

## INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

**The quality of this reproduction is dependent upon the quality of the copy submitted.** Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

**UMI<sup>®</sup>**

Bell & Howell Information and Learning  
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA  
800-521-0600



Diophantine Properties of Atkin-Lehner Quotients of  
Shimura Curves

by

Srinath Baba

A dissertation submitted to the Graduate Faculty in  
Mathematics in partial fulfillment of the requirements  
for the degree of Doctor of Philosophy,  
The City University of New York.

1999

**UMI Number: 9946135**

---

**UMI Microform 9946135**  
**Copyright 1999, by UMI Company. All rights reserved.**

**This microform edition is protected against unauthorized  
copying under Title 17, United States Code.**

---

**UMI**  
**300 North Zeeb Road**  
**Ann Arbor, MI 48103**

This manuscript has been read and accepted by the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

23 April 1999  
Date

Bruce W. Jordan  
Chair of Examining Committee

23 April 1999  
Date

J. O. G.  
Executive Officer

Bruce W. Jordan Bruce W. Jordan

Raymond Hoobler Raymond T. Hoobler

Carlos J. Moreno Carlos J. Moreno

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

# Abstract

## Diophantine Properties of Atkin-Lehner Quotients of Shimura Curves

by

Srinath Baba

Advisor: Bruce Jordan

Let  $V_{\mathbf{B}}$  be the Shimura curve attached to an indefinite rational quaternion algebra  $\mathbf{B}$  of odd discriminant  $D$ , and  $W$  be the group of Atkin-Lehner involutions acting on it. In this thesis, we study the Diophantine properties of quotients  $V_{\mathbf{B}}/G$ , where  $G$  is any subgroup of  $W$ .

We analyse the existence of rational points over local fields. Using the results obtained, we study the existence of divisors and divisor classes of degree  $d$  over local fields. Using this information, we analyse the Cassels-Tate pairing on  $\text{III}(A/Q)$ , where  $A = \text{Pic}^0(V_{\mathbf{B}}/G)$ , and conclude exactly when it is alternating and when it fails to be alternating, using the criteria of Poonen and Stoll.

.

## Contents

Introduction	1
Chapter 1. Shimura curves and Atkin-Lehner involutions	6
1. Rational quaternion algebras and maximal orders	6
2. Shimura curves and their moduli interpretation	7
3. Atkin-Lehner involutions on $V_{\mathbf{B}}$	9
4. CM points and fixed points of modular involutions	9
Chapter 2. Bad reduction of Atkin-Lehner quotients	13
1. The $p$ -adic upper half plane and admissible curves	13
2. The Cerednik-Drinfeld $p$ -adic uniformization	15
3. Bad reduction of $V^G$ and the dual graph.	17
4. Rational points on $V^G$ defined over $K/\mathbb{Q}_p$	19
Chapter 3. Divisors and divisor classes over completions of $\mathbb{Q}$	25
1. Points, divisors and divisor classes on $V^G$ over $\mathbb{R}$	25
2. The non-archimidean case: divisors over local fields	26
3. Divisor classes over local fields	29
Chapter 4. Shimura curve quotients with odd jacobians	35
1. The Shafarevich-Tate group and the Cassels-Tate pairing	35
2. The Poonen-Stoll theory of odd and even abelian varieties	37
3. Shimura curve quotients with odd jacobians	38

CONTENTS

v

Chapter 5. Families of quotients with odd jacobians	43
1. Families from $\mathbf{B}(pq)$	43
2. Families from $\mathbf{B}(pqrs)$ .	45
3. The invariant $\mathbf{N}(V^G)$	46
Appendix A - PARI code for calculating odd quotients	49
Appendix B - Some results from the program	56
Bibliography	67

## Introduction

Let  $\mathbf{B}$  be an indefinite quaternion algebra defined over  $\mathbb{Q}$ , and let  $\mathfrak{m} \subset \mathbf{B}$  be a maximal order. Since  $\mathbf{B}$  is indefinite, we have an isomorphism  $f : \mathbf{B} \otimes_{\mathbb{Q}} \mathbb{R} \rightarrow \mathbb{M}_2(\mathbb{R})$ . The image of  $f$  on  $\mathfrak{m}$  is a discrete subgroup of  $\mathbb{M}_2(\mathbb{R})$ , and the units in  $\mathfrak{m}$  embed as a discrete subgroup  $\Gamma$  of  $SL_2(\mathbb{R})$ . It is well known that  $\Gamma$  is a Fuchsian group of the first kind, and is cocompact. Hence, the quotient  $\Gamma \backslash \mathcal{H}$  is a compact Riemann surface  $C_{\mathbf{B}}$ , where  $\mathcal{H}$  is the Poincaré upper half plane. Shimura observed that the curves  $C_{\mathbf{B}}$  parametrise abelian surfaces with an action by  $\mathfrak{m}$ , and that  $C_{\mathbf{B}}$  has a canonical model  $V_{\mathbf{B}}$  over  $\mathbb{Q}$ . We call  $V_{\mathbf{B}}$  the Shimura curve attached to the quaternion algebra  $\mathbf{B}$ .

Since the early 1970s people have been studying the diophantine arithmetic of Shimura curves. In the local archimedean setting, Ogg and Michon classified hyperelliptic Shimura curves and studied real points on Shimura curves and certain quotients. Kurihara, Cerednik and Drinfeld studied models for the bad reduction of Shimura curves. Jordan and Livné studied questions about the existence of rational points, divisors and divisor classes on Shimura curves over local fields. More recently, works of Ribet, Wiles and others, have generated a lot of interest in the study of Shimura curves, mainly because of their connections to elliptic modular curves, Galois representations, and the Langlands correspondence.

Shimura curves, like modular curves, come with a set  $W_{\mathbf{B}}$  of canonical modular involutions on them, called the Atkin-Lehner involutions. These form a finite group of involutions defined over  $\mathbb{Q}$ . Let  $G$  be any subgroup of the group of Atkin-Lehner involutions, and consider the curve  $V^G = V_{\mathbf{B}}/G$ , this curve has a model defined over  $\mathbb{Q}$ . In this thesis, I study the diophantine arithmetic of such quotients.

In [JL3] in 1998, Jordan and Livne examined the local diophantine arithmetic of a quotient of a Shimura curve in one particular situation, where  $\mathbf{B}$  has discriminant  $pq$  and  $G$  is generated by a single involution. The main motivation of this study was to generate families of Shimura curve quotients whose jacobians are “odd” as defined by Poonen and Stoll. In brief, the Poonen-Stoll theory is as follows:

Let  $A/K$  be an principally polarized abelian variety, where  $K$  is a global field. The Shafarevich-Tate group  $\text{III}(A/K)$ , which classifies isomorphism classes of locally trivial principal homogeneous spaces over  $A$  is conjecturally finite. From work of Cassels and Tate ([Ta]), it is known that there is a bilinear pairing on  $\text{III}(A/K) \times \text{III}(\hat{A}/K)$ , where  $\hat{A}$  is the dual of  $A$ , and from the polarization on  $A$ , we have a pairing  $\langle, \rangle$  on  $\text{III}(A/K) \times \text{III}(A/K)$ . In the case of elliptic curves, Cassels and Tate showed that this pairing (called the Cassels-Tate pairing) is alternating, i.e.,  $\langle x, y \rangle = -\langle y, x \rangle$  and hence,  $\text{III}(A/K)$  has even order. In the higher dimensional situation, Poonen and Stoll showed that the Cassels-Tate pairing is *not* necessarily alternating, it is antisymmetric, i.e.  $\langle x, x \rangle = 0$ . By studying the pairing, Poonen and Stoll show

that a certain principal homogeneous space over  $A$  can generate a non-trivial 2-torsion class in  $\text{III}(A/K)$ . Hence, the (conjectural) structure of  $\text{III}(A/K)$  is of the form  $\mathbb{Z}/2\mathbb{Z} \times G \times G$  (the odd case), or  $G \times G$  (the even case), for a finite abelian group  $G$ . In addition, they gave local diophantine criteria on curves to decide if their jacobians (equipped with the canonical polarization) are odd or even. In particular, by using the local diophantine results in [JL1], they showed that Shimura curves all have even jacobians, and that a positive proportion of hyperelliptic curves of even genus over  $\mathbb{Q}$  have odd jacobians. In their 1998 paper [JL3], Jordan and Livne produced the first known set of examples of non-hyperelliptic curves of arbitrarily high genus with odd jacobians, these curves are Atkin-Lehner quotients of Shimura curves of discriminant  $pq$ .

In this thesis, I study the diophantine arithmetic of Atkin-Lehner quotients of Shimura curves of arbitrary discriminant by arbitrary subgroups  $G \subset W_{\mathbf{B}}$ , with the aim of producing new examples of quotients with odd jacobians. In order to apply the Poonen-Stoll test, we need to study the existence of rational divisors of specific degree on the curve  $V^G$  over local fields. To study this, we need to establish criteria for the existence of points on  $V^G$  over local fields. In Chapter 2, I prove the following:

**Theorem 1.** *If  $K/\mathbb{Q}_p$  is a finite extension, where  $p$  is a prime of bad reduction of  $V_{\mathbf{B}}$  and  $w_p \notin G$ , then  $V^G(K) \neq \emptyset$  if and only if*

- (a)  *$f(K/\mathbb{Q}_p)$  is even, or*
- (b)  *$e(K/\mathbb{Q}_p)$  is even, and  $\exists w_d \in G$ ,  $p \nmid d$ , so that  $\mathbb{Q}(\sqrt{-pd})$  splits  $\mathbf{B}$ ,*

or

(c)  $\exists w_d \in G, p|d$  so that  $\mathbb{Q}(\sqrt{-pd})$  splits  $\mathbf{B}^{p-int}$ , where  $\mathbf{B}^{p-int}$  is the definite quaternion algebra of discriminant  $D/p$ , or

(d)  $\exists w_{d_1}, w_{d_2} \in G$ , so that  $\mathbf{B}^{p-int} \simeq \mathbf{B}(-d_1p, -d_2)$

In [JL2], Jordan and Livne establish criteria for existence of divisors on  $V_{\mathbf{B}}$  over local fields  $K/\mathbb{Q}_p$ , where  $p$  is a prime of bad reduction of  $V_{\mathbf{B}}$ . Using the theorem above, it is easy to extend their results to  $V^G$ . Let  $\text{Pic}^d(V^G)(K)$  denote the set of degree  $d$  divisor classes defined over  $K$ , and  $\text{Pic}^d(V^G)(K)^+$  be the subset of degree  $d$  divisor classes represented by a divisor over  $K$ , we have the following proposition.

