Twists of Shimura Curves

by

James Henry Stankewicz

(Under the direction of Peter Louis Clark and Dino Jacques Lorenzini)

Abstract

In this thesis we determine conditions for local points on the twist of the Shimura curve $X_0^D(N)_{/\mathbf{Q}}$ by an Atkin-Lehner involution w_m and a quadratic extension of $\mathbf{Q}$. These conditions are complete and exhaustive, except for the case of $\mathbf{Q}_p$-points when $p \mid 2DN$ is ramified in the quadratic field extension.

Index words: Shimura curves, Modular curves, Rational points on varieties, Quaternion algebras, Elliptic Curves, Complex multiplication

Twists of Shimura Curves

by

James Henry Stankewicz

B.A., University of Connecticut, 2005

M.S., University of Connecticut, 2007

A Dissertation Submitted to the Graduate Faculty

of The University of Georgia in Partial Fulfillment

of the

Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2012

Twists of Shimura Curves

by

James Henry Stankewicz

Approved:

Major Professors: Peter Clark
Dino Lorenzini

Committee: Daniel Krashen
Robert Rumely

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
June 2012

Twists of Shimura Curves

James Henry Stankewicz

April 25, 2012

Contents

Chapter 1

Introduction

Given $a, b \in \mathbf{Q}^\times$, define the *quaternion algebra* $\left(\frac{a,b}{\mathbf{Q}}\right)$ to be the set of all $x + yi + zj + wk$ with $x, y, z, w \in \mathbf{Q}$ such that $i^2 = a, j^2 = b$, and $ij = -ji = k$.

It can be shown that if B is a quaternion algebra, then for all but finitely many primes p, $B \otimes_{\mathbf{Q}} \mathbf{Q}_p \cong M_2(\mathbf{Q}_p)$. Call the product of these finitely many primes D. If $D = 1$, then $B \cong M_2(\mathbf{Q})$ and D is the product of an even number of primes if and only if there exists an embedding $\psi : B \hookrightarrow M_2(\mathbf{R})$. For special $\mathbf{Z}$-sublattices $\mathcal{O}$ of B called *Eichler orders*, we may form the *Shimura curve* $\psi(\mathcal{O}^1)\backslash\mathcal{H}^*$ where $\mathcal{O}^1$ is the inverse image of $\mathrm{SL}_2(\mathbf{R})$ under ψ in $\mathcal{O}$ and $\mathcal{H}^*$ is either the upper half-plane $\mathcal{H}$ of complex analysis if $D \neq 1$ or $\mathcal{H} \cup \mathbb{P}^1(\mathbf{Q}) \subset \mathbb{P}^1(\mathbf{C})$ if $D = 1$.

Given any integer $N \geq 1$ which we call the *level*, consider the following example. In the quaternion algebra $\left(\frac{1,1}{\mathbf{Q}}\right) \cong M_2(\mathbf{Q})$ we have the Eichler order

$$\mathcal{O}_0(N) = \left\{ \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} : a, b, c, d \in \mathbf{Z} \right\}.$$

The Shimura curve $\mathcal{O}_0(N)^1\backslash\mathcal{H}^*$ is the classical modular curve $X_0(N)_{\mathbf{C}}$, the geometric object which gives rise to modular forms. We may generalize this construction from $M_2(\mathbf{Q})$

to an arbitrary quaternion algebra in $M_2(\mathbf{R})$ of discriminant D. Work of Shimura [Shi71] shows that this $X_0^D(N)_{\mathbf{C}}$ may be given the structure of a variety over $\mathbf{Q}$. Shimura also showed that $X_0^D(N)_{\mathbf{Q}}(\mathbf{Q})$ is non-empty if and only if $D = 1$, i.e., $X_0^D(N) = X_0(N)$.

While there is a sense in which the variety $X_0^D(N)$ is canonical, it is not unique. We understand the non-uniqueness using the following language.

Definition 1.0.1. *By a* twist *of a variety $V_{/\mathbf{Q}}$, we will mean a variety $V'_{/\mathbf{Q}}$ which is isomorphic to V over an extension field K. If $[K : \mathbf{Q}] = 2$ and ω is an automorphism of $V_{/\mathbf{Q}}$, we may uniquely define the* twist of V by ω and K. *[Cla07]*

The curve $X_0^D(N)_{/\mathbf{Q}}$ comes naturally equipped with a group $W = \{w_m : m|DN\}$ of $\mathbf{Q}$-rational automorphisms such that $w_m^2 = 1$ called the *Atkin-Lehner group.* As an example, if $D = 1$, then the action of the Fricke involution w_N is usually given as the action on $\mathcal{H}$ by the map $z \mapsto \frac{-1}{Nz}$. We use the phrase *Atkin-Lehner Twist* to denote a twist of $X_0^D(N)_{/\mathbf{Q}}$ by an Atkin-Lehner involution and a quadratic field K which we fix for the remainder of the introduction. Conjecturally [KR08], for all but finitely many D and N, $W = \mathrm{Aut}_{\mathbf{C}}(X_0^D(N)_{\mathbf{C}})$ and thus any quadratic twist is an Atkin-Lehner twist.

This thesis is concerned with determining the rational points of Atkin-Lehner twists of Shimura curves. To someone familiar with the theory of elliptic curves, it may be strange to talk at such length about the presence or absence of rational points on quadratic twists. The reader should however be cautioned that even genus one curves may possess involutions ω where it may be difficult to determine if a twist by ω has rational points as in the following example.

Example 1.0.2. *It can be shown [GR06] that if $D = 14$ and $N = 1$ then $X_0^D(N)_{\mathbf{Q}}$ can be given by the affine equation*

$$y^2 = -x^4 + 13x^2 - 128.$$

Moreover the action of w_{14} is $(x, y) \mapsto (x, -y)$, and so the twist by w_{14} and $\mathbf{Q}(\sqrt{d})$ has *rational points if d is a value of $-x^4 + 13x^2 - 128 \in \mathbf{Z}[x]$. However, the action of w_2 is $(x, y) \mapsto (-x, y)$ and therefore the twist of $X_0^D(N)$ by w_2 and $\mathbf{Q}(\sqrt{d})$ is given by*

$$y^2 = -d^2x^4 + 13dx^2 - 128.$$

It is a difficult question to determine for which d this twist has rational points.

Note that in the case $D = 14$ and $N = 1$ we have an explicit equation for $X_0^D(N)$ because it is hyperelliptic. It turns out that unless $D = 1$ or $X_0^D(N)$ is hyperelliptic, there are no known or conjectured equations for $X_0^D(N)$ [Mol10, p.4]. Therefore we need to use different techniques.

In chapter 4, we begin by exploring some basics of quaternion arithmetic needed for a systematic study of Shimura curves. The topics include orders, ideals, ideal classes, embeddings of quadratic orders and others. Towards the end we will introduce some novel theorems on the simultaneous embeddings of imaginary quadratic orders into Eichler orders in definite quaternion algebras.

In chapter 5, we give the definition of a Shimura curve as a coarse moduli scheme. To do so, we will review some background on abelian schemes, especially abelian schemes with "large" endomorphism algebras. After giving a proper definition of a Shimura curve, we will describe certain well-known models of Shimura curves. Finally, we will study the direct relation yielded by Ribet's bimodules between the arithmetic of certain abelian schemes and the arithmetic of quaternion algebras.

Chapter 6 is where we first study rational points on twists of Shimura curves. That is, if p is a prime not dividing DN which is unramified in a quadratic field K, we determine when $X_0^D(N)(\mathbf{Q}_p)$ is nonempty. The relevant techniques used here are Shimura's zeta function, Eichler's trace formula, and Ribet's bimodules.

In chapter 7, we study p-adic points on Atkin Lehner twists when p is ramified in K.

As a $\mathbf{Z}_p$-regular model for these twists was not previously known, we construct one in this chapter. We then determine the $\mathbb{F}_p$-rational points using either the Serre-Tate canonical lift of an ordinary abelian variety or the theorems of chapter 4 on simultaneous embeddings. We then apply Hensel's Lemma to obtain our results. If we combine these results with the results of Ekin Ozman [Ozm09], we obtain congruence conditions for the splitting modulo p of Hilbert Class Polynomials.

In chapter 8, we study p-adic points on Atkin Lehner twists when $p|N$ is unramified in K. We also obtain criteria for p-adic points on $X_0^D(N)$ when $p|N$, and no criteria seemed to be known beforehand. The relevant techniques here are Ribet's bimodules and the theorems on simultaneous embeddings in chapter 4.

In chapter 9, we study p-adic points on Atkin Lehner twists when $p|D$ is unramified in K. We also give a new proof of the criteria for p-adic points on $X_0^D(N)$ when $p|D$, as determined by Jordan-Livné [JL85] and Ogg [Ogg85]. The relevant techniques here are once again Ribet's bimodules and the theorems on simultaneous embeddings in chapter 4.

The theorems of these chapters comprehensively determine the local behavior of these twisted Shimura curves and are thus too long to state in an introduction. We now provide explicit examples of families of Shimura curves which have local points everywhere to illustrate this.

Example (9.2.4)**.** *Suppose that q is an odd prime and consider $X_0^{2q}(1)_{/\mathbf{Q}}$, a curve of genus g. Note that this curve is hyperelliptic over $\mathbf{Q}$ if and only if q is one of the following primes $\{13, 19, 29, 31, 37, 43, 47, 67, 73, 97, 103\}$ [Ogg83, Theorem 7]. Let $p \equiv 3 \bmod 8$ be a prime such that $\left(\frac{-p}{q}\right) = -1$ and such that for all odd primes ℓ less than $4g^2$, $\left(\frac{-p}{\ell}\right) = -1$. Let the twist of $X_0^{2q}(1)$ by $\mathbf{Q}(\sqrt{-p})$ and w_{2q} be denoted by $C^{2q}(1, -p, 2q)_{/\mathbf{Q}}$. Then $C^{2q}(1, -p, 2q)$ has $\mathbf{Q}_v$-rational points for all places v of $\mathbf{Q}$.*

If $q = 13$, then the genus of $X_0^{26}(1)$ is two. Therefore $X_0^{26}(1)$ is hyperelliptic, and has the following explicit model, where w_{2q} is identified with the hyperelliptic involution [GR04]:

$$y^2 = -2x^6 + 19x^4 - 24x^2 - 169.$$

Hence, an explicit model for $C^{26}(1, -p, 2q)$ is given by the affine equation

$$y^2 = 2px^6 - 19px^4 + 24px^2 + 169p.$$

The primes less than 2000 satisfying the congruence conditions in the above example are $p = 67, 163$, and 1747. It can be checked that the explicit model of $C^{26}(1, -67, 26)$ has at least the rational points $\left(\frac{\pm 9}{5}, \frac{\pm 10988}{125}\right)$, and that $C^{26}(1, -163, 26)$ has at least the rational points $\left(\frac{\pm 67}{35}, \frac{\pm 5270116}{42875}\right)$. If $p = 1747$, a point search in `sage` [S+12] failed to produce any rational points and the `TwoCoverDescent` command in `MAGMA` did not determine if $C^{26}(1, -1747, 26)$ has no rational points.

Example (8.2.7)**.** *Let $q \equiv 3 \bmod 4$ be a prime and consider the curve $X_0(q)_{/\mathbf{Q}}$. Let $p \equiv 1 \bmod 4$ be a prime such that $\left(\frac{p}{q}\right) = -1$ and let $C^1(q, p, q)_{/\mathbf{Q}}$ denote the twist of $X_0(q)$ by $\mathbf{Q}(\sqrt{p})$ and w_q. Then $C^1(q, p, q)$ has $\mathbf{Q}_v$-rational points for all places v of $\mathbf{Q}$.*

If $q = 23$, the least two primes satisfying the above are $p = 5$ and $p = 13$. Using a hyperelliptic model of the genus 2 curve $X_0(23)$ [GR91] as above, it can be verified that $C^1(23, 5, 23)(\mathbf{Q})$ is nonempty. Meanwhile, the `TwoCoverDescent` command in `MAGMA` determined that $C^1(23, 13, 23)(\mathbf{Q})$ is empty.

Example 1.0.3. *Let $q \equiv 3 \bmod 4$ be a prime. Let p be a prime such that $\left(\frac{p}{q}\right) = -1$ and $p \equiv 1 \bmod 8$. Let $C^1(2q, p, 2q)_{/\mathbf{Q}}$ denote the twist of $X_0^1(2q)_{/\mathbf{Q}}$ by $\mathbf{Q}(\sqrt{p})$ and w_{2q}. Then $C^1(2q, p, 2q)$ has $\mathbf{Q}_v$-rational points for all places v of $\mathbf{Q}$.*

In chapter 10, we intensively explore Example 1.0.3 when $q = 7$. In particular, if we assume a certain well-known conjecture, there are congruence classes of primes p such that the twist of $X_0(14)$ by w_{14} and $\mathbf{Q}(\sqrt{p})$ not only has rational points, but is an elliptic curve of rank one. We complete the chapter by conditionally re-deriving some of Shih's results on the inverse Galois problem. The relevant techniques are the results of the previous chapters and the careful study of Selmer and Shafarevich-Tate groups.

Chapter 2

Statements of Main Theorems

Throughout, D is a squarefree product of an even number of primes, N is a squarefree integer coprime to D, $m|DN$ is a positive integer, and d is a squarefree integer. Moreover, $X_0^D(N)$ is a Shimura curve over $\mathbf{Q}$ and $C^D(N,d,m)$ is its twist by the automorphism w_m and the quadratic field $\mathbf{Q}(\sqrt{d})$.

Corollary (6.3.2)**.** *If $p \nmid DN$ is inert in $\mathbf{Q}(\sqrt{d})$, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty when $m = DN$.*

Theorem (7.0.1)**.** *Suppose that $p \nmid 2DN$ is a prime which is ramified in $\mathbf{Q}(\sqrt{d})$ and $m|DN$. Then $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$ if and only if one of the following occurs.*

1. *$e_{D,N}(-4m) \neq 0$, $\left(\frac{-m}{p}\right) = 1$, and $H_{-4m}(X) = 0$ has a root modulo p*

2. *$m \equiv 3 \bmod 4$, $e_{D,N}(-m) \neq 0$, $\left(\frac{-m}{p}\right) = 1$, and $H_{-m}(X) = 0$ has a root modulo p*

3. *$m = DN$, $2 \nmid D$, $\left(\frac{-DN}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid D$, and $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid N$ such that $q \neq 2$*

4. *$m = DN/2$, $2 \mid N$, $\left(\frac{-DN/2}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid D$, and $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid N$ such that $q \neq 2$*

5. $m = DN$, $2 \mid D$, $p \equiv \pm 3 \bmod 8$, $\left(\frac{-DN}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid (D/2)$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$.

6. $m = DN/2$, $2 \mid D$, $DN \equiv 2, 6,$ *or* $10 \bmod 16$, $p \equiv \pm 3 \bmod 8$, $\left(\frac{-DN/2}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$.

Theorem (8.0.1)**.** *Let* $p \mid N$ *be unramified in* $\mathbf{Q}(\sqrt{d})$ *and* $m \mid DN$. *Then* $C^D(N, d, m)(\mathbf{Q}_p)$ *is nonempty if and only if the conditions of (a) or (b) hold.*

(a) p *is split in* $\mathbf{Q}(\sqrt{d})$ *and one of the following conditions holds.*

- $D = 1$
- $p = 2$, $D = \prod_i p_i$ *with each* $p_i \equiv 3 \bmod 4$, *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 4$
- $p = 3$, $D = \prod_i p_i$ *with each* $p_i \equiv 2 \bmod 3$, *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 3$
- *The following inequality holds*

$$\sum_{0 \neq s = -\lfloor 2\sqrt{p} \rfloor}^{\lfloor 2\sqrt{p} \rfloor} \sum_{f \mid f(s^2-4p)} \frac{e_{D,N/p}\left(\frac{s^2-4p}{f^2}\right)}{w\left(\frac{s^2-4p}{f^2}\right)} > 0$$

(b) p *is inert in* $\mathbf{Q}(\sqrt{d})$, *and there are prime factorizations* $Dp = \prod_i p_i$, $N/p = \prod_j q_j$ *such that one of the following two conditions holds*

(i) $p \mid m$, *and one of the following two conditions holds.*

- $p = 2$, $m = p$ *or* DN, *for all* i, $p_i \equiv 3 \bmod 4$, *and for all* j, $q_j \equiv 1 \bmod 4$
- $p \equiv 3 \bmod 4$, $m = p$ *or* $2p$, *for all* i, $p_i \not\equiv 1 \bmod 4$, *and for all* j, $q_j \not\equiv 3 \bmod 4$

(ii) $p \nmid m$ *and one of the following nine conditions holds.*

- $m = D = 1$
- $p = 2$, $m = 1$, *for all* i, $p_i \equiv 3 \bmod 4$, *and for all* j, $q_j \equiv 1 \bmod 4$

- $p = 3$, $m = 1$, *for all* i, $p_i \equiv 2 \bmod 3$, *and for all* j, $q_j \equiv 1 \bmod 3$
- $p \equiv 3 \bmod 4$, $m = DN/2p$, $p_i \not\equiv 1 \bmod 4$ *for all* i, *and* $q_j \not\equiv 3 \bmod 4$ *for all* j
- $p \equiv 2 \bmod 3$, $m = DN/3p$, $p_i \not\equiv 1 \bmod 3$ *for all* i, *and* $q_j \not\equiv 2 \bmod 3$ *for all* j
- $m = DN/p$, $p_i \not\equiv 1 \bmod 4$ *for all* i, *and* $q_j \not\equiv 3 \bmod 4$ *for all* j
- $m = DN/p$, $p_i \not\equiv 1 \bmod 3$ *for all* i, *and* $q_j \not\equiv 2 \bmod 3$ *for all* j
- $mp \not\equiv 3 \bmod 4$ *and* $(p+1) - \mathrm{tr}(T_{pm}) > \frac{e_{Dp,N/p}(-4mp)}{w(-4mp)}$
- $mp \equiv 3 \bmod 4$ *and* $(p+1) - \mathrm{tr}(T_{pm}) > \frac{e_{Dp,N/p}(-mp)}{w(-mp)} + \frac{e_{D,N/p}(-4mp)}{w(-4mp)}$

Theorem (9.0.1)**.** *Suppose that* $p \mid D$ *is unramified in* $\mathbf{Q}(\sqrt{d})$ *and* $m \mid DN$. *Let* p_i, q_j *be primes such that* $D/p = \prod_i p_i$ *and* $N = \prod_j q_j$.

- *Suppose* p *is split in* $\mathbf{Q}(\sqrt{d})$. *Then* $C^D(N,d,m)(\mathbf{Q}_p)$ *is nonempty if and only if one of the following two cases occurs [Theorem 9.2.2].*

    1. $p = 2$, $p_i \equiv 3 \bmod 4$ *for all* i, *and* $q_j \equiv 1 \bmod 4$ *for all* j
    2. $p \equiv 1 \bmod 4$, $D = 2p$, *and* $N = 1$

- *Suppose that* p *is inert in* $\mathbf{Q}(\sqrt{d})$.

    – *If* $p \mid m$, $C^D(N,d,m)(\mathbf{Q}_p)$ *is nonempty if and only if one of the following four cases occurs.*

        1. $m = p$, $p_i \not\equiv 1 \bmod 3$ *for all* i, *and* $q_j \not\equiv 2 \bmod 3$ *for all* j *[Lemma 9.1.3]*
        2. $m = 2p$ *and one of* $e_{D/p,N}(-4)$ *or* $e_{D/p,N}(-8)$ *is nonzero [Lemma 9.1.4]*
        3. $m/p \not\equiv 3 \bmod 4$ *and* $e_{D/p,N}(-4m/p)$ *is nonzero [Lemma 9.1.4]*
        4. $m/p \equiv 3 \bmod 4$ *and one of* $e_{D/p,N}(-4m/p)$ *or* $e_{D/p,N}(-m/p)$ *is nonzero [Lemma 9.1.4]*

– *If $p \nmid m$, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if one of the following four cases occurs [Theorem 9.2.2].*

1. $p = 2$, $m = 1$, $p_i \equiv 3 \bmod 4$ *for all* i, *and* $q_j \equiv 1 \bmod 4$ *for all* j
2. $p \equiv 1 \bmod 4$, $m = DN/(2p)$, *for all* i, $p_i \not\equiv 1 \bmod 4$, *and for all* j, $q_j \not\equiv 3 \bmod 4$
3. $p = 2$, $m = DN/2$, $p_i \equiv 3 \bmod 4$ *for all* i, *and* $q_j \equiv 1 \bmod 4$ *for all* i
4. $p \equiv 1 \bmod 4$, $m = DN/p$, *for all* i, $p_i \not\equiv 1 \bmod 4$, *and for all* j, $q_j \not\equiv 3 \bmod 4$

Theorem (4.2.1)**.** *Fix square-free positive integers D', N' such that $(D', N') = 1$ and D' is the product of an odd number of primes. Fix also $m > 1$ such that $m | D'N'$. The following are equivalent.*

1. *There is a definite quaternion algebra B' over $\mathbf{Q}$ of discriminant D', an Eichler order $\mathcal{O}'$ of level N' in B' and elements ω_1 and ω_2 contained in $\mathcal{O}'$ such that $\omega_1^2 = -1$ and $\omega_2^2 = -m$.*
2. *There are factorizations $D' = \prod_i p_i$ and $N' = \prod_j q_j$ into distinct primes such that*
   - $m = D'N'$ *or* $2 | D'N'$ *and* $m = D'N'/2$
   - *for all i either $p_i = 2$ or $p_i \equiv 3 \bmod 4$*
   - *for all j either $q_j = 2$ or $q_j \equiv 1 \bmod 4$*

Theorem (4.2.5)**.** *Fix squarefree positive integers D', N' such that $(D', N') = 1$ and D' is the product of an odd number of primes. Fix also $m | D'N'$ such that $m > 1$, $m \neq 3$. The following are equivalent*

1. *There is a definite quaternion algebra B' of discriminant D', an Eichler order $\mathcal{O}'$ of level N' in B' and $\frac{1+\omega_1}{2}, \omega_2 \in \mathcal{O}'$ such that $\omega_1^2 = -3$ and $\omega_2^2 = -m$.*
2. *There are factorizations $D' = \prod_i p_i$, $N' = \prod_j q_j$ into distinct primes such that*

- $m = D'N'$, *or* $3 \mid D'N'$ *and* $m = D'N'/3$
- *for all* i *either* $p_i = 3$ *or* $p_i \equiv 2 \bmod 3$
- *for all* j *either* $q_j = 3$ *or* $q_j \equiv 1 \bmod 3$

Theorem (4.2.9)**.** *Let* D *be the squarefree product of an even number of primes,* N *a squarefree integer coprime to* D*, and* p *a prime not dividing* DN*. Let* $B' = B_{Dp}$ *and let* $m \mid DN$ *be an integer greater than one. We have the following equivalences.*

1. *Suppose that* $2 \nmid DNp$*. There is an Eichler order* $\mathcal{O}'$ *of level* N *in* B' *and embeddings* $\psi_1 : \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ *and* $\psi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ *if and only if* $m = DN$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$*, and* $\left(\frac{-DN}{p}\right) = -1$.

2. *Suppose that* $2 \mid N$*. There is an Eichler order* $\mathcal{O}'$ *of level* N *in* B' *and embeddings* $\psi_1 : \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ *and* $\psi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ *if and only if one of the following two cases occurs.*

   - $m = DN$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid (N/2)$*, and* $\left(\frac{-DN}{p}\right) = -1$
   - $m = DN/2$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid (N/2)$*, and* $\left(\frac{-DN/2}{p}\right) = -1$

3. *Suppose* $2 \mid D$ *and* $\left(\frac{-DN}{p}\right) = -1$*. There is an Eichler order* $\mathcal{O}'$ *of level* N *in* B' *and embeddings* $\psi_1 : \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ *and* $\psi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ *if and only if* $m = DN$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid (D/2)$, $p \not\equiv 7 \bmod 8$*, and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$.

4. *Suppose* $2 \mid D$ *and* $\left(\frac{-DN}{p}\right) = 1$*. There is an Eichler order* $\mathcal{O}'$ *of level* N *in* B' *and embeddings* $\psi_1 : \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ *and* $\psi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ *if and only if* $m = DN/2$, $DN \equiv 2, 6,$ *or* $10 \bmod 16$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid (D/2)$, $p \not\equiv 7 \bmod 8$*, and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$.

5. *Suppose that* $p = 2$*. There is an Eichler order* $\mathcal{O}'$ *of level* N *in* B' *and embeddings* $\psi_1 : \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ *and* $\psi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ *if and only if* $m = DN \equiv \pm 3 \bmod 8$, $\left(\frac{-2}{q}\right) = -1$ *for all primes* $q \mid D$*, and* $\left(\frac{-2}{q}\right) = 1$ *for all primes* $q \mid N$.

Corollary (7.0.3)**.** *Let* $p \neq 2$ *be a prime and let* N *be a squarefree integer such that* $\left(\frac{-N}{p}\right) = -1$*. It follows that the Hilbert class polynomial* $H_{-4N}(X)$ *has a root modulo* p *if and only if for all odd primes* $q \mid N$, $\left(\frac{-p}{q}\right) = 1$.

Theorem (10.0.1)**.** *Assuming Conjecture 10.4.1, if* p *is a prime congruent to one of* $17, 33$ *or* $41 \bmod 56$ *then* $C^1(14, p, 14)$ *has infinitely many* $\mathbf{Q}$*-rational points, and in fact is an elliptic curve of rank one over* $\mathbf{Q}$.

Chapter 3

Acknowledgments

The author was financially supported by the National Science Foundation through VIGRE grant DMS-0738586. The author was also financially supported by the University of Georgia graduate school dissertation completion award and through a mathematics department teaching assistantship.

The author would like to thank Pete Clark for teaching the author about CM elliptic curves, Modular curves, Shih's method and the circle of ideas which led to this thesis. The author would also like to thank Professor Clark for innumerable discussions about all kinds of mathematics and a careful reading of this manuscript. The author is proud to be Pete Clark's first PhD student.

The author would like to thank Dino Lorenzini for his commitment to learning and especially in this thesis for teaching the author about models of curves. The author would also like to thank Professor Lorenzini for his seemingly tireless attention to detail. Without his frequent draft comments, this thesis would be far less readable.

The author would like to thank his committee, which includes both his advisors and Professors Krashen and Rumely, for carefully reading this manuscript. The author also acknowledges some helpful discussions on the Čerednik-Drinfeld graph with John Voight and on some elementary properties of stacks with David Zureick-Brown.

For inspiration, the author would like to acknowledge many people. In the study of quaternion algebras, the author learned much from the papers of Eichler, Pizer and Vigneras. In the study of Modular and Shimura curves, the author learned much from the papers of Buzzard, Darmon, Kurihara, Ogg, Mazur, Ribet, and Shimura. In this area, he would also like to acknowledge an intellectual debt to Gonzalez, Molina, Rotger, and the whole Pilar Bayer school of Shimura curves.

The author would like to acknowledge the intellectual support of the mathematics department at the University of Georgia, especially the Algebraic Geometry and Number Theory research groups. More generally, the author would like to acknowledge the intellectual support of the Emory and Georgia Tech number theory groups. The author would especially like to thank the University of Georgia administrative staff, Laura Ackerley, Heather Adams, Tamara Haag, Michele Lott, Christy McDonald, Julie McEver and Connie Poore for helping him navigate through the administrative crises which arise on the way to graduation.

The author would like to acknowledge the earlier developmental role of several people at the University of Connecticut mathematics department. In particular, the author would like to thank Keith Conrad for turning him on to number theory; Evarist Gine, Masha Gordina and Gerald Leibowitz for constant encouragement; and James Hurley for the first class that truly challenged him.

The author would like to thank Kate Thompson for constant love and support. He would like to thank his father for teaching him the value of not being afraid to do things differently and his mother for being his very first math teacher.

Chapter 4

Quaternion Arithmetic

This chapter will give the background in quaternion arithmetic necessary to study Shimura curves and their twists. Most of this material is not new and can be found in the papers and books of Eichler [Eic73] and Vigneras [Vig80]. The new material in this chapter is found in section 4.2, and concerns the question of simultaneous embeddings of quadratic orders into Eichler orders of squarefree level in a definite rational quaternion algebra. These results will be used in section 5.3 to control the arithmetic and geometry of so-called *superspecial surfaces.* Theorems based upon Theorem 4.2.9 will in turn be used to prove results on rational points in Chapter 7. Theorems based upon Theorem 4.2.1 and Theorem 4.2.5 will be used to prove results on rational points in Chapters 8 and 9.

4.1 Basic definitions and theorems

Definition 4.1.1. *A* quaternion algebra *over a field K is a four-dimensional central simple K-algebra.*

Example 4.1.2. *If the characteristic of K is not 2, and $a, b \in K^\times$ then there is a quaternion algebra over K which we denote $\left(\frac{a,b}{K}\right)$. This algebra has a K-basis $\langle 1, i, j, k\rangle$ such that $i^2 = a$,*

$j^2 = b$ *and* $k = ij = -ji$.

Definition 4.1.3. *Let K be a number field. We say that a quaternion algebra B is* ramified *at a place v of K if $B \otimes_K K_v$ is a division algebra.*

Definition 4.1.4. *If $K = \mathbf{Q}$, we say that a quaternion algebra B is* definite *if B is ramified at infinity. Likewise we say that B is* indefinite *if B is unramified at infinity.*

It is well-known that if K is a number field, the quaternion algebras B are determined up to isomorphism by the even number of places of K at which B ramifies [Mil11, Example VIII.4.4(b)]. It follows that if $K = \mathbf{Q}$, B is definite if and only if B is ramified at an odd number of primes. Therefore we make the following definition.

Definition 4.1.5. *Let $D > 0$ be a squarefree positive integer. Let B_D denote the unique quaternion $\mathbf{Q}$-algebra such that B_D is ramified at p if and only if $p \mid D$. To any quaternion $\mathbf{Q}$-algebra, we associate its discriminant* $\operatorname{disc}(B)$*, the unique positive squarefree number such that $B \cong B_{\operatorname{disc}(B)}$.*

Definition 4.1.6. *Let B be a quaternion K-algebra and let $a \mapsto \overline{a}$ denote the* main involution *of B over K [Shi10, IV.20.6a]. Define the trace $a \mapsto \operatorname{tr}(a) = a + \overline{a}$ and the norm $\mathrm{N}(a) = a\overline{a}$.*

Definition 4.1.7. *A $\mathbf{Z}$-order $\mathcal{O}$ in a quaternion $\mathbf{Q}$-algebra B is a rank four $\mathbf{Z}$-subalgebra of B such that for all $\theta \in \mathcal{O}$, $\operatorname{tr}(\theta) \in \mathbf{Z}$ and $\mathrm{N}(\theta) \in \mathbf{Z}$.*

Definition 4.1.8. *The discriminant of a $\mathbf{Z}$-order $\mathcal{O}$ with a $\mathbf{Z}$-basis $e_1, \ldots, e_4$, is $\operatorname{disc}(\mathcal{O}) = \det(\operatorname{tr}(e_i e_j))$.*

Lemma 4.1.9. *[Vig80, Corollaire I.4.8] If $\mathcal{O}_1 \supset \mathcal{O}_2$ then $\operatorname{disc}(\mathcal{O}_1) \mid \operatorname{disc}(\mathcal{O}_2)$. Moreover, $[\mathcal{O}_1 : \mathcal{O}_2] = \sqrt{\left|\frac{\operatorname{disc}(\mathcal{O}_2)}{\operatorname{disc}(\mathcal{O}_1)}\right|}$ so if $\operatorname{disc}(\mathcal{O}_2) = \operatorname{disc}(\mathcal{O}_1)$ then $\mathcal{O}_1 = \mathcal{O}_2$.*

Definition 4.1.10. *An order in a quaternion algebra will be called* maximal *if it is maximal with respect to inclusion.*

Lemma 4.1.11. *[Vig80, Corollaire II.5.3] An order $\mathcal{O}$ in a quaternion $\mathbf{Q}$-algebra B is maximal if and only if* $\operatorname{disc}(B) = \sqrt{|\operatorname{disc}(\mathcal{O})|}$.

If an order $\mathcal{O}$ is contained in two maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$, then $[\mathcal{O}_1 : \mathcal{O}] = [\mathcal{O}_2 : \mathcal{O}]$ by Lemma 4.1.9.

Definition 4.1.12. *A $\mathbf{Z}$-order $\mathcal{O} \subset B$ is called an* Eichler order *when it is the intersection of two (not necessarily distinct) maximal $\mathbf{Z}$-orders. The* level *of an Eichler order is its index in either maximal order.*

Definition 4.1.13. *By Lemma 4.1.9, if $\mathcal{O}$ is an Eichler order, $\sqrt{|\operatorname{disc}(\mathcal{O})|}$ is a positive integer, which we may sometimes refer to as the* reduced discriminant.

Definition 4.1.14. *Let $\mathbf{Z}_{p^2}$ denote the unique irreducible unramified degree two ring extension of $\mathbf{Z}_p$.*

Lemma 4.1.15. *Let B be a quaternion $\mathbf{Q}$-algebra ramified at p. Then $B \otimes \mathbf{Q}_p$ has a unique maximal $\mathbf{Z}_p$-order $\mathcal{O}$. Moreover, there exists an element $\pi \in B \otimes \mathbf{Q}_p$ such that $\pi^2 \mathcal{O} = p\mathcal{O}$ and $\mathcal{O} \cong \mathbf{Z}_{p^2} \oplus \pi \mathbf{Z}_{p^2}$. It follows that for $a \in \mathbf{Z}_{p^2}$, $\pi a \pi^{-1} = \sigma(a)$ where $\langle \sigma \rangle = \operatorname{Aut}_{\mathbf{Z}_p}(\mathbf{Z}_{p^2})$.*

Proof. The uniqueness of a maximal order for a division quaternion algebra over any local field K and its structure as a $\mathbf{Z}_K$-module is well-known [Vig80, Corollaire II.1.7]. Since $\mathcal{O}$ is unique, conjugation by π is an automorphism of $\mathcal{O}$. In fact, conjugation by π is an automorphism of $\mathbf{Z}_{p^2}$ since $\pi \mathbf{Z}_p$ commutes with π. If π commuted with all of $\mathbf{Z}_{p^2}$, then $\mathcal{O}$ and thus B would be commutative, a contradiction. Therefore conjugation by π induces the unique non-identity element of $\operatorname{Aut}_{\mathbf{Z}_p}(\mathbf{Z}_{p^2})$. □

Hereon, we suppress the $\mathbf{Z}$ as all of our quaternion algebras will be over $\mathbf{Q}$ (or be the base change of a quaternion algebra over $\mathbf{Q}$).

Lemma 4.1.16. *[Vig80, Lemme II.2.4], [Vig80, Corollaire III.5.2] Let B be a quaternion $\mathbf{Q}$-algebra and $\mathcal{O}$ an Eichler order of level N. If $p \nmid \operatorname{disc}(B)$, then there is an embedding*

$\mathcal{O} \otimes \mathbf{Z}_p \hookrightarrow M_2(\mathbf{Z}_p)$. *Moreover there is a unique integer* n *such that* $\mathcal{O} \otimes \mathbf{Z}_p$ *is conjugate to an order in* $M_2(\mathbf{Z}_p)$ *of the form*

$$\begin{pmatrix} \mathbf{Z}_p & \mathbf{Z}_p \\ p^n\mathbf{Z}_p & \mathbf{Z}_p \end{pmatrix}.$$

We may explicitly give n *as the non-negative integer such that* $p^n \mid N$ *but* $p^{n+1} \nmid N$.

Definition 4.1.17. *We say that an order* $\mathcal{O}$ *is* ramified *at* p *if* $p \mid \operatorname{disc}(\mathcal{O})$.

Definition 4.1.18. *[Eic73, p.17] Let* B *be a quaternion algebra over* $\mathbf{Q}$ *and* $\mathcal{O} \subset B$ *an order. A left* $\mathcal{O}$*-ideal is a left* $\mathcal{O}$*-module* M *contained in* B *such that* $\mathcal{O}M = M$ *and for all primes* p *of* $\mathbf{Q}$*, there exist* $m_p \in B$ *such that* $\mathbf{Z}_p \otimes M = \mathbf{Z}_p \otimes \mathcal{O}m_p$. *If* M *is a left* $\mathcal{O}$*-ideal then we call* $\mathcal{O}_r(M) := \{x \in B : Mx \subset M\}$ *the* right order *of* M. *We say that* M *is two-sided if* $\mathcal{O} = \mathcal{O}_r(M)$. *We may similarly define right ideals* I *and their left orders* $\mathcal{O}_l(I)$.

Definition 4.1.19. *Let* B *be a quaternion algebra and* $\mathcal{O} \subset B$ *an order. We say that a (left, right or two-sided)* $\mathcal{O}$*-ideal* M *is* integral *if* $M \subset \mathcal{O}$.

Definition 4.1.20. *Let* B *be a quaternion algebra and* $\mathcal{O} \subset B$ *an order. We say a left* $\mathcal{O}$*-ideal* M *is* principal *if there is some* $m \in B$ *such that* $M = \mathcal{O}m$*, and similarly for right* $\mathcal{O}$*-ideals.*

Lemma 4.1.21. *If* B *is indefinite and* $\mathcal{O}$ *is an Eichler order in* B *(of any level), then every left (or right)* $\mathcal{O}$*-ideal is principal. Therefore, the Eichler orders (of any given level) are conjugate.*

Proof. If B is indefinite, then $\{\infty\}$ satisfies the Eichler Condition [Vig80, Definition, p.81]. Therefore, the class number of $\mathcal{O}$ is the class number of $\mathbf{Q}$ [Vig80, Corollaire III.5.7(1)]. This is to say, the class number of $\mathcal{O}$ is one. Then we note that the number of left (or right) ideals up to isomorphism of an Eichler order (of any level) is at least the number of Eichler orders (of that level) up to conjugation, and this can be made precise [Vig80, Lemme III.5.6]. □

Lemma 4.1.22. *If B is definite and $\mathcal{O}$ is an Eichler order in B then $\mathcal{O}^\times$ is finite. The number of left (or right) ideals up to right (or left) multiplication by $B^\times$ is finite.*

Proof. In a maximal order there are only finitely many units [Vig80, Proposition V.3.1], and any order is contained in a maximal order. The finiteness of left (or right) ideal classes is true in broad generality. If F is a totally real field and $B_{/F}$ is a totally definite quaternion algebra (which is to say that for all embeddings $\epsilon : F \to \mathbf{R}$, $B \otimes_\epsilon \mathbf{R}$ is division) and $\mathcal{O}$ is an Eichler $\mathbf{Z}_F$-order of B then the left $\mathcal{O}$-ideals up to $B^\times$-multiplication is finite [Vig80, Corollaire V.2.3]. □

Lemma 4.1.23. *[Eic73, Theorem II.1.1] Let B be a quaternion algebra of discriminant D. If $\mathcal{O}$ is an Eichler order of square-free level N in B, then the two-sided ideals of $\mathcal{O}$ form an abelian group under multiplication. For each prime $p \mid DN$, there is a unique two-sided integral ideal $\wp_p$ such that $\wp_p^2 = \mathcal{O}p = p\mathcal{O}$. Moreover, any two-sided ideal of $\mathcal{O}$ is equal to one of the form*

$$\Big(\prod_{p \mid DN} \wp_p^{\epsilon_p}\Big) r$$

where $r \in \mathbf{Q}$ and $\epsilon_p \in \{0, 1\}$.

Definition 4.1.24. *Let A be a finitely-generated, torsion-free $\mathbf{Z}$-algebra, let A^0 be $A \otimes_{\mathbf{Z}} \mathbf{Q}$ and let $\epsilon_A : A \to A^0$ be the natural embedding $a \mapsto a \otimes 1$. Suppose that there exists an embedding $\phi : A_1 \hookrightarrow A_2$ of finitely generated torsion-free $\mathbf{Z}$-algebras. Define $\phi^0 : A_1^0 \hookrightarrow A_2^0$ to be the induced embedding $a \otimes r/s \mapsto \phi(a) \otimes r/s$. We say that ϕ is* optimal *if $\epsilon_{A_1}(A_1) = (\phi^0)^{-1}(\epsilon_{A_2}(A_2))$.*

Let $\phi : A_1 \hookrightarrow A_2$ be an embedding of finitely generated torsion-free $\mathbf{Z}$-algebras. Define $A_1' := (\phi^0)^{-1}(\epsilon_{A_2}(A_2))$ and note that A_1' is a finitely generated torsion-free $\mathbf{Z}$-algebra. Note also that $A_1^0 \supset A_1' \supset A_1$ because ϕ^0 induces an embedding $A_1' \hookrightarrow A_2$. Moreover, this embedding is an optimal embedding $\psi : (\phi^0)^{-1}(\epsilon_{A_2}(A_2)) \to A_2$.

We define optimal embeddings in order to study embeddings of quadratic orders into quaternion orders. Namely, if R is an order in a quadratic number field K, then any embedding of R into a quaternion order $\mathcal{O}$ is optimal for some order R' where $K \supset R' \supset R$. We shall see in Theorem 4.1.28 that there are strictly numerical criteria for optimal embeddings of quadratic orders into quaternion orders $\mathcal{O}$, and so summing those conditions over all $K \supset R' \supset R$ gives criteria for any embeddings of R into $\mathcal{O}$.

