
3.3 Čerednik-Drinfeld’s special fiber

In this section we exploit the results of §3.1 to describe the specialization of Heegner points on Shimura curves $X_0(D, N)$ at primes $p \mid D$. In order to do so, we will use the moduli interpretation of Čerednik-Drinfeld’s special fiber of $X_0(D, N)$ at $p$ introduced in §2.2.

Let $p$ be a prime dividing $D$, fix $\mathbb{F}$ an algebraic closure of $\mathbb{F}_p$ and let $\tilde{X}_0(D, N) = X_0(D, N) \times \text{Spec}(\mathbb{F}_p)$. By the work of Čerednik and Drinfeld, all irreducible components of $\tilde{X}_0(D, N)$ are reduced smooth conics, meeting transversally at ordinary double points.

By Theorem 2.2.1, singular points of $X_0(D, N)$ correspond to abelian surfaces $(\tilde{A}, \tilde{i})$ with QM by $\mathcal{O}$ such that $a(\tilde{A}) = 2$ and their corresponding bimodule is admissible at $p$, of type $(1, 1)$.

Let $P = [A, i] \in \text{CM}(R)$ be a Heegner point and let $\varphi(P) \in \text{CM}_{D,N}(R)$ be the optimal embedding attached to $P$. By Proposition 1.2.3, if such an optimal embedding exists, $R$ is maximal at $p$ and it either ramifies or is inert in $K$. Thus, $[\tilde{A}, \tilde{i}]$ is supersingular in $\tilde{X}_0(D, N)$ and the bimodule associated to $\tilde{P}$ is $\mathcal{M}_{\tilde{P}} = \mathcal{O} \otimes_R S$, by Theorem 3.1.1. Moreover, by Remark 2.4.2 the embedding $\phi_P$ is optimal.

**Proposition 3.3.1.** Assume that $p$ ramifies in $K$. Then $\mathcal{M}_{\tilde{P}}$ is admissible at $p$ and $(\mathcal{M}_{\tilde{P}})_p$ is of type $(1, 1)$. Furthermore, the algebra $\text{End}_{\mathcal{O}}(\mathcal{M}_{\tilde{P}})$ admits a natural structure of oriented Eichler order of level $Np$ in the quaternion algebra of discriminant $\frac{D}{p}$.

**Proof.** Since $\mathcal{O}_p = S_p$ is free as right $R_p$-module, we may choose a basis of $\mathcal{O}_p$ over $R_p$. In terms of this basis, the action of $\mathcal{O}_p$ on itself given by right multiplication is described by a homomorphism

$$f : \mathcal{O}_p \hookrightarrow M_2(R_p).$$

Since $p$ ramifies in $K$, the maximal ideal $\mathfrak{p}_{\mathcal{O}_p}$ of $\mathcal{O}_p$ is generated by an uniformizer $\pi$ of $R_p$ (cf. [74, Corollaire II.1.7]). This proves that $f(\mathfrak{p}_{\mathcal{O}_p}) \subseteq M_2(\pi R_p)$.

This allows us to conclude that $\mathcal{M}_p$ is admissible at $p$. Indeed, in matrix terms, the local bimodule $\mathcal{M}_p$ is given by the composition of $f$ with the natural embedding $M_2(R_p) \hookrightarrow M_2(S_p)$. Notice that $M_2(\pi R_p)$ is mapped into $M_2(\mathfrak{p}_{S_p})$ under that inclusion.

In order to check that $r_p = 1$, reduction modulo $\mathfrak{p}_{\mathcal{O}_p}$ yields an embedding

$$\tilde{f} : \mathcal{O}/\mathfrak{p}_\mathcal{O} \hookrightarrow M_2(\mathbb{F}_p)$$

because the residue field of $K$ at $p$ is the prime field $\mathbb{F}_p$. After extending to a quadratic extension of $\mathbb{F}_p$, this representation of $\mathcal{O}/\mathfrak{p}_\mathcal{O} \cong \mathbb{F}_{p^2}$ necessarily splits into the direct sum of the two embeddings of $\mathbb{F}_{p^2}$ into $\mathbb{F}$. Besides, we know that $\mathcal{M}_p = \mathcal{O}_p^s \times \mathfrak{p}_{\mathcal{O}_p}^r$ with $s + r = 2$. Consequently, we deduce that $\mathcal{M}_p \cong \mathcal{O}_p \times \mathfrak{p}_{\mathcal{O}_p}$ and $\mathcal{M}_p$ is of type $(1, 1)$.

Finally, since in this case $D_0 = \frac{D}{p}$ and $N_0 = p$, it follows from Theorem 2.1.6 that $\text{End}_{\mathcal{O}}(\mathcal{M}) \in \mathcal{E}(D/p, Np)$.

**Theorem 3.3.2.** If $p \mid D$, a Heegner point $P \in \text{CM}(R)$ of $X_0(D, N)$ reduces to a singular point of $\tilde{X}_0(D, N)$ if and only if $p$ ramifies in $K$.

**Proof.** As remarked above, $p$ is inert or ramifies in $K$. Assume first that $p$ ramifies in $K$. Then by Proposition 3.3.1 the bimodule $\mathcal{M}_{\tilde{P}}$ is admissible at $p$ and of type $(1, 1)$. Thus it follows that the point $\tilde{P} \in \tilde{X}_0(D, N)$ is singular.
Suppose now that $\tilde{P} = [A, \tilde{\tau}]$ is singular. Then its corresponding $\mathcal{O}$-$S$-bimodule $\mathcal{M}_{\tilde{P}}$ is admissible at $p$ and of type $(1, 1)$. Thus $\text{End}(\tilde{A}, \tilde{\tau}) = \text{End}_{D}^{S}(\mathcal{M}_{\tilde{P}}) \in \text{Pic}(D/p, Np)$ and the conjugacy class of the optimal embedding $\phi_{P} : R \hookrightarrow \text{End}_{D}^{S}(\mathcal{M}_{\tilde{P}})$ is an element of $\text{CM}_{p, Np}(R)$. Again by Proposition 1.2.3, if such an embedding exists, then $p$ can not be inert in $K$. Hence $p$ ramifies in $K$. □

That points $P \in \text{CM}(R)$ specialize to the non-singular locus of $\tilde{X}_{0}(D, N)$ when $p$ is unramified in $K$ was already known by the experts (cf. e.g. [48]) and can also be easily deduced by rigid analytic methods.

### 3.3.1 Heegner points and the singular locus

As explained in §2.2, for $p \mid D$, singular points of $\tilde{X}_{0}(D, N)$ are in one-to-one correspondence with isomorphism classes of $\mathcal{O}$-$S$-bimodules which are admissible at $p$ and of type $(1, 1)$. Such isomorphism classes are, in turn, in one-to-one correspondence with the set $\text{Pic}(D/p, Np)$ by means of the map $\mathcal{M} \mapsto \text{End}_{D}^{S}(\mathcal{M})$.

Let $P = [A, \tilde{\tau}] \in \text{CM}(R)$ be a Heegner point. As proved in Theorem 3.3.2, $P$ specializes to a singular point $\tilde{P}$ if and only if $p$ ramifies in $K$. If this is the case, the optimal embedding $\phi_{P} : R \hookrightarrow \text{End}_{D}^{S}(\mathcal{M}_{\tilde{P}})$ provides an element of $\text{CM}_{p, Np}(R)$.

Therefore, the map $\phi$ of (3.1.7), which was constructed by means of the reduction of $X_{0}(D, N)$ modulo $p$, can be interpreted as a map between CM-sets:

$$ \phi_{s} : \text{CM}(R) \longrightarrow \text{CM}_{p, Np}(R), $$

for $p$ ramified in $K$. Moreover, composing with the isomorphism $\text{CM}(R) \simeq \text{CM}_{D,N}(R)$ of (1.4.10) and the projection $\pi : \text{CM}_{p, Np}(R) \rightarrow \text{Pic}(D_{p}, Np)$ of (1.1.9), the resulting map $\text{CM}(R) \rightarrow \text{Pic}(D_{p}, Np)$ describes the specialization of $P \in \text{CM}(R)$ at $p$,

$$ \varepsilon_{s}(\tilde{P}) = \pi(\phi_{s}(\varphi(P))). $$

### Theorem 3.3.3

The map $\phi_{s} : \text{CM}_{D,N}(R) \longrightarrow \text{CM}_{p, Np}(R)$ is equivariant for the action of $W(D, N)$ and, up to sign, of $\text{Pic}(R)$. More precisely:

$$ \phi_{s}(J \ast \varphi) = [J]^{-1} \ast \phi_{s}(\varphi), \quad \phi_{s}(\omega_{m}(\varphi)) = \omega_{m}(\phi_{s}(\varphi)) $$

for all $m \parallel DN$, $[J] \in \text{Pic}(R)$ and $\varphi : R \hookrightarrow \mathcal{O}$ in $\text{CM}_{D,N}(R)$. Moreover, if $N$ is square free, $\phi_{s}$ is bijective.

**Proof.** The statement for Pic($R$) is Corollary 3.1.9. It follows from Theorem 3.1.10 and Remark 3.1.11 that $\phi_{s}(\omega_{m}(\varphi)) = \omega_{m}(\phi_{s}(\varphi))$ for all $m \parallel ND/p$. Since $p$ ramifies in $K$, $\omega_{p} \in W(D, N) \cong W_{p, Np}(R)$ preserves local equivalence by [74, Theorem II.3.1]. Hence the action of $\omega_{p}$ coincides with the action of some $[\mathfrak{P}] \in \text{Pic}(R)$. This shows that $\phi_{s}(\omega_{m}(\varphi)) = \omega_{m}(\phi_{s}(\varphi))$ for all $m \parallel ND$.

Finally, in order to check that $\phi_{s}$ is a bijection when $N$ is square free, observe that $\text{Pic}(R) \times W_{D,N}(R) = \text{Pic}(R) \times W_{p, Np}(R)$ acts freely and transitively both on $\text{CM}_{D,N}(R)$ and on $\text{CM}_{p, Np}(R)$. □
3.3.2 Heegner points and the smooth locus

Let \( \tilde{\Lambda}, \tilde{i} \in \tilde{X}_0(D, \mathcal{N}) \) be a non-singular point and assume that \( a(\tilde{\Lambda}) = 2 \). Let \( \tilde{\mathcal{M}}_\tilde{p} \) be its associated \((\mathcal{O}, \mathcal{S})\)-bimodule and write \( \tilde{H}_\tilde{p} \) for the unique \( \mathcal{O} \)-stable subgroup of \( \tilde{\Lambda} \) isomorphic to \( \alpha_p \). By Theorem 2.2.1, the irreducible component where \( \tilde{p} \) lies is characterized by the bimodule \( \tilde{\mathcal{M}}_\tilde{p} \) attached to the pure abelian surface \((\tilde{B}, \tilde{j})\) with QM by \( \mathcal{O} \) such that \( \Theta(\tilde{\Lambda}, \tilde{i}, \tilde{H}_\tilde{p}) = (\tilde{B}, \tilde{j}, \tilde{I}) \).

The subgroup scheme \( H_\tilde{p} \) gives rise to a degree-\( p \) isogeny \( \mu_\tilde{p} : \tilde{\Lambda} \to \tilde{B} = \tilde{\Lambda}/H_\tilde{p} \) such that \( \mu_\tilde{p}\tilde{\Lambda}(\alpha) = \tilde{j}(\alpha)\mu_\tilde{p} \) for all \( \alpha \in \mathcal{O} \).

Since \( \tilde{\Lambda} \cong \tilde{B} \cong \tilde{E}^2 \), we may fix an isomorphism of algebras \( \text{End}_\mathbb{F}(\tilde{\Lambda}) \to M_2(\mathcal{S}) \). Then each isogeny can be regarded as a matrix with coefficients in \( \mathcal{S} \). In order to characterize the bimodule \( \tilde{\mathcal{M}}_\tilde{p} \) in terms of \( \tilde{\mathcal{M}}_\tilde{p} \) we shall use the following proposition.

**Proposition 3.3.4.** Let \( (A, i) / \mathbb{F} \) and \( (\tilde{A}, \tilde{i}) / \mathbb{F} \) be abelian surfaces with QM by \( \mathcal{O} \) such that \( a(A) = 2 \). Let \( \mathcal{M} \) and \( \tilde{\mathcal{M}} \) be their associated \((\mathcal{O}, \mathcal{S})\)-bimodules. Consider the usual morphisms attached to each bimodule

\[
\begin{align*}
\text{f}_\mathcal{M} : \mathcal{O} &\to M_2(\mathcal{S}), \\
\text{f}_{\tilde{\mathcal{M}}} : \mathcal{O} &\to M_2(\mathcal{S}),
\end{align*}
\]

and assume there exists an isogeny \( \gamma : A \to \mathcal{A} \) such that \( \text{f}_\mathcal{M}(\alpha)\gamma = \gamma\text{f}_{\tilde{\mathcal{M}}}(\alpha) \) for all \( \alpha \in \mathcal{O} \). Then the image \( \gamma\mathcal{M} \), where \( \mathcal{M} \) is viewed as a free right \( \mathcal{S} \)-module of rank 2, is \( \mathcal{O} \)-stable. Furthermore \( \tilde{\mathcal{M}} \cong \gamma\mathcal{M} \) as \((\mathcal{O}, \mathcal{S})\)-bimodules.

**Proof.** The right \( \mathcal{S} \)-module \( \gamma\mathcal{M} \) is \( \mathcal{S} \)-free of rank 2 with basis \( \{\gamma e_1, \gamma e_2\} \), provided that \( \{e_1, e_2\} \) is a \( \mathcal{S} \)-basis for \( \mathcal{M} \). An element of \( \gamma\mathcal{M} \) can be written as:

\[
\gamma e_1a + \gamma e_2b = (\gamma e_1 \ \gamma e_2) \begin{pmatrix} a \\ b \end{pmatrix} = ( \begin{pmatrix} e_1 & e_2 \end{pmatrix} \gamma \begin{pmatrix} a \\ b \end{pmatrix}).
\]

Therefore any \( \alpha \in \mathcal{O} \) acts on it as follows:

\[
( e_1 \ e_2 ) \text{f}_\mathcal{M}(\alpha)\gamma \begin{pmatrix} a \\ b \end{pmatrix} = ( e_1 \ e_2 ) \gamma\text{f}_{\tilde{\mathcal{M}}}(\alpha) \begin{pmatrix} a \\ b \end{pmatrix} = ( \gamma e_1 \gamma e_2 ) \text{f}_{\tilde{\mathcal{M}}}(\alpha) \begin{pmatrix} a \\ b \end{pmatrix}.
\]

Thus \( \gamma\mathcal{M} \) is \( \mathcal{O} \)-stable and \( \mathcal{O} \) acts on it through the map \( \text{f}_{\tilde{\mathcal{M}}} \). We conclude that \( \gamma\mathcal{M} \cong \tilde{\mathcal{M}} \) as \((\mathcal{O}, \mathcal{S})\)-bimodules.

Applying the above proposition to \( \text{f}_\mathcal{M} = j, \text{f}_{\tilde{\mathcal{M}}} = j \) and \( \gamma = \mu_\tilde{p} \), we obtain that \( \mu_\tilde{p}\tilde{\mathcal{M}}_\tilde{p} = \tilde{\mathcal{M}}_\tilde{p} \).

Note that endomorphisms \( \lambda \in \text{End}(\tilde{A}) \) which fix \( H_\tilde{p} \) give rise to endomorphisms \( \tilde{\lambda} \in \text{End}(\tilde{B}) \). If in addition \( \lambda \in \text{End}(\tilde{\Lambda}, \tilde{i}) \) then \( \tilde{\lambda} \) lies in \( \text{End}(\tilde{B}, \tilde{j}) \).

**Lemma 3.3.5.** Every endomorphism in \( \text{End}(\tilde{\Lambda}, \tilde{i}) \) fixes \( H_\tilde{p} \).

**Proof.** Let \( \lambda \in \text{End}(\tilde{\Lambda}, \tilde{i}) \). Then \( \lambda(H_\tilde{p}) \) is either trivial or a subgroup scheme of rank \( p \). If \( \lambda(H_\tilde{p}) = 0 \), the statement follows. Assume thus that \( \lambda(H_\tilde{p}) \) is a subgroup scheme of rank \( p \). Since \( \tilde{\Lambda} \) is supersingular, \( \lambda(H_\tilde{p}) \) is isomorphic to \( \alpha_p \). Moreover, for all \( \alpha \in \mathcal{O} \) we have that \( \tilde{i}(\alpha)(\lambda(H_\tilde{p})) = \lambda(\tilde{i}(\alpha)(H_\tilde{p})) = \lambda(H_\tilde{p}) \). Therefore \( \lambda(H_\tilde{p}) \) is \( \mathcal{O} \)-stable and consequently \( \lambda(H_\tilde{p}) = H_\tilde{p} \), by uniqueness. \( \square \)
By the preceding result, there is a monomorphism \( \text{End}(\tilde{A}, \tilde{t}) \to \text{End}(\tilde{B}, \tilde{j}) \) corresponding, via bimodules, to the monomorphism \( \delta_p : \text{End}_O^S(\mathcal{M}_\mathcal{P}) \to \text{End}_O^S(\mathcal{M}_\mathcal{P}^f) \) that maps every \( \lambda \in \text{End}_O^S(\mathcal{M}_\mathcal{P}) \) to its single extension to \( \mathcal{M}_\mathcal{P}^f \supset \mathcal{M}_\mathcal{P} \).

Let \( (N, \psi) \in \text{CM}_{O, S}^M(R) \). By §2.1.3, \( N = \mathcal{M}(A, \tilde{t}) \) for some abelian surface \((A', \tilde{t})\) with QM by \( \mathcal{O} \). As explained in §2.2, whether \([A', \tilde{t}]\) is a singular point of \( \tilde{X}_0(D, N) \) or not depends on the local isomorphism class of \( \mathcal{M}(A', \tilde{t}) \) at \( p \). Since \( \mathcal{M}(A, \tilde{t}) \) and \( \mathcal{M}_\mathcal{P} \) are locally isomorphic, \([A', \tilde{t}] = \tilde{Q} \notin \tilde{X}_0(D, N)_{\text{sing}} \) and we may write \( \mathcal{M}(A, \tilde{t}) = \mathcal{M}_{\tilde{Q}} \). The composition of \( \psi \) with \( \delta_{\tilde{Q}} \) gives rise to an embedding \( R \hookrightarrow \text{End}_O^S(\mathcal{M}_{\tilde{Q}}) \), which we claim is optimal.

Indeed, since \( \mu_{\tilde{Q}} \) has degree \( p \), \([ \mathcal{M}_{\tilde{Q}} : \mathcal{M}_{\tilde{Q}} ] = p \). Hence the inclusion \( \text{End}_O^S(\mathcal{M}_{\tilde{Q}}) \subset \text{End}_O^S(\mathcal{M}_{\tilde{Q}}^f) \) has also \( p \)-power index. Due to the fact that \( \psi \) is optimal,

\[
\delta_{\tilde{Q}} \circ \psi(R) = \delta_{\tilde{Q}}(\text{End}_O^S(\mathcal{M}_{\tilde{Q}}) \cap \psi(K)) \subseteq \text{End}_O^S(\mathcal{M}_{\tilde{Q}}^f) \cap \delta_{\tilde{Q}} \circ \psi(K) =: \delta_{\tilde{Q}} \circ \psi(R'),
\]

where \( R' \) is an order in \( K \) such that \( R \subseteq R' \) has \( p \)-power index. Recall that \( R \) is maximal at \( p \), hence we conclude that \( R' = R \) and \( \delta_{\tilde{Q}} \circ \psi \) is optimal.

Since \( H_{\tilde{Q}} \) is the single \( \mathcal{O} \)-stable subgroup scheme of \( A' \) of rank \( p \), \( \mathcal{M}_{\tilde{Q}} \) is the single \( \mathcal{O} \)-stable extension of \( \mathcal{M}_Q \) of index \( p \). Moreover, it is characterized by the local isomorphism class of \( \mathcal{M}_{\tilde{Q}} \) at \( p \). More precisely, if \( \mathcal{M}_\mathcal{P} \) and \( \mathcal{M}_{\tilde{Q}} \) are locally isomorphic, then \( \mathcal{M}_{\mathcal{P}} \) and \( \mathcal{M}_{\tilde{Q}} \) must be locally isomorphic also. Thus the correspondence \( (N = \mathcal{M}_{\tilde{Q}}, \psi) \to (\mathcal{M}_{\tilde{Q}}, \delta_{\tilde{Q}} \circ \psi) \) induces a map

\[
\delta : \text{CM}_{O, S}^{M_\mathcal{P}}(R) \to \text{CM}_{O, S}^{M_\mathcal{P}}(R),
\]

(3.3.17)

Both sets are equipped with an action of \( \text{Pic}(R) \) and involutions \( \omega_{\mathcal{O}^n} \), for all \( q^n \parallel DN \), \( q \neq p \). Besides, since \( \mathcal{M}_{\mathcal{P}} \) is admissible of type \((2,0)\) or \((0,2)\), we identify \( \text{CM}_{O, S}^{M_\mathcal{P}}(R) \) with \( \text{CM}_{D/p, N}(R) \) by Theorem 2.1.6.

**Lemma 3.3.6.** The map \( \delta : \text{CM}_{O, S}^{M_\mathcal{P}}(R) \to \text{CM}_{D/p, N}(R) \) is equivariant under the actions of \( \text{Pic}(R) \) and \( W(D/p, N) \).

**Proof.** Let \( (\mathcal{M}_{\tilde{Q}}, \psi) \in \text{CM}_{O, S}^{M_\mathcal{P}}(R) \), let \([J] \in \text{Pic}(R)\) and write \( \Lambda = \text{End}_O^S(\mathcal{M}_{\tilde{Q}}) \). We denote by \( \tilde{Q}^{[J]} \in \tilde{X}_0(D, N) \) the point attached to the bimodule \([J] \ast \mathcal{M}_{\tilde{Q}} = \psi(J^{-1}) \Lambda \otimes \mathcal{M}_{\tilde{Q}} = \mathcal{M}_{\tilde{Q}^{[J]}} \).

Write \( \Lambda' = \text{End}_O^S(\mathcal{M}_{\tilde{Q}}^f) \supset \Lambda \) and consider the bimodule \([J] \ast \mathcal{M}_{\tilde{Q}} = \psi(J^{-1}) \Lambda' \otimes \Lambda, \mathcal{M}_{\tilde{Q}^{[J]}} \in \text{Pic}_S(\mathcal{M}_{\mathcal{P}}^f) \). Then \([J] \ast \mathcal{M}_{\tilde{Q}} \subset [J] \ast \mathcal{M}_{\tilde{Q}}^f \) is \( \mathcal{O} \)-stable of index \( p \) and \([J] \ast \mathcal{M}_{\tilde{Q}} = \mathcal{M}_{\tilde{Q}^{[J]}} \) by uniqueness. Since \([J] \ast \psi \) and \([J] \ast (\delta_{\tilde{Q}} \circ \psi) \) are given by the action of \( R \) on \( \mathcal{M}_{\tilde{Q}^{[J]}} \) and \( \mathcal{M}_{\tilde{Q}^{[J]}} \) respectively,

\[
\delta([J] \ast (\mathcal{M}_{\tilde{Q}}, \psi)) = (\mathcal{M}_{\tilde{Q}^{[J]}}, \delta_{\tilde{Q}^{[J]}} \circ [J] \ast \psi) = ([J] \ast \mathcal{M}_{\tilde{Q}}^f, [J] \ast (\delta_{\tilde{Q}} \circ \psi)) = [J] \ast (\delta_{\tilde{Q}}, \psi).
\]

As for the Atkin-Lehner involution \( \omega_{\mathcal{O}^n} \), let \( \Omega_{\mathcal{O}} \) be the single two-sided ideal of \( \mathcal{O} \) of norm \( q^n \). Again \( \Omega_{\mathcal{O}} \otimes \mathcal{M}_{\tilde{Q}}^f \) is an \( \mathcal{O} \)-stable extension of \( \Omega_{\mathcal{O}} \otimes \mathcal{M}_{\tilde{Q}} \) of index \( p \). Hence \( \mathcal{M}_{\tilde{Q}}^f \otimes \mathcal{M}_{\tilde{Q}}^f = \mathcal{M}_{\omega_{\mathcal{O}^n}(\tilde{Q})}^f \), where \( \omega_{\mathcal{O}^n}(\tilde{Q}) \in \tilde{X}_0(D, N) \) is the non-singular point attached to \( \Omega_{\mathcal{O}} \otimes \mathcal{M}_{\tilde{Q}}^f \). This concludes that \( \delta \circ \omega_{\mathcal{O}^n} = \omega_{\mathcal{O}^n} \circ \delta \). □
3.4. SUPERSINGULAR VS. ORDINARY GOOD REDUCTION

Let \( P = [A, i] \in \text{CM}(R) \) be a Heegner point such that \( \tilde{P} \notin \tilde{X}_0(D, N)_{\text{sing}} \). Let \( \mathcal{M}_{\tilde{P}} \) the bimodule attached to its specialization \( \tilde{P} = [\tilde{A}, \tilde{i}] \in \tilde{X}_0(D, N) \). Recall the map \( \phi : \text{CM}_{D,N}(R) \rightarrow \bigsqcup_M \text{CM}_{D,M}^{\mathcal{M}_S}(R) \) of (3.1.7), induced by the natural injection \( \text{End}(A, i) \hookrightarrow \text{End}(\tilde{A}, \tilde{i}) \) and the correspondences of (1.4.10) and (2.1.1).

The aim of the rest of this section is to modify \( \phi \) in order to obtain a map

\[
\phi_c : \text{CM}_{D,N}(R) \rightarrow \text{CM}_{D,N}(R) \sqcup \text{CM}_{D,N}(R)
\]

which composed with the projection \( \pi : \text{CM}_{D,N}(R) \sqcup \text{CM}_{D,N}(R) \rightarrow \text{Pic}(\frac{D}{p}, N) \sqcup \text{Pic}(\frac{D}{p}, N) \) and the correspondence of (1.4.10), assigns to \( D, N \) the Eichler order that describes the irreducible component at which \( P \) specializes.

**Theorem 3.3.7.** The embedding \( \text{End}(A, i) \hookrightarrow \text{End}(\tilde{A}, \tilde{i}) \hookrightarrow \text{End}(\tilde{B}, j) \in \text{Pic}(\frac{D}{p}, N) \) induces a map

\[
\phi_c : \text{CM}_{D,N}(R) \rightarrow \text{CM}_{D,N}(R) \sqcup \text{CM}_{D,N}(R),
\]

which is equivariant for the action of \( \text{W}_{\frac{D}{p}, N}(R) \) and satisfies the reciprocity law \( \phi_c([J] * \varphi) = [J]^{-1} * \phi_c(\varphi) \) for all \( [J] \in \text{Pic}(R) \) and \( \varphi \in \text{CM}_{D,N}(R) \).