**Proposition 2.**  $\text{Pic}^d(V^G)(K)^+ = \emptyset$  if and only if  $d$  is odd and  $V^G(K) = \emptyset$ .

Theorem 1 and proposition 2 suffice to construct families of quotients with odd jacobians. I outline this below.

Another interesting question that comes up is to decide when there are divisor *classes* over local fields, i.e., when  $\text{Pic}^d(V^G)(K) \neq \emptyset$ . The following settles this:

**Theorem 3.**  $\text{Pic}^d(V^G)(K) = \emptyset$  if and only if  $\text{Pic}^d(V^G)(K)^+ = \emptyset$ , and the genus  $g(V^G)$  is odd.

In Chapter 4, I outline the Poonen-Stoll theory of odd and even jacobians. In order to produce families of Shimura curve quotients with odd jacobians, one needs to decide which quotients can have even genus. Using the Eichler mass formula and the Riemann-Hurwitz theorem, it

is easy to calculate which quotients can have odd jacobians.

**Theorem 4.**  $V^G/\mathbb{Q}$  has odd jacobian only if  $[W_{\mathbf{B}} : G] = 2$ , and  $w_D \notin G$ , where  $D = \text{Disc}\mathbf{B}$

To construct families of curves with odd jacobians, one then needs only to look at quotients satisfying the conditions in the previous theorem. Once we have picked  $G$  satisfying these conditions, we use the proposition to generate the families of curves. In chapter 5, I construct families of quotients in the situation where  $D$  is a product of 4 primes. I also produce new examples in the situation  $D = pq$ , to extend the families produced in [JL3]. Some examples are:

**Example 1.**  $V_{\mathbf{B}(39)}/w_3$  has odd jacobian.

**Example 2.**  $V_{\mathbf{B}(5 \cdot 7 \cdot 11 \cdot 79)}/G$ , where  $G$  is generated by  $w_7, w_{11}$  and  $w_5$ , has odd jacobian.

Using the results above, I define a numerical invariant  $\mathbf{N}(V^G)$  which measures the number of primes where  $V^G$  does not have divisors of degree 1, and the parity of the genus of  $V^G$ . Its definition shows that  $\mathbf{N}(V^G)$  is odd if and only if  $V^G$  has odd jacobian over  $\mathbb{Q}$ . This invariant is easy to calculate, and I demonstrate how to code it using PARI, and calculate examples using it.

I would like to thank Bruce Jordan for having guided me through this thesis, and for being a wonderful advisor and friend. Thanks are also due to Ray Hoobler and Shiv Sikri for many helpful discussions, and to Florian Lengyel for having written the program in appendix A. Finally I would like to express my gratitude to all my friends at CUNY,

especially Jack Levinson, Ananya Mukherjea and Effie Maclachlan, for their support and love.

## CHAPTER 1

### Shimura curves and Atkin-Lehner involutions

#### 1. Rational quaternion algebras and maximal orders

Let  $\mathbf{B}/\mathbb{Q}$  be a central simple algebra of rank 4. If  $p$  is any prime in  $\mathbb{Z}$ , we can extend the scalars of  $\mathbf{B}$  to  $\mathbb{Q}_p$  to get  $\mathbf{B}_p = \mathbf{B} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ , which is a rank 4 central simple algebra over  $\mathbb{Q}_p$  ( we let  $\mathbb{Q}_{\infty} = \mathbb{R}$ ). There are exactly two isomorphism classes of quaternion algebras over  $\mathbb{Q}_p$ : they are  $\mathbb{M}_2(\mathbb{Q}_p)$  and  $\mathbb{H}_p$ , the quaternion division algebra (in the case  $p = \infty$ , this is the Hamiltonian quaternions).

$\mathbf{B}$  is said to *ramify* at  $p$  if and only if  $\mathbf{B}_p \simeq \mathbb{H}_p$ , and  $\mathbf{B}$  is said to *split* at  $p$  otherwise. The product of all finite primes ramified in  $\mathbf{B}$  is called the *discriminant* of  $\mathbf{B}$ , denoted  $\text{Disc}\mathbf{B}$ . A classical theorem of Hasse states that  $\mathbf{B}$  is completely determined by the set of primes where it ramifies, and the number of ramified primes in  $\mathbf{B}$  is always even. Furthermore, for any given finite set of primes of even cardinality, there is a unique quaternion algebra ramified exactly at the given primes. If  $\infty$  is ramified in  $\mathbf{B}$ , then  $\mathbf{B}$  is called *definite*, otherwise it is *indefinite*.

There is a natural basis for  $\mathbf{B}$  over  $\mathbb{Q}$  of the form  $\{1, i, j, k\}$ , where  $i \cdot j = -j \cdot i = k$ . Furthermore,  $i^2 = r, j^2 = s$ , where  $r, s \in \mathbb{Q}$ . We write  $\mathbf{B} = \mathbf{B}(r, s)$ . The following is well known, see for example [Vig].

**Lemma 1.1.1.**  $\mathbf{B}(r, s)$  is ramified at a prime  $p$  if and only if the Hilbert symbol  $(r, s)_p = -1$ .

$\mathbf{B}(r, s)$  is definite if and only if both  $r$  and  $s$  are negative rational numbers. For example,  $\mathbf{B}(-1, -1)$ , the Hamiltonian quaternion algebra, is definite, while  $\mathbf{B}(-19, 6)$  is indefinite. (in fact, it has discriminant 6, which is a product of 2 primes).

If  $\mathbf{B} = \mathbf{B}(r, s)$ , then we can define the *reduced norm*  $N_{\mathbf{B}/\mathbb{Q}}$  and *trace*  $\text{Tr}_{\mathbf{B}/\mathbb{Q}}$  as follows: if  $\alpha \in \mathbf{B}, \alpha = x + iy + jz + kw$ , where  $x, y, z, w \in \mathbb{Q}$  and  $i^2 = r, j^2 = s, ij = -ji = k$ , then

$$N_{\mathbf{B}/\mathbb{Q}}(\alpha) = x^2 - ry^2 - sz^2 + rsw^2, \text{ and } \text{Tr}_{\mathbf{B}/\mathbb{Q}}(\alpha) = 2x.$$

An order  $\mathfrak{m}$  in  $\mathbf{B}$  is a  $\mathbb{Z}$  algebra of rank 4 in  $\mathbf{B}$ .  $\mathfrak{m}$  is maximal if it is not contained in any other order; from the Skolem-Noether theorem it follows that all maximal orders in a quaternion algebra are conjugate.

If  $\mathfrak{m}$  is a maximal order in  $\mathbf{B}$ , we let  $\mathfrak{m}^\times$  denote the units in  $\mathfrak{m}$ , and  $\mathfrak{m}_+^\times$  denote the units of positive norm in  $\mathfrak{m}$ .

## 2. Shimura curves and their moduli interpretation

Following the notation from the previous section, we fix  $\mathbf{B}$ ,  $\mathfrak{m}$  and  $\mathfrak{m}_+^\times$ . We also recall that by the Skolem-Noether theorem,  $\mathfrak{m}$ , and hence  $\mathfrak{m}_+^\times$  is unique upto conjugation in  $\mathbf{B}$ .

Since  $\mathbf{B}$  is indefinite, there is an isomorphism

$$\Theta : \mathbf{B} \otimes_{\mathbb{Q}} \mathbb{R} \longrightarrow \mathbb{M}_2(\mathbb{R}).$$

If we restrict the  $\Theta$  action to  $\mathfrak{m}_+^\times$ , we get

$$\Theta|_{\mathfrak{m}_\mp^*} : \mathfrak{m}_\mp^* \hookrightarrow \mathrm{SL}_2(\mathbb{R})$$

If  $\Gamma$  is the image of  $\mathfrak{m}_\mp^*$  in  $\mathrm{SL}_2(\mathbb{R})$ , then clearly  $\Gamma$  is a discrete subgroup of  $\mathrm{SL}_2(\mathbb{R})$ . Poincare observed that  $\Gamma$  is a Fuchsian group of the first kind, i.e., it is cocompact. Hence,  $\Gamma$  acts on the upper half plane  $\mathcal{H}$ , and the quotient is a compact Riemann surface. Since all choices of maximal order  $\mathfrak{m}$  in  $\mathbf{B}$  are conjugate, the isomorphism type of the quotient Riemann surface is independent of the choice of maximal order in  $\mathbf{B}$  and the embedding  $\Theta$ . We denote it by  $C_{\mathbf{B}}$ .

Shimura showed that  $C_{\mathbf{B}}$  has a moduli interpretation as follows:  $C_{\mathbf{B}}$  is the coarse moduli scheme over  $\mathbb{C}$  that classifies isomorphism classes of abelian surface  $(A, i, C)$ , where  $A/\mathbb{C}$  is an abelian surface,  $i : \mathfrak{m} \hookrightarrow \mathrm{End}(A)$  is an injection, and  $C$  is a weak polarization on  $A$  so that  $\mathrm{Ros}(C)$ , the Rosati involution attached to  $C$  is “compatible” with  $i$ , i.e.,  $\mathrm{Ros}(C)(i(b)) = i(b^*)$ , where  $bb^* = N_{\mathbf{B}/\mathbb{Q}}(b)$ . We call such triples *Abelian surfaces with quaternionic multiplication*, or QM abelian surfaces.

In [Sh1], Shimura showed that  $C_{\mathbf{B}}$ , which are a priori only algebraic curves over  $\mathbb{C}$ , have models over  $\mathbb{Q}$ , and, moreover, there is a canonical such model for each such  $C_{\mathbf{B}}$ , we denote it  $V_{\mathbf{B}}$ . For example, If  $\mathbf{B}$  has discriminant 6, then the canonical model  $V_{\mathbf{B}}$  has equation  $x^2 + y^2 + 3 = 0$ . Kurihara, Jordan, and Michon compiled equations of  $V_{\mathbf{B}}$  for many discriminants in [Ku], [Jo], and [Mic]. From now on, we will refer to  $V_{\mathbf{B}}$  as “the Shimura curve attached to  $\mathbf{B}$ ”, or “the Shimura curve of discriminant  $D$ ”, where  $D$  is the discriminant of the quaternion algebra  $\mathbf{B}$ . We also fix  $\phi : \mathcal{H} \rightarrow V_{\mathbf{B}}$ , the quotienting map that defines  $V_{\mathbf{B}}$ .