Definition 4.1.25. *Let Δ be an integer which is congruent to zero or one modulo four. We will denote by R_Δ the unique quadratic order of discriminant Δ. If Δ is not a square, $R_\Delta \otimes \mathbf{Q}$ is a quadratic field $K_\Delta = \mathbf{Q}(\sqrt{\Delta})$. In this case, we may define the class number $h(\Delta) := \#\operatorname{Pic}(R_\Delta)$ and the conductor $f(\Delta) := [\mathbf{Z}_{K_\Delta} : R_\Delta]$. We also fix $w(\Delta) := \#R_\Delta^\times$.*

Definition 4.1.26. *Let p be a prime, and let $\left(\frac{\cdot}{p}\right)$ denote the Kronecker symbol. That is, if p is odd, the Kronecker symbol is the Legendre symbol. If $p = 2$ then $\left(\frac{2}{2}\right) = 0$ and if q is an odd prime then $\left(\frac{q}{2}\right) = (-1)^{(q^2-1)/8}$. We obtain the Kronecker symbol by extending multiplicatively.*

The Eichler symbol may then be defined in terms of the Kronecker symbol as follows:

$$\left\{\frac{\Delta}{p}\right\} = \begin{cases} 1 & p \mid f(\Delta) \\ \left(\frac{\Delta}{p}\right) & else \end{cases}$$

Definition 4.1.27. *For square-free coprime integers D and N and some integer $\Delta \equiv 0, 1 \bmod 4$, we define the quantity*

$$e_{D,N}(\Delta) := h(\Delta) \prod_{p \mid D} \left(1 - \left\{\frac{\Delta}{p}\right\}\right) \prod_{q \mid N} \left(1 + \left\{\frac{\Delta}{p}\right\}\right).$$

Theorem 4.1.28 (Eichler's embedding theorem)**.** *Let D and N be square-free coprime integers. If B_D is indefinite, i.e. if an even number of primes divide D, then the number of optimal embeddings of a quadratic order R of discriminant Δ into some Eichler order $\mathcal{O}$ of square-free level N in B_D up to $\mathcal{O}^\times$ conjugacy is $e_{D,N}(\Delta)$. If B_D is definite, i.e., if an odd number of primes divide D, then the number of optimal embeddings of a quadratic order R of* *discriminant Δ into some Eichler order $\mathcal{O}$ of square-free level N in B_D up to $\mathcal{O}^\times$ conjugacy is $e_{D,N}(\Delta)/w(\Delta)$.*

Proof. This is proven separately in the indefinite case [Vig80, Corollaire III.5.12] and in the definite case [Eic73, Proposition 5]. $\square$

Corollary 4.1.29. *If DN is square-free, $\mathbf{Z}[\sqrt{-1}] = \mathbf{Z}[\zeta_4]$ embeds into an Eichler order of level N in B_D if and only if for all $p \mid D$, $p = 2$ or $p \equiv 3 \bmod 4$, and for all $q \mid N$, $q = 2$ or $q \equiv 1 \bmod 4$.*

Corollary 4.1.30. *If DN is square-free, $\mathbf{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbf{Z}[\zeta_6]$ embeds into an Eichler order of level N in B_D if and only if for all $p \mid D$, $p = 3$ or $p \equiv 2 \bmod 3$, and for all $q \mid N$, $q = 3$ or $q \equiv 1 \bmod 3$.*

4.2 Simultaneous embeddings into Eichler orders

In the following section, we describe sone new results on embeddings of quadratic orders into Eichler orders of definite quaternion algebras in the style of Brzezinski and Eichler [BE92]. These results will be useful in the remainder of the thesis.

Let B' be a definite quaternion $\mathbf{Q}$-algebra. Suppose that there exist $\omega_1, \omega_2 \in B'$ such that $\omega_1^2 = -q$ and $\omega_2^2 = -d$ for $q, d \in \mathbf{Z}$. Then clearly $\omega_1\omega_2 \in B'$ is of norm qd. Although ω_1 and ω_2 are integral, it may be the case that $\omega_1\omega_2$ is not integral. We only know that $\operatorname{tr}(\omega_1\omega_2) < 4qd$. In order for $\omega_1\omega_2$ to be integral it is necessary and sufficient that $\operatorname{tr}(\omega_1\omega_2) = \omega_1\omega_2 + \omega_2\omega_1 = s \in \mathbf{Z}$.

Now let us grant that $\operatorname{tr}(\omega_1\omega_2) \in \mathbf{Z}$. Since ω_1, ω_2, and $\omega_1\omega_2$ are integral, any order $\mathcal{O}'$ that contains ω_1 and ω_2 contains $\omega_1\omega_2$. Note that the $\mathbf{Z}$-module generated by 1, ω_1, ω_2 and $\omega_1\omega_2$ is an order of B' if and only if $\langle 1, \omega_1, \omega_2, \omega_1\omega_2\rangle$ is a basis for B' over $\mathbf{Q}$.

In the latter case, we may compute that the reduced discriminant of $\mathbf{Z}\oplus\mathbf{Z}\omega_1\oplus\mathbf{Z}\omega_2\oplus\mathbf{Z}\omega_1\omega_2$

is $4qd - s^2$. If $q \equiv 3 \bmod 4$, $\dfrac{1+\omega_1}{2}$ is integral and the reduced discriminant of

$$\mathbf{Z} \oplus \mathbf{Z}\frac{1+\omega_1}{2} \oplus \mathbf{Z}\omega_2 \oplus \mathbf{Z}\frac{1+\omega_1}{2}\omega_2$$

is $dq - \left(\frac{s}{2}\right)^2$.

We now prove the following.

Theorem 4.2.1. *Fix square-free positive integers D', N' such that $(D', N') = 1$ and D' is the product of an odd number of primes. Fix also $m > 1$ such that $m | D'N'$. The following are equivalent.*

1. *There is a definite quaternion algebra B' over $\mathbf{Q}$ of discriminant D', an Eichler order $\mathcal{O}'$ of level N' in B' and elements ω_1 and ω_2 contained in $\mathcal{O}'$ such that $\omega_1^2 = -1$ and $\omega_2^2 = -m$.*

2. *There are factorizations $D' = \prod_i p_i$ and $N' = \prod_j q_j$ into distinct primes such that*

    - *$m = D'N'$ or $2 | D'N'$ and $m = D'N'/2$*
    - *for all i either $p_i = 2$ or $p_i \equiv 3 \bmod 4$*
    - *for all j either $q_j = 2$ or $q_j \equiv 1 \bmod 4$*

Proof. For (1) $\Rightarrow$ (2), we know in the first place by Eichler's Theorem on embeddings that if $\mathbf{Z}[\zeta_4] \hookrightarrow \mathcal{O}'$ then $p_i = 2$ or $p_i \equiv 3 \bmod 4$ and $q_j = 2$ or $q_j \equiv 1 \bmod 4$. While a priori it may seem that we could use Eichler's theorem to narrow down the possible choices of m, it is more profitable to directly use the knowledge that we have simultaneous embeddings and conclude at the end that $D'N'$ and (if possible) $D'N'/2$ satisfy Eichler's Theorem.

Since $m > 1$, $\mathbf{Z}[\zeta_4] \not\hookrightarrow \mathbf{Z}[\sqrt{-m}]$ and vice versa. Therefore $\mathcal{O}' \supset \mathbf{Z} \oplus \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2 \oplus \mathbf{Z}\omega_1\omega_2$ and so $m \mid D'N' \mid 4m - s^2$. If $s = 0$, we have $m \mid D'N' \mid 2m$ since $D'N'$ is squarefree.

If $s \neq 0$, $m \mid 4m - s^2$ implies that $m \mid s$ and $m \leq |s|$. Since $m^2 \leq s^2 < 4m$, we have $m < 4$ and in fact $m = 2$ or $m = 3$. If $m = 2$ and $0 < s^2 < 4m = 8$ then $m|s$ implies that $|s| = 2$ and thus $2 \mid D'N' \mid 4$. Then $D'N'$ square-free and $D' > 1$ implies that $m = D' = D'N' = 2$. If $m = 3$ and $0 < s^2 < 4m = 12$ then $m \mid s$ implies that $|s| = 3$ and thus $3 \mid D'N' \mid 3$ so $m = D' = D'N' = 3$.

For (2) $\Rightarrow$ (1), we may exclude the case $D'N' = 3$ because the quaternion algebra $\left(\frac{-1,-3}{\mathbf{Q}}\right)$ of discriminant 3 has a unique maximal order.

Therefore it suffices to consider the quaternion algebra $A = \left(\frac{-1,-D'N'}{\mathbf{Q}}\right)$ which we take for now to be generated by ω_1 and ω_2, fixing $\omega_2^2 = -D'N'$ because if $2 \mid D'N'$, $\left(\frac{1+\omega_1}{2}\right)\omega_2$ squares to $-D'N'/2$.

We note first that under these conditions, A has discriminant D'. First we note that if p does not divide $D'N'$ then A splits over $\mathbf{Q}_p$ because the Chevalley-Warning theorem [Ser73, §I.2.2] tells us that a four variable quadratic form over a finite field is isotropic. Hence by Hensel's Lemma we are done. If $p \mid D'N'$ is an odd prime, then $x^2 + y^2$ represents p if and only if $p \equiv 1 \bmod 4$ so again by Hensel's Lemma, A does not split over $\mathbf{Q}_p$ for p odd if and only if $p \mid D'$. Finally if $2 \mid D'$ then $D'N'/2 \equiv 1 \bmod 4$ so $D'N' \equiv 2 \bmod 8$ and thus $-D'N'$ is not a sum of two squares in $\mathbf{Z}/8\mathbf{Z}$. If $2 \mid N'$, $D'N'/2 \equiv 3 \bmod 4$ so $D'N' \equiv 6 \bmod 8$ and so $-D'N'$ is a sum of squares in $\mathbf{Q}_2$.

We now exhibit an explicit order $\mathcal{O}'$ of level N'.

If $2 \nmid D'N'$ then $D'N' \equiv 3 \bmod 4$ and so $\frac{1+\omega_2}{2}$ is integral and so $\mathbf{Z} \oplus \mathbf{Z}\omega_1 \oplus \mathbf{Z}\left(\frac{1+\omega_2}{2}\right) \oplus \mathbf{Z}\omega_1\left(\frac{1+\omega_2}{2}\right)$ has reduced discriminant $D'N'$.

If $2 \mid D'N'$, let $\omega_2' = \left(\frac{1+\omega_1}{2}\right)\omega_2$ then as before, the reduced discriminant of $\mathbf{Z} \oplus \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2' \oplus \mathbf{Z}\omega_1\omega_2'$ is $4D'N'/2 = 2D'N'$. In this case, we consider the "Hurwitz quaternions"

$$\mathbf{Z} \oplus \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2' \oplus \mathbf{Z}\frac{1+\omega_1+\omega_2'+\omega_1\omega_2'}{2}$$

which have reduced discriminant $D'N'$. $\square$

We note that we gave a very explicit example of an order satisfying Theorem 4.2.1 (1) in the proof above. An interesting fact is that such an order is unique up to $B^\times$-conjugacy.

Theorem 4.2.2 (Pizer)**.** *Let B' be a definite $\mathbf{Q}$-quaternion algebra and suppose that for all $p \mid \operatorname{disc}(B')$, $\left(\frac{-4}{p}\right) = -1$. Let N be a squarefree integer such that for all $p \mid N$, $\left(\frac{-4}{p}\right) = 1$. Then there is a unique conjugacy class of Eichler orders of level N in B' into which $\mathbf{Z}[\zeta_4]$ embeds.*

Similarly, suppose that for all $p \mid \operatorname{disc}(B')$, $\left(\frac{-3}{p}\right) = -1$, and let N be a squarefree integer such that for all $p \mid N$, $\left(\frac{-3}{p}\right) = 1$. Then there is a unique conjugacy class of Eichler orders of level N in B' into which $\mathbf{Z}[\zeta_6]$ embeds.

Proof. Let $\mathfrak{o}$ be an order in an imaginary quadratic field. Recall the definition given by Pizer [Piz76, Definition 11] of $D(\mathfrak{o})$ as the number of $(B')^\times$-conjugacy classes of Eichler orders of level N in B into which $\mathfrak{o}$ is optimally embedded. During the proof of Theorem 16 on page 73 of the same article, it is proven that if $\mathfrak{o} = \mathbf{Z}[\zeta_4]$ then $D(\mathfrak{o})$ is zero or one depending on whether or not there is an optimal embedding. Similarly on page 75 of the same article, the same thing is proven for $\mathbf{Z}[\zeta_6]$. $\square$

Corollary 4.2.3. *Let B' be a definite quaternion algebra of discriminant D', and let $\mathcal{O}'$ be an Eichler order of B' of squarefree level N' such that $\mathbf{Z}[\zeta_4] \hookrightarrow \mathcal{O}'$. If $m \mid D'N'$ and $m \neq 1$, then $\mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = D'N'$ or $2 \mid D'N'$ and $m = D'N'/2$.*

Proof. Since there exists some $\phi_1 : \mathbf{Z}[\zeta_4] \hookrightarrow \mathcal{O}'$, $\mathcal{O}'$ is unique up to $B^\times$-conjugacy. If there exists some $\phi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ then let $\omega_1 = \phi_1(\zeta_4)$ and $\omega_2 = \phi_2(\sqrt{-m})$. It follows that $\mathcal{O}' \supset \mathbf{Z} \oplus \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2 \oplus \mathbf{Z}\omega_1\omega_2$ since $m \neq 1$ and so neither quadratic order is contained in the other. By Theorem 4.2.1, $m = D'N'$ or $D'N'/2$.

Suppose now that $m = D'N'$ or $D'N'/2$. By Theorem 4.2.1, there is some order $\mathfrak{S}$ of B' admitting embeddings of both $\mathbf{Z}[\zeta_4]$ and $\mathbf{Z}[\sqrt{-m}]$. Since $\mathfrak{S}$ admits an embedding of

$\mathbf{Z}[\zeta_4]$, it must be conjugate to $\mathcal{O}'$ by Theorem 4.2.2 and thus $\mathcal{O}'$ admits an embedding of $\mathbf{Z}[\sqrt{-m}]$. $\square$

Corollary 4.2.4. *When the conditions of Theorem 4.2.1 are satisfied,* $B' \cong \left(\frac{-1,-D'N'}{\mathbf{Q}}\right)$ *and* $\mathcal{O}'$ *is* $(B')^\times$*-conjugate to one of the following:*

1. *The unique maximal order in* B' *if* $D' = 2$ *or* 3.

2. $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}\frac{1+j}{2} \oplus \mathbf{Z}\frac{i+k}{2}$ *if* $2 \nmid D'N'$.

3. $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}\frac{j+k}{2} \oplus \mathbf{Z}\left(\frac{1+i}{2} + \frac{j+k}{4}\right)$ *if* $2 \mid D'N'$.

Moreover if $2 \mid D'N'$ *we note that the order in 3. contains* $\dfrac{j+k}{2}$, *a square root of* $-D'N'/2$.

We now turn our attention to simultaneous embeddings of $\mathbf{Z}[\zeta_6]$ and $\mathbf{Z}[\sqrt{-m}]$.

Theorem 4.2.5. *Fix squarefree positive integers* D', N' *such that* $(D', N') = 1$ *and* D' *is the product of an odd number of primes. Fix also* $m | D'N'$ *such that* $m > 1$, $m \neq 3$. *The following are equivalent*

1. *There is a definite quaternion algebra* B' *of discriminant* D', *an Eichler order* $\mathcal{O}'$ *of level* N' *in* B' *and* $\frac{1+\omega_1}{2}, \omega_2 \in \mathcal{O}'$ *such that* $\omega_1^2 = -3$ *and* $\omega_2^2 = -m$.

2. *There are factorizations* $D' = \prod_i p_i$, $N' = \prod_j q_j$ *into distinct primes such that*

   - $m = D'N'$, *or* $3 \mid D'N'$ *and* $m = D'N'/3$
   - *for all* i *either* $p_i = 3$ *or* $p_i \equiv 2 \bmod 3$
   - *for all* j *either* $q_j = 3$ *or* $q_j \equiv 1 \bmod 3$

Proof. To show that (1) implies (2), we note first by Eichler's Theorem on embeddings that if $\mathbf{Z}[\zeta_6] \hookrightarrow \mathcal{O}'$ then $p_i = 3$ or $p_i \equiv 2 \bmod 3$ and $q_j = 3$ or $q_j \equiv 1 \bmod 3$.

Note that since $m > 1$ and $m \neq 3$, $\mathbf{Z}[\zeta_6] \not\supset \mathbf{Z}[\sqrt{-m}]$ and vice versa. We know that since $\mathcal{O}' \supset \mathbf{Z} \oplus \mathbf{Z}\left(\frac{1+\omega_1}{2}\right) \oplus \mathbf{Z}\omega_2 \oplus \mathbf{Z}\left(\frac{1+\omega_1}{2}\right)\omega_2$, $m \mid D'N' \mid 3m - (s/2)^2$. If $s = 0$, we have the result that $m \mid D'N' \mid 3m$.

If $s \neq 0$, $m \mid 3m - (s/2)^2$ implies that $m \mid (s/2)$ and $m^2 \leq (s/2)^2 < 3m$ so $m = 2$. If $0 < (s/2)^2 < 6$ and $2 \mid (s/2)$ then $s = 4$ so $m = D' = D'N' = 2$.

To show that (2) implies (1), we may exclude the case $D'N' = 2$ because the quaternion algebra $\left(\frac{-1,-1}{\mathbf{Q}}\right)$ of discriminant 2 has a unique maximal order. Therefore it suffices to consider the quaternion algebra $A = \left(\frac{-3,-D'N'}{\mathbf{Q}}\right)$ which we take for now to be generated by ω_1 and ω_2, fixing $\omega_2^2 = -D'N'$ because if $3 \mid D'N'$, $(\omega_1\omega_2)^2 = -3D'N'$ so $(1/3)\omega_1\omega_2$ squares to $-D'N'/3$.

We note first that under these conditions, A has discriminant D'. First we note that if p does not divide $D'N'$ then A splits because the Chevalley-Warning theorem [Ser73, §I.2.2] tells us that a four variable quadratic form over a finite field is isotropic. If $p \mid D'N'$ is an odd prime, then $x^2 + 3y^2$ represents p if and only if $p \equiv 1 \bmod 3$ or $p = 3$, and if $2 \mid D'$, A does not split because $x^2 + 3y^2$ is not isotropic over $\mathbf{Q}_2$.

We now exhibit an explicit order $\mathcal{O}'$ of level N'.

- If $3 \mid D'N'$ then $\omega_2' = \frac{\omega_1}{3}\omega_2$ is such that $(\omega_2')^2 + D'N'/3 = 0$ and so the reduced discriminant of $\mathbf{Z} \oplus \mathbf{Z}\frac{1+\omega_1}{2} \oplus \mathbf{Z}\omega_2' \oplus \mathbf{Z}\frac{1+\omega_1}{2}\omega_2'$ is $3(D'N'/3) = D'N'$.
- If $3 \nmid D'N'$, then $D'N' \equiv -1 \bmod 3$. Therefore we can show that $\alpha = \mathbf{Z}\frac{1+\omega_1}{2}$, $\beta = \frac{1+\omega_2}{2} + \frac{\omega_1 + \omega_1\omega_2}{6}$ and $\gamma = \frac{-3+\omega_1 - 2\omega_1\omega_2}{6}$ are all integral with $N(\alpha) = 1$, $N(\beta) = N(\gamma) = \frac{D'N'+1}{3}$. It can thus be easily calculated that $\mathbf{Z} \oplus \mathbf{Z}\alpha \oplus \mathbf{Z}\beta \oplus \mathbf{Z}\gamma$ is a suitable Eichler order of level N' in A.

□

Corollary 4.2.6. *Let B' be a definite quaternion algebra of discriminant D' and let $\mathcal{O}'$ be* *an Eichler order of B' of squarefree level N' such that $\mathbf{Z}[\zeta_6] \hookrightarrow \mathcal{O}'$. If $m \mid D'N'$ and $m \neq 1, 3$, then $\mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = D'N'$ or $D'N'/3$.*

Proof. Since there exists some $\phi_1 : \mathbf{Z}[\zeta_6] \hookrightarrow \mathcal{O}'$, $\mathcal{O}'$ is unique up to $B^\times$-conjugacy. If there exists some $\phi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ then let $\omega_1 = 2\phi_1(\zeta_6) - 1$ and $\omega_2 = \phi_2(\sqrt{-m})$. It follows that $\mathcal{O}' \supset \mathbf{Z} \oplus \mathbf{Z}\frac{1+\omega_1}{2} \oplus \mathbf{Z}\omega_2 \oplus \mathbf{Z}\frac{1+\omega_1}{2}\omega_2$ since $m \neq 1, 3$ and so neither quadratic order is contained in the other. By Theorem 4.2.5, $m = D'N'$ or $D'N'/3$.

Suppose now that $m = D'N'$ or $D'N'/3$. By Theorem 4.2.5, there is some order $\mathfrak{S}$ of B' admitting embeddings of both $\mathbf{Z}[\zeta_6]$ and $\mathbf{Z}[\sqrt{-m}]$. Since $\mathfrak{S}$ admits an embedding of $\mathbf{Z}[\zeta_6]$, it must be conjugate to $\mathcal{O}'$ by Theorem 4.2.2 and thus $\mathcal{O}'$ admits an embedding of $\mathbf{Z}[\sqrt{-m}]$. $\square$

Corollary 4.2.7. *When the conditions of Theorem 4.2.5 are satisfied, $B' \cong \left(\frac{-3, -D'N'}{\mathbf{Q}}\right)$ and $\mathcal{O}'$ is $B^\times$-conjugate to one of the following:*

1. *The unique maximal order in B' if $D' = 2$*
2. $\mathbf{Z} \oplus \mathbf{Z}\frac{1+i}{2} \oplus \mathbf{Z}\left(\frac{1+j}{2} + \frac{i+k}{6}\right) \oplus \mathbf{Z}\frac{-3+i-2k}{6}$ *if $3 \nmid D'N'$*
3. $\mathbf{Z} \oplus \mathbf{Z}\frac{1+i}{2} \oplus \mathbf{Z}\frac{k}{3} \oplus \mathbf{Z}\frac{k-j}{6}$ *if $3 \mid D'N'$*

Moreover if $3 \mid D'N'$, the order in 3. contains $k/3$, a square root of $-D'N'/3$.

We prove one final theorem on simultaneous embeddings. For the remainder of the section, let D be the squarefree product of an even number of primes, N a squarefree integer coprime to D, and p a prime not dividing DN. We shall also set $B' := B_{Dp}$ and let $m \mid DN$ be an integer greater than one.

Lemma 4.2.8. *We have the following isomorphisms of $\mathbf{Q}$-algebras.*

1. *If $2 \nmid DNp$, $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid N$, and $\left(\frac{-DN}{p}\right) = -1$, then $B' \cong \left(\frac{-p, -DN}{\mathbf{Q}}\right)$.*

2. *If* $2 \mid N$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid (N/2)$, *and* $\left(\frac{-DN}{p}\right) = -1$, *then* $B' \cong \left(\frac{-p,-DN}{\mathbf{Q}}\right) \cong \left(\frac{-p,-DN/2}{\mathbf{Q}}\right)$.

3. *If* $2 \mid D$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$, *and* $\left(\frac{-DN}{p}\right) = -1$, *then* $B' \cong \left(\frac{-p,-DN}{\mathbf{Q}}\right)$.

4. *If* $2 \mid D$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$, *and* $\left(\frac{-DN/2}{p}\right) = -1$, *then* $B' \cong \left(\frac{-p,-DN/2}{\mathbf{Q}}\right)$.

5. *If* $p = 2$, $\left(\frac{-2}{q}\right) = -1$ *for all primes* $q \mid D$, *and* $\left(\frac{-2}{q}\right) = 1$ *for all primes* $q \mid N$ *then* $B' \cong \left(\frac{-2,-DN}{\mathbf{Q}}\right)$.

Proof. Let q be an odd prime, and let $m \mid DN$ so that if an odd prime divides DN then it divides m. Recall that $B(m) := \left(\frac{-p,-m}{\mathbf{Q}}\right)$ is ramified at q if and only if the quadratic form $x^2 + py^2 + mz^2 + mpw^2$ is anisotropic over $\mathbf{Q}_q$ if and only if it is anisotropic over $\mathbb{F}_q$.

If $q \nmid DNp$, then $q \nmid m$ and $q \nmid p$ so by the Chevalley-Warning Theorem, $B(m)$ is unramified at q. If $q \mid N$ then $x^2 + py^2$ is isotropic over $\mathbb{F}_q$ because $\left(\frac{-p}{q}\right) = 1$, so $B(m)$ is unramified at q. If $q \mid D$ then $x^2 + py^2$ is anisotropic over $\mathbb{F}_q$ because $\left(\frac{-p}{q}\right) = -1$ so $B(m)$ is ramified at q. If p is odd and m is an integer such that $\left(\frac{-m}{p}\right) = -1$ then $x^2 + my^2$ is anisotropic over $\mathbb{F}_p$, so $B(m)$ is ramified at p. Finally note that $B \otimes \mathbf{R}$ is division.

Therefore, if $2 \nmid DNp$ then $B(m) \cong B' \cong B_{Dp}$, or equivalently, $B(m)$ is unramified at 2. If $B(m)$ were ramified at 2, it would be ramified at an odd number of places of $\mathbf{Q}$, and hence $B(m)$ is ramified precisely at the primes dividing Dp.

If $2 \mid N$ then p is odd, all primes not dividing DNp are odd, and hence $B(m) \cong B'$ whether $m = DN$ or $DN/2$.

If $2 \mid D$, then p is odd and we have $\left(\frac{-p}{2}\right) = \left(\frac{p}{2}\right) = \left(\frac{2}{p}\right) = -1$. Therefore

$$\left(\frac{-DN}{p}\right) = \left(\frac{-DN/2}{p}\right)\left(\frac{2}{p}\right) = -\left(\frac{-DN/2}{p}\right),$$

so $m = DN$ or $DN/2$ but not both. Whether $m = DN$ or $DN/2$, we have shown that $B(m)$ is ramified at p, ∞ and precisely the odd number of odd primes dividing D. It follows that for the appropriate choice of m, $B(m)$ is ramified at 2 and thus $B(m) \cong B_{Dp}$.

If $p = 2$ then $B(m)$ is ramified both at ∞ and at the even number of primes dividing D, so it must be ramified at 2. It follows that $B(m) \cong B'$. $\square$

Theorem 4.2.9. *Recall that D is the squarefree product of an even number of primes, N a squarefree integer coprime to D, and p a prime not dividing DN. Recall further that $B' = B_{Dp}$ and let $m \mid DN$ be an integer greater than one. We have the following equivalences.*

1. *Suppose that $2 \nmid DNp$. There is an Eichler order $\mathcal{O}'$ of level N in B' and embeddings $\psi_1 : \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ and $\psi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = DN$, $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid N$, and $\left(\frac{-DN}{p}\right) = -1$.*

2. *Suppose that $2 \mid N$. There is an Eichler order $\mathcal{O}'$ of level N in B' and embeddings $\psi_1 : \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ and $\psi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if one of the following two cases occurs.*

   - *$m = DN$, $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid (N/2)$, and $\left(\frac{-DN}{p}\right) = -1$*
   - *$m = DN/2$, $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid (N/2)$, and $\left(\frac{-DN/2}{p}\right) = -1$*

3. *Suppose $2 \mid D$ and $\left(\frac{-DN}{p}\right) = -1$. There is an Eichler order $\mathcal{O}'$ of level N in B' and embeddings $\psi_1 : \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ and $\psi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = DN$, $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid (D/2)$, $p \not\equiv 7 \bmod 8$, and $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid N$.*

4. *Suppose $2 \mid D$ and $\left(\frac{-DN}{p}\right) = 1$. There is an Eichler order $\mathcal{O}'$ of level N in B' and embeddings $\psi_1 : \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ and $\psi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = DN/2$,*

$DN \equiv 2, 6,$ or $10 \bmod 16$, $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid (D/2)$, $p \not\equiv 7 \bmod 8$, and $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid N$.

5. *Suppose that $p = 2$. There is an Eichler order $\mathcal{O}'$ of level N in B' and embeddings $\psi_1 : \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ and $\psi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ if and only if $m = DN \equiv \pm 3 \bmod 8$, $\left(\frac{-2}{q}\right) = -1$ for all primes $q \mid D$, and $\left(\frac{-2}{q}\right) = 1$ for all primes $q \mid N$.*

Proof. Suppose first that there exist embeddings $\psi_1 : \mathbf{Z}[\sqrt{-p}] \hookrightarrow \mathcal{O}'$ and $\psi_2 : \mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$ into some Eichler order $\mathcal{O}'$ of level N in B_{Dp}. Let $\omega_1 = \psi_1(\sqrt{-p})$ and $\omega_2 = \psi_2(\sqrt{-m})$, so $\mathcal{O}' \supset \{1, \omega_1, \omega_2, \omega_1\omega_2\}$. Since $(p, m) = 1$, $\mathbf{Z}[\sqrt{-p}] \notin \mathbf{Z}[\sqrt{-m}]$ and $\mathbf{Z}[\sqrt{-m} \notin \mathbf{Z}[\sqrt{-p}]$. Thus,

$$\mathcal{O}' \supset \mathbf{Z} \oplus \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2 \oplus \mathbf{Z}\omega_1\omega_2,$$

an order of reduced discriminant $4mp - s^2$ where s is the trace of $\omega_1\omega_2$. Therefore $DNp \mid 4mp - s^2$, and since $mp \mid DNp$, we must have $mp \mid s^2$. Since mp is squarefree, $mp \mid s$ and so either $mp \leq \mid s \mid$ or $s = 0$.

If $s \neq 0$ then $m^2p^2 \leq s^2 < 4mp$ and thus $mp < 4$. However, recall that m is an integer greater than one and p is a prime, so $mp \geq 4$. Therefore $s = 0$ and $mp \mid DNp \mid 4mp$. In fact, since DNp is squarefree, it divides the squarefree part of $4mp$. If $2 \nmid mp$ then $mp \mid DNp \mid 2mp$ and either $2 \nmid DN$ and $m = DN$ or $2 \mid DN$ and $m = DN/2$. If $2 \mid m$ then $mp \mid DNp \mid mp$ and so $m = DN$. If $p = 2$ then once more $mp \mid DNp \mid mp$ and so $m = DN$. Recall now that if n is squarefree and q is an odd prime then $\left\{\frac{4\Delta}{q}\right\} = \left(\frac{4\Delta}{q}\right) = \left(\frac{\Delta}{q}\right)$. Therefore Theorem 4.1.28 gives us the following congruence conditions.

- If $2 \nmid DNp$ then $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid N$, and $\left(\frac{-DN}{p}\right) = -1$.
- If $2 \mid N$ and $m = DN$ then $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid (N/2)$, and $\left(\frac{-DN}{p}\right) = -1$

- If $2 \mid N$ and $m = DN/2$ then $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid D$, $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid (N/2)$, and $\left(\frac{-DN/2}{p}\right) = -1$
- If $2 \mid D$ and $m = DN$, then $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid (D/2)$, $p \equiv \pm 3 \bmod 8$, and $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid N$.
- If $2 \mid D$ and $m = DN/2$, then $DN \equiv 2, 6, 10 \bmod 16$, $\left(\frac{-p}{q}\right) = -1$ for all primes $q \mid (D/2)$, $p \equiv \pm 3 \bmod 8$, and $\left(\frac{-p}{q}\right) = 1$ for all primes $q \mid N$.
- If $p = 2$ then $DN \equiv \pm 3 \bmod 8$, $\left(\frac{-2}{q}\right) = -1$ for all primes $q \mid D$, and $\left(\frac{-2}{q}\right) = 1$ for all primes $q \mid N$.

A word may be required on why we have no congruence conditions on p at 2 or $DN/2$ at 2 when $2 \mid N$. If $p \equiv 3 \bmod 4$ then $2 \mid f(-4p)$ and thus $\left\{\frac{-4p}{2}\right\} = 1$. If $p \equiv 1 \bmod 4$ then $2 \nmid f(-4p)$ and thus $\left\{\frac{-4p}{2}\right\} = \left(\frac{-4p}{2}\right) = 0$. The same holds for $DN/2$ since $DN/2$ is odd.

We now prove the converse when $2 \nmid DNp$. By Lemma 4.2.8(1), $B_{Dp} \cong B' = \left(\frac{-p,-DN}{\mathbf{Q}}\right)$. Contained in B' is the order $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}ij$ of reduced discriminant $4DNp$. If $p \equiv 3 \bmod 4$ then $\mathbf{Z} \oplus \mathbf{Z}\frac{1+i}{2} \oplus \mathbf{Z}j \oplus \mathbf{Z}\left(\frac{1+i}{2}\right)j$ is an appropriate order of discriminant DNp, and is thus an Eichler order of level N. Likewise if $DN \equiv 3 \bmod 4$ there is an appropriate Eichler order of level N. Assume now that $p \equiv 1 \bmod 4$. Then

$$\left(\frac{-DN}{p}\right) = \left(\frac{DN}{p}\right) = \prod_{q \mid DN} \left(\frac{q}{p}\right) = \prod_{q \mid DN} \left(\frac{p}{q}\right) = \prod_{q \mid DN} \left(\frac{-p}{q}\right)(-1)^r$$

where r is the number of primes $q \mid DN$ such that $q \equiv 3 \bmod 4$. Moreover, since D is the product of an even number of primes, $\left(\frac{-p}{q}\right) = -1$ if $q \mid D$, and $\left(\frac{-p}{q}\right) = 1$ if $q \mid N$, it follows that $\prod_{q \mid DN} \left(\frac{-p}{q}\right) = 1$. Putting this all together we have shown that if $p \equiv 1 \bmod 4$, then

$$-1 = \left(\frac{-DN}{p}\right) = \begin{cases} 1 & DN \equiv 1 \bmod 4 \\ -1 & DN \equiv 3 \bmod 4 \end{cases}.$$

We now prove the converse when $2 \mid N$ and $m = DN$. By Lemma 4.2.8(2), $B_{Dp} \cong B' = \left(\frac{-p,-DN}{\mathbf{Q}}\right)$. Contained in B' is the order $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}ij$ of reduced discriminant $4DNp$. If $p \equiv 3 \bmod 4$ then $\mathbf{Z} \oplus \mathbf{Z}\frac{1+i}{2} \oplus \mathbf{Z}j \oplus \mathbf{Z}\left(\frac{1+i}{2}\right)j$ is an appropriate order of discriminant DNp, and is thus an Eichler order of level N. If $p \equiv 1 \bmod 4$ then $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}\left(\frac{1+i+j}{2}\right) \oplus \mathbf{Z}\left(\frac{-1-i+ij}{2}\right)$ is an appropriate order of discriminant DNp.

We now prove the converse when $2 \mid N$ and $m = DN/2$. By Lemma 4.2.8(2), $B_{Dp} \cong B' = \left(\frac{-p,-DN/2}{\mathbf{Q}}\right)$. Contained in B' is the order $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}ij$ of reduced discriminant $2DNp$. It follows that the "Hurwitz quaternions" $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}\left(\frac{1+i+j+ij}{2}\right)$ are an appropriate Eichler order of discriminant DNp.

We now prove the converse when $2 \mid D$ and $m = DN$. By Lemma 4.2.8(3), $B_{Dp} \cong B' = \left(\frac{-p,-DN}{\mathbf{Q}}\right)$. Contained in B' is the order $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}ij$ of reduced discriminant $4DNp$. If $p \equiv 3 \bmod 8$ then $\mathbf{Z} \oplus \mathbf{Z}\frac{1+i}{2} \oplus \mathbf{Z}j \oplus \mathbf{Z}\left(\frac{1+i}{2}\right)j$ is an appropriate order of discriminant DNp, and is thus an Eichler order of level N. If $p \equiv 5 \bmod 8$ then $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}\left(\frac{1+i+j}{2}\right) \oplus \mathbf{Z}\left(\frac{-1-i+ij}{2}\right)$ is an appropriate order of discriminant DNp.

We now prove the converse when $2 \mid D$ and $m = DN/2$. By Lemma 4.2.8(4), $B_{Dp} \cong B' = \left(\frac{-p,-DN/2}{\mathbf{Q}}\right)$. Contained in B' is the order $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}ij$ of reduced discriminant $2DNp$. It follows that $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}\left(\frac{1+i+j+ij}{2}\right)$ are an appropriate Eichler order of discriminant DNp.

We now prove the converse when $p = 2$. By Lemma 4.2.8(5), $B_{Dp} \cong B' = \left(\frac{-2,-DN}{\mathbf{Q}}\right)$. Contained in B' is the order $\mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}ij$ of reduced discriminant $4DNp$. If $DN \equiv 3 \bmod 8$ then $\mathbf{Z} \oplus \mathbf{Z}\frac{1+j}{2} \oplus \mathbf{Z}i \oplus \mathbf{Z}\left(\frac{1+j}{2}\right)i$ is an appropriate order of discriminant DNp, and is thus an Eichler order of level N. If $DN \equiv 5 \bmod 8$ then $\mathbf{Z} \oplus \mathbf{Z}j \oplus \mathbf{Z}\left(\frac{1+i+j}{2}\right) \oplus \mathbf{Z}\left(\frac{-1-j+ij}{2}\right)$ is an appropriate order of discriminant DNp.

$\square$

Chapter 5

A Moduli Problem

We wish here to construct a scheme $X_0^D(N)_{/S}$ for any scheme S. Informally, we define it to be the coarse moduli scheme for QM-abelian surfaces with $\Gamma_0(N)$-structure. A reader who finds that definition sufficient and knows (even informally) how to define the Atkin-Lehner involutions may skip the first two sections and proceed on to section 5.3.

Section 5.3 concerns abelian varieties which are in the literature referred to as *superspecial*. These varieties will play a very important role in the remainder of this thesis. The reason is that the action of Galois on these surfaces can be understood using the theorems of chapter 4.

In order to state these results, we will first record some basics on abelian surfaces. After that, we record at length the different equivalent moduli problems which define the coarse moduli scheme $X_0^D(N)_{/S}$. Then we will recall some results on the explicit forms of the models of $X_0^D(N)_{\mathbf{Z}_p}$. Finally, after completing section 5.3, we will be able to prove the main theorems of this thesis.

Throughout this chapter, we will assume by convention that D is a squarefree product of an even number of primes and that N is squarefree and coprime to D.

5.1 Basics on Abelian Surfaces

Definition 5.1.1. *An* abelian scheme $A \to S$ *is a smooth, proper S-group scheme with connected fibers. This map has an identity section, which we denote $0 : S \to A$. If all geometric fibers of $A \to S$ have the same dimension d, we define* $\dim_S(A) := d$.

Definition 5.1.2. *If $A \to S$ is an abelian scheme, and $\gamma : A \to A$ is an S-morphism such that $\gamma 0 = 0$, we say that γ is an S-endomorphism of A. We denote the $\mathbf{Z}$-algebra of S-endomorphisms of A by* $\mathrm{End}_S(A)$.

Definition 5.1.3. *Let S be a scheme and let $(A_1, 0_1)$, $(A_2, 0_2)$ be abelian schemes over S. We say that ϕ is an* isogeny *if $\phi : A_1 \to A_2$ is a finite flat S-morphism such that $\phi 0_1 = 0_2$. In that case,* $\ker(\phi) := \phi^* 0_2(S)$ *is a finite flat subgroup scheme of A_1.*

Definition 5.1.4. *Let $\alpha_{p,\mathbf{Z}}$ be the group scheme such that for all rings R, $\alpha_p(R) = \{x \in R : x^p = 0\}$. If $k/\mathbb{F}_p$ is a field and $A_{/k}$ is an abelian variety such that there is no embedding of k-schemes $\alpha_{p,k} \hookrightarrow A[p]$ then we say that A is* ordinary.

Definition 5.1.5. *An* abelian surface $A_{/S}$ *is a two-dimensional abelian scheme over S.*

If $A_{/S}$ is an abelian surface, $s \in S$ is a closed point and A_s is an abelian variety over $k(s)$ then define $\mathrm{Lie}(A_s) := \mathrm{Hom}(\mathcal{O}_{A_s,0}, k(s)[\varepsilon]/(\varepsilon^2))$ [Liu02, Exercise 4.2.7]. Since A_s is nonsingular, $\mathrm{End}_{k(s)}(\mathrm{Lie}(A_s)) \cong M_2(k(s))$. By the definition of an endomorphism of an abelian scheme, there is a natural action of $\mathrm{End}_{k(s)}(A_s)$ on $\mathcal{O}_{A_s,0}$. It follows that there is a natural action of $\mathrm{End}_{k(s)}(A_s)$ on $\mathrm{Lie}(A_s)$. Moreover, if $k(s)$ has characteristic p, there is a natural action of $\mathrm{End}_{k(s)}(A_s)/(p)$ on $\mathrm{Lie}(A_s)$. Therefore, there is a homomorphism $\phi : \mathrm{End}_{k(s)}(A_s)/(p) \to M_2(k(s))$.

Suppose that ℓ is a finite subfield of $\mathrm{End}_{k(s)}(A_s)/(p)$ and consider the image of ℓ in $M_2(k(s))$. Since ℓ is separable over $\mathbb{F}_p$, the Jordan canonical form of any particular element of $\phi(\ell)$ has two Jordan blocks. Since ℓ is commutative, $\phi(\ell)$ is simultaneously diagonalizable if $k(s)$ is algebraically closed. It follows that if $k(s) = \overline{k(s)}$ then ϕ defines a pair of homomorphisms $\ell \to k(s)$.

Definition 5.1.6. *Let B_D be the quaternion algebra over $\mathbf{Q}$ of discriminant D and let $\mathcal{O}$ be a fixed Eichler order of level N in B_D with $(D, N) = 1$. An* abelian $\mathcal{O}$-surface $(A_{/S}, \iota)$ *is an abelian surface with an optimal embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}_S(A)$. If $\mathcal{O}$ is clear from context, we may refer to (A, ι) as a* QM-abelian surface.

Note that if $\iota : \mathcal{O} \hookrightarrow \mathrm{End}_S(A)$, then ι also induces $\mathcal{O}/N\mathcal{O} \hookrightarrow \mathrm{End}_S(A)/N\,\mathrm{End}_S(A)$. This is because if $f, g \in \iota(\mathcal{O})$ and $f - g \in N\,\mathrm{End}_S(A)$ then $f - g \in \iota(N\mathcal{O})$.