If \( N \) is square free, then \( \phi_c \) is bijective, i.e. it establishes a bijection of \( \text{W}_{\frac{D}{p}, N}(R) \) sets between \( \text{CM}_{D,N}(R)/\omega_p \) and \( \text{CM}_{D,N}(R) \).

Notice that we are considering \( \text{W}(\frac{D}{p}, N) \) as a subgroup of \( \text{W}(D, N) \), so that \( \text{W}(\frac{D}{p}, N) \) acts naturally on \( \text{CM}_{D,N}(R) \). Since points in \( \text{CM}(R) \) have good reduction, \( p \) is inert in \( K \) by Theorem 3.3.2. Therefore, by [74, Theorem 3.1], \( m_p = 2 \) and the subgroups \( \text{W}_{D,N}(R)/\langle \omega_p \rangle \) and \( \text{W}_{\frac{D}{p}, N}(R) \) are isomorphic. Hence we can consider \( \text{CM}_{D,N}(R)/\omega_p \) as a \( \text{W}_{\frac{D}{p}, N}(R) \) set.

**Proof.** The map \( \phi_c : \text{CM}_{D,N}(R) \rightarrow \text{CM}_{D,N}(R) \sqcup \text{CM}_{D,N}(R) \) arises as the map composition

\[
\text{CM}_{D,N}(R) \xrightarrow{\phi} \bigsqcup_M \text{CM}_{D,M}^{\mathcal{M}_S}(R) \xrightarrow{\delta} \text{CM}_{D/p,N}(R) \sqcup \text{CM}_{D/p,N}(R).
\]

Then Lemma 3.3.6, Theorem 3.1.8 and Theorem 3.1.10 prove the first statement.

Assume that \( N \) is square free. Then freeness and transitivity of the action of \( \text{W}_{D/p,N}(R) \times \text{Pic}(R) \) on both \( \text{CM}_{D,N}(R)/\omega_p \) and \( \text{CM}_{D,N}(R) \) show that the corresponding map between them is bijective. Since the Atkin-Lehner involution \( \omega_p \) exchanges the two components of \( \text{CM}_{D/p,N}(R) \sqcup \text{CM}_{D/p,N}(R) \), we conclude that \( \phi_c : \text{CM}_{D,N}(R) \rightarrow \text{CM}_{D/p,N}(R) \sqcup \text{CM}_{D/p,N}(R) \) is also bijective.

\[\square\]

### 3.4 Supersingular vs. ordinary good reduction

Exploiting the results of §3.1, we can also describe the supersingular reduction of Heegner points at primes \( q \) of good reduction of the Shimura curve \( X_0(D, N) \). Let \( q \nmid DN \) be a prime, let \( F \) be an algebraic closure of \( F_q \), and let \( \tilde{X}_0(D, N) = X_0(D, N) \times F_q \). Recall that the set of supersingular points \( \tilde{X}_0(D, N)_{ss} \) is in one-to-one correspondence with \( \text{Pic}(Dq, N) \) by means of (2.3.5).
Let $P = [A, i] \in \text{CM}(R)$ be a Heegner point and assume that the conductor $c$ of $R$ is coprime to $q$. Since $A$ is isomorphic to a product of two elliptic curves with CM by $R$, it follows from the classical work of Deuring that $A$ has supersingular specialization if and only if $q$ does not split in $K$.

First, we proceed to describe the specialization of those Heegner points that lie in the non-supersingular locus $\tilde{X}_0(D, N) \setminus \tilde{X}_0(D, N)_{ss}$.

**Proposition 3.4.1.** Let $P = [A, i] \in \text{CM}(R)$ be a Heegner point and assume that $\tilde{P} = [\tilde{A}, \tilde{i}] \notin \tilde{X}_0(D, N)_{ss}$ (i.e. $p$ splits in $K$). Then the natural maps $\phi_P : \text{End}(A, i) \hookrightarrow \text{End}(\tilde{A}, \tilde{i})$ and $\text{End}(A) \hookrightarrow \text{End}(\tilde{A})$ are isomorphisms.

**Proof.** We have $A \simeq E_1 \times E_2$, where $E_1$ and $E_2$ are isogenous elliptic curves with CM by $R$. Write $\tilde{E}_1$ and $\tilde{E}_2$ for their specialization modulo $q$. Since $[\tilde{A}, \tilde{i}] \notin \tilde{X}_0(D, N)_{ss}$, each curve $\tilde{E}_i$ is an ordinary elliptic curve over $\mathbb{F}$ and $K = \text{End}^0(E_1) = \text{End}^0(\tilde{E}_1)$. This implies that $\text{End}^0(\tilde{A}) = M_2(K) = \text{End}^0(A)$ and consequently $\phi_P(\text{End}^0(A, i)) = \text{End}^0(\tilde{A}, \tilde{i})$. Finally, by Remark 2.4.2, the map $\phi_P$ is injective and satisfies $\phi_P(\text{End}^0(A, i)) \cap \text{End}(\tilde{A}, \tilde{i}) = \phi_P(\text{End}(A, i))$. Therefore $\phi_P(\text{End}(A, i)) = \text{End}(\tilde{A}, \tilde{i})$ and we conclude that $\phi_P$ is an isomorphism. Similarly, the optimality of $\text{End}(A) \hookrightarrow \text{End}(\tilde{A})$ implies $\text{End}(A) \simeq \text{End}(\tilde{A})$. 

Throughout the rest of this section assume that $P \in \text{CM}(R)$ is such that $\tilde{P} = [\tilde{A}, \tilde{i}] \in \tilde{X}_0(D, N)_{ss}$ (i.e. $p$ does not split in $K$). In this case, the map $\phi$ of (3.1.7) becomes

$$\phi_{ss} : \text{CM}_{D,N}(R) \rightarrow \text{CM}_{D,q,N}(R)$$

by means of the natural identification (3.1.9). Composing with the natural projection

$$\pi : \text{CM}_{D,q,N}(R) \rightarrow \text{Pic}(D_q, N)$$

and the correspondence of (1.4.10), one obtains a map $\text{CM}(R) \rightarrow \text{Pic}(D_q, N)$ which assigns to $P = [A, i] \in \text{CM}(R)$ the Eichler order $\text{End}(\tilde{A}, \tilde{i})$ that describes its supersingular specialization

$$\varepsilon_{ss}(\tilde{P})) = \pi(\phi_{ss}(\phi(P))).$$

**Theorem 3.4.2.** The map $\phi_{ss} : \text{CM}_{D,N}(R) \rightarrow \text{CM}_{D,q,N}(R)$ is equivariant for the action of $W(D, N)$ and, up to sign, of $\text{Pic}(R)$. More precisely:

$$\phi_{ss}([J] \ast \varphi) = [J]^{-1} \ast \phi_{ss}(\varphi), \quad \phi_{ss}(\omega_m(\varphi)) = \omega_m(\phi_{ss}(\varphi))$$

for all $m \mid DN$, $[J] \in \text{Pic}(R)$ and $\varphi : R \hookrightarrow \mathcal{O}$ in $\text{CM}_{D,N}(R)$.

Assume that $N$ is square free. If $q$ ramifies in $K$, the map $\phi_{ss}$ is bijective. If $q$ is inert in $K$, the induced map

$$\text{CM}_{D,N}(R) \xrightarrow{\phi_{ss}} \text{CM}_{D,q,N}(R) \rightarrow \text{CM}_{D,q,N}(R)/\omega_q$$

is also bijective.

**Proof.** The first statement follows directly from Theorem 3.1.8 and Theorem 3.1.10. Assume that $N$ is square free. If $p$ ramifies in $K$, we have that $W_{D,N}(R) = W_{D,q,N}(R)$. Then $\text{Pic}(R) \times W_{D,N}(R)$ acts simply and transitively on both $\text{CM}_{D,N}(R)$ and $\text{CM}_{D,N}(R)$ and $\phi_{ss}$ is bijective. If $p$ is inert in $K$, then $W_{D,N}(R) = W_{D,q,N}(R)/\omega_q$ and the last assertion holds. 

3.5 Deligne-Rapoport-Buzzard special fiber

In this section we exploit the results of §3.4 to describe the specialization of Heegner points on Shimura curves $X_0(D, N)$ at primes $q \parallel N$. In order to do so, we will use the moduli interpretation of Deligne-Rapoport-Buzzard special fiber of $X_0(D, N)$ at $q$ introduced in §2.3.

Let $q$ be a prime dividing exactly $N$, fix $\mathbb{F}$ an algebraic closure of $\mathbb{F}_q$ and let $\tilde{X}_0(D, N)$ denote the special fiber at $q$. Recall that $\tilde{X}_0(D, N)$ has two irreducible components isomorphic to $\tilde{X}_0(D, N/q)_\mathbb{F}$, meeting transversally at the supersingular points of $\tilde{X}_0(D, N/q)$. As in §2.3, write $\delta, \delta\omega_i : \tilde{X}_0(D, N) \to \tilde{X}_0(D, N/q)$ for the degeneracy maps described in Appendix A.

Let $P = [A, i] \in \text{CM}(R)$ be a Heegner point and let $\tilde{P} = [\tilde{A}, \tilde{i}] \in \tilde{X}_0(D, N)$ denote its specialization. Assume, in addition, that $q$ does not divide the conductor of $R$. According to the description of the special fiber given in §2.3, the point $\tilde{P}$ is singular if and only if $\delta(\tilde{A}, \tilde{i})$ is supersingular, or, equivalently, if and only if $(A, i)$ is supersingular because $(A, i)$ and $\delta(A, i)$ are isogenous. By Proposition 1.2.3, the fact that $\text{CM}(R) \neq \emptyset$ implies that $q$ is not inert in $K$. Since $A$ is the product of two elliptic curves with CM by $R$, we obtain the following result, with the reader should compare with Theorem 3.3.2.

**Proposition 3.5.1.** If $p \mid N$ and $p \nmid c$, a Heegner point $P \in \text{CM}(R)$ reduces to a singular point of $X_0(D, N)$ if and only if $q$ ramifies in $K$.

**Proof.** The point $P$ specializes to a singular point if and only if $(\tilde{A}, \tilde{i})$ is supersingular. Since $q$ is not inert in $K$ and any elliptic curve with CM by $R$ has supersingular specialization if and only if $q$ is not split in $K$, we conclude that $q$ ramifies in $K$. \qed

3.5.1 Heegner points and the smooth locus

Let $O' \supset O$ be an Eichler order in $B$ of level $N/q$. Notice that $O'$ defines the Shimura curve $X_0(D, N/q)$. Let $\text{CM}(R)$ be a set of Heegner points that specialize to non-singular points in $X_0(D, N)$ and let $P \in \text{CM}(R)$. The inclusion $O' \supset O$ defines one of the two degeneracy maps $d : X_0(D, N) \to X_0(D, N/q)$ as in Appendix A. By the identification of (1.4.10), $P$ corresponds to $\varphi(P) \in \text{CM}_{D,N}(R)$ and its image $d(P)$ corresponds to $\varphi(d(P)) \in \text{CM}_{D,N/q}(R')$, where $\varphi(P)(R') = \varphi(P)(K) \cap O'$ and $\varphi(d(P)) : R' \hookrightarrow O'$ is the restriction of $\varphi(P)$ to $R'$. Since $[O' : O] = q$, the inclusion $R \subseteq R'$ has also $q$-power index. According to the fact that the conductor of $R$ is prime to $q$, we deduce that $R = R'$.

Hence, restricting the natural degeneracy maps $X_0(D, N) \Rightarrow X_0(D, N/q)$ to $\text{CM}(R)$, we obtain a map

$$\text{CM}_{D,N}(R) \to \text{CM}_{D,N/q}(R) \sqcup \text{CM}_{D,N/q}(R). \quad (3.5.21)$$

Observe that we have the analogous situation to §3.3.2 and Theorem 3.3.7. We have a map $\text{CM}_{D,N}(R) \to \text{CM}_{D,N/q}(R) \sqcup \text{CM}_{D,N/q}(R)$, which is clearly $\text{Pic}(R) \times W(D, N/q)$ equivariant and a bijection if $N$ is square free, with the property that the natural map

$$\text{CM}_{D,N/q}(R) \sqcup \text{CM}_{D,N/q}(R) \Rightarrow \text{Pic}(D, N/q) \sqcup \text{Pic}(D, N/q)$$

gives the irreducible component where the point lies. Notice that there are two irreducible components and $\# \text{Pic}(D, N/q) = 1$, since $D$ is the reduced discriminant of an indefinite quaternion algebra.
3.5.2 Heegner points and the singular locus

Let $O' \supset O$ be as above, let $(A, i)$ be an abelian surface with QM by $O'$ and let $(A, i)$ be an abelian surface with QM by $O'$. Given the triple $(A, i, C)$, write $P = [A, i, C]$ for the isomorphism class of $(A, i, C)$, often regarded as a point on $X_0(D, N)(\mathbb{Q})$ by Appendix A.

Let $P = [A, i, C] \in \text{CM}(\mathbb{R})$ be a Heegner point with singular specialization in $\tilde{X}_0(D, N)$. Then $[A, i] \in X_0(D, N/q)$ is the image of $P$ through the natural map $d : X_0(D, N) \to X_0(D, N/q)$ given by $O' \supset O$. Using the same argumentation as in the above setting, we can deduce that $\text{End}(A, i) = \text{End}(A, i, C) = \mathbb{R}$.

Let $[\tilde{A}, \tilde{i}, \tilde{C}] \in \tilde{X}_0(D, N)$ be its specialization. Since it is supersingular, $\tilde{C} = \ker(F_{\tilde{A}/\mathbb{F}})$. Thanks to the fact that the $F_{\tilde{A}/\mathbb{F}}$ lies in the center of $\text{End}(\tilde{A})$, we obtain that $\text{End}(\tilde{A}, \tilde{i}, \tilde{C}) = \text{End}(\tilde{A}, \tilde{i})$. Thus the embedding $\text{End}(A, i, C) \hookrightarrow \text{End}(\tilde{A}, \tilde{i}, \tilde{C})$ is optimal and it is identified with $\text{End}(A, i) \hookrightarrow \text{End}(\tilde{A}, \tilde{i})$, which has been considered in §3.4. In conclusion we obtain a map $\phi_s : \text{CM}_{D, N}(\mathbb{R}) \to \text{CM}_{Dq, N/q}(\mathbb{R})$ as in §3.3.1 and, since $q$ ramifies in $K$, a result analogous to Theorem 3.3.3.

**Theorem 3.5.2.** The map

$$\phi_s : \text{CM}_{D, N}(\mathbb{R}) \to \text{CM}_{Dq, N/q}(\mathbb{R})$$

is equivariant for the action of $W(D, N)$ and, up to sign, of $\text{Pic}(\mathbb{R})$. More precisely:

$$\phi_s([J] * \varphi) = [J]^{-1} * \phi_s(\varphi), \quad \phi_s(\omega_m(\varphi)) = \omega_m(\phi_s(\varphi))$$

for all $m \parallel DN$, $[J] \in \text{Pic}(\mathbb{R})$ and $\varphi : \mathbb{R} \to O$ in $\text{CM}_{D, N}(\mathbb{R})$. Moreover, it is bijective if $N$ is square free.

3.6 Numerical example

Let $X = X_0(77, 1)$ be the Shimura curve of discriminant $D = 77$. By the theory of Čerednik-Drinfeld, the dual graph of the special fiber $\tilde{X}$ of $X$ at $p = 7$ is given by (cf. [42, §3] for a step-by-step guide on the computation of these graphs, using MAGMA):

$$\ell(v_2) = 3, \quad \ell(v_1) = 2, \quad \ell(v_1') = 1$$

Hence the special fiber $\tilde{X}$ has the form:
where each of the four irreducible components \( v_2, v'_2, v_3, v'_3 \) are smooth curves of genus 0 over \( \mathbb{F}_7 \), meeting transversally at points whose coordinates lie in \( \mathbb{F}_{49} \). The involution \( \omega_{11} \) fixes each of these components, while the straight horizontal line is the symmetry axis of the Atkin-Lehner involution \( \omega_7 \). Let \( x_1, y_1, x_3, y_3 \) denote the four intersection points which lie on this axis. The subindex 1 or 3 stands for the thickness of the points (cf. Chapter 4 for the definition).

Let \( K \) be the imaginary quadratic field \( \mathbb{Q}(\sqrt{-77}) \) and let \( R \) be its maximal order. By Theorem 3.3.2, any Heegner point in \( \text{CM}(R) \) specializes to a singular point. By [56, §1], every \( P \in \text{CM}(R) \) is fixed by \( \omega_{77} \) and it follows from the above discussion that its specialization at \( \tilde{X} \) lies in the symmetry line of \( \omega_7 \). Thus \( \tilde{P} \) is one of the singular points \( \{x_1, y_1, x_3, y_3\} \).

By Theorem 3.3.3 and upon the identification of (1.4.10), the map \( \phi_s \) provides a bijection between \( \text{CM}(R) \) and \( \text{CM}_{11,7}(R) \). Moreover, composing with the natural projection \( \pi: \text{CM}_{11,7}(R) \rightarrow \text{Pic}(11,7) \), one obtains the specialization of the points in \( \text{CM}(R) \) at \( \tilde{X} \). Via \( \phi_s \), the action of \( \text{Pic}(R) \) on \( \text{CM}_{11,7}(R) \) becomes the Galois action of \( \text{Gal}(H_R/K) \approx \text{Pic}(R) \) by Shimura’s reciprocity law [66, Main Theorem I]. This allows us to explicitly compute the specializations of the points \( P \in \text{CM}(R) \) to the set \( \{x_1, y_1, x_3, y_3\} \).

Namely, we computed with Magma that \( \text{Pic}(R) = \langle [I], [J] \rangle \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \). Let \( \sigma: \text{Pic}(R) \rightarrow \text{Gal}(H_R/K) \),

stand for the inverse of Artin’s reciprocity map. We obtained that \( P \) and \( P^{\sigma([J]I)} \) specialize to the same singular point of thickness 3, say \( x_3 \); \( P^{\sigma([I]J)} \) and \( P^{\sigma([J]I)} \) specialize to the same singular point of thickness 1, say \( x_1 \); \( P^{\sigma([J])} \) and \( P^{\sigma([J]I)} \) specialize to \( y_1 \); and \( P^{\sigma([J])} \) and \( P^{\sigma([J]I)} \) specialize to \( y_3 \).
Chapter 4

Equations of hyperelliptic Shimura curves

4.1 Semi-stable hyperelliptic curves

Let $X$ be a smooth, geometrically connected, projective curve of genus $g > 1$ defined over a field $k$. It is said that $X$ is a hyperelliptic curve over $k$ if there exists a finite separable morphism $X \to \mathbb{P}_k^1$ of degree 2. Whenever there is no risk of confusion about the field $k$ we shall only say that $X$ is hyperelliptic. This is equivalent to the existence of an involution $\omega$ defined over $k$ such that the quotient curve $X/\omega$ has genus 0 and $k$-rational points. When this is the case, this involution is unique and is called the hyperelliptic involution. Moreover, it is well known that there exist functions $x, y \in k(X)$ satisfying a relation of the type

$$y^2 + Q(x)y + P(x) = 0, \quad P, Q \in k[x], \quad 2g + 1 \leq \max\{\deg P, 2\deg Q\} \leq 2g + 2,$$

(4.1.1)

and such that the function field of $X$ is $k(X) = k(x, y)$. The hyperelliptic involution $\omega$ is then given by $(x, y) \mapsto (x, Q(x) - y)$ and, for the particular case that $\text{char}(k) \neq 2$, we can take $Q(x) = 0$.

We shall denote by $\text{WP}(X)$ the set of Weierstrass points of $X$. It coincides with the set of fixed points of $\omega$. Hence, $\text{WP}(X)$ contains the point at infinity if $\deg(Q(x)^2 - 4P(x)) = 2g + 1$, or a pair of points at infinity if $\deg(Q(x)^2 - 4P(x)) = 2g + 2$. In the later case, both points are either $k$-rational or Galois conjugate over a quadratic extension of $k$.

If $k = \mathbb{Q}$, a Weierstrass model for $X$ is a model $W$ over $\mathbb{Z}$, i.e. a normal fibered surface over $\text{Spec}(\mathbb{Z})$ with generic fiber $X$, such that $\omega$ can be extended to an involution on $W$, which we still denote by $\omega$, and the quotient $W/\langle \omega \rangle$ is smooth over $\mathbb{Z}$. We shall also denote by $\text{WP}(W)$ the set of fixed points of $\omega$ on $W$. By [51, Remark 3.5], every smooth model of $\mathbb{P}_\mathbb{Q}^1$ is isomorphic to $\mathbb{P}_\mathbb{Z}^1$. Hence, any Weierstrass model $W$ satisfies $W/\langle \omega \rangle = \mathbb{P}_\mathbb{Z}^1$ and, by [46, Lemme 1], $W$ is the projective closure of the affine curve defined by:

$$y^2 + Q(x)y + P(x) = 0, \quad P, Q \in \mathbb{Z}[x], \quad 2g + 1 \leq \max\{\deg P, 2\deg Q\} \leq 2g + 2.$$

(4.1.2)

Given such a hyperelliptic equation, we define the discriminant of the Weierstrass model as
4.1. SEMI-STABLE HYPERELLIPTIC CURVES

follows:

$$
\Delta(W) = \begin{cases}
2^{-4(g+1)}\text{disc}(R(x)) & \text{if } \deg R(x) = 2g + 2, \\
2^{-4(g+1)}c^2\text{disc}(R(x)) & \text{if } \deg R(x) = 2g + 1,
\end{cases}
$$

where $R(x) = Q(x)^2 - 4P(x)$ and $c$ is its leading coefficient. The special fiber $W_p$ of $W$ at $p$ is smooth over $F_p$ if and only if $p \nmid \Delta(W)$ (c.f. [46]).

Assume now that $k$ is algebraically closed, let $C$ be an algebraic curve over $k$, and let $x \in C(k)$. We say that $x$ is an ordinary double point if

$$
\tilde{O}_{C,x} \simeq k[[u,v]]/(uv) \simeq k[[u,v]]/(u^2 - v^2),
$$

where $\tilde{O}_{C,x}$ is the completion of the local ring $O_{C,x}$. A curve $C$ over $k$ is said to be semi-stable if it is reduced and all its singular points are ordinary double points.

Let $S$ be an affine Dedekind scheme of dimension 1, with fraction field $K$. Let $C$ be a normal, connected, projective curve over $K$. A model of $C$ over $S$ is a normal fibred surface $C \to S$ together with an isomorphism of its generic fiber $f : C_0 \to C$. We say that the model $C \to S$ is semi-stable if for each $s \in S$ the geometric fiber $C_s \times_{k(s)} k(s)$ is semi-stable over $k(s)$, where $k(s)$ stands for the residue field of $S$ at $s$.

**Proposition 4.1.1.** [47, Corollary 10.3.22] Let $C \to S$ be a semi-stable model of a curve $C$. Let $s \in S$, and let $x \in C_s$ be a singular point of $C_s$. Then there exists a Dedekind scheme $S'$, étale over $S$, such that any point $x' \in C' := C \times_S S'$ above $x$ lying on $C'_{s'}$ is an ordinary double point in $C'_{s'} \to \text{Spec}(k(s'))$. Moreover,

$$
\tilde{O}_{C',x'} \cong \tilde{O}_{S',s'}[[u,v]]/(uv - c) \quad c \in m_{s'}O_{S',s'},
$$

where $\tilde{O}_{C',x'}$ and $\tilde{O}_{S',s'}$ are the completions of $O_{C',x'}$ and $O_{S',s'}$ respectively.

If $C$ is smooth, then $c \neq 0$. Let $e_x$ be the normalized valuation of $c$ in $O_{S',s'}$, then $e_x$ does not depend on the scheme $S'$ chosen.

**Definition 4.1.2.** The value $e_x$ described in the above proposition is called the thickness of the singularity $x \in C_s$.

**Theorem 4.1.3.** Let $W \to \text{Spec}(\mathbb{Z})$ be a Weierstrass semi-stable model, and let $p$ be an odd prime of bad reduction. Let $P \in W_p(\mathbb{F}_p)$ be a singular point lying in an affine open defined by an equation $y^2 + Q(x)y + P(x) = 0$. Then, there exist exactly two Weierstrass points $P_1, P_2 \in \text{WP}(X)$ that specialize to $P$. Moreover, the thickness of $P$ is $e_P = 2\nu(\gamma_1 - \gamma_2)$, where $\nu$ is the normalized valuation at $p$ and $\gamma_i$ are the roots of $R(x) = Q(x)^2 - 4P(x)$ corresponding to $P_1$ and $P_2$.

To prove this result we need the following technical lemma.

**Lemma 4.1.4.** Let $A$ be a ring such that $n \in A^*$. Then $s = (1 + t)^n - 1 \in A[[t]]$ satisfies $A[[t]] = A[[s]]$ and, moreover, there exists $f(s) \in sA[[s]]$ such that $1 + s = (1 + f(s))^n$.

**Proof.** This is exercise 1.3.9 of [47]. The proof is left to the reader. \□

**Proof of Theorem 4.1.3.** First we shall prove that there are exactly two Weierstrass points $P_1, P_2 \in \text{WP}(X)$ specializing to $P$. Write $\overline{W}_p = W \times \text{Spec}(\mathbb{F}_p)$ for the geometric fiber of $W$ at $p$. Since $p \neq 2$, an affine open $\mathcal{U}$ of $\overline{W}_p$ shall be of the form $\mathcal{U} = \text{Spec}(\mathbb{F}_p[x,y]/(y^2 - \tilde{R}(x)))$, where
\( \tilde{R}(x) \) is the reduction of \( R(x) \) modulo \( p \). Hence it is clear that the singularities of \( \mathcal{U} \) correspond to the multiple roots of \( \tilde{R}(x) \). Without loss of generality, assume \( x = 0 \) is the multiple root of \( \tilde{R}(x) \) corresponding to \( \tilde{P} \). We get \( \tilde{R}(x) = x^m \tilde{h}(x) \), where \( \tilde{h}(x) = \tilde{h}(0)(1+x \tilde{r}(x)) \) and \( \tilde{h}(0) \neq 0 \). The local ring \( O_{\mathcal{W}, \tilde{P}} \) at \( \tilde{P} \) is given by:

\[
O_{\mathcal{W}, \tilde{P}} = (\mathbb{F}_p[x, y]/(y^2 - x^m \tilde{h}(x)))(x, y),
\]

and it follows that

\[
O_{\mathcal{W}, \tilde{P}} = \mathbb{F}_p[[x, y]]/(y^2 - x^m).
\]

By Lemma 4.1.4, taking \( A = \mathbb{F}_p[[y]] \), \( t = x \tilde{r}(x) \) and \( n = 2 \), we obtain that \( \tilde{h}(x) \) is a square in \( (\mathbb{F}_p[[x, y]])^* \). Hence \( O_{\mathcal{W}, \tilde{P}} = A_m \), where

\[
A_m := \mathbb{F}_p[[x, y]]/(y^2 - x^m), \quad m \geq 2.
\]

Since \( \mathcal{W} \) is semi-stable, \( \tilde{W}_p/\mathbb{F}_p \) must be semi-stable. Therefore \( \tilde{P} \) is an ordinary double point and \( O_{\tilde{W}, \tilde{P}} \simeq \mathbb{F}_p[[x, y]]/(y^2 - x^2) = A_2 \). From \( A_2 \simeq A_m \), it follows that \( m = 2 \). As a consequence, \( \tilde{P} \) is attached to a root \( \tilde{\gamma} \) of \( \tilde{R}(x) \) with multiplicity 2 and we conclude that there exist exactly two \( P_1, P_2 \in WP(X) \) that specialize to \( P \) (attached to the roots \( \gamma_1 \) and \( \gamma_2 \) of \( R(x) \) that reduce to \( \tilde{\gamma} \)).