### 3. Atkin-Lehner involutions on $V_{\mathbf{B}}$

From the description of  $C_{\mathbf{B}}$  as a  $\Gamma \backslash \mathcal{H}$ , it is easy to see that it has certain *modular automorphisms*. Namely, via the inclusion

$$\mathbf{B} \hookrightarrow \mathbf{B} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{M}_2(\mathbb{R}),$$

$\mathbf{B}_+^*$  acts on  $\mathcal{H}$ , where  $\mathbf{B}_+^*$  is the set of non-zero elements of positive norm in  $\mathbf{B}$ . Following, for example [Mic], one can see that the action of  $\alpha \in \mathbf{B}_+^*$  on  $\mathcal{H}$  descends to an action on  $C_{\mathbf{B}}$  if and only if  $\alpha \in \text{Norm}_{\mathbf{B}_+^*}(\mathfrak{m}_+^*)$ . In fact, if  $2r$  is the number of prime divisors of  $D = \text{Disc}\mathbf{B}$ , then

$$\text{Norm}_{\mathbf{B}_+^*}(\mathfrak{m}_+^*)/\mathbb{Q}^*\mathfrak{m}_+^* \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}.$$

Hence, the group of modular involutions has order  $2^{2r}$ , and a set of representatives is generated by any set of elements  $\{\alpha_d\}_{d|D}, \alpha_d \in \mathfrak{m}$ ,  $N_{\mathbf{B}/\mathbb{Q}}(\alpha_d) = d$ .

Following standard notation, we shall call these involutions Atkin-Lehner involutions, and the group of these involutions, the Atkin-Lehner group. We denote it by  $W_{\mathbf{B}}$ , and we denote the involution defined by  $\alpha_d$  as  $w_d$ . Thus, we have the following

$$\text{Norm}_{\mathbf{B}_+^*}(\mathfrak{m}_+^*)/\mathbb{Q}^*\mathfrak{m}_+^* \hookrightarrow W_{\mathbf{B}} \subset \text{Aut}(C_{\mathbf{B}})$$

It is well known that  $w_d$  induces a  $\mathbb{Q}$ -rational involution on  $V_{\mathbf{B}}$ , we will denote it as  $w_d$ . Henceforth,  $W_{\mathbf{B}}$ , the Atkin-Lehner group, will be considered as a group of  $\mathbb{Q}$ -rational involutions on  $V_{\mathbf{B}}$ .

### 4. CM points and fixed points of modular involutions

CM points, or complex multiplication points play an important role in the study of the arithmetic of Shimura curves. Since Shimura curves

are compact, there are no obvious analogues of cusps on them, as one has in the case of modular curves. The closest canonical set of points one can define, therefore, are the CM points.

Let  $\phi : \mathcal{H} \rightarrow V_{\mathbf{B}}$  be the uniformization of  $V_{\mathbf{B}}$  by the upper half plane. Let  $z \in \mathcal{H}$ , then from the action of  $\mathbf{B}_+^*$  on  $\mathcal{H}$ ,  $\text{Stab}_{\mathbf{B}_+^*}(z) = \mathbb{Q}^*$ , or  $\text{Stab}_{\mathbf{B}_+^*}(z) = K^*$ , where  $K/\mathbb{Q}$  is an imaginary quadratic field. The former is the generic case, in the latter case we say that  $z$  has CM by  $K$ , and we extend the definition to  $\phi(z) \in V_{\mathbf{B}}$ . There is a 1-1 correspondence between points on  $\mathcal{H}$  with CM by  $K$  and quadratic fields in  $\mathbf{B}$  isomorphic to  $K$ .

One can also define CM by orders  $\mathcal{O}$  in  $K$ . We say that  $z \in \mathcal{H}$  has CM by  $\mathcal{O}$  if  $\text{Stab}_{\mathfrak{m}_+ - 0}(z) = \mathcal{O} - 0$ , and we say that  $x \in V_{\mathbf{B}}$  has CM by  $\mathcal{O}$  if  $\phi^{-1}(x) \in \mathcal{H}$ , for any choice of preimage, has CM by  $\mathcal{O}$ . The points in  $\mathcal{H}$  with CM by  $\mathcal{O}$  are in 1-1 correspondence with normalised  $\mathcal{O}$ -optimal embeddings of  $K$  into  $\mathbf{B}$ . We let  $\text{CM}(\mathcal{O})$  be the locus of points  $x \in V_{\mathbf{B}}$  with CM by  $\mathcal{O}$ . The following proposition characterises  $\text{CM}(\mathcal{O})$  (see [Jo]).

**Proposition 1.4.2.** *Let  $K$  be an imaginary quadratic field which splits  $\mathbf{B}$ , and set  $s$  equal to the number of primes  $p$  which divide  $\text{Disc}(\mathbf{B})$  and which do not ramify in  $K$ . Then, for any order  $\mathcal{O} \subset K$ , the cardinality of  $\text{CM}(\mathcal{O})$  is given by  $2^s \cdot h(\mathcal{O})$ , where  $h(\mathcal{O})$  denotes the class number of the order  $\mathcal{O}$ .*

The  $2^s$  factor comes in because of the  $W_{\mathbf{B}}$  action on the CM locus, for full details, see [Mic] or [Jo].

The fixed points of the modular involutions are easily characterised in terms of CM loci in the following proposition (see [Mic]).

**Proposition 1.4.3.** *If  $d \mid \text{Disc}(\mathbf{B})$ , then the set of fixed points of  $w_d$  acting on  $V_{\mathbf{B}}$  is  $CM(\mathbb{Z}[\sqrt{-d}]) \cup CM(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})})$ , if  $d \neq 2$ , and  $CM(\mathbb{Z}[\sqrt{-1}])$  if  $d = 2$ , where  $\mathcal{O}_K$  denotes the ring of integers in the number field  $K$ .*

In particular, we have the following corollary:

**Corollary 1.4.4.** *If  $d \mid \text{Disc}(\mathbf{B})$ , and  $\mathbb{Q}(\sqrt{-d})$  doesn't split  $\mathbf{B}$ , then  $w_d$  has no fixed points on  $V_{\mathbf{B}}$ .*

The following will be useful:

**Proposition 1.4.5.** *Let  $e(w_d)$  denote the number of fixed points of  $w_d$  on  $V_{\mathbf{B}}$ , where  $\text{Disc} \mathbf{B}$  is odd. Then  $\#(W_{\mathbf{B}}) \mid e(w_d)$ .*

**Proof.** Since  $D$  is odd, we have two possibilities:

I.  $d \equiv 1 \pmod{4}$ . Then  $-d \equiv 3 \pmod{4}$ , and hence  $\mathbb{Z}[\sqrt{-d}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ . Hence, by proposition 2.4.2 above,  $e(w_d) = 2^s \cdot h(\mathcal{O})$ . Now,  $s$  must be the number of primes divisors of  $D/d$ , and by the genus theory of quadratic imaginary fields,  $h(\mathcal{O})$  is divisible by  $2^r$ , where  $r$  is the number of prime factors of  $d$ . Thus  $2^s \cdot h(\mathcal{O})$  is divisible by  $2^{r+s} = \#(W_{\mathbf{B}})$ .

II.  $d \equiv 3 \pmod{4}$ . Then,  $\mathbb{Z}[\sqrt{-d}]$  is an order of conductor 2 in  $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ . From [Sh2], it is immediate that  $h(\mathbb{Z}[\sqrt{-d}])$  is an odd multiple of  $h(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})})$ . If  $r$  denotes the number of prime factors of  $d$ , then both are exactly divisible by  $2^{r-1}$ . Hence, clearly their sum is divisible by  $2^r$ . The argument is then the same as in I above.

Frequently, we will want to check if a given quadratic field  $K$  splits the quaternion algebra  $\mathbf{B}$ . A famous theorem of Hasse tell us how to do this. For a proof, see [Vig].

**Theorem 1.4.6** (Hasse's Criterion). *A quadratic field  $K$  splits a quaternion algebra  $\mathbf{B}$  if and only if every prime that ramifies in  $\mathbf{B}$  does not split in  $K$ .*

So for example, Look at  $\mathbf{B}(39)$ , the quaternion algebra of discriminant 39. It is indefinite, and is ramified at exactly 3 and 13. The quadratic field  $\mathbb{Q}(\sqrt{-3})$  doesn't split  $\mathbf{B}$  because 13 splits in  $\mathbb{Q}(\sqrt{-3})$ , and thus by the corollary and Hasse's criterion,  $w_3$  has no fixed points on  $V_{\mathbf{B}(39)}$ .

## CHAPTER 2

### Bad reduction of Atkin-Lehner quotients

We fix  $\mathbf{B}$ , an indefinite quaternion algebra over  $\mathbb{Q}$  of odd discriminant  $D$ ,  $V_{\mathbf{B}}$ , a subgroup  $G \subset W_{\mathbf{B}}$ , the quotient  $V^G := V_{\mathbf{B}}/G$ , and a prime  $p|D$ .

From Morita [Mo], it is well known that  $V_{\mathbf{B}}$  has good reduction at precisely those primes  $q$  where  $q$  does not divide  $D$ . The primes of bad reduction, therefore, are exactly the prime divisors of  $D$ . From Drinfeld etc., it follows that the involutions reduce modulo all primes of good reduction. Hence, the primes of bad reduction of  $V^G$  are precisely those of  $V_{\mathbf{B}}$ , i.e., the prime divisors of  $D$ . The analysis of rational points on  $V^G$  defined over completions of  $\mathbb{Q}$  at good places involves the Trace formula and the Eichler-Shimura relations on  $V^G$ . I hope to work on this in the near future, in this chapter I analyse points over completions of  $\mathbb{Q}$  at primes of bad reduction.

#### 1. The $p$ -adic upper half plane and admissible curves

In order to study the bad fibre of  $V^G$  at  $p$ , where  $p|D$ , we need to understand the Cerednik-Drinfel'd  $p$ -adic uniformization of  $V_{\mathbf{B}}$ . We recall that  $\mathcal{H}_p$ , the  $p$ -adic upper half plane has the following properties:

- 1)  $\mathcal{H}_p$  is a formal scheme, flat and locally of finite type over  $\mathbb{Z}_p$ .  $\mathcal{H}_p$  is regular and irreducible, and admits a natural action by  $\mathrm{PGL}_2(\mathbb{Q}_p)$ .
- 2) The special fibre  $\mathcal{H}_{p,0}$  of  $\mathcal{H}_p$  is reduced and geometrically connected.