Definition 5.1.7. *A morphism of abelian $\mathcal{O}$-surfaces $f : (A_{/S}, \iota) \to (A'_{/S}, \iota')$ is an S-morphism $f : A \to A'$ such that $f\iota(\cdot) = \iota'(\cdot)f$. If the morphism f is an isogeny or isomorphism, we will say that $f : (A, \iota) \to (A', \iota')$ is an isogeny or isomorphism of abelian $\mathcal{O}$-surfaces.*

Let $\mathcal{O}$ be an Eichler order of level N in B_D with $(D, N) = 1$. Recall by Lemma 4.1.15 that if $p \mid D$, $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_{p^2} \oplus \mathbb{F}_{p^2}\pi_p$. Further recall that if $a \in \mathbb{F}_{p^2}$, π_p must be such that $a^p\pi_p = \pi_p a$

Definition 5.1.8. *Let $(A_{/S}, \iota)$ be an abelian $\mathcal{O}$-surface and $p \mid D$. Thus $\mathbb{F}_{p^2} \subset \mathcal{O}/p\mathcal{O}$ acts on $\mathrm{Lie}(A_s)$ through ι. For all closed points $s \in S$ such that $k(s)$ is algebraically closed of characteristic p, let $\sigma_s, \tau_s : \mathbb{F}_{p^2} \to k(s)$ the distinct embeddings. Consider $\mathrm{Lie}(A_s)$ as a $k(s)$-vector space and let $\mathrm{Lie}(A_s)[\phi]$ denote the subspace of $\mathrm{Lie}(A_s)$ on which $\mathbb{F}_{p^2} \subset \mathcal{O}/p\mathcal{O}$ acts through $\phi : \mathbb{F}_{p^2} \hookrightarrow k(s)$. We say that $(A_{/S}, \iota)$ is* mixed *if for all such $s \in S$, both $\mathrm{Lie}(A_s)[\sigma_s]$ and $\mathrm{Lie}(A_s)[\tau_s]$ are one-dimensional $k(s)$-vector spaces.*

Remark 5.1.9. *Notice that over $\mathbf{Z}[1/D]$-schemes, every abelian $\mathcal{O}$-surface is mixed.*

Definition 5.1.10. *Let $A \to S$ is an abelian scheme and $A^t \to S$ its dual abelian scheme [FC90, Theorem I.1.9]. If there exists a principal polarization $\Pi : A \tilde{\to} A^t$ [FC90, Definition*

I.1.6] then there is an involution on $\mathrm{End}_S(A)$ *given by* $\phi \mapsto \phi^\dagger = \Pi^{-1}\phi^t\Pi$ *called the* Rosati Involution *associated to* Π.

Recall that if $\mathcal{O}^D$ is a maximal order in B_D, then there exists some $\mu \in \mathcal{O}^D$ such that $\mu^2 + D = 0$ by Theorem 4.1.28. Denote by $\overline{\alpha}$ the main involution of $B_D = \mathcal{O}^D \otimes \mathbf{Q}$ applied to α as in Definition 4.1.6.

Definition 5.1.11. *Let* $(A_{/S}, \iota)$ *is an abelian* $\mathcal{O}^D$*-surface. Fix some* $\mu \in \mathcal{O}^D$ *such that* $\mu^2+D = 0$*. A* μ*-polarization on* (A,ι) *is a principal polarization of* A *such that* $\iota(\alpha)^\dagger = \iota(\mu^{-1}\overline{\alpha}\mu)$.

Lemma 5.1.12. *Let* $\mathcal{O}^D$ *be a maximal order in* B_D *and let* (A,ι) *is a mixed abelian* $\mathcal{O}^D$*-surface over a scheme* S*. If* $\mu \in \mathcal{O}^D$ *is such that* $\mu^2 + D = 0$*, then* A *has a* μ*-polarization.*

Proof. Over $\mathbf{Z}[1/D]$, a unique μ-polarization can be determined by a close examination of ℓ-divisible groups [Buz97, p.3]. Over $\mathbf{Z}_p$ for $p \mid D$, a unique μ-polarization may be determined using formal groups [Dri76, Proposition 4.3], [BC91, III.3.5]. To descend from $\mathbf{Z}_p$ to $\mathbf{Z}_{(p)}$, we use faithfully flat descent, that is, $\Pi_{\mathbf{Z}_p}$ descends down to $\mathbf{Z}_{(p)}$ if and only if $p_1^*\Pi = p_2^*\Pi$ where p_1, p_2 are the projections $\mathrm{Spec}(\mathbf{Z}_p \otimes_{\mathbf{Z}_{(p)}} \mathbf{Z}_p) \cong \mathrm{Spec}(\mathbf{Z}_p) \times_{\mathrm{Spec}(\mathbf{Z}_{(p)})} \mathrm{Spec}(\mathbf{Z}_p) \to \mathrm{Spec}(\mathbf{Z}_p)$[SGA03, Corollaire VIII.1.2]. But then $\mathbf{Z}_p \otimes_{\mathbf{Z}_{(p)}} \mathbf{Z}_p$ is a $\mathbf{Z}_p$-scheme so there is a unique μ-polarization using Drinfeld's result. Finally, we may glue the μ-polarizations over $\mathbf{Z}[1/D]$ and $\mathbf{Z}_{(p)}$ to obtain a μ-polarization over $\mathbf{Z}[p/D]$, and thus over $\mathbf{Z}$. □

Remark 5.1.13. *Although we shall only speak of the* μ*-polarization above, there may be other principal polarizations given to* A*, even some compatible in some way with* ι *[Rot04].*

5.2 Some Moduli Problems

We now list a few categories and functors of abelian surfaces. We will show that if two such functors have the same discrete invariants and base schemes, they are isomorphic as functors.

Moreover, they have coarse moduli spaces. These coarse moduli spaces will be what we will call Shimura curves.

Definition 5.2.1. *Suppose that $(D,N)=1$, $\mathcal{O}$ is an Eichler order of level N in B_D and S is a scheme. Let T be an S-scheme and let $\mathcal{C}_0^D(N)(T)$ denote the category whose objects are mixed abelian $\mathcal{O}$-surfaces $(A,\iota)_{/T}$ and whose morphisms $f:(A,\iota)\to(A',\iota')$ are isomorphisms $f:A\to A'$ such that for all $\alpha\in\mathcal{O}$, $f\iota(\alpha)=\iota'(\alpha)f$. For all objects (A,ι) of $\mathcal{C}_0^D(N)(T)$ define the equivalence class $[(A,\iota)]$ to be such that $[(A,\iota)]=[(A',\iota')]$ if there is a morphism $f:A\to A'$ of $\mathcal{C}_0^D(N)(T)$. Let $\mathcal{F}_0^D(N)_S$ denote the contravariant functor from the category of S-schemes to the category of sets defined as follows. If T is an S-scheme, define $\mathcal{F}_0^D(N)(T)$ to be the set of all equivalence classes $[(A,\iota)]$ where (A,ι) is an object of $\mathcal{C}_0^D(N)(T)$.*

Notice that $\mathcal{F}_0^D(N)_S$ is a functor because if $\phi:T\to T'$ is a morphism and (A,ι) is an object of $\mathcal{C}_0^D(N)(T')$ then we can form the base change morphism $b:A_T\to A$. Therefore, consider the embedding $b^*:\mathrm{End}_{T'}(A)\hookrightarrow\mathrm{End}_T(A_T)$, which induces a map of sets $\phi^*:\mathcal{C}_0^D(N)(T')\to\mathcal{C}_0^D(N)(T)$ by $(A,\iota)\mapsto(A_T,b^*\iota)$. Note that $b^*\iota:\mathcal{O}\hookrightarrow\mathrm{End}_T(A_T)$ is optimal. If not, there is a larger order $\mathcal{O}'\supset\mathcal{O}$ and an embedding $\epsilon:\mathcal{O}'\hookrightarrow\mathrm{End}_T(A_T)$ such that for all $\gamma\in\mathcal{O}$, $\epsilon(\gamma)=b^*\iota(\gamma)$. Recall now that $\mathcal{O}$ is the intersection of two maximal orders. Since $\mathcal{O}'$ is an order which properly contains $\mathcal{O}$, it must lie in exactly one of these maximal orders, which we now call $\mathcal{O}^D$. Since $[\mathcal{O}^D:\mathcal{O}]=N$, for all $\alpha\in\mathcal{O}'\smallsetminus\mathcal{O}$, $N\alpha\in\mathcal{O}$. Now since $b^*\iota(N\alpha)=\epsilon(N\alpha)=\epsilon(\alpha)[N]_{A_T}$, the kernel of $b^*\iota(N\alpha)$ contains the kernel of $[N]_{A_T}$. Since b^* is an embedding, the kernel of $\iota(N\alpha)$ admits an embedding of the kernel of $[N]_A$ and thus ι extends to an embedding $\mathcal{O}'\hookrightarrow\mathrm{End}_{T'}(A)$, in contradiction to the optimality of ι.

In addition to defining this moduli functor, we will define a natural tranformation of functors $w_q:\mathcal{F}_0^D(N)_S\to\mathcal{F}_0^D(N)_S$ for all schemes S. Suppose that $q\mid DN$ is prime so that there is a unique two-sided ideal $\mathfrak{Q}$ of $\mathcal{O}$ of norm q by Lemma 4.1.23. Since B_D is indefinite, all ideals are principal and thus there exists some $\beta_q\in\mathcal{O}$, unique up to multiplication by $\mathcal{O}^\times$ such that $\mathfrak{Q}=\beta_q\mathcal{O}=\mathcal{O}\beta_q$. Suppose that $\mathcal{O}$ is an Eichler order of level N in B_D and S is a scheme.

There is a self-bijection of $\mathcal{F}_0^D(N)_S(T)$ induced by $\mathfrak{Q}$ as follows. Let $w_q : [(A,\iota)] \mapsto [(A,\iota_{\beta_q})]$ where $\iota_{\beta_q}(x) = \iota(\beta_q)^{-1}\iota(x)\iota(\beta_q)$. Notice that if $u \in \mathcal{O}^\times$ then $\iota(u)$ induces an $\mathcal{O}$-equivariant isomorphism between $(A,\iota(\cdot))$ and $(A,\iota(u)^{-1}\iota(\cdot)\iota(u))$. Therefore $[(A,\iota_{\beta_q u})] = [(A,\iota_{\beta_q})]$ and thus $w_q[(A,\iota)]$ depends only on q. Notice also that if $s \in S$ is a closed point such that $k(s)$ is an algebraically closed field of characteristic $p \mid D$ then either $p \neq q$ and conjugating by $\iota(\beta_q)$ preserves $\mathrm{Lie}(A_s)[\sigma_s]$ and $\mathrm{Lie}(A_s)[\tau_s]$, or $p = q$ and conjugating by $\iota(\beta_p)$ interchanges them by Lemma 4.1.15.

Now consider that the following diagram commutes:

$$\begin{tikzcd}
\mathcal{F}_0^D(N)(T') \arrow[r, "w_q"] \arrow[d, "\phi^*"] & \mathcal{F}_0^D(N)(T') \arrow[d, "\phi^*"] \\
\mathcal{F}_0^D(N)(T) \arrow[r, "w_q"] & \mathcal{F}_0^D(N)(T),
\end{tikzcd}$$

so w_q defines a natural transformation $\mathcal{F}_0^D(N)_S \to \mathcal{F}_0^D(N)_S$. To see the diagram commutes, note first that $[(A_T, b^*(\iota_{\beta_q}(\cdot)))] = \phi^*[(A,\iota_{\beta_q})] = \phi^* w_q[(A,\iota)]$. For all $\alpha \in \mathcal{O}$,

$$b^*(\iota(\beta_q)^{-1}\iota(\alpha)\iota(\beta_q)) = (b^*\iota(\beta_q))^{-1} b^*\iota(\alpha) b^*\iota(\beta_q),$$

because b^* is a homomorphism. Since $[(A_T,(b^*\iota)_{\beta_q})] = w_q[(A_T, b^*\iota)] = w_q\phi^*[(A,\iota)]$, we see that for all elements of $\mathcal{F}_0^D(N)(T')$, $\phi^* w_q[(A,\iota)] = w_q\phi^*[(A,\iota)]$.

Definition 5.2.2. *For all $m \mid DN$ we define an automorphism $w_m : \mathcal{F}_0^D(N)_S \to \mathcal{F}_0^D(N)_S$ as the composition of w_q for all $q \mid m$ prime. We will call w_m the m-th* Atkin-Lehner involution. *Define the set W of all such w_m to be the* Atkin-Lehner group.

Note that by Lemma 4.1.23, the two-sided ideals form an abelian group, so the above definition of w_m makes sense.

Definition 5.2.3. *We say that (A,ι) is fixed by w_m if $[(A,\iota)] = [(A,\iota_{\beta_m})]$, where β_m is a generator of the unique integral two-sided ideal of $\mathcal{O}$ of norm m.*

Equivalently, (A,ι) is w_m-fixed if for all $\alpha \in \mathcal{O}$, $\iota(\beta_m)^{-1}\iota(\alpha)\iota(\beta_m) = \iota(\alpha)$. This is to say that $\iota(\beta_m)$ lies in the commutant of $\iota(\mathcal{O})$ in $\mathrm{End}_T(A)$. Let M be the two-sided ideal of $\mathcal{O}$ of norm m. Thus $\iota(M)$ is the unique integral two-sided ideal of norm m in $\iota(\mathcal{O})$. Since β_m generates M if and only if $\iota(\beta_m)$ generates $\iota(M)$, (A,ι) is w_m-fixed if and only if the commutant of $\iota(\mathcal{O})$ in $\mathrm{End}_T(A)$ contains a generator of $\iota(M)$.

Definition 5.2.4. *Suppose that $\mathcal{O}^D$ is a maximal order in B_D, $\mu \in \mathcal{O}^D$ such that $\mu^2 + D = 0$, S is a scheme and T is an S-scheme. Let $\mathcal{C}^D_\mu(N)(T)$ the category whose objects are isogenies of mixed abelian $\mathcal{O}^D$-surfaces $\phi : (A_{/T},\iota) \to (A'_{/T},\iota')$ such that $\phi^\dagger\phi = [N]_A$ where $()^\dagger$ is the Rosati involution associated to the unique μ-polarization on A. The morphisms $(\phi : (A,\iota) \to (A',\iota')) \to (\psi : (B,\epsilon) \to (B'\epsilon'))$ are pairs of isomorphisms $f : A \to B$, $g : A' \to B'$ such that for all $\alpha \in \mathcal{O}^D$, $f\iota(\alpha) = \epsilon(\alpha)f$, $g\iota'(\alpha) = \epsilon'(\alpha)g$ and $g\phi = \psi f$. For all objects $\phi : (A_{/T},\iota) \to (A'_{/T},\iota')$ of $\mathcal{F}^D_\mu(N)(T)$ let $[\phi]$ denote the equivalence class such that $[\phi] = [\psi]$ if there is a morphism (f,g) of $\mathcal{C}^D_\mu(N)(T)$ such that $g\phi = \psi f$. Let $\mathcal{F}^D_\mu(N)_S$ denote the contravariant functor from the category of S-schemes to the category of sets defined as follows. To an S-scheme T, we associate the set of all equivalence classes $[\phi]$ with ϕ an object of $\mathcal{C}^D_\mu(N)(T)$.*

Note that $\mathcal{F}^D_\mu(N)_S$ is a functor because isogenies pull back along morphisms of schemes. That is, fix a principal polarization of A and let $\phi : A \to A'$ be an isogeny of T'-schemes such that $\phi^\dagger\phi = [N]_A$. If $T \to T'$ is a morphism of schemes and $b : A_T \to A$ is the base change morphism, then let $\phi_T : A_T \to A'_T$ be the base change of ϕ along b. Likewise let $\phi^\dagger_T$ be the base change of $\phi^\dagger$. Since $b\phi^\dagger_T\phi_T = \phi^\dagger\phi b = [N]_A b = b[N]_{A_T}$, $\phi^\dagger_T\phi_T = [N]_{A_T}$.

Definition 5.2.5. *Suppose that $\mathcal{O}^D$ is a maximal order in B_D, $(D,N) = 1$, and S is a scheme. Let T be an S-scheme and let $\mathcal{C}^D_{\mathrm{cl}}(N)(T)$ denote the category whose objects are triples $(A,\iota,K)_{/T}$ where (A,ι) is a mixed abelian $\mathcal{O}^D$-surface and K is a closed $\mathcal{O}^D$-invariant subgroup scheme of $A[N]$ of order N^2. The morphisms $(A,\iota,K) \to (A',\iota',K')$ are isomor-*

phisms $f : A \to A'$ such that $f\iota(\cdot) = \iota'(\cdot)f$ and $f(K) = K'$. For all objects (A, ι, K) of $\mathcal{C}^D_{\mathrm{cl}}(N)(T)$, let $[(A, \iota, K)]$ denote the equivalence class such that $[(A, \iota, K)] = [(A', \iota', K')]$ if there is a morphism $f : (A, \iota, K) \to (A', \iota', K')$ which is a morphism of $\mathcal{C}^D_{\mathrm{cl}}(N)(T)$. Let $\mathcal{F}^D_{\mathrm{cl}}(N)_S$ denote the contravariant functor from the category of S-schemes to the category of sets defined as follows. To an S-scheme T we associate the set of all equivalence classes $[(A, \iota, K)]$ where (A, ι, K) is an object of $\mathcal{C}^D_{\mathrm{cl}}(N)(T)$.

Note for the following definition that if $\iota : \mathcal{O}^D \hookrightarrow \mathrm{End}_S(A)$, ι induces an embedding $[\iota/N] : \mathcal{O}^D \otimes \mathbf{Z}/N\mathbf{Z} \hookrightarrow \mathrm{End}_S(A) \otimes \mathbf{Z}/N\mathbf{Z}$.

Definition 5.2.6. *Suppose that $\mathcal{O}^D$ is a maximal order in B_D, $(D, N) = 1$, and S is a scheme. Let T be an S-scheme. For any fixed isomorphism $\psi : M_2(\mathbf{Z}/N\mathbf{Z}) \to \mathcal{O}^D \otimes \mathbf{Z}/N\mathbf{Z}$, let $e = \psi\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. With this data, define a category $\mathcal{C}^\psi(T)$ whose objects are triples $(A, \iota, K)_{/T}$ where (A, ι) is a mixed abelian $\mathcal{O}^D$-scheme and K is a closed subgroup scheme of $\ker([\iota/N](e))$ which is locally free of rank N. The morphisms $(A, \iota, K) \to (A', \iota', K')$ are isomorphisms $f : A \to A'$ such that $f\iota(\cdot) = \iota'(\cdot)f$ and $f(K) = K'$. Let $[(A, \iota, K)]_\psi$ denote the equivalence class of objects of $\mathcal{C}^\psi(T)$ such that $[(A, \iota, K)]_\psi = [(A', \iota', K')]_\psi$ if there is a morphism $f : (A, \iota, K) \to (A', \iota', K')$ of $\mathcal{C}^\psi(T)$. Let $\mathcal{F}^\psi_S$ be the contravariant functor from the category of S-schemes to the category of sets defined as follows. To an S-scheme T associate the set of all equivalence classes $[(A, \iota, K)]_\psi$ with (A, ι, K) an object of $\mathcal{C}^\psi(T)$.*

We note that these are functors because the rank of a finite group scheme is preserved under base change. We also note that for all T there is a natural "forgetful" functor $\mathcal{C}^D_{\mathrm{cl}}(N)(T) \to \mathcal{C}^D_{\mathrm{cl}}(1)(T)$ sending an object (A, ι, K) to $(A, \iota, \{0_A\}$ and a morphism f to itself.

Lemma 5.2.7. *The categories $\mathcal{C}^D_\mu(N)(T)$, $\mathcal{C}^D_{cl}(N)(T)$ and $\mathcal{C}^\psi(T)$ are equivalent for all maximal orders $\mathcal{O}^D$, for all μ such that $\mu^2 + D = 0$, for all $\psi : M_2(\mathbf{Z}/N\mathbf{Z}) \to \mathcal{O}^D \otimes \mathbf{Z}/N\mathbf{Z}$ and for all schemes S.*

Proof. Since N is square-free, it is equivalent to give a closed subgroup with is locally free of rank N and to give closed subgroups which are locally free of rank p for all $p \mid N$. That is, if K is such a subgroup, take $\ker([p]_A : K \to K)$ for all $p \mid N$ and if $\{K_p\}_{p|N}$ is a collection of such subgroups, take their product. Recall that if N is prime there is a bijection between the objects of $\mathcal{C}^D_\mu(N)(T)$, $\mathcal{C}^D_{cl}(N)(T)$ and $\mathcal{C}^\psi(T)$ [Buz97, pp. 8-9] and by the decomposition of K into groups of prime order, this bijection extends to all squarefree N.

Note that a morphism of $\mathcal{C}^D_{\mathrm{cl}}(N)(T)$ is a morphism of $\mathcal{C}^\psi(T)$ and vice versa. If (A,ι,K) is an object of $\mathcal{C}^\psi(T)$ and $t = \psi\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, then let $K' = tK$. It follows that an $\mathcal{O}^D$-equivariant isomorphism $f : A \to B$ fixes K if and only if f fixes $K \times K'$.

If $\phi : (A,\iota) \to (A',\iota')$ and $\psi : (B,\epsilon) \to (B',\epsilon')$ are objects of $\mathcal{C}^D_\mu(N)(T)$ and $(f : (A,\iota) \to (B,\epsilon), g : (A',\iota') \to (B',\epsilon'))$ is a morphism of $\mathcal{C}^D_\mu(N)(T)$ then f is $\mathcal{O}^D$-equivariant and $f(\ker\phi) = \ker\psi$. Therefore f is a morphism of $\mathcal{C}^D_{\mathrm{cl}}(N)(T)$. Conversely if $f : (A,\iota,K) \to (B,\epsilon,C)$ is a morphism of $\mathcal{C}^D_{\mathrm{cl}}(N)(T)$ and $g : A/K \to B/C$ induced by f then (f,g) is a morphism of $\mathcal{C}^D_\mu(N)(T)$. $\square$

Note also that by the proof above, especially the argument on subgroup schemes of prime or prime-power order, for all primes $p \mid N$, we have a pair of natural transformations of functors $\mathcal{F}^D_{\mathrm{cl}}(N)_S \to \mathcal{F}^D_{\mathrm{cl}}(N/p)_S \times_{\mathcal{F}^D_{\mathrm{cl}}(1)_S} \mathcal{F}^D_{\mathrm{cl}}(p)_S \to \mathcal{F}^D_{\mathrm{cl}}(N)_S$ which compose to the identity. We may thus use the forgetful functor $\mathcal{C}^D_{\mathrm{cl}}(p)(T) \to \mathcal{C}^D_{\mathrm{cl}}(1)(T)$ to define a "forgetful" natural transformation $\mathcal{F}^D_{\mathrm{cl}}(N)_S \to \mathcal{F}^D_{\mathrm{cl}}(N/p)_S$.

Lemma 5.2.8. *If S is a scheme then there are a pair of natural tranformations $\mathcal{F}^D_0(N)_S \to \mathcal{F}^D_{cl}(N)_S \to \mathcal{F}^D_0(N)_S$ which compose to the identity.*

Proof. We first note that considering these two functors, we are taking a choice of a maximal order $\mathcal{O}^D$ and a level N Eichler order $\mathcal{O}$, which we may take to be contained in $\mathcal{O}^D$. To give an isomorphism, pick a generator β_N of the unique two-sided ideal of norm N in $\mathcal{O}$. The interested reader is encouraged to notice the similarities to the approach of Molina[Mol10, Appendix]. This naturally determines a unit u such that $\beta_N^2 = Nu$ or rather that $\beta_N\beta_N u^{-1} = N$. This also realizes $\mathcal{O} = \mathcal{O}^D \cap \beta_N^{-1}\mathcal{O}^D\beta_N$ with index N in each. It follows that the unique two-sided $\mathcal{O}$-ideal of norm N is $\beta_N\mathcal{O} = \beta_N\mathcal{O}^D \cap \mathcal{O}^D\beta_N$ and the index of $\beta_N\mathcal{O}$ in each is N, and moreover that both $\beta_N\mathcal{O}^D$ and $\mathcal{O}^D\beta_N$ have index N in $\mathcal{O}$. Finally note that since u is a unit of $\mathcal{O}$, it is a unit of $\mathcal{O}^D$ and so $\beta_N u^{-1}\mathcal{O}^D = \beta_N\mathcal{O}^D$.

Let T be an S-scheme and let (A,ι) be an abelian $\mathcal{O}$-surface. Define abelian surfaces $A_0 := A/\ker_{\ker(\iota(\beta_N))}(\iota(\mathcal{O}^D\beta_N))$, $A_0' := A/\ker_{\ker(\iota(\beta_N u^{-1}))}(\iota(\beta_N u^{-1}\mathcal{O}^D))$ and let ρ,ρ' be the respective reduction morphisms.

Notice that we have taken A_0' to be isomorphic to $A/\ker_{\ker(\iota_{\beta_N\mathcal{O}}(\beta_N u^{-1}))}(\iota_{\beta_N\mathcal{O}}(\mathcal{O}^D\beta_N))$ under the definition of $\iota_{\beta_N\mathcal{O}}$ in Definition 5.2.2. We may take $\eta : A_0 \to A$, $\eta' : A_0' \to A$ such that $\eta\rho = \iota(\beta_N)$, $\eta'\rho' = \iota(\beta_N u^{-1})$. If we define $\phi_0 := \rho'\eta$ and $\phi_0' := \rho\eta'$ then

$$\eta\phi_0'\phi_0 = \iota(\beta_N)\iota(\beta_N u^{-1})\eta = [N]_A\eta = \eta[N]_{A_0}$$

so $\phi_0'\phi_0 = [N]_{A_0}$. In summary, the following diagram commutes.

$$\begin{tikzcd}
A_0 \arrow[r, "\phi_0"] \arrow[d, "\eta"] & A_0' \arrow[r, "\phi_0'"] \arrow[d, "\eta'"] & A_0 \arrow[d, "\eta"] \\
A \arrow[r, "\iota(\beta_N u^{-1})"'] \arrow[ur, "\rho'"] & A \arrow[r, "\iota(\beta_N)"'] \arrow[ur, "\rho"] & A
\end{tikzcd}$$

Since we have shown that the Atkin-Lehner involution w_N interchanges ϕ_0 and ϕ_0', $\#\ker(\phi_0) = \#\ker(\phi_0') = N^2$.

Now consider that $\beta_N u^{-1}\mathcal{O}^D \subset \mathcal{O}$, so that $\iota(\beta_N u^{-1}\alpha) \in \operatorname{End}_T(A)$. In fact, $\ker(\iota(\beta_N u^{-1})) \subset \ker(\iota(\beta_N u^{-1}\alpha))$, so $\rho\iota(\beta_N u^{-1}\alpha)\eta \in N\operatorname{End}_T(A_0)$. Note also that for all $\alpha,\gamma \in \mathcal{O}^D$,

$$\begin{aligned}\frac{1}{[N^2]_{A_0}}\rho\iota(\beta_N u^{-1}\alpha)\eta\rho\iota(\beta_N u^{-1}\gamma)\eta &= \frac{1}{[N^2]_{A_0}}\rho\iota(\beta_N u^{-1}\alpha)\iota(\beta_N\beta_N u^{-1}\gamma)\eta \\ &= \frac{1}{[N^2]_{A_0}}\rho\iota(\beta_N u^{-1}\alpha N\gamma)\eta \\ &= \frac{1}{[N]_{A_0}}\rho\iota(\beta_N u^{-1}\alpha\gamma)\eta\end{aligned}$$

Therefore we define $\iota_0 : \mathcal{O}^D \hookrightarrow \mathrm{End}_T(A_0)$ by $\iota_0(\alpha) = \frac{1}{[N]_{A_0}}\rho\iota(\beta_N u^{-1}\alpha)\eta$. Therefore, given an object (A,ι) of $\mathcal{C}_0^D(N)(T)$, we associate the object $(A_0, \iota_0, \ker(\phi_0))$ of $\mathcal{C}_{\mathrm{cl}}^D(N)(T)$. Suppose that (B,ϵ) is an object of $\mathcal{C}_0^D(N)(T)$ and as we obtained (ρ,ρ',η,η') from (A,ι), let us obtain $(\sigma,\sigma',\zeta,\zeta')$ from (B,ϵ). To a morphism $f:(A,\iota)\to(B,\epsilon)$ of $\mathcal{C}_0^D(N)(T)$, we associate the morphism $\frac{1}{[N]_{B_0}}\sigma f\eta'\phi_0 : (A_0,\iota_0)\to(B_0,\epsilon_0)$ of $\mathcal{C}_{\mathrm{cl}}^D(N)(T)$. We have thus defined a functor $\mathcal{C}_0^D(N)(T)\to\mathcal{C}_{\mathrm{cl}}^D(N)(T)$.

Now suppose that T is an S-scheme, (A_0,ι_0) is an abelian $\mathcal{O}^D$-surface and K a closed subgroup of A_0, locally free of rank N^2. Consider the closed subgroup scheme $K\cap\ker\iota_0(\beta_N)$, define $A := A_0/(K\cap\ker\iota(\beta_N))$ and let $\eta : A_0\to A$ be the reduction map. Let also $\rho : A\to \frac{A_0/K\cap\ker\iota_0(\beta_N)}{\ker(\iota_0(\beta_N))/(K\cap\ker(\iota_0(\beta_N)))}\cong\frac{A_0}{\ker(\iota_0(\beta_N))}\cong A_0$. Additionally define $\phi_0' : A_0/(K\cap\ker\iota(\beta_N))\to \frac{A_0/(K\cap\ker\iota(\beta_N))}{A_0[N]/(K\cap\ker\iota(\beta_N))}$. Note that $\frac{A_0/(K\cap\ker\iota(\beta_N))}{A_0[N]/(K\cap\ker\iota(\beta_N))}\cong\frac{A_0}{A_0[N]}\cong A_0$. Note that since $\beta_N\mathcal{O}=\mathcal{O}\beta_N$, $\iota_0(\mathcal{O})\ker(\iota_0(\beta_N))\subset\ker(\iota_0(\beta_N))$ and therefore ι_0 induces an embedding $\iota:\mathcal{O}\hookrightarrow\mathrm{End}_T(A)$.

More precisely, for all $\alpha\in\mathcal{O}$, define $\iota(\alpha)=\frac{1}{[N]_A}\eta\iota_0(\alpha)\phi_0'\rho'$. Moreover, this embedding ι is optimal because the set of $\alpha\in\mathcal{O}^D$ such that $\iota_0(\alpha)\ker(\iota_0(\beta_N))\subset\ker(\iota_0(\beta_N))$ is the set of $\alpha\in\mathcal{O}^D$ such that $\beta_N\alpha\in\mathcal{O}^D\beta_N$. This is to say that $\alpha\in\mathcal{O}^D\cap\beta_N^{-1}\mathcal{O}^D\beta_N = \mathcal{O}$ and therefore $\mathcal{O}$ is the largest order L in B_D such that ι_0 can induce an embedding $L\hookrightarrow\mathrm{End}_T(A)$. Therefore to an object (A_0,ι_0,K) of $\mathcal{C}_{\mathrm{cl}}^D(N)(T)$ we associate the object $(A_0/(K\cap\ker(\iota_0(\beta_N))), \frac{1}{[N]_A}\eta\iota_0(\cdot)\phi_0'\rho')$ of $\mathcal{C}_0^D(N)(T)$.

Suppose now that (B_0,ϵ_0,C) is another object of $\mathcal{C}_{\mathrm{cl}}^D(N)(T)$, and as we have obtained $(A_0',\phi_0,\phi_0',\eta,\rho,\rho')$ from (A_0,ι_0,K), let us obtain $(B_0',\psi_0,\psi_0',\zeta,\sigma,\sigma')$ from (B_0,ϵ_0,C). Suppose further that $f_0 : (A_0, \iota_0, K) \to (B_0, \epsilon_0, C)$ is a morphism in $\mathcal{C}^D_{\mathrm{cl}}(N)(T)$. Then we associate to f_0 the morphism $\frac{1}{[N]_B}\zeta f_0 \phi_0' \rho$ of $\mathcal{C}^D_0(N)$.

Note therefore that if (A, ι) is an object of $\mathcal{C}^D_0(N)(T)$, the object of $\mathcal{C}^D_0(N)(T)$ associated to $(A/\ker_{\ker(\iota(\beta_N))}(\iota(\mathcal{O}^D\beta_N)), \frac{1}{[N]_{A_0}}\rho\iota(\beta_N u^{-1}\cdot)\eta, \ker(\rho'\eta))$ is

$$\left(\frac{\frac{A}{\ker_{\ker(\iota(\beta_N))}(\iota(\mathcal{O}^D\beta_N))}}{\frac{(\ker(\rho'\eta)\cap\ker(\frac{1}{[N]_{A_0}}\rho\iota(\beta_N u^{-1}\beta_N)\eta))}{\ker_{\ker(\iota(\beta_N))}(\iota(\mathcal{O}^D\beta_N))}}, \frac{1}{[N]_A}\eta\frac{1}{[N]_{A_0}}\rho\iota(\beta_N u^{-1}\cdot)\eta\phi_0'\rho' \right)$$

Note first that $\rho\iota(\beta_N u^{-1}\beta_N)\eta = \rho\eta'\rho'\eta\rho\eta = [N]_{A_0}\rho\eta$. Therefore

$$\frac{\frac{A}{\ker_{\ker(\iota(\beta_N))}(\iota(\mathcal{O}^D\beta_N))}}{\frac{(\ker(\rho'\eta)\cap\ker(\frac{1}{[N]_{A_0}}\rho\iota(\beta_N u^{-1}\beta_N)\eta))}{\ker_{\ker(\iota(\beta_N))}(\iota(\mathcal{O}^D\beta_N))}} \xrightarrow{\sim} \frac{A_0}{\ker(\rho'\eta)\cap\ker(\rho\eta)} \xrightarrow{\sim} \frac{A}{\ker(\rho')\cap\ker(\rho)} \cong A,$$

because $\ker(\rho')\cap\ker(\rho) = 0$.

Note now that $\eta\phi_0'\rho' = [N]_A$ so that $\frac{1}{[N]_A}\eta\frac{1}{[N]_{A_0}}\rho\iota(\beta_N u^{-1}\cdot)\eta\phi_0'\rho' = \eta\frac{1}{[N]_{A_0}}\rho\iota(\beta_N u^{-1}\cdot) = \frac{1}{[N]_A}\eta\rho\iota(\beta_N u^{-1})\iota(\cdot) = \frac{1}{[N]_A}\iota(\beta_N\beta_N u^{-1})\iota(\cdot) = \iota(\cdot)$.

Note also that the functor $\mathcal{C}^D_0(N)(T) \to \mathcal{C}^D_0(N)(T)$ takes a morphism f to

$$\frac{1}{[N]_B}\zeta\left(\frac{1}{[N]_{B_0}}\sigma f\eta'\phi_0\right)\phi_0'\rho' = \frac{1}{[N^2]_B}\epsilon(\beta_N)f\eta'\rho'(\eta\phi_0'\rho') = \frac{1}{[N]_B}\epsilon(\beta_N\beta_N u^{-1})f = f.$$

$\square$

Remark 5.2.9. *It may be interesting to produce a proof of the above using Serre's tensor product construction.*

Recall now that if $A_{/S}$ is an abelian scheme and $\iota : \mathcal{O}^D \hookrightarrow \mathrm{End}_S(A)$ then there is a natural left action of $\mathcal{O}^D$ on $A[n]$ for any positive integer n. Similarly, there is a natural left action of $\mathcal{O}^D$ on $\mathcal{O}^D\otimes\mathbf{Z}/n\mathbf{Z}$. Note also that since $\mathcal{O}^D \cong \mathbf{Z}^4$ as an additive group, $\mathcal{O}^D\otimes\mathbf{Z}/n\mathbf{Z} \cong (\mathbf{Z}/n\mathbf{Z})^4$ as an additive group. Therefore if we denote by $(\mathcal{O}^D\otimes\mathbf{Z}/n\mathbf{Z})_S$ the constant group scheme over S with the natural left action of $\mathcal{O}^D$, the following definition makes sense.

Definition 5.2.10. *Let $\mathcal{O}^D$ be a maximal order in B_D, S a scheme and $(A_{/S}, \iota)$ an abelian $\mathcal{O}^D$-surface. Let n be an integer coprime to D. A* full level n structure *on an abelian $\mathcal{O}^D$-surface is an isomorphism of group schemes $\nu : (\mathcal{O}^D \otimes \mathbf{Z}/n\mathbf{Z})_S \xrightarrow{\sim} A[n]$ commuting with the action of each as a left $\mathcal{O}^D$-module.*

Lemma 5.2.11. *Suppose that S is a $\mathbf{Z}[1/n]$-scheme and $(D,n) = 1$. Fix an isomorphism $\psi : M_2(\mathbf{Z}/n\mathbf{Z})_S \to (\mathcal{O}^D \otimes \mathbf{Z}/n\mathbf{Z})_S$ and let $e = \psi \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. It is equivalent to give a full level n structure to a QM abelian surface (A, ι) and to give an isomorphism* $\ker(e) \cong (\mathbf{Z}/n\mathbf{Z})_S^2$.

Proof. Let ν be a full level n structure on (A, ι). Set $t = \psi \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, which induces an isomorphism between $\ker(e)$ and $\ker(1-e)$. Since for any idempotent we have an exact sequence

$$0 \to \ker(e) \to A[n] \xrightarrow{e} eA[n] \to 0$$

with a splitting given by $1-e$, we have $\ker(e) \cong (1-e)A[n] \cong (\mathbf{Z}/n\mathbf{Z})_S^2$.

Conversely, suppose we have an isomorphism $\ker(e) \cong (\mathbf{Z}/n\mathbf{Z})_S^2$. We still have $\ker(e) \cong (1-e)A[n]$ by splitting the exact sequence above and since $\ker(e) \cong \ker(1-e)$ we can pick $P_1, P_2 \in eA[n]$ mapping to $(1,0)$, $(0,1)$ under our isomorphism $eA[n] \cong \ker(1-e) \cong \ker(e) \cong (\mathbf{Z}/n\mathbf{Z})_S^2$. Note that since there exist $P_1', P_2' \in A[n]$ such that $P_i = eP_i'$ so $eP_i = e^2 P_i' = eP_i' = P_i$. Note also that $P_3 = tP_1$ and $P_4 = tP_2$ realize $(1-e)A[n] \cong \ker(e) \cong (\mathbf{Z}/n\mathbf{Z})_S^2$ and similarly $(1-e)P_{2+i} = tet^2eP_i' = te^2P_i' = teP_i' = tP_i = P_{2+i}$. Under ψ, $\{e, et, te, tet\}$ forms the standard $(\mathbf{Z}/n\mathbf{Z})_S$ generating set of $M_2(\mathbf{Z}/n\mathbf{Z})_S$ by elementary matrices. Therefore, identifying $aP_1 + bP_2 + cP_3 + dP_4$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ determines a left $\mathcal{O}^D$-linear isomorphism between $A[n]$ and $M_2(\mathbf{Z}/n\mathbf{Z})_S \cong (\mathcal{O}^D \otimes \mathbf{Z}/n\mathbf{Z})_S$. ∎

Theorem 5.2.12 (Čerednik-Drinfeld). *Let $n \geq 3$ be an integer and $D > 1$. Consider the functor $\mathcal{F}^D(n)$ sending a $\mathbf{Z}[1/n]$-scheme S to the set of all $(A_{/S}, \iota, \nu)$ up to S-isomorphism where $(A_{/S}, \iota)$ is a mixed abelian $\mathcal{O}_D$-surface and ν is a full level n structure on (A, ι). The functor $\mathcal{F}^D(n)$ is representable by a projective $\mathbf{Z}[1/n]$-scheme which we denote $X^D(n)$.*

Proof. This theorem is [Dri76, Proposition 4.4]. □

It is well-known that $\mathcal{F}^1(n)$ is *not* represented by a proper scheme, but there is a natural compactification of the scheme which represents $\mathcal{F}^1(n)$ which has been well-studied.

Theorem 5.2.13. *Let $n \geq 3$ and let $\mathcal{O}^1$ be a maximal order in $B_1 \cong M_2(\mathbf{Q})$. Let $\mathcal{F}'(n)$ denote the contravariant functor from the category of schemes to the category of sets as follows. To a scheme S, associate the set of S-isomorphism classes of (A, ι, ν) where ν is a full level n structure and A is either an abelian $\mathcal{O}$-surface or the square of a Néron n-gon in the sense of [DR73, II.3.1]. Then $\mathcal{F}'(n)$ is representable by a smooth, projective $\mathbf{Z}[1/n]$-scheme which we denote $X^1(n)$.*

Note that in the setting of elliptic curves, it is more common to refer to $X^1(n)$ as $X(n)$ [Sil92, p.354].

Proof. We first note that $\mathcal{F}^1(n)$ is naturally a subfunctor of $\mathcal{F}'(n)$. If we can show that $\mathcal{F}^1(n)$ actually sends T to the set of T-isomorphism classes of elliptic curves with level n structures, we are done [DR73, Corollaire IV.2.9] because by Lemma 5.2.11 we are using the same definition of a level structure as Deligne and Rapoport. Since $D = 1$, $\mathcal{O}^1$ contains nontrivial idempotents e. A nontrivial idempotent in $\mathcal{O}^1 \cong M_2(\mathbf{Z})$ gives a decomposition of A as E^2 with $E \cong \ker(e) \cong \ker(1-e)$ an elliptic curve. □

Corollary 5.2.14. *Let $n \geq 3$ a multiple of N coprime to D such that $(N, n/N) = 1$. Let S be a flat $\mathbf{Z}[1/n]$-scheme and T an S-scheme. Let $\mathcal{O}$ be an Eichler order of level N in B_D and $\mathcal{O}^D$ a maximal order containing $\mathcal{O}$. We may define an action of $g \in \Gamma = (\mathcal{O} \otimes \mathbf{Z}/n\mathbf{Z})^\times$ on*

$X^D(n)$ by $(A_{/T}, \iota : \mathcal{O}^D \hookrightarrow \mathrm{End}_T(A), \nu) \mapsto (A_{/T}, \iota, \nu g)$ since $\mathcal{O}^D \supset \mathcal{O}$. The quotient $X^D(n)/\Gamma$ is a coarse moduli scheme for $\mathcal{F}_0^D(N)_S$.

Proof. First, we may assume $D > 1$ [DR73, Proposition IV.3.10].