Next, we proceed to compute the thickness \( e_{\tilde{P}} \) of \( \tilde{P} \): the equation \( Y^2 = R(x) = Q(x)^2 - 4P(x) \) defines \( \mathcal{W} \) in a neighborhood of \((p) \in \text{Spec}(\mathbb{Z})\). After extending to a finite extension \( k' \supseteq \mathbb{F}_p \), if necessary, we can suppose that any singular point \( \tilde{P}' \in \tilde{W}_p \times \text{Spec}(k') \) lying over \( \tilde{P} \) is \( k' \)-rational. Without loss of generality, assume that \( P' \) is defined by \( x = 0 \), \( y = 0 \). That is,

\[
\tilde{R}(x) = x^2 \tilde{h}(x), \quad \tilde{h}(0) \neq 0.
\]

We can choose an étale scheme \( S' \) over \( \text{Spec}(\mathbb{Z}) \) and a point \( \pi \in S' \) above \((p) \) such that \( k' = \mathbb{F}_p(\pi') \). Notice that, if we write \( \mathcal{W}' = \mathcal{W} \times_{S} S' \), the point \( \tilde{P}' \) lies in \( \mathcal{W}'(\pi') \) and its local ring is \( O_{\mathcal{W}', (\pi', \tilde{P}')} = (O_{S', \pi'}[x, Y]/(Y^2 - R(x)))(x, y) \).

Let \( \tilde{O}_{S', \pi'} \) be the completion of \( O_{S', \pi'} \) and denote by \( \nu \) its normalized valuation. Let us consider \( R(x) \) over \( \tilde{O}_{S', \pi'} \). Since its reduction is \( \tilde{R}(x) = x^2 \tilde{h}(x) \) with \( \tilde{h}(0) \neq 0 \), we apply the Classical Hensel's Lemma (cf.[59]) to \( x^2 \) and \( \tilde{h}(x) \) and we obtain that \( R(x) = (x^2 + ax + b) \cdot \tilde{h}(x) \), where \( \nu(\tilde{h}(0)) = 0 \), \( \nu(a) > 0 \) and \( \nu(b) > 0 \). Extending \( S' \) to a bigger étale \( \text{Spec}(\mathbb{Z}) \)-scheme if necessary, we can suppose that \( h(0) \) has a square root in \( \tilde{O}_{S', \pi'} \). Since \( h(x) = h(0)(1+x \cdot \tilde{r}(x)) \in \tilde{O}_{S', \pi'}[[x]]^* \), by Lemma 4.1.4, there exists \( s(x) \in \tilde{O}_{S', \pi'}[[x]]^* \) such that \( s(x)^2 = h(x) \). Therefore

\[
O_{\mathcal{W}', (\pi', \tilde{P}')} = \tilde{O}_{S', \pi'}[[x, Y]]/(Y^2 - (x^2 + ax + b) \cdot h(x)) = \tilde{O}_{S', \pi'}[[x, Y]]/(\left( \frac{Y}{s(x)} \right)^2 - \left( x + \frac{a}{2} \right)^2 - \Delta),
\]

where \( \Delta = a^2 - 4 \cdot b \). Writing \( u = Y/s(x) + x + a/2 \) and \( v = Y/s(x) - x - a/2 \), we obtain that \( \tilde{O}_{S', \pi'}[[x, Y]] = \tilde{O}_{S', \pi'}[[u, v]] \) and

\[
O_{\mathcal{W}', (\pi', \tilde{P}')} = \tilde{O}_{S', \pi'}[[u, v]]/(u \cdot v - \Delta).
\]

Hence, we deduce that \( e_{\tilde{P}} = \nu(\Delta) \).

Since the roots of the polynomial \( x^2 + ax + b \) are precisely the two unique roots \( \gamma_1, \gamma_2 \in \overline{\mathbb{Q}} \) that reduce to \( \tilde{\gamma} \), and \( \Delta \) is the discriminant of the polynomial \( x^2 + ax + b \), it follows that \( \Delta = (\gamma_1 - \gamma_2)^2 \) and \( e_{\tilde{P}} = 2\nu(\gamma_1 - \gamma_2) \). \( \square \)
4.2 Hyperelliptic Shimura curves

Let $B$ be an indefinite division quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O}$ be a maximal order in $B$. Let us denote by $X_0^D/Q := X_0(D,1)/\mathbb{Q}$ a Shimura’s canonical model of the Shimura curve attached to $\mathcal{O}$. Let $X_0^D := X_0(D,1)$ denote Morita’s integral model of $X_0^D$. Recall that $X_0^D$ is semi-stable at every prime $p$ dividing $D$, and the thicknesses of singular points of $\tilde{X}_0^D := X_0^D \times \text{Spec}(\mathbb{F}_p)$ can be recovered by means of Theorem 2.2.1. In this section we shall consider those Shimura curves that are hyperelliptic. If this is the case, the hyperelliptic involution turns out to be an Atkin-Lehner involution $\omega_m$. In order to obtain the set of Weierstrass points of the curve we present the following proposition due to Ogg:

**Proposition 4.2.1.** [56, §1] Let $m \mid D$, $m > 0$. The set $\mathfrak{F}_{\omega_m}$ of fixed points of the Atkin-Lehner involution $\omega_m$ acting on $X_0^D$ is

$$\mathfrak{F}_{\omega_m} = \begin{cases} \text{CM}(\mathbb{Z}[\sqrt{-1}]) \cup \text{CM}(\mathbb{Z}[\sqrt{-2}]) & \text{if } m = 2 \\ \text{CM}(\mathbb{Z}[\sqrt{-m}]) & \text{if } m \equiv 3 \mod 4 \\ \text{CM}(\mathbb{Z}[\sqrt{-m}]) & \text{otherwise.} \end{cases}$$

Ogg determined in [56] the 24 values of $D$ for which $X_0^D$ is hyperelliptic over $\overline{\mathbb{Q}}$ and proved that only for 21 values of them the corresponding curves $X_0^D$ are hyperelliptic over $\mathbb{Q}$. The aim of this chapter is to give a procedure to compute hyperelliptic equations for all these cases. Since those of genus 2 were computed by J. González and V. Rotger in [29], we assume that $X_0^D/Q$ is hyperelliptic over $\mathbb{Q}$ of genus $g > 2$. We present the values of $D$ and the corresponding genera for the remaining 18 cases:

<table>
<thead>
<tr>
<th>$g$</th>
<th>$D$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$2 \cdot 31, 2 \cdot 47, 3 \cdot 13, 3 \cdot 17, 3 \cdot 23, 5 \cdot 7, 5 \cdot 11$</td>
</tr>
<tr>
<td>4</td>
<td>$2 \cdot 37, 2 \cdot 43$</td>
</tr>
<tr>
<td>5</td>
<td>$3 \cdot 29$</td>
</tr>
<tr>
<td>6</td>
<td>$2 \cdot 67$</td>
</tr>
<tr>
<td>7</td>
<td>$2 \cdot 73, 3 \cdot 37, 5 \cdot 19$</td>
</tr>
<tr>
<td>9</td>
<td>$2 \cdot 97, 2 \cdot 103, 3 \cdot 53, 7 \cdot 17$</td>
</tr>
</tbody>
</table>

**Table 1**

The hyperelliptic involution $\omega$ of $X_0^D$ in all these cases turns out to be the Atkin-Lehner involution $\omega_D$. Since the action of $\omega_D$ has an interpretation in terms of the moduli problem, it can be extended to an involution on the integral model $X_0^D$. Moreover, we have an explicit description of the fibers $\tilde{X}_0^D$ and the action of $\omega = \omega_D$ on them. Hence we can easily check whether the quotient $X_0^D/\langle \omega \rangle$ is smooth over $\mathbb{Z}$. If $X_0^D/\langle \omega \rangle$ is not smooth over $\mathbb{Z}$, then $X_0^D$ is not a Weierstrass model for $X_0^D$. Sometimes it is possible to blow-down certain exceptional irreducible components in order to obtain a model $W$ such that $W/\langle \omega \rangle$ is smooth over $\mathbb{Z}$ and, thus, defined by an equation of the form (4.1.2):

$$W: y^2 + Q(x)y + P(x) = 0, \quad P, Q \in \mathbb{Z}[x], \quad 2g + 1 \leq \max\{2\deg(Q), \deg(P)\} \leq 2g + 2.$$ 

**Remark 4.2.2.** But this is not always possible. For example, the special fiber of Morita’s integral model of $X_0^{87}$ at $p = 29$ has the following form:
Clearly, by blowing-down exceptional divisors it is not possible to obtain a fiber $\tilde{\mathcal{W}}$ such that $\tilde{\mathcal{W}}/\langle \omega \rangle$ is smooth over $\mathbb{F}_p$.

In order to obtain explicit equations, we will focus our attention in two directions:

1. **Determination of the thicknesses of Weierstrass points at every prime $p \mid D$.** Since the hyperelliptic involution is the Atkin-Lehner involution $\omega_D$, we have that $WP(\mathcal{W}) = \bigsqcup_i \text{CM}(R_i)$, where $\{R_i\}$ is the set of the orders in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ containing the order $\mathbb{Z}[\sqrt{-D}]$. By Theorem 4.1.3, thicknesses of singular specializations of $WP(\mathcal{W})$ are related with roots of the polynomial $R(x) = P(x)^2 - 4Q(x)$. In §3.3.1, we proved that the singular specialization of any $P \in$ CM($R_i$) in $X^D_0$ is characterized by the composition of maps

$$\text{CM}(R) \xrightarrow{\varphi} \text{CM}_{D,1}(R) \xrightarrow{\phi_s} \text{CM}_{D,p}(R) \xrightarrow{\pi} \text{Pic}\left(\frac{D}{p}\right).$$

Moreover, by Theorem 2.2.1, its thickness in $X^D_0$ is given by $e_{\tilde{\rho}} = e(\pi(\phi_s(\varphi(P))))$. Thanks to the computational description of $\phi_s$ detailed in §3.1.1, we are able to compute $e_{\tilde{\rho}}$ for all $P \in \bigsqcup_i \text{CM}(R_i)$.

Once we know the specialization and the thickness of a singular Heegner point in $X^D_0$, we can easily determine its specialization and its thickness in $\mathcal{W}$. Indeed, if $pr : X^D_0 \to \mathcal{W}$ is the blown-down map, then the thickness of a singular point $\tilde{Q} \in \mathcal{W}$ is:

$$e_{\tilde{Q}} = \sum_{\tilde{P} \in X^D_0, pr(\tilde{P}) = \tilde{Q}} e_{\tilde{P}} + \#\{C\text{ irreducible component, } pr(C) = \tilde{Q}\} - 1 \quad (4.2.5)$$

2. **Determination of the leading coefficient of $R(x) = P(x)^2 - 4Q(x)$.**

Given the Weierstrass model $\mathcal{W}$ of $X^D_0$, let $\mathcal{U}$ be the affine open defined by the equation $y^2 + P(x)y + Q(x) = 0$. The set of points at infinity of $\mathcal{U}$ is the set of geometric points of the generic fiber of $\mathcal{W} \setminus \mathcal{U}$. Since Shimura curves do not have real points (cf. [67, Proposition 4.4]), this set corresponds to a pair of conjugate points living in a quadratic extension of $\mathbb{Q}$ such that the hyperelliptic involution acts on them via the unique non-trivial Galois conjugation. In particular, this implies that $\text{deg}(P^2 - 4Q) = 2g + 2$. In order to fix a hyperelliptic equation of $\mathcal{W}$, we must choose a pair of points defined over an imaginary quadratic field such that the hyperelliptic involution acts suitably on them.

It turns out that for every value $D$ in Table 1, there exists a maximal order $R_\infty$ in an imaginary quadratic field $K_\infty$ with class number $h(R_\infty) = 1$, i.e. $K_\infty = H_{R_\infty}$, discriminant coprime to $D$ and such that $\text{CM}(R_\infty) \neq \emptyset$. By Theorem 1.4.3, complex conjugation acts on every $P_\infty \in \text{CM}(R_\infty)$ as the hyperelliptic involution $\omega_D$. We fix $P_\infty \in \text{CM}(R_\infty)$ and we choose the set $\{P_\infty, \omega_D(P_\infty)\}$ to be our set of points at infinity. This choice shall fix a hyperelliptic equation $y^2 + P(x)y + Q(x) = 0$ of $\mathcal{W}$, up to transformations of the form $(x, y) \mapsto (x + a, y + h(x)), \ a \in \mathbb{Z}, h(x) \in \mathbb{Z}[x], \text{deg}(h(x)) \leq g + 1$.

Our goal is to determine the leading coefficient $a_R$ of the polynomial $R(x) = P(x)^2 - 4Q(x)$. As a first approach, recall that the field of definition of $P_\infty$ is $K_\infty = \mathbb{Q}(\sqrt{-R})$. Moreover, a
prime $p$ divides $a_R$ if and only if $P_\infty$ and $\omega_D(P_\infty)$ specialize to the same $F_p$-rational Weierstrass point. Hence, the determination of the specialization of these specific Heegner points will give a valuable information about the leading coefficient $a_R \in \mathbb{Z}$.

Since any $p \mid D$ is inert in $R_\infty$, $P_\infty$ has good reduction at $p$. Any Weierstrass point has singular specialization at any prime dividing $D$, hence $(a_R, D) = 1$. In order to determine the remaining $p$-adic valuations of $a_R$, we introduce the following definition:

**Definition 4.2.3.** Let $R$ be a local valuation ring with uniformizer $\pi$. The intersection index of two ideals $I_1$ and $I_2$ of an algebra $A$ over $R$ is the length of the algebra $A/(I_1 + I_2)$.

Let $P_1$ and $P_2$ be the points in $\text{Spec}(A)$ defined by $I_1$ and $I_2$. By [65, Lemma 3.13], the intersection index of $I_1$ and $I_2$ measures the maximal power $n$ of $\pi$ in which their inverse image $\tilde{P}_1$ and $\tilde{P}_2$ coincide in $\text{Spec}(A \otimes_R (R/\pi^n R))$.

Recall that $P_\infty$ lies in the affine open defined by the relation $z^2 + Q_1(v)z + P_1(v) = 0$, where $Q_1(v) = v^{q+1}Q(1/v)$ and $P_1(v) = v^{q^2+2}P(1/v)$. Moreover, the ideals defining $P_\infty$ and $\omega_D(P_\infty)$ are

$$I_{P_\infty} = \langle v, z + \frac{Q_1(0) + \sqrt{a_R}}{2} \rangle, \quad I_{\omega_D(P_\infty)} = \langle v, z + \frac{Q_1(0) - \sqrt{a_R}}{2} \rangle.$$  

Set $K_p = K_\infty \otimes \mathbb{Q} Q_p$, let $K_p^{nr}$ be the maximal unramified extension of $K_p$ and let $R_p^{nr}$ be its integer ring with uniformizer $\pi$. Write $W_p^{nr}$ for the extension of scalars $W \times \text{Spec}(R_p^{nr})$ and denote also by $P_\infty$ and $\omega_D(P_\infty)$ their inverse image in $W_p^{nr}$. Write $(P_\infty, \omega_D(P_\infty))_p$ for the intersection index between $P_\infty$ and $\omega_D(P_\infty)$ in $W_p^{nr}$. Then, it is easy to check that $(P_\infty, \omega_D(P_\infty))_p$ is precisely $\nu_p(a_R)$, if $p$ ramifies or splits in $K_\infty$, and $\nu_p(a_R)/2$, if $p$ is inert in $K_\infty$.

Assume that $p \nmid D$. Since $X_0^D/\mathbb{Z}$ is the coarse moduli space associated to the algebraic stack that classifies abelian surfaces with QM by $\mathfrak{O}$ over any arbitrary base scheme (cf. [13]) and $W_p^{nr} = (X_0^D)_{p}^{nr}$, this intersection index can be interpreted in terms of the algebraic objects classified by $P_\infty = [A_\infty, i_\infty]$ and $\omega_D(P_\infty) = [A'_\infty, i'_\infty]$. Namely,

$$(P_\infty, \omega_D(P_\infty))_p := \max\{n \geq 1 : (A_\infty, i_\infty) \simeq (A'_\infty, i'_\infty) \text{ over } R_p^{nr}/\pi^n R_p^{nr}\}.$$  

The aim of the rest of the section is to provide a description of $(P_\infty, \omega_D(P_\infty))_p$ in purely algebraic and computable terms.

**Lemma 4.2.4.** Let $R$ be an order of conductor $c$ in an imaginary quadratic field $K$ such that $h(R) = 1$. Let $P = [A, i] \in \text{CM}(R)$ be a Heegner point, let $p$ be a prime not dividing $c$ and let $m \mid D$. Then, if $p$ splits in $K$, $(P, \omega_m(P))_p = 0$.

**Proof.** Let $m = \alpha_m \mathcal{O}$ be the unique two-sided $\mathcal{O}$-ideal of norm $m$. Write $\omega_m(P) = [A', i'] \in \text{CM}(R)$ and assume that $P = [J, \tau] \in \mathcal{Y}_0(D, N) = \mathcal{O}^\times \backslash B^\times \times \mathbb{P} / B^\times$. Recall that $(A', i') \in \{ A, i \}$ and, by Lemma 1.3.10, $(A, i)$ is identified with $((\mathcal{O}^\times \backslash B^\times / Q^\times) \times \{ \tau \}) / B^\times$. By definition, $\omega_m(P)$ corresponds to the pair $(J\alpha_m, \tau)$. Hence $(A', i') \simeq (A, j)$, where $j(\alpha) = i(\alpha_m^{-1} \alpha_m)$ for all $\alpha \in \mathcal{O}$.

Since $p$ splits in $K$, $P$ has ordinary good reduction. Moreover $\omega_m(P) = [A, j]$, thus $\omega_m(\tilde{P}) = [\tilde{A}, j]$. By Proposition 3.4.1 $\text{End}(A) \simeq \text{End}(\tilde{A})$, hence $i = i$ and $j = j$. It follows that $\tilde{P} = [\tilde{A}, i] \neq \omega_m(\tilde{P}) = [\tilde{A}, j]$, that is $(P, \omega_m(P))_p = 0$.  

Recall that if $p$ does not split in $K$ and $p \nmid cD$, $P = [A, i]$ has supersingular smooth specialization. We proved in §3.4 that the embedding $\text{End}(A, i) \hookrightarrow \text{End}(\tilde{A}, \tilde{i})$ defines a CM map

$$\phi_{ss} : \text{CM}_{D,1}(R) \longrightarrow \text{CM}_{Dp,1}(R),$$

that provides $\tilde{P}$ via the composition of maps

$$\text{CM}(R) \xrightarrow{\varphi} \text{CM}_{D,1}(R) \xrightarrow{\phi_{ss}} \text{CM}_{Dp,1} \xrightarrow{\pi} \text{Pic}(Dp, 1) \xrightarrow{\varepsilon_p^{-1}} (\bar{X}_D^0)_{ss}.$$

The following theorem computes $(P, \omega_m(P))_p$ in this case.

**Theorem 4.2.5.** Let $R$ be an order of conductor $c$ in an imaginary quadratic field $K$ such that $(\text{disc}(K), D) = 1$ and $h(R) = 1$. Let $P = [A, i] \in \text{CM}(R)$ be a Heegner point and let $m \mid D$. Let $p \nmid Dc$ be a prime that does not split in $K$. Set $\Lambda = \text{End}(A, i) \in \text{Pic}(Dp, 1)$ and write $\Lambda^0 = \Lambda^0_+ + \Lambda^0_-$, where $\Lambda^0_+ = \phi_{ss}(\varphi(P))(K)$ and $\Lambda^0_-$ is its quaternionic complement. Let $\Lambda \simeq R \oplus eR$ be the decomposition of $\Lambda$ provided by its free right $R$-module structure via $\phi_{ss}(\varphi(P))$. For any $\lambda \in \Lambda^0$, write $\lambda = \lambda_+ + \lambda_-$, where $\lambda_+ \in \Lambda^0_+$ and $\lambda_- \in \Lambda^0_-$. Finally, for any $\lambda \in \Lambda$, write $\lambda = \lambda^+ + e\lambda^-$, where $\lambda^+, \lambda^- \in R$. Then, the integer $(\omega_m(P), P)_p$ is given by:

$$(\omega_m(P), P)_p = \max \left\{ \frac{\text{ord}_p(N(\lambda^-))}{1 - \left(\frac{d}{p}\right)} + 1 : \lambda \in \Lambda, N(\lambda) = m \right\}$$  \hspace{1cm} (4.2.7)

where $d$ is the discriminant of $K$ and $\left(\frac{d}{p}\right)$ is the usual Kronecker symbol. Moreover, if $\lambda \in \Lambda$ is such that $N(\lambda) = m$, the following equality holds:

$$-dc^2 = -mdc^2N\left(\frac{\lambda^+}{m}\right) + N(\lambda^-)\frac{D}{m} \cdot p, \hspace{1cm} dc^2N\left(\frac{\lambda^+}{m}\right) \in \mathbb{Z}.$$  \hspace{1cm} (4.2.8)

**Proof.** Write $\omega_m(P) = [A', i'] \in \text{CM}(R)$ as above (again $(A', i') \in \{A, i\}$). As in §3.2, set $W_n = R^0_{p^n}/\pi^n R^0_p$, $\Lambda^0 = \text{End}_{H_n}(A, i)$ and write $I_m^n = \text{Hom}_{H_n}((A, i), (A', i'))$ for the set of isogenies between $(A, i)/W_n$ and $(A', i')/W_n$. Recall that $I_m^n$ is a right $\Lambda^n$-module and $(A, i) \simeq (A', i')$ over $W_n$ if and only if $I_m^n$ is principal.

By the invariance of $\phi_{ss}$ under $\omega_m$, $I_m^n = \text{Hom}_{\mathbb{F}}((A, i), (A', i'))$ is the single (two-sided) ideal of $\Lambda$ of norm $m$. Hence, if $(A, i)$ and $(A', i')$ were isomorphic over $\mathbb{F}$, $I_m^n$ would be principal, i.e. it would be generated by an element $\lambda \in \Lambda$ of norm $m$.

Since $p \nmid D$, under the embedding $\Lambda^n \hookrightarrow \Lambda$, the ideal $I_m^n$ is the only ideal in $\Lambda^n$ lying above $I_m^1$. This means that $I_m^n$ is principal if and only if there exists an element $\lambda \in \Lambda_n$ that generates $I_m^n$, or equivalently, $\lambda \in \Lambda$, $N(\lambda) = m$ and $dN(\lambda^-) \equiv 0 \mod p \cdot N(\mathfrak{p})^{n-1}$ by Lemma 3.2.2. Computing the norm $N(\mathfrak{p})$ in both cases $p \mid d$ and $p \nmid d$ we conclude that :

$$(\omega_m(P), P)_p = \left\{ \begin{array}{ll} \max\{\text{ord}_p(d \cdot N(\lambda^-)) : \lambda \in \Lambda, N(\lambda) = m\} & p \mid d \\ \max\left\{ \frac{1}{2}(\text{ord}_p(N(\lambda^-)) + 1) : \lambda \in \Lambda, N(\lambda) = m\right\} & p \nmid d \end{array} \right.$$  \hspace{1cm} (4.2.9)

Finally, the decomposition $\Lambda \simeq R \oplus eR$, where $e = e_+ + e_-$, allows us to compute the reduced discriminant of $\Lambda$ in terms of $R$ and $e$. Indeed we obtain that $\text{disc}(\Lambda) = e_+^2e_-^2d$. Since $\Lambda \in \text{Pic}(Dp, 1)$ we deduce $Dp = e_+^2e_-^2d$ (Notice that $d < 0$ and $e^2_+ < 0$ since $\Lambda^0 = \left(\frac{d e^2_+}{d}\right)$ is definite).
For any $\lambda \in \Lambda$, we have that $\lambda_+ = \lambda^+ + \lambda^- \cdot e_+$ and $\lambda_- = e_- \cdot \lambda^-$. If in addition $N(\lambda) = m$, then $N(\lambda) = N(\lambda_+) + N(\lambda_-) = m$, where $N(\lambda_-) = -e^-_+ \cdot N(\lambda^-) = -\frac{N(\lambda^-)Dp}{ord}$. Thus,

$$-dc^2m = -dc^2N(\lambda_+) + N(\lambda^-)Dp.$$  

Since $m \mid dc^2N(\lambda_+)$ and all primes dividing $m \mid D$ are inert in $K$, $m^2 \mid dc^2N(\lambda_+)$ which implies $dc^2N(\frac{\lambda_+}{m}) \in \mathbb{Z}$. Dividing the above equation by $m$ one obtains (4.2.8).

Since by hypothesis $ord_p(c) = 0$, we have that

$$ord_p(d \cdot N(\lambda_-)) = ord_p(dc^2 \cdot N(\lambda_-)) = ord_p(-pD \cdot N(\lambda^-)) = ord_p(N(\lambda^-)) + 1.$$

Finally, one obtains the desired formula from (4.2.9).

**Remark 4.2.6.** Notice that the integers $-dc^2, -dc^2N(\frac{\lambda_+}{m})$ and $N(\lambda_-)Dm^2p$ are all positive. Hence, given $D$, $m$ and $d$, equation (4.2.8) gives a finite number of possible $p$ and $N(\lambda_-)$. Moreover, the valuation of such $N(\lambda_-)$ at $p$ provides the intersection index $(\omega_m(P), P)_p$.

### 4.3 Algorithm to compute equations

Let $X = X_0^D/Q$ be an hyperelliptic Shimura curve of genus $g \geq 3$ and let $\mathcal{X} = X_0^D/Z$ be Morita’s integral model of $X$. Assume that we can obtain a Weierstrass model $\mathcal{W}$ of $X$ by blowing down certain exceptional divisors of some special fibers of $\mathcal{X}$. We proceed to describe an algorithm to compute an hyperelliptic equation for $\mathcal{W}$ over $\mathbb{Z}[1/2]$: $\mathcal{W}: y^2 = R(x), \quad R(x) \in \mathbb{Z}[x], \quad deg(R) = 2g + 2$.