All of its components are smooth rational curves defined over  $\mathbb{F}_p$ , which intersect transversally at  $\mathbb{F}_p$  rational points.

3) The dual graph of the special fibre, with the induced  $\mathrm{PGL}_2(\mathbb{Q}_p)$  action is canonically identified with the Bruhat-Tits building  $\Delta$  of  $\mathrm{SL}_2(\mathbb{Q}_p)$ , where the dual graph is defined by assigning a vertex to each component, and an edge to each intersection.

A curve  $C/\mathrm{Spec}R$ , for a DVR  $R$ , is called admissible if  $C$  is proper and flat, its generic fibre is a nonsingular curve, and its reduced fibre is a union of rational curves intersecting at reduced normal crossings. We refer the reader to [JL1] for details on admissible curves.

In [Ku], Kurihara shows the following:

**Proposition 2.1.7.** *Let  $\Gamma \subset \mathrm{PGL}_2(\mathbb{Q}_p)$  be discrete, cocompact. Then  $(\Gamma \backslash \mathcal{H}_p)/\mathbb{Z}_p$  is an admissible curve. Moreover, there is an isomorphism of pairs*

$$(\mathrm{Gr}(\Gamma \backslash \mathcal{H}_p)/\mathbb{Z}_p, \mathrm{Frob}(\Gamma \backslash \mathcal{H}_p)/\mathbb{Z}_p) \simeq ((\Gamma \backslash \Delta)^* , id).$$

where  $\mathrm{Gr}(\Gamma \backslash \mathcal{H}_p)$  denotes the dual graph of the special fibre of the quotient  $\Gamma \backslash \mathcal{H}_p$ , and  $\mathrm{Frob}_p$  denotes the action of Frobenius on the dual graph. The  $*$  suffix describes the contraction of edges  $y = \bar{y}$ , for detailed proofs and explanations, see [Ku] or [JL1]. It follows that each component on the special fibre has multiplicity 1.

The following theorem of Kurihara relates the genus of an admissible curve with the combinatorics of its dual graph:

**Theorem 2.1.8.**  $g(C) = 1 + \bar{\mathrm{Ed}}(\mathrm{Gr}(C)) - \mathrm{Ver}(\mathrm{Gr}(C))$

where we count the edges without orientation. For proofs, see [Ku]

## 2. The Cerednik-Drinfeld $p$ -adic uniformization

In [Dr], Drinfeld constructs a scheme  $M_{\mathbf{B}}$  which represents the coarse moduli problem for isomorphism classes of abelian surfaces with QM by  $\mathfrak{m}$  and satisfies the following properties:

- 1)  $M_{\mathbf{B}} \otimes \mathbb{Q} = V_{\mathbf{B}}$
- 2)  $M_{\mathbf{B}}$  is projective over  $\mathbb{Z}$
- 3)  $M_{\mathbf{B}} \otimes \mathbb{F}_p$  is the reduction of  $V_{\mathbf{B}}$  at  $p$  studied by Morita, if  $p \nmid D$ .

The Cerednik-Drinfeld theory constructs a uniformization of  $M_{\mathbf{B}} \otimes \mathbb{F}_p$ , where  $p \mid D$  by  $\mathcal{H}_p$ , the  $p$ -adic upper half plane. We will construct a model for the special fibre and its dual graph, and study the action of  $W_{\mathbf{B}}$  on it.

We need to fix some notation: Let  $\mathbf{B}^{p-int}$  be the *definite* quaternion algebra of discriminant  $-D/p$ , we refer to it as the the quaternion algebra obtained from  $\mathbf{B}$  by interchanging local invariants at  $p$  and  $\infty$ . Fix a maximal order  $\mathcal{M}$  in  $\mathbf{B}^{p-int}$ .

Define

$$\mathbb{Z}^{(p)} = \mathbb{Z}[1/p]; \mathcal{M}^{(p)} = \mathcal{M} \otimes \mathbb{Z}^{(p)}; \mathcal{M}_p = \mathcal{M} \otimes \mathbb{Z}_p$$

$$\tilde{\Gamma}_0 = \mathcal{M}^{(p)*}$$

$$\tilde{\Gamma}_+ = \{x \in \tilde{\Gamma}_0 \mid v_p(\det x) \text{ is even}\}, \text{ where } v_p(a) \text{ is the } p\text{-adic valuation of } a.$$

$$Z = \mathbb{Z}^{(p)*} \subset \mathcal{M}^{(p)*}$$

$$\Gamma_0 = \tilde{\Gamma}_0 / Z$$

$$\Gamma_+ = \tilde{\Gamma}_+ / Z$$

If we fix an identification of  $\mathfrak{m} \otimes \mathbb{Q}_p$  with  $M_2(\mathbb{Q}_p)$ , then  $\tilde{\Gamma}_0$  and  $\tilde{\Gamma}_+$  are discrete cocompact subgroups of  $GL_2(\mathbb{Q}_p)$ , and  $\Gamma_0$  and  $\Gamma_+$  are discrete

subgroups of  $\mathrm{PGL}_2(\mathbb{Q}_p)$ , hence we can consider them as groups acting on  $\mathcal{H}_p$ , and thus on  $\Delta$ .

From their definitions, it is clear that  $\tilde{\Gamma}_+$  is a normal subgroup of  $\tilde{\Gamma}_0$  of index 2. If  $W = \tilde{\Gamma}_0/\tilde{\Gamma}_+$ , then  $W = \{1, w_p\}$ , where  $w_p$  can be represented by an element  $\gamma_p \in \mathcal{M}$  of norm  $p$ .

Also, since  $W$  is also isomorphic to  $\Gamma_0/\Gamma_+$ , there is an action of  $W$  on each of  $\Gamma_+\backslash\mathcal{H}_p$ ,  $\tilde{\Gamma}_+\backslash\mathcal{H}_p$ , and the graph  $\Gamma_+\backslash\Delta$ . The Cerednik-Drinfeld construction shows that the action of  $w_p$  on each of these is the same as that of  $\mathrm{Frob}_p$ . In [JL1], Jordan and Livne give a proof of this, and show, using the Eichler-Shimura relations that the dual graph of  $M_{\mathbf{B}} \times \mathbb{Z}_p/\mathbb{Z}_p$  is the following:

$$\mathrm{Gr}(M_{\mathbf{B}} \times \mathbb{Z}_p/\mathbb{Z}_p, \mathrm{Frob}_p) \simeq ((\Gamma_+\backslash\Delta)^*, w_p)$$

and further, give an extension to the case of  $K/\mathbb{Q}_p$ , a finite extension.

$$\mathrm{Gr}(M_{\mathbf{B}} \times \mathcal{O}_K/\mathcal{O}_K, \mathrm{Frob}) \simeq (((\Gamma_+\backslash\Delta)^*)^e, w_p^f)$$

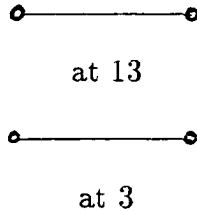
where  $e = e(K/\mathbb{Q}_p)$ ,  $f = f(K/\mathbb{Q}_p)$ .

In essence, this means the following: The Shimura curve  $V_{\mathbf{B}}$  considered as a curve over  $\mathcal{O}_K$  is admissible. Using proposition 3.1.7, one can analyse its dual graph. Cerednik and Drinfeld say that this dual graph is the same as the dual graph of the special fibre of  $M_{\mathbf{B}}$ , it has one vertex corresponding to each component of the special fibre, and one edge corresponding to each intersection. This graph is bipartite, i.e, the set of vertices can be partitioned into two sets, which we call the odd and even vertices, and no two vertices of the same parity are connected by an edge. The action of Frobenius on the vertices is the same as the action of  $w_p$  on the vertices and edges. This is a graph with lengths, i.e.

each edge has an associated integral length, defined as follows: Since the graph is a quotient of the  $\Delta$  by  $\Gamma$ , the edges are obtained by this action. The order of the stabilizer subgroup in  $\Gamma_+$  of any preimage in  $\Delta$  of an edge  $e$  on  $\text{Gr}(V)$  is its length. Furthermore, by base change to  $K$ , the dual graph of the special fibre over  $K$  is the same as that over  $\mathbb{Q}_p$ , but the lengths of the edges are multiplied by  $e$ .

The action of the group  $W_{\mathbf{B}}$  on the graph is as follows: the group  $W_{\mathbf{B}}$  has a subgroup  $H$ , which is generated by all involutions  $w_d$  where  $p \nmid d$ . The two cosets of  $H$  in  $W_{\mathbf{B}}$ , i.e.  $H$  and  $w_p H$  do the following:  $H$  preserves the parity of the vertices, and  $w_p H$  switches the parity of the vertices. In particular  $H$  cannot fix any edges, and  $w_p H$  cannot fix any vertices. Clearly the action of  $W_{\mathbf{B}}$  preserves the lengths of edges.

As an example, let us construct the dual graph of the curve  $V_{\mathbf{B}(39)}$ . Following Kurihara, we have



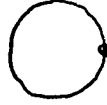
### 3. Bad reduction of $V^G$ and the dual graph.

Since, from the previous section, we know how  $W_{\mathbf{B}}$ , and hence  $G$  acts on the dual graph of  $V_{\mathbf{B}}$ , it is easy to figure out what the dual graph of the quotient  $V^G$  is. The set of vertices  $\text{Ver}(\text{Gr}(V^G))$  is the same as  $\text{Ver}(\text{Gr}(V))/G$ , and the edge set is also the correct quotient, the lengths multiply by a factor of at most  $(G)$ . So, for example, the graph of  $V_{\mathbf{B}(39)}/w_3$  looks like

.