To obtain a coarse moduli space, we must have a stack. We shall show that over $\mathbf{Z}[1/n]$, the quotient functor $\mathcal{F}^D(n)/\Gamma$ agrees with $\mathcal{F}_0^D(N)$. The quotient functor is represented by a stack in the étale topology on S, in fact the Deligne-Mumford quotient stack $[X^D(n)/\Gamma]$ since the constant group scheme Γ is étale [LMB00, 4.6.1]. The result follows [DR73, I.8.2.2] once we show that $\mathcal{F}_0^D(N)$ is the appropriate quotient functor. The following is essentially an expansion of Buzzard's Lemma 4.4 [Buz97].

Let T be an S-scheme and $(A, \iota, [\nu]_\Gamma)$ an object of $\mathcal{F}^D(n)/\Gamma(T)$. Since Γ is étale, there is, after an étale base extension $T' \to T$, a full level structure ν on $A_{T'}$. Since finite étale maps are fpqc, and there is an equivalence of categories between quasi-coherent T-modules and quasi-coherent T'-modules with descent data [BLR90, Theorem 6.4], there is no harm in working with $(A_{T'}, \iota : \mathcal{O} \hookrightarrow \mathrm{End}_T(A) \hookrightarrow \mathrm{End}_{T'}(A_{T'}), \nu)$ and descent data given by the action of Γ.

To fix ideas, fix an isomorphism $\psi : M_2(\mathbf{Z}/N\mathbf{Z}) \to \mathcal{O}^D \otimes \mathbf{Z}/N\mathbf{Z}$ and $\mathcal{O} \cong \mathcal{O}_0^D(N)$. Define $\mathcal{O}_0^D(N)$ to be the set of elements of $\mathcal{O}^D$ which become upper-triangular in $\mathcal{O}^D \otimes \mathbf{Z}/N\mathbf{Z}$ via ψ. By Theorem 4.1.21, $\mathcal{O}$ is conjugate to $\mathcal{O}_0^D(N)$, so without loss of generality we assume $\mathcal{O} = \mathcal{O}_0^D(N)$. Since $n = Nd$ with $(d, N) = 1$, $\mathcal{O}^D \otimes \mathbf{Z}/n\mathbf{Z} \cong \mathcal{O}^D \otimes \mathbf{Z}/N\mathbf{Z} \oplus \mathcal{O}^D \otimes \mathbf{Z}/d\mathbf{Z}$ as left $\mathcal{O}^D$-modules. Consider the element of $\mathcal{F}_0^D(N)(T')$ given by $(A, \iota, \nu(M))$ with $M = \begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix} \oplus \{0\} \subset \mathcal{O}^D \otimes \mathbf{Z}/N\mathbf{Z} \oplus \mathcal{O}^D \otimes \mathbf{Z}/d\mathbf{Z}$. Observe that the subgroup M is invariant under the (right multiplication) action of $(\mathcal{O} \otimes \mathbf{Z}/n\mathbf{Z})^\times$, so the triple $(A, \iota, \nu(M))$ descends down to T.

Conversely, we know that since we are working over a $\mathbf{Z}[1/n]$-scheme, after an étale extension $S' \to S$, there is an isomorphism $A[n] \cong (\mathbf{Z}/n\mathbf{Z})^4_{T'}$. Let e be an idempotent of

$\mathcal{O}^D \otimes \mathbf{Z}/n\mathbf{Z}$. Since $\ker(e) \cong \ker(1-e)$ and $A[n] \cong \ker(e) \times \ker(1-e)$, $\ker(e) \cong (\mathbf{Z}/n\mathbf{Z})^2_T$ and therefore by Lemma 5.2.11, there is a level n structure ν. This level structure is not unique, but the choice of any two level structures ν, ν' determines an isomorphism $g : M_2(\mathbf{Z}/n\mathbf{Z}) \to M_2(\mathbf{Z}/n\mathbf{Z})$ such that $\nu' = \nu g$. Note here that the automorphisms of $M_2(\mathbf{Z}/n\mathbf{Z})$ are exactly $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$.

Suppose now that K is a subgroup of $\ker(e)$ which is locally free of rank N and K' is its isomorphic image in $\ker(1-e)$. Make an étale base extension $T' \to T$ so that there exist isomorphisms $\ker(e) \cong (\mathbf{Z}/n\mathbf{Z})^2_{T'} \cong (\mathbf{Z}/N\mathbf{Z})^2_{T'} \times (\mathbf{Z}/d\mathbf{Z})^2_{T'}$ and thus $\psi : \mathbf{Z}/N\mathbf{Z}_{T'} \to K$ and $\psi' : \mathbf{Z}/N\mathbf{Z}_{S'} \to K'$. Let $P_2 = \psi(1)$ and $P_4 = \psi'(1)$ as in the proof of Lemma 5.2.11, and let ν be a level structure extending these. The choice of ν fixing $K \times K'$ is not unique, but all others are given by the right multiples by a subgroup of $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) \cong \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z}) \oplus \mathrm{GL}_2(\mathbf{Z}/d\mathbf{Z})$. In particular, as we have identified $K \times K'$ with the subgroup $\begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix} \oplus \{0\}$ of $M_2(\mathbf{Z}/N\mathbf{Z}) \oplus M_2(\mathbf{Z}/d\mathbf{Z})$, $K \times K'$ is fixed under right multiplication by $g \in \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ if and only if g is upper-triangular modulo N. Therefore we map $(A_{/T'}, \iota, K \times K')$ to $(A_{T'}, \iota, \nu)$. Moreover we may choose $T' \to T$ with descent data given by right multiplication by Γ, inducing a map $\mathcal{F}^D_0(N)(T) \to \mathcal{F}^D(n)/\Gamma(T)$ by $(A_{/T}, \iota, K \times K') \mapsto (A_{/T}, \iota, [\nu]_\Gamma)$. □

Remark 5.2.15. *Note that this definition is independent of the choice of n used in Corollary 5.2.14, so $X^D_0(N)_S$ may be defined for any scheme S over $\mathbf{Z}[1/N]$.*

Definition 5.2.16. *Let $X^D_0(N)_{/S}$ be the coarse moduli scheme given in Corollary 5.2.14.*

Note that by the definition of a coarse moduli space [DR73, Definition I.8.1], if $k = \overline{k}$ and $\mathcal{S}$ is the coarse moduli space for a functor $\mathcal{F}$, then $\mathcal{F}(k)$ is in natural bijection with $\mathcal{S}(k)$.

Definition 5.2.17. *If an abelian $\mathcal{O}$-surface (A, ι) over k has a certain property (e.g., being w_m-fixed or* superspecial *in the sense of Definition 5.3.6) then we may also say that the point $x : \mathrm{Spec}(k) \to X^D_0(N)$ corresponding to (A, ι) has that property.*

We now state some theorems on explicit descriptions of $X_0^D(N)_S$ over various schemes S.

Theorem 5.2.18. *If S is a flat $\mathbf{Z}[1/DN]$-scheme, then $X_0^D(N)_{/S}$ is smooth.*

Proof. This is generally attributed to Y. Morita in his Master's Thesis [Mor70]. Milne shows that $X_0^D(1)_{\mathbf{Z}[1/D]}$ is smooth [Mil79, p.172]. Over $\mathbf{Z}[1/DN]$, the map $X_0^D(N) \to X_0^D(1)$ is étale and therefore $X_0^D(N)$ is smooth over $\mathbf{Z}[1/DN]$. □

Definition 5.2.19. *Let D, N be positive square-free integers and let $\mathcal{O}$ be an Eichler order of level N in B_D. Define* $\mathrm{Pic}(D,N)$ *to be the set of isomorphism classes of right $\mathcal{O}$-ideals.*

Lemma 4.1.21 shows that $\mathrm{Pic}(D,N) = \{[\mathcal{O}]\}$ when B_D is indefinite. When B_D is definite, there exist formulas for the size of $\mathrm{Pic}(D,N)$ [Piz76, Theorem 16].

Definition 5.2.20. *For $[I]$ in* $\mathrm{Pic}(D,N)$*, the* length *is* $\ell([I]) := \#(\mathcal{O}_l(I)^\times/\pm 1)$.

We shall use the length to make sense of the reduction $X_0^D(N)_{\mathbb{F}_p}$ when $p|D$.

Definition 5.2.21. *We say a normal, proper, flat relative curve $M_{/\mathbf{Z}_p}$ is a* Mumford curve *if each component of the special fiber is isomorphic over $\mathbb{F}_p$ to $\mathbb{P}^1_{\mathbb{F}_p}$ and the intersection points are all $\mathbb{F}_p$-rational double points.*

Theorem 5.2.22. *Let $p \mid D$. There is a Mumford curve $M_{(D,N)/\mathbf{Z}_p}$ whose components over $\mathbb{F}_p$ are in bijection with two copies of* $\mathrm{Pic}(D/p,N)$ *interchanged by an involution a_p of $M_{(D,N)}$, whose intersection points are in bijection with* $\mathrm{Pic}(D/p,Np)$*, and whose dual graph is bipartite. Moreover let x be an intersection point between two components of $(M_{(D,N)})_{\mathbb{F}_p}$ corresponding to $[I] \in$* $\mathrm{Pic}(D/p,Np)$*. Then the following holds:*

$$\widehat{\mathcal{O}_{M_{(D,N)},x}} \cong \mathbf{Z}_p[[X,Y]]/(XY - p^{\ell([I])}).$$

Most importantly, there is an isomorphism $\phi : X_0^D(N)_{\mathbf{Z}_{p^2}} \tilde{\to} (M_{(D,N)})_{\mathbf{Z}_{p^2}}$ *such that* $\phi w_p = a_p \phi$. *If* $\langle\sigma\rangle = \mathrm{Aut}_{\mathbf{Z}_p}(\mathbf{Z}_{p^2})$, *this isomorphism realizes* $X_0^D(N)_{\mathbf{Z}_p}$ *as the étale quotient of* $(M_{(D,N)})_{\mathbf{Z}_{p^2}}$ *by the action of* σa_p.

Proof. Although this was first done in the case $N = 1$ by Kurihara [Kur79, §5], a proof for general level can be found in many places [Ogg85, p.201-202],[Cla03, Corollary 78]. In particular, the relation between $M_{(D,N)}$ and $X_0^D(N)_{\mathbf{Z}_p}$ can be deduced as follows. In the notation of Clark [Cla03, p.54], $M_{(D,N)}$ may be defined as $\Gamma_+\backslash\mathcal{P}$. In the notation of Ogg [Ogg85, p.201], the dual graph of $(M_{(D,N)})_{\mathbb{F}_p}$ may be explicitly given as Δ/Γ_+. Also in Ogg's notation, Vertices(Δ/Γ) = Vertices$(\Delta)/\Gamma$ is in natural bijection with $\mathrm{Pic}(D/p, N)$ and the directed edges of Δ/Γ are in bijection with $\mathrm{Pic}(D/p, Np)$ where Γ/Γ_+ is generated by a_p. Finally we note that for all I, $\ell([I])$ may be realized as a certain stabilizer in Γ. $\square$

Remark 5.2.23. *Thinking of the dual graph in this way yields an algorithm to compute dual graphs which the author has implemented in* `MAGMA`*[BCP97]. If we fix* $\mathcal{O} \supset \mathcal{O}^D$, *it is possible to effectively compute representatives* $\{I_1, \dots, I_a\}$ *for* $\mathrm{Pic}(\mathcal{O}^D)$ *and* $\{J_1, \dots, J_b\}$ *for* $\mathrm{Pic}(\mathcal{O})$. *Under the reduction map* $\Delta/\Gamma_+ \to \Delta/\Gamma$ *the* origin *of* J_j *is the unique* I_i *such that* $J_j\mathcal{O}^D \cong I_i$. *Also, via the* `PrimeIdeal` *command, we may compute the unique two-sided integral ideal* $\wp$ *of* $\mathcal{O}$. *Therefore we may compute* $w_p[J_j] = [J_j\wp]$ *in the style of Theorem 5.3.14. The terminus of* J_j *is then the origin of* $[J_j\wp]$.

For a ring A of characteristic p, let $W(A)$ denote the Witt vectors of A [Ser79, §II.6]. Recall that N is always assumed to be square-free.

Theorem 5.2.24. *Fix a maximal order* $\mathcal{O}^D$ *in* B_D, *a square root* μ *of* $-D$ *in* $\mathcal{O}^D$, *and let* $p \mid N$. *Let* $S = \mathrm{Spec}(R)$ *be a flat* $\mathbf{Z}_{(p)}$*-scheme and consider* $\mathcal{F}_\mu^D(N)$ *to be the functor of Definition 5.2.4. Then for all* μ, $\mathcal{F}_\mu^D(N)$ *admits a coarse moduli scheme* $X_0^D(N)_{/S}$. *If* T *is an* $\mathbb{F}_p$*-scheme then there is a closed embedding* $c : X_0^D(N/p)_T \to X_0^D(N)_T$. *Moreover if* T *is an* S*-scheme and if* $\Phi : X_0^D(N)_T \to X_0^D(N/p)_T$ *is the forgetful map* $X_0^D(N) \cong X_0^D(N/p) \times_{X_0^D(1)} X_0^D(p) \to$

$X_0^D(N/p)$, *then* Φc *is the identity and* $\Phi w_p c$ *is the Frobenius map* $(A, \iota) \mapsto (A^{(p)}, \mathrm{Frob}_{p,*}\, \iota)$ *(see Definition 6.0.3). Moreover,* $X_0^D(N)_T$ *fits into the following diagram*

$$\begin{tikzcd}
X_0^D(N/p)_T \arrow[dr, "c"] \arrow[dd, "id"'] & & X_0^D(N/p)_T \arrow[dl, "w_p c"'] \arrow[dd, "id"] \\
& X_0^D(N)_T \arrow[dl, "\Phi"'] \arrow[dr, "\Phi w_p"] & \\
X_0^D(N/p)_T & & X_0^D(N/p)_T
\end{tikzcd}$$

If t *is a closed point of* T *such that* $k(t) = \overline{k(t)}$, *the intersection of* $c(X_0^D(N/p)(k(t)))$ *and* $w_p c(X_0^D(N/p)(k(t)))$ *is precisely the set of superspecial points (in the sense of Definition 5.3.6), which are in bijection with* $\mathrm{Pic}(Dp, N/p)$. *Moreover, for each superspecial point* x *over* t *corresponding to* $[I] \in \mathrm{Pic}(Dp, N/p)$, *the strictly henselian complete local ring of* $X_0^D(N)$ *at* x *is isomorphic to* $R \otimes W(\overline{\mathbb{F}}_p)[[X, Y]]/(XY - p^{\ell([I])})$.

Proof. The bijection between superspecial points and $\mathrm{Pic}(Dp, N/p)$ is Theorem 5.3.10. The actual result is Theorem 1.7.2 of David Helm's PhD thesis [Hel03] and was later published [Hel07, Theorem 10.3]. To recognize this more easily, note that Helm's embedding Frob is c here and Helm's embedding Ver is $w_p c$. $\square$

Lemma 5.2.25. *The components and singular points of the* $\overline{\mathbb{F}}_p$ *special fiber can be put into the following* W*-equivariant bijections.*

	Components	*Intersection Points*
$p \mid D$	$\mathrm{Pic}(D/p, N) \coprod \mathrm{Pic}(D/p, N)$	$\mathrm{Pic}(D/p, Np)$
$p \mid N$	$\mathrm{Pic}(D, N/p) \coprod \mathrm{Pic}(D, N/p)$	$\mathrm{Pic}(Dp, N/p)$

Moreover, if $p \mid D$, *the bijection of a set of components with* $\mathrm{Pic}(D/p, N)$ *is* $W/\langle w_p \rangle$*-equivariant with* w_p *interchanging each. If* $p \nmid DN$, *the superspecial points of* $X_0^D(N)_{\overline{\mathbb{F}}_p}$ *can be put into* W*-equivariant bijection with* $\mathrm{Pic}(Dp, N)$ *via the embedding* $c : X_0^D(N)_{\overline{\mathbb{F}}_p} \to X_0^D(Np)_{\overline{\mathbb{F}}_p}$.

Proof. This is a summary of a part of Theorem 1.1 in [Mol10]. For $p \mid D$ this lemma may be deduced from Theorem 5.3 of [Rib89], which gives a natural bijection between the components and intersection points and certain types of superspecial surfaces. For $p \mid N$, this may be deduced from Theorem 1.7.2 in [Hel03]. $\square$

Let S be an irreducible, faithfully flat $\mathbf{Z}_p$-scheme and let η be its generic point. Since $X_0^D(N)_{/S}$ may have quotient singularities, it may not be a regular scheme. For this reason, we reserve the word *model* for a regular proper scheme $\mathcal{X}_{/S}$ whose generic fiber is $X_0^D(N)_\eta$. We may obtain such a scheme by resolving the singularities on $X_0^D(N)$ [Liu02, Example 8.3.50].

5.3 Superspecial surfaces

Fix a prime number p and a maximal order $\mathcal{S}$ in the quaternion algebra B_p over $\mathbf{Q}$ ramified precisely at p and ∞. By a theorem of Deuring, there is a supersingular elliptic curve E over the algebraic closure $\mathbb{F}$ of $\mathbb{F}_p$ such that $\mathrm{End}_{\mathbb{F}}(E) \cong \mathcal{S}$ [Rib89, p.23].

Definition 5.3.1. *Fix $E_{/\mathbb{F}}$, a* supersingular *elliptic curve with $\mathrm{End}_{\mathbb{F}}(E) \cong \mathcal{S}$. We say that an abelian variety $A_{/\mathbb{F}}$ is supersingular when there is an isogeny $A \to E^{\dim(A)}$.*

Note that if $E'_{\mathbb{F}}$ is supersingular then E is isogenous to E' so the above definition does not depend on the choice of E.

Theorem 5.3.2. *[Cla03, Appendix]If A is an abelian surface defined over $\mathbb{F}_q$, then the only possibilities for $\mathrm{End}^0_{\mathbb{F}_q}(A)$ are the following.*

1. *A quartic CM field.*

2. *A quaternion algebra over an imaginary quadratic number field K in which p splits. The discriminant of this quaternion algebra is $p\mathbf{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$.*

3. A product of distinct imaginary quadratic fields $K_1 \times K_2$.

4. The product $B_p \times K$ with K an imaginary quadratic number field.

5. $M_2(K)$ where K is an imaginary quadratic field.

6. The matrix algebra $M_2(B_p)$.

Correspondingly, an abelian surface over $\mathbb{F}_q$ is isogenous over $\mathbb{F}_q$ to one of the following.

1. An ordinary simple abelian surface $A_{\mathbb{F}_q}$ (whose endomorphism algebra is an order in a CM quartic field).

2. A simple abelian surface over $A_{\mathbb{F}_q}$ with K-quaternionic multiplication.

3. A product of non-isogenous ordinary elliptic curves $(E_1)_{\mathbb{F}_q}$ and $(E_2)_{\mathbb{F}_q}$.

4. The product of an ordinary elliptic curve $E^0_{\mathbb{F}_q}$ with a supersingular elliptic curve $E^s_{\mathbb{F}_q}$.

5. The square of an ordinary elliptic curve $E^0_{\mathbb{F}_q}$.

6. The square of a supersingular elliptic curve $E^s_{\mathbb{F}_q}$.

Let $\mathcal{O}$ be an Eichler order of level N in B_D. If A came equipped with some $\iota : \mathcal{O} \to \mathrm{End}_{\mathbb{F}_q}(A)$ and thus we had an embedding $B_D \to \mathrm{End}^0_{\mathbb{F}_q}(A)$. If $(A_1)_{\mathbb{F}_q}, (A_2)_{\mathbb{F}_q}$ are two non-isogenous abelian varieties, then $\mathrm{End}^0_{\mathbb{F}_q}(A_1 \times A_2) \cong \mathrm{End}^0_{\mathbb{F}_q}(A_1) \oplus \mathrm{End}^0_{\mathbb{F}_q}(A_2)$ so we can rule out Theorem 5.3.2(3-4) because simple algebras must map into simple algebras and $B_D \ncong B_p$.

Lemma 5.3.3. *If K is an imaginary quadratic field and B is a quaternion algebra, the following are equivalent.*

1. There exists an embedding $K \hookrightarrow B$.

2. There exists an isomorphism $B \otimes_{\mathbf{Q}} K \cong M_2(K)$.

3. There exists an embedding $B \hookrightarrow M_2(K)$.

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) is obvious. If there exists an embedding $B \hookrightarrow M_2(K)$ then there exists an embedding $B \otimes_{\mathbf{Q}} K \hookrightarrow M_2(K) \otimes_{\mathbf{Q}} K$. Note that

$$M_2(K) \otimes_{\mathbf{Q}} K \cong M_2(\mathbf{Q}) \otimes_{\mathbf{Q}} K \otimes_{\mathbf{Q}} K \cong M_2(\mathbf{Q}) \otimes_{\mathbf{Q}} (K \oplus K) \cong M_2(K) \oplus M_2(K).$$

If K does not embed into B then $B \otimes_{\mathbf{Q}} K$ is a division algebra, because if $K \cong \mathbf{Q}(\sqrt{d})$ then K does not embed into B if and only if $X^2 - d$ is irreducible over B and $B \otimes_{\mathbf{Q}} K \cong B[X]/(X^2 - d)$. Since $B \otimes_{\mathbf{Q}} K$ is also a simple algebra it must also be an 8-dimensional sub-algebra of the 16-dimensional algebra $M_2(K) \oplus M_2(K)$. Thus $B \otimes_{\mathbf{Q}} K$ must be a sub-algebra of one of the copies of $M_2(K)$. This is impossible since $M_2(K)$ that has zero-divisors and $B \otimes_{\mathbf{Q}} K$ does not. □

Let E be as in Definition 5.3.1. Note that $\mathrm{End}^0(E) \cong B_p$. Is it possible that there exists an embedding $B_D \hookrightarrow M_2(B_p)$? Consider the following:

Lemma 5.3.4. *We have an isomorphism of $\mathbf{Q}$-algebras $B_D \otimes B_{Dp} \cong M_2(B_p)$ if $p \nmid D$ and $B_D \otimes B_{D/p} \cong M_2(B_p)$ if $p \mid D$.*

Proof. This is a simple Brauer group calculation. We know $B_D \otimes B_{Dp}$ (or $B_D \otimes B_{D/p}$) is a central simple algebra over $\mathbf{Q}$ of dimension 16 ramified precisely at p and ∞, that is $M_n(B_p)$ such that $4n^2 = 16$. □

Corollary 5.3.5. *If $A_{\mathbb{F}_q}$ is an abelian surface and $B_D \hookrightarrow \mathrm{End}^0_{\mathbb{F}_q}(A)$, A is isogenous over $\mathbb{F}_q$ to the square of an elliptic curve $(E_0)_{\mathbb{F}_q}$. Moreover if $p \mid D$ this elliptic curve must be supersingular.*

Proof. We have established that Theorem 5.3.2(5-6) can occur and Theorem 5.3.2(3-4) cannot, hence it suffices to eliminate (1-2). A abelian surface as in Theorem 5.3.2(1) cannot admit such an embedding since B_D is non-commutative, so we need only ask if B_D can be mapped into the K-quaternion algebra $H_{\mathfrak{p}_1\mathfrak{p}_2}$.

If there exists an embedding $B_D \hookrightarrow H_{\mathfrak{p}_1\mathfrak{p}_2}$, tensoring with K gives $B_D \otimes_{\mathbf{Q}} K \hookrightarrow H_{\mathfrak{p}_1\mathfrak{p}_2}^{\oplus 2}$. Since simple algebras must map to simple algebras, we must have $B_D \otimes_{\mathbf{Q}} K \cong H_{\mathfrak{p}_1\mathfrak{p}_2}$ by equality of dimension. If $p \nmid D$ this is false since $M_2(K)$ is not a division algebra. If $p \mid D$, there exists some $q \mid D$ such that $q \neq p$ since B_D is indefinite. Pick a prime $\mathfrak{q}$ lying above q. It follows that $B_D \otimes K_{\mathfrak{q}}$ is a division algebra over K while $H_{\mathfrak{p}_1\mathfrak{p}_2} \otimes K_{\mathfrak{q}}$ is not. Hence we have established the existence of an elliptic curve E' such that $A \sim_{\overline{\mathbb{F}}_q} (E')^2$.

Finally the last assertion of this corollary is well-known [Rib89, Lemma 4.1]. □

Definition 5.3.6. *We say that an abelian surface $A_{/\mathbb{F}}$ is* superspecial *if $A \cong E_i \times E_j$ with E_i, E_j supersingular elliptic curves over $\mathbb{F}$.*

Lemma 5.3.7. *[Rib89, p. 21-22] Suppose that A is a supersingular abelian $\mathcal{O}$-surface over $\mathbb{F}$ with $p \nmid D$. Then A is superspecial.*

Note that if A is supersingular, it need not be superspecial. When A is ordinary, we have the following.

Theorem 5.3.8. *If $(A_{/k}, \iota)$ is an ordinary QM-abelian surface over a finite field k, then there exist ordinary elliptic curves E_0, E_0' over k such that $A \cong E_0 \times E_0'$. Moreover if $m > 1$ then (A, ι) is w_m-fixed (see Definition 5.2.3) if and only if $\mathrm{End}_k(E_0) \cong_k \mathrm{End}_k(E_0')$. Moreover, $\mathrm{End}_k(E_0)$ must be isomorphic to one of $\mathbf{Z}[\sqrt{-m}]$ or $\mathbf{Z}[\frac{1+\sqrt{-m}}{2}]$.*

Proof. The first part of the statement is part of a more general theorem of Kani [Kan11, Theorem 2], who calls ordinary elliptic curves CM. For the second part, note that $(A_{/S}, \iota)$ is w_m-fixed if and only if $R = \mathbf{Z}[\sqrt{-m}]$ (or $\mathbf{Z}[\zeta_4]$ if $m = 2$) embeds into the commutant of $\iota(\mathcal{O})$ in $\mathrm{End}_S(A)$.

Let k be a finite field, $A_{/k}$ be ordinary, and (A, ι) be w_m-fixed. Also let $W(k)$ denote the Witt vectors of k [Ser79, §II.6], which in this case are just a finite étale extension of

$\mathbf{Z}_p$. Then there is a canonical choice of an abelian scheme $\mathcal{A}_{W(k)}$ with an isomorphism $f : \mathrm{End}_k(A) \xrightarrow{\sim} \mathrm{End}_{W(k)}(\mathcal{A})$ [Mes72, Theorem V.3.3]. Therefore the Serre-Tate canonical lift $(\mathcal{A}, f \circ \iota)$ is a QM-abelian surface. Therefore so is $\mathcal{A}_{\mathbf{C}}$ (the choice of embedding $W(k) \hookrightarrow \mathbf{C}$ does not matter [Del69, 7.Théorème]), and there is an embedding of R into $\mathrm{End}_{f(\iota(\mathcal{O}))}(\mathcal{A}_{\mathbf{C}})$. Then we may find both an optimal embedding $\varphi : R' \hookrightarrow \mathcal{O}$ for some imaginary quadratic order $R' \supset R$ and an isomorphism $\mathcal{A}_{\mathbf{C}} \cong E_1 \times E_2$ where the E_i's have CM by R' and $f \circ \iota$ is given by φ [Mol10, p. 6].

Now let $K := W(k) \otimes \mathbf{Q}$, which must therefore be a finite unramified extension of $\mathbf{Q}_p$. We can then show that $\mathcal{A}_K \cong E_1' \times E_2'$ where $E_i' \otimes \mathbf{C} \cong E_i$ [Kan11, Lemma 60]. Moreover, each E_i' has CM by R' since $\mathcal{O} \hookrightarrow \mathrm{End}_K(\mathcal{A}_K)$ and we have $\varphi : R' \hookrightarrow \mathcal{O}$. Now, if V is an abelian variety over K, let $NM(V)$ denote its Néron model over $W(k)$ [BLR90, Definition I.2.1]. It follows that since $\mathcal{A}$ is an abelian scheme, it is the Néron model of its generic fiber [BLR90, Proposition I.2.8], and thus

$$\mathcal{A} \cong NM(\mathcal{A}_K) \cong NM(E_1' \times E_2') \cong NM(E_1') \times NM(E_2').$$

Therefore $\mathcal{A}_k \cong NM(E_1')_k \times NM(E_2')_k$ and the theorem is proved. □

Theorem 5.3.9. *Let $E_{/\mathbb{F}}$ be as in Definition 5.3.1 and let $A_{/\mathbb{F}}$ be an abelian surface isomorphic to the product of any two supersingular elliptic curves. Then $A \cong E \times E$.*

Proof. This is attributed to Deligne by Shioda [Shi79, Theorem 3.5]. □

Recall that $\mathcal{S}$ is a maximal order in B_p and $p \mid D$. Recall also that an $(\mathcal{O}, \mathcal{S})$-bimodule is a left $\mathcal{O}$-module M which is also a right $\mathcal{S}$-module such that if $x \in \mathcal{O}$, $y \in \mathcal{S}$, and $m \in M$, then $(xm)y = x(my)$. This implies that we have homomorphisms $\mathcal{O} \to \mathrm{End}_{\mathcal{S}}(M)$ and $\mathcal{S}^{\mathrm{op}} \to \mathrm{End}_{\mathcal{O}}(M)$. If both of these homomorphisms are *optimal* we say that M is an *optimal* $(\mathcal{O}, \mathcal{S})$ bimodule.

Theorem 5.3.10. *Suppose that $\mathcal{O}$ is an Eichler order of square-free level N in an indefinite quaternion algebra B of discriminant D with $(D,N)=1$. There is a bijection between the following sets.*

- *superspecial $\mathcal{O}$-abelian surfaces $(A,\iota)_{/\mathbb{F}}$ up to isomorphism*
- *$\mathbf{Z}$-rank 8 optimal $(\mathcal{O},\mathcal{S})$ bi-modules up to isomorphism*

Proof. Ribet [Rib89, p.38] proved this in the case where $\mathcal{O}$ is maximal (and thus optimality is guaranteed) by showing each were in bijection with the set of homomorphisms $f:\mathcal{O}\to M_2(\mathcal{S})$ up to $\mathrm{GL}_2(\mathcal{S})$ multiplication. To get a QM surface from f, consider $(E\times E,f)$ and note that we have $\mathrm{End}_{\mathbb{F}}(E)\cong\mathcal{S}$. To get a bi-module from f, consider $\mathcal{S}\oplus\mathcal{S}$ given the component-wise right $\mathcal{S}$ action and left $\mathcal{O}$-action by the homomorphism $f:\mathcal{O}\to M_2(\mathcal{S})\cong\mathrm{End}_{\mathcal{S}}(\mathcal{S}\oplus\mathcal{S})$. □

Lemma 5.3.11. *Let $q|DN$ and let $\mathfrak{Q}$ denote the unique two-sided integral ideal of norm q in $\mathcal{O}$. Under the bijection in Theorem 5.3.10, the action of w_q described in Definition 5.2.2 corresponds to the action $M\mapsto\mathfrak{Q}\otimes_{\mathcal{O}}M$.*

Proof. Take the isomorphism class of a superspecial surface (A,ι) to the $\mathrm{GL}_2(\mathcal{S})$ equivalence class of the homomorphism ι which corresponds to the bi-module M. The bi-module $\mathfrak{Q}\otimes_{\mathcal{O}}M$ is then isomorphic to $\beta_q M$ as an $(\mathcal{O},\mathcal{S})$-bi-module since $\mathfrak{Q}=\beta_q\mathcal{O}=\mathcal{O}\beta_q$. Therefore to get an action of $\mathcal{O}$ on this bi-module, we must pre-compose by β_q^{-1} and post-compose by β_q. □

Definition 5.3.12. *Let $\mathcal{O},\mathcal{S}$ be Eichler orders in a quaternion algebra over a number field K. We say that two $(\mathcal{O},\mathcal{S})$-bi-modules M,N are* locally isomorphic *if for all places v of K, $M_v\cong N_v$ as $(\mathcal{O}_v,\mathcal{S}_v)$-bi-modules.*

Remark 5.3.13. *It is in the condition of local isomorphism that we can keep track of whether or not a surface (A,ι) is mixed or not [Rib89, p.39].*

Theorem 5.3.14. *Let $\mathcal{O}, \mathcal{S}$ be as in Theorem 5.3.10 and fix an $(\mathcal{O}, \mathcal{S})$-bi-module M. Then $\Lambda := \mathrm{End}_{\mathcal{O},\mathcal{S}}(M)$ is an Eichler order in either B_{Dp} if $p \nmid D$ or $B_{D/p}$ if $p \mid D$. Moreover, if we fix a bi-module M, there is a bijection between the following two sets*

- *$(\mathcal{O}, \mathcal{S})$-bi-modules N locally isomorphic to M up to isomorphism and*
- *Rank one projective right Λ modules up to isomorphism.*

Let $q \neq p$ be prime. This bijection sends the action described in Lemma 5.3.11 to the action $[I] \mapsto [I\mathfrak{Q}_\Lambda]$, where $\mathfrak{Q}_\Lambda$ is the unique two-sided ideal of norm q of Λ.

Proof. The bijection in the case where $\mathcal{O}$ is a maximal order is a theorem of Ribet [Rib89, Theorem 2.3]. The extension to Eichler orders (even of non-square-free level) as well as showing the way the action of Lemma 5.3.11 transforms is due to Molina [Mol10, Remark 4.11]. His proof depends on showing that $\mathrm{Hom}_{\mathcal{O},\mathcal{S}}(N, \mathfrak{Q}_{\mathcal{O}} \otimes N)$ is $\mathfrak{Q}_\Lambda$. □

Definition 5.3.15. *Retaining the notation of Theorem 5.3.14, the action $[I] \mapsto [I\mathfrak{Q}_\Lambda]$ will be referred to as w_q. Moreover if m is the product of primes ramified in Λ, we define w_m as the composition of all w_q ranging over $q \mid m$.*

Corollary 5.3.16. *Let $m > 1$. A superspecial $\mathcal{O}$-abelian surface (A, ι) with corresponding bi-module M is fixed under the action of w_m if and only if there is an embedding of $\mathbf{Z}[\sqrt{-m}]$ (or $\mathbf{Z}[\zeta_4]$ if $m = 2$) into $\Lambda = \mathrm{End}_{\mathcal{O},\mathcal{S}}(M)$.*

Proof. By Theorem 5.3.14, (A, ι) is fixed by the action of w_m if and only if $[\prod_{q|m} \mathfrak{Q}_\Lambda] = [1]$, which is to say if and only if the unique two-sided ideal of norm m is principal. Therefore there is a fixed point if and only if there is an element γ of $\mathrm{End}_{\mathcal{O},\mathcal{S}}(M)$ which can serve as the principal generator. That is, $\gamma^2\Lambda = m\Lambda$ so there is a unit u of Λ such that $\gamma^2 = um$. Therefore, $u \in \mathbf{Z}_F$ where $F = \mathbf{Q}(\gamma)$, an imaginary quadratic extension of $\mathbf{Q}$. Following Kurihara [Kur79, Proposition 4-4], $u \neq 1$ since Λ is definite, $u^2 + 1 = 0$ can only happen if $m = 2$, or $u^2 \pm u + 1 = 0$

can only happen if $m = 3$. This exhausts all possibilities since $\mathbf{Q}(u) \subset F$. If $u^2 + 1 = 0$ then $\mathbf{Z}[u] \cong \mathbf{Z}[\gamma]$ with $u \mapsto \gamma + 1$. If $u^2 \pm u + 1 = 0$ then $\mathbf{Z}[u] \cong \mathbf{Z}[\gamma]$ with $u \mapsto \gamma \pm 1$. $\square$

This is of particular interest to us because of the following lemma.

Lemma 5.3.17. *If (A, ι) is a superspecial abelian $\mathcal{O}$-surface over $\mathbb{F}$, then $w_p(A, \iota)$ (in the sense of Theorem 5.3.14) is its $\mathbb{F}_{p^2}/\mathbb{F}_p$-Galois conjugate. Equivalently, if $P : \mathrm{Spec}(\mathbb{F}) \to X_0^D(N)$ corresponds to a superspecial abelian $\mathcal{O}$-surface (A, ι) over $\mathbb{F}$ and $\phi_1 : \mathbb{F} \to \mathbb{F}$ is the p-th power map, the following diagram commutes.*

$$\begin{array}{ccc} \mathrm{Spec}(\mathbb{F}) & \xrightarrow{P} & X_0^D(N) \\ \downarrow{\scriptstyle \phi_1^*} & & \downarrow{\scriptstyle w_p} \\ \mathrm{Spec}(\mathbb{F}) & \xrightarrow{P} & X_0^D(N) \end{array}$$

Proof. If $p \mid D$, then for *all* points $P : \mathrm{Spec}(\mathbb{F}) \to X_0^D(N)$, the square of this Lemma commutes. If $p \mid N$, and $P : \mathrm{Spec}(\mathbb{F}) \to X_0^D(N)$ corresponds to an abelian $\mathcal{O}$-surface $(A_{\mathbb{F}}, \iota)$ then by Theorem 5.2.24, $w_p P$ corresponds to $(A^{(p)}, \mathrm{Frob}_{p,*}\,\iota)$. By Lemma 6.0.4, this corresponds to the point $P\phi_1^*$. If $p \nmid DN$, we can reduce to the case $p \mid N$ via the embedding $c : X_0^D(N)_{\mathbb{F}} \to X_0^D(Np)_{\mathbb{F}}$. $\square$

Definition 5.3.18. *Let (A, ι) be a superspecial $\mathcal{O}$-abelian surface over $\mathbb{F}$ with corresponding bi-module M. The* length *of (A, ι) is $\#(\mathrm{End}_{(\mathcal{O},\mathcal{S})}(M)^\times / \pm 1)$.*

Note that $\mathrm{End}_{(\mathcal{O},\mathcal{S})}(M) \cong \mathrm{End}_{\mathbb{F}}(A, \iota)$ [Mol10, Equation 3.5]. Therefore if (A, ι) corresponds to a point of $X_0^D(N)(\mathbb{F})$ then this definition agrees with Definition 5.2.20.

Corollary 5.3.19. *Let (A, ι) be a mixed superspecial $\mathcal{O}$-abelian surface with corresponding bi-module M and whose length is divisible by three. Let N' be the level of $\mathcal{O}' = \mathrm{End}_{(\mathcal{O},\mathcal{S})}(M)$ and D' the discriminant of $\mathcal{O}' \otimes \mathbf{Q}$. Then for all $p \mid D'$, $p = 3$ or $p \equiv 2 \bmod 3$, and for all $q \mid N'$, $q = 3$ or $q \equiv 1 \bmod 3$. Moreover, (A, ι) is fixed by w_m if and only if $m = 1, 3, D'N'$ or $D'N'/3$ if $3 \mid D'N'$.*

Proof. Unless $D' = 2, 3$ and $N' = 1$, the only possible such length is three[Vig80, Proposition V.3.1], and in each of those cases if $p \mid D'$ then $p = 2$ or $p = 3$. If $(D', N') \neq (2,1), (3,1)$, the length of (A, ι) is three if and only if $\mathbf{Z}[\zeta_6] \hookrightarrow \mathcal{O}'$ and the first part of our statement holds by Theorem 4.1.28.

Regarding Atkin-Lehner fixed points, recall first that any (A, ι) is fixed by w_1. If $\mathbf{Z}[\zeta_6]$ embeds into $\mathcal{O}'$ note that $\mathbf{Z}[\sqrt{-3}] \subset \mathbf{Z}[\zeta_6] \hookrightarrow \mathcal{O}'$ so (A, ι) is fixed by w_3 if $3 \mid D'N'$. Now suppose that $m \neq 3$ so by Corollary 5.3.16 we additionally have an embedding $\mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$. Since $\mathbf{Z}[\zeta_6]$ does not contain $\mathbf{Z}[\sqrt{-m}]$ and vice versa, we have simultaneous embeddings if and only if $m = D'N'$ or $D'N'/3$ if $3 \mid D'N'$ by Theorem 4.2.5. $\square$

Corollary 5.3.20. *Let (A, ι) be a mixed superspecial $\mathcal{O}$-abelian surface with corresponding bi-module M and whose length is even. Let N' be the level of $\mathcal{O}' = \mathrm{End}_{(\mathcal{O},\mathcal{S})}(M)$ and D' the discriminant of $\mathcal{O}' \otimes \mathbf{Q}$. Then for all $p \mid D'$, $p = 2$ or $p \equiv 3 \bmod 4$, and for all $q \mid N'$, $q = 2$ or $q \equiv 1 \bmod 4$. Moreover, (A', ι') is fixed by w_m if and only if $m = 1, 2, D'N'$ or $D'N'/2$ if $2 \mid D'N'$.*

Proof. Recall that unless $D' = 2, 3$ and $N' = 1$, the only possible even length is two[Vig80, Proposition V.3.1], and in each of those cases our conditions hold. If $(D', N') \neq (2,1), (3,1)$, the length of (A, ι) is two if and only if $\mathbf{Z}[\zeta_4] \hookrightarrow \mathcal{O}'$ and the first part of our statement holds by Theorem 4.1.28.

Regarding Atkin-Lehner fixed points, recall first that any (A, ι) is fixed by w_1. If we have $\mathbf{Z}[\zeta_4] \hookrightarrow \mathcal{O}'$ then (A, ι) is fixed by w_2 if $2 \mid D'N'$. Now suppose that $m > 2$ so by Corollary 5.3.16 we additionally have an embedding $\mathbf{Z}[\sqrt{-m}] \hookrightarrow \mathcal{O}'$. Since $\mathbf{Z}[\zeta_4]$ does not contain $\mathbf{Z}[\sqrt{-m}]$ and vice versa, we have simultaneous embeddings if and only if $m = D'N'$ or $D'N'/2$ if $2 \mid D'N'$ by Theorem 4.2.1. $\square$

Recall now that $\mathcal{O}$ is an Eichler order of square-free level N in B_D where D is the square-free product of an even number of primes and N is coprime to D. Let $m \mid DN$ and let p be a prime not dividing DN. As usual $\mathcal{S}$ is a maximal order in B_p.

Corollary 5.3.21. *There is a mixed superspecial abelian $\mathcal{O}$ surface $(A_{\mathbb{F}_2}, \iota)$ fixed by w_m if and only if one of the following occurs.*

1. $m = DN$, $q \equiv 3 \bmod 4$ *for all* $q \mid D$, *and* $q \equiv 1 \bmod 4$ *for all* $q \mid N$.