**Step 1: Reduction of the set of Weierstrass points at bad primes**

Let $\text{CM}(R_i)$ be a set of Heegner points in $\text{WP}(X)$. By Corollary 1.2.5, $\text{CM}_{D,1}(R_i)$ is a $\text{Pic}(R_i)$-orbit. Thus by Theorem 1.4.2, the set $\text{CM}(R_i)$ is a Galois orbit. The decomposition $\text{WP}(\mathcal{W}) = \bigsqcup_i \text{CM}(R_i)$ gives rise to a factorization $R(x) = \prod p_{R_i}(x)$, where each $p_{R_i} \in \mathbb{Z}[x]$ is irreducible, $deg(p_{R_i}) = \#\text{Pic}(R_i)$ and roots of $p_{R_i}$ correspond to Weierstrass points $\text{CM}(R_i)$. Moreover, the splitting field of each $p_{R_i}$ coincides with the field of definition of any $P \in \text{CM}(R_i)$.

Fix $P \in \text{CM}(R_i)$ and let $p \mid D$ be a prime. Since $R_i^0 = Q(\sqrt{-D})$, Theorem 3.3.3 asserts that its specialization $\tilde{P}$ lies in the singular locus $\tilde{X}_{\text{sing}}$. By (3.3.16), we are able to compute $\tilde{P}$ through the map $\phi_s$ of Theorem 3.3.3. Indeed,

$$\varepsilon_s(\tilde{P}) = \pi(\phi_s(\varphi(P))) \in \text{Pic}(D/p, p).$$

Finally, in order to compute $\phi_s$ we exploit the algebraic description of $\phi_s$. In fact, Theorem 3.1.3 gives $\phi_s(P)$ explicitly.

Once we have obtained $\varepsilon_s(\tilde{P})$ for a fixed $P \in \text{CM}(R_i)$, we proceed to obtain the specialization of all $Q \in \text{CM}(R_i)$ using the fact that $\text{CM}(R_i)$ is a Galois orbit. By Theorem 3.3.3,

$$\varepsilon_s(P_{\phi_s(\varphi(Q))}) = \pi(\phi_s([J]^{-1} \cdot \varphi(P))) = \pi([J] \ast \phi_s(\varphi(P))).$$

Moreover, since we have an explicit description of $\phi_s(\varphi(P))$ and the $\text{Pic}(R)$-action on $\phi_s(P)$ is easily computable with MAGMA [12], we obtain the specialization of all points in $\text{CM}(R_i)$.

Notice that this recipe provides $\varepsilon_s(Q) \in \text{Pic}(D/p, Np)$ for all $Q \in \bigsqcup_i \text{CM}(R_i)$ which, by Theorem 2.2.1, describes its specialization and its thickness in $\tilde{X}$. In order to obtain its thickness in $\mathcal{W}$ we apply formula (4.2.5).
Step 2: Choice of the points at infinity

As pointed out in §4.2, we may choose an order \( R_\infty \) with class number \( h(R_\infty) = 1 \) in an imaginary quadratic field \( K_\infty \) of discriminant prime-to-\( D \) and such that \( \text{CM}(R_\infty) \neq \emptyset \). Notice that we can always assume that \( R_\infty \) is maximal. Fix \( P_\infty = [A_\infty, t_\infty] \in \text{CM}(R_\infty) \) and assume that \( \{P_\infty, \omega_D(P_\infty)\} \) are the points at infinity. This fixes an affine open set of \( W \) defined, over \( \mathbb{Z}[1/2] \), by the equation \( y^2 = R(x) = \prod p_R(x) \), where \( \deg(R(x)) = 2g+2 \) and the factorization \( R(x) = \prod p_R(x) \) is attached to the decomposition \( WP(W) = \bigsqcup \text{CM}(R_i) \). Let \( a_R \) and \( a_{R_i} \) be the leading coefficients of \( R(x) \) and \( p_R(x) \) respectively, \( a_R = \prod_i a_{R_i} \). Since \( \mathbb{Q}(\sqrt{a_R}) = K_\infty \), we control the sign of \( a_R \) (which is negative since \( K_\infty \) is imaginary) and its absolute value modulo squares.

In order to determine \( a_R \), recall that \( (a_R, D) = 1 \) and

\[
\nu_p(a_R) = \left( 1 - \left( \frac{d}{p} \right) \right) \nu_p(d),
\]

By Lemma 4.2.4, \( (P_\infty, \omega_D(P_\infty)) \) is unbounded. If this is the case, we deduce from Theorem 4.2.5 that:

\[
\nu_p(a_R) = \max \left\{ \text{ord}_p(N(\lambda^-)) + 1 - \left( \frac{d}{p} \right) \lambda : \lambda \in \text{End}(\tilde{A}_\infty, \tilde{t}_\infty), \ N(\gamma) = D \right\}
\]

where \( d \) is the discriminant of \( K_\infty \). Moreover, for any \( \lambda \in \Lambda \) such that \( N(\lambda) = D \), the following relation holds:

\[
-d = -DdN \left( \frac{\lambda}{D} \right) + N(\lambda^-)p, \quad dN \left( \frac{\lambda}{D} \right) \in \mathbb{Z}.
\]

This gives a finite number of possible \( p \) and \( N(\lambda^-) \) for given \( D \) and \( d = \text{disc}(K_\infty) \). Consequently, we have a finite number of possible \( \nu_p(a_R) \).

Once we have the set of possible \( p \) dividing \( a_R \), in order to determine which \( a_{R_i} \) is divisible by \( p \) recall the maps \( \phi_{ss} \) of (3.4.20) attached to supersingular specialization. Notice that \( p \neq 2 \) divides \( a_{R_i} \) if and only if \( \varepsilon_{ss}(\tilde{P}_\infty) = \pi(\phi_{ss}(\varphi(P_\infty))) \in \pi(\phi_{ss}(\text{CM}(Dp_i, 1(R_i)))) \). Equivalently, \( R_i \) is embedded in \( \varepsilon_{ss}(P_\infty) \in \text{Pic}(Dp_i, 1) \) optimally. There exists no pair of orders \( R_i \neq R_j \) embedding optimally in the same \( \Lambda \in \text{Pic}(Dp_i, 1) \) since \( \phi_{ss} \) is injective and two Weierstrass points can not have the same specialization whenever \( p \) is a prime of good reduction.

We are able to compute \( \varepsilon_{ss}(\tilde{P}_\infty) = R_\infty \oplus eR_\infty \), and consequently we shall check whether \( R_i \) is embedded optimally in it.

In case \( p = 2 \), we control the valuation \( \nu_2(a_R) \) but we do not control the 2-valuation of each \( a_{R_i} \) if \( \nu_2(a_{R_i}) \neq 0 \). In any case we have an upper bound; \( \nu_2(a_{R_i}) \leq \nu_2(a_R) \).

Step 3: Discriminants, Resultants and Fields of definition

For any \( P \in WP(W) \), write \( \gamma_P \) for the root of \( R(x) \) attached to \( P \). Since we control the specialization of every point in \( WP(W) \) and we know how to compute its thickness, Theorem 4.1.3 yields the valuations \( \nu_p(\gamma_P - \gamma_{P'}) \) for every \( P, P' \in WP(W) \) and every \( p \neq 2 \). This provides the discriminants \( \text{disc}(p_{R_i}) \) and the resultants \( \text{Res}(p_{R_i}, p_{R_j}) \) up to a power-of-2 factor, namely

\[
\nu_p(\text{disc}(p_{R_i})) = \sum_{P, P' \in \text{CM}(R_i)} 2 \nu_p(\gamma_P - \gamma_{P'}), \quad \nu_p(\text{Res}(p_{R_i}, p_{R_j})) = \sum_{P \in \text{CM}(R_i)} \nu_p(\gamma_P - \gamma_Q).
\]

(4.3.11)
If in addition we assume good reduction at 2, by (4.1.3) we have that
\[ 4(g + 1) = \nu_2(\text{disc}(R)) = \sum_i \nu_2(\text{disc}(p_{R_i})) + \sum_{i,j} \nu_2(\text{Res}(p_{R_i}, p_{R_j}))^2. \] (4.3.12)

In general we obtain a finite number of possible powers of 2 dividing $\text{disc}(p_{R_i})$ and $\text{Res}(p_{R_i}, p_{R_j})$.

Let $M_{R_i}$ be the isomorphism class of the field $\mathbb{Q}(P)$, for any $P \in \text{CM}(R_i)$. By Theorem 1.4.3, $M_{R_i}$ is characterized by certain $\{a\} \in \text{Pic}(R_i)/\text{Pic}(R_i)^2$ such that
\[ B \simeq \left(\frac{-D, N_{K/\mathbb{Q}}(a)}{\mathbb{Q}}\right), \] (4.3.13)

In our particular setting, the conductor of $R_i$ is at most 2 and, thus, the index between the Hilbert class field and $H_{R_i}$ is either 1 or 3. By Remark 1.4.4, this implies that there is a unique class in $\text{Pic}(R_i)/\text{Pic}(R_i)^2$ satisfying (4.3.13). Since condition (4.3.13) is completely explicit, we will be able to compute the field $M_{R_i}$ attached to $\text{CM}(R_i)$. Recall that $M_{R_i}$ coincides with the splitting field of $p_{R_i}(x)$.

Step 4: Computing equations

Since we have computed the leading coefficients of each $p_{R_i}$, we are able to convert them into monic polynomials. Given $p_{R_i}(x) \in \mathbb{Z}[x]$ of discriminant $d$, leading coefficient $a_{R_i}$ and degree $n$, the polynomial $q_{R_i}(x) = a_{R_i}^{-1}(p_{R_i}(x/a_{R_i}))$ turns out to be monic with integer coefficients and discriminant $a_{R_i}^{2n-2}d$. It has the same splitting field than $p_{R_i}(x)$.

Let $\delta_{R_i}$ be any root of $q_{R_i}$. Since $q_{R_i} \in \mathbb{Z}[x]$ is monic, the root $\delta_{R_i}$ belongs to $\mathcal{O}_{M_{R_i}}$, the ring of integers of $M_{R_i}$. Moreover, $\text{disc}(q_{R_i})$ provides the $\mathbb{Z}$-index $[\mathcal{O}_{M_{R_i}} : \mathbb{Z}[\delta_{R_i}]]$. Through the instruction $\text{IndexFormEquation}$ of MAGMA [12] we obtain all possible $\delta_{R_i}$ of given index, up to sign and translations by integers. Thus, we are able compute all possible polynomials $q_{R_i}$ (and consequently $p_{R_i}$) up to transformations of the form $p(x) \to p(\pm x + r)$ with $r \in \mathbb{Z}$.

The polynomials $p_{R_i}$ can be determined with no ambiguity by means of the resultant $R_{i,j} = \text{Res}(p_{R_i}, p_{R_j})$. Namely, given $p_{R_i}(x + r_i)$ and $p_{R_j}(x + r_j)$, the equation $R_{i,j} = \text{Res}(p_{R_i}(x + r_i), p_{R_j}(x + r_j))$ provides the difference $r_i - r_j$. This way we obtain the product $p_{R_i} \cdot p_{R_j}$ up to translations by an integer. Notice that, given the equation $y^2 = R(x)$, the polynomial $R(x)$ is also defined up to translations by an integer.

4.4 Case $D = 3 \cdot 13$

In this section we shall compute an explicit equation for the hyperelliptic Shimura curve of discriminant $D = 39$ exploiting the algorithm explained above. This curve was used in [70] by Siksek and Skorobogatov in order to find a counterexample to the Hasse principle explained by the Manin obstruction. Since their results depend on the conjectural equation of the curve given by Kurihara [44], the verification of such conjectural equation shows that the results of [70] are unconditionally true.

Step 1: Reduction of the set of Weierstrass points at bad primes

Let $X$ denote the hyperelliptic Shimura curve $X_0^{39}/\mathbb{Q}$. By Proposition 4.2.1, $\text{WP}(X) = \text{CM}(R) \cup \text{CM}(R_0)$, where $R_0 = \mathbb{Z}[[1 + \sqrt{-39}]]$ and $R = \mathbb{Z}[\sqrt{-39}]$. Let $K = \mathbb{Q}(\sqrt{-39})$. Notice that both $R$ and $R_0$ have class number 4, so both ring class fields have degree 4 over $K$. 

\[ \text{Step 1: Reduction of the set of Weierstrass points at bad primes} \]
We can compute the geometric special fiber of $X$ at 3 and 13 by means of Čerednik-Drinfeld’s theory (cf. [42, §3] for a step-by-step guide on the computation of these special fibers using MAGMA [12]). Notice that, in this case, $X = W$ since $X/\langle \omega_D \rangle$ is smooth over $\mathbb{Z}$.

In the drawings below, the integer on each singular point stands for its thickness:

- Special fiber at $p=3$
- Special fiber at $p=13$

Let $\mathcal{O}$ be a maximal order in the quaternion algebra $B$ of discriminant 39. Choose arbitrary points $P \in \text{CM}(R)$ and $P_0 \in \text{CM}(R_0)$. As it is more convenient for computations to work with optimal embeddings instead of Heegner points, let $\varphi(P) \in \text{CM}_{39,1}(R)$ and $\varphi(P_0) \in \text{CM}_{39,1}(R_0)$ be the optimal embeddings attached to $P$ and $P_0$, respectively, via (3.1.7). In particular, $\varphi(P)$ and $\varphi(P_0)$ yield the following decompositions computed with MAGMA [12]:

$$
\begin{cases}
B = K \oplus i_1K \\
\mathcal{O} = R \oplus e_1I_1
\end{cases} \quad \text{where} \quad \begin{cases}
i_1 \text{ is a quaternionic complement of } \varphi(P), \quad i_1^2 = 447 \\
e_1 = i_1 + (7 \cdot \sqrt{-39} + 18) \\
I_1 = \langle \frac{1}{2}, \frac{\sqrt{-39}}{894} + \frac{63}{298} \rangle_R
\end{cases}
$$

and

$$
\begin{cases}
B = K \oplus i'_1K \\
\mathcal{O} = R_0 \oplus e'_1I'_1
\end{cases} \quad \text{where} \quad \begin{cases}
i'_1 \text{ is a quaternionic complement of } \varphi(P_0), \quad i'_1^2 = 6 \\
e'_1 = i'_1 \\
I'_1 = \langle 1, \frac{\sqrt{-39} - 9}{12} \rangle_{R_0}
\end{cases}
$$

**Reduction modulo 3**

In order to compute the specialization modulo $p = 3$ of $P$ and $P_0$, we shall compute the optimal embeddings $\psi_R \in \text{CM}_{13,3}(R)$ and $\psi_{R_0} \in \text{CM}_{13,3}(R_0)$ of Theorem 3.1.1. Their targets are maximal orders $S_3$ and $S'_3$ of the quaternion algebra $H_3$ of discriminant 3. Again both embeddings define the following decompositions:

$$
\begin{cases}
H_3 = K \oplus i_2K \\
S_3 = R \oplus e_2I_2
\end{cases} \quad \text{where} \quad \begin{cases}
i_2 \text{ is a quaternionic complement of } \psi_R, \quad i_2^2 = -43 \\
e_2 = i_2 - 387 \\
I_2 = \langle \frac{1}{7}, \frac{\sqrt{-39}}{118} - \frac{10}{39} \rangle_R
\end{cases}
$$

and

$$
\begin{cases}
H_3 = K \oplus i'_2K \\
S'_3 = R_0 \oplus e'_2I'_2
\end{cases} \quad \text{where} \quad \begin{cases}
i'_2 \text{ is a quaternionic complement of } \psi_{R_0}, \quad i'_2^2 = -12 \\
e'_2 = i'_2 - 12 \\
I'_2 = \langle 1, \frac{\sqrt{-39} - 1}{156 - 2} - \frac{29}{18} \rangle_{R_0}
\end{cases}
$$

Hence, by Theorem 3.1.3 the optimal embedding $\phi_s(\varphi(P)) : R \mapsto \text{End}_{\mathcal{O}}^S(\mathcal{O} \otimes R S_3) = \Lambda_3$ of (3.3.15) is given by the decomposition:

$$
\begin{cases}
\Lambda_3 \otimes \mathbb{Q} = K \oplus i_3K \\
\Lambda_3 = R \oplus e_3I_3
\end{cases} \quad \text{where} \quad \begin{cases}
i_3 \text{ is a quaternionic complement of } \phi_s(\varphi(P)), \quad i_3^2 = -43 \cdot 447 \\
e_3 = -387 \cdot (18 - 7 \cdot \sqrt{-39}) - i_3 \\
I_3 = (I_2 \cap \frac{1}{387}R) I_2 \cap \frac{1}{18 - 7 \cdot \sqrt{-39}} I_2
\end{cases}
$$
Similarly, $\phi_s(\varphi(P_0)) : R_0 \rightarrow \text{End}_{O}^{S_3}(O \otimes R_0 \mathcal{S}_3^\prime) = \Lambda'_3$ is given by:

\[
\begin{aligned}
\left\{ \begin{array}{l}
\Lambda'_3 \otimes \mathbb{Q} = K \oplus i_3K \\
\Lambda'_3 = R_0 \oplus e_3I_3' 
\end{array} \right. \\
\text{where} \\
\begin{array}{l}
i_3' \text{ is a quaternionic complement of } \phi_s(\varphi(P_0)), \\
e_3' = -12 \cdot 6 \\
I'_3 = (I'_2 \cap \frac{1}{12} R_0)T_1.
\end{array}
\end{aligned}
\]

Once we have a characterization of the embeddings $\phi_s(\varphi(P))$ and $\phi_s(\varphi(P_0))$, we proceed to describe the specialization of all Heegner points in CM($R$) and CM($R_0$). Recall that, in both cases, the sets CM($R$) and CM($R_0$) are Pick($R$) and Pick($R_0$)-orbits respectively. Moreover, Pick($R$) $\simeq$ Pick($R_0$) $\cong \mathbb{Z}/4\mathbb{Z}$.

**Case CM($R$):** We pick a representative $J$ of a generator $[J] \in \text{Pic}(R)$. We construct the left-$\Lambda_3$-ideals $\Lambda_3\phi_s(\varphi(P))(J)$, $\Lambda_3\phi_s(\varphi(P))(J^2)$, $\Lambda_3\phi_s(\varphi(P))(J^3)$ and we compute their right orders $\pi([J] * \phi_s(\varphi(P)))$. We obtain that their number of units are:

\[
\#(\Lambda'_3)/2 = \#((\pi([J] * \phi_s(\varphi(P))))/2 = \#((\pi([J^2] * \phi_s(\varphi(P))))/2 = \#((\pi([J^3] * \phi_s(\varphi(P))))/2 = 1.
\]

Thus, by (2.2.3), such integers are the thickness of each singular specialization.

Besides, we checked that $\Lambda_3\phi_s(\varphi(P))(J)$ and $\Lambda_3\phi_s(\varphi(P))(J^2)(\Lambda_3\phi_s(\varphi(P))(J^3))^{-1}$ are principal, whereas $\Lambda_3\phi_s(\varphi(P))(J^2)$, $\Lambda_3\phi_s(\varphi(P))(J^3)$, $\Lambda_3\phi_s(\varphi(P))(J)(\Lambda_3\phi_s(\varphi(P))(J^2))^{-1}$, $\Lambda_3\phi_s(\varphi(P))(J)(\Lambda_3\phi_s(\varphi(P))(J^3))^{-1}$ are not. Since for any pair of left-$\Lambda_3$-ideals $I_1$ and $I_2$ their right orders are isomorphic as oriented Eichler orders if and only if $I_1 \cdot I_2^{-1}$ is principal, it follows from (4.3.10) that

\[
\tilde{P} = \varepsilon_s^{-1}(\pi(\phi_s(\varphi(P)))) = \varepsilon_s^{-1}(\pi([J] * \phi_s(\varphi(P)))) = P^{\Phi_R([J])}
\]

\[
\tilde{P}^{\Phi_R([J^2])} = \varepsilon_s^{-1}(\pi([J^2] * \phi_s(\varphi(P)))) = \varepsilon_s^{-1}(\pi([J^3] * \phi_s(\varphi(P)))) = P^{\Phi_R([J^3])}.
\]

**Case CM($R_0$):** Let $J^s$ be a representative of a generator of $\text{Pic}(R_0)$. Similarly as above, we construct the corresponding left-$\Lambda'_3$-ideals and we obtain:

\[
\#(\Lambda'_3)/2 = \#((\pi([J^s] * \phi_s(\varphi(P_0))))/2 = \#((\pi([J^2] * \phi_s(\varphi(P_0))))/2 = \#((\pi([J^3] * \phi_s(\varphi(P_0))))/2 = 1.
\]

Moreover, we checked that $\Lambda'_3\phi_s(\varphi(P_0))(J)$ and $\Lambda'_3\phi_s(\varphi(P_0))(J^2)(\Lambda'_3\phi_s(\varphi(P_0))(J^3))^{-1}$ are principal, whereas the remaining ones are not. Thus

\[
\tilde{P}_0 = P_0^{\Phi_R([J^s])} \text{ and } P_0^{\Phi_R([J^2])} = P_0^{\Phi_R([J^3])}.
\]

In conclusion we obtain the following diagram, describing the specialization of the Weierstrass points modulo $p = 3$. 

![Diagram](attachment:diagram.png)
Reduction modulo 13

With the same computations as in the previous setting, we obtain that the reduction of \(CM(R)\) and \(CM(R_0)\) modulo \(p = 13\) is given by the following diagram:

```
CM(R)    CM(R0)

|J| |J^2| |J^3|

2   3
```

\(\mathcal{X} \text{ mod } 13\)

**Step 2: Choice of the points at infinity**

Let \(K_\infty = \mathbb{Q}(\sqrt{-7})\) and let \(R_\infty\) be its maximal order. As it is well known, \(#\text{Pic}(R_\infty) = 1\). Hence, by §4.3, for any \(P_\infty \in CM(R_\infty)\) we can choose \(P_\infty\) and \(\omega_{39}(P_\infty)\) to be our points at infinity. This choice gives rise to an equation of the form

\[
y^2 = R(x), \quad \deg(R(x)) = 2g + 2 = 8,
\]

defining the Weierstrass model \(W\). Let \(R(x) = p_R(x) \cdot p_{R_0}(x)\) be the factorization attached to the decomposition \(WP(W) = CM(R) \cup CM(R_0)\). Let \(a_R\) and \(a_{R_0}\) be the leading coefficients of \(p_R\) and \(p_{R_0}\) respectively.

Since \(\mathbb{Q}(\sqrt{a_R \cdot a_{R_0}}) = K_\infty = \mathbb{Q}(\sqrt{-7})\), we deduce that \(a_R \cdot a_{R_0} = -7 \cdot N^2\) for some \(N \in \mathbb{Z}\). Given a prime \(p\) dividing \(a_R \cdot a_{R_0}\), by (4.2.8) we know that:

\[
7 = 39 \cdot m + N(\lambda^-) \cdot p, \text{ where } m = 7N\left(\frac{\lambda + 39}{39}\right) \in \mathbb{Z}^+.
\]

Thus \(m = 0, p = 7\) and \(N(\lambda^-) = 1\). Finally, by (4.2.7) one concludes that the leading coefficient of the hyperelliptic equation must be \(a_R \cdot a_{R_0} = -7\).

Moreover, we can compute \(\varepsilon_{ss}(P_\infty) = \pi(\phi_{ss}(\varphi(P_\infty))) \in \text{Pic}(39, 7, 1)\). Namely,

\[
\pi(\phi_{ss}(\varphi(P_\infty))) = R_\infty \oplus jR_\infty,
\]

where \(jR_\infty\) is the quaternionic complement of \(R_\infty\) with \(j^2 = -39\). Since it can be checked that \(R_0 = \mathbb{Z}[\frac{1 + \sqrt{-39}}{2}]\) can not be embedded in \(\Lambda\), we conclude that \(R = \mathbb{Z}[\sqrt{-39}]\) is embedded optimally in it. Therefore, \(a_{R_0} = 1\) and \(a_R = -7\).

**Step 3: Discriminants, Resultants and Fields of definition**

By Theorem 1.4.3, points in \(CM(R)\) and \(CM(R_0)\) are defined over a subfield of index 2 of the Hilbert class field \(H_K\) of \(K\). By Remark 1.4.4, to find such subextension we must find an ideal \(a\) of \(R\) verifying (4.3.13). As one checks, any \(a\) such that \(N_{K/Q}(a) = 5\) does. Notice that 5 splits in \(K\), hence writing \(5 = \mathfrak{P} \cdot \mathfrak{P}'\) we have \(N_{K/Q}(\mathfrak{P}) = N_{K/Q}(\mathfrak{P}') = 5\).

We used MAGMA [12] to compute that the Hilbert class field of \(K\) is defined by the polynomial \(q(x) = x^4 + 4x^2 - 48\) over \(K\). If \(\alpha\) is any root of \(q(x)\), then \(H_K = \mathbb{Q}(\alpha, \sqrt{-39})\).
The automorphisms $\Phi_R(\mathfrak{P})$ and complex conjugation $c$ act on $H_K$ by the rules:

$$
\Phi_R(\mathfrak{P}) : \begin{cases} 
\sqrt{-39} \rightarrow \sqrt{-39} \\
\alpha \rightarrow \frac{-\sqrt{-39}a^3}{156} - \frac{7\sqrt{-39}a}{39}
\end{cases}
$$

$$
c : \begin{cases} 
\sqrt{-39} \rightarrow -\sqrt{-39} \\
\alpha \rightarrow -\alpha
\end{cases}
$$

Thus $\sigma = c \cdot \Phi_R(\mathfrak{P})$ acts as:

$$
\sigma : \begin{cases} 
\sqrt{-39} \rightarrow -\sqrt{-39} \\
\alpha \rightarrow \frac{-\sqrt{-39}a^3}{156} + \frac{7\sqrt{-39}a}{39}
\end{cases}
$$

We obtain that $M_R$, the fixed field by $\sigma$, is defined by the polynomial $x^4 + 8x^2 - 24x + 16$ over $\mathbb{Q}$. Since $\text{disc}(M_R) = 3^2 \cdot 13$, we have that $\text{disc}(p_R), \text{disc}(p_{R_0}) = N^2 \cdot 3^2 \cdot 13$, for certain $N \in \mathbb{Z}$.

Recall the following diagram summarizing the specialization of the Weierstrass points:

![Diagram]

By Theorem 4.1.3 and (4.3.11), we have that $|\text{disc}(p_R)| = 2^{2k} \cdot 3^2 \cdot 13^3$, $|\text{disc}(p_{R_0})| = 2^{2k'} \cdot 3^2 \cdot 13^3$ and $\text{Res}(p_R, p_{R_0})^2 = 2^{2k''} \cdot 13^4$. Moreover, since $X^{39}_0$ has good reduction at 2, (4.3.12) shows that $2k + 2k' + 2k'' = 16$.

**Step 4: Computing equations**

Since the leading coefficient of $p_R$ is $a_R = -7$, we deduce that $q_R(x) = 7^3p_R(x/7)$ is a monic polynomial of discriminant $7^6\text{disc}(p_R) = 2^{2k} \cdot 3^2 \cdot 13^3$. 76.