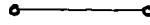


at 13



at 3

and the graph of  $V_{\mathbf{B}(39)}/w_{13}$  looks like



at 3



at 13

We can give a description of the special fibre and its dual graph of  $V^G$  similar to that of  $V_{\mathbf{B}}$  as follows:

For each  $w_d \in G$ , let  $\gamma_d$  be an element of the normaliser of  $\tilde{\Gamma}_+$  in  $\mathcal{M}^*$  of norm  $d$ . Set

$$\tilde{\Gamma}_{+,G} = \langle \tilde{\Gamma}_+, \{\gamma_d\}_d \rangle \in \text{PGL}_2(\mathbb{Q}_p),$$

$$\Gamma_{+,G} = \tilde{\Gamma}_{+,G}/\mathbb{Z}[1/p]^*$$

Since  $\gamma_d$  induces the action of  $w_d$  on  $M_{\mathbf{B}}$ , we see that  $V^G \times \mathbb{Q}_p$  is uniformised by the action of  $\Gamma_{+,G}$  on  $\Delta$ , with  $\text{Frob}_p$  acting as  $w_p$ . Thus, we have the following:

$$(\text{Gr}(M_{\mathbf{B}}/G \times \mathbb{Z}_p/\mathbb{Z}_p), \text{Frob}_p) \simeq ((\Gamma_{+,G} \backslash \Delta)^*, w_p)$$

and by base extension to  $K/\mathbb{Q}_p$ , we have

$$(\text{Gr}(M_{\mathbf{B}}/G \times \mathcal{O}_K/\mathcal{O}_K), F(M_{\mathbf{B}}/G \times \mathcal{O}_K/\mathcal{O}_K)) \simeq (((\Gamma_{+,G} \backslash \Delta)^*)^e, w_p^f)$$

**4. Rational points on  $V^G$  defined over  $K/\mathbb{Q}_p$** 

In order to study the existence of  $\mathbb{Q}_p$ -rational points, we will use Hensel's lemma. For completeness' sake, I include a version of the statement from [JL1].

**Theorem 2.4.9.** (*Hensel's Lemma*) *Let  $R$  be a complete DVR,  $K$  its fractions field,  $\mathfrak{m}$  its maximal ideal, and  $k$  its residue field. If  $f : X \rightarrow \text{Spec}R$  is a proper and flat morphism, where  $X$  is a regular scheme, then the generic fibre  $X \times_S \text{Spec}K$  has a  $K$ -rational point if and only if the special fibre  $X \times_S \text{Spec}k$  has a smooth  $k$ -rational point.*

In order to study  $V^G(K)$ , where  $K/\mathbb{Q}_p$  is a finite extension, we apply Hensel's Lemma to  $K$  and conclude that  $V^G(K) \neq \emptyset$  if and only if the special fibre of  $V^G \times \mathcal{O}_K$  has smooth  $k$  rational points. In the case  $f$  is even, we know that the special fibre of  $V \times \mathcal{O}_K$  has  $k$  rational points. and these reduce to the points we want for  $V^G$ . Thus we only need to analyse the case where  $f$  is odd.

The possibilities for a smooth  $k$ -rational point  $x_0$  are the following:

- 1)  $x_0$  is a smooth point on a component of the special fibre, i.e.,  $x_0$  is on a vertex in the dual graph, or
- 2)  $x_0$  lies on a component which comes from blowing up the special fibre at its singular points. i.e.,  $x_0$  is on an edge of the dual graph before it is blown up.

In case 1, if  $x_0$  is to be fixed by Frobenius, its component must be fixed by it. hence, we need to make sure that there is a component that is fixed by Frobenius, and that there is a smooth point on it. In particular, we need a vertex on the dual graph to be fixed by Frobenius,

or, by 3.1, by  $w_p^f$ , which, since  $f$  is odd, and  $w_p$  is an involution, is  $w_p$ . Moreover, we need to ascertain when this component has a smooth  $k$ -rational point on it. The following theorem decides this:

**Theorem 2.4.10.** *Suppose  $w_p \notin G$ . If  $v$  is a vertex on  $\text{Gr}(V^G)$  fixed by  $w_p$ , and  $C$  is the connected component corresponding to  $v$ , then there is a smooth point  $x_0 \in C(k)$ .*

**Proof.** Since  $v$  is fixed by  $w_p$ ,  $v$  is fixed by  $\text{Frob}_p$ , and hence the component corresponding to  $v$  is a  $P^1(\mathbb{F}_p)$ , which has  $p + 1$  points on it. Since the Frobenius action on this  $P^1$  is twisted by  $w_p$ , the  $\mathbb{F}_p$  rational crossing points are exactly those points on  $C$  that are fixed by  $w_p$ . Since  $w_p$  can have at most 2 fixed points, there must be rational points that are not crossing points, and hence  $C(K)$  has smooth points on it (see [JLV] for a more general result).

In case 2, if  $x_0$  comes from an edge on  $V^G$ , then  $\text{Frob}_p$  must either fix the edge or reverse it. We see the following:

**Lemma 2.4.11.** *There is a rational point  $x_0$  coming from an edge  $s$  of  $\Gamma_{+,G} \setminus \Delta$  if and only if  $w_p(s) = \bar{s}$ , and  $e \cdot \ell(s)$  is even, where  $\ell(s)$  is the length of the edge  $s$ .*

**Proof.** Working with  $K = \mathbb{Q}_p$ , we see that by blowing up the singularity corresponding to the edge  $s$ , we get a chain of edges of length 1, and thus we have added a string of  $\ell(s) - 1$  vertices (see [JL1] for blowing up singularities). Since the point  $x_0$  must lie on one of these vertices, we must fix one, i.e the middle one, which means that  $\ell(s) - 1$  must be odd, clearly base change to  $K$  proves the lemma. Details are

exactly similar to the proof of theorem 5.2 in [JL1].

Thus, if  $e$  is even, we need an edge  $s$  on  $\text{Gr}(V)$  which is switched by  $w_{pd}$  for  $w_d \in G$ . The following proposition shows when this can happen.

**Proposition 2.4.12.**  $\exists s$  an edge on  $\text{Gr}(V)$  so that  $w_r(s) = \bar{s}$ , where  $p|r, p \neq r$  if and only if  $\mathbb{Q}(\sqrt{-r})$  splits  $\mathbf{B}$ .

**Proof.** Let  $t$  be an edge on  $\Delta$  lying above  $s$ . Then, there exists an element  $\gamma_r \in \mathcal{M}^{(p)}$  so that  $N(\gamma_r) = r$ , and  $\gamma_r t = \bar{t}$ . Thus,  $\gamma_r^2$  fixes the initial and final vertex of  $t$ ,  $v_i$  and  $v_f$ . By the definition of the Bruhat-Tits building, each vertex  $v$  corresponds to a maximal order  $\mathfrak{m}_v$  in  $\text{PGL}_2(\mathbb{Q}_p)$ , and so  $\gamma_r^2 \in \mathbb{Q}^* \mathfrak{m}_{v_i}^*$ .

By conjugating  $\gamma_r$  appropriately, we can assume that  $\gamma_r^2 = ru$ , where  $u$  is a unit in  $\mathfrak{m}_{v_i}$ . Since  $u$  lies in a quadratic imaginary field,  $u$  is a root of unity of order 2, 3 or 4. If  $u$  is an order 3 or 4 root of unity, then  $r = 2$  or  $r = 3$ , both impossible. Thus,  $\mathbb{Q}(\gamma_r) = \mathbb{Q}(\sqrt{-r})$ . Thus,  $\gamma_r$  satisfies the equation  $X^2 + r = 0$  in  $\mathbf{B}^{p-int}$ , so  $\mathbb{Q}(\sqrt{-r})$  splits  $\mathbf{B}^{p-int}$ .

Conversely, suppose  $\mathbb{Q}(\sqrt{-r})$  splits  $\mathbf{B}^{p-int}$ . If  $\gamma_r$  satisfies  $X^2 + r = 0$ , then  $\gamma_r^2$  fixes some vertex  $v$ , and clearly also fixes  $\gamma_r v$ . Since  $p|r$ ,  $\text{dist}(v, \gamma_r v) = 1$ . Thus there is an edge  $e$  joining these two vertices that is switched by  $\gamma_r$ . This edge descends on  $\text{Gr}(V)$  to an edge switched by  $w_r$ .

We have a similar result for when a vertex is fixed:

**Proposition 2.4.13.**  $\exists v$  a vertex on  $\text{Gr}(V)$  so that  $w_r(v) = v$ , where  $p \nmid r$ , if and only if  $\mathbb{Q}(\sqrt{-r})$  splits  $\mathbf{B}^{p-int}$ .

**Proof.** Following the argument as above, we lift  $v$  to a vertex  $\mu$  on  $\Delta$ , and we again find an element  $\gamma_r \in \mathfrak{m}_\mu$  which fixes  $\mu$ . By the same argument,  $\mathbb{Q}(\sqrt{-r})$  splits  $\mathbf{B}^{p-int}$ .

We notice the following for  $V^G$ :

**Observation 2.4.14.** *Suppose  $K/\mathbb{Q}_p$  is a finite extension. Then*

*a) If  $f$  is even, then  $V^G(K) \neq \emptyset$ .*

*b) If  $e$  is even, then  $V^G(K) \neq \emptyset$  if and only if  $\exists w_d \in G$  and an edge  $e$  on  $\text{Gr}(V^G)$  so that  $w_{pd}(e) = \bar{e}$ .*

*If  $e$  and  $f$  are both odd, then  $V^G(K) \neq \emptyset$  if and only if*

*c) there is a vertex  $v$  on the dual graph  $\text{Gr}(V^G)$  of  $V^G$  which is fixed by  $w_p$ , i.e.  $w_p(v) = v$ , or*

*d) there is an edge  $s$  on  $\text{Gr}(V^G)$  with of even length which is switched by  $w_p$ , i.e.  $w_p(s) = \bar{s}$ .*

**Theorem 2.4.15.** *Suppose  $w_p \notin G$ , and  $K/\mathbb{Q}_p$  is a finite extension.*

*Then  $V^G(K) \neq \emptyset$  if and only if*

*(I)  $f$  is even, or*

*(II)  $e$  is even and  $\exists w_d \in G$  with  $p \nmid d$  and  $\mathbb{Q}(\sqrt{-pd})$  splits  $\mathbf{B}$ , or*

*(III)  $\exists w_d \in G, p|d$ , with  $\mathbb{Q}(\sqrt{-pd})$  splits  $\mathbf{B}^{p-int}$ , or*

*(IV)  $\mathbf{B}^{p-int} \simeq \mathbf{B}(-d_1p, -d_2)$ , where  $w_{d_1}, w_{d_2} \in G$*

**Proof.** I is done above. To prove II, we use b) in the observation along with proposition 3.4.12. Clearly, if  $w_{pd}$  fixes an edge  $e$  on  $\text{Gr}(V)$ , then  $w_p$  fixes the edge below  $e$  on  $\text{Gr}(V^G)$ .

III follows from proposition 3.4. and part c) of the observation. By

theorem 3.4.10, if we have a component fixed by  $w_p$ , then it has a smooth point on it.