2. $m = DN \equiv \pm 3 \bmod 8$, $\left(\frac{-2}{q}\right) = -1$ *for all primes* $q \mid D$, *and* $\left(\frac{-2}{q}\right) = 1$ *for all primes* $q \mid N$.

If $p \neq 2$, *there is a mixed superspecial abelian $\mathcal{O}$ surface $(A_{\mathbb{F}_p}, \iota)$ fixed by w_m if and only if one of the following occurs.*

1. $2 \nmid D$, $m = DN$, $\left(\frac{-DN}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ *for all* $q \mid D$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all* $q \mid N$ *such that* $q \neq 2$.

2. $2 \mid N$, $m = DN/2$, $\left(\frac{-DN/2}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ *for all* $q \mid D$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all* $q \mid N$ *such that* $q \neq 2$.

3. $2 \mid D$, $m = DN$, $p \equiv \pm 3 \bmod 8$, $\left(\frac{-DN}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ *for all* $q \mid (D/2)$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all* $q \mid N$.

4. $2 \mid D$, $m = DN/2$, $DN \equiv 2, 6, 10 \bmod 16$, $p \equiv \pm 3 \bmod 8$, $\left(\frac{-DN/2}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ *for all* $q \mid D$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all* $q \mid N$.

Remark 5.3.22. *Note that we deal equally with the cases where* $2 \mid N$ *and* $2 \nmid DN$ *if* $m = DN$.

Proof. By Lemma 5.3.17, a superspecial abelian surface $(A_{/\mathbb{F}_{p^2}}, \iota)$ with corresponding bimodule M is defined over $\mathbb{F}_p$ if and only if it is w_p-fixed. Therefore there is some $(A_{\mathbb{F}_p}, \iota)$ fixed by w_m if and only if there is some Eichler order of level N in B_{Dp} which admits an embedding of both $\mathbf{Z}[\sqrt{-m}]$ (or $\mathbf{Z}[\zeta_4]$ if $m = 2$) and $\mathbf{Z}[\sqrt{-p}]$ (or $\mathbf{Z}[\zeta_4]$ if $p = 2$).

Let us first assume $p = 2$. Condition 1 is precisely Corollary 5.3.20 applied to the situation where $(m, 2) = 1$. Condition 2 is Theorem 4.2.9(5).

Now let us assume $p \neq 2$. Conditions 1 and 2 are Theorem 4.2.9(1-2). Similarly condition 3 is Theorem 4.2.9(3) and condition 4 is Theorem 4.2.9(4).

$\square$

Chapter 6

Primes of Good Reduction

Throughout this chapter we will fix D the discriminant of an indefinite quaternion $\mathbf{Q}$-algebra, N a square-free integer coprime to D, an integer $m \mid DN$ and a prime $p \nmid DN$. Recall that $X_0^D(N)_{/\mathbf{Z}_p}$ has a smooth special fiber by Theorem 5.2.18. Let w_m be as in Definition 5.2.2. Let $\mathbf{Z}_{p^2}$ be as in Definition 4.1.14 with $\langle\sigma\rangle = \mathrm{Aut}_{\mathbf{Z}_p}(\mathbf{Z}_{p^2})$ and let $\mathcal{Z}_{/\mathbf{Z}_p}$ denote the quotient of $X_0^D(N)_{\mathbf{Z}_{p^2}}$ by the action of $w_m\sigma$.

If p is split in $\mathbf{Q}(\sqrt{d})$, then $X_0^D(N)$ is isomorphic to $C^D(N,d,m)$ over $\mathbf{Q}_p$. We may then obtain results on local points without appealing to $\mathcal{Z}$.

If p is inert in $\mathbf{Q}(\sqrt{d})$ and $C^D(N,d,m)_{/\mathbf{Q}}$ is the twist of $X_0^D(N)_{/\mathbf{Q}}$ by w_m and $\mathbf{Q}(\sqrt{d})$ then $\mathcal{Z}$ is a $\mathbf{Z}_p$-model for $C^D(N,d,m)_{\mathbf{Q}_p}$. This is because it follows from applying the theorem on étale base change [Liu02, Proposition 10.1.21(c)] to the map $X_0^D(N)_{\mathbf{Z}_{p^2}}$ that $\mathcal{Z}_{\mathbb{F}_p}$ is also smooth.

Some easy results present themselves. For instance we may use Weil's bounds to show that we have p-adic points for all but finitely many primes p. Throughout this section, assume that g is the genus of $X_0^D(N)_{/\mathbf{Q}}$.

Theorem 6.0.1. *Suppose that p is unramified in $\mathbf{Q}(\sqrt{d})$ and $p > 4g^2$. It follows that $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$.*

Proof. Recall that Weil's bounds [Liu02, Exercise 9.1.15] tell us that if X is a smooth projective curve over $\mathbb{F}_p$ then

$$|\#X(\mathbb{F}_p) - (p+1)| \leq 2g\sqrt{p},$$

and thus $\#X(\mathbb{F}_p) \geq p + 1 - 2g\sqrt{p} > 4g^2 - 4g^2 + 1 = 1$. Hensel's Lemma tells us that if we let $\mathcal{Z}_{/\mathbf{Z}_p}$ be a regular model of $C^D(N,d,m)_{\mathbf{Q}_p}$ and set $X = \mathcal{Z}_{\mathbb{F}_p}$ then $C^D(N,d,m)(\mathbf{Q}_p) = \mathcal{Z}(\mathbf{Q}_p)$ is nonempty since $g = g(C^D(N,d,m)_{\mathbb{F}_p})$. □

For $p < 4g^2$, we must use another technique. In the split case we use Shimura's construction of the zeta function of $X_0^D(N)_{\mathbb{F}_p}$ using Hecke operators to give an exact formula for the size of $X_0^D(N)(\mathbb{F}_p)$. In the inert case, we give a partial answer in terms of superspecial points.

Definition 6.0.2. *Let S be an $\mathbb{F}_p$-scheme and let $A_{/S}$ be an abelian scheme. Let* $\mathrm{Frob}_{p^r} : A \to A^{(p^r)}$ *and* $\mathrm{Ver}_{p^r} : A^{(p^r)} \to A$ *be the Frobenius and Verschiebung isogenies, so that* $\mathrm{Frob}_{p^r}\mathrm{Ver}_{p^r} = \mathrm{Ver}_{p^r}\mathrm{Frob}_{p^r} = [p^r]$ *on $A^{(p^r)}$ and A respectively.*

Definition 6.0.3. *Let S be an $\mathbb{F}_p$-scheme and let (A,ι) be an abelian $\mathcal{O}$-surface. By* $\mathrm{Frob}_{p^r,*}\iota$ *we denote the unique optimal embedding* $\mathcal{O} \hookrightarrow \mathrm{End}_S(A^{(p^r)})$ *such that for all $\alpha \in \mathcal{O}$ the following commutes:*

$$\begin{array}{ccc} A & \overset{\iota(\alpha)}{\to} & A \\ \mathrm{Frob}_{p^r}\downarrow & & \downarrow \mathrm{Frob}_{p^r} \\ A^{(p^r)} & \overset{\mathrm{Frob}_{p^r,*}\iota(\alpha)}{\to} & A^{(p^r)} \end{array}.$$

Lemma 6.0.4. *Let $S = \mathrm{Spec}(\overline{\mathbb{F}}_p)$ and $\phi_r : S \to S$ be the morphism given by the p^r-th power map. Let $(A_{/S},\iota)$ be a QM-abelian surface as in Definition 5.1.8 corresponding to a point $P : S \to X_0^D(N)_S$. Let $P \circ \phi_r : S \to S \to X_0^D(N)_S$ denote the Galois conjugate point. Then the QM-abelian surface corresponding to $P \circ \phi_r$ is* $\mathrm{Frob}_{p^r}(A,\iota)$.

Proof. Fix an Eichler order $\mathcal{O}$ of level N in B_D. Note that $\mathrm{Frob}_{p^r}(A,\iota) = (A^{(p^r)}, \mathrm{Frob}_{p^r,*}\iota)$.

Denote by $\mathrm{Ver}_{p^r,*}\,\iota : \mathcal{O} \hookrightarrow \mathrm{End}_S(A)$ the unique optimal embedding such that for all $\alpha \in \mathcal{O}$ the following commutes:

$$\begin{array}{ccc} A^{(p^r)} & \overset{\iota(\alpha)}{\to} & A^{(p^r)} \\ \mathrm{Ver}_{p^r} \downarrow & & \downarrow \mathrm{Ver}_{p^r} \\ A & \overset{\mathrm{Ver}_{p^r,*}\,\iota(\alpha)}{\to} & A \end{array}.$$

Suppose that $\epsilon : \mathcal{O} \hookrightarrow \mathrm{End}_S(A)$ is an optimal embedding. Then denote by $\mathrm{Ver}^*_{p^r}\,\epsilon : \mathcal{O} \hookrightarrow \mathrm{End}_S(A)$ the unique optimal embedding such that for all $\alpha \in \mathcal{O}$ the following commutes:

$$\begin{array}{ccc} A^{(p^r)} & \overset{\mathrm{Ver}^*_{p^r}\,\epsilon(\alpha)}{\to} & A^{(p^r)} \\ \mathrm{Ver}_{p^r} \downarrow & & \downarrow \mathrm{Ver}_{p^r} \\ A & \overset{\epsilon(\alpha)}{\to} & A \end{array}.$$

We may now combine these to make the following diagram:

$$\begin{array}{ccc} A & \overset{\iota(\alpha)}{\to} & A \\ \mathrm{Frob}_{p^r} \downarrow & & \downarrow \mathrm{Frob}_{p^r} \\ A^{(p^r)} & \overset{\mathrm{Frob}_{p^r,*}\,\iota(\alpha)}{\to} & A^{(p^r)} \\ \mathrm{Ver}_{p^r} \downarrow & & \downarrow \mathrm{Ver}_{p^r} \\ A & \overset{\mathrm{Ver}_{p^r,*}\,\mathrm{Frob}_{p^r,*}\,\iota(\alpha)}{\to} & A \end{array}.$$

Noting that $\mathrm{Ver}_{p^r}\,\mathrm{Frob}_{p^r} = [p^r]_A$ and that $\iota(\alpha)[p^r]_A = [p^r]_A\iota(\alpha)$ for all $\alpha \in \mathcal{O}$, we must have $\mathrm{Ver}_{p^r,*}\,\mathrm{Frob}_{p^r,*}\,\iota = \iota$. Therefore, by the uniqueness of fiber products, $\mathrm{Frob}_{p^r,*}\,\iota(\alpha) = \mathrm{Ver}^*_{p^r}\,\iota(\alpha)$ and moreover $\mathrm{Frob}_{p^r}(A,\iota) = \mathrm{Ver}^*_{p^r}(A,\iota)$. Since Ver_{p^r} itself is the pullback of ϕ_r along $A \to S$ [Liu02, p.94] we obtain our result. □

We may thus observe the following. Let k is an algebraic extension of $\mathbb{F}_p$ and let $(A_{/k},\iota)$ be a QM abelian surface. Let $x_0 \in X_0^D(N)(\overline{k})$ correspond to $(A,\iota)_{\overline{k}}$. Furthermore let x_r correspond to $\mathrm{Frob}_{p^r}(A,\iota)$. Then the set of $\mathrm{Gal}(k/\mathbb{F}_p)$-conjugates of x_0 is $\{x_r : r \geq 0\}$.

6.1 Split primes and the Eichler-Selberg trace formula

Definition 6.1.1. *Let S be a $\mathbf{Z}_p$-scheme with $p \nmid DN$. Let $X_0^D(N)$ be defined over S. If $(n, DN) = 1$, T_n is the correspondence*

$$\begin{tikzcd}
 & X_0^D(Nn)_S \arrow[dl, "\Phi_1"'] \arrow[dr, "\Phi_2"] & \\
X_0^D(N)_S & & X_0^D(N)_S
\end{tikzcd}$$

where Φ_1 is the modular forgetful map and $\Phi_2 = \Phi_1 \circ w_n$.

The correspondences T_n are commonly known as *Hecke correspondences*. Let s be a closed point of S with $k(s) = \overline{k(s)}$ so that $X_0^D(N)_s$ has a $k(s)$-rational point so that correspondences on $X_0^D(N)$ are in bijection with endomorphisms of $J_0^D(N)_s$ [Mil86, Corollary 6.3]. Thus we may also use T_n to denote the endomorphism of $J_0^D(N)_s \cong J(X_0^D(N)_s)$ induced by the map of sets $X_0^D(N)_s \to \mathrm{Div}(X_0^D(N)_s)$ such that $P \mapsto (\Phi_{2,*}\Phi_1^*)P$. This operator on $J_0^D(N)_s$ is commonly referred to as a *Hecke operator*. We will explore the case $(n, DN) > 1$ in section 6.2.

Theorem 6.1.2 (Eichler-Shimura)**.** *There is an equality of endomorphisms of $J_0^D(N)_s$ between T_p and* $\mathrm{Frob}_p + \mathrm{Ver}_p$.

Proof. The particularly simple proof given below was sketched by Stein in the case of the elliptic modular curve $X_0^1(N)$ [RS11, Theorem 12.6.4]. We will show in fact that $P \mapsto (\Phi_{2,*}\Phi_1^*)P$ agrees with $\mathrm{Frob}_{p,*} + \mathrm{Frob}_p^*$ as functions $X_0^D(N)_{\overline{\mathbb{F}}_p} \to \mathrm{Div}(X_0^D(N)_{\overline{\mathbb{F}}_p})$. First we note that if the above holds for all but finitely many points, then by continuity we have our result. Therefore, it suffices to check that we have equality away from the superspecial points.

By Theorem 5.2.24, $X_0^D(Np)_s^o = c(X_0^D(N)_s^o) \coprod w_p c(X_0^D(N)_s^o)$ where X^o refers to removing the superspecial points, c is the natural embedding $X_0^D(N) \hookrightarrow X_0^D(Np)$ and w_p is the

p-th Atkin-Lehner involution.

It follows that if $P \in X_0^D(N)_s^o$ then

$$(\Phi_1^* P) = c_*(c^*(\Phi_1^* P)) + (w_p c)_*(w_p c)^*(\Phi_1^* P) = c_*(\Phi_1 c)^* P + (w_p c)_*(\Phi_1 w_p c)^* P.$$

Recall now that $\Phi_1 c$ is the identity and $\Phi w_p c$ is the Frobenius Frob_p . Thus $\Phi_1^* P = c_*(P) + (w_p c)_*(\mathrm{Frob}_p^* P)$. This implies that

$$\begin{aligned} \Phi_{2,*}\Phi_1^* P &= \Phi_{1,*} w_{p,*} \Phi_1^* P \\ &= \Phi_{1,*} w_{p,*}(c_*(P) + (w_p c)_*(\mathrm{Frob}_p^* P)) \\ &= \Phi_{1,*}(w_{p,*} c_*(P) + c_*(\mathrm{Frob}_p^* P)) \\ &= \Phi_{1,*} w_{p,*} c_* P + \Phi_{1,*} c_* \mathrm{Frob}_p^* P \\ &= \mathrm{Frob}_{p,*} P + \mathrm{Frob}_p^* P \end{aligned}$$

Now note that $\mathrm{Frob}_{p,*}$ as a function $X_0^D(N)_{\overline{\mathbb{F}}_p} \to \mathrm{Div}(X_0^D(N)_{\overline{\mathbb{F}}_p}$ induces the Frobenius isogeny Frob_p on $J_0^D(N)$. Note also that since $\mathrm{Frob}_{p,*} \mathrm{Frob}_p^* H = pH$ for all divisors H on $X_0^D(N)_s$ [Liu02, Proposition 9.2.11], Frob_p^* induces $\mathrm{Ver}_p = \mathrm{Frob}_p^t$, the unique dual isogeny to Frob_p, on $J_0^D(N)_{\overline{\mathbb{F}}_p}$.

□

Definition 6.1.3. *If $C_{\mathbb{F}_p}$ is a smooth, projective curve, we may define the zeta function of C as*

$$Z(C,x) := \exp\left(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{p^r})\frac{x^r}{r}\right).$$

Shimura [Shi67] proved that the trace of Hecke operators carries a deep relation to the number of points of a modular curve over a finite field. Namely he showed the following explicit formula for the zeta function.

Theorem 6.1.4. *If we fix a prime $\ell \nmid pDN$, then*

$$Z(X_0^D(N)_{\mathbb{F}_p}, x) = \frac{\det_{H^0(X_0^D(N),\Omega)}(I_g - T_p x + px^2 I_g)}{(1-x)(1-px)}. \tag{6.1}$$

Proof. First we note that for a complex curve X, there is a natural isomorphism between $\overline{H^0(X,\Omega)}$ and $H^0(X,\Omega)^\vee$ given by the map $\omega \mapsto \int_X \cdot \wedge \omega$. Here Ω is the canonical sheaf, which in this case is the sheaf of holomorphic differential one-forms. Therefore the standard Hodge decomposition of $H^1(X(\mathbf{C}))$ in the classical topology can be written as $H^0(X,\Omega) \oplus H^0(X,\Omega)^\vee$. Suppose now X is the generic fiber of a smooth and proper relative curve $\mathcal{X}$ over a mixed-characteristic discrete valuation ring with separably closed residue field and $\widetilde{X}$ is the special fiber of $\mathcal{X}$. Then, we can invoke smooth and proper base change [Mil80, Corollary VI.4.2] twice to realize

$$\begin{aligned}
H^1(\widetilde{X}, \mathbf{Q}_\ell) &\cong H^1(X, \mathbf{Q}_\ell) \\
&\cong H^1(X(\mathbf{C})) \\
&\cong H^1(X,\Omega) \oplus \overline{H^1(X,\Omega)} \\
&\cong H^1(X,\Omega) \oplus H^1(X,\Omega)^\vee \\
&\cong H^1(\widetilde{X},\Omega) \oplus H^1(\widetilde{X},\Omega)^\vee
\end{aligned}$$

Now we invoke the Weil Conjectures for curves [Mil80, Corollary V.2.6]. That is,

$$Z_p(X_0^D(N)_s, x) = \prod_{i=0}^{2} \det\left(Id - x\,\mathrm{Frob}_p \mid H^i(X_0^D(N)_s, \mathbf{Q}_\ell)\right)^{(-1)^{(1+i)}}$$

We now recall briefly that since $\dim X_0^D(N)_s = 1$, $(Id - x\,\mathrm{Frob}_p \mid H^0(X_0^D(N)_s, \mathbf{Q}_\ell)) = (1-x)$ and $(Id - x\,\mathrm{Frob}_p \mid H^2(X_0^D(N)_s, \mathbf{Q}_\ell)) = (1-px)$. However, since $H^1(X_0^D(N)_s, \mathbf{Q}_\ell) \cong$

$H^0(X_0^D(N)_s,\Omega)\oplus H^0(X_0^D(N)_s,\Omega)^\vee\cong H^0(J_0^D(N)_s,\Omega)\oplus H^0(J_0^D(N)_s,\Omega)^\vee$[Mil86, Proposition 2.2], we have $(Id - x\,\mathrm{Frob}_p \mid H^1(X_0^D(N)_s,\mathbf{Q}_\ell))$ equal to

$$\begin{aligned}
&= (Id - x\,\mathrm{Frob}_p \mid H^0(J_0^D(N)_s,\Omega))(Id - x\,\mathrm{Frob}_p^\vee \mid H^0(J_0^D(N)_s,\Omega))\\
&= (Id - x(\mathrm{Frob}_p+\mathrm{Ver}_p) + x^2\,\mathrm{Frob}_p\,\mathrm{Ver}_p)\mid_{H^0(X_0^D(N),\Omega)}\\
&= (Id - T_p x + px^2 Id)\mid_{H^0(X_0^D(N),\Omega)}.
\end{aligned}$$

□

Corollary 6.1.5. *[JL85, Proposition 2.1] If $r>1$ then*

$$\#X_0^D(N)(\mathbb{F}_{p^r})) = p^r + 1 - \mathrm{tr}(T_{p^r}) + p\,\mathrm{tr}(T_{p^{r-2}}) \tag{6.2}$$

and if $r=1$,

$$\#X_0^D(N)(\mathbb{F}_p)) = p + 1 - \mathrm{tr}(T_p) \tag{6.3}$$

Let σ_1 as the usual divisor sum function. Let w, f be as in Definition 4.1.25 and $e_{D,N}$ be as in Definition 4.1.27.

Theorem 6.1.6. *[Eichler's Trace Formula, [Eic56, §4]] Let D be the discriminant of an indefinite rational quaternion algebra, N a square-free integer coprime to D and ℓ a prime not dividing DN. Let $\mathrm{tr}(T_n)$ denote the trace of T_n on $H^0(X_0^D(N)_{\mathbf{C}},\mathbf{Q}_\ell)$.*

If n is not a square and $(n,DN)=1$, then

$$\mathrm{tr}(T_n) = \sigma_1(n) - \sum_{s=-\lfloor 2\sqrt{n}\rfloor}^{\lfloor 2\sqrt{n}\rfloor} \sum_{f\mid f(s^2-4n)} \frac{e_{D,N}\left(\frac{s^2-4n}{f^2}\right)}{w\left(\frac{s^2-4n}{f^2}\right)}. \tag{6.4}$$

Corollary 6.1.7.

$$\#X_0^D(N)(\mathbb{F}_p) = \sum_{s=-\lfloor 2\sqrt{p}\rfloor}^{\lfloor 2\sqrt{p}\rfloor} \sum_{f\mid f(s^2-4p)} \frac{e_{D,N}\left(\frac{s^2-4p}{f^2}\right)}{w\left(\frac{s^2-4p}{f^2}\right)}$$

6.2 Inert primes and the Eichler-Selberg trace formula

We shall briefly follow Rotger, Skorobogatov and Yafaev [RSY05, §2] to obtain a formula for the number of points of $C^D(N,d,m)(\mathbb{F}_p)$. This will not give a strict numerical criterion for the presence or absence of points, but it will give an exact formula as we will see in Theorem 6.2.6. In certain cases however, such as when $m = DN$, we will be able to use the properties of superspecial points to get numerical criterion, as in Corollary 6.3.2. We begin by extending the definition of Hecke operators T_n.

Suppose that $(DN, \frac{n}{(n,DN)}) = 1$, $m = (n,DN)|DN$ and $n' = \frac{n}{(n,DN)}$. Let S be a $\mathbf{Z}_p$-scheme and $\Phi_1 : X_0^D(Nn')_S \to X_0^D(N)_S$ be the forgetful map. By abuse of notation, let w_m denote the Atkin-Lehner involution on either $X_0^D(Nn')_S$ or $X_0^D(N)_S$. Note that $\Phi_1 w_m = w_m \Phi_1$, so if s is a closed point of S with $k(s) = \overline{k(s)}$, $T_{n'} w_m = w_m T_{n'} : X_0^D(N)_s \to \mathrm{Div}(X_0^D(N)_s)$.

Definition 6.2.1. *Suppose that $(DN, \frac{n}{(n,DN)}) = 1$, $m = (n,DN)|DN$ and $n' = \frac{n}{(n,DN)}$. Then define $T_n = w_m T_{n'}$.*

Let $m \mid DN$ and consider the quotient $(X_0^D(N)/w_m)_s$. Let Ω denote the canonical sheaf of $(X_0^D(N))_s$. Since w_m is an involution, $H^0(X_0^D(N)_s, \Omega)$ decomposes into the direct sum of the $+1$ and -1 eigenspaces under its action. Note that $H^0((X_0^D(N)/w_m)_s, \Omega)$ is the $+1$ eigenspace.

Suppose that $v \in H^0(X_0^D(N)_s, \Omega)$ such that $w_m v = v$. Then $w_m T_p v = T_p w_m v = T_p v$ and therefore T_p acts on $H^0((X_0^D(N)/w_m)_s, \Omega)$.

Definition 6.2.2. *If $p \nmid DN$ and $m|DN$, then by $T_p^{(m)}$ we denote the restriction of T_p to $H^0((X_0^D(N)/w_m)_s, \Omega)$.*

Note that since $T_p^{(m)}$ is just T_p on a smaller vector space,

$$T_p^{(m)} = \mathrm{Frob}_p + \mathrm{Ver}_p$$

on $\mathrm{Jac}((X_0^D(N)/w_m)_s)$ by Theorem 6.1.2.

Corollary 6.2.3. *Let g' be the genus of $(X_0^D(N))/w_m)_{\mathbb{F}_p}$. The zeta function of the quotient curve is*

$$Z_p(X_0^D(N)/w_m, s) = \frac{\det_{H^0(X_0^D(N)/w_m,\Omega)}(I_{g'} - T_p^{(m)} s + ps^2 I_{g'})}{(1-s)(1-ps)}.$$

Proof. Since $T_p^{(m)} = \mathrm{Frob}_p + \mathrm{Ver}_p$ on $\mathrm{Jac}((X_0^D(N)/w_m)_s)$, we may say that Eichler-Shimura holds on $(X_0^D(N)/w_m)_{\mathbb{F}_p}$. Therefore we may reuse the proof of Theorem 6.1.4. □

We may thus see that if $r > 1$ then

$$\#(X_0^D(N)/w_m)(\mathbb{F}_{p^r}) = p^r + 1 - \mathrm{tr}(T_{p^r}^{(m)}) + p\,\mathrm{tr}(T_{p^{r-2}}^{(m)}),$$

and

$$\#(X_0^D(N)/w_m)(\mathbb{F}_p) = p + 1 - \mathrm{tr}(T_p^{(m)}).$$

We now reinterpret these quantities. If we let $u_1, \ldots, u_{g'}$ be a basis for the +1 eigenspace of w_m and $v_1, \ldots, v_{g-g'}$ a basis for the −1 eigenspace, we have

$$\begin{aligned} T_{p^r} w_m(a_1 u_1 + \cdots + a_g v_{g-g'}) &= T_{p^r}(a_1 u_1 + \cdots + a_{g'} u_{g'}) \\ &- T_{p^r}(a_{g'+1} v_1 + \cdots + a_g v_{g-g'}) \end{aligned}$$

Thus $T_{p^r} + T_{p^r m} = 2T_{p^r}^{(m)}$ and so

$$\mathrm{tr}(T_{p^r}^{(m)}) = \mathrm{tr}\left(\frac{T_{p^r} + T_{p^r m}}{2}\right) \tag{6.5}$$

$$= \frac{1}{2}(\mathrm{tr}(T_{p^r}) + \mathrm{tr}(T_{p^r m})) \tag{6.6}$$

We may thus explicitly compute the traces on the quotient curve using Eichler's Trace Formula 6.1.6 to obtain the following.

Theorem 6.2.4. *If $r > 1$ then*

$$\#(X_0^D(N)/w_m)(\mathbb{F}_{p^r}) = p^r + 1 - \frac{\mathrm{tr}(T_{p^r}) + \mathrm{tr}(T_{p^r m})}{2} + \frac{p(\mathrm{tr}(T_{p^{r-2}}) + \mathrm{tr}(T_{p^{r-2}m}))}{2} \tag{6.7}$$

and if $r = 1$ then

$$\#(X_0^D(N)/w_m)(\mathbb{F}_p) = p + 1 - \frac{\mathrm{tr}(T_p) + \mathrm{tr}(T_{pm})}{2} \tag{6.8}$$

We may again use the trace formula to determine $C^D(N,d,m)(\mathbb{F}_{p^r})$, though in a somewhat oblique way. Consider that for any prime number p if $\left(\frac{d}{p}\right) = 1$ then $\mathbf{Q}(\sqrt{d}) \hookrightarrow \mathbf{Q}_p$ by Hensel's Lemma. Hence $C^D(N,d,m) \cong_{\mathbf{Q}_p} X_0^D(N)$ since they're already isomorphic over $\mathbf{Q}(\sqrt{d})$ by definition.

Suppose alternately that $\left(\frac{d}{p}\right) = -1$. Consider the following:

Lemma 6.2.5.

$$2\#X_0^D(N)/w_m(\mathbb{F}_{p^r}) = \#X_0^D(N)(\mathbb{F}_{p^r}) + \#C^D(N,d,m)(\mathbb{F}_{p^r}) \tag{6.9}$$

Proof. Consider the quotient maps

$$\begin{array}{ccc} X_0^D(N)(\mathbb{F}_{p^r}) & & C^D(N,d,m)(\mathbb{F}_{p^r}) \\ & \searrow \quad \swarrow & \\ & X_0^D(N)/w_m(\mathbb{F}_{p^r}) & \end{array}$$

Consider that $X_0^D(N)/w_m(\mathbb{F}_{p^r})$ is made up of the set of equivalence classes $[P,Q]$ such that $P,Q \in X_0^D(N)(\overline{\mathbb{F}}_{p^r})$, $w_m(P) = Q$ and for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_{p^r}/\mathbb{F}_{p^r})$ either $\sigma P = Q$ and $\sigma Q = P$ or $\sigma P = P$ and $\sigma Q = Q$. In either case, $P,Q \in \mathbb{F}_{p^{2r}}$ and we may fix σ as the generator of $\mathrm{Gal}(\mathbb{F}_{p^{2r}}/\mathbb{F}_{p^r})$. The former case indicates that $w_m\sigma P = w_m Q = P$ and thus $P,Q \in C^D(N,d,m)(\mathbb{F}_{p^r})$ while the latter case indicates that $P,Q \in X_0^D(N)(\mathbb{F}_{p^r})$.

If $P \neq Q$ then $[P,Q]$ is a point over which the (geometric) map $X_0^D(N) \to X_0^D(N)/w_m$

is unramified, and so gives rise to two points in either $X_0^D(N)(\mathbb{F}_{p^r})$ or $C^D(N,d,m)(\mathbb{F}_{p^r})$ as the case may be. If $P = Q$ then $[P,Q] = [P,P]$ is a ramification point for the above map. Note however that we have both $w_m \sigma P = P$ and $\sigma P = P$ so P lies both on $X_0^D(N)(\mathbb{F}_{p^r})$ and $C^D(N,d,m)(\mathbb{F}_{p^r})$. In either case a rational point on $X_0^D(N)/w_m$ gives rise to two rational points on the disjoint union of the two $\mathbb{F}_{p^r}$ twists of $X_0^D(N)$.

□

We are instantly left with the following result:

Theorem 6.2.6. *Let p be inert in $\mathbf{Q}(\sqrt{d})$ and let $m|DN$. If $r > 1$ then*

$$\#C^D(N,d,m)(\mathbb{F}_{p^r}) = p^r + 1 - \operatorname{tr}(T_{p^r m}) + p \operatorname{tr}(T_{p^{r-2} m}) \tag{6.10}$$

and if $r = 1$ then

$$\#C^D(N,d,m)(\mathbb{F}_p) = p + 1 - \operatorname{tr}(T_{pm}) \tag{6.11}$$

Proof.

$$\begin{aligned}
\#C^D(N,d,m)(\mathbb{F}_{p^r}) &= 2\#X_0^D(N)/w_m(\mathbb{F}_{p^r}) - \#X_0^D(N)(\mathbb{F}_{p^r}) \\
&= 2p^r + 2 - \operatorname{tr}(T_{p^r}) - \operatorname{tr}(T_{p^r m}) \\
&+ p \operatorname{tr}(T_{p^{r-2}}) + p \operatorname{tr}(T_{p^{r-2} m}) \\
&- (p^r + 1 - \operatorname{tr}(T_{p^r}) + p \operatorname{tr}(T_{p^{r-2}})) \\
&= p^r + 1 - \operatorname{tr}(T_{p^r m}) + p \operatorname{tr}(T_{p^{r-2} m})
\end{aligned}$$

□

6.3 Inert primes and superspecial points

We now use the theory of superspecial points to gain explicit criteria for the presence of rational points in certain situations. Recall that the superspecial points of $X_0^D(N)(\overline{\mathbb{F}}_p)$ are in bijection with $\mathrm{Pic}(Dp, N)$ via the embedding $c : X_0^D(N)_{\mathbb{F}_p} \to X_0^D(Np)_{\mathbb{F}_p}$ by Lemma 5.2.25. Recall also that the action of $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ on the superspecial points in $X_0^D(N)(\overline{\mathbb{F}}_p)$ is given by w_p by Lemma 5.3.17.

Theorem 6.3.1. *If $p \nmid DN$ is inert in $\mathbf{Q}(\sqrt{d})$, then $C^D(N, d, m)(\mathbf{Q}_p)$ is nonempty if either*

- $mp \not\equiv 3 \bmod 4$ *and* $e_{Dp,N}(-4mp) \neq 0$, *or*
- $mp \equiv 3 \bmod 4$ *and one of* $e_{Dp,N}(-4mp)$ *or* $e_{Dp,N}(-mp)$ *is nonzero, or*
- $p = 2$, $m = 1$, *and one of* $e_{Dp,N}(-4), e_{Dp,N}(-8)$ *is nonzero.*

Proof. Let ϕ_1 denote the p-th power map on $\overline{\mathbb{F}}_p$. We wish to determine if $\mathcal{Z}(\mathbb{F}_p)$ contains a superspecial point. That is, we wish to determine if $\mathcal{Z}(\overline{\mathbb{F}}_p)$ contains a point invariant under the action of Galois which corresponds (via the bijection of $\mathcal{Z}(\overline{\mathbb{F}}_p)$ with $X_0^D(N)(\overline{\mathbb{F}}_p)$) to a superspecial abelian surface over $\mathbb{F}_p$. This occurs if and only if there is a superspecial point $P \in X_0^D(N)(\overline{\mathbb{F}}_p)$ such that $P = w_m P \phi_1^*$, which in this context becomes $w_{mp}P$.

By Corollary 5.3.16, there is a superspecial w_{mp}-fixed point if and only if there is an embedding of $\mathbf{Z}[\sqrt{-mp}]$ into the $\mathrm{End}_{\iota(\mathcal{O})}(A)$ of the superspecial abelian surface (A, ι) corresponding to P, or possibly $\mathbf{Z}[\zeta_4]$ if $mp = 2$. Now recall that every embedding of an order R induces an optimal embedding of some $R' \supset R$.

If $mp = 2$ then both $\mathbf{Z}[\zeta_4]$ and $\mathbf{Z}[\sqrt{-2}]$ are maximal orders, of discriminants -4 and -8 respectively. If $mp \equiv 1 \bmod 4$, then $\mathbf{Z}[\sqrt{-mp}]$ is maximal and of discriminant $-4mp$.

If $mp \equiv 3 \bmod 4$ then $\mathbf{Z}[\sqrt{-mp}]$ again has discriminant $-4mp$ but is no longer maximal. It is contained in $\mathbf{Z}[\frac{1+\sqrt{-mp}}{2}]$, which is maximal and has discriminant $-mp$. Since there are no intermediate orders, this completes the proof. $\square$

Corollary 6.3.2. *If $p \nmid DN$ is inert in $\mathbf{Q}(\sqrt{d})$, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty when $m = DN$. Moreover, $\mathcal{Z}(\mathbb{F}_p)$ contains a point whose base change to $\overline{\mathbb{F}}_p$ corresponds to a superspecial surface.*

Proof. It suffices to note the following.

$$\begin{aligned} e_{Dp,N}(-4DNp) &= h(-4DNp)\prod_{q|Dp}\left(1-\left\{\frac{-4DNp}{q}\right\}\right)\prod_{q|N}\left(1+\left\{\frac{-4DNp}{q}\right\}\right) \\ &= h(-4DNp)\prod_{q|Dp}(1)\prod_{q|N}(1). \end{aligned}$$

Since $e_{Dp,N}(-4DNp) \neq 0$, Theorem 6.3.1 implies that $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty. □

Chapter 7

Ramified Primes

Throughout this chapter we will fix D the discriminant of an indefinite quaternion $\mathbf{Q}$-algebra, N a squarefree integer coprime to D, a squarefree integer d, an integer $m \mid DN$ and a prime $p \nmid DN$ ramified in $\mathbf{Q}(\sqrt{d})$. Let $X_0^D(N)_{/\mathbf{Q}}$ be given by Corollary 5.2.14. Let w_m be as in Definition 5.2.2. Let $C^D(N,d,m)_{/\mathbf{Q}}$ the twist of $X_0^D(N)$ by $\mathbf{Q}(\sqrt{d})$ and w_m. If $\Delta < 0$, let $H_\Delta(X) \in \mathbf{Z}[X]$ [Cox89, p.285] denote the Hilbert Class Polynomial of discriminant Δ, and recall that this is simply the polynomial whose roots are the j-invariants of elliptic curves with complex multiplication by R_Δ in the sense of Definition 4.1.25. Recall $e_{D,N}$ from Definition 4.1.27. The purpose of this chapter is to prove the following theorem.

Theorem 7.0.1. *Suppose that $p \nmid 2DN$ is a prime which is ramified in $\mathbf{Q}(\sqrt{d})$ and $m|DN$. Then $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$ if and only if one of the following occurs.*

1. $e_{D,N}(-4m) \neq 0$, $\left(\frac{-m}{p}\right) = 1$, *and* $H_{-4m}(X) = 0$ *has a root modulo* p
2. $m \equiv 3 \bmod 4$, $e_{D,N}(-m) \neq 0$, $\left(\frac{-m}{p}\right) = 1$, *and* $H_{-m}(X) = 0$ *has a root modulo* p
3. $m = DN$, $2 \nmid D$, $\left(\frac{-DN}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$ *such that* $q \neq 2$

4. $m = DN/2$, $2 \mid N$, $\left(\frac{-DN/2}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$ *such that* $q \neq 2$

5. $m = DN$, $2 \mid D$, $p \equiv \pm 3 \bmod 8$, $\left(\frac{-DN}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid (D/2)$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$.

6. $m = DN/2$, $2 \mid D$, $DN \equiv 2, 6,$ *or* $10 \bmod 16$, $p \equiv \pm 3 \bmod 8$, $\left(\frac{-DN/2}{p}\right) = -1$, $\left(\frac{-p}{q}\right) = -1$ *for all primes* $q \mid D$, *and* $\left(\frac{-p}{q}\right) = 1$ *for all primes* $q \mid N$.

Compare this to the following theorem.

Theorem 7.0.2. *Let p be a prime, $(p, 2N) = 1$, $D = 1$, and $m = N$. Then $C^D(N, d, m)(\mathbf{Q}_p)$ is nonempty if and only if either $H_{-4m}(X) = 0$ has a root modulo p.*

Proof. Suppose that $p > 2$, $D = 1$ and $m = N$. By [Ozm09, Proposition 5.5], $C^D(N, d, m)(\mathbf{Q}_p)$ is nonempty if and only if there is a prime ν of $\mathbb{B} = \mathbf{Q}[X]/(H_{-4m}(X))$ such that $f(\nu|p) = 1$. But then since $p \neq 2$ does not divide N, p is unramified in $\mathbb{B}$. Therefore there exists a prime ν such that $f(\nu|p) = 1$ if and only if $H_{-4m}(X) = 0$ has a root modulo p [Ser79, Proposition 15]. □

We may combine the results of Theorem 7.0.1(3) with those of Theorem 7.0.2 to yield the following.

Corollary 7.0.3. *Let $p \neq 2$ be a prime and let N be a squarefree integer such that $\left(\frac{-N}{p}\right) = -1$. It follows that $H_{-4N}(X)$ has a root modulo p if and only if for all odd primes $q \mid N$, $\left(\frac{-p}{q}\right) = 1$.*

To establish Theorem 7.0.1 and Corollary 7.0.3, we determine a regular model over $\mathbf{Z}_p$ of $C^D(N, d, m)_{\mathbf{Q}_p}$. We shall indeed show the following.

Theorem 7.0.4. *There is a regular model $\mathcal{X}_{/\mathbf{Z}_p}$ of $C^D(N, d, m)_{\mathbf{Q}_p}$ with the following properties. There is an equality of divisors on $\mathcal{X}$,*

$$\mathcal{X}_{\mathbb{F}_p} = \sum_{i=0}^{b} d_i \Gamma_i,$$

such that each Γ_i is defined over $\mathbb{F}_p$ and is prime, each $d_i \le 2$, $d_0 = 2$, $\Gamma_0 \cong (X_0^D(N)/w_m)_{\mathbb{F}_p}$, and for all $i > 0$, $p_a(\Gamma_i) = 0$.

Suppose additionally that $p \neq 2$. Then for all $i > 0$, $d_i = 1$ and Γ_0 intersects with Γ_i in a unique point Q_i is such that $\sum_{i=1}^{b} Q_i$ is the branch divisor of $X_0^D(N)_{\mathbb{F}_p} \to (X_0^D(N)/w_m)_{\mathbb{F}_p}$.

In fact, we shall show that if $p \neq 2$, $\mathcal{X}$ is the blowup of a scheme $\mathcal{Z}_{/\mathbf{Z}_p}$ such that there is an equality of divisors $\mathcal{Z}_{\mathbb{F}_p} = 2\Gamma$ where $\Gamma \cong (X_0^D(N)/w_m)_{\mathbb{F}_p}$. Therefore there are smooth points of $\mathcal{X}(\mathbb{F}_p)$ if and only if $\mathbb{F}_p = \mathbb{F}_p(P_i) = \mathbb{F}_p(\Gamma_i)$ since $\Gamma_i \cong \mathbb{P}^1_{\mathbb{F}_p(Q_i)}$ [Liu02, Theorem 8.1.19(b)]. After constructing $\mathcal{Z}$ and $\mathcal{X}$, we will describe $\mathbb{F}_p(Q_i)$, i.e., the $\mathbb{F}_p$-rationality of w_m-fixed points.

7.1 The first steps towards forming a model

Let us begin with a few foundational facts.