The instruction $\text{IndexFormEquation}$ of MAGMA [12] provides the possible candidates for $p_{R_0}$, $q_R$ and $p_R$ (denoted $\tilde{p}_{R_0}$, $\tilde{q}_R$ and $\tilde{p}_R$ respectively), up to transformations of the form $p(x) \rightarrow p(\pm x + r)$ with $r \in \mathbb{Z}$. We obtain that

$$
\tilde{p}_R(x) = \begin{cases} 
-7x^4 - 51x^3 - 16x^2 - 84x - 19 \\
-7x^4 - 74x^3 - 200x^2 - 22x - 1 \\
-7x^4 + 38x^3 + 16x^2 - 182x - 169
\end{cases}
$$

and there are 16 more candidates $\tilde{p}_{R_0}(x)$ for $p_{R_0}(x)$, with discriminants $3 \cdot 13$, $2^4 \cdot 3 \cdot 13$, $2^{12} \cdot 3 \cdot 13$ and $2^{14} \cdot 3 \cdot 13$. If we compute the resultant $\text{Res}(\tilde{p}_R(\mp x + \alpha), \tilde{p}_{R_0}(x))$ and look for solutions $\alpha \in \mathbb{Z}$ such that $\text{Res}(\tilde{p}_R(\mp x + \alpha), \tilde{p}_{R_0}(x))^2 = 2^{2k''} \cdot 13^4$, we obtain a single solution:

$$
p_{R_0}(x) = x^4 + 9x^3 + 29x^2 + 39x + 19, \quad p_R(x) = -7x^4 - 79x^3 - 311x^2 - 497x - 277.
$$
In conclusion the equation we are looking for is

\[ y^2 = -(7x^4 + 79x^3 + 311x^2 + 497x + 277) \cdot (x^4 + 9x^3 + 29x^2 + 39x + 19). \]

Notice that this curve coincides with the one conjectured by Kurihara in [44].

### 4.5 Case \( D = 5 \cdot 11 \)

Let \( \mathcal{X} \) be the hyperelliptic Shimura curve \( \mathcal{X}_{55}^{55}/\mathbb{Q} \). In this case the set of Weierstrass points is \( \text{WP}(\mathcal{X}) = \text{CM}(\mathbb{Z}[\sqrt{-55}]) \sqcup \text{CM}(\mathbb{Z}[\frac{1+\sqrt{-55}}{2}]) \) and both \( \mathbb{Z}[\frac{1+\sqrt{-55}}{2}] \) and \( \mathbb{Z}[\sqrt{-55}] \) have class number 4. As in the above situation, we can compute the geometric special fiber of \( \mathcal{X} \) at 5 and 11 using [42, §3]. In this case, the integral model \( \mathcal{X} \) does not correspond to a Weierstrass model since \( \mathcal{X}/(\omega_D) \) is not smooth over \( \mathbb{Z} \).

In order to transform \( \mathcal{X} \) into a Weierstrass model \( \mathcal{W} \) we shall need to blow down the exceptional divisors and apply relation (4.2.5) to obtain new thicknesses.

Applying our algorithm, we obtain that the specialization of the Heegner points \( \text{CM}(\mathbb{Z}[\sqrt{-55}]) \) and \( \text{CM}(\mathbb{Z}[\frac{1+\sqrt{-55}}{2}]) \) in \( \mathcal{X} \) is given by the following diagram:
Hence, blowing-down \( \mathcal{X} \) as above, we obtain the thickness of the specialization of each Weierstrass point \( P \in \text{WP}(\mathcal{W}) \). Applying the rest of the algorithm just as in §4.4, we obtain that the model \( \mathcal{W} \) over \( \mathbb{Z}[1/2] \) is given by the equation:

\[
y^2 = (-3x^4 + 32x^3 - 130x^2 + 237x - 163) \cdot (x^4 - 8x^3 + 34x^2 - 83x + 81).
\]

This curve also coincides with the one conjectured by Kurihara (cf. [44]) in this case.

### 4.6 Atkin-Lehner quotients

In §4.3 we gave an algorithm which in principle works for any hyperelliptic Shimura curve of odd discriminant admitting a Weierstrass model \( \mathcal{W} \) obtained by blowing-down exceptional divisors of \( \mathcal{X} \). However, this algorithm exploits the instruction \textit{IndexFormEquation}, which is implemented in \textit{MAGMA} only for small degree field extensions. As long as the genus increases, the degrees of the fields involved in the computation become so large that make impossible to proceed with the algorithm.

In this section we shall explain how to adapt the algorithm of §4.3 to compute equations of hyperelliptic quotients of Shimura curves by Atkin-Lehner involutions. We expect that the degrees of the fields involved in this case will be smaller and, consequently, we shall be able to compute more examples.

#### 4.6.1 Quotient of the special fiber

As above, denote by \( \mathcal{X} = \mathcal{X}_0^D / \mathbb{Z} \) Morita’s integral model of \( X = X_0^D \). Write \( Y = X/\langle \omega_m \rangle \) and \( \mathcal{Y} = \mathcal{X}/\langle \omega_m \rangle \). Due to Čerednik-Drinfeld’s uniformization, we have an explicit description of the fiber \( \bar{X} \) at \( p | D \) and the action of the Atkin-Lehner involutions on its set of irreducible components and singular points. This allows us to compute the irreducible components of the fiber \( \bar{Y} \). In order to obtain the thicknesses of its singular points \( (\bar{Y})_{\text{sing}} \), recall that the completed local ring of any singular point \( x \) of \( \bar{X} \) is of the form:

\[
\hat{O}_{\mathcal{X},x'} \simeq \hat{O}_{\mathcal{S},x}[u,v]/(uv - c) \quad c \in m_p,
\]

Here, \( u \) and \( v \) vanish respectively on each of the irreducible components that meet in \( x \).

Let \( \pi : \mathcal{X} \rightarrow \mathcal{Y} \) be the quotient map. If \( \omega_m \) fixes \( x \) there are two possibilities: \( \omega_m \) fixes \( u \) and \( v \) or \( \omega_m \) exchanges them. If \( \omega_m \) fixes \( u \) and \( v \), the completed local ring of the image \( \pi(x) \) is given by

\[
\hat{O}_{\mathcal{Y},\pi(x')} \simeq \hat{O}_{\mathcal{S},x}[x,y]/(xy - c^2),
\]

where the induced pull-back \( \pi^* : \hat{O}_{\mathcal{Y},\pi(x')} \rightarrow \hat{O}_{\mathcal{X},x'} \) is given by \( x \mapsto u^2, \ y \mapsto v^2 \). Thus the thickness of the singular point \( \pi(x) \) is twice the thickness of \( x \). If \( \omega_m u = v \), the completed local ring of the image \( \pi(x) \) is given by

\[
\hat{O}_{\mathcal{Y},\pi(x')} \simeq \hat{O}_{\mathcal{S},x}[z]/(z - c),
\]

where the induced pull-back \( \pi^* : \hat{O}_{\mathcal{Y},\pi(x')} \rightarrow \hat{O}_{\mathcal{X},x'} \) is given by \( z \mapsto uv \). Thus \( \pi(x) \) becomes a non-singular point of \( \mathcal{Y}_p \). Finally, if \( \omega_m(x) = x' \neq x \) the map \( \pi \) is not ramified at \( x \). Hence it provides an isomorphism of local rings \( O_{\mathcal{X},x} \simeq O_{\mathcal{Y},\pi(x)} \). This implies that the thickness of \( \pi(x) \) coincides with that of \( x \). Notice that, since we control the singular specialization of Heegner points in \( \bar{X} \), we also control that of their image in \( \bar{Y} \).
CHAPTER 4. EQUATIONS OF HYPERELLIPTIC SHIMURA CURVES

4.6.2 Weierstrass points, leading coefficients and fields of definition

We shall assume that there exists a quadratic order \( R_\infty \subset K_\infty \) of discriminant prime-to-\( D \) and class number \( h(R_\infty) = 1 \) such that \( \emptyset \neq CM(R_\infty) \subset X(K_\infty) \). Assume also that \( Y \) is hyperelliptic and that the hyperelliptic involution \( \omega \) of \( Y \) is the image of \( \omega_n \) for some \( n \mid D \). Notice that all hyperelliptic Shimura curves in Table 1 verify these assumptions. Clearly \( n \neq m \) since \( \omega_m \) is trivial on \( X \). Finally, assume that blowing-down suitably exceptional divisors of \( Y \) we can obtain a Weierstrass model \( W_Y \) of \( Y \).

As above, the set of Weierstrass points \( WP(Y) \) coincides with the set of fixed points of \( \omega \). Let \( \pi(P) \in WP(Y) \). Then \( \pi(P) = \omega(\pi(P)) = \pi(\omega_n(P)) \), thus \( \omega_n(P) = P \) or \( \omega_n(P) = \omega_m(P) \). It follows that the set \( WP(Y) \) is the image of the union of the set of fixed points of \( \omega_n \) of \( \omega_m \) or \( \omega_n = \omega_{m/n}/\text{gcd}(m,n) \). By Proposition 4.2.1, this set coincides with a set of Heegner points \( \bigsqcup CM(R_i) \), where \( R_i = \mathbb{Q}(\sqrt{-n}) \) or \( \mathbb{Q}(\sqrt{-n \cdot m}) \).

By Theorem 1.4.3, if \( P \in CM(R_i) \) is fixed by \( \omega_n \), \( n \neq D \), then the field of definition of \( P \) is just \( H_{R_i} \). Otherwise, \( \mathbb{Q}(P) \) can be computed as in §4.3. The following proposition describes the field of definition of each \( \pi(P) \in WP(Y) \):

**Proposition 4.6.1.** Let \( n \neq m \) be divisors of \( D \). Let \( P \in CM(R) \) be a Heegner point fixed by \( \omega_n \). Write \( Y = X/\langle \omega_m \rangle \) and set \( \pi : X \to Y \) for the quotient map. Fix an embedding \( H_R \subset \mathbb{C} \) and let \( \zeta \) denote complex conjugation \( P \to \overline{P} \).

1. If \( m \mid n \) then \( \mathbb{Q}(\pi(P)) \) is the subfield of \( \mathbb{Q}(P) \) fixed by \( \Phi_R(m) \), where \( m \) is the unique ideal of \( R \) of norm \( m \).

2. If \( \omega_m(P) = \omega_D(P) \) (i.e. either \( m = D \) or \( n = D/m \)) then \( \mathbb{Q}(\pi(P)) \) is the subfield of \( \mathbb{Q}(P) \) fixed by \( \zeta \cdot \Phi_R([a]) \), where \( a \) is an ideal of \( R \) (depending on \( P \)) satisfying

\[
B \simeq \left( -\frac{n}{m} \cdot \frac{D \cdot N_{R_\infty}/Q(a)}{Q} \right).
\]

3. If \( \omega_m(P) \neq \omega_D(P) \) and \( m \nmid n \) then \( \mathbb{Q}(\pi(P)) = \mathbb{Q}(P) \).

**Proof.** The first assertion follows from the fact that if \( m \mid \text{disc}(K) \) then \( \omega_m(P) = P^{\Phi_R(m)} \). Indeed, directly from the definition, \( \omega_m(\varphi) = [m] \ast \varphi \) for all \( \varphi \in \text{CM}_{D,1}(R) \).

By Theorem 1.4.3, if \( \omega_m(P) = \omega_D(P) \) then \( \omega_m(P) = \overline{P}^{\Phi_R([a])} \) for suitable \( [a] \in \text{Pic}(R) \) satisfying (4.6.14). Thus the second assertion holds.

Finally, if neither \( m \mid n \) nor \( \omega_m(P) = \omega_D(P) \) then \( \omega_m \) acts transitively on the \( \text{Gal}(H_R/\mathbb{Q}) \)-orbit of \( P \). Thus \( \mathbb{Q}(\pi(P)) = \mathbb{Q}(P) \). \( \square \)

As in §4.3, the ideal \( a \) depends on \( P \) but its class \( \{a\} \in \text{Pic}(R_i)/\text{Pic}(R_i)^2 \) only depends on \( R \) and determines the isomorphism class of \( \mathbb{Q}(\pi(P)) \) for every \( P \in CM(R) \). Furthermore, in our particular setting where \( [H : H_R] \) is odd, the class \( \{a\} \) is uniquely determined by (4.6.14).

As in the previous case, the model \( Y \) can be non-hyperelliptic (i.e. \( Y/\omega \) may not be smooth over \( \mathbb{Z} \)). According to our previous assumptions, we can turn it into an hyperelliptic model \( W_Y/\mathbb{Z} \) by blowing-down suitably irreducible components. By means of formula (4.2.5), we can recover the thickness of the singular points of the fiber \( W_Y \). Since we control the specialization of the Weierstrass points \( WP(Y) \) in \( \hat{Y} \), we also control the specialization of the Weierstrass points in \( WP(W_Y) \).
Notice that there may exist Weierstrass points $\pi(P) \in \text{WP}(Y)$ specializing to non-singular points on $Y$, but having singular specialization on $\mathcal{W}_Y$. This happens because their specialization on $Y$ lie on irreducible components which were blown-down in order to obtain $\mathcal{W}_Y$. By means of (3.3.19), we control the irreducible component where the specialization $P$ lies. Hence we control the singular specialization of $\pi(P)$ in the fiber $\mathcal{W}_Y$.

Choose $P_\infty \in \text{CM}(R_\infty)$. Since $h_{R_\infty} = 1$, the set $\text{CM}(R_\infty)$ is a $W(D)$-orbit. Moreover, $\pi(\omega_n(P_\infty)) = \omega(\pi(P_\infty)) \neq \pi(P_\infty)$ since $\omega_n(P_\infty) \neq \omega_m(P_\infty)$, and $\pi(P_\infty)$ is defined over a subfield of $K_\infty$. This implies that we can set $\pi(P_\infty)$ and $\omega(\pi(P_\infty))$ to be our points at infinity.

Once we fix the points at infinity, the model $\mathcal{W}_Y$ is defined, over $\mathbb{Z}[1/2]$, by an equation of the form

$$y^2 = R(x) = \prod_i p_{R_i}(x),$$

where each of the polynomials $p_{R_i}(x)$ is attached to $\pi(\text{CM}(R_i))$, and we control the field that each one defines.

We deduced in §4.2 that the valuation of the leading coefficient $a_R$ at any prime $p$ can be obtained from the intersection index between $\pi(P_\infty)$ and $\omega(\pi(P_\infty))$ at $p$. By the projection formula,

$$(\pi(P_\infty), \pi(\omega_n(P_\infty)))_p = (P_\infty, \pi^n(\omega_n(P_\infty)))_p = (P_\infty, \omega_n(P_\infty))_p + (P_\infty, \omega_{n'}(P_\infty))_p,$$

where $n' = \frac{n-m}{\gcd(m,n)^2}$. Hence, the valuation of the leading coefficient at any prime,

$$\nu_p(a_R) = \left(1 - \left(\frac{K_\infty}{p}\right)\right)(\pi(P_\infty), \pi(\omega_n(P_\infty)))_p,$$

can be computed by means of (4.2.7). Since the leading coefficient $a_{R_i}$ of each $p_{R_i}(x)$ also detects whether $P_\infty$ specializes to the same supersingular point as an element of $\text{CM}(R_i)$, we can compute each $a_{R_i}$ just as in §4.3.

At this point, assuming that $D$ is odd, we can proceed with the algorithm of §4.3 in order to obtain an equation for $\mathcal{W}_Y$. Indeed, we control the leading coefficient of each $p_{R_i}(x)$, their splitting field and the singular specialization of any $\pi(P) \in \text{WP}(\mathcal{W}_Y)$.

### 4.6.3 Example

Let $X = X_0^{35}/\mathbb{Q}$ be the Shimura curve of discriminant 35. In this section we shall compute the quotient curve $Y = X/\langle \omega_5 \rangle$. Since $X$ is itself hyperelliptic we deduce that $Y$ is hyperelliptic. Moreover, we check that it satisfies the assumptions of the previous section.

Write $\pi : \mathcal{X} \to \mathcal{Y}$ for the quotient map as above. The set of Weierstrass points of $Y$ is the image through $\pi$ of the set of Heegner points $\mathcal{S} = \text{CM}(R^{35}) \cup \text{CM}(R_0^{35}) \cup \text{CM}(R^7) \cup \text{CM}(R_0^7)$, where $R^{35} = \mathbb{Z}[\frac{1+\sqrt{-35}}{2}]$, $R_0^{35} = \mathbb{Z}[\sqrt{-35}]$, $R^7 = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ and $R_0^7 = \mathbb{Z}[\sqrt{-7}]$. We obtain that $R^{35}$ has Picard number 2, $R_0^{35}$ has Picard number 6, and both $R^7$ and $R_0^7$ have Picard number 1. Here, we present a diagram that describes the special fibers of $\mathcal{X}$ at $p = 5, 7$ and the specialization of $\mathcal{S}$ computed using the techniques of §4.3.
By Čerednik-Drinfeld’s description of the fiber $\mathcal{X}_5$, we know that $\omega_5$ exchanges its irreducible components, moreover, it exchanges its singular points of thickness 1 and its singular points of thickness 2. Similarly, $\omega_5$ fixes the irreducible components of $\mathcal{X}_7$, exchanges its singular points of thickness 3 and fixes its singular points of thickness 1. Applying the recipe detailed in §4.6.1, we obtained that the specialization of $\pi(\mathcal{S})$ and the special fibers $\mathcal{Y}_5$ and $\mathcal{Y}_7$ are given by the following diagram:

Let $R_\infty$ be the maximal order of $K_\infty = \mathbb{Q}(\sqrt{-43})$. Since $h(R_\infty) = 1$ and $\text{CM}(R_\infty) \neq \emptyset$, we choose $\{\pi(P_\infty), \pi(\omega_D(P_\infty))\} \subseteq \pi(\text{CM}(R_\infty))$ to be our points at infinity. Then, by (4.6.15),

$$\nu_p(a_R) = \left(1 - \left(\frac{K_\infty}{p}\right)\right)((P_\infty, \omega_D(P_\infty))_p + (P_\infty, \omega_D/n(P_\infty))_p)$$

In order to compute $(P_\infty, \omega_D(P_\infty))_p$, we apply (4.2.8) and it follows that

$$43 = 35 \cdot n + N(\lambda^-) \cdot p, \quad n = 43 \cdot N\left(\frac{\lambda^-}{35}\right) \in \mathbb{Z}.$$ 

Hence the solutions are $n = 0$, $p = 43$, $N(\lambda^-) = 1$ and $n = 1$, $p = 2$, $N(\lambda^-) = 4$. Applying formula (4.2.7), we deduce that $(P_\infty, \omega_D(P_\infty))_{43} = 1$ and $(P_\infty, \omega_D(P_\infty))_2 = 2$. 

4.6. ATKIN-LEHNER QUOTIENTS

Similarly for \((P_\infty, \omega_D/m(P_\infty))_p\), we apply formula (4.2.8) obtaining:

\[
43 = 7 \cdot n + N(\lambda^-) \cdot 5 \cdot p, \quad n = 43 \cdot N\left(\frac{\lambda_+}{7}\right) \in \mathbb{Z}.
\]

This implies \(n \equiv 4 \pmod{5}\) and, thus, \(n = 4, p = 3, N(\lambda^-) = 1\). By means of (4.2.7) we have that \((P_\infty, \omega_D(P_\infty))_3 = 1\).

Therefore the unique primes that divide \(a_R\) are 43, 3 and 2 and their valuations are \(\nu_{43}(a_R) = 1, \nu_3(a_R) = 2\) and \(\nu_2(a_R) = 4\). Moreover, we can compute the specialization of \(P_\infty\) and \(\omega(P_\infty)\) at \(p = 3, 43\) and determine which Weierstrass point lie at the same supersingular point as them. We obtained that \(\nu_{43}(a_{R^5}) = 1\) and \(\nu_3(a_{R^5}) = 2\). We can not control the 2-valuation of any leading coefficient \(a_R\), but we know the valuation of the product \(4 = \nu_2(a_R) = \sum_i \nu_2(a_{R_i})\) and this gives an upper bound for all of them.

Finally, applying the rest of the algorithm of §4.3, we obtained that \(Y\) is defined by the equation:

\[
y^2 = -x \cdot (9x + 4) \cdot (4x + 1) \cdot (172x^3 + 176x^2 + 60x + 7).
\]

4.6.4 Results

In this section we present a table with all the equations obtained using the algorithms explained in §4.3 and §4.6:

<table>
<thead>
<tr>
<th>(g)</th>
<th>curve</th>
<th>(y^2 = p(x))</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>(X_0^{39})</td>
<td>(y^2 = -(7x^4 + 79x^3 + 311x^2 + 497x + 277) \cdot (x^4 + 9x^3 + 29x^2 + 39x + 19))</td>
</tr>
<tr>
<td>3</td>
<td>(X_0^{55})</td>
<td>(y^2 = -(3x^4 - 32x^3 + 130x^2 - 237x + 163) \cdot (x^4 - 8x^3 + 34x^2 - 83x + 81))</td>
</tr>
<tr>
<td>2</td>
<td>(X_0^{35}/\langle \omega_5 \rangle)</td>
<td>(y^2 = -x \cdot (9x + 4) \cdot (4x + 1) \cdot (172x^3 + 176x^2 + 60x + 7))</td>
</tr>
<tr>
<td>2</td>
<td>(X_0^{51}/\langle \omega_{17} \rangle)</td>
<td>(y^2 = -x \cdot (7x^3 + 52x^2 + 116x + 68) \cdot (x - 1) \cdot (x + 3))</td>
</tr>
<tr>
<td>2</td>
<td>(X_0^{57}/\langle \omega_3 \rangle)</td>
<td>(y^2 = -(x - 9) \cdot (x^3 - 19x^2 + 119x - 249) \cdot (7x^2 - 104x + 388))</td>
</tr>
<tr>
<td>2</td>
<td>(X_0^{65}/\langle \omega_{13} \rangle)</td>
<td>(y^2 = -(x^2 - 3x + 1) \cdot (7x^4 - 3x^3 - 32x^2 + 25x - 5))</td>
</tr>
<tr>
<td>2</td>
<td>(X_0^{65}/\langle \omega_5 \rangle)</td>
<td>(y^2 = -(x^2 + 7x + 9) \cdot (7x^4 + 81x^3 + 319x^2 + 508x + 268))</td>
</tr>
<tr>
<td>2</td>
<td>(X_0^{69}/\langle \omega_{23} \rangle)</td>
<td>(y^2 = -x \cdot (x + 4) \cdot (4x^4 - 16x^3 + 11x^2 + 10x + 3))</td>
</tr>
<tr>
<td>2</td>
<td>(X_0^{85}/\langle \omega_5 \rangle)</td>
<td>(y^2 = -(3x^2 - 41x + 133) \cdot (x^4 - 23x^3 + 183x^2 - 556x + 412))</td>
</tr>
<tr>
<td>2</td>
<td>(X_0^{85}/\langle \omega_{85} \rangle)</td>
<td>(y^2 = (x^2 - 3x + 1) \cdot (x^4 + x^3 - 15x^2 + 20x - 8))</td>
</tr>
</tbody>
</table>

Table 2
Chapter 5

Further applications

5.1 Equidistribution

In Chapter 2 we showed that, if \( p \parallel DN \), the set of singular points and irreducible components of the fiber \( \tilde{X}_0(D, N) = X_0(D, N) \times \text{Spec}(\mathbb{F}_p) \) are in one-to-one correspondence, respectively, with a suitable set of conjugacy classes of oriented Eichler orders as depicted in the following table:

| \( p \mid D \) | \( \text{Pic}(\frac{D}{p}, Np) \) | \( \bigsqcup_{i=1}^2 \text{Pic}(\frac{D_i}{p}, N) \) |
| \( p \parallel N \) | \( \text{Pic}(Dp, \frac{N}{p}) \) | \( \bigsqcup_{i=1}^2 \text{Pic}(D, \frac{N_i}{p}) \) |

Let \( R \) be an order in an imaginary quadratic field \( K \). The main bulk of Chapter 3 was devoted to construct CM maps \( \phi_s \) and \( \phi_c \) that describe the singular point the or irreducible component, respectively, where a Heegner point \( P \in \text{CM}(R) \) lies. Namely, we obtain commutative diagrams:

\[
\begin{array}{ccc}
\text{CM}_{D,N}(R) & \xrightarrow{\phi_s} & \text{CM}_{Dp,Np}(R) \\
\downarrow \varphi & & \downarrow \pi \\
\text{CM}(R) & \xrightarrow{\phi} & \text{Pic}(\frac{D}{p}, Np) \\
\end{array}
\]

\[
\begin{array}{ccc}
\text{CM}_{D,N}(R) & \xrightarrow{\phi_c} & \bigsqcup_{i=1}^2 \text{CM}_{Dp,N}(R) \\
\downarrow \varphi & & \downarrow \pi \\
\text{CM}(R) & \xrightarrow{\phi} & \bigsqcup_{i=1}^2 \text{Pic}(\frac{D}{p}, N) \\
\end{array}
\]

\[
\begin{array}{ccc}
\text{CM}_{D,N}(R) & \xrightarrow{\phi_s} & \text{CM}_{Dp,N}(R) \\
\downarrow \varphi & & \downarrow \pi \\
\text{CM}(R) & \xrightarrow{\phi} & \text{Pic}(Dp, \frac{N}{p}) \\
\end{array}
\]

Moreover, the maps \( \phi_s \) and \( \phi_c \) intertwine the action of the Atkin-Lehner group \( W(D, N) \) an the action of \( \text{Pic}(R) \) and they are bijective if \( DN \) is square free (see Theorem 3.3.3, Theorem 3.3.7 and Theorem 3.5.2).

The aim of this section is to prove that these results can be combined with recent work of P. Michel [53] concerning the equidistribution of optimal embeddings \( \text{CM}_{d,n}(R) \) in \( \text{Pic}(d, n) \).
in order to obtain a result of equidistribution for the sets \( \text{CM}(R) \) among the set of irreducible components or singular points of the special fiber \( \tilde{X}_0(D, N) \).

### 5.1. Equidistribution

#### 5.1.1 Gross formulas and special values of L-functions

Let \( M \) be a square-free integer. Suppose that \( M \) factorizes as \( M = d \cdot n \), where \( d \) is the product of an odd number of primes. Let \( B \) be the definite quaternion algebra of discriminant \( d \) over \( \mathbb{Q} \). We denote by \( \mathbb{M} \) the free \( \mathbb{Z} \)-module generated by the elements of \( \text{Pic}(d, n) \) and define a pairing

\[
\langle \cdot, \cdot \rangle : \mathbb{M} \times \mathbb{M} \to \mathbb{Z}
\]

by the rule \( \langle \mathcal{O}_i, \mathcal{O}_j \rangle = e(\mathcal{O}_i) \delta_{ij} \), for any \( \mathcal{O}_i, \mathcal{O}_j \in \text{Pic}(d, n) \). Here \( e : \text{Pic}(d, n) \to \mathbb{Z} \) is the map defined in (2.2.3).