All that remains, therefore, is the edge situation, i.e. (d) in the observation. Suppose we have an edge  $e$  on  $\text{Gr}(V^G)$  of even length that is fixed by  $w_p$ . Let  $s$  be an edge on  $\text{Gr}(V)$  above  $e$ . Then, there are two possibilities for  $s$ : either

- (i)  $s$  has even length or  $w_{d_1}(s) = s$  for  $w_{d_1} \in G$ ,
- (ii)  $w_p(s) = \bar{s}$  or  $w_p(s) = w_{d_2}(\bar{s})$  for  $w_{d_2} \in G$ .

Following the argument in [JL3], we see that the possibilities are the following:

- 1)  $s$  has even length and  $w_{pd_2}(s) = \bar{s}$
- 2)  $w_p(s) = \bar{s}, w_{d_1}(s) = s$
- 3)  $w_{pd_2}(s) = \bar{s}, w_{d_1}(s) = s$ .

In case 1) let  $\gamma_{pd_2} \in \mathcal{M}$  represent  $w_{pd_2}$ . We can assume that  $N(\gamma_{pd_2}) = pd_2$ . If  $\tilde{s}$  lies on  $\Delta$  above  $s$ , we can conjugate  $\gamma_{pd_2}$  to make sure that  $\gamma_{pd_2}(\tilde{s}) = \tilde{s}$ . Following the argument in [JL1], theorem 5.6, we get the condition  $\mathbf{B}^{p-int} \simeq \mathbf{B}(-1, -pd_2)$ . Reading the same argument backwards gives us an edge  $s$  of length 2 with  $w_{pd_2}(s) = \bar{s}$ .

In case 2), Let  $\gamma_p, \gamma_{d_1} \in \mathcal{M}$  of norms  $p$  and  $d_1$  respectively, that represent  $w_p$  and  $w_{d_1}$  so that  $\gamma_p(\tilde{s}) = \bar{\tilde{s}}$  and  $\gamma_{d_1}(\tilde{s}) = \tilde{s}$ . Then, following the analysis in [Ku], we see that  $\gamma_p^2, \gamma_{d_1}^2 \in \mathbb{Q}$ , and  $\gamma_{d_1}$  and  $\gamma_p \cdot \gamma_{d_1} \cdot \gamma_p^{-1}$  both fix  $\tilde{s}$  and hence,  $\mathbf{B}^{p-int} \simeq \mathbf{B}(-p, -d_1)$ . Conversely, if the two quaternion algebras are isomorphic, then we can pick  $\gamma_p$  and  $\gamma_{d_1}$  with the above properties, and we will get  $s$  as in 2).

In case 3), let  $\gamma_{d_1}$  and  $\gamma_{pd_2}$  be as in the previous paragraph, we get that

$\mathbf{B}^{p-int} \simeq \mathbf{B}(-pd_2, -d_1)$  by the same analysis.

Putting all of the above together, we get the statement in the theorem.

This completes the proof.

Specialising to the case where  $e = f = 1$ , we have:

**Theorem 2.4.16.** *If  $w_p \notin G$ , then  $V^G(\mathbb{Q}_p) \neq \emptyset$  if and only if*

*(a)  $\exists w_d \in G, p \nmid d$ , with  $\mathbb{Q}(\sqrt{-d})$  splits  $\mathbf{B}^{p-int}$ ; or*

*(b)  $\mathbf{B}^{p-int} \simeq \mathbf{B}(-d_1p, -d_2)$ , where  $w_{d_1}, w_{d_2} \in G$ .*

**Corollary 2.4.17.** *If  $G, K$  are as above, and  $L/K$  is odd. then*

*$V^G(L) = \emptyset$  if and only if  $V^G(K) = \emptyset$*

## CHAPTER 3

### Divisors and divisor classes over completions of $\mathbb{Q}$

Throughout this chapter, we let  $V^G$  be as before. We also fix the following notation:

For a smooth, projective, geometrically irreducible curve  $C = C/K$  over a field  $K$ , we let

$\text{Pic}(C)$  be the  $K$ -variety of divisor classes on  $C$ ,

$\text{Pic}^d(C)$  the  $K$ -variety of degree  $d$  divisor classes on  $C$

$\text{Pic}^d(C)(L)$  the set of degree  $d$  divisor classes on  $C$  defined over  $L$ , for  $L/K$  a field extension,

$\text{Pic}^d(C)(L)^+$  the subset of degree  $\text{Pic}^d(C)(L)$  represented by an  $L$ -rational divisor.

For simplicity, we split up the completions into the archimedean and non-archimedean cases.

#### 1. Points, divisors and divisor classes on $V^G$ over $\mathbb{R}$

The real locus of  $V^G$  is easy to characterise. Following Ogg ([Ogg]), we prove the following:

**Theorem 3.1.18.**  *$V^G(\mathbb{R}) \neq \emptyset$  if and only if  $\exists w_d \in G$  so that  $\mathbb{Q}(\sqrt{d})$  splits  $\mathbf{B}$ .*

**Proof** Suppose  $x_0 \in V^G(\mathbb{R})$  Let  $y_0 \in V_{\mathbf{B}}$  be a point on  $V_{\mathbf{B}}$  above it. Then, since  $V_{\mathbf{B}}(\mathbb{R}) = \emptyset$ , it is clear that  $\tau(y_0) = w_d(y_0)$ , where  $\tau$  denotes

complex conjugation, and  $w_d \in G$ . From [Ogg], it follows that  $\mathbb{Q}(\sqrt{d})$  splits  $\mathbf{B}$ .

The main aim of this chapter is to analyse the existence of divisors and divisor classes over various completions of  $\mathbb{Q}$ . The following result is known classically.

**Theorem 3.1.19.** *If  $C/K$  is a smooth, projective, geometrically irreducible curve over a field  $K$ , then*

(a)  $\text{Pic}^d(C)(\mathbb{R})^+ = \emptyset$  if and only if  $C(\mathbb{R}) = \emptyset$ , and  $d$  is odd.

(b)  $\text{Pic}^d(C)(\mathbb{R}) = \emptyset$  if and only if  $\text{Pic}^d(C)(\mathbb{R})^+ = \emptyset$  and the genus  $g(C)$  is odd.

For detailed proofs, see, for example, [GH].

So, for example, when  $C = V^G$ , we know that  $\text{Pic}^d(V^G)(\mathbb{R})^+ = \emptyset$  if and only if  $V^G(\mathbb{R}) = \emptyset$ , and we know then  $\text{Pic}^d(V^G)(\mathbb{R})$  is empty iff  $\text{Pic}^d(V^G)(\mathbb{R})^+$  is.

## 2. The non-archimidean case: divisors over local fields

Suppose  $K/\mathbb{Q}_p$  is a finite extension. with ring of integers  $\mathcal{O}_K$ , and residue field  $k$ . Fix  $\bar{K}/K$ , an algebraic closure with residue field  $\bar{k}/k$ , and  $L \subset \bar{K}$  a finite extension with residue field  $l$ . We are interested in  $\text{Pic}^d(V^G)(K)^+$ , i.e., we want to know when there are degree  $d$  divisors on  $V^G$  defined over  $K$ . The case when  $p$  is a prime of bad reduction, as remarked in [JL2], is surprisingly similar to the archimedean case, the interchange of local invariants at  $p$  and  $\infty$  relates the two.

In the case where  $p$  is a prime of good reduction, there is a more general result in [JL2].

**Proposition 3.2.20.** *If  $C/K$  is a smooth projective geometrically irreducible curve with good reduction, then  $\text{Pic}^d(C)(K)^+ \neq \emptyset$  for all  $d$ .*

**Proof.**(From [JL2]) Choose a regular model  $C/\mathcal{O}_K$ . If  $K_r$  denotes the unramified extension over  $K$  of degree  $r$ , and  $k_r$  its residue field, then there is some  $n \in \mathbb{Z}$  so that  $C(k_r) \neq \emptyset$  in  $r \geq n$ . Hence, by Hensel's lemma,  $C(K_r) \neq \emptyset$  for  $r \geq n$ . To get a divisor of degree 1, pick  $P \in C(K_{n+1}), Q \in C(K_n)$ , then

$$\mathcal{G} = \sum_{\tau \in \text{Gal}(K_{n+1}/K)} P^\sigma - \sum_{\tau \in \text{Gal}(K_n/K)} Q^\tau$$

is a divisor of degree 1 and is clearly defined over  $K$ . multiplying by  $d$  gives us a divisor of degree  $d$  defined over  $K$ .

So, in particular, if  $p \nmid D = \text{Disc}(\mathbf{B})$ ,  $V$ , and hence  $V^G$  have divisors of degree 1 and hence every degree over  $\mathbb{Q}_p$ .

In the case of bad reduction, we have the following.

**Proposition 3.2.21.** *If  $K/\mathbb{Q}_p$ , where  $p|D$ , and  $w_p \notin G$ , then  $\text{Pic}^d(V^G)(K)^+ = \emptyset$  if and only if  $d$  is odd and  $V^G(K) = \emptyset$*

**Proof.** Clearly  $V^G(K) \neq \emptyset$  would mean  $\text{Pic}^d(V^G)(K)^+ \neq \emptyset$ . Also, by theorem 3.4.15, if  $K_2$  is the unramified quadratic extension of  $K$ , then  $V^G(K_2) \neq \emptyset$ . Hence,

$$\mathcal{G} = \sum_{\sigma \in \text{Gal}(K_2/K)} P^\sigma$$

is a divisor of degree 2 defined over  $K$ , multiplying by  $d/2$  gives us a divisor of degree  $d$  when  $d$  is even.

Conversely, suppose we have a divisor  $\mathcal{G} \in \text{Pic}^d(V^G)(K)^+$  with  $d$  odd. Then  $\text{Supp}\mathcal{G}$ , the support of  $\mathcal{G}$  is  $\text{Gal}(\bar{K}/K)$  invariant, and has an odd number of points on it. This means that there is a point  $\alpha \in \text{Supp}\mathcal{G}$

so that the orbit  $\{\text{Gal}(\bar{K}/K).\alpha\}$  has odd cardinality. Hence,  $\alpha$  must be in  $V^G(L)$ , where  $[L : K]$  is odd. Now from the corollary [3.4.14],  $V^G(L) \neq \emptyset \implies V^G(K) \neq \emptyset$ .

This leaves the case where  $w_p \in G$ . The following proposition can be deduced from [JL3].