Lemma 7.1.1. *The modular automorphism $w_m : X_0^D(N) \to X_0^D(N)$ (over any base) is the identity map precisely when $m = 1$. In particular if $m \neq 1$ and k is any field, $w_m : X_0^D(N)_k \to X_0^D(N)_k$ is not the identity.*

Proof. This is simply a consequence of the action of w_m as in Definition 5.2.2 on QM abelian surfaces up to isomorphism. □

Lemma 7.1.2. *Let $X_{/K}$ be a curve with potentially semistable reduction realized by a cyclic totally ramified extension L/K of local fields. Let k be their common residue field and let S/R be the corresponding extension of discrete valuation rings. Let $\mathcal{Y} \to \operatorname{Spec}(S)$ be a regular model of X_L, $\operatorname{Gal}(L/K) = \langle\sigma\rangle$ and assume that there exists some α an automorphism of $\mathcal{Y}$ above $\sigma : \operatorname{Spec}(S) \to \operatorname{Spec}(S)$ extending the Galois action on X_L.*

1. *The quotient $\mathcal{Z} = \mathcal{Y}/\langle\alpha\rangle$ is a scheme of relative dimension one over $\operatorname{Spec}(R)$ with generic fiber X,*

2. *Let $\xi_1, \ldots, \xi_n$ be the generic points of the irreducible components $C_1, \ldots, C_n$ of $\mathcal{Y}_k$ lying above a component C of $\mathcal{Z}_k$ with generic point ξ. Let $D_i = D(\xi_i|\xi)$, $I_i = I(\xi_i|\xi)$ denote the decomposition and inertia groups, respectively. Then the multiplicity of ξ in $\mathcal{Z}_k$ is $|D_i|n/|I_i|$.*

Proof. That $\mathcal{Z}$ is a Spec(R)-scheme follows from the universal properties of the quotient as outlined in [Vie77, 3.6]. In particular by the definition of τ lying above σ, the map $\mathcal{Y} \to \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is τ-invariant and thus induces a map $\mathcal{Z} \to \mathrm{Spec}(R)$.

To obtain the multiplicities, we recall [Liu02, VIII.3.9] that the multiplicity of ξ_i is $v_i(s)$ where v_i is the discrete valuation of $\mathcal{O}_{\mathcal{Y},\xi_i}$ and s is a uniformizer of S. As $\mathcal{Y}$ has semistable reduction, $v_i(s) = 1$ for all i. Likewise the multiplicity of ξ is $v(r)$ where v is the discrete valuation of $\mathcal{O}_{\mathcal{Z},\xi}$ and r is a uniformizer of R. As $\mathcal{Y} \to \mathcal{Z}$ is Galois, there are positive integers e, q such that $v_i \mid_R = ev$ and $q = \mid D_i/I_i \mid$ for all i and $[L : K] = eqn$. As L/K is totally ramified, $rS = s^{eqn}S$. It then follows that

$$ev(r) = v_i(r) = v_i(s^{eqn}) = eqnv_i(s)$$

and thus

$$v(r) = qnv_i(s) = qn = \mid D_i/I_i \mid n = \mid D_i \mid n / \mid I_i \mid .$$

□

Lemma 7.1.3. *Under the hypotheses of Lemma 7.1.2, the non-regular points of $\mathcal{Z}$ are precisely the branch points $Q_1, \ldots, Q_b$ of $\mathcal{Y}_k \to \mathcal{Z}_k$*

Proof. Since $X_L \to X$ is étale the ramification points of f are exactly $P_1 := f^{-1}(Q_1), \ldots, P_b := f^{-1}(Q_b)$. To see this, note that $\mathcal{Z}$ is Noetherian, and thus normal [Kir10, Proposition 2.2.1] and thus geometrically unibranch. Since $\dim \mathcal{Y} = \dim \mathcal{Z}$ we find that f is étale away from $P_1, \ldots, P_b$ [Gro64, IV.18.10.1] and thus $\mathcal{Z}$ is regular outside of $f(P_1), \ldots, f(P_b)$. Conversely if these points were regular, f would be flat [AK70, V.3.6] and in that case the branch locus is either empty or pure of codimension one [AK70, VI.6.8] and thus dimension one. But this cannot be as we just proved the branch locus of f was the zero-dimensional set $\{f(P_1), \ldots, f(P_b)\}$ by showing that the ramification locus of f is precisely the domain on which f is not étale. $\square$

Now we apply these lemmas to our situation. If $K = \mathbf{Q}_p$ and $L = \mathbf{Q}_p(\sqrt{d})$ then $R = \mathbf{Z}_p$, $S = \mathbf{Z}_p[\sqrt{d}]$, $k = \mathbb{F}_p$, and $\sigma(\sqrt{d}) = -\sqrt{d}$. If additionally $X = X_0^D(N)_{\mathbf{Q}_p}$, then $\mathcal{Y}_{\mathbb{F}_p}$ is smooth and we may realize $\mathcal{Y} \cong X_0^D(N)_{/\mathbf{Z}_p[\sqrt{d}]}$ from Corollary 5.2.14. If we take $\alpha = w_m \circ \sigma$ and take $\mathcal{Z} = \mathcal{Y}/\langle\alpha\rangle$, then the following holds.

Theorem 7.1.4. *The scheme $\mathcal{Z}_{/\mathbf{Z}_p} = \mathcal{Y}/\langle\alpha\rangle$ has generic fiber $C^D(N, d, m)_{\mathbf{Q}_p}$, and there is an equality of divisors $\mathcal{Z}_{\mathbb{F}_p} = 2\Gamma$ where $\Gamma \cong (X_0^D(N)/w_m)_{\mathbb{F}_p}$.*

Proof. The scheme $\mathcal{Z}$ was constructed to have $C^D(N, d, m)_{\mathbf{Q}_p}$ as its generic fiber. Since there is a unique component of $\mathcal{Y}_{\mathbb{F}_p}$, there is a unique component of $\mathcal{Z}_{\mathbb{F}_p}$ so $n = 1$. Let ξ', ξ be the generic points of the components of $\mathcal{Y}_{\mathbb{F}_p}$ and $\mathcal{Z}_{\mathbb{F}_p}$ respectively. Then $D(\xi'|\xi) = \langle\alpha\rangle$ since α preserves $\mathcal{Y}_{\mathbb{F}_p}$. By Lemma 7.1.1, $I(\xi'|\xi) = \{\mathrm{id}\}$, so the multiplicity of the component corresponding to ξ is 2.

To determine the Γ such that $2\Gamma = \mathcal{Z}_{\mathbb{F}_p}$, recall that the pushforward under $f : \mathcal{Y} \to \mathcal{Z}$ of $\mathcal{Y}_{\mathbb{F}_p}$ forms a prime divisor of $\mathcal{Z}$ in $\mathcal{Z}_{\mathbb{F}_p}$ and must therefore be Γ. To determine this pushforward, note that the induced action of σ on $\mathrm{Spec}(\mathbb{F}_p)$ is trivial and consider the following commutative square.

$$\begin{tikzcd}
\mathcal{Y} \arrow[r, "\alpha"] \arrow[d] & \mathcal{Y} \arrow[d] \\
\mathrm{Spec}(\mathbf{Z}_p[\sqrt{d}]) \arrow[r, "\sigma"] & \mathrm{Spec}(\mathbf{Z}_p[\sqrt{d}])
\end{tikzcd}$$

The fiber product of this square with $\mathrm{Spec}(\mathbb{F}_p) \to \mathrm{Spec}(\mathbf{Z}_p[\sqrt{d}])$ is simply the $\mathrm{Spec}(\mathbb{F}_p)$-involution w_m on $\mathcal{Y}_{\mathbb{F}_p} = X_0^D(N)_{\mathbb{F}_p}$. This is to say that it becomes the following triangle.

$$\begin{tikzcd}
X_0^D(N)_{\mathbb{F}_p} \arrow[rr, "w_m"] \arrow[dr] & & X_0^D(N)_{\mathbb{F}_p} \arrow[dl] \\
& \mathrm{Spec}(\mathbb{F}_p) &
\end{tikzcd}$$

It follows that f, when restricted to $\mathcal{Y}_{\mathbb{F}_p}$ becomes simply the quotient map $X_0^D(N)_{\mathbb{F}_p} \to (X_0^D(N)/w_m)_{\mathbb{F}_p}$, and therefore $\Gamma \cong (X_0^D(N)/w_m)_{\mathbb{F}_p}$. $\square$

We note that by Lemma 7.1.3, that $\mathcal{Z}$ is not generally a regular scheme, and may require some singularities to be resolved. To make this easier, we fix the following.

Definition 7.1.5. *Fix an ordering $\{Q_i\}$ of the branch points of the quotient map $f : X_0^D(N)_{\mathbb{F}_p} \to (X_0^D(N)/w_m)_{\mathbb{F}_p}$. Let P_i denote the unique preimage of Q_i under f.*

Note that by definition, the P_i are exactly the points of $X_0^D(N)_{\mathbb{F}_p}$ fixed by w_m. We will explicitly describe a desingularization in the strong sense [Liu02, Definition 8.3.39] of $\mathcal{Z}$ and thus a regular model of $C^D(N,d,m)_{\mathbf{Q}_p}$, at least when $p \neq 2$. However, we will first describe the branch points $\{Q_i\}$ and their $\mathbb{F}_p$-rationality.

7.2 Atkin-Lehner fixed points over finite fields

Throughout this section, we will keep the notation of Definition 7.1.5. Note that since $\mathbf{Q}_p[\sqrt{d}]$ is totally ramified over $\mathbf{Q}_p$, $\mathbb{F}_p(Q_i) \cong \mathbb{F}_p(P_i)$. It can be shown [Liu02, Corollary 8.3.51] that $\mathcal{Z}$ admits a desingularization in the strong sense [Liu02, Definition 8.3.39]. The following lemma shows that if we make an assumption on the form of a desingularization of $\mathcal{Z}$, we can draw conclusions about $\mathcal{Z}(\mathbf{Q}_p)$.

Lemma 7.2.1. *Let $\pi : \mathcal{X} \to \mathcal{Z}$ be a desingularization in the strong sense and assume that for all i, $\pi^{-1}(Q_i)$ is a chain of rational curves such that at least one has multiplicity one. Then $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if either*

1. $\left(\frac{-m}{p}\right) = 1$ *and one of the following holds:*
   - $m = 2$ *or*
   - $H_{-4m}(X)$ *has a root modulo p or*
   - $m \equiv 3 \bmod 4$ *and $H_{-m}(X)$ has a root modulo p,*
2. *or* $\left(\frac{-m}{p}\right) = -1$ *and one of the conditions of Corollary 5.3.21 are satisfied.*

Proof. Note first that each component in $\pi^{-1}(Q_i)$ must be isomorphic to $\mathbb{P}^1_{\mathbb{F}_p(Q_i)}$. Therefore by our assumption on π, $\mathbb{F}_p = \mathbb{F}_p(Q_i)$ if and only if there is a reduced copy of $\mathbb{P}^1_{\mathbb{F}_p}$ in $\pi^{-1}(Q_i)$.

By Corollary 5.3.5, any QM abelian surface over a finite field must be either ordinary or supersingular. Suppose first that (A,ι) is supersingular and fixed by w_m. By Lemma 5.3.7, if (A,ι) is a supersingular QM-abelian surface over a finite field of characteristic p, then (A,ι) is superspecial. Therefore, one of the conditions of Corollary 5.3.21 hold if and only if there is a QM abelian surface (A,ι) fixed by w_m whose corresponding point P_i is $\mathbb{F}_p$-rational.

Now suppose that (A,ι) is an ordinary QM-abelian surface over a finite field k fixed by w_m. By Theorem 5.3.8, there are elliptic curves E, E' such that $\mathrm{End}_k(E) \cong \mathrm{End}_k(E') \cong R' = \mathbf{Z}[\sqrt{-m}]$ or $\mathbf{Z}[\frac{1+\sqrt{-m}}{2}]$ (or $\mathbf{Z}[\zeta_4]$ if $m = 2$) and $A \cong E \times E'$. Now note that the j-invariants of E, E' are both roots of $H_{-4m}(X) \bmod p$, $H_{-m}(X) \bmod p$ if $m \equiv 3 \bmod 4$, or $H_{-4}(X)$ if $m = 2$. Note also that if $m = 2$, then $H_{-4}(X)$ and $H_{-8}(X)$ have degree one. Since the j-invariants of E and E' are defined over $\mathbb{F}_p$, (A,ι) is defined over $\mathbb{F}_p$. Therefore if P_i corresponds to the surface (A,ι) then $\mathbb{F}_p(P_i) = \mathbb{F}_p$.

Since the reduction modulo a prime lying above p of an elliptic curve with CM by R_Δ is ordinary if and only if $\left(\frac{\Delta}{p}\right) = 1$ [Lan87, Theorem 13.12], we obtain that $\left(\frac{-m}{p}\right) = 1$ if and only if (A,ι) is ordinary.

We have thus shown that either condition 1 or condition 2 holds if and only if there is a reduced copy of $\mathbb{P}^1_{\mathbb{F}_p}$ in some $\pi^{-1}(Q_i)$. Since the strict transform of Γ in $\mathcal{X}$ has multiplicity two, the presence of a reduced copy of $\mathbb{P}^1_{\mathbb{F}_p}$ in some $\pi^{-1}(Q_i)$ is equivalent to the presence of a smooth point of $\mathcal{X}(\mathbb{F}_p)$. By Hensel's Lemma [JL85, Lemma 1.1], the presence of a smooth point in $\mathcal{X}(\mathbb{F}_p)$ is equivalent to $\mathcal{X}(\mathbf{Q}_p)$ and thus $C^D(N,d,m)(\mathbf{Q}_p)$ being nonempty. □

Remark 7.2.2. *Note that by Lemma 7.2.1, it is* necessary *in any case that some Q_i is $\mathbb{F}_p$-rational in order for $C^D(N,d,m)(\mathbf{Q}_p)$ to be nonempty.*

7.3 Tame Potential Good Reduction

In this section we construct a regular model of $C^D(N,d,m)_{\mathbf{Q}_p}$. Let $\mathcal{X}_{\mathbf{Z}_p} := \mathrm{Bl}_{\{Q_i\}}(\mathcal{Z})$, the blowup of $\mathcal{Z}$ along the branch divisor of $\mathcal{Y}_{\mathbb{F}_p} \to \mathcal{Z}_{\mathbb{F}_p}$ [Liu02, Definition 8.1.1]. Since the blowup construction gives a map $\mathcal{X} \to \mathcal{Z}$ which is an isomorphism away from $\{Q_i\}$, $\mathcal{X}$ is a regular model if and only if $\mathcal{X} \to \mathcal{Z}$ is a desingularization in the strong sense if and only if $\mathcal{X}$ is a regular scheme.

To see that this is a regular scheme, let $\overline{R} = \mathbf{Z}_p^{nr}$, a strict henselization of $\mathbf{Z}_p$. We will construct in this section an auxiliary scheme $\mathcal{X}'_{/\overline{R}}$. If we can show that $\mathcal{X}_{\overline{R}} \cong \mathcal{X}'$, it will follow that $\mathcal{X}$ is regular [CES03, Lemma 2.1.1]. Thus, the hypotheses of Lemma 7.2.1 would be satisfied and thus Theorem 7.0.1 would be proved.

We first recall the following.

Definition 7.3.1. *[CES03, Definition 2.3.6] Let $X'_{/D}$ be a normal curve with smooth generic fiber over a connected Dedekind scheme D. Let also δ be a closed point of D with perfect residue field, let ζ be a generator of $\mu_n(\overline{k(\delta)})$, and let π_δ be a uniformizer for δ in $\mathcal{O}_{D,\delta}$. A closed point x' in a closed fiber X'_δ is a* tame cyclic quotient singularity *of type (n,r) if there are non-negative integers n, r, m_1, m_2 such that $\widehat{\mathcal{O}^{sh}_{X',x'}}$ is isomorphic to the subalgebra* *of* $\mu_n(\overline{k(\delta)})$*-invariants in* $\widehat{\mathcal{O}^{sh}_{D,\delta}}[[t_1,t_2]]/(t_1^{m_1}t_2^{m_2}-\pi_\delta)$ *under the action* $t_1 \mapsto \zeta t_1$, $t_2 \mapsto \zeta^r t_2$, *subject to the following.*

- *The integer* n *is greater than one and not divisible by* $\mathrm{char}(k(\delta))$*.*
- *The integer* r *is coprime to* n*.*
- *The integers* m_1 *is positive and* $m_1 \equiv -rm_2 \bmod n$*.*

Also fix $\overline{S} = \overline{R}[\sqrt{d}]$, k' the residue field of $\overline{S}$, k the residue field of $\overline{R}$, and note that both k and k' must be isomorphic to $\overline{\mathbb{F}}_p$. We now note the following.

Lemma 7.3.2. *Suppose that* $p \neq 2$ *and let* Q *be a point of* $Q_i \times_{\mathbf{Z}_p} \overline{R}$*. Then* Q *is a tame cyclic quotient singularity with* $n = 2$ *and* $r = 1$*.*

Proof. By Lemma 7.1.1, the action of w_m at a w_m-fixed point of $X_0^D(N)_k$ is nontrivial. Let $\overline{\alpha}$ on $\mathcal{Y}_{\overline{S}}$ denote the extension of α on $\mathcal{Y}$. We wish to show that $\widehat{\mathcal{O}^{sh}_{\mathcal{Z},Q}}$ is the ring of invariants of a μ_2 (or since $p \neq 2$, $\mathbf{Z}/2\mathbf{Z}$) action. Fix an isomorphism $\overline{S}[[X]] \cong \widehat{\mathcal{O}_{\mathcal{Y}_{\overline{S}},P}}$ where P is the unique preimage of Q under $\overline{f} : \mathcal{Y}_{\overline{S}} \to \mathcal{Z}_{\overline{R}}$. Since w_m is always Galois-equivariant, $\overline{\alpha}(\sqrt{d}) = -\sqrt{d}$. Since $\overline{\alpha}$ induces an isomorphism $\overline{S}[[T]] \cong \overline{S}[[\overline{\alpha}(T)]]$, $\overline{\alpha}(T) = P_\alpha(T) = \sum_{j\geq 1} \alpha_j T^j$. Since $\overline{\alpha}$ is an involution, $\alpha_1 = -1$. Note then that since $p \neq 2$, $\overline{\alpha}(T) - T = -2T(1+O(T))$, i.e. $\overline{\alpha}(T) - T \equiv -2T \bmod (T^2)$. Since $-2 \notin \mathfrak{m}_{\overline{S}}$, $\overline{S}[[T]] \cong \overline{S}[[T']]$ where $T' := \overline{\alpha}(T) - T$. Note also that $\overline{\alpha}(T') = \overline{\alpha}(\overline{\alpha}(T) - T) = T - \overline{\alpha}(T) = -(T')$. Therefore $\sqrt{d}$ and T' form a basis of uniformizers for the two-dimensional local ring $\widehat{\mathcal{O}_{\mathcal{Y}_{\overline{S}},P}}$ and $\overline{\alpha}$ acts as -1 on both $\sqrt{d}$ and T'.

Note now that $\widehat{\mathcal{O}_{\mathcal{Z}_{\overline{R}},Q}}$ is the ring of invariants of the μ_2-action given by $\overline{\alpha}$ on $\overline{S}[[T']]$. Recall that since $p \neq 2$ is a uniformizer for R and p is ramified in $\mathbf{Q}(\sqrt{d})$ where d is square-free, d is also a uniformizer. Therefore $\overline{S}[[T']] \cong \overline{R}[[t_1,t_2]]/(t_1^{m_1}t_2^{m_2} - d)$ where $m_1 = 2$, $t_2 = T'$, and $m_2 = 0$. It follows that Q is a tame cyclic quotient singularity with $n = 2$ and $r = 1$. □

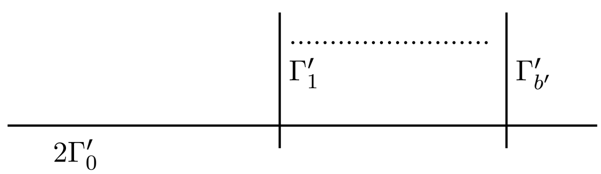
From here on, let b' be such that $\sum_{i=1}^{b} Q_i \times \overline{R} = \sum_{i=1}^{b'} Q'_i$.

Definition 7.3.3. *Let R be a discrete valuation ring with algebraically closed residue field, $X_{/R}$ be a scheme, and P a tame cyclic quotient singularity of X of type n, r. Then [CES03, Theorem 2.4.1] we can inductively produce a chain of divisors $E_1, \ldots E_\lambda$ and a set of integers $b_1, \ldots, b_\lambda$ such that*

- *There is a resolution $\tilde{X}_P \to X$ of the singularity at P whose fiber over P is the chain made up of the E_i's*
- $E_i \cdot E_j = \delta_{i,j\pm 1}$ *if* $i \neq j$, $E_j^2 = -b_j < -1$,
- $\frac{n}{r} = b_1 - \frac{1}{b_2 - \frac{1}{\cdots - \frac{1}{b_\lambda}}}$.

This $\tilde{X}_P$ is called the Hirzebruch-Jung desingularization at P.

Theorem 7.3.4. *If $p \neq 2$ there is a desingularization of $\overline{R}$-schemes $\mathcal{X}' \to \mathcal{Z}_{\overline{R}}$ such that $\mathcal{X}'_k$ has the form*



where Γ'_0 is the strict transform of $\Gamma_{\overline{R}}$ and for all $i > 0$, $\Gamma'_i \cong \mathbb{P}^1_k$. This is to say that there is an equality of divisors on $\mathcal{X}'$ between $\mathcal{X}'_k$ and $2\Gamma'_0 + \sum_{i=1}^{b'} \Gamma'_i$, $\Gamma'_0 \cap \Gamma'_i = Q'_i \in Q_i \times_{\mathbf{Z}_p} \overline{R}$, and all intersections are transverse. Moreover $\mathcal{X}_{\overline{R}} \cong \mathcal{X}'$, and since $\mathcal{X}'$ is a regular scheme, so is $\mathcal{X}$. It follows that $\mathcal{X}$ is a regular $\mathbf{Z}_p$ model for $C^D(N, d, m)_{\mathbf{Q}_p}$.

Proof. We construct $\mathcal{X}'$ by performing the Hirzebruch-Jung desingularization at Q for all Q in all $Q_i \times \overline{R}$. By Lemma 7.3.2, $n = 2$, $r = 1$ and thus $\lambda = 1$ and $b_1 = \frac{2}{1}$ in Definition 7.3.3. Therefore $\mathcal{X}'_k$ has the form above [CES03, Theorem 2.4.1].

Recall now that $\mathcal{X}' \to \mathcal{Z}_{\overline{R}}$, $\mathcal{X}_{\overline{R}} \to \mathcal{Z}_{\overline{R}}$ are birational morphisms and so there is a birational map $f : \mathcal{X}_{\overline{R}} \dashrightarrow \mathcal{X}'$ making the following diagram commute.

$$\begin{tikzcd} \mathcal{X}_{\overline{R}} \arrow[r, dashed, "f"] \arrow[dr] & \mathcal{X}' \arrow[r, dashed, "f^{-1}"] \arrow[d] & \mathcal{X}_{\overline{R}} \arrow[dl] \\ & \mathcal{Z}_{\overline{R}} & \end{tikzcd}$$

Since $\overline{R}$ is Dedekind, $f^{-1}|_{\Gamma_0'}$ is the identity and f can be extended so that the preimage of each divisor on either $\mathcal{X}_{\overline{R}}$ or $\mathcal{X}'$ is again a divisor, we find that f is a morphism and thus an isomorphism [Liu02, Theorem 8.3.20]. It follows that $\mathcal{X}_{\overline{R}}$ is regular and therefore $\mathcal{X}$ is regular [CES03, Lemma 2.1.1]. □

Corollary 7.3.5. *Theorem 7.0.1 holds.*

Proof. By Theorem 7.3.4, the conditions of Lemma 7.2.1 hold. □

Remark 7.3.6. *It can be easily shown that $\mathcal{X}$ is actually the minimal regular $\mathbf{Z}_p$ model of $C^D(N,d,m)_{\mathbf{Q}_p}$ if its genus is at least one, because there are no exceptional divisors in that case. In fact we have shown that for all $i > 0$, Γ_i is a -2 curve and thus if the genus of $C^D(N,d,m)_{\mathbf{Q}_p}$ is at least two then $\mathcal{Z}$ is the canonical model.*

Remark 7.3.7. *In the case that $X_0^D(N)/w_m \cong \mathbb{P}^1_{\mathbb{F}_p}$ we may deduce this theorem from work of Sadek [Sad10].*

7.4 Wild Singularities

Retaining the notation of Lemma 7.1.3, if $p = 2$ we still have that $\mathcal{Z}_{/\mathbf{Z}_2}$ is a normal scheme, non-regular precisely at the fixed points on the special fiber of w_m. Moreover, these singularities are still $\mathbf{Z}/2\mathbf{Z}$-quotient singularities. Once more, we may resolve these singularities to give a regular model of $C^D(N,d,m)$. If one tried to run through the arguments of the tame section, one would find that among other things, the argument for finding a new uniformizer in Lemma 7.3.2 fails spectacularly.

In contrast to the case $p \neq 2$, these cyclic quotient singularities must be *wild*, which is to say that $p \mid \#I$, whenever I is the inertia group of a fixed point of w_m. As such, the resolution of these singularities is not given by inserting a single reduced component, but rather a tree of possibly non-reduced components about which we know very little. It is known that if $g > 1$, the dual graph of the resolution must contain a node [Lor11, Theorem 5.3], but there is not much control otherwise.

The fact that the case $D = 1$ and $D > 1$ are so similar in other respects suggests that at least one of the components is reduced in the resolution of one of the singular points of $\mathcal{Z}$ [Ozm09, Lemma 5.8]. It is however not clear how to proceed on this without some knowledge of the higher ramification groups at these singular points.

Chapter 8

Primes dividing the level

Throughout this chapter we will fix D the discriminant of an indefinite quaternion $\mathbf{Q}$-algebra, N a squarefree integer coprime to D, a squarefree integer d, an integer $m \mid DN$, and a prime $p \mid N$ unramified in $\mathbf{Q}(\sqrt{d})$. Let w_m be as in Definition 5.2.2. Let $X_0^D(N)_{/\mathbf{Q}}$ be as defined in Corollary 5.2.14, and let $C^D(N,d,m)_{/\mathbf{Q}}$ be its twist by $\mathbf{Q}(\sqrt{d})$ and w_m. The purpose of this section is to prove the following theorem.

Theorem 8.0.1. *Let $p \mid N$ be unramified in $\mathbf{Q}(\sqrt{d})$ and $m \mid DN$. We have $C^D(N,d,m)(\mathbf{Q}_p)$ nonempty if and only if the conditions of (a) or (b) hold.*

(a) p is split in $\mathbf{Q}(\sqrt{d})$ and one of the following conditions holds.

- $D = 1$ *[Lemma 8.2.1]*
- $p = 2$, $D = \prod_i p_i$ *with each* $p_i \equiv 3 \bmod 4$, *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 4$ *[Lemma 8.2.3]*
- $p = 3$, $D = \prod_i p_i$ *with each* $p_i \equiv 2 \bmod 3$, *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 3$ *[Lemma 8.2.4]*

- *The following inequality [Lemma 8.2.5] holds*

$$\sum_{\substack{s=-\lfloor 2\sqrt{p}\rfloor \\ s\neq 0}}^{\lfloor 2\sqrt{p}\rfloor} \left(\sum_{f \mid f(s^2-4p)} \frac{e_{D,N/p}\left(\frac{s^2-4p}{f^2}\right)}{w\left(\frac{s^2-4p}{f^2}\right)} \right) > 0$$

(b) p is inert in $\mathbf{Q}(\sqrt{d})$, and there are prime factorizations $Dp = \prod_i p_i$, $N/p = \prod_j q_j$ such that one of the following two conditions holds

(i) $p \mid m$, and one of the following two conditions [Theorem 8.1.2] holds.

- $p = 2$, $m = p$ *or* DN, *for all* i, $p_i \equiv 3 \bmod 4$, *and for all* j, $q_j \equiv 1 \bmod 4$
- $p \equiv 3 \bmod 4$, $m = p$ *or* $2p$, *for all* i, $p_i \not\equiv 1 \bmod 4$, *and for all* j, $q_j \not\equiv 3 \bmod 4$

(ii) $p \nmid m$ and one of the following nine conditions holds.

- $m = D = 1$ *[Lemma 8.2.1]*
- $p = 2$, $m = 1$, *for all* i, $p_i \equiv 3 \bmod 4$, *and for all* j, $q_j \equiv 1 \bmod 4$ *[Lemma 8.2.3]*
- $p = 3$, $m = 1$, *for all* i, $p_i \equiv 2 \bmod 3$, *and for all* j, $q_j \equiv 1 \bmod 3$ *[Lemma 8.2.4]*
- $p \equiv 3 \bmod 4$, $m = DN/2p$, $p_i \not\equiv 1 \bmod 4$ *for all* i, *and* $q_j \not\equiv 3 \bmod 4$ *for all* j *[Lemma 8.2.3]*
- $p \equiv 2 \bmod 3$, $m = DN/3p$, $p_i \not\equiv 1 \bmod 3$ *for all* i, *and* $q_j \not\equiv 2 \bmod 3$ *for all* j *[Lemma 8.2.4]*
- $m = DN/p$, $p_i \not\equiv 1 \bmod 4$ *for all* i, *and* $q_j \not\equiv 3 \bmod 4$ *for all* j *[Lemma 8.2.3]*
- $m = DN/p$, $p_i \not\equiv 1 \bmod 3$ *for all* i, *and* $q_j \not\equiv 2 \bmod 3$ *for all* j *[Lemma 8.2.4]*
- $mp \not\equiv 3 \bmod 4$ *and* $(p+1) - \mathrm{tr}(T_{pm}) > \frac{e_{Dp,N/p}(-4mp)}{w(-4mp)}$ *[Lemma 8.2.5]*
- $mp \equiv 3 \bmod 4$ *and* $(p+1) - \mathrm{tr}(T_{pm}) > \frac{e_{Dp,N/p}(-mp)}{w(-mp)} + \frac{e_{D,N/p}(-4mp)}{w(-4mp)}$ *[Lemma 8.2.5]*

As a special case, we recover the following explicit numerical conditions.

Corollary 8.0.2. *Let p be a prime dividing N such that p is unramified in $\mathbf{Q}(\sqrt{d})$. Then $C^D(N,d,DN)(\mathbf{Q}_p)$ is nonempty if and only if*

- *p is split in $\mathbf{Q}(\sqrt{d})$ and one of the following conditions holds.*
  - $D = 1$
  - $p = 2,\ D = \prod_i p_i$ *with each* $p_i \equiv 3 \bmod 4,$ *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 4$
  - $p = 3,\ D = \prod_i p_i$ *with each* $p_i \equiv 2 \bmod 3,$ *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 3$
  - *The following inequality holds:*

$$\sum_{\substack{s=-\lfloor 2\sqrt{p}\rfloor \\ s\neq 0}}^{\lfloor 2\sqrt{p}\rfloor} \left(\sum_{f \mid f(s^2-4p)} \frac{e_{D,N/p}\left(\frac{s^2-4p}{f^2}\right)}{w\left(\frac{s^2-4p}{f^2}\right)} \right) > 0$$

- *p is inert in $\mathbf{Q}(\sqrt{d})$ with $Dp = \prod_i p_i$, $N/p = \prod_j q_j$ such that one of the following holds.*
  - $p = 2,$ *for all* i, $p_i \equiv 3 \bmod 4$ *and for all* j, $q_j \equiv 1 \bmod 4$
  - $p \equiv 3 \bmod 4,\ D = 1$ *and* $N = p$ *or* $2p$

Proof. The only part of this special case which does not immediately follow from the theorem is why we must have $D = 1$ if $p \neq 2$ is inert in $\mathbf{Q}(\sqrt{d})$. If $m = DN = p$ then since $p \mid N$ we must have $D = 1$ and $N = p$. Suppose now that $m = DN = 2p$. Recall that since B_D is indefinite, if $D > 1$ then there are at least two primes which divide D. Therefore if $D > 1$, we must have $D = 2p$ in contradiction to our assumption that $p \mid N$. It follows that $D = 1$ and $N = 2p$. □

We also note that we obtain results on rational points of $X_0^D(N)_{/\mathbf{Q}_p}$ when $p \mid N$ and $D > 1$. These do not seem to appear anywhere in the literature.

Corollary 8.0.3. *Let D be the squarefree product of an even number of primes, N a squarefree integer coprime to D, and $p \mid N$ be a prime. We have $X_0^D(N)(\mathbf{Q}_p) \neq \varnothing$ if and only if either*

- $D = 1$, *or*

- $p = 2$, $D = \prod_i p_i$ *with each* $p_i \equiv 3 \bmod 4$, *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 4$ *or*

- $p = 3$, $D = \prod_i p_i$ *with each* $p_i \equiv 2 \bmod 3$, *and* $N/p = \prod_j q_j$ *with each* $q_j \equiv 1 \bmod 3$ *or*

- *The following inequality holds:*

$$\sum_{\substack{s=-\lfloor 2\sqrt{p}\rfloor \\ s\neq 0}}^{\lfloor 2\sqrt{p}\rfloor} \left(\sum_{f \mid f(s^2-4p)} \frac{e_{D,N/p}\left(\frac{s^2-4p}{f^2}\right)}{w\left(\frac{s^2-4p}{f^2}\right)} \right) > 0$$

To prove Theorem 8.0.1, we will have to make the following definitions.

Definition 8.0.4. *Assume that* $p \mid N$. *Let* $X_0^D(N)_{/\mathbf{Z}_p}$ *be as in Theorem 5.2.24 and let* $\pi : \mathcal{X} \to X_0^D(N)$ *be a minimal desingularization, so that* $\mathcal{X}_{\mathbf{Z}_p}$ *is a regular model for* $X_0^D(N)_{\mathbf{Q}_p}$.

Note that if $n \mid DN$ then extending the automorphism w_n from Definition 5.2.2 to $\mathcal{X}$ makes sense. This is because $w_n : X_0^D(N) \to X_0^D(N)$ induces a birational morphism $\mathcal{X} \dashrightarrow \mathcal{X}$ permuting the components of $\mathcal{X}_{\mathbb{F}_p}$. Therefore w_n on $X_0^D(N)$ induces an isomorphism $\mathcal{X} \to \mathcal{X}$ [Liu02, Remark 8.3.25].

The model $\mathcal{X}$ is equipped with a closed embedding $c' : X_0^D(N/p)_{/\mathbb{F}_p} \to \mathcal{X}$ such that $\pi c' = c$, the embedding defined in Theorem 5.2.24. Let σ be such that $\langle \sigma \rangle = \mathrm{Aut}_{\mathbf{Z}_p}(\mathbf{Z}_{p^2})$.

Definition 8.0.5. *Let* $\mathcal{Z}$ *be the étale quotient of* $\mathcal{X}_{\mathbf{Z}_{p^2}}$ *by the action of* $w_m \circ \sigma$.

Note that if p is inert in $\mathbf{Q}(\sqrt{d})$ then $\mathbf{Z}_p[\sqrt{d}] \cong \mathbf{Z}_{p^2}$ and thus the generic fiber of $\mathcal{Z}$ is $C^D(N,d,m)_{\mathbf{Q}_p}$. Therefore $\mathcal{Z}$ is a regular model of $C^D(N,d,m)_{\mathbf{Q}_p}$ if p is inert in $\mathbf{Q}(\sqrt{d})$.

We also note that if p is split in $\mathbf{Q}(\sqrt{d})$, or if p is inert and $m = 1$, then $C^D(N,d,m)_{\mathbf{Q}_p} \cong X_0^D(N)_{\mathbf{Q}_p}$. Therefore, if p is split in $\mathbf{Q}(\sqrt{d})$, we can consider d' to be any squarefree integer such that p is inert in $\mathbf{Q}(\sqrt{d}')$ and $\mathcal{Z}'$ to be the regular model of $C^D(N,d',1)_{\mathbf{Q}_p} \cong X_0^D(N)_{\mathbf{Q}_p}$. Therefore, we shall obtain our results when p is split as a corollary to our results when $p \nmid m$.

We shall organize our results into two sections. In the first, we will consider the case when $p \mid m$. In that case, w_m and thus the twisted action of Galois will permute $c'(X_0^D(N/p)_{\mathbb{F}_p})$ and $w_p c'(X_0^D(N/p)_{\mathbb{F}_p})$ on the special fiber. In that case, any $\mathbb{F}_p$-rational point must come from a fixed superspecial point of length greater than one. In the second, we will consider the case when $p \nmid m$ and we may have to additionally allow for points on $c'(X_0^D(N/p)_{\mathbb{F}_p})$. Note also that if X^o denotes the complement of the superspecial points in X, $X_0^D(N)^o_{\mathbb{F}_p} = c'(X_0^D(N/p)^o_{\mathbb{F}_p}) \coprod w_p c'(X_0^D(N/p)^o_{\mathbb{F}_p})$.

8.1 The proof when $p \mid m$ is inert

Suppose that D is the discriminant of an indefinite $\mathbf{Q}$-quaternion algebra, N, d are square-free integers with $(D, N) = 1$, $m \mid DN$, and $p \mid m$ is inert in $\mathbf{Q}(\sqrt{d})$. Fix $\mathcal{X}$ and $\mathcal{Z}$ as in Definition 8.0.4. If $p \mid m$, the action of w_m on the regular model $\mathcal{X}$ interchanges $c'(X_0^D(N/p)_{\mathbb{F}_p})$ and $w_p c'(X_0^D(N)_{\mathbb{F}_p}$. Therefore if P denotes an element of $\mathcal{Z}(\mathbb{F}_p)$ then $\pi(P(\mathrm{Spec}(\mathbb{F}_p))$ must lie on both copies of $X_0^D(N/p)_{\mathbb{F}_p}$. This is to say that the base change to $\overline{\mathbb{F}}_p$ of πP is a superspecial point, say x.

Moreover, we have the following.

Lemma 8.1.1. *If D, N, d, m, p are as described in the beginning of this chapter and $p \mid m$ is inert in $\mathbf{Q}(\sqrt{d})$, then $C^D(N, d, m)(\mathbf{Q}_p) \neq \varnothing$ if and only if there is a superspecial $w_{m/p}$-fixed point $x \in X_0^D(N)(\overline{\mathbb{F}}_p)$ of even length.*

Proof. By abuse of notation, let $\mathrm{Frob}_p = \phi_1^* : \mathrm{Spec}(\overline{\mathbb{F}}_p) \to \mathrm{Spec}(\overline{\mathbb{F}}_p)$ where $\phi_1 : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$. Note that under the bijection from $\mathcal{Z}(\overline{\mathbb{F}}_p)$ to $\mathcal{X}(\overline{\mathbb{F}}_p)$, the action $P \mapsto P\,\mathrm{Frob}_p$ on $\mathcal{Z}(\overline{\mathbb{F}}_p)$ translates to the action of $P \mapsto w_m P\,\mathrm{Frob}_p$ on $\mathcal{X}(\overline{\mathbb{F}}_p)$.

Suppose that $C^D(N, d, m)(\mathbf{Q}_p)$ is nonempty. Then by Hensel's Lemma [JL85, Lemma 1.1] there must be an element of $\mathcal{Z}^{sm}(\mathbb{F}_p)$, or rather a smooth point such that $P = w_m P\,\mathrm{Frob}_p$ in $\mathcal{X}(\overline{\mathbb{F}}_p)$. Since $p \mid m$, w_m interchanges $c(X_0^D(N/p)_{\overline{\mathbb{F}}_p})$ with $w_p c(X_0^D(N/p)_{\overline{\mathbb{F}}_p})$. A smooth fixed point P of $w_m \circ \mathrm{Frob}_p$ must therefore satisfy $\pi(P) = x \in X_0^D(N)(\overline{\mathbb{F}}_p)$ with x lying in $c(X_0^D(N/p))(\overline{\mathbb{F}}_p)$ and $w_p c(X_0^D(N/p))(\overline{\mathbb{F}}_p)$. That is, x is a superspecial point.

Suppose there is such a smooth fixed point P. Let $\ell = \ell(x)$, so that if $\ell = 1$ then $\pi^* x(\mathrm{Spec}(\overline{\mathbb{F}}_p)) = P$ and thus P is a singular point. Of course this is a contradiction. If $\ell > 1$ then $\pi^* x(\mathrm{Spec}(\overline{\mathbb{F}}_p)) = \bigcup_{i=1}^{\ell-1} C_i$ with $C_i \cong \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ and if $i < j$,

$$C_i \cdot C_j = \begin{cases} 1 & j = i+1, 1 \le i < \ell \\ 0 & else \end{cases}.$$

By Lemma 5.3.17 $x\,\mathrm{Frob}_p = w_p(x)$, so we have $w_m \circ \mathrm{Frob}_p(x) = w_{mp}(x) = w_{m/p}(x)$. Therefore by continuity, $w_{m/p}$ fixes each C_i and for each i, $w_p C_i = C_{\ell-i}$. If ℓ is odd, there are no fixed components so $P(\mathrm{Spec}(\overline{\mathbb{F}}_p))$ must be the unique intersection point of $C_{\frac{\ell-1}{2}}$ with $C_{\frac{\ell+1}{2}}$, and thus singular. Therefore, unless ℓ is even we arrive at a contradiction.

Conversely suppose that there is a superspecial point x such that $\ell = \ell(x)$ is even and $w_{m/p}(x) = x$. Then we have $C_1, \dots C_{\ell-1}$ fixed by $w_{m/p}$ as above and w_p fixes $C_{\ell/2}$, so $C_{\ell/2}$ is defined over $\mathbb{F}_p$. Let $P_1 = C_{\ell/2-1} \cap C_{\ell/2}$ and $P_2 = C_{\ell/2} \cap C_{\ell/2+1}$ be the singular points of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ lying on $C_{\ell/2}$, and note that $w_p P_1 = P_2$. Therefore the fixed points of $\mathrm{Frob}_p\, w_m$ are nonsingular. There is a smooth fixed point P of $w_m \circ \mathrm{Frob}_p$ on $C_{\ell/2}$ and therefore by Hensel's Lemma, $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$.

□

Theorem 8.1.2. *Suppose that D, N, d, m and p are as in Theorem 8.0.1 and $p \mid m$ is inert in $\mathbf{Q}(\sqrt{d})$. Then $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$ if and only if*

- *$p = 2$, $m = p$ or DN, for all $q \mid D$, $q \equiv 3 \bmod 4$, and for all $q \mid (N/2)$, $q \equiv 1 \bmod 4$, or*
- *$p \equiv 3 \bmod 4$, $m = p$ or $2p$, for all $q \mid D$ either $q = 2$ or $q \equiv 3 \bmod 4$, and for all $q \mid (N/p)$, $q = 2$ or $q \equiv 1 \bmod 4$.*

Proof. By Lemma 8.1.1, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if there is a superspecial $w_{m/p}$-fixed point of even length in $X_0^D(N)(\overline{\mathbb{F}}_p)$. By Lemma 5.2.25, the QM endomorphism ring of a superspecial point on $X_0^D(N)(\overline{\mathbb{F}}_p)$ has discriminant $D' = Dp$ and level $N' = N/p$. Note that $D'N' = DN$. By Lemma 5.3.20, there is a superspecial $w_{m/p}$-fixed point of even length if and only if

- $m/p = 1, 2, DN/2$ or DN and
- for all $q \mid Dp$, $q = 2$ or $q \equiv 3 \bmod 4$ and
- for all $q \mid (N/p)$, $q = 2$ or $q \equiv 1 \bmod 4$.