Let \( K \) be an imaginary quadratic field of discriminant \( \Delta \) and let \( u \) denote the order of the roots of unity in \( K \). Let \( R \) be an order in \( K \) of conductor \( c \) prime-to-\( M \). Consider the set \( \text{CM}_{d,n}(R) \) of optimal embeddings introduced in §1.2. Fix \( \varphi \in \text{CM}_{d,n}(R) \) and denote by \( \xi = \pi(\varphi) \) its image by the natural map \( \text{CM}_{d,n}(R) \to \text{Pic}(d, n) \subset \mathbb{M} \). For any \( g \in \text{Pic}(R) \), denote also by \( \xi^g \) the image of \( g \cdot \varphi \in \text{CM}_{d,n}(R) \) in \( \text{Pic}(d, n) \). For any character \( \chi : \text{Pic}(R) \to \mathbb{C}^\times \), we denote by \( \xi^\chi \) the expression

\[
\xi^\chi = \sum_{g \in \text{Pic}(R)} \chi^{-1}(g) \xi^g \in \mathbb{Z}[\chi] \otimes \mathbb{M},
\]

Fix an Eichler order \( \mathcal{O} \) of level \( n \) in \( B \). Since \( \text{Pic}(d, n) \simeq \hat{\mathcal{O}}^\times \backslash \hat{B}^\times /B^\times \), we can define a Hecke operator \( T_\ell \) on \( \mathbb{M} \) for every \( \ell \nmid M \) by the rule:

\[
T_\ell(\hat{\mathcal{O}}^\times \hat{b}B^\times) = \sum_{i=0}^{\ell} \hat{\mathcal{O}}^\times g_i \hat{b}B^\times \in \mathbb{M},
\]

where \( \{g_0, g_1, \ldots, g_\ell\} \) are the \( \ell+1 \) matrices corresponding to the \( \ell+1 \) neighbors of the principal vertex of the Bruhat-Tits tree \( \mathcal{O}^\times \backslash B^\times /Q^\times \) (Notice that \( \hat{\mathcal{O}}^\times \hat{B}^\times /B^\times = \prod_i (\mathcal{O}^\times_i \backslash B^\times_i /Q^\times_i) /B^\times \)). More precisely, \( B_\ell \simeq M_2(\mathbb{Q}_\ell), \mathcal{O}_\ell \simeq M_2(\mathbb{Z}_\ell) \) and \( \mathcal{O}^\times_i \backslash B^\times_i /Q^\times_i \simeq \text{PGL}_2(\mathbb{Z}_\ell) \backslash \text{PGL}_2(\mathbb{Q}_\ell) \) is identified to similarity classes of rank two \( \mathbb{Z}_\ell \)-lattices in \( \mathbb{Q}^2_\ell \). The principal vertex corresponds to the lattice \( \mathbb{Z}^2_\ell \) and its \( \ell+1 \) neighbors correspond to the \( \ell \) + \( 1 \) lattices of index \( \ell \) in \( \mathbb{Z}^2_\ell \). We can also define Atkin-Lehner operators \( \omega_p \) for all \( p \mid M \) by setting \( \omega_p(\mathcal{O}) = [\mathbb{P}] \cdot \mathcal{O} \) (cf. Definition 1.1.11), where \( [\mathbb{P}] \) is the unique bilateral \( \mathcal{O}_\ell \)-ideal of norm \( p \). One can easily check that the pairing \( \langle \cdot, \cdot \rangle \) is equivariant for the action of Hecke operators and Atkin-Lehner involutions.

Let \( \mathbb{T} \) be the ring generated over \( \mathbb{Z} \) by \( T_\ell \), if \( \ell \nmid M \), and \( \omega_p \), if \( p \mid M \). Given a normalized newform \( f \in S_2(\Gamma_0(M))^{\text{new}} \) of weight 2 and level \( M \), the Jacquet-Langlands correspondence provides an algebra homomorphism

\[
\phi_f : \mathbb{T} \to R_f, \quad \text{If } \ell \mid dn \text{ then } \omega_p \mapsto a_p \quad \text{If } p \mid d \text{ then } \omega_q \mapsto -a_q \quad \text{If } q \mid n \text{ then }
\]

where \( R_f \) is the ring of integers of the number field \( K_f \) generated by the Fourier coefficients of \( f \).

By [24], there exists an unique \( \nu_f \in \mathbb{M} \otimes K_f \) such that \( \langle \nu_f, \nu_f \rangle = 1 \) and such that \( T(\nu_f) = \phi_f(T)\nu_f \) for every \( T \in \mathbb{T} \). In fact, the vector

\[
\nu_{\text{Eins}} = \left( \sum_{\mathcal{O}_i \in \text{Pic}(d, n)^{-1}} e(\mathcal{O}_i)^{-1} \right)^{-\frac{1}{2}} \cdot \sum_{\mathcal{O}_i \in \text{Pic}(d, n)} e(\mathcal{O}_i)^{-1} \mathcal{O}_i
\]
corresponds to an Eisenstein series because, since \( \langle v_{\text{Eins}}, O_i \rangle = \left( \sum_i \epsilon(O_i)^{-1} \right)^{-\frac{1}{2}} \), we have that
\( T_{\ell}(v_{\text{Eins}}) = (\ell + 1) \cdot v_{\text{Eins}} \) for all \( \ell \nmid d \cdot n \) and \( \langle v_{\text{Eins}}, v_{\text{Eins}} \rangle = 1 \). More precisely, the Eichler’s basis problem [24] says that a \( \mathbb{R} \)-basis for \( \langle v_{\text{Eins}} \rangle^\perp \subset M \otimes \mathbb{R} \) is given by

\[
\mathcal{B}_{d,n} = \{ \omega_n - (\pi_{n^+}^* (v_f)) : n^+ \cdot n^- \mid n, f \in S_2^{\text{new}}(\Gamma_0(d \cdot n^+)) \text{ normalized newform} \},
\]

where \( \pi_{n^+} : M \to M_{n^+} :\mathbb{Z} \text{Pic}(d,n^+)^{\ast} \) is the natural map induced by the forgetful projection \( \text{Pic}(d,n^+) \to \text{Pic}(d,n) \) and \( \langle \cdot, \cdot \rangle \) stands for the orthogonal complement of \( \langle v_{\text{Eins}} \rangle \) by means of the pairing \( \langle \cdot, \cdot \rangle \) above. Define

\[
c_f : M \to K_f \quad \nu \mapsto \langle v_f, \nu \rangle.
\]

The following formula, due to Gross [32] if \( M \) is prime and to Böcherer and Schulze-Pillot [10] for arbitrary \( M \), relates \( c_f(\xi^\chi) \in K_f \) to the special value of the L-series of \( f \) twisted by \( \chi \).

**Theorem 5.1.1.** Suppose that \( \chi : \text{Pic}(R) \to \mathbb{C}^\times \) is a primitive character. Then

\[
c_f(\xi^\chi)^2 = W_{d,n}^K L(f/K, \chi, 1) \sqrt{\Delta} \cdot (u/2),
\]

where \( W_{d,n}^K = \frac{1}{2\pi i (d,n)} \prod_{p \mid d} \left( 1 - \left( \frac{\Delta}{p} \right) \right) \prod_{q \mid n} \left( 1 + \left( \frac{\Delta}{q} \right) \right) \), \( (f,f) \) is the Petersson scalar product of \( f \).

**Remark 5.1.2.** Notice that (5.1.1) is trivial when \( \prod_{p \mid d} \left( 1 - \left( \frac{\Delta}{p} \right) \right) \prod_{q \mid n} \left( 1 + \left( \frac{\Delta}{q} \right) \right) = 0 \). In this case, \( \text{CM}_{d,n}(R) = \emptyset \).

### 5.1.2 Subconvexity problem and equidistribution

The following theorem and proof can be found in [53, Theorem 10]. We have preferred to sketch the details of the proof because in [53] the theorem is stated under the hypothesis that \( M = d \cdot n \) is prime to \( \Delta = \text{disc}(K) \), although the proof works in our current more general setting.

**Theorem 5.1.3.** Let \( \varphi \in \text{CM}_{d,n}(R) \). As \( \Delta \to +\infty \), the orbit \( \text{Pic}(R) \ast \varphi \) becomes equidistributed in the set \( \text{Pic}(d,n) = \{ O_1, \ldots, O_h \} \) relatively to the measure given by

\[
\mu(O_i) = \frac{\epsilon(O_i)^{-1}}{\sum_{j=1}^h \epsilon(O_j)^{-1}}.
\]

More precisely, there exists an absolute constant \( \eta > 0 \) such that

\[
\frac{\# \{ \varphi' \in \text{Pic}(R) \ast \varphi, \pi(\varphi') = O_i \}}{\# \text{Pic}(R)} = \mu(O_i) + O(\Delta^{-\eta})
\]

for any \( i \in \{ 1, \ldots, h \} \). Here, the implied constant \( \eta \) depends on \( M = d \cdot n \) only.
5.1. EQUIDISTRIBUTION

Proof. Write \( \epsilon_i = \epsilon(O_i) \). For any fixed \( j \in \{1, \ldots, h\} \), write \( O_j - \langle O_j, v_{\text{Eins}} \rangle \cdot v_{\text{Eins}} \in \langle v_{\text{Eins}} \rangle^\perp \) as a linear combination of elements of the basis \( \mathcal{B}_{d,n} \) above

\[
O_j - \langle O_j, v_{\text{Eins}} \rangle \cdot v_{\text{Eins}} = \sum_{n^+ = n} \sum_{f \in S_{d,n}^+} x_{n}^f \cdot \omega_n - (\pi_{n^+}^*(v_f)).
\]

Set \( \xi^1 = \sum_{g \in \text{Pic}(R)} g \cdot \xi \) and \( h(R) = \#\text{Pic}(R) \). It follows that

\[
\frac{1}{h(R)} \langle O_i, \xi^1 \rangle = \epsilon_i \cdot \frac{\#\{ \varphi' \in \text{Pic}(R) \cdot \varphi : \pi(\varphi') = O_i \}}{h(R)}.
\]

Besides, \( \langle O_k, v_{\text{Eins}} \rangle = \left( \sum_{i=1}^h \epsilon_i^{-1} \right)^{-\frac{1}{2}} \) for all \( k \), hence

\[
\langle \xi^1, v_{\text{Eins}} \rangle = h(R) \cdot \left( \sum_{i=1}^h \epsilon_i^{-1} \right)^{-\frac{1}{2}}.
\]

This implies that

\[
\frac{1}{h(R)} \langle O_i, \xi^1 \rangle = \sum_{i=1}^h \frac{\epsilon_i^{-1}}{h(R)} \sum_{n^+ = n} \sum_{f \in S_{d,n}^+} x_{n}^f \cdot \langle \xi^1, \omega_n - (\pi_{n^+}^*(v_f)) \rangle.
\]

By the equivariance of the pairing \( \langle \cdot, \cdot \rangle \) under the action of Hecke and Atkin-Lehner operators, we have that

\[
\langle \xi^1, \omega_n - (\pi_{n^+}^*(v_f)) \rangle = \left\langle \sum_{g \in \text{Pic}(R)} g \cdot \xi, v_f \right\rangle,
\]

where \( \xi = \pi_{n^+}^*(\omega_n - (\xi)) \). By Theorem 5.1.1,

\[
\langle \xi^1, \omega_n - (\pi_{n^+}^*(v_f)) \rangle = \sqrt{W_{d,n}^K \frac{L(f/K, 1)}{(f, f)} \Delta \cdot (u/2)}.
\]

By [53, Theorem 2] on the subconvexity problem, we have that \( L(f/K, 1) \ll \Delta^{\frac{1}{2} - \frac{1}{100}} \). Hence

\[
\epsilon_i \cdot \frac{\#\{ \varphi' \in \text{Pic}(R) \cdot \varphi : \pi(\varphi') = O_i \}}{h(R)} - \sum_{i=1}^h \epsilon_i^{-1} \ll \frac{\Delta^{\frac{1}{2} - \frac{1}{100}}}{h(R)}.
\]

Finally, the sought-after result is a consequence of the fact that \( h(R) \geq h(K) \gg \Delta^{\frac{1}{2} + \epsilon} \), as it follows from the Class Number Formula and Siegel’s Theorem. Here \( h(K) \) stands for the class number of \( K \).

Combining the above theorem with our results about specialization of Heegner points, we also obtain the following equidistribution result, which the reader may like to view as complementary to those of Cornut-Vatsal [17].

**Corollary 5.1.4.** Let \( p \) be a prime, assume that \( D \) square-free and write \( \tilde{X}_0(D, N) \) for the special fiber at \( p \) of the Shimura curve \( X_0(D, N) \).

(i) Assume \( p \parallel DN \) and \( p \mid \Delta \). Let \( \tilde{X}_0(D, N)_{\text{sing}} = \{ s_1, s_2, \ldots, s_h \} \) be the set of singular points of \( X_0(D, N) \) and let

\[
\text{CM}(R) \to \tilde{X}_0(D, N)_{\text{sing}}, \; P \mapsto \tilde{P},
\]
denote the specialization map. Then, as $\Delta \to \infty$ and $R$ runs over the set of orders in $K$ with conductor prime to $p$, the Galois orbits $\text{Pic}(R) * Q$, for all $Q \in \text{CM}(R)$, are equidistributed in $\tilde{X}_0(D, N)_{\text{sing}}$ relatively to the measure given by

$$
\mu(s_i) = \epsilon_i^{-1}/\left(\sum_{j=1}^{h} \epsilon_j^{-1}\right),
$$

where $\epsilon_i$ stands for the thickness of $s_i$. More precisely, there exists an absolute constant $\eta > 0$ such that

$$
\#\left\{ P \in \text{Pic}(R) * Q : \tilde{P} = s_i \right\} / h(R) = \mu(s_i) + O(\Delta^{-\eta}).
$$

(ii) Assume $p \mid D$ and is inert in $K$. Let $\tilde{X}_0(D, N)_c = \{ c_1, c_2, \ldots, c_t \}$ be the set of irreducible components of $\tilde{X}_0(D, N)$ and let $\Pi_c : \text{CM}(R) \to \tilde{X}_0(D, N)_c$ denote the map which assigns to a point $P \in \text{CM}(R)$ the irreducible component where its specialization lies. Then, as $\Delta \to \infty$, the Galois orbits $\text{Pic}(R) * Q \subseteq \text{CM}(R)$ are equidistributed in $\tilde{X}_0(D, N)_c$ relatively to the measure $\mu$ of (5.1.2). More precisely, there exists an absolute constant $\eta > 0$ such that

$$
\#\left\{ P \in \text{Pic}(R) * Q : \Pi_c(P) = c_i \right\} / h(R) = \mu(c_i) + O(\Delta^{-\eta}).
$$
5.2 Group of automorphisms of a Shimura curve

Given the Shimura curve $X_0(D, N)$, we defined in §1 the Atkin-Lehner group $W(D, N)$ as a subgroup of the group of automorphisms $\text{Aut}(X_0(D, N))$. It is a 2-elementary abelian group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$, where $r = \#\{p \mid DN\}$. The following proposition characterizes $\text{Aut}(X_0(D, N))$ also as a 2-elementary abelian group, in case that the genus is at least 2.

**Proposition 5.2.1.** [42, Proposition 1.5] Let $U \subseteq W(D, N)$ be a subgroup and let $X_0(D, N)/U$ denote the quotient curve. If the genus of $X_0(D, N)/U$ is at least 2, then all automorphisms of $X_0(D, N)/U$ are defined over $\mathbb{Q}$ and

$$\text{Aut}(X_0(D, N)/U) = (\mathbb{Z}/2\mathbb{Z})^s$$

for some $s \geq r - \text{rank}_{\mathbb{Z}}(U)$.

The following conjecture predicts the structure of $\text{Aut}(X_0(D, N)/U)$:

**Conjecture 5.2.2.** Let $U \subseteq W(D, N)$ and $X_0(D, N)/U$ be as above. Then,

$$\text{Aut}(X_0(D, N)/U) = (\mathbb{Z}/2\mathbb{Z})^{r - \text{rank}_{\mathbb{Z}}(U)}.$$

Assume for simplicity that $N = 1$ and write $X_0^D = X_0(D, 1)$. The following result, due to Kontogeorgis and Rotger, proves Conjecture 5.2.2 for almost all $D \leq 1500$.

**Proposition 5.2.3.** [42, Proposition 3.5] For $D \leq 1500$, the only automorphisms of $X_0^D$ are the Atkin-Lehner involutions, provided $g(X_0^D) \geq 2$ and $D \neq 493, 583, 667, 697, 943$.

The aim of this short section is to show how the material developed in the previous chapters can be used to prove Conjecture 5.2.2 in cases where the techniques of [42] turn out to be insufficient. We illustrate it with an specific example.

**Proposition 5.2.4.** If $D = 667$, $\text{Aut}(X_0^D) = W(D, 1)$.

Before offering the proof, let us invoke first a lemma due to A. Ogg.

**Lemma 5.2.5.** [55] Let $K$ be a field and $\mu(K)$ its group of roots of unity. Let $\rho = \max\{1, \text{char}(K)\}$ be the characteristic exponent of $K$. Let $C$ be an irreducible curve defined over $K$ and $P \in C(K)$ a regular point on it. Let $G$ be a finite group of $K$-automorphisms acting on $C$ and fixing the point $P$. Then there is a homomorphism $f : G \to \mu(K)$ whose kernel is a $p$-group.

**Proof of Proposition 5.2.4.** By Theorem 4.2.1, the set of fixed points of $\omega_{667}$ is $\mathfrak{G}_{\omega_{667}} = \text{CM}(R_0) \sqcup \text{CM}(R)$, where $R_0 = \mathbb{Z}[(1 + \sqrt{-667})/2]$ and $R = \mathbb{Z}[(\sqrt{-667})]$. We computed that $h(R_0) = 4$ and $h(R) = 12$. By Theorem 1.4.2 (Shimura’s reciprocity law), points in $\text{CM}(R_0)$ and points in $\text{CM}(R)$ are defined over different fields, hence $\phi(P) \not\in \text{CM}(R)$, for all $P \in \text{CM}(R_0)$ and all $\phi \in \text{Aut}(X_0^D)$. Moreover, since $\text{Aut}(X_0^D)$ is abelian,

$$\omega_{667}(\phi(P)) = \phi(\omega_{667}(P)) = \phi(P),$$

for all $\phi \in \text{Aut}(X_0^D)$ and $P \in \mathfrak{G}_{\omega_{667}}$. Hence $\phi(\mathfrak{G}_{\omega_{667}}) = \mathfrak{G}_{\omega_{667}}$, and, thus, $\phi(\text{CM}(R_0)) = \text{CM}(R_0)$. 


Let $p = 29$ and write $\tilde{X}_0^D$ for the special fiber of $X_0^D$ at $p$. Since $p$ ramifies in $K = \mathbb{Q}(\sqrt{-667})$, any $P \in \text{CM}(R_0)$ has singular specialization. Recall that the specialization of any point in $\text{CM}(R_0)$ is characterized by the composition of maps

$$\text{CM}(R_0) \xrightarrow{\varphi} \text{CM}_{667,1}(R_0) \xrightarrow{\phi} \text{CM}_{23,29}(R_0) \xrightarrow{\pi} \text{Pic}(23, 29),$$

and the maps $\varphi$ and $\phi_s$ are bijections.

We computed the optimal embeddings $\text{CM}_{23,29}(R_0)$ and their images through the map $\pi$, and we obtained that $\text{CM}_{23,29}(R_0) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$, $\pi(\varphi_1) = \mathcal{O}_1$, $\pi(\varphi_2) = \pi(\varphi_4) = \mathcal{O}_2$, $\pi(\varphi_3) = \mathcal{O}_3$, $\mathcal{O}_1 \neq \mathcal{O}_3$ and $\epsilon(\mathcal{O}_1) = \epsilon(\mathcal{O}_3) = 2$, $\epsilon(\mathcal{O}_2) = 1$, where $\epsilon : \text{Pic}(23, 29) \to \mathbb{Z}$ stands for the map defined as in (2.2.3). By Theorem 3.3.3, this implies that $\text{CM}(R) = \{P_1, P_2, P_3, P_4\}$ specialize to $\tilde{P}_2 = \tilde{P}_4$, $\tilde{P}_1 \neq \tilde{P}_3 \neq \tilde{P}_2$ with thicknesses $\epsilon_{\tilde{P}_1} = \epsilon_{\tilde{P}_3} = 2$ and $\epsilon_{\tilde{P}_2} = 1$.

Applying Lemma 5.2.5 to $C = X_0^D$, where $\rho = 1$, $f$ is injective and $G \cong (\mathbb{Z}/2\mathbb{Z})^t$, we deduce that $G = 1$ or $\mathbb{Z}/2\mathbb{Z}$, since $\mu(K)$ must be cyclic. This implies that there can only exists at most one $\phi \in \text{Aut}(X_0^D)$ such that $\phi(P) = P$ for a given $P \in X_0^D(\overline{\mathbb{Q}})$.

Notice that $\text{Aut}(X_0^D)$ fixes the subset of points in $\text{CM}(R_0)$ that specialize to singular points with the same thicknesses. Thus $\text{Aut}(X_0^D)$ fixes $\{P_1, P_3\}$ (Also $\{P_2, P_4\}$). Since the unique automorphism that fixes $P_1$ or $P_3$ is $\omega_{667}$ by Ogg’s Lemma, we deduce that $\text{Aut}(X_0^D) = (\mathbb{Z}/2\mathbb{Z})^2 = W(667, 1)$. 

$\Box$
5.3 Groups of connected components and the conjecture of Birch and Swinnerton-Dyer

5.3.1 Group of connected components

Let $R_H$ be a complete valuation ring, with fraction field $H$ and algebraically closed residue field $k$. Let $X_H$ be a smooth, proper, geometrically connected curve over $H$. Let $X$ be a proper flat model of $X_H$ over $R_H$, such that the only singularities of the special fiber $X_k$ are ordinary double points. We also assume that the irreducible components of $X_k$ are smooth.

Let $J_H$ be the jacobian of $X_H$, let $J$ be the Néron model of $J_H$ over $R_H$ and let $\Phi = J_k/J^0_k$ be the group of connected components of $J_k$. Let $r : X^{\min} \to X$ denote the minimal resolution of $X$ and let $G^{\min}$ be the dual graph of the special fiber $X_k^{\min}$ of $X^{\min}$. This is the graph whose set of vertices is the set $C^{\min}$ of irreducible components of $X_k^{\min}$ and whose set of edges is the set $\mathcal{S}^{\min}$ of singular points, verifying that an edge joins two vertices if and only if the corresponding irreducible components meet the corresponding singular point. The elements in $C^{\min}$ are Cartier divisors on $X^{\min}$ and the intersection pairing yields a morphism of free $\mathbb{Z}$-modules:

$$\alpha : \mathbb{Z}^{C^{\min}} \longrightarrow \mathbb{Z}^{C^{\min}} \quad \sum C(C', C')C'$$

A theorem of Raynaud (cf. [11, Theorem 9.6/1]) gives a canonical description of $\Phi$ as the homology of the complex:

$$\mathbb{Z}^{C^{\min}} \xrightarrow{\alpha} \mathbb{Z}^{C^{\min}} \xrightarrow{+} \mathbb{Z},$$

where the map $+$ is defined by the rule $\sum_i n_i C_i \mapsto \sum_i n_i$.

Grothendieck gave another description of $\Phi$ in terms of the graph $G^{\min}$ (cf. [34, Theorem 11.5]). Let us compare both descriptions.

Choose an orientation of $G^{\min}$, i.e. choose two maps $s$ and $t$ from $\mathcal{S}^{\min}$ to $C^{\min}$ such that for all edges $x$, $s(x)$ and $t(x)$ are the vertices meeting $x$. We get induced maps:

$$s_* , t_* : \mathbb{Z}^{\mathcal{S}^{\min}} \longrightarrow \mathbb{Z}^{C^{\min}}, \quad s^*, t^* : \mathbb{Z}^{C^{\min}} \longrightarrow \mathbb{Z}^{\mathcal{S}^{\min}}$$

$$x \mapsto s(x), t(x) \quad C \mapsto \sum_{s(x) = C} x \sum_{t(x) = C} x.$$

It is clear that $s_*, t_*$ and $s^*, t^*$ are dual each other if we identify $\mathbb{Z}^{C^{\min}} = \text{Hom}(\mathbb{Z}^{C^{\min}}, \mathbb{Z}) = (\mathbb{Z}^{C^{\min}})^\vee$ and $\mathbb{Z}^{\mathcal{S}^{\min}} = \text{Hom}(\mathbb{Z}^{\mathcal{S}^{\min}}, \mathbb{Z}) = (\mathbb{Z}^{\mathcal{S}^{\min}})^\vee$ by means of the natural pairing. With this notation, we can define the usual boundary and coboundary maps:

$$d_* := t_* - s_* : \mathbb{Z}^{\mathcal{S}^{\min}} \longrightarrow \mathbb{Z}^{C^{\min}}, \quad d^* := t^* - s^* : \mathbb{Z}^{C^{\min}} \longrightarrow \mathbb{Z}^{\mathcal{S}^{\min}}.$$

By definition, $\ker(d_*)$ is the homology group $H_1(G^{\min}, \mathbb{Z})$ and $\text{coker}(d^*) = H^1(G^{\min}, \mathbb{Z})$ (these isomorphisms depend on the orientation chosen). Since $G^{\min}$ is connected, $\ker(d^*) = H^0(G^{\min}, \mathbb{Z})$ is the diagonal map in $\mathbb{Z}^{C^{\min}}$, and $\text{coker}(d_*) = H_0(G^{\min}, \mathbb{Z})$ is $\mathbb{Z}$, via the map $+ : \mathbb{Z}^{C^{\min}} \longrightarrow \mathbb{Z}$.

Note that, if $C \neq C'$, we have $(C, C') = 1$ if and only if there exists $x \in \mathcal{S}^{\min}$ such that either $s(x) = C$ and $t(x) = C'$, or $t(x) = C$ and $s(x) = C'$. Otherwise $(C, C') = 0$. Furthermore, by [47, Proposition 9.1.21],

$$(C, C) = - \sum_{C' \neq C} (C, C') = -\# \{ x \in \mathcal{S}^{\min} : s(x) = C \} - \# \{ x \in \mathcal{S}^{\min} : t(x) = C \}.$$
Hence,
\[
\sum_{C' \neq C} (C, C') C' = \sum_{s(x)=C} t(x) + \sum_{t(x)=C} s(x) = t* s*(f) + s* t*(f)
\]
and
\[
(C, C) C = - \sum_{s(x)=C} s(x) - \sum_{t(x)=C} t(x) = -s* s*(f) - t* t*(f).
\]
In conclusion we obtain
\[
\alpha = s* t* + t* s* - s* s* - t* t* = -(t* - s*)(t* - s*) = -d* d*.
\]

Write \(M = H_1(G_{min}, \mathbb{Z})\) and let \(M^\vee\) be the \(\mathbb{Z}\)-linear dual of \(M\). Note that there is a canonical isomorphism between \(M^\vee\) and \(H_1(G_{min}, \mathbb{Z})\). The equalities \(H_1(G_{min}, \mathbb{Z}) \cong \ker(d*)\), \(H_1(G_{min}, \mathbb{Z}) \cong \coker(d*)\) and \(\alpha = -d* d*\) give rise to the following commutative diagram:

\begin{equation}
\begin{array}{cccccc}
0 & \rightarrow & M & \rightarrow & M^\vee & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \rightarrow & \mathbb{Z} & \rightarrow & \mathbb{Z}_{C_{min}}^{\vee} & \rightarrow & \mathbb{Z}_{C_{min}}^{[+]}
\end{array}
\end{equation}

where \(\mathbb{Z}_{C_{min}}^{[+]} = \ker(+ : \mathbb{Z}_{C_{min}} \rightarrow \mathbb{Z})\) and \(\text{diag} : \mathbb{Z} \rightarrow \mathbb{Z}_{C_{min}}\) is the usual diagonal map.