**Proposition 3.2.22.** *If  $w_p \in G$ , then  $\text{Pic}^1(V^G)(\mathbb{Q}_p)^+ \neq \emptyset$ .*

**Proof.** It suffices to show that if  $G = \{1, w_p\}$ , then the proposition is true. In the case of larger  $G$ ,  $V^G$  is clearly a quotient of  $V_{\mathbf{B}}/w_p$ .

When  $G = \{1, w_p\}$ , we see that  $V^G$  is clearly uniformised by  $\mathcal{H}_p$ , the  $p$ -adic upper half plane as in Chapter 3, and we get a model for  $V^G$  over  $\mathbb{Z}_p$  whose special fibre consists of  $\mathbb{F}_p$ -rational  $\mathbb{P}^1$ 's crossing at  $\mathbb{F}_p$ -rational points. In particular, we have smooth  $\mathbb{F}_{p^r}$  points for any  $r \geq 2$ . By Hensel's lemma, we have points over the Witt vectors  $W(\mathbb{F}_{p^r})$  for any  $r \geq 2$ . The trace to  $\mathbb{Q}_p$  of such a point gives us a divisor of degree  $r$  defined over  $\mathbb{Q}_p$ .

Let  $\mathcal{D}_1$  and  $\mathcal{D}_2$  be two such  $\mathbb{Q}_p$  rational divisors of degree 3 and 2, respectively. Then  $\mathcal{D}_1 - \mathcal{D}_2$  is a  $\mathbb{Q}_p$ -rational divisor of degree 1, and hence  $\text{Pic}^1(V^G)(\mathbb{Q}_p)^+ \neq \emptyset$ .

**Note :** Since there is no twist by  $w_p$  on the special fibre described above, the analysis in Chapter 3 doesn't work on this special fibre, as the action of  $w_p$  is trivial. Hence, studying the existence of rational points on  $V^G$  if  $w_p \in G$  is non-trivial, but divisors come for free.

### 3. Divisor classes over local fields

As in the case of divisors, the existence of divisor classes over a given field is similar to the archimidean case. In [JL2], Jordan and Livne give criteria analogous to those in theorem 4.1.19 for  $V$ , the following is an extension to  $V^G$ .

**Theorem 3.3.23.**  $\text{Pic}^d(V^G)(K) = \emptyset$  if and only if  $\text{Pic}^d(V^G)(K)^+ = \emptyset$  and the genus  $g(V^G)$  is odd.

The proof is similar to that for  $V_{\mathbf{B}}$ , we will use some propositions from [JL2], I will state them in the form that we need.

Suppose  $L/K$  is an extension, and let  $\Lambda(L) = \text{Pic}(V^G)(L)/\text{Pic}(V^G)(L)^+$ . Also, let  $g = g(V^G)$  be the genus. Then,

**Proposition 3.3.24.** *If  $L/K$  is a cyclic extension of local fields with  $V^G(L) \neq \emptyset$ , then  $\Lambda(K)$  is of order  $m$  with  $m|[L : K]$  and  $2g-2 \equiv 0 \pmod{m}$ . Also, if  $A \in \text{Pic}V^G(K)$  generates  $\Lambda(K)$ , then  $\deg A \equiv g - 1 \pmod{m}$ .*

In order to prove the theorem, we need only consider  $K/\mathbb{Q}_p$  where  $p|D$ , and  $\text{Pic}^1(V^G)(K) = \emptyset$ , so when  $V^G(K) = \emptyset$  and  $w_p \notin G$  suffices. We need to prove the following two assertions:

(\*)

$$g(V^G) \text{ odd and } \text{Pic}^1(V^G)(K)^+ = \emptyset \implies \text{Pic}^1(V^G)(K) = \emptyset.$$

(\*\*)

$$g(V^G) \text{ even} \implies \text{Pic}^1(V^G)(K) \neq \emptyset.$$

**Proof of \*.** We apply proposition 4.3.24 to  $L = K_2$ , the unramified quadratic extension of  $K$ . We know that  $V^G(K_2) \neq \emptyset$ , assume that

$\text{Pic}^1(V^G)(K) \neq \emptyset$ . Then, by the proposition,  $m|[K_2 : K]$ . we have two cases:

(i)  $m = 1$ . Then  $\text{Pic}(V^G)(K)^+ = \text{Pic}(V^G)(K)$ , and so, by assumption,  $\text{Pic}^1(V^G)(K)^+ \neq \emptyset$ . But  $V^G(K) = \emptyset$ , and we have a contradiction by proposition 4.2.21.

(ii)  $m = 2$ . Then, by proposition 4.3.24, there is a divisor  $A \in \text{Pic}(V^G)(K)$  that generates  $\Lambda(K)$  so that  $\deg A$  is even. Since, by assumption,  $\text{Pic}^1(V^G)(K) \neq \emptyset$ , there is a divisor  $B \in \text{Pic}(V^G)(K)^+$  so that  $A + B \in \text{Pic}^1(V^G)(K)$ . Since  $\text{Pic}^1(V^G)(K)^+ = \emptyset$ ,  $B$  must have even degree, and hence so must  $A + B$ , this is a contradiction.

The even genus case is considerably more difficult. Once again, we will require some results from [JL2]. Our aim is the following: we shall show that if the genus is even, then the class  $[\text{Pic}^1(V^G)]$  is trivial in the Weil-Chatelet group  $\text{WC}(\text{Pic}^0(V^G)/K, K_2)$ , and this will establish the non-emptiness of  $\text{Pic}^1(V^G)(K)$ .

We need the following notation: For an Abelian variety  $A/K$  with Neron model  $\mathcal{A}$ , denote by  $\Phi$  the group of connected components of the special fiber. This is a  $\text{Gal}(\bar{k}/k)$  module, and hence, for any subfield  $l \subset \bar{k}$ , we have  $\Phi_l = \Phi^{\text{Gal}(\bar{k}/l)}$ , this is a  $\text{Gal}(l/k)$  module. We define  $\text{WC}(A/K, L)$ , for an abelian variety  $A/K$ : it is the group of isomorphism classes of principal homogeneous spaces for  $A/K$  which become trivial over  $L$ . There is a natural identification of  $\text{WC}(A/K, L)$  with the kernel of

$$\text{Res} : H^1(\text{Gal}(\bar{K}/K), A(\bar{K})) \longrightarrow H^1(\text{Gal}(\bar{K}/L), A(\bar{K})),$$

and if  $L/K$  is Galois, then we have an isomorphism

$$\mathrm{WC}(A/K, L) \simeq H^1(\mathrm{Gal}(L/K), A(L)).$$

Further, from [Ma], there is a natural isomorphism

(I).

$$\alpha : \mathrm{WC}(A/K, L) \simeq H^1(\mathrm{Gal}(L/K), \Phi_l).$$

In our situation, i.e.  $A = \mathrm{Pic}^0(V^G)$ , we can use a result of Raynaud [Ray] to describe  $\Phi$  easily. Let  $\mathcal{L}$  denotes the free abelian group of the reduced components  $C_1, C_2, \dots, C_m$  of the special fibre of  $\mathcal{C} \times_{\bar{k}}$  for a regular model  $\mathcal{C}$  of  $V^G$  over  $\mathcal{O}$ . We know, from chapter 2, that each component  $C_i$  occurs with multiplicity 1 in the special fibre. Also, if we assume that  $V^G(K) = \emptyset$ , then clearly each of the components  $C_i$  are moved by  $\mathrm{Frob}_p$ . Hence,  $\mathcal{L}$  is a twist of  $\mathbb{Z}^{2n}$ , where  $2n = m$  is the number of components in the reduction, and there is an action of  $\mathrm{Gal}(k_2/k) = \{1, \mathrm{Frob}_p\}$  on it. Thus, we can identify  $\mathcal{L}$  with  $\mathrm{Ind}_1^{\mathrm{Gal}(k_2/k)}(\mathbb{Z}^n)$ . Define a linear map  $\mathcal{D} : \mathcal{L} \rightarrow \mathcal{L}$  by  $\mathcal{D}(C_i) = \sum_j (C_i, C_j) C_j$ , where  $C_j$  runs through all components, and  $(C_i, C_j)$  is the intersection number of the components  $C_i$  and  $C_j$  if  $i \neq j$ , and  $(C_i, C_i) = -\sum_{j \neq i} (C_i, C_j)$ .

We have the following facts:

$\mathcal{L}$  is a  $\mathrm{Gal}(\bar{k}/k)$  module,  $\mathcal{D}$  is Galois equivariant,  $\mathrm{deg} : \mathcal{L} \rightarrow \mathbb{Z}$  is Galois equivariant, where  $\mathrm{deg}(\sum n_i C_i) = \sum n_i$ . If  $\mathcal{L}_0 = \ker(\mathrm{deg})$ , then we have the following  $\mathrm{Gal}(\bar{k}/k)$ -equivariant exact sequences

(II).

$$0 \rightarrow \mathcal{L}_0 \rightarrow \mathcal{L} \rightarrow \mathbb{Z} \rightarrow 0$$

(III).

$$0 \rightarrow \mathcal{D}(\mathcal{L}) \hookrightarrow \mathcal{L}_0 \rightarrow \Phi \rightarrow 0$$

We have the following proposition

**Proposition 3.3.25.** *Suppose  $\text{Pic}^d(V^G)(L)^+ \neq \emptyset$  for  $L/K$  unramified. Then, the class of  $[\text{Pic}^d(V^G)] \in \text{WC}(\text{Pic}^0 V^G/K, L)$  is in the image of the composition*

$$H^1(\text{Gal}(l/k), \mathcal{L}_0^{\text{Gal}(\bar{k}/l)}) \xrightarrow{\beta_*} H^1(\text{Gal}(l/k), \Phi_l) \xrightarrow{\alpha^{-1}} \text{WC}(\text{Pic}^0(V^G)/K, L)$$

**Proof.** For the proof, see prop 3.4 in [JL2].

Suppose we let  $\Gamma = \text{Gal}(k_2/k)$ . Then, we see immediately that  $\mathcal{L}$  is a  $\Gamma$  module, and that  $\Phi$  is the same as  $\Phi_{k_2}$ . As in [JL2], we have the following:

**Lemma 3.3.26.**  $H^1(\Gamma, \mathcal{L}_0) \simeq \mathbb{Z}/2\mathbb{Z}$

**Proof.** Using the long exact sequence associated to the Galois cohomology for  $\Gamma$  for the exact sequence in equation I above, we get

$$\mathcal{L}^\Gamma \longrightarrow \mathbb{Z} \longrightarrow H^1(\Gamma, \mathcal{L}_0) \longrightarrow H^1(\Gamma, \mathcal{L})$$

By Shapiro's lemma, ([AW]), we see that  $H^1(\Gamma, \mathcal{L}) \simeq H^1(1, \mathbb{Z}^{2n}) = 0$ . Furthermore, since  $\mathcal{L}^\Gamma = \sum_i \alpha_i (C_i + C_i^{\text{Frob}_p})$ , we see that the image of  $\mathcal{L}^\Gamma$  in  $\mathbb{Z}$  is  $2\mathbb{Z}$ . Hence the lemma follows.