We shall begin our analysis by applying the top condition first and using the latter two conditions later. We may immediately see that $(m/p) \mid (DN/p) < DN$ so $m/p \neq DN$. If $m/p = 1$ then $m = p$ and either $p = 2$, or $p \equiv 3 \bmod 4$ by the second condition. If $p = 2$, $2 \mid (DN/2)$ so the second and third conditions say that for all $q \mid D$, $q \equiv 3 \bmod 4$, and for all $q \mid (N/2)$, $q \equiv 1 \bmod 4$.

If $m/p = 2$ then $m = 2p$ and we conclude that $p \equiv 3 \bmod 4$ by the second condition. If $m/p = DN/2$ then $DNp/2 = m \mid DN$ and we conclude that $p = 2$. □

8.2 The proof when $p \nmid m$ is split or inert

We begin with the following observation regarding cusps, which are points that can only exist on $X_0^D(N)_S$ or $C^D(N,d,m)_S$ if $D = 1$.

Lemma 8.2.1. *If N is square-free and $m \mid N$, then w_m fixes a cusp of $X_0^1(N)$ if and only if $m = 1$. Therefore if N, d are square-free and $p \mid N$ is a prime, then $C^1(N,d,m)(\mathbf{Q}_p)$ contains a cusp if and only if either p is split in $\mathbf{Q}(\sqrt{d})$ or $m = 1$.*

Proof. This is proved as part of a stronger theorem of Ogg [Ogg74, Proposition 3] which shows that even if N is not square-free, the only possible Atkin-Lehner involution on $X_0^1(N)_{\overline{\mathbf{Q}}}$ which leaves a cusp fixed is w_4. If N is square-free, all cusps are $\mathbf{Q}$-rational [Ogg83, p.290] and the result follows. $\square$

Lemma 8.2.2. *Let D, N, d, m, p be as in Theorem 8.0.1 and suppose $p \nmid m$ is unramified in $\mathbf{Q}(\sqrt{d})$. Suppose that $C^D(N,d,m)(\mathbf{Q}_p)$ does not contain a cusp. Then $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$ if and only if one of the following occurs.*

- *There is a superspecial w_{mp}-fixed point of even length on $X_0^D(N)(\overline{\mathbb{F}}_p)$.*
- *There is a superspecial w_{mp}-fixed point of length divisible by three on $X_0^D(N)(\overline{\mathbb{F}}_p)$.*
- *There is a non-superspecial point of $C^D(N/p,d,m)(\mathbb{F}_p)$.*

Proof. Recall that the possible lengths of a superspecial point x are $1, 2, 3, 6$ or 12 [Vig80, pp.146-147], so that if $\ell(x)$ is neither even nor divisible by three then $\ell(x) = 1$. Let Frob_p : $\mathrm{Spec}(\overline{\mathbb{F}}_p) \to \mathrm{Spec}(\overline{\mathbb{F}}_p)$ be induced by the p-th power map. Recall also the regular models $\mathcal{X}, \mathcal{Z}$ of Definition 8.0.4, and that there is a bijection from $\mathcal{Z}(\overline{\mathbb{F}}_p)$ to $\mathcal{X}(\overline{\mathbb{F}}_p)$ and under this bijection, the action $P \mapsto P\,\mathrm{Frob}_p$ on $\mathcal{Z}(\overline{\mathbb{F}}_p)$ translates to the action $P \mapsto w_m P\,\mathrm{Frob}_p$ on $\mathcal{X}(\overline{\mathbb{F}}_p)$. Moreover by Lemma 5.3.17, the action of Frob_p on the superspecial points of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ is the action of w_p. Therefore a superspecial $\mathbb{F}_p$-rational point of $\mathcal{Z}$ corresponds to a superspecial w_{mp}-fixed point of $X_0^D(N)_{\overline{\mathbb{F}}_p}$.

Suppose now that $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty, or equivalently by Hensel's Lemma [JL85, Lemma 1.1] that $\mathcal{Z}^{sm}(\mathbb{F}_p)$ is nonempty. Suppose further that there are no superspecial w_{mp}-fixed points of length divisible by 2 or 3. It follows that if P is a smooth fixed point of w_{mp} in $\mathcal{X}(\overline{\mathbb{F}}_p)$, then $\pi(P) = x$ is not superspecial. If x were superspecial then its length would be one. It follows that $\pi^{-1}x = P$ is not a smooth point. Finally, recall that the non-superspecial points of $\mathcal{X}(\overline{\mathbb{F}}_p)$ lie on exactly one of $c'(X_0^D(N)(\overline{\mathbb{F}}_p))$ or $w_p c'(X_0^D(N)(\overline{\mathbb{F}}_p))$. If P is $w_m P\,\mathrm{Frob}_p$ and lies in $X_0^D(N/p)(\overline{\mathbb{F}}_p)$ then $P \in \mathcal{Z}(\mathbb{F}_p)$.

Conversely, suppose first that there is an $\mathbb{F}_p$-rational point of $\mathcal{Z}$ which is not superspecial. By the embedding $c : X_0^D(N/p)_{\mathbb{F}_p} \to X_0^D(N)_{\mathbb{F}_p}$, there is a non-superspecial $\mathbb{F}_p$-rational point of $\mathcal{Z}$. Since $X_0^D(N)_{\overline{\mathbb{F}}_p}$ is smooth away from superspecial points, this $\mathbb{F}_p$-rational point lifts via Hensel's lemma to an element of $C^D(N,d,m)(\mathbf{Q}_p)$.

Now suppose there is a superspecial w_{mp}-fixed point x with $\ell = \ell(x) > 1$. It follows that $\pi^*(x(\mathrm{Spec}(\overline{\mathbb{F}}_p))) = \bigcup_{i=1}^{\ell-1} C_i$ with $C_i \cong \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ and at most two singular points in $\mathcal{X}_{\overline{\mathbb{F}}_p}$ on each C_i. Since $w_m x \,\mathrm{Frob}_p = w_{mp}(x) = x$, for all i, $w_m C_i = w_{mp} C_i = C_i$ by continuity of π. Therefore C_i defines an $\mathbb{F}_p$-rational component of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$ with at most two singular points. Therefore $\mathcal{Z}^{sm}(\mathbb{F}_p)$ is nonempty and by Hensel's Lemma, $\mathcal{Z}(\mathbf{Q}_p)$ is nonempty. □

We now obtain conditions for each of these to occur.

Lemma 8.2.3. *There is a superspecial w_{mp}-fixed point of even length on $X_0^D(N)_{\overline{\mathbb{F}}_p}$ if and only if one of the following occurs.*

1. $p = 2$, $m = 1$, $q \equiv 3 \bmod 4$ *for all primes* $q \mid D$, *and* $q \equiv 1 \bmod 4$ *for all primes* $q \mid (N/2)$.
2. $p \equiv 3 \bmod 4$, $2 \mid DN/p$, $m = DN/2p$, $q \not\equiv 1 \bmod 4$ *for all primes* $q \mid D$, *and* $q \not\equiv 3 \bmod 4$ *for all primes* $q \mid (N/p)$.
3. $m = DN/p$, $p \not\equiv 1 \bmod 4$, $q \not\equiv 1 \bmod 4$ *for all primes* $q \mid D$, *and* $q \not\equiv 3 \bmod 4$ *for all primes* $q \mid (N/p)$.

Proof. By Lemma 5.2.25, if (A, ι) corresponds to a superspecial point $x \in X_0^D(N)(\overline{\mathbb{F}}_p)$ then $\mathrm{End}_{\iota(\mathcal{O})}(A)$ has discriminant $D' = Dp$ and level $N' = N/p$. Note that $D'N' = DN$. By Lemma 5.3.20, there is a superspecial w_{mp}-fixed point of even length if and only if all of the following occur:

- $mp = 1, 2, DN/2$ or DN,
- for all primes $q \mid Dp$, $q = 2$ or $q \equiv 3 \bmod 4$,

- for all primes $q \mid (N/p)$, $q = 2$ or $q \equiv 1 \bmod 4$.

The proof will be complete once we have individually exhausted each option from condition one and applied conditions two and three to those options. Since $p \mid mp$, $mp \neq 1$. If $mp = 2$ then $p = 2$, so $2 \nmid (DN/p)$, and $m = 1$. If $mp = DN/2$ then $p \mid (DN/2)$ and thus $p \neq 2$ because DN is square-free. It follows from the second condition that $m = DN/(2p)$ with $p \equiv 3 \bmod 4$. The only remaining case is $mp = DN$, and the second condition tells us that $p = 2$ or $p \equiv 3 \bmod 4$. □

Lemma 8.2.4. *There is a superspecial point of length divisible by three in $X_0^D(N)(\overline{\mathbb{F}}_p)$ fixed by w_{mp} if and only if one of the following occurs.*

- $p = 3$, $m = 1$, $q \equiv 2 \bmod 3$ *for all primes* $q \mid D$, *and* $q \equiv 1 \bmod 3$ *for all primes* $q \mid (N/3)$.
- $p \equiv 2 \bmod 3$, $3 \mid DN/p$, $m = DN/3p$, $q \not\equiv 1 \bmod 3$ *for all primes* $q \mid D$, *and* $q \not\equiv 2 \bmod 3$ *for all primes* $q \mid (N/p)$.
- $m = DN/p$, $p \not\equiv 1 \bmod 3$, $q \not\equiv 1 \bmod 3$ *for all primes* $q \mid D$, *and* $q \not\equiv 2 \bmod 3$ *for all primes* $q \mid (N/p)$.

Proof. By Lemma 5.2.25, if (A, ι) is a superspecial surface corresponding to a point $x \in X_0^D(N)(\overline{\mathbb{F}}_p)$ then $\mathrm{End}_{\iota(\mathcal{O})}(A)$ has discriminant $D' = Dp$ and level $N' = N/p$. Note that $D'N' = DN$. By Lemma 5.3.19, there is a superspecial w_{mp}-fixed point of length divisible by three if and only if all of the following occur:

- $mp = 1, 3, DN/3$ or DN,
- for all primes $q \mid Dp$, $q = 3$ or $q \equiv 2 \bmod 3$,
- for all primes $q \mid (N/p)$, $q = 3$ or $q \equiv 1 \bmod 3$.

The proof will be complete once we have individually exhausted each option from condition one and applied conditions two and three to those options. Since $p \mid mp$, $mp \neq 1$. If $mp = 3$ then $p = 3$, so $3 \nmid (DN/p)$, and $m = 1$. If $mp = DN/3$ then $p \mid (DN/3)$ and thus $p \neq 3$ because DN is square-free. It follows from the second condition that $m = DN/(3p)$ with $p \equiv 2 \bmod 3$. The only remaining case is $mp = DN$, and the second condition tells us that $p = 3$ or $p \equiv 2 \bmod 3$. $\square$

Lemma 8.2.5. *There is a non-superspecial $\mathbb{F}_p$-rational point of $\mathcal{Z}$ if and only if one of the following holds. Here $T_{mp} := w_m T_p$ is as in Definition 6.1.1, and acts on $H^0(X_0^D(N)_{\overline{\mathbb{F}}_p}, \Omega)$.*

- $mp = 2$ *and* $(p+1) - \mathrm{tr}(T_{mp}) > \frac{e_{Dp,N/p}(-4)}{w(-4)} + \frac{e_{Dp,N/p}(-8)}{w(-8)}$
- $mp \neq 2$, $mp \not\equiv 3 \bmod 4$ *and* $(p+1) - \mathrm{tr}(T_{mp}) > \frac{e_{Dp,N/p}(-4mp)}{w(-4mp)}$
- $mp \equiv 3 \bmod 4$ *and* $(p+1) - \mathrm{tr}(T_{mp}) > \frac{e_{Dp,N/p}(-mp)}{w(-mp)} + \frac{e_{Dp,N/p}(-4mp)}{w(-4mp)}$

Proof. Let $\mathcal{Y}_{/\mathbf{Z}_p}$ denote the smooth model of $C^D(N/p, d, m)$. By Theorem 6.2.6, $\#\mathcal{Y}(\mathbb{F}_p) = (p+1) - \mathrm{tr}(T_{pm})$. By Lemma 5.3.17, w_p acts as Frob_p on the superspecial points, so there is a superspecial point in $\mathcal{Y}(\mathbb{F}_p)$ if and only if there is a superspecial point fixed by w_{mp} in $X_0^D(N)(\overline{\mathbb{F}}_p)$. By Corollary 5.3.16, there is a superspecial point x in $X_0^D(N/p)(\overline{\mathbb{F}}_p)$ fixed by w_{mp} if and only if $\mathbf{Z}[\sqrt{-mp}]$ (or $\mathbf{Z}[\zeta_4]$ if $mp = 2$) embeds into $\mathrm{End}_{\iota(\mathcal{O})}(A)$ where (A, ι) corresponds to x.

We now count the number n_{mp} of w_{mp}-fixed superspecial points. Suppose that $\mathcal{O}'$ is an Eichler order $\mathcal{O}'$ of level N/p in B_{Dp}, $\wp_m$ is the unique two-sided ideal of norm mp in $\mathcal{O}'$, and $M_1, \ldots, M_h$ are right ideals of $\mathcal{O}'$ which form a complete set of representatives of $\mathrm{Pic}(D/p, Np)$. Under Lemma 5.2.25, n_{mp} is the number of indices i such that $M_i \cong M_i \otimes \wp_m$. Thus [Vig80, p.152], the number of such superspecial fixed points is the number of embeddings of $\mathbf{Z}[\sqrt{-mp}]$ (or $\mathbf{Z}[\zeta_4]$ if $mp = 2$) into any left order of an M_i. If $mp = 2$ the number of these is $\frac{e_{Dp,N/p}(-4)}{w(-4)} + \frac{e_{Dp,N/p}(-8)}{w(-8)}$. If $mp \neq 2$ and $mp \not\equiv 3 \bmod 4$ then the number of these is $\frac{e_{Dp,N/p}(-4mp)}{w(-4mp)}$. If $mp \equiv 3 \bmod 4$ then the number of these is $\frac{e_{Dp,N/p}(-mp)}{w(-mp)} + \frac{e_{Dp,N/p}(-4mp)}{w(-4mp)}$. $\square$

We note here that if $mp = 2$ and $e_{Dp,N/p}(-4) \neq 0$ then $p = 2$, $m = 1$, for all primes $q \mid D$, $q \equiv 3 \bmod 4$ and for all primes $q \mid (N/p)$, $q \equiv 1 \bmod 4$. Therefore by Lemma 8.2.3, there is a superspecial fixed point of even length which gives rise to an element of $C^D(N,d,m)(\mathbf{Q}_p)$. Therefore, from the perspective of giving equivalent conditions for the presence of local points, if $mp = 2$, we may assume that $e_{Dp,N/p}(-4) = 0$ and our condition becomes $(p+1) - \operatorname{tr}(T_{mp}) > \frac{e_{Dp,N/p}(-8)}{w(-8)}$. This is to say, $(p+1) - \operatorname{tr}(T_{mp}) > \frac{e_{Dp,N/p}(-4mp)}{w(-4mp)}$, precisely the condition for all other m, p such that $mp \not\equiv 3 \bmod 4$.

Theorem 8.2.6. *Let D be the discriminant of an indefinite $\mathbf{Q}$-quaternion algebra, N a square-free integer coprime to D and $p \mid N$. Then $X_0^D(N)(\mathbf{Q}_p)$ is nonempty if and only if one of the following occurs.*

1. $D = 1$.
2. $p = 2$, *for all* $q \mid D$, $q \equiv 3 \bmod 4$, *and for all* $q \mid (N/2)$, $q \equiv 1 \bmod 4$.
3. $p = 3$, $m = 1$, *for all* $q \mid D$, $q \equiv 2 \bmod 3$, *and for all* $q \mid (N/3)$, $q \equiv 1 \bmod 3$.
4. *The following inequality holds*

$$\sum_{\substack{s=-\lfloor 2\sqrt{p}\rfloor \\ s\neq 0}}^{\lfloor 2\sqrt{p}\rfloor} \left(\sum_{f \mid f(s^2-4p)} \frac{e_{D,N/p}\left(\frac{s^2-4p}{f^2}\right)}{w\left(\frac{s^2-4p}{f^2}\right)} \right) > 0.$$

Proof. First we note that if $D = 1$, then there is a $\mathbf{Q}$-rational cusp by Lemma 8.2.1. Set $m = 1$ and assume $D \neq 1$. By Lemma 8.2.2, $X_0^D(N)(\mathbf{Q}_p)$ is non-empty if and only if one of the following occurs.

- There is a superspecial w_p-fixed point of even length in $X_0^D(N)(\overline{\mathbb{F}}_p)$.

- There is a superspecial w_p-fixed point of length divisible by three in $X_0^D(N)(\overline{\mathbb{F}}_p)$.

- There is a non-superspecial $\mathbb{F}_p$-rational point.

By Lemma 8.2.3, there is a w_p fixed point of even length if and only if one of the following occurs.

- $p = 2$, for all $q \mid D$, $q \equiv 3 \bmod 4$ and for all $q \mid (N/2)$, $q \equiv 1 \bmod 4$

- $p \equiv 3 \bmod 4$ and $DN = 2p$

- $DN = p$ and $p = 2$ or $p \equiv 3 \bmod 4$

However, if either of the latter two occurs, $D = 1$ in contradiction to our assumption.

By Lemma 8.2.4, there is a w_p fixed point of length divisible by three if and only if one of the following occurs.

- $p = 3$, for all $q \mid D$, $q \equiv 2 \bmod 3$ and for all $q \mid (N/3)$, $q \equiv 1 \bmod 3$

- $p \equiv 2 \bmod 3$ and $DN = 3p$

- $DN = p$ and $p = 3$ or $p \equiv 2 \bmod 3$

Once again, if either of the latter two occurs, $D = 1$. Suppose now that in addition to $D \neq 1$, there are no superspecial points of length two, so the number of non-superspecial $\mathbb{F}_p$-rational points on $X_0^D(N/p)$ can be written as

$$(p+1) - \operatorname{tr}(T_p) - \sum_{f \mid f(-4p)} \frac{e_{Dp,N/p}\left(\frac{-4p}{f^2}\right)}{w\left(\frac{-4p}{f^2}\right)}.$$

Recall now Theorem 6.1.6, the Eichler-Selberg trace formula on $H^0(X_0^D(N/p)_{\overline{\mathbb{F}}_p}, \Omega)$:

$$\operatorname{tr}(T_p) = (p+1) - \sum_{s=-\lfloor 2\sqrt{p} \rfloor}^{\lfloor 2\sqrt{p} \rfloor} \left(\sum_{f \mid f(s^2-4p)} \frac{e_{D,N/p}\left(\frac{s^2-4p}{f^2}\right)}{w\left(\frac{s^2-4p}{f^2}\right)} \right).$$

Therefore, there is a non-superspecial $\mathbb{F}_p$-rational point of $X_0^D(N/p)$ if and only if the following quantity is nonzero.

$$\begin{aligned}
(p+1) \quad &- \quad \left((p+1) - \sum_{s=-\lfloor 2\sqrt{p}\rfloor}^{\lfloor 2\sqrt{p}\rfloor}\left(\sum_{f\mid f(s^2-4p)} \frac{e_{D,N/p}\left(\frac{s^2-4p}{f^2}\right)}{w\left(\frac{s^2-4p}{f^2}\right)}\right)\right) - \sum_{f\mid f(-4p)} \frac{e_{Dp,N/p}\left(\frac{-4p}{f^2}\right)}{w\left(\frac{-4p}{f^2}\right)} \\
&= \quad \left(\sum_{\substack{s=-\lfloor 2\sqrt{p}\rfloor \\ s\neq 0}}^{\lfloor 2\sqrt{p}\rfloor}\left(\sum_{f\mid f(s^2-4p)} \frac{e_{D,N/p}\left(\frac{s^2-4p}{f^2}\right)}{w\left(\frac{s^2-4p}{f^2}\right)}\right)\right) + \sum_{f\mid f(-4p)} \frac{e_{D,N/p}\left(\frac{-4p}{f^2}\right) - e_{Dp,N/p}\left(\frac{-4p}{f^2}\right)}{w\left(\frac{-4p}{f^2}\right)}
\end{aligned}$$

Now recall that $e_{D,N}(\Delta) = h(\Delta)\prod_{p\mid D}\left(1 - \left\{\frac{\Delta}{p}\right\}\right)\prod_{q\mid N}\left(1 + \left\{\frac{\Delta}{p}\right\}\right)$ and $f(\Delta)$ is the conductor of R_Δ. Therefore $e_{Dp,N/p}(\Delta) = \left(1 - \left\{\frac{\Delta}{p}\right\}\right)e_{D,N/p}(\Delta)$ and thus $e_{D,N/p}(\Delta) - e_{Dp,N/p}(\Delta) = \left\{\frac{\Delta}{p}\right\}e_{D,N/p}(\Delta)$. However, consider that $f(-4p) = 1$ or 2, depending on $p \bmod 4$. Moreover, if $p = 2$ then $f(-8) = 1$. Therefore, since $p \mid \frac{-4p}{f^2}$ for all $f \mid f(-4p)$, $\left\{\frac{\frac{-4p}{f^2}}{p}\right\} = 0$.

$\square$

We now find, for infinitely many pairs of integers D and N, infinitely many nontrivial twists of $X_0^D(N)$ which have points everywhere locally.

Example 8.2.7. *Let q be a prime which is $3 \bmod 4$ and consider the curve $X_0^1(q)$. We will show that if $p \equiv 1 \bmod 4$ is a prime such that $\left(\frac{q}{p}\right) = -1$ then $C^1(q,p,q)(\mathbf{Q}_v)$ is nonempty for all places v of $\mathbf{Q}$. Since $p > 0$, $C^1(q,p,q) \cong_{\mathbf{R}} X_0^1(q)$ and thus $C^1(q,p,q)(\mathbf{R}) \neq \varnothing$. We note that since $p \equiv 1 \bmod 4$, $\mathbf{Q}(\sqrt{p})$ is ramified precisely at p. Therefore if $\ell \nmid pq$ is a prime, then ℓ is unramified in $\mathbf{Q}(\sqrt{p})$. If ℓ splits in $\mathbf{Q}(\sqrt{p})$, then $C^1(q,p,q) \cong_{\mathbf{Q}_\ell} X_0^1(q)$ and thus $C^1(q,p,q)(\mathbf{Q}_\ell) \neq \varnothing$. If ℓ is inert in $\mathbf{Q}(\sqrt{p})$, then $C^1(q,p,q)(\mathbf{Q}_\ell) \neq \varnothing$ by Corollary 6.3.2.*

Since $p \equiv 1 \bmod 4$, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1$, q is inert in $\mathbf{Q}(\sqrt{p})$. Therefore by Theorem 8.0.1(b), $C^1(q,p,q)(\mathbf{Q}_q)$ is nonempty. Moreover, $\left(\frac{-q}{p}\right) = \left(\frac{q}{p}\right) = -1$ and so by Theorem 7.0.1, $C^1(q,p,q)(\mathbf{Q}_p) \neq \varnothing$.

Chapter 9

Primes dividing the quaternionic discriminant

Throughout this chapter we will fix D the discriminant of an indefinite quaternion $\mathbf{Q}$-algebra, N a squarefree integer coprime to D, a squarefree integer d, an integer $m \mid DN$ and a prime $p \mid D$ unramified in $\mathbf{Q}(\sqrt{d})$. Let w_m be as in Definition 5.2.2. Let $X_0^D(N)_{/\mathbf{Q}}$ be as defined in Corollary 5.2.14, and let $C^D(N,d,m)_{/\mathbf{Q}}$ be its twist by $\mathbf{Q}(\sqrt{d})$ and w_m. The purpose of this section is to prove the following theorem.

Theorem 9.0.1. *Suppose that $p \mid D$ is unramified in $\mathbf{Q}(\sqrt{d})$ and $m \mid DN$. Let p_i, q_j be primes such that $D/p = \prod_i p_i$ and $N = \prod_j q_j$.*

- *Suppose p is split in $\mathbf{Q}(\sqrt{d})$. Then $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if one of the following two cases occurs [Theorem 9.2.2].*

    1. *$p = 2$, $p_i \equiv 3 \bmod 4$ for all i, and $q_j \equiv 1 \bmod 4$ for all j*
    2. *$p \equiv 1 \bmod 4$, $D = 2p$, and $N = 1$*

- *Suppose that p is inert in $\mathbf{Q}(\sqrt{d})$.*

– *If* $p \mid m$*,* $C^D(N,d,m)(\mathbf{Q}_p)$ *is nonempty if and only if one of the following four cases occurs.*

1. $m = p$*,* $p_i \not\equiv 1 \bmod 3$ *for all* i*, and* $q_j \not\equiv 2 \bmod 3$ *for all* j *[Lemma 9.1.3]*
2. $m = 2p$ *and one of* $e_{D/p,N}(-4)$ *or* $e_{D/p,N}(-8)$ *is nonzero [Lemma 9.1.4]*
3. $m/p \not\equiv 3 \bmod 4$ *and* $e_{D/p,N}(-4m/p)$ *is nonzero [Lemma 9.1.4]*
4. $m/p \equiv 3 \bmod 4$ *and one of* $e_{D/p,N}(-4m/p)$ *or* $e_{D/p,N}(-m/p)$ *is nonzero [Lemma 9.1.4]*

– *If* $p \nmid m$*,* $C^D(N,d,m)(\mathbf{Q}_p)$ *is nonempty if and only if one of the following four cases occurs [Theorem 9.2.2].*

1. $p = 2$*,* $m = 1$*,* $p_i \equiv 3 \bmod 4$ *for all* i*, and* $q_j \equiv 1 \bmod 4$ *for all* j
2. $p \equiv 1 \bmod 4$*,* $m = DN/(2p)$*, for all* i*,* $p_i \not\equiv 1 \bmod 4$*, and for all* j*,* $q_j \not\equiv 3 \bmod 4$
3. $p = 2$*,* $m = DN/2$*,* $p_i \equiv 3 \bmod 4$ *for all* i*, and* $q_j \equiv 1 \bmod 4$ *for all* i
4. $p \equiv 1 \bmod 4$*,* $m = DN/p$*, for all* i*,* $p_i \not\equiv 1 \bmod 4$*, and for all* j*,* $q_j \not\equiv 3 \bmod 4$

As opposed to the case where $p \mid N$, all conditions here are determined by congruences. For completeness, we record the following.

Corollary 9.0.2. *Let* p_i*,* q_j *be primes such that* $D/p = \prod_i p_i$ *and* $N = \prod_j q_j$*.*

- *If* p *is split in* $\mathbf{Q}(\sqrt{d})$*, then* $C^D(N,d,DN) \cong X_0^D(N)$ *over* $\mathbf{Q}_p$ *and* $X_0^D(N)(\mathbf{Q}_p)$ *is nonempty if and only if one of the following two cases occurs.*

  1. $p = 2$*,* $p_i \equiv 3 \bmod 4$ *for all* i*, and* $q_j \equiv 1 \bmod 4$ *for all* j
  2. $p \equiv 1 \bmod 4$*,* $D = 2p$*, and* $N = 1$

- *If* p *is inert in* $\mathbf{Q}(\sqrt{d})$ *then* $C^D(N,d,DN)(\mathbf{Q}_p)$ *is nonempty.*

Proof. Note that $e_{D/p,N}(-4DN/p)$ is always nonzero by Theorem 4.1.28. □

To prove Theorem 9.0.1, we shall need to work with regular models for $X_0^D(N)_{\mathbf{Q}_p}$ and $C^D(N,d,m)_{\mathbf{Q}_p}$.

Definition 9.0.3. *Let $\pi : \mathcal{X} \to X_0^D(N)_{/\mathbf{Z}_p}$ denote a minimal desingularization.*

For $n \mid DN$, let w_n denote the automorphism of Definition 5.2.2. Note that extending the automorphism w_n from Definition 5.2.2 to $\mathcal{X}$ makes sense because $w_n : X_0^D(N) \to X_0^D(N)$ induces a birational morphism $\mathcal{X} \dashrightarrow \mathcal{X}$ permuting the components of $\mathcal{X}_{\mathbb{F}_p}$. Therefore w_n on $X_0^D(N)$ induces an isomorphism $\mathcal{X} \to \mathcal{X}$ [Liu02, Remark 8.3.25].

We note also that the components of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ are in W-equivariant bijection with $\mathrm{Pic}(D/p,N) \coprod \mathrm{Pic}(D/p,N)$ by Theorem 5.2.22. The intersection points, which can only link a component in one copy of $\mathrm{Pic}(D/p,N)$ to a component in the other copy of $\mathrm{Pic}(D/p,N)$ are in W-equivariant bijection with $\mathrm{Pic}(D/p,Np)$ as in Theorem 5.2.22.

The bijection of the two sets of components with two copies of $\mathrm{Pic}(D/p,N)$ is $W/\langle w_p\rangle$-equivariant. As explained in Lemma 5.2.25, w_p interchanges the two copies of $\mathrm{Pic}(D/p,N)$. The length ℓ of an intersection point $x \in X_0^D(N)(\overline{\mathbb{F}}_p)$ is given as in Definition 5.2.20. Therefore if $\ell > 1$, $\pi^*(x(\mathrm{Spec}(\overline{\mathbb{F}}_p))) = \bigcup_{i=1}^{\ell-1} C_i$ with exactly two points of C_i singular in $\mathcal{X}_{\overline{\mathbb{F}}_p}$ and for all i, $C_i \cong \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ [Ogg85, p.202]. We define the length of a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ by the length of the associated element of $\mathrm{Pic}(D/p,N)$ as in Definition 5.2.20.

Definition 9.0.4. *Let σ be such that $\langle\sigma\rangle = \mathrm{Aut}_{\mathbf{Z}_p}(\mathbf{Z}_{p^2})$. We denote by $\mathcal{Z}_{/\mathbf{Z}_p}$ the regular model of $C^D(N,d,m)_{\mathbf{Q}_p}$ obtained as the étale quotient $\mathcal{Z}$ of $\mathcal{X}_{\mathbf{Z}_{p^2}}$ by the action of $w_m \circ \sigma$.*

Note that if p is inert in $\mathbf{Q}(\sqrt{d})$ then $\mathbf{Z}_p[\sqrt{d}] \cong \mathbf{Z}_{p^2}$ and thus the generic fiber of $\mathcal{Z}$ is $C^D(N,d,m)_{\mathbf{Q}_p}$. Therefore $\mathcal{Z}$ is a regular model of $C^D(N,d,m)_{\mathbf{Q}_p}$ if p is inert in $\mathbf{Q}(\sqrt{d})$.

We also note that if p is split in $\mathbf{Q}(\sqrt{d})$, or if p is inert and $m=1$, then $C^D(N,d,m)_{\mathbf{Q}_p} \cong X_0^D(N)_{\mathbf{Q}_p}$. Therefore, if p is split in $\mathbf{Q}(\sqrt{d})$, we can consider d' to be any squarefree integer such that p is inert in $\mathbf{Q}(\sqrt{d'})$ and $\mathcal{Z}'$ to be the regular model of $C^D(N,d',1)_{\mathbf{Q}_p} \cong X_0^D(N)_{\mathbf{Q}_p}$. Therefore, we shall obtain our results when p is split as a corollary to our results when $p \nmid m$.

If $m = p$, there is a morphism π' from $\mathcal{Z}$ to the curve $M_{(D,N)/\mathbf{Z}_p}$ of Theorem 5.2.22, given by possibly blowing down components. We shall begin by discussing this case and more generally the case when $p \mid m$. As with the case $p \mid N$, we shall obtain results on $X_0^D(N)(\mathbf{Q}_p)$ as a corollary to the case when $p \nmid m$. In doing so, we recover Corollary 9.2.3, giving a new proof a theorem of Jordan-Livné on $X_0^D(1)(\mathbf{Q}_p)$[JL85, Theorem 5.6] and its extension by Ogg [Ogg85, Theorème,§1].

9.1 The proof when $p \mid m$

We begin with an elementary lemma on quadratic twists of $\mathbb{P}^1_{\overline{\mathbb{F}}_p}$.

Lemma 9.1.1. *Let $w : \mathbb{P}^1_{\mathbb{F}_p} \to \mathbb{P}^1_{\mathbb{F}_p}$ be an $\mathbb{F}_p$-rational involution. Let $\phi_1 : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ denote the p-th power map. Then the set of points $P : \mathrm{Spec}(\overline{\mathbb{F}}_p) \to \mathbb{P}^1$ such that $wP\phi_1^* = P$ contains at most two points such that $P\phi_1^* = P$.*

Proof. The set of points P such that $P = wP\phi_1^* = wP$ has cardinality at most two because w^2 is the identity but w is a nonidentity automorphism of $\mathbb{P}^1$. □

This lemma can be restated as follows. Let $M_{(D,N)}$ denote the Mumford curve of Theorem 5.2.22. Let w be an $\mathbb{F}_p$-rational involution which sends a component $C \cong \mathbb{P}^1_{\mathbb{F}_p}$ of $(M_{(D,N)})_{\mathbb{F}_p}$ to itself. Let T be the twist of C by w and $\mathbb{F}_{p^2}$. Then at most two points of $C(\mathbb{F}_p)$ lie in $T(\mathbb{F}_p)$. We can now state the following.

Lemma 9.1.2. *Let $p \mid D$ be unramified in $\mathbf{Q}(\sqrt{d})$ and $p \mid m$. Then $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if one of the following occurs.*

(1) $p = m$ and there is some component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ with length greater than one

(2) $p \neq m$ and there is a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ fixed by $w_{m/p}$

Proof. Let $\mathrm{Frob}_p = \phi_1^*$ where $\phi_1 : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ is the p-th power map. Fix a bijection from $\mathcal{Z}(\overline{\mathbb{F}}_p)$ to $\mathcal{X}(\overline{\mathbb{F}}_p)$ under which the action of $P \mapsto P\,\mathrm{Frob}_p$ is translated to the action of $P \mapsto w_m P\,\mathrm{Frob}_p$. By Lemma 5.2.25, the action of Frob_p on the components and intersection points of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$ is given by $w_m w_p = w_{m/p}$. Therefore a component or intersection point of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$ is defined over $\mathbb{F}_p$ if and only if that component or intersection point is $w_{m/p}$-fixed.

If $p = m$ this is the obvious extension of a result of Rotger-Skorobogatov-Yafaev [RSY05, Proposition 3.4]. Since $m/p = 1$ and w_1 is the identity, all components and intersection points are $\mathbb{F}_p$-rational. This sounds great except that there are generically $p+1$ $\mathbb{F}_p$-rational intersection points on each component. Namely, let y be a component and $\{x_i\}$ the intersection points on that component, so that $\ell(x_i) \mid \ell(y)$ for all i and [KR08, 3.6]

$$\sum_i \frac{1}{\ell(x_i)} = \frac{p+1}{\ell(y)}.$$

It follows that if $\ell(y) = 1$ then there are precisely $p+1$ intersection points x_i, and thus no smooth $\mathbb{F}_p$-rational points on y. Therefore if $\ell(y) = 1$ for all components of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$, $\mathcal{Z}^{sm}(\mathbb{F}_p)$ is empty and thus by Hensel's Lemma, $C^D(N,d,m)(\mathbf{Q}_p)$ is empty.

On the other hand suppose that $\ell(y) > 1$. If $\ell(x_i) = 1$ for all i, then

$$p+1 > \frac{p+1}{\ell(y)} = \sum_i \frac{1}{\ell(x_i)} = \#\{x_i\}.$$

Clearly then, there are $p+1-\#\{x_i\}$ smooth $\mathbb{F}_p$-rational points on y which lift to points of $C^D(N,d,m)(\mathbf{Q}_p)$ by Hensel's Lemma.

Suppose there exists some x which maps $\mathrm{Spec}(\overline{\mathbb{F}}_p)$ to $y \subset X_0^D(N)_{\overline{\mathbb{F}}_p}$ and $\ell(x) > 1$. Then $\pi^*(x(\mathrm{Spec}(\overline{\mathbb{F}}_p))) = \bigcup_{j=1}^{\ell(x)-1} C_j$ with $C_j \cong \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ for all j. In $\mathcal{X}_{\overline{\mathbb{F}}_p}$, $w_p C_j = C_{\ell(x)-j}$ by continuity so $w_{m/p} C_j = C_j$. It follows that C_j defines an $\mathbb{F}_p$-rational component of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$ containing at most two singular points of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$. Therefore, there is a smooth point of $\mathcal{Z}(\mathbb{F}_p)$ coming from C_j.

Now suppose that $p \mid m$ but $p \neq m$ and recall the curve $M_{/\mathbf{Z}_p}$ of Theorem 5.2.22. Let $\pi' :$

$N \to M$ be a minimal desingularization, so that $N_{\mathbb{F}_p}$ is the twist of $\mathcal{Z}_{\mathbb{F}_p}$ by $\mathbb{F}_{p^2}$ and $w_{m/p}$. Since $m \neq p$, $w_{m/p}$ is not the identity. We may apply Lemma 9.1.1 to say that $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if a component of N is fixed by $w_{m/p}$. Suppose that a component of $N_{\overline{\mathbb{F}}_p}$ is fixed by $w_{m/p}$ (under the isomorphism $N_{\overline{\mathbb{F}}_p} \cong \mathcal{Z}_{\overline{\mathbb{F}}_p} \cong \mathcal{X}_{\overline{\mathbb{F}}_p}$). Therefore there is a component y of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$ which is $\mathbb{F}_p$-rational. Since all intersection points are rational, y contains the image of a smooth $\mathbb{F}_p$ rational point. This is because at most 2 singular intersection points stayed $\mathbb{F}_p$-rational. Since there is a smooth point of $\mathcal{Z}(\mathbb{F}_p)$, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty by Hensel's Lemma. Finally we note that if a component C of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ is fixed by $w_{m/p}$ then so is its image $\pi(C)$. If $\pi(C)$ is a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$, we are done. If $\pi(C)$ is an intersection point of two components C_1, C_2 of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ then $w_{m/p}$ either fixes both of them or interchanges them. However, Theorem 5.2.22 tells us that under the bijection between components of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ and $\mathrm{Pic}(D/p,N) \coprod \mathrm{Pic}(D/p,N)$, C_1 must lie in one copy and C_2 in the other. Since these bijections are $W/\langle w_p\rangle$-equivariant, $w_{m/p}$ cannot interchange C_1 and C_2 and must therefore fix them.

□

Lemma 9.1.3. *If $p = m$ and p is inert in $\mathbf{Q}(\sqrt{d})$, then $C^D(N,d,m)(\mathbf{Q}_p) \neq \varnothing$ if and only if one of the following occurs.*

(1) For all primes $q \mid (D/p)$, either $q = 2$ or $q \equiv 3 \bmod 4$, and for all primes $q \mid N$, either $q = 2$ or $q \equiv 1 \bmod 4$.

(2) For all primes $q \mid (D/p)$, either $q = 3$ or $q \equiv 2 \bmod 3$, and for all primes $q \mid N$, either $q = 3$ or $q \equiv 1 \bmod 3$.

Proof. By Theorem 4.1.28, condition (1) is equivalent to $e_{D/p,N}(-4) \neq 0$ and condition (2) is equivalent to $e_{D/p,N}(-3) \neq 0$. Recall that the possible lengths of a component are 12 if $(D/p,N) = (2,1)$, 6 if $(D/p,N) = (3,1)$, and 1, 2 or 3 otherwise [Vig80, Proposition

V.3.1]. Therefore a component corresponding to $[I]$ has length divisible by 2 if and only if $\mathbf{Z}[\zeta_4] \hookrightarrow \mathcal{O}_l(I)$ and has length divisible by 3 if and only if $\mathbf{Z}[\zeta_6] \hookrightarrow \mathcal{O}_l(I)$. Therefore $e_{D/p,N}(-4) \neq 0$ if and only if there is a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ of length divisible by two and $e_{D/p,N}(-3) \neq 0$ if and only if there is a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ of length divisible by three. This is to say that one of the two conditions of the Lemma occurs if and only if there is a component y of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ such that $\ell(y) > 1$. But then by Lemma 9.1.2 there is such a component if and only if $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty. □

Lemma 9.1.4. *If $p \mid m$ and $p \neq m$, then $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if one of the following occurs.*

- *$m = 2p$ and one of $e_{D/p,N}(-4), e_{D/p,N}(-8)$ is nonzero.*
- *$m/p \not\equiv 3 \bmod 4$ and $e_{D/p,N}(-4m/p)$ is nonzero.*
- *$m/p \equiv 3 \bmod 4$ and one of $e_{D/p,N}(-4m/p)$ or $e_{D/p,N}(-m/p)$ is nonzero.*

Proof. Suppose that $p \mid m$ and $p \neq m$. After Lemma 9.1.2, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ is fixed by $w_{m/p}$. After Lemma 5.2.25, such a component corresponds to an element of $\mathrm{Pic}(D/p,N)$. After Lemma 5.3.16, such a component is fixed by $w_{m/p}$ if and only if there is an embedding of $\mathbf{Z}[\sqrt{-m/p}]$ (or $\mathbf{Z}[\zeta_4]$ if $m/p = 2$) into the QM endomorphisms of (A,ι). Such an embedding of an order R exists if and only if there is an optimal embedding of an order $R' \supset R$. In this case, the only orders which contain $\mathbf{Z}[\sqrt{-m/p}]$ are itself or $\mathbf{Z}\left[\frac{1+\sqrt{-m/p}}{2}\right]$ if $m/p \equiv 3 \bmod 4$. Respectively, their discriminants are $-4m/p$ and $-m/p$, so the result follows from Theorem 4.1.28. □

We close by noting that if $m/p = 1$ then $m/p \not\equiv 3 \bmod 4$. Furthermore, $e_{D/p,N}(-4) \neq 0$ if and only if for all $q \mid (D/p)$, either $q = 2$ or $q \equiv 3 \bmod 4$ and for all $q \mid N$, either $q = 2$ or $q \equiv 1 \bmod 4$. Therefore, there is a component of $X_0^D(N)_{\overline{\mathbb{F}}_p}$ of length divisible by two. Therefore, we absorb that condition of Theorem 9.0.1 into the case that $m/p \not\equiv 3 \bmod 4$.