As a consequence, we obtain the short exact sequence:
\[
0 \rightarrow M \rightarrow M^\vee \rightarrow \Phi \rightarrow 0.
\]

One obtains that for all \(m_1 = \sum_{x \in S_{min}} m_1(x)x\) and \(m_2 = \sum_{x \in S_{min}} m_2(x)x\) in \(M\) (see [22]):
\[
(i(m_1))(m_2) = \sum_{x \in S_{min}} m_1(x)m_2(x).
\]

Exact sequence (5.3.4) and equality (5.3.5) give an explicit description of \(\Phi\), which is due to Grothendieck. The commutative diagram (5.3.3) gives a translation between Raynaud’s and Grothendieck’s points of view.

We devote the rest of this section to describe \(M\) and \(\Phi\) in terms of \(X\) instead of \(X_{min}\). Let \(\mathcal{G}\) be the graph associated to \(X\), defined similarly as before: the set of vertices of \(\mathcal{G}\) is the set \(\mathcal{C}\) of irreducible components of \(X_k\), the set of edges is the set \(\mathcal{S}\) of singular points of \(X_k\) and two vertices \(v\) and \(v'\) are linked by those edges corresponding to intersection points of the components associated with \(v\) and \(v'\).

Recall the birational map \(r : X_{min} \rightarrow X\). For \(x\) in \(\mathcal{S}\) we denote by \(\epsilon(x)\) the thickness of the singularity at \(x\). It is well known that \(r^{-1}(x)\) is a chain of \(\epsilon(x) - 1\) projective lines. In
terms of graphs, this means that \( G_{\text{min}} \) is obtained from \( G \) by replacing each edge \( x \) of \( G \) by a path of \( \epsilon(x) \) edges. It is clear that an orientation on \( G \) induces an orientation on \( G_{\text{min}} \). We assume that the orientation of \( G_{\text{min}} \) comes from an orientation on \( G \); the corresponding maps \( S \to C \) shall also be denoted by \( s \) and \( t \). It is also clear that \( H_1(G, \mathbb{Z}) \) and \( H_1(G_{\text{min}}, \mathbb{Z}) \) are canonically isomorphic. The transformation from \( G \) to \( G_{\text{min}} \), that replaces an edge \( x \) by \( \epsilon(x) \) edges, suggests considering the following maps:

\[
\begin{align*}
h_C : \mathbb{Z}^C & \to \mathbb{Z}^{C_{\text{min}}} , \\
h_S : \mathbb{Z}^S & \to \mathbb{Z}^{S_{\text{min}}} , \\
x & \mapsto \sum_{y \in r^{-1}(x)} y
\end{align*}
\]

where \( \tilde{C} \) stands for the strict transform of \( C \). One easily derives the following commutative diagram:

\[
\begin{array}{ccccccc}
0 & \to & M & \xrightarrow{d_s} & \mathbb{Z}^S & \xrightarrow{h_S} & \mathbb{Z}^C & \to & 0 \\
\id & & \downarrow & & \downarrow & & \downarrow & & \id \\
0 & \to & M & \xrightarrow{d_s} & \mathbb{Z}^{S_{\text{min}}} & \xrightarrow{h_C} & \mathbb{Z}^{C_{\text{min}}} & \to & 0.
\end{array}
\]

Taking duals, we obtain yet another commutative diagram

\[
\begin{array}{ccccccc}
0 & \to & \mathbb{Z} & \xrightarrow{\text{diag}} & \mathbb{Z}^{C_{\text{min}}} & \xrightarrow{d^*} & \mathbb{Z}^{S_{\text{min}}} & \to & \mathbb{Z} & \to & 0 \\
\id & & \downarrow & & \downarrow & & \downarrow & & \id \\
0 & \to & \mathbb{Z} & \xrightarrow{\text{diag}} & \mathbb{Z}^C & \xrightarrow{d^*} & \mathbb{Z}^S & \to & \mathbb{Z} & \to & 0.
\end{array}
\]

where \( h_S^\vee \) and \( h_C^\vee \) are given by:

\[
\begin{align*}
h_C^\vee : \mathbb{Z}^{C_{\text{min}}} & \to \mathbb{Z}^C , \\
h_S^\vee : \mathbb{Z}^{S_{\text{min}}} & \to \mathbb{Z}^S , \\
y & \mapsto r(y).
\end{align*}
\]

Here \( r_* (\tilde{C}) \) is defined to be zero if \( r(\tilde{C}) \) is a point, while \( r_* (\tilde{C}) = r(\tilde{C}) \) otherwise.

The map \( h_S \) introduced above is injective; it induces an inner product on \( \mathbb{Z}^S \) arising from the standard inner product on \( \mathbb{Z}^{S_{\text{min}}} \):

\[
\langle \cdot, \cdot \rangle : \mathbb{Z}^S \times \mathbb{Z}^S \to \mathbb{Z}, \quad \left\langle \sum_{x \in S} n_1(x)x, \sum_{x \in S} n_2(x)x \right\rangle = \sum_{x \in S} \epsilon(x)n_1(x)n_2(x). \tag{5.3.6}
\]

As a consequence, when we view \( M \) as a submodule of \( \mathbb{Z}^S \) and \( M^\vee \) as a quotient of it, the map \( i : M \to M^\vee \) is given by:

\[
m_1, m_2 \in M, \quad (i(m_1))(m_2) = \sum_{x \in S} \epsilon(x)m_1(x)m_2(x).
\]

This discussion allows us to translate between Raynaud’s description of \( \Phi \) in terms of \( X_{\text{min}} \) and Grothendieck’s.
Specialization of divisors of degree zero

Since \( X \) and \( X_{\text{min}} \) are proper over \( R_H \), we can identify \( X(H), X(R_H) \) and \( X_{\text{min}}(R_H) \). The closure in \( X_{\text{min}} \) of an effective divisor on \( X_H \) is a Cartier divisor. Extending by linearity, one can associate to each divisor \( D \) on \( X_H \) a Cartier divisor \( \overline{D} \) on \( X_{\text{min}} \).

Let \( D \) be a divisor of degree zero on \( X_H \). Its class up to linear equivalence corresponds to an element \([D]\) of \( J(H) = J(R_H) \). Let \( \xi_D \) denote the image of \([D]\) in \( \Phi \). Below we shall obtain an expression for \( \xi_D \) in terms of \( \mathbb{Z}^C \) and \( \mathbb{Z}^S \). For simplicity assume that, after extending \( H \) if it is necessary, \( D \) has support in the set of \( H \)-rational points of \( X \). Write

\[
D = \sum_P n_P P,
\]

where \( n_P \in \mathbb{Z} \), \( P \in X(H) \). Since \( X_{\text{min}} \) is regular, each \( P \) in \( X(H) \) specializes to a unique element \( c(P) \) in \( C_{\text{min}} \) (cf. [71, Corollary IV.4.4]). Thus \( \xi_D \) is given by the element \( \sum_P n_P c(P) \) of \( C_{\text{min}} \).

Suppose that \( P \) is such that \( c(P) \) is not in \( C \). Let \( x \in S \) be the image of \( c(P) \) under the morphism \( r : X_{\text{min}} \to X \). The inverse image \( r^{-1}(x) \) corresponds to a chain of edges \( x_1, x_2, \ldots, x_{t(x)} \):

\[
\bullet s(x) \quad x \quad \bullet t(x)
\]

\[
\bullet x_1 \bullet x_2 \bullet \ldots \bullet x_{m(P)} \bullet x(P) \bullet \ldots \bar{\bullet} \bar{x}(x) \bullet
\]

The integer \( m(P) \) is defined by the condition that \( c(P) \) is the \( m(P) \)-th projective line in the chain of projective lines from \( s(x) \) to \( t(x) \) in \( X_{\text{min}} \). We have

\[
c(P) = t_*(x_{m(P)}) = d_*(x_1) + d_*(x_2) + \cdots + d_*(x_{m(P)}) + h_C(s(x)).
\]

Since \( h_C(x_1 + x_2 + \cdots + x_{m(P)}) = r(x_1) + r(x_2) + \cdots + r(x_{m(P)}) = m(P)x \) and \( x = r(c(P)) \), we obtain two contributions for \( \phi(D) \):

\[
\sum_{c(P) \in C} n_P c(P) + \sum_{c(P) \not\in C} n_P s(r(c(P))) \in \mathbb{Z}^C[+] \subseteq \mathbb{Z}^{C_{\text{min}}}[+], \tag{5.3.7}
\]

and

\[
\sum_{c(P) \not\in C} n_P m(P)r(c(P)) \in \mathbb{Z}^S. \tag{5.3.8}
\]

Finally, let us give an interpretation of the integers \( m(P) \). Suppose that \( P \in X(H) \) is such that \( c(P) \) is not in \( C \). Let \( x \) denote the element \( r(c(P)) \) of \( S \). Let \( \pi \) be a uniformizer of \( R_H \) and let \( u \) and \( v \) be elements of the complete local ring \( \hat{O}_{X,x} \) such that \( \hat{O}_{X,x} = R_H[[u,v]]/(uv - \pi^t(x)) \).

By interchanging \( u \) and \( v \) if necessary, we can assume that \( (u, \pi) \) is the ideal of the branch \( s(x) \). Let \( c_0, c_1, \ldots, c_{t(x)} \) be the irreducible components of \( r^{-1}(x) \) such that \( s(x_i) = c_{i-1} \) and \( t(x_i) = c_i \). In [22, Pag. 5] it is computed the divisor \( \text{Div}(v) \) of \( v \) on the completion \( X_{\text{min}} \) along \( r^{-1}(x) \). Namely:

\[
\text{Div}(v) = \sum_{i=0}^{t(x)} i c_i.
\]
This equality gives an interpretation of the integer \( m(P) \):

\[
m(P) = (P, m(P)c(P)) = (P, \sum_{i=0}^{\epsilon(x)} (P, i_c) = (P, \text{Div}(v)) = \text{val}_{R_H}(P^\ast(v)),
\]

(5.3.9)

where \( \text{val}_{R_H} \) denotes the valuation on \( R_H \) such that \( \text{val}_{R_H}(\pi) = 1 \) and \( P^\ast \) is the ring homomorphism \( \mathcal{O}_{X,x} \to R_H \) induced by the morphism of schemes \( P : \text{Spec}(R_H) \to X \).

### 5.3.2 Specialization of Heegner points on the group of connected components

In this section we shall compute the image of a Heegner divisor on the group of connected components of the special fiber at \( p \mid DN \) of the Jacobian \( J_0(D, N) \) of the Shimura curve \( X_0(D, N) \). In order to deal with this computation, we shall exploit our results on the specialization of Heegner points presented in §3.

Assume \( DN \) is square free, let \( \mathcal{X}_0(D, N) \) denote Morita’s integral model of \( X_0(D, N) \) and set \( X_0(D, N) = \mathcal{X}_0(D, N) \times \text{Spec}(\mathbb{F}_p) \). Fix \( \mathbb{F} \) an algebraic closure of \( \mathbb{F}_p \) and an embedding \( \mathbb{Q} \to \mathbb{Q}_p \). Let \( K \) be an imaginary quadratic field. Write \( J_0(D, N) \times \text{Spec}(K) \) and \( \Phi^K \) for the group of connected components of \( J_0(D, N) \), the special fiber of \( J_0(D, N) \) at a prime ideal \( \mathfrak{p} \) above \( p \).

**Heegner points of good reduction**

Let \( R \) be an order in \( K \) and assume that \( p \) does not ramify in \( K \) and the conductor of \( R \) is prime to \( p \). Let \( \mathbb{Q}_p^{nr} \) be the maximal unramified extension of \( \mathbb{Q}_p \) and let \( H_R \) be the ring class field of \( R \). Let \( P_1, \ldots, P_k \in \text{CM}(R) \) be Heegner points and let \( D = \sum_{i=1}^k n_i P_i \) be a degree zero divisor. Since \( P_i \in X_0(D, N)(H_R) \) and \( H_R \subset \mathbb{Q}_p^{nr} \), by extending scalars to \( \mathbb{Q}_p^{nr} \) we can apply the results of the above section in order to obtain the image of \( D \) on \( \Phi^K \). By (5.3.7), such image \( \xi_D \in \Phi^K \) arises from the contribution \( \sum_{i=1}^k n_i \Pi_c(P_i) \in \mathbb{Z}^C \), where \( \Pi_c : X_0(D, N)(\mathbb{F}_p) \to C \) is the map that assigns to each non-singular point the irreducible component where it lies. In turn, \( \Pi_c(\tilde{P}_i) \) is characterized by the image of \( P_i \) through the maps

\[
\text{CM}(R) \xrightarrow{\varphi} \text{CM}_{D,N}(R) \xrightarrow{\phi_c} \text{CM}_{d,n}(R) \xrightarrow{\pi} \text{Pic}(d, n) \cup \text{Pic}(d, n),
\]

where \( (d, n) = (D/p, N) \) or \( (D, N/p) \) depending whether \( p \mid D \) or \( p \mid N \) and \( \phi_c \) are the maps of (3.5.21) and (3.3.18), respectively. Hence, \( \xi_D \) will be the image of \( \sum_{i=1}^k n_i \pi(\phi_c(\varphi(P_i))) \in \mathbb{M} \oplus \mathbb{M} \simeq \mathbb{Z}^C \), where \( \mathbb{M} = \mathbb{Z}^\text{Pic}(d, n) \), through the corresponding natural map \( \mathbb{M} \oplus \mathbb{M}[-] \to \Phi^K \).

**Heegner points of bad reduction**

Assume that \( p \mid DN \) and \( p \) ramifies in \( K \). Let \( P \in \text{CM}(R) \) be a Heegner point. By Theorem 3.3.2, \( P \) specializes to a singular point \( \tilde{P} \in X_0(D, N)_{\text{sing}} \). Let \( K_p^{nr} \) denote the maximal unramified extension of \( K_p \). Since the conductor of \( R \) is prime to \( p \), \( H_R \subset K_p^{nr} \) and \( P \in X_0(D, N)(K_p^{nr}) \). Let \( R_p^{nr} \) be the integer ring of \( K_p^{nr} \) and fix an uniformizer \( \tau_R \). Notice that \( [K_p^{nr} : \mathbb{Q}_p^{nr}] = 2 \) and \( \text{ord}_{\mathfrak{p}_R}(p) = 2 \).

Let \( \mathcal{D} = \sum_{i=1}^k n_i P_i \) be a degree zero divisor, where \( P_i \in \text{CM}(R) \) are Heegner points of singular specialization. By relations (5.3.7) and (5.3.8), the image \( \xi_D \) of the divisor in the
group of connected components $\Phi^K$ is given by the image of

$$\xi_D^C = \sum_i n_i s(P_i) \in \mathbb{Z}^C[+] \quad \text{and} \quad \xi_D^S = \sum_i m(P_i) n_i \tilde{P}_i \in \mathbb{Z}^S.$$ 

In order to compute $\xi_D^C$ we distinguish two cases:

1. If $p \mid N$, the special fiber $\tilde{X}_0(D, N)$ has two irreducible components. We can choose the map $s : S \to C$ to be the map that sends every singular point to one fixed irreducible component. Then $s(\tilde{P}_i) = s(\tilde{P}_j)$ for all $i, j$ and $\xi_D^C = 0$ since $\sum_i n_i = 0$.

2. If $p \mid D$, the irreducible components of $\tilde{X}_0(D, N)$ are in one-to-one correspondence with two copies of $\text{Pic}(D/p, N)$ and the set of singular points with $\text{Pic}(D/p, Np)$. Moreover, given a point $\tilde{P} \in \tilde{X}_0(D, N)_{\text{sing}}$ corresponding to $\varepsilon_s(\tilde{P}) \in \text{Pic}(D/p, Np)$, the two components meeting at $\tilde{P}$ are in correspondence with the images of $\varepsilon_s(\tilde{P})$ through the natural forgetful maps

$$\delta, \delta \circ \omega_p : \text{Pic} \left( \frac{D}{p}, Np \right) \cong \text{Pic} \left( \frac{D}{p}, N \right).$$

If we fix $s : S \to C$ to be the map attached to the map $\delta : \text{Pic}(D/p, Np) \to \text{Pic}(D/p, N)$ induced by the orientations at $p$, then by (3.3.16):

$$\xi_D^C = \sum_i n_i \delta(\varepsilon_s(\tilde{P}_i)) = \sum_i n_i \delta(\pi(\phi_s(\varphi(P_i)))) \in \mathbb{M} \subset \mathbb{M} \oplus \mathbb{M} \cong \mathbb{Z}^C,$$

where $\mathbb{M} = \mathbb{Z}^{\text{Pic}(D/p, N)}$.

In order to carry on the computation of $\xi_D$ we shall need to compute the integer $m(P)$ for every $P \in \text{CM}(R)$. Recall that the local ring of $\mathcal{X} := \mathcal{X}_0(D, N) \times \text{Spec}(R^\text{nr}_p)$ at $\tilde{P}$ corresponds to

$$\mathcal{O}_{\mathcal{X}, \tilde{P}} = \frac{R_p^\text{max}[u, v]}{(uv - P^*(\varepsilon_s(\tilde{P}))},$$

by Theorem 2.2.1. Thus, by (5.3.9), $m(P)$ is given by $m(P) = \text{val}_{\pi_R}(P^*(v))$.

The Atkin-Lehner involution $\omega_p$ exchanges $u$ and $v$. Moreover, since $p$ ramifies in $K$, $\omega_p$ turns out to act as a Galois conjugation on $P$. Since Galois conjugations do not change the valuations $\text{val}_{\pi_R}(P^*(v))$, $\text{val}_{\pi_R}(P^*(u))$ and $\text{val}_{\pi_R}(P^*(v)) + \text{val}_{\pi_R}(P^*(u)) = \text{val}_{\pi_R}(p^*(\varepsilon_s(\tilde{P})))$, we conclude that

$$m(P) = \text{val}_{\pi_R}(P^*(v)) = \text{val}_{\pi_R}(P^*(u)) = \varepsilon(\varepsilon_s(\tilde{P})) \cdot \frac{\text{val}_{\pi_R}(p)}{2} = \varepsilon(\varepsilon_s(\tilde{P})).$$

In conclusion,

$$\xi_D^S = \sum_i \varepsilon(\varepsilon_s(\tilde{P}_i)) m_i \varepsilon_s(\tilde{P}_i) = \sum_i \varepsilon(\pi(\phi_s(\varphi(P_i)))) m_i \pi(\phi_s(\varphi(P_i))) \in \mathbb{M}_s \cong \mathbb{Z}^S, \quad (5.3.10)$$

where $\mathbb{M}_s = \mathbb{Z}^{\text{Pic}(d, n)}$; $(d, n) = (D/p, Np)$ or $(Dp, N/p)$ depending whether $p \mid D$ or $p \mid N$, respectively.

Recall that in §5.1.1 we introduced a natural pairing

$$\mathbb{M}_s \times \mathbb{M}_s \to \mathbb{Z}, \quad \langle O_i, O_j \rangle = \varepsilon(O_i) \delta_{i,j}$$
that induces a map $\kappa : M_s \to M_s^\vee$, $\mathcal{O}_i \mapsto (\mathcal{O}_j \mapsto (\mathcal{O}_i, \mathcal{O}_j))$. Also recall the short exact sequence

$$0 \to M \xrightarrow{i} M^\vee \to \Phi^K \to 0$$

of (5.3.4), where $M = \ker(d_s)$ and $M^\vee = \coker(d^*)$. Regarding $M$ as a submodule of $M_s$, we have $i = 2\kappa$. Moreover, $\xi_D^C = \kappa(\varepsilon_s(D))$ where $\varepsilon_s(D) = \sum_i n_i \varepsilon_s(\tilde{P}_i)$.

As above we distinguish two cases:

1. If $p \mid N$ the map $d_s$ corresponds to the natural map $M_s \xrightarrow{d_s} \mathbb{Z} \times \mathbb{Z}$, $\mathcal{O}_i \mapsto (1, -1)$. Thus $M = \ker(d_s)$ is identified with

$$M \cong M_s^0 = \left\{ \sum_i n_i \mathcal{O}_i : \sum_i n_i = 0 \right\} = \ker(\deg : M_s \to \mathbb{Z}).$$

Recall that, in this case, $\xi_D^C = 0$ and $\xi_D^S = \kappa(\varepsilon_s(D))$, where $\varepsilon_s(D) \in M_s^0$.

2. If $p \mid D$ the map $d_s$ is identified with

$$M_s \xrightarrow{d_s} M \times M, \quad \mathcal{O}_i \mapsto (\delta(\mathcal{O}_i), -\delta(\omega_p(\mathcal{O}_i))),$$

where $M = \mathbb{Z}^{\Pic(D/p, \mathbb{N})}$. Thus $\ker(d_s) = M \cong M_s^0 := \{ m \in M_s; \delta(m) = 0 \} = \ker(\delta)$, where $\delta : M_s \to M$ is the morphism induced by the map $\delta : \Pic(D/p, \mathbb{N}) \to \Pic(D/p, \mathbb{N})$ introduced above. Notice that, in our case, $\xi_D^C = \delta(\varepsilon_s(D))$ and $\xi_D^S = \kappa(\varepsilon_s(D))$. If we also assume that $\omega_p(D) = D$, then clearly $\delta(\varepsilon_s(D)) = \delta(\omega_p(\varepsilon_s(D))) = 0$. Hence, $\xi_D^C = 0$ and $\varepsilon_s(D) \in M_s^0$.

Since $i = 2\kappa$, (5.3.4) gives rise to an exact sequence

$$0 \to M_s^0 \to M_s^0 \xrightarrow{2} M_s^0 \xrightarrow{\lambda} \Phi^K \to (M_s^0)^{\vee} / \kappa(M_s^0) \to 0. \quad (5.3.11)$$

Moreover, in both cases (assuming that if $p \mid D$, $\omega_p(D) = D$) $\xi_D = \lambda(\varepsilon_s(D))$.

**Remark 5.3.1.** The exact sequence (5.3.11) implies that the image of such singular Heegner divisors lies in $\Phi^K[2]$, the 2-torsion subgroup of $\Phi^K$.

### 5.3.3 Heegner points and special values of L-functions

Let $p \mid DN$ be a prime of bad reduction of $X_0(D, N)$ and assume that $DN$ is square-free. Let $\mathcal{J}_0(D, N)$ and $\Phi^K$ be as in the previous section.

Let $f \in S_2(\Gamma_0(M))_{\text{new}}$ be a normalized newform of weight 2. Let $T$ be the ring generated over $\mathbb{Z}$ by the Hecke correspondences $T_\ell$ for primes $\ell \nmid DN$ and by the Atkin-Lehner involutions on $X_0(D, N)$, equipped with the degree map

$$\deg : T \to \mathbb{Z}, \quad T_\ell \mapsto \ell + 1, \quad \omega_m \mapsto 1.$$

Write $T_0 \subset T$ for the kernel of the degree map. The Hecke algebra $T$ acts in a compatible way on $\mathcal{J}_0(D, N)(H_R)$, $\mathcal{J}_0(D, N)$ and on $\Phi^K$. Write $\phi_f : T \to R_f$ for the homomorphism associated to $f$ by the Jacquet-Langlands correspondence. By the Eichler’s basis problem (cf. [24]), there exists a unique idempotent $\pi_f \in T \otimes K_f$ such that $T \circ \pi_f = \phi_f(T)\pi_f$ for all $T \in T$. 

---
The group of connected components $\Phi^K$ is equipped with a Hecke equivariant canonical monodromy pairing (cf. [34])

$$[\cdot, \cdot] : \Phi^K \times \Phi^K \rightarrow \mathbb{Q}/\mathbb{Z},$$

which is defined as follows. The map $2\kappa$ induces an isomorphism between $M^0_s \otimes \mathbb{Q}$ and $\text{Hom}(M^0_s, \mathbb{Q})$ which allows us to extend the pairing $2\langle \cdot, \cdot \rangle$ to a $\mathbb{Q}$-valued pairing on $(M^0_s)^\vee \subseteq \text{Hom}(M^0_s, \mathbb{Q})$. The reader may check that, passing to the quotient, it gives rise to a well defined pairing on $\Phi^K = (M^0_s)^\vee/2\kappa(M^0_s)$ with values in $\mathbb{Q}/\mathbb{Z}$. Considering the morphism $\lambda : M^0_s \rightarrow \Phi^K$ of (5.3.11), one checks that

$$[\lambda D, \lambda D'] = \frac{1}{2} \langle D, D' \rangle \pmod{\mathbb{Z}}. \quad (5.3.12)$$

Combining our results on the image of the Heegner divisors in $\Phi$ with formula (5.1.1) we obtain the following result, completely analogous to [7, Theorem A]. Let $K$ be an imaginary quadratic field and let $\Delta = \text{disc}(K)$ denote its discriminant. Let $R$ be an order in $K$ of conductor $c$ prime to $p$ and assume that $p$ ramifies in $K$.

**Theorem 5.3.2.** Let $P \in \text{CM}(R) \subset X_0(D, N)(H_K)$ be a Heegner point, let $\chi$ be a primitive character of $\text{Pic}(R)$ and let $\xi_f^T$ be the image of $e_\chi(T(P))$ in $\Phi^K$, where $e_\chi = \sum_{g \in \text{Pic}(R)} \lambda(g)^{-1} g \in \mathbb{Z}[[\text{Pic}(R)]]$ and $T \in T_0$.

Choose $n_f \in \mathbb{Z}$ such that $n_f \pi_f \in T \otimes R_f$ and assume that, in case $p | D$, $p = \mathfrak{p}^2$ with $\chi(\mathfrak{p}) = 1$. Then,

$$[\xi_f^T, n_f \pi_f(\xi_f^T)] = \phi_f(T)^2 \cdot W_{d,n}^K \frac{L(f/K, \chi, 1)}{(f, f)} \sqrt{\Delta} \cdot (u/2) \cdot n_f \pmod{R_f[\chi]},$$

where $(d, n) = (D/p, N)$ if $p | D$ or $(D, N/p)$ if $p | N$.