9.2 The proof when $p \nmid m$

Once more, we shall use Hensel's Lemma to determine whether $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty in terms of $\mathcal{X}_{\overline{\mathbb{F}}_p}$. If $p \nmid m$ then the action of Frob_p on the components and intersection points of $\mathcal{Z}_{\overline{\mathbb{F}}_p} \cong \mathcal{X}_{\overline{\mathbb{F}}_p}$ coincides with the action of w_{mp}. However, by Lemma 5.2.25, the action of w_{mp} on $X_0^D(N)_{\overline{\mathbb{F}}_p}$ fixes no component. In fact, we conclude the following.

Lemma 9.2.1. *Suppose that $p \nmid m$ is unramified in $\mathbf{Q}(\sqrt{d})$. Then $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if there is a superspecial w_{mp}-fixed intersection point x of even length in $X_0^D(N)_{\overline{\mathbb{F}}_p}$.*

Proof. If $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty, then by Hensel's Lemma there is a smooth point of $\mathcal{Z}(\mathbb{F}_p)$. Therefore, there is a smooth point P of $\mathcal{X}(\overline{\mathbb{F}}_p)$ fixed by $P \mapsto w_m P\,\mathrm{Frob}_p$. By Lemma 5.2.25, the action of w_{mp} on $X_0^D(N)_{\overline{\mathbb{F}}_p}$ fixes no component. Therefore, $\pi(P) = x$ is the intersection point of two components. Since P is smooth, $\pi^*(x(\mathrm{Spec}(\overline{\mathbb{F}}_p))) \neq P(\mathrm{Spec}(\overline{\mathbb{F}}_p))$. Therefore $\ell = \ell(x) > 1$ and $\pi^*(x(\mathrm{Spec}(\overline{\mathbb{F}}_p))) = \bigcup_{i=1}^{\ell-1} C_i$ with $C_i \cong \mathbb{P}^1_{\overline{\mathbb{F}}_p}$. Since $w_{mp}(x) = x$, $w_{mp}C_i = C_{\ell-i}$. Therefore, the only component which could be fixed by w_{mp} is $C_{\ell/2}$. If such a component exists, then ℓ must be even. Since $P(\mathrm{Spec}(\overline{\mathbb{F}}_p)) \in C_i$ for some i, there must be a fixed component and thus ℓ must be even.

Conversely, if there is a superspecial w_{mp}-fixed intersection point x of even length then $\pi^*(x(\mathrm{Spec}(\overline{\mathbb{F}}_p))) = \bigcup_{i=1}^{\ell-1} C_i$. Since $w_{mp}C_{\ell/2} = C_{\ell/2}$, there is a component of $\mathcal{Z}_{\overline{\mathbb{F}}_p}$ which is defined over $\mathbb{F}_p$. It follows that there is a smooth point in $\mathcal{Z}(\mathbb{F}_p)$ and therefore $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty. □

Theorem 9.2.2. *If $p \nmid m$, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if one of the following occurs.*

1. $p = 2$, $m = 1$, $q \equiv 3 \bmod 4$ *for all* $q \mid (D/2)$, *and* $q \equiv 1 \bmod 4$ *for all* $q \mid N$.

2. $p \equiv 1 \bmod 4$, $m = DN/(2p)$, $q \not\equiv 1 \bmod 4$ *for all* $q \mid (D/p)$, *and* $q \not\equiv 3 \bmod 4$ *for all* $q \mid N$.

3. $p = 2$, $m = DN/2$, $q \equiv 3 \bmod 4$ *for all* $q \mid (D/2)$ *and* $q \equiv 1 \bmod 4$ *for all* $q \mid N$.

4. $p \equiv 1 \bmod 4$, $m = DN/p$, , $q \not\equiv 1 \bmod 4$ *for all* $q \mid (D/p)$, *and* $q \not\equiv 3 \bmod 4$ *for all* $q \mid N$.

Proof. By Lemma 9.2.1, $C^D(N,d,m)(\mathbf{Q}_p)$ is nonempty if and only if there is a superspecial w_{mp}-fixed intersection point of even length. By Corollary 5.3.20, this can occur if and only if all of the following occur.

- $mp = 1, 2, DN/2$ or DN.
- for all $q \mid (D/p)$, either $q = 2$ or $q \equiv 3 \bmod 4$
- for all $q \mid Np$, either $q = 2$ or $q \equiv 1 \bmod 4$

Since $p \mid mp$, $mp \neq 1$. If $mp = 2$ then $m = 1$ and $p = 2$. This is the first case of the Theorem. If $mp = DN/2$ then $p \neq 2$ and since $p \mid Np$, we must have $p \equiv 1 \bmod 4$. Since $m = DN/(2p)$ and $p \equiv 1 \bmod 4$, this is the second case of the Theorem. If $mp = DN$ then $m = DN/p$ and either $p = 2$ or $p \equiv 1 \bmod 4$. These are respectively the third and fourth cases of the Theorem. □

Corollary 9.2.3. *Let D be the discriminant of an indefinite $\mathbf{Q}$-quaternion algebra, N a square-free integer coprime to D and $p \mid D$. Then $X_0^D(N)(\mathbf{Q}_p)$ is nonempty if and only if one of the following occurs.*

- $p = 2$, $q \equiv 3 \bmod 4$ *for all* $q \mid (D/2)$ *and* $q \equiv 1 \bmod 4$ *for all* $q \mid N$
- $p \equiv 1 \bmod 4$, $D = 2p$ *and* $N = 1$

Proof. If $p = 2$ we are at the first case of Theorem 9.2.2. We cannot have $p = DN$ for any p since $p \mid D$ and thus D is divisible by at least two primes, so the third and fourth cases of Theorem 9.2.2 cannot occur. If $DN = 2p$ with $p \equiv 1 \bmod 4$ then by the same reasoning we must at least have $(2p) \mid D$, but then $D = 2p$ and $N = 1$. □

Finally we give a family of examples of twists of $X_0^D(N)$ which have points everywhere locally.

Example 9.2.4. *Let q be an odd prime, consider the curve $X_0^{2q}(1)$ and let g be its genus. Let $p \equiv 3 \bmod 8$ such that $\left(\frac{-p}{q}\right) = -1$ and for all odd primes ℓ less than $4g^2$, $\left(\frac{-p}{\ell}\right) = -1$. Consider the twist $C^{2q}(1, -p.2q)$ of $X_0^{2q}(1)$.*

Note that since $p \equiv 3 \bmod 8$ and $\left(\frac{-p}{q}\right) = -1$, $C^{2q}(1, -p, 2q)(\mathbf{Q}_2)$ and $C^{2q}(1, -p, 2q)(\mathbf{Q}_q)$ are both nonempty by Corollary 9.0.2.

Since $\left(\frac{-p}{q}\right) = -1$ and $p \equiv 3 \bmod 4$, $\left(\frac{q}{p}\right) = -1$. Since $p \equiv 3 \bmod 8$, $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{2}{p}\right) = -1$. Therefore $\left(\frac{-2q}{p}\right) = -1$ and $\left(\frac{-p}{2}\right) = \left(\frac{p}{2}\right) = -1$. Since we already had $\left(\frac{-p}{q}\right) = -1$, we may apply Theorem 7.0.1 to say $C^{2q}(1, -p, 2q)(\mathbf{Q}_p) \neq \varnothing$.

Let $\ell \nmid 2pq$ be a prime. If $\ell > 4g^2$ then we may apply Theorem 6.0.1 to see that $C^{2q}(1, -p.2q)(\mathbf{Q}_\ell)$ is nonempty. If $\ell < 4g^2$ then we may apply Corollary 6.3.2 to see that $C^{2q}(1, -p, 2q)(\mathbf{Q}_\ell)$ is nonempty.

Finally, since $-p < 0$, $C^{2q}(1, -p, 2q) \not\cong_{\mathbf{R}} X_0^{2q}(1)$, the latter of which does not have real points [Cla03, Theorem 55]. Therefore $(X_0^{2q}(1)/w_{2q})(\mathbf{R}) \neq \varnothing$ if and only if $C^{2q}(1, -p, 2q)(\mathbf{R})$ is nonempty. But then by Theorem 4.1.28, there is an embedding of $\mathbf{Z}[\sqrt{-2q}]$ into any maximal order in B_{2q} and thus $X_0^{2q}(1)/w_{2q}$ has real points [Ogg83, Theorem 3].

Chapter 10

A Worked Example: $X_0(14)$ twisted by w_{14}

Let d be a squarefree integer and let $C^1(14, d, 14)_{/\mathbf{Q}}$ denote the twist of $X_0(14)$ by w_{14} and $\mathbf{Q}(\sqrt{d})$. As shorthand, we may refer to this curve as $C^1(14, d)$ or even $C(14, d)$.

We note that since the genus of $X_0(14)$ is one, the genus of $C(14, d)$ is also one for all d. This does not necessarily mean that $C(14, d)$ is an elliptic curve, as it may lack $\mathbf{Q}$-rational points. We shall however study a family of squarefree integers d such that $C(14, d)$ is an elliptic curve, contingent on a well-known conjecture on ranks of elliptic curves. In fact, we will show the following.

Theorem 10.0.1. *Assuming Conjecture 10.4.1, if p is a prime congruent to one of* $17, 33$ *or* $41 \bmod 56$ *then $C(14, p)$ has infinitely many $\mathbf{Q}$-rational points, and in fact is an elliptic curve of rank one over $\mathbf{Q}$.*

We will also give applications of this theorem to the inverse Galois problem.

10.1 Local Points

To give points in $C(14,d)(\mathbf{Q})$, we will first establish some basic results on local points. In fact we will establish basic results for local points on $C^1(2q,d,2q)$ for $q \equiv 3 \bmod 4$.

Lemma 10.1.1. *If $D = 1$, $C^D(N,d,N)(\mathbf{R}) \neq \varnothing$.*

Proof. If $d > 0$, then $C^1(N,d,N) \cong_{\mathbf{R}} X_0(N)$ which has cuspidal real points. If $d < 0$, then Eichler's embedding theorem states that $\sqrt{-N} \hookrightarrow \mathcal{O}_0(N)$ and so by Ogg's theorem [Ogg83, Theorem 3] there are real points on $X_0(N)/w_N$ and thus on $C^1(N,d,N)$. $\square$

Lemma 10.1.2. *If $p \nmid 2q$ is unramified in $\mathbf{Q}(\sqrt{d})$ then $C^1(2q,d,2q)(\mathbf{Q}_p)$ is nonempty.*

Proof. Assume that $p \nmid 2q$ is unramified in $\mathbf{Q}(\sqrt{d})$, which is to say that p is either split or inert. If p is split in $\mathbf{Q}(\sqrt{d})$ then $C^1(2q,d,2q) \cong_{\mathbf{Q}_p} X_0^1(2q)$ and we know that $X_0^1(2q)(\mathbf{Q}_p) \neq \varnothing$. If p is inert in $\mathbf{Q}(\sqrt{d})$ then we may apply Corollary 6.3.2 to find $C^1(2q,d,2q)(\mathbf{Q}_p) \neq \varnothing$. $\square$

Lemma 10.1.3. *If $p = 2$ is unramified in $\mathbf{Q}(\sqrt{d})$, $C^1(2q,d,2q)(\mathbf{Q}_2)$ is nonempty if and only if $\left(\dfrac{d}{2}\right) = 1$.*

Proof. If $\left(\dfrac{d}{2}\right) = 1$, then by Theorem 8.0.1 (a), $C^1(2q,d,2q)(\mathbf{Q}_2)$ is nonempty. If $\left(\dfrac{d}{2}\right) = -1$ then by Theorem 8.0.1 (b)(ii), $C^1(2q,d,2q)(\mathbf{Q}_2)$ is empty since $q \not\equiv 1 \bmod 4$ and in terms of that theorem, $q = N/2$. $\square$

Lemma 10.1.4. *If q is unramified in $\mathbf{Q}(\sqrt{d})$, $C^1(2q,d,2q)(\mathbf{Q}_q)$ is nonempty.*

Proof. If $\left(\dfrac{d}{q}\right) = 1$, then by Theorem 8.0.1 (a), $C^1(2q,d,2q)(\mathbf{Q}_q)$ is nonempty. If $\left(\dfrac{d}{q}\right) = -1$ then by Theorem 8.0.1 (b)(ii), $C^1(2q,d,2q)(\mathbf{Q}_q)$ is nonempty since $Dq = q \equiv 3 \bmod 4$ and $N/q = 2$. $\square$

Lemma 10.1.5. *If p is ramified in $\mathbf{Q}(\sqrt{d})$ and $\left(\frac{-2q}{p}\right) = -1$ then $C^1(2q,d,2q)(\mathbf{Q}_p) \neq \varnothing$ if and only if $\left(\frac{-p}{q}\right) = 1$ if and only if $\left(\frac{-q}{p}\right) = -1$.*

Proof. This follows from Theorem 7.0.1. $\square$

Theorem 10.1.6. *Suppose that $d \equiv 1 \bmod 8$ is divisible only by primes p such that $\left(\frac{2}{p}\right) = \left(\frac{-p}{q}\right) = 1$. Then for all places v of $\mathbf{Q}$, $C^1(2q, d, 2q)(\mathbf{Q}_v)$ is nonempty. In particular, $C(14, d)(\mathbf{Q}_v) \neq \varnothing$ for all places v of $\mathbf{Q}$.*

Proof. Recall that $d \equiv 1 \bmod 8$ if and only if 2 is unramified in $\mathbf{Q}(\sqrt{d})$ and $\left(\frac{d}{2}\right) = 1$. Since $\left(\frac{d}{2}\right) = 1$, $C^1(2q, d, 2q)(\mathbf{Q}_2) \neq \varnothing$ by Lemma 10.1.3. Moreover p is ramified in $\mathbf{Q}(\sqrt{d})$ if and only if $p \mid d$. For all such p, we have $C^1(2q, d, 2q)(\mathbf{Q}_p) \neq \varnothing$ by Lemma 10.1.5. Since q is unramified in $\mathbf{Q}(\sqrt{d})$, $C^1(2q, d, 2q)(\mathbf{Q}_q) \neq \varnothing$ by Lemma 10.1.4. By Lemma 10.1.2, if $p \nmid 2q$ is unramified in $\mathbf{Q}(\sqrt{d})$, $C^1(2q, d, 2q)(\mathbf{Q}_p) \neq \varnothing$. Finally by Lemma 10.1.1, $C^1(2q, d, 2q)(\mathbf{R}) \neq \varnothing$ and the result follows. $\square$

Definition 10.1.7. *If p is an odd prime, then $p^* := (-1)^{(p-1)/2}$.*

Note that $\mathbf{Q}(\sqrt{p^*})$ is ramified precisely at the prime p.

Corollary 10.1.8. *Suppose that p is a prime such that $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{-7}{p}\right) = -1$. Then $C(14, p^*)(\mathbf{Q}_v)$ is nonempty for all places v of $\mathbf{Q}$.*

Proof. Since $\left(\frac{2}{p}\right) = 1$, $p \equiv \pm 1 \bmod 8$. Therefore $p^* \equiv 1 \bmod 8$ and we may apply Theorem 10.1.6. The result follows. $\square$

10.2 Jacobians of Twists

As we have obtained conditions for $C(14, p^*)$ to have points everywhere locally, we would like to put that information together and discover global points. Note that as $C(14, p^*)$ is a genus one curve over $\mathbf{Q}$ with points everywhere locally, there exists some elliptic curve $E_{/\mathbf{Q}}$ such that $C(14, p^*)$ is an element of $Ш(E, \mathbf{Q})$. If we can show that $Ш(E, \mathbf{Q})$ is small enough, we can show in fact that $C(14, p^*)$ represents the identity element of $Ш(E, \mathbf{Q})$, or equivalently that $C(14, p^*) \cong E$. We now explicitly determine $E_p := \mathrm{Jac}(C(14, p^*))$.

Lemma 10.2.1. *Let C be the hyperelliptic curve of genus one given by the model*

$$y^2 = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

and let C_d denote the twist of C by the hyperelliptic involution, thus given equally by the model

$$y^2 = da_4x^4 + da_3x^3 + da_2x^2 + da_1x + da_0,$$

or

$$dy^2 = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.$$

Then

1. *the Jacobian of C is given by the model*

$$y^2 = 4x^3 - x(a_0a_4 - 4a_1a_3 + 3a_2^2) - (a_0a_2a_4 + 2a_1a_2a_3 - a_0a_3^2 - a_4a_1^2 - a_2^3)$$

2. *the Jacobian of C_d is given equally by the model*

$$y^2 = 4x^3 - xd^2(a_0a_4 - 4a_1a_3 + 3a_2^2) - d^3(a_0a_2a_4 + 2a_1a_2a_3 - a_0a_3^2 - a_4a_1^2 - a_2^3)$$

or

$$dy^2 = 4x^3 - x(a_0a_4 - 4a_1a_3 + 3a_2^2) - (a_0a_2a_4 + 2a_1a_2a_3 - a_0a_3^2 - a_4a_1^2 - a_2^3)$$

In particular the Jacobian of the twist of C by $\mathbf{Q}(\sqrt{d})$ and the hyperelliptic involution is the twist of the Jacobian of C by $\mathbf{Q}(\sqrt{d})$ and the elliptic involution.

Proof. Let $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ and define $I(f) := a_0a_4 - 4a_1a_3 + 3a_2^2$ and $J(f) := a_0a_2a_4 + 2a_1a_2a_3 - a_0a_3^2 - a_4a_1^2 - a_2^3$. The result of An et al. [AKM+01, §3.2] is that the Jacobian of the curve over $\mathbf{Q}$ given by $y^2 = f(x)$ is an elliptic curve over $\mathbf{Q}$. Precisely, it is given as $y^2 = 4x^3 - I(f)x - J(f)$.

Recall now that the curve over $\mathbf{Q}$ given by $dy^2 = f(x)$ is isomorphic to the curve over $\mathbf{Q}$ given by $y^2/d = f(x)$. The isomorphism is given by the change of variables $(x, y) \mapsto (x, y/d)$. Therefore the curve over $\mathbf{Q}$ given by $dy^2 = f(x)$ is isomorphic to the curve given by $y^2 = df(x)$. Note now that $I(f)$ is a quadratic form in the coefficients of f and $J(f)$ is a cubic form in the coefficients of f. Therefore $I(df) = d^2 I(f)$ and $J(df) = d^3 J(f)$. The change of variables $(x, y) \mapsto (x/d, y/d^2)$ gives the change of models in (2). $\square$

Gonzalez [GR91] found equations for all hyperelliptic modular curves of genus $g > 0$, and moreover determined when the Atkin-Lehner involutions are hyperelliptic. In particular the hyperelliptic model for $(X_0(14), w_{14})$ is

$$y^2 = x^4 - 14x^3 + 19x^2 - 14x + 1.$$

We verify that for the hyperelliptic curve $(X_0(14), w_{14})$, $(I, J) = (300, 8158)$. Therefore, for E_p, $(I, J) = (300(p^*)^2, 8158(p^*)^3)$. Recall now that since $X_0(14)$ possesses exactly one $\mathbf{Q}$-rational two torsion point, so does E_p. We collect our results and some convenient Weierstrass forms for E_p in the following.

Corollary 10.2.2. *The elliptic curve E_p can be recognized as the standard quadratic twist of $X_0(14)$ by p^*. In particular we can write down its short Weierstrass model*

$$y^2 = x^3 + 5805(p^*)^2 x - 285714(p^*)^3$$

This elliptic curve has exactly one 2-torsion point over $\mathbf{Q}$ and when we shift that point to $(0, 0)$ we have the model

$$y^2 = x^3 + 117(p^*)x^2 + 10368(p^*)^2 x.$$

10.3 Two Descent and Shafarevich-Tate Groups

Now that we've acquired local data about $C(14, p^*)$, we need to use some Galois cohomology to generate some global data. Since it has points everywhere locally, $C(14, p^*)$ corresponds to a cohomology class ξ which is an element of $Ш(\mathbf{Q}, E_p)$. We can even show that it is an element of $Ш(\mathbf{Q}, E_p)[2]$ as follows.

In the previous subsection we saw $C(14, p^*)$ as a curve whose Jacobian is actually E_p, so ξ is not just an element of $H^1(\mathbf{Q}, \mathrm{Aut}(X_0(14))) = H^1(\mathbf{Q}, \mathrm{Aut}(E_p))$ but in fact an element of $H^1(\mathbf{Q}, E_p)$. Moreover since $C(14, p^*) \cong X_0(14) \cong E_p$ over $\mathbf{Q}(\sqrt{p})$ any cocycle representing ξ factors through the quotient $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}(\sqrt{p^*})/\mathbf{Q})$. Thus the support of any such cocycle is the support of the induced cocycle $\mathbf{Z}/2\mathbf{Z} \to E_p$. However, the cocycle condition mandates that two-torsion elements be taken to two-torsion elements, hence ξ is in the image of $H^1(\mathbf{Q}, E_p[2])$, and thus $H^1(\mathbf{Q}, E_p)[2]$.

We wish to show that $Ш(E_p, \mathbf{Q})[2]$ is trivial for each p in our congruence classes. To do this we recall for any isogeny of elliptic curves $\phi\, E \to E'$ the Kummer sequence $0 \to E[\phi] \to E \to E' \to 0$ and the induced sequence

$$0 \to \frac{E'(\mathbf{Q})}{\phi E(\mathbf{Q})} \to \mathrm{Sel}_\phi(E, \mathbf{Q}) \to Ш(E, \mathbf{Q})[\phi] \to 0$$

We are of course primarily interested in the case where $\phi = [2]$, but we are also interested in the case where ϕ is the isogeny given by modding out by a point of order 2. In this case if we let $\widehat{\phi}$ be the dual isogeny, $\phi\widehat{\phi} = \widehat{\phi}\phi = [2]$. The process of putting these together is classically known as descent via two-isogeny [Sil92, Remark X.4.7], expressed in the following exact sequences:

$$
\begin{array}{ccccccccc}
 & & 0 & & & & & & \\
 & & \downarrow & & & & & & \\
 & & \frac{E'[\widehat{\phi}](\mathbf{Q})}{\phi(E[2](\mathbf{Q})\cap E'[\widehat{\phi}](\mathbf{Q})} & & & & & & \\
 & & \downarrow & & & & & & \\
0 & \to & \frac{E'(\mathbf{Q})}{\phi E(\mathbf{Q})} & \to & \mathrm{Sel}_{\phi}(\mathbf{Q},E) & \to & Ш(\mathbf{Q},E)[\phi] & \to & 0 \\
 & & \downarrow & & & & & & \\
0 & \to & \frac{E(\mathbf{Q})}{2E(\mathbf{Q})} & \to & \mathrm{Sel}_{2}(\mathbf{Q},E) & \to & Ш(\mathbf{Q},E)[2] & \to & 0 \\
 & & \downarrow & & & & & & \\
0 & \to & \frac{E(\mathbf{Q})}{\widehat{\phi}E'(\mathbf{Q})} & \to & \mathrm{Sel}_{\widehat{\phi}}(\mathbf{Q},E') & \to & Ш(\mathbf{Q},E')[\widehat{\phi}] & \to & 0 \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}
$$

Moreover, elements of $\mathrm{Sel}_{\phi}(\mathbf{Q},E)$ and $\mathrm{Sel}_{\widehat{\phi}}(\mathbf{Q},E')$ are readily described as hyperelliptic degree 2 covers of E, E'. These correspond to squarefree elements of $\mathbf{Q}$ with zero valuation outside the primes dividing 2∞ and the primes of bad reduction. We will refer to this set of primes as S and these squarefree elements as $\mathbf{Q}(S,2)$.

For an elliptic curve in this particular Weierstrass form, Silverman [Sil92, Proposition X.4.9] gives a very explicit description of the principal homogeneous spaces in the image of $\mathbf{Q}(S,2) \cong H^1(\mathbf{Q}, E[\phi]; S)$.

For $d \in \mathbf{Q}(S,2)$ and $E = E_p$,

$$C_d : dw^2 = d^2 - (2)(3^2)(13)(p^*)(d)z^2 - (3^4)(p^*)^2(7^3)z^4$$

Here S is the set of archimedean places, places dividing 2 and the primes of bad reduction for E_p. For this S, the classes of cocycles unramified at S, $H^1(\mathbf{Q}, E_p[\phi]; S) \supset \mathrm{Sel}_{\phi}(\mathbf{Q},E)$ where ϕ is the isogeny with kernel generated by the rational 2-torsion.

Moreover, we can make the change of variables $z \mapsto z/3$ to get

$$C_d : dw^2 = d^2 - (2)(13)(p^*)(d)z^2 - (p^*)^2(7^3)z^4.$$

We will now determine which of these C_d have rational points.

Lemma 10.3.1. *On a hyperelliptic curve of even degree*

$$y^2 = a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \cdots + a_1 x + a_0$$

there are (two) rational points at infinity if and only if a_{2n} is a rational square.

Proof. A point at infinity is the a point on curve with $x = 0$ after the change of coordinates $x \mapsto 1/x$. To have this make sense, we have to make the additional substitution $y \mapsto x^n y$. When we do this substitution and set $x = 0$ we have the equation $y^2 = a_{2n}$ □

First we work with $\mathrm{Sel}_\phi(\mathbf{Q}, E_p)$. Recognize that $\mathbf{Q}(S,2) = \langle -1, 2, 7, p \rangle$. The leading term of one $f_d(z)$ such that $w^2 = f_d(z)$ determines C_d is $\frac{-343p^2}{d}$. By our lemma, C_d has rational points at infinity precisely when $d = -7$, so we have an automatic element of the Selmer group which maps to zero in Ш.

We may immediately remove 2 from consideration. Consider the Newton polygon of $f_2(z)$ over $\mathbf{Q}_2$ for $C_2 : w^2 = 2 - 26p^* z^2 - \frac{343}{2}p^2 z^4$. It is a single segment of slope $-1/2$. Therefore $f_2(z) = 0$ has no roots in $\mathbf{Q}_2$. Therefore C_2 has no points with $w = 0$. If $w \neq 0$ multiply the equation by 2. Taking v_2 of both sides of $2w^2 = 4 - 52p^* z^2 - 343p^2 z^4$ yields $1 + 2v_2(w) \geq 0$ if $v_2(z) \geq 0$. If $v_2(z) > 0$ then $1 + 2v_2(w) = 2$, which can't happen. If $v_2(z) = 0$ then $1 + 2v_2(w) = 0$, which also can't happen. Thus there are no 2-adic points on C_2 and thus it's not part of the Selmer group. Moreover, these same methods show that if $2 \mid d$ then C_d has no 2-adic points.

For $d = 7$, we can look p-adically and see there are no points when $w = 0$ by studying the Newton polygon of $f_7(z)$ over $\mathbf{Q}_7$ (recall that $\left(\frac{7}{p}\right) = -1$). Then if $v_p(z) > 0$, $2v_p(w) = 1$, which can't happen. Thus we may also remove 7 from consideration.

For $d = -1$ we use a careful application of Hensel's Lemma due to Birch and Swinnerton-Dyer on the solubility of such hyperelliptics in $\mathbf{Q}_2$. Note as we apply this that we show along the way that if $p \equiv 1 \bmod 8$, there are no $\mathbf{Q}_2$ points for $d = -p$.

Lemma 10.3.2 (BS-D,Lemma 7)**.** *Let $(x_0, y_0) \in \mathbf{Z}^2$ be a solution to $y^2 \equiv P_4(x) \bmod 2^n$ and let $l = v_2(P_4(x_0))$ and $m = v_2(P_4'(x_0))$. Then there exists a 2-adic solution $(X_0, Y_0) \equiv (x_0, y_0) \bmod 2^n$ if one of the following occurs:*

- *$P_4(x_0)$ is a 2-adic square*
- *$n > m$ and $l \geq m + n$*
- *$n > m$ and $l = m + n - 1$ and l even*
- *$n > m$ and $l = m + n - 2$ and l even and $\frac{P_4(x_0)}{2^l} \equiv 1 \bmod 4$*

If one of the following occurs, n is too small to be conclusive:

- *$m \geq n$ and $l \geq 2n$*
- *$m \geq n$ and $l = 2n - 2$ and $\frac{P_4(x_0)}{2^l} \equiv 1 \bmod 4$*

If none of the above occurs, there are no such 2-adic solutions.

Let $n = 2$ so we are working mod 4. We have solutions for $x_0 = 1, 3$ so $P_4(x_0) \equiv 28 = (2^2)(7) \bmod 32$. Thus $l = 2$ and similarly $m = 3$, moreover $P_4(x_0)/4 \equiv 7 \bmod 8$ so $P_4(x_0)$ is not a 2-adic square. Thus we have shown that if $p \equiv 1 \bmod 8$, $\mathrm{Sel}_\phi(\mathbf{Q}, E_p) \hookrightarrow \{1, -7, p, -7p\}$.

We also consider $\mathrm{Sel}_{\widehat{\phi}}(\mathbf{Q}, E'_p)$. Recall that E'_p is $y^2 = x^3 - 26px^2 - 343p^2x$ whose primes of bad reduction are $2, 7$ and p so $\mathbf{Q}(S, 2) = \langle -1, 2, 7, p\rangle$. The principal homogeneous spaces there are of the form

$$C_d : dw^2 = d^2 - 26pdz^2 + p^2 \cdot 23 \cdot 67z^4$$

None of these principal homogeneous spaces have points at infinity. If $d < 0$, there are no $\mathbf{R}$-points. The same 2-adic Newton polygon argument carries over verbatim for $2 \mid d$ and for $d = 7$ the same valuation argument carries over. Thus $\#\,\mathrm{Sel}_{\widehat{\phi}}(\mathbf{Q}, E'_p)) \leq 3$ and so $\dim_2 \mathrm{Sel}_{\widehat{\phi}}(\mathbf{Q}, E'_p) \leq 1$. Then we note this implies $\mathrm{rank}(E'_p(\mathbf{Q})) \leq 1$ and $\dim_2 Ш(\mathbf{Q}, E'_p)[\widehat{\phi}] \leq 1$.

10.4 The L-function and the parity conjecture

It follows from work of previous sections both that $\mathrm{rank}(E_p(\mathbf{Q})) \leq 1$ and $\dim_2 Ш(\mathbf{Q}, E_p)[\phi] \leq 1$ since we already know that $E_p[\phi](\mathbf{Q}) \neq (0)$. We note now that $X_0(14)$ has rank zero and the sign of the functional equation for its L-function is $+1$. Therefore [Cla07, Theorem 3], the sign in the functional equation of $L(E_p, s)$ is -1 precisely when $p \equiv 1 \bmod 4$, as is our case here.

We now make use of the following weaker form of the Birch and Swinnerton-Dyer conjecture.

Conjecture 10.4.1 (The Parity Conjecture)**.** *The order of vanishing of $L(E_p, s)$ is congruent to the parity of the rank of $E_p(\mathbf{Q})$ modulo two.*

Assuming this, we have $\mathrm{rank}(E_p(\mathbf{Q})) = 1$ and $Ш(\mathbf{Q}, E_p)[\phi] = (0)$. To get our result, we need $Ш(\mathbf{Q}, E_p)[2] = 0$. Moreover since isogenies preserve the rank of an elliptic curve, $E'_p(\mathbf{Q})$ has rank one and $Ш(\mathbf{Q}, E'_p)[\widehat{\phi}] = (0)$.

Theorem 10.4.2. *Assuming the parity conjecture,* $Ш(\mathbf{Q}, E_p)[2] = 0$ *and thus* $E_p \cong C(14, p)$ *for* $p \equiv 17, 33, 41 \bmod 56$. *Moreover, in that case E_p is an elliptic curve of rank one.*

Proof. If the parity conjecture is true, then E_p has rank one. It follows that $Ш(\mathbf{Q}, E_p)[\phi] = Ш(\mathbf{Q}, E'_p)[\widehat{\phi}] = (0)$. We may then apply the exact sequence [Sil92, Proposition X.6.2]

$$0 \to Ш(\mathbf{Q}, E)[\phi] \to Ш(\mathbf{Q}, E)[2] \to Ш(\mathbf{Q}, E')[\phi]$$

to obtain that $Ш(\mathbf{Q}, E_p)[2] = (0)$. It follows then, since $C(14, p)$ defines a cocycle in $Ш(\mathbf{Q}, E_p)[2]$ which is trivial according to whether $C(14, p) \cong E_p$ or not, that $C(14, p) \cong E_p$, an elliptic curve of rank one. □

10.5 An application to the inverse Galois problem

Recall the following theorem of Shih.

Theorem 10.5.1 (K.-y. Shih, 1974)**.** *Suppose p is an odd prime such that either $\left(\frac{2}{p}\right), \left(\frac{3}{p}\right)$ or $\left(\frac{7}{p}\right) = -1$. Then there exists a Galois extension $L/\mathbf{Q}$ such that* $\mathrm{Gal}(L/\mathbf{Q}) = \mathrm{PSL}_2(\mathbf{Z}/p\mathbf{Z})$.

This was accomplished by studying twists of $X_0(N)$ by $\mathbf{Q}(\sqrt{p^*})$ and w_N where $X_0(N)$ has genus zero. In particular, if $N \in \{2, 3, 7\}$ then there are rational points on $C^1(N, p^*, N)$ when $\left(\frac{N}{p}\right) = -1$. The latter condition guarantees that a twist of the full p-torsion representation of the universal elliptic curve over all but finitely many points of $X_0(N)$ is regular. Therefore by Hilbert's Irreducibility Theorem, this descends down to $\mathbf{Q}$.

In his "Topics in Galois Theory" [Ser08], Serre proposed a complement to Shih's theorem where we can relax the condition that $C^1(N, p^*, N)$ is $\mathbb{P}^1$ to the condition that $C^1(N, p^*, N)$ is a curve with infinitely many rational points. This was used to show that, contingent on the parity conjecture, $N = 11$ or 19 can also be used [Cla07].

Note however that for all $N \in \{2, 3, 7, 11, 19\}$, there is already a w_N-fixed point in $X_0(N)(\mathbf{Q})$ and these are the only N for which this can occur. The following shows that this is not an obstacle to generating Galois groups.

Corollary 10.5.2. *Assuming the parity conjecture, if* p *is a prime congruent to one of* $17, 33$ *or* $41 \bmod 56$ *then* $\mathrm{PSL}_2(\mathbf{Z}/p\mathbf{Z})$ *is a Galois Group over* $\mathbf{Q}$.

Chapter 11

Bibliography

[AK70] Allen Altman and Steven Kleiman, *Introduction to Grothendieck duality theory*, Lecture Notes in Mathematics, Vol. 146, Springer-Verlag, Berlin, 1970.

[AKM+01] Sang Yook An, Seog Young Kim, David C. Marshall, Susan H. Marshall, William G. McCallum, and Alexander R. Perlis, *Jacobians of genus one curves*, J. Number Theory **90** (2001), no. 2, 304–315.

[BC91] J.-F. Boutot and H. Carayol, *Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfel′d*, Astérisque (1991), no. 196-197, 7, 45–158 (1992), Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[BE92] J. Brzezinski and M. Eichler, *On the imbeddings of imaginary quadratic orders in definite quaternion orders*, J. Reine Angew. Math. **426** (1992), 91–105.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990.

[Buz97] Kevin Buzzard, *Integral models of certain Shimura curves*, Duke Math. J. **87** (1997), no. 3, 591–612.

[CES03] Brian Conrad, Bas Edixhoven, and William Stein, $J_1(p)$ *has connected fibers*, Doc. Math. **8** (2003), 331–408 (electronic).

[Cla03] Pete L. Clark, *Rational points on Atkin-Lehner quotients of Shimura curves*, Ph.D. thesis, Harvard, 2003.

[Cla07] ______, *Galois groups via Atkin-Lehner twists*, Proc. Amer. Math. Soc. **135** (2007), no. 3, 617–624 (electronic).

[Cox89] David A. Cox, *Primes of the form* $x^2 + ny^2$, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989, Fermat, class field theory and complex multiplication.

[Del69] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.

[Dri76] V. G. Drinfel′d, *Coverings of p-adic symmetric domains*, Funkcional. Anal. i Priložen. **10** (1976), no. 2, 29–40.

[Eic56] Martin Eichler, *Modular correspondences and their representations*, J. Indian Math. Soc. (N.S.) **20** (1956), 163–206.

[Eic73] ———, *The basis problem for modular forms and the traces of the Hecke operators*, Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 75–151. Lecture Notes in Math., Vol. 320.

[FC90] Gerd Faltings and Ching-Li Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 22, Springer-Verlag, Berlin, 1990, With an appendix by David Mumford.

[GR91] Josep Gonzàlez Rovira, *Equations of hyperelliptic modular curves*, Ann. Inst. Fourier (Grenoble) **41** (1991), no. 4, 779–795.

[GR04] Josep González and Victor Rotger, *Equations of Shimura curves of genus two*, Int. Math. Res. Not. (2004), no. 14, 661–674.

[GR06] ———, *Non-elliptic Shimura curves of genus one*, J. Math. Soc. Japan **58** (2006), no. 4, 927–948.

[Gro64] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I*, Inst. Hautes Études Sci. Publ. Math. (1964), no. 20.

[Hel03] David Helm, *Jacobians of Shimura curves and Jacquet-Langlands correspondences*, Ph.D. thesis, Berkeley, 2003.

[Hel07] ———, *On maps between modular Jacobians and Jacobians of Shimura curves*, Israel J. Math. **160** (2007), 61–117.

[JL85] Bruce W. Jordan and Ron A. Livné, *Local Diophantine properties of Shimura curves*, Math. Ann. **270** (1985), no. 2, 235–248.

[Kan11] Ernst Kani, *Products of CM elliptic curves*, Collect. Math. **62** (2011), no. 3, 297–339.

[Kir10] Franz Kiraly, *Wild quotient singularities of arithmetic surfaces and their regular models*, Ph.D. thesis, Ulm, 2010.

[KR08] Aristides Kontogeorgis and Victor Rotger, *On the non-existence of exceptional automorphisms on Shimura curves*, Bull. Lond. Math. Soc. **40** (2008), no. 3, 363–374.

[Kur79] Akira Kurihara, *On some examples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25** (1979), no. 3, 277–300.

[Lan87] Serge Lang, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987, With an appendix by J. Tate.

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications.

[LMB00] Gérard Laumon and Laurent Moret-Bailly, *Champs algébriques*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 39, Springer-Verlag, Berlin, 2000.

[Lor11] Dino J. Lorenzini, *Wild models of curves*, http://www.math.uga.edu/ lorenz/Paper2.pdf, 2011.

[Mes72] William Messing, *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Mathematics, Vol. 264, Springer-Verlag, Berlin, 1972.

[Mil79] James S. Milne, *Points on Shimura varieties mod p*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 165–184.

[Mil80] ———, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.

[Mil86] ———, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.

[Mil11] ———, *Class field theory*, http://www.jmilne.org/math/CourseNotes/cft.html, 2011.

[Mol10] Santiago Molina, *Ribet bimodules and the specialization of Heegner points*, http://www.crm.es/Publications/10/Pr928.pdf, 2010.

[Mor70] Yasuo Morita, *Ihara's conjectures and moduli space of abelian varieties*, Master's Thesis, University of Tokyo, 1970.

[Ogg74] Andrew P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462.

[Ogg83] ———, *Real points on Shimura curves*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 277–307.

[Ogg85] ———, *Mauvaise réduction des courbes de Shimura*, Séminaire de théorie des nombres, Paris 1983–84, Progr. Math., vol. 59, Birkhäuser Boston, Boston, MA, 1985, pp. 199–217.

[Ozm09] Ekin Ozman, *Local points on quadratic twists of* $X_0(n)$, http://arxiv.org/abs/0911.4537, 2009.

[Piz76] Arnold Pizer, *On the arithmetic of quaternion algebras*, Acta Arith. **31** (1976), no. 1, 61–89.

[Rib89] Kenneth A. Ribet, *Bimodules and abelian surfaces*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 359–407.

[Rot04] Victor Rotger, *Shimura curves embedded in Igusa's threefold*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 263–276.

[RS11] Ken Ribet and William Stein, *Lectures on modular forms and Hecke operators*, http://wstein.org/books/ribet-stein/main.pdf, 2011.

[RSY05] Victor Rotger, Alexei Skorobogatov, and Andrei Yafaev, *Failure of the Hasse principle for Atkin-Lehner quotients of Shimura curves over* $\mathbb{Q}$, Mosc. Math. J. **5** (2005), no. 2, 463–476, 495.

[S+12] W. A. Stein et al., *Sage Mathematics Software (Version 4.8)*, The Sage Development Team, 2012, `http://www.sagemath.org`.

[Sad10] Mohammad Sadek, *On quadratic twists of hyperelliptic curves*, http://arxiv.org/abs/1010.0732, 2010.

[Ser73] Jean-Pierre Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.

[Ser79] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[Ser08] ———, *Topics in Galois theory*, second ed., Research Notes in Mathematics, vol. 1, A K Peters Ltd., Wellesley, MA, 2008, With notes by Henri Darmon.

[SGA03] *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3, Société Mathématique de France, Paris, 2003, Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original.

[Shi67] Goro Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) **85** (1967), 58–159.

[Shi71] ———, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971, Kanô Memorial Lectures, No. 1.

[Shi79] Tetsuji Shioda, *Supersingular $K3$ surfaces*, Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978), Lecture Notes in Math., vol. 732, Springer, Berlin, 1979, pp. 564–591.

[Shi10] Goro Shimura, *Arithmetic of quadratic forms*, Springer Monographs in Mathematics, Springer, New York, 2010.

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Vie77] Eckart Viehweg, *Invarianten der degenerierten Fasern in lokalen Familien von Kurven*, J. Reine Angew. Math. **293/294** (1977), 284–308.

[Vig80] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.