**Proof.** Since $T \in T_0$, $e_\chi(T(P))$ has degree 0 and we can apply the results of the previous section. Assume $p \nmid \Delta$. Then the specialization of $e_\chi(T(P))$ at $p$ is a divisor whose support is a set of singular Heegner points. The condition $\chi(\mathfrak{p}) = 1$ implies that $e_\chi(P) = \chi(\mathfrak{p})e_\chi(P) = \sum_{g \in \text{Pic}(R)} \chi([\mathfrak{p}]^{-1} g)^{-1} P_{g,R}(g) = \sum_{g \in \text{Pic}(R)} \chi(g)^{-1}(P_{g,R}(\mathfrak{p}))^{\Phi_R(g)} = \omega_p(e_\chi(P))$,

Since $\omega_p(P) = P_{g,R}(\mathfrak{p})$. Thus $\varepsilon_s(\varepsilon_\chi(T(P))) \in M^0_s$. Therefore,

$$[\xi_f^T, n_f \pi_f(\xi_f^T)] = n_f[\lambda(\varepsilon_s(e_\chi(T(\tilde{P})))), \pi_f\lambda(\varepsilon_s(e_\chi(T(\tilde{P}))))] \quad \text{by (5.3.11)}$$

$$= n_f \frac{\phi_f(T)^2}{2} \lambda(\varepsilon_s(e_\chi(\tilde{P}))), \pi_f\lambda(\varepsilon_s(e_\chi(\tilde{P})))) \quad \text{by Hecke equivariance}$$

$$\equiv n_f \frac{\phi_f(T)^2}{2} \lambda(\varepsilon_s(e_\chi(\tilde{P}))), \pi_f\lambda(\varepsilon_s(e_\chi(\tilde{P})))) \quad \text{by (5.3.12)}$$

$$= n_f \frac{\phi_f(T)^2}{2} \langle \pi(\varepsilon_s(e_\chi(\varphi(P)))), \pi_f(\varepsilon_s(e_\chi(\varphi(P)))) \rangle \quad \text{by (3.3.16) and (3.5.22)}$$

$$= n_f \frac{\phi_f(T)^2}{2} \cdot W_{d,n}^K \frac{L(f/K, \chi, 1)}{(f, f)} \sqrt{\Delta} \cdot (u/2) \quad \text{by (5.1.1)},$$

where $(d, n) = (D/p, N/p)$ if $p | D$ or $(D, N/p)$ if $p | N$ and the last step follows from the fact that $\pi_f\nu = \langle v_f, \nu \rangle v_f = c_f v_f$, hence, $\langle \nu, \pi_f\nu \rangle = c_f \langle \nu, v_f \rangle = c_f^2$, with the notation of §5.1.1. Finally, since $p \mid \Delta$, $W_{d,n}^K/2 = W_{d,n}^K$ and the result follows.

\[\square\]
5.3.4 The conjecture of Birch and Swinnerton-Dyer for analytic rank 0

In this section we explain how our computation of the image of a Heegner point of non-singular specialization in the group of connected components of the Jacobian of a Shimura curve can be exploited in order to deal with the Birch Swinnerton-Dyer conjecture in the case of analytic rank 0. We follow the exposition by Longo and Vigni in [50], giving an alternative proof of [50, Theorem 7.3] by replacing their results on Čerednik-Drinfeld’s p-adic uniformization with our results on the specialization of Heegner points.

Let \( E/\mathbb{Q} \) be an elliptic curve of square free conductor \( M \) without complex multiplication associated to the normalized newform \( f \in S_2(\Gamma_0(M))^{\text{new}} \). Let \( K \) be an imaginary quadratic field of discriminant \( \Delta \) prime to \( M \). The extension \( K/\mathbb{Q} \) determines a factorization \( M = D \cdot N \) where a prime \( p \) divides \( D \) (respectively, \( N \)) if and only if it is inert in \( K \) (respectively, splits). Assume that the number of primes dividing \( D \) is odd, which amounts to saying that the sign of the functional equation of \( L(E/K,\chi,s) \) is \(+1\).

Let \( R \) be an order in \( K \) of conductor \( c \) prime to \( M \). Write \( H_R \) for the ring class field of \( R \) and let \( h(R) \) denote its ring class number. Let \( \chi \) be a primitive character of \( \text{Gal}(H_R/K) \cong \text{Pic}(R) \) and assume that the twisted L-function \( L(f/K,\chi,s) \) does not vanish at \( s = 1 \). This makes sense because, since \( \chi \) is unramified at the primes dividing the conductor of \( E \), the sign of the functional equation of \( L(f/K,\chi,s) \) continues to be \(+1\).

The algebraic part of \( L(f/K,\chi,1) \) is the algebraic integer

\[
L(f,\chi) = \frac{L(f/K,\chi,1)}{(f,f)}\sqrt{\Delta} \cdot (u/2) \in \mathbb{Z}[\chi].
\]

Throughout the rest of this section we fix a prime \( p \) satisfying the following properties:

(i) \( p \geq 5 \) and \( p \nmid cMh(R) \).

(ii) The Galois representation \( \rho_{E,p} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(E[p]) \) is surjective.

(iii) \( p \) does not divide the minimal degree of the modular parametrization \( \varphi : X_0(M) \rightarrow E \).

(iv) The image of the algebraic part \( L(f,\chi) \) in the quotient \( \mathbb{Z}[\chi]/p\mathbb{Z}[\chi] \) is not zero.

(v) If \( q \) is a prime of \( H_R \) dividing \( N \) and \( H_{R,q} \) is the completion of \( H_R \) at \( q \) then \( p \) does not divide the order of the torsion subgroup of \( E(H_{R,q}) \).

Our hypothesis on \( E \) ensure that these restrictions on \( p \) exclude only a finite set of primes. One says that a prime number \( \ell \) is admissible relative to \( f \) and \( p \) (or simply admissible) if it satisfies the following conditions:

1. \( \ell \) does not divide \( cpM \);
2. \( \ell \) is inert in \( K \);
3. \( p \) does not divide \( \ell^2 - 1 \);
4. \( p \) divides \((\ell + 1)^2 - a_f^2\).

Čebotarev’s density theorem and the surjectivity of \( \rho_{E,p} \) can be used to prove that there exist infinitely many admissible primes \( \ell \).
Since $D$ is an odd product of primes, we can consider the Shimura curve $X_0(D\ell, N)$. Denote by $J_0(D\ell, N)$ the Néron model of the Jacobian variety $J_0(D\ell, N)$ of $X_0(D\ell, N)$ and write $\Phi_\ell$ for its group of connected components. Write $T(M)$ (respectively, $T(M\ell)$) for the Hecke algebra acting on $S_2(\Gamma_0(M))$ (respectively, $S_2(\Gamma_0(M\ell))$). Write, in turn, $T_{\text{new}}(M\ell)$ (respectively, $T_{\text{new}}(M\ell)$) for the quotient of $T(M\ell)$ (respectively, $T(M\ell)$) acting faithfully on the space of cusp forms which are new at $D$ (respectively, at $D\ell$). In the following, the Hecke operators in $T(N\ell)$ (respectively, $T(\ell)$) will be denoted $T_q$ (respectively, $t_q$) for primes $q \nmid \ell$ (respectively, $q \mid \ell$) and $U_q$ (respectively, $u_q$) for primes $q \mid M$ (respectively, $q \mid \ell$) and $U_q$ (respectively, $u_q$) for primes $q \mid M$ (respectively, $q \mid \ell$). Write

$$\phi_f : T(M) \rightarrow \mathbb{Z}, \quad \phi_f : T_{\text{new}}(M\ell) \rightarrow \mathbb{Z}$$

for the natural morphisms attached to $f$. By composing $\phi_f$ with the projection onto $\mathbb{Z}/p\mathbb{Z}$ we obtain surjections

$$\tilde{\phi}_f : T(M) \rightarrow \mathbb{Z}/p\mathbb{Z}, \quad \tilde{\phi}_f : T_{\text{new}}(M\ell) \rightarrow \mathbb{Z}/p\mathbb{Z}$$

Under the above assumptions on $p$ and $\ell$, a Ribet’s level raising argument as in [8, Theorem 5.15] and [62, Theorem 7.3] shows that there exists a surjective homomorphism

$$\phi^\ell_f : T_{\text{new}}(M\ell) \rightarrow \mathbb{Z}/p\mathbb{Z}$$

such that

1. $\phi^\ell_f(t_q) = \tilde{\phi}_f(T_q)$ for all primes $q \nmid \ell$;
2. $\phi^\ell_f(u_q) = \tilde{\phi}_f(U_q)$ for all primes $q \mid \ell$;
3. $\phi^\ell_f(u_\ell) = \epsilon (\text{mod } p)$ where $p$ divides $\ell + 1 - \epsilon \phi_f(T_\ell)$.

Let $m_f \subset T_{\text{new}}(M\ell)$ be the kernel of $\phi^\ell_f$.

**Proposition 5.3.3.** [8, Theorem 5.15, Theorem 5.17][62, Theorem 7.3] Under our assumptions on $p$ and $\ell$, there is a group isomorphism

$$\Phi_\ell/m_f \simeq \mathbb{Z}/p\mathbb{Z} \quad (5.3.13)$$

and there is a Gal($\mathbb{Q}/\mathbb{Q}$)-module isomorphism

$$T_{a_p}(J_0(D\ell, N))/m_f \simeq E[p], \quad (5.3.14)$$

where $T_{a_p}(J_0(D\ell, N))$ stands for the Tate module of $J_0(D\ell, N)$ at $p$.

Since $\ell$ is inert in $K$ and does not divide $c$, the set $\text{CM}(R) \subset X_0(D\ell, N)$ is not empty. Let $P \in \text{CM}(R)$ be a fixed Heegner point. Write

$$D_P^\chi = \sum_{\sigma \in \text{Gal}(H_R/K)} \chi(\sigma)^{-1} P^\sigma,$$

and $\eta_q = T_q-(q+1) \in T(M)$, for a suitable $q$ such that $a_q \neq q+1 \text{ (mod } p)$ (again, Čebotarev’s density theorem and the surjectivity of $\rho_{E,p}$ imply that there exist infinitely many such primes). Since $\eta_q$ has degree $0$, $\eta_q(D_P^\chi)$ has also degree $0$, hence we can consider its image $\eta_q(\xi_P^\chi)$ in $\Phi_\ell$.

The following theorem is completely analogous to [50, Theorem 7.3]. Here we present an alternative proof which exploits our results on the specialization of smooth divisors. As a piece of notation, for any ring $A$ and any $a, b \in A$ let $a \doteq b$ mean that there exists $c \in A^\times$ such that $a = b \cdot c$. 
Theorem 5.3.4. Write $\pi_1 : \mathbb{Z}[\chi] \to \mathbb{Z}[\chi]/p\mathbb{Z}[\chi]$ and $\pi_2 : \mathbb{Z}[\chi] \otimes \Phi_\ell \to \mathbb{Z}[\chi] \otimes \Phi_\ell/m_f$ for the natural projections. Then, upon the identification $\mathbb{Z}[\chi] \otimes \Phi_\ell/m_f \simeq \mathbb{Z}[\chi]/p\mathbb{Z}[\chi]$ of (5.3.13),

$$\pi_2(\eta_q(\xi_h^\lambda)) = \pi_1(\sqrt{\mathcal{L}(f, \chi)}).$$  \hfill (5.3.15)

Proof. Recall the map $\lambda : \mathbb{Z}_C^\ast \to \Phi_\ell$ introduced in (5.3.3). Upon the isomorphism $\mathbb{Z}_C^\ast \simeq \mathbb{M} \oplus \mathbb{M}$, where $\mathbb{M} = \mathbb{Z}\text{Pic}(D, N)$, we deduced in §5.3.2 that

$$\eta_q(\xi_h^\lambda) = \lambda \left( \eta_q \left( \sum_{g \in \text{Pic}(R)} \chi(g)^{-1}\pi(\phi_c(g^{-1} \ast \varphi(P))) \right) \right)$$

$$= \lambda \left( \eta_q \left( \sum_{g \in \text{Pic}(R)} \chi(g)^{-1}\pi(g \ast \phi_c(\varphi(P))) \right) \right), \quad \text{by Theorem 3.3.7.}$$  \hfill (5.3.16)

Write $\xi_h^\lambda = \sum_{g \in \text{Pic}(R)} \chi(g)^{-1}\pi(\phi_c(\varphi(P))) \in \mathbb{M} \subset \mathbb{M} \oplus \mathbb{M}$. Let $v_f$ denote the unique element of $\mathbb{M}$ such that $\langle v_f, v_f \rangle = 1$ and $T(v_f) = \phi_f(T)v_f$ for all $T \in T(M)$.

Let $\Pi_f : \mathbb{M} \to \mathbb{M}/\ker(\phi_f)\mathbb{M}$ denote the natural projection. We have $\Pi_f(c_fv_f) = c_f$ and $\mathbb{M}/\ker(\phi_f)\mathbb{M} \simeq \mathbb{Z}$ by the Eichler’s basis problem [24]. By Gross’s formula (5.1.1), $\Pi_f(\xi_h^\lambda) = c_f(\xi_h^\lambda) = \sqrt{\mathcal{L}(f, \chi)}$.

Besides, since $\phi_f$ restricted to $\mathbb{T}_{\text{new}}/(T_\ell)$ coincides with $\phi_f^\ell$ restricted to $\mathbb{T}_{\ell}^\text{new}/(u_\ell)$, we have the following commutative diagram

$$
\begin{array}{ccc}
\mathbb{M} & \xrightarrow{\lambda} & \Phi_\ell \\
\pi_f \downarrow & & \downarrow \pi_2 \\
\mathbb{Z} & \xrightarrow{\Phi_\ell/m_f} & \mathbb{Z}/p\mathbb{Z}
\end{array}
$$  \hfill (5.3.18)

where the bottom row stands for the natural projection. Notice that $\eta_q$ provides a natural map $\mathbb{M} \overset{\eta_q}{\longrightarrow} \mathbb{M}[+]$. Since $a_q \neq q + 1 \pmod{p}$, for all $\xi \in \mathbb{M}$ there exists $c^* \in (\mathbb{Z}/p\mathbb{Z})^\ast$ such that $\pi_2(\lambda(\eta_q(\xi))) = c^* \cdot \pi_f(\xi) \pmod{p}$. Thus

$$\pi_2(\eta_q(\xi_h^\lambda)) = \pi_2(\lambda(\eta_q(\xi_h^\lambda))) = \pi_1(\pi_f(\xi_h^\lambda)) = \pi_1(\sqrt{\mathcal{L}(f, \chi)}).$$

The above theorem provides a crucial step in the proof of the main result of [50], which we present below (see [49, Lemma 8.14] for a reformulation of such theorem in the real quadratic setting).

Theorem 5.3.5. [50, Theorem 1.2] If $L(f/K, \chi, 1) \neq 0$ then

$$\text{Sel}_p(E/H_R)^\chi = \{ x \in \text{Sel}_p(E/H_R) \otimes \mathbb{F}_p : \sigma(x) = \chi(\sigma)x, \text{ for all } \sigma \in \text{Gal}(H_R/K) \} = 0$$

and $\text{Sel}_p^H(E/H_R) = 0$, for all but finitely many primes $p$.

As a sketch of the proof, let us remark that, by (5.3.14), the divisor $D_\ell^\chi$ provides a class $s_\ell^\chi \in H^1(H_R, E[p])$ by means of the composition of the maps

$$J(D_\ell, N)(H_R) \to H^1(H_R, \text{Ta}_p(J_0(D_\ell, N))) \to H^1(H_R, \text{Ta}_p(J_0(D_\ell, N))/m_f) \simeq H^1(H_R, E[p]).$$
where $\kappa$ is the Kummer map. The assumption $L(f/K, \chi, 1) \neq 0$ implies $L(f, \chi) \neq 0$ and consequently the image of $D^\chi_P$ in $\Phi_\ell$ is non-zero. Longo and Vigni prove that this fact implies that the restriction $\text{res}_\ell(s^\chi_P) \in H^1_{\text{sing}}(H_{R, \ell}, E[p])$ is non-zero. Letting $\ell$ run over the set of all admissible primes relative to $f$ and $p$, they obtain by global Tate duality that $\text{Sel}_p(E/H_R)^{\chi}$ must be zero.

As a direct consequence of the theorem above, we obtain a new proof of the following particular case of the conjecture of Birch and Swinnerton-Dyer.

Theorem 5.3.6. [50, Theorem 1.3] If $L(f/K, \chi, 1) \neq 0$ then

$$E(H_R)^{\chi} = \{ P \in E(H_R) \otimes \mathbb{C} : P^\sigma = \chi(\sigma)P, \text{ for all } \sigma \in \text{Gal}(H_R/K) \} = 0.$$
Appendix: Moduli interpretations of Shimura curves

In this appendix, we describe an interpretation of the moduli problem solved by the Shimura curve $X_0(D,N)$, which slightly differs from the one already considered in Chapter 1. This moduli interpretation is also well-known to the experts, but we provide here some details because of the lack of suitable reference.

Let \( \{O_N\}_{(N,D)=1} \) be a system of Eichler orders in \( B \) such that each \( O_N \) has level \( N \) and \( O_N \subseteq O_M \) for \( M \mid N \). Let now \( M \mid N \), by what we mean a divisor \( M \) of \( N \) such that \( (M, N/M) = 1 \). Since \( O_N \subseteq O_M \), there is a natural map \( \delta : X_0(D,N) \rightarrow X_0(D,M) \); composing with the Atkin-Lehner involution \( \omega_{N/M} \), we obtain a second map \( \delta \circ \omega_{N/M} : X_0(D,N) \rightarrow X_0(D,M) \) and the product of both yields an embedding \( j : X_0(D,N) \hookrightarrow X_0(D,M) \times X_0(D,M) \) (cf. [35] for more details).

Note that the image by \( j \) of an abelian surface \((A,i)\) over a field \( K \) with QM by \( O_N \) is a pair \(((A_0,i_0)/K,(A'_0,i'_0)/K)\) of abelian surfaces with QM by \( O_M \), related by an isogeny \( \phi_{N/M} : (A_0,i_0) \rightarrow (A'_0,i'_0) \) of degree \((N/M)^2\), compatible with the multiplication by \( O_M \). Assume that either \( \text{char}(K) = 0 \) or \( (N, \text{char}(K)) = 1 \), thus giving a pair \(((A_0,i_0),(A'_0,i'_0))\) is equivalent to giving the triple \((A_0,i_0,C_{N/M})\), where \( C_{N/M} = \ker(\phi_{N/M}) \) is a subgroup scheme of \( A_0 \) of rank \((N/M)^2\), stable by the action of \( O_M \) and cyclic as an \( O_M \)-module. The group \( C_{N/M} \) is what we call a \( \Gamma_0(N/M) \)-structure.

Let us explain now how to recover the pair \((A,i)\) from a triple \((A_0,i_0,C_{N/M})\) as above. Along the way, we shall also relate the endomorphism algebra \( \text{End}(A_0,i_0,C_{N/M}) \) of the triple to the endomorphism algebra \( \text{End}(A,i) \). The construction of the abelian surface \((A,i)\) will be such that the triple \((A_0,i_0,C_{N/M})\) is the image of \((A,i)\) by the map \( j \). This will establish an equivalence of the moduli functors under consideration, and will allow us to regard points on the Shimura curve \( X_0(D,N) \) either as isomorphism classes of abelian surfaces \((A,i)\) with QM by \( O_N \) or as isomorphism classes of triples \((A_0,i_0,C_{N/M})\) with QM by \( O_M \) and a \( \Gamma_0(N/M) \)-structure, for any \( M \mid N \).

Since \( C_{N/M} \) is cyclic as a \( O_M \)-module, \( C_{N/M} = O_M P \) for some point \( P \in A_0 \). We define

\[
\text{Ann}(P) = \{ \beta \in O_M, \text{ s.t. } \beta P = 0 \}.
\]

It is clear that \( \text{Ann}(P) \) is a left ideal of \( O_M \) of norm \( N/M \), since \( C_{N/M} \cong O_M/\text{Ann}(P) \). Let \( \alpha \) be its generator. Assume \( C = C_{N/M} \cap \ker(i_0(\alpha)) \) and let \( A := A_0/C \) be the quotient abelian surface, related with \( A_0 \) by the isogeny \( \varphi : A_0 \rightarrow A \).

We identify

\[
C = \{ \beta P, \text{ s.t. } \beta \in O_M, \alpha \beta \in \text{Ann}(P) = O_M \alpha \} = \{ \beta P, \text{ s.t. } \beta \in \alpha^{-1} O_M \alpha \cap O_M \}.
\]

97
The order \( \alpha^{-1}\mathcal{O}_M \cap \mathcal{O}_M \) is an Eichler order of discriminant \( N \), hence \( C = \{ \beta P, \text{s.t. } \beta \in \mathcal{O}_N \} \).

Since \( \mathcal{O}_N = \{ \beta \in \mathcal{O}_M, \text{s.t. } \beta C \subseteq C \} \subseteq \mathcal{O}_M \), the embedding \( i_0 \) induces a monomorphism \( i : \mathcal{O}_N \hookrightarrow \text{End}(A) \) such that \( i(B) \cap \text{End}(A) = i(\mathcal{O}_N) \). Then we conclude that \( (A, i) \) has QM by \( \mathcal{O}_N \). Recovering the moduli interpretation of \( X_0(D, N) \), it can be checked that \( \delta(A, i) = (A_0, i_0) \).

Let \( \text{End}(A_0, i_0, C_{N/M}) \) be the subalgebra of endomorphisms \( \psi \in \text{End}(A_0, i_0) \), such that \( \psi(C_{N/M}) \subseteq C_{N/M} \). Identifying \( \text{End}(A_0, i_0') \) inside \( \text{End}^0(A_0, i_0) \) via \( \phi_{N/M} \), we obtain that \( \text{End}(A_0, i_0, C_{N/M}) = \text{End}(A_0, i_0) \cap \text{End}(A_0', i_0') \). Let \( \psi \in \text{End}(A_0, i_0, C_{N/M}) \). Since \( \psi \) commutes with \( i_0(\alpha) \), we have that \( \psi(\ker(i_0(\alpha))) \subseteq \ker(i_0(\alpha)) \). Moreover it fixes \( C_{N/M} \) by definition, hence \( \psi(C) \subseteq C \) and therefore each element of \( \text{End}(A_0, i_0, C_{N/M}) \) induces an endomorphism of \( \text{End}(A, i) \). We have obtained a monomorphism \( \text{End}(A_0, i_0, C_{N/M}) \hookrightarrow \text{End}(A, i) \).

**Proposition 5.3.7.** Let \( (A, i) \) obtained from \( (A_0, i_0, C_{M/N}) \) by the above construction. Then \( \text{End}(A, i) \simeq \text{End}(A_0, i_0, C_{N/M}) \).

**Proof.** We have proved that \( \text{End}(A_0, i_0, C_{N/M}) \hookrightarrow \text{End}(A, i) \), if we check that \( \text{End}(A, i) \hookrightarrow \text{End}(A_0, i_0) \) and \( \text{End}(A, i) \hookrightarrow \text{End}(A', i_0') \), we will obtain the equality, since \( \text{End}(A_0, i_0, C_{N/M}) = \text{End}(A_0, i_0) \cap \text{End}(A_0', i_0') \).

Due to the fact that \( C \subseteq C_{N/M} \), the isogeny \( \phi_{N/M} \) factors through \( \varphi \). By the same reason \( i_0(\alpha) \) also factors through \( \varphi \), and we have the following commutative diagram:

\[
\begin{array}{ccc}
A_0 & \xrightarrow{i_0(\alpha)} & A_0 \\
\downarrow{\phi_{N/M}} & & \downarrow{\varphi} \\
A_0 & \xrightarrow{i(\alpha)} & A \\
\downarrow{\rho} & & \downarrow{\varphi} \\
A_0 & \xrightarrow{i(\alpha)} & A
\end{array}
\]

We can suppose that \( \alpha \) is a generator of the two-sided ideal of \( \mathcal{O}_N \) of norm \( N/M \). It can be done since \( \mathcal{O}_N = \mathcal{O}_M \cap \alpha^{-1}\mathcal{O}_M \alpha \), thus \( \alpha \) can differ from the generator of such ideal by an unit of \( \mathcal{O}_M^\times \), namely an isomorphism in \( \text{End}_C(A_0) \).

The orientation \( \mathcal{O}_N \subseteq \mathcal{O}_M \) induces an homomorphism, \( \mu : \mathcal{O}_N \to \mathcal{O}_N / \mathcal{O}_M \alpha \cong \mathbb{Z} / \frac{N}{M} \mathbb{Z} \). We consider the subgroup scheme

\[ C_1 = \{ P \in \ker(i(\alpha)) \text{ s.t. } i(\beta)P = \mu(\beta)P, \text{ for all } \beta \in \mathcal{O}_N \} \].

**Claim:** \( C_1 = \ker(\eta) \). Clearly \( \ker(\eta) \subseteq \ker(i(\alpha)) \). Moreover \( \ker(\eta) = \varphi(\ker(i_0(\alpha))) \) are those points in \( \ker(i(\alpha)) \) annihilated by \( i(\mathcal{O}_M \alpha) \), thus they correspond to the eigenvectors with eigenvalues \( \mu(\beta) \), for all \( \beta \in \mathcal{O}_N \).

We also have the homomorphism, \( \mu \circ \omega_{N/M} : \mathcal{O}_N \to \mathcal{O}_N / \alpha \mathcal{O}_M \cong \mathbb{Z} / \frac{N}{M} \mathbb{Z} \). Again, we consider the subgroup scheme

\[ C_2 = \{ P \in \ker(i(\alpha)) \text{ s.t. } i(\beta)P = \mu \circ \omega_{N/M}(\beta)P, \text{ for all } \beta \in \mathcal{O}_N \} \].

**Claim:** \( C_2 = \ker(\rho) \). In this case, we have that \( \ker(\rho) = \varphi(C_{N/M}) \), where \( C_{N/M} = \mathcal{O}_M P \). Due to the fact that \( \alpha \mathcal{O}_M \subseteq \mathcal{O}_N \) and \( \ker(\varphi) = \mathcal{O}_NP \), we obtain that \( \ker(\rho) \subseteq \ker(i(\alpha)) \). By the same reason, \( \ker(\rho) \) is the subgroup of \( \ker(i(\alpha)) \) annihilated by \( i(\alpha \mathcal{O}_M) \), therefore \( \ker(\rho) = C_2 \) as stated.

Finally let \( \gamma \in \text{End}(A, i) \). Since it commutes with \( i(\beta) \) for all \( \beta \in \mathcal{O}_N \), it is clear that \( \gamma(C_2) \subseteq C_2 \). Then the isogeny \( \rho \) induces an embedding \( \text{End}(A, i) \subseteq \text{End}(A_0, i_0') \). Furthermore
we have that $i_0(\alpha)i_0(\pi) = N/M$, then $\hat{\phi} = \eta \circ i_0(\pi) = i(\alpha) \circ \eta$. Since $\gamma$ commutes with $i(\pi)$ and $\gamma(C_1) \subseteq C_1$, we obtain that $\hat{\phi}$ induces an embedding $\text{End}(A, i) \subseteq \text{End}(A_0, i_0)$. We conclude that $\text{End}(A, i) = \text{End}(A_0, i_0) \cap \text{End}(A'_0, i'_0) = \text{End}(A_0, i_0, C_{N/M})$.  
\qed
Bibliography


[34] A. Grothendieck. *Groupes de monodromie en geometrie algébrique. SGA 7 I*. Exposé IX.