From the definition of the connecting homomorphism, we get the following:

**Lemma 3.3.27.** *Suppose  $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}$  so that*

*$\sum \alpha_i \equiv 1 \pmod{2}$ . If we let  $D = \sum \alpha_i C_i$ , then the cohomology class of the 1-cocycle defined by the map  $f : \Gamma \longrightarrow \mathcal{L}_0$ , where for  $\tau \in \Gamma$ ,  $f(\tau) = D^\tau - D$  generates  $H^1(\Gamma, \mathcal{L}_0)$ .*

we can now begin to construct the proof of (\*\*). We first need to notice that if we apply Galois cohomology to equation III, we get

$$H^1(\Gamma, \mathcal{D}(\mathcal{L})) \xrightarrow{\gamma_*} H^1(\Gamma, \mathcal{L}_0) \longrightarrow H^1(\Gamma, \Phi)$$

Furthermore, if we let  $L = K_2$  in proposition 4.3.25, then we have the following the class of  $[\text{Pic}^d V^G] \in \text{WC}(\text{Pic}^0 V^G / K, L)$  is in the image of the composition

$$\begin{aligned} & H^1(\text{Gal}(k_2/k), \mathcal{L}_0^{\text{Gal}(\bar{k}/k_2)}) \xrightarrow{\beta_*} \\ & H^1(\text{Gal}(k_2/k), \Phi_l) \xrightarrow{\alpha^{-1}} \text{WC}(\text{Pic}^0(V^G)/K, K_2) \end{aligned}$$

Suppose we can find a  $D$  as in lemma 4.3.27. Then, we see that  $\gamma_*$  must be surjective. But since  $V^G(K_2) \neq \emptyset$ , using the equation above, we get  $\alpha([\text{Pic}^1(V^G)]) = 0$ . Hence, we can conclude that  $[\text{Pic}^1(V^G)] = 0$ , since  $\alpha$  is an isomorphism, and hence  $\text{Pic}^1(V^G)(K) \neq \emptyset$ .

Hence, it is clear that all that remains is to show that we can find a  $D$  that satisfies the conditions in lemma 4.3.27. We show this in the following. Since  $V^G(K) = \emptyset$ , no vertex is fixed by  $w_p$ , and hence the set of components is partitioned into  $\{C_i\}_i$  and  $\{C_i^\tau\}_i$ , where  $\tau = \text{Frob}_p$ .

**Proposition 3.3.28.** *If  $\mathcal{G} = \sum_i C_i$ , where  $C_i$  varies as above, then  $\mathcal{D}(\mathcal{G})$  generates  $H^1(\Gamma, \mathcal{L}_0)$ .*

**Proof.** By definition,

$$\mathcal{D}(\mathcal{G}) = \sum_{i,j} (C_i, C_j) C_j + \sum_{i,j} (C_i, C_j^\tau)$$

The first thing we notice is that

$$(C_i, C_j) = (C_j, C_i) = (C_i^\tau, C_j^\tau)$$

If we let  $D = \sum_{i,j} (C_i, C_j) C_j$ , then  $\mathcal{D}(\mathcal{G}) = D - D^\tau$ . This is because the coefficient of  $C_i$  and the coefficient of  $C_i^\tau$  are negatives of each other. since

$$\sum_j (C_j, C_i) = - \sum_j (C_j^\tau, C_i).$$

Now, the  $\deg(D) = \sum_{i,j} (C_j, C_i)$ , which, since  $(C_i, C_j) = (C_j, C_i)$  has the same parity as  $\sum_i (C_i, C_i)$ . From the above, this is the same as  $\sum_i (C_i^\tau, C_i)$ . Now from Kurihara's theorem, 3.1.8, since the genus is even the total number of edges is odd, and hence, since all other edges must account for an even number, by  $w_p$  action, the total number of edges of the form  $[v_i, w_p(v_i)]$  must be odd, and hence  $\sum_i (C_i^\tau, C_i)$  is odd. So  $D$  satisfies the conditions of lemma 4.3.27, and this proves the proposition.

## CHAPTER 4

### Shimura curve quotients with odd jacobians

In [PSt], Poonen and Stoll showed that under the standard conjectures, the Shafarevich-Tate group  $\text{III}(A/K)$  is of the type  $G \times G$ , or  $G \times G \times \mathbb{Z}/2\mathbb{Z}$  for a finite group  $G$ . They also showed that in the case where  $A = \text{Pic}^0(C)$  for a curve  $C$  of genus  $g$ , the additional 2-torsion element in the second case comes from the principal homogeneous space  $\text{Pic}^{g-1}(C)$ . Following their convention, we say that  $A/K$  is odd if  $\text{III}(A/K) \simeq G \times G \times \mathbb{Z}/2\mathbb{Z}$ , and even otherwise.

#### 1. The Shafarevich-Tate group and the Cassels-Tate pairing

In this section, we will have the following notation:

$A/K$  will denote an abelian variety  $A$  defined over a global field  $K$ .

$\mathcal{S}$  will denote the set of places of  $K$ , both finite and infinite

For  $\pi \in \mathcal{S}$ ,  $K_\pi$  will denote the completion of  $K$  at  $\pi$

$\Gamma = \text{Gal}(\bar{K}/K)$

$\Gamma_\pi = \text{Gal}(\bar{K}_\pi/K)$ , the decomposition group at  $\pi$ .

The Hasse-Weil local global principle relates the existence of global points on  $A$ ,  $A(K)$  to that of the existence of local points on  $A$ , i.e.  $A(K_\pi)$ . The Shafarevich-Tate group  $\text{III}(A/K)$  measures the obstruction to the Hasse-Weil principle. A formal definition of  $\text{III}$  follows.

For each prime  $\pi \in \mathcal{S}$ , we have a map

$$\Theta_\pi : \text{H}^1(\Gamma, A(\bar{K})) \longrightarrow \text{H}^1(\Gamma_\pi, A(\bar{K}_\pi)).$$

Since the image of  $\Theta_\pi$  on any element is non-trivial for only a finite set of primes  $\pi$ , we have a map

$$\Theta : H^1(\Gamma, A(\bar{K})) \longrightarrow \bigoplus_\pi H^1(\Gamma_\pi, A(\bar{K}_\pi)).$$

The kernel of this map  $\Theta$  is defined to be the Shafarevich-Tate group  $\text{III}(A/K)$ .

Very little is known in general about  $\text{III}(A/K)$ . A standard conjecture says that it is finite, and we usually consider  $\text{III}(A/K)_{red}$ , the reduced Shafarevich-Tate group, which is just  $\text{III}(A/K)/D$ , where  $D$  is the maximal divisible subgroup of  $\text{III}(A/K)$ .

From [Ta], we know that there is a pairing

$$\text{III}(A/K) \times \text{III}(\hat{A}/K) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

We will define this pairing as done in [PSt]

Suppose  $a \in \text{III}(A/K)$ ,  $\hat{a} \in \text{III}(\hat{A}/K)$ . let  $X$  be the principal homogeneous space over  $K$  representing  $a$ . Then  $\text{Pic}^0(X(\bar{K}))$  is canonically isomorphic as a  $\Gamma = \text{Gal}(\bar{K}/K)$  module to  $\hat{A}(\bar{K})$ . Hence,  $\hat{a}$  can be considered as an element of  $H^1(\Gamma, \text{Pic}^0(X(\bar{K})))$ . Using the long exact sequence in Galois cohomology associated to

$$0 \longrightarrow \bar{K}(X)^*/\bar{K}^* \longrightarrow \text{Div}^0(X)(\bar{K}) \longrightarrow \text{Pic}^0(X)(\bar{K}) \longrightarrow 0.$$

we can map the element  $\hat{a}$  to an element  $b \in H^2(\Gamma, \bar{K}(X)^*/\bar{K}^*)$ . Again, using the long exact sequence associated to Galois cohomology of

$$0 \longrightarrow \bar{K}^* \longrightarrow \bar{K}(X)^* \longrightarrow \bar{K}(X)^*/\bar{K}^* \longrightarrow 0$$

we have

$$H^2(\Gamma, \bar{K}(X)^*) \longrightarrow H^2(\Gamma, \bar{K}(X)^*/\bar{K}^*) \longrightarrow H^3(\Gamma, \bar{K}^*)$$

2. THE POONEN-STOLL THEORY OF ODD AND EVEN ABELIAN VARIETIES

Now, the  $H^3$  term is 0, and hence the element  $b$  gives us an element  $f \in H^2(\Gamma, \bar{K}(X)^*)$ . Then, from [Mil], it follows that locally,  $f_\pi$  is the image of an element  $c_\pi \in H^2(\Gamma_\pi, \bar{K}_v^*)$ . We define

$$\langle a, \hat{a} \rangle = \sum_\pi \text{inv}(c_\pi) \in \mathbb{Q}/\mathbb{Z},$$

and for  $\lambda : A \rightarrow \hat{A}$  a polarization,  $\langle a, b \rangle_\lambda = \langle a, \lambda b \rangle$ , and thus we get a pairing on  $\text{III}(A/K) \times \text{III}(A/K)$ .

**2. The Poonen-Stoll theory of odd and even abelian varieties**

In section 6 of [PSt], Poonen and Stoll show that the pairing  $\langle \cdot, \cdot \rangle_\lambda$ , where  $\lambda : A \rightarrow \hat{A}$  is a polarization, is antisymmetric. Associated to a polarization  $\lambda$ , they construct a homogeneous space  $c$  which is of order 2 in  $\text{III}(A/K)$ . Furthermore, they show the following in corollary 7.

**Theorem 4.2.29.** *If  $\text{III}(A/K)_{\text{red}}$  is finite, then either*

1.  $\langle c, c \rangle = 0$ , and  $\text{III}(A/K)_{\text{red}} \simeq T \times T$ , where  $T$  is a finite abelian group, hence the order of  $\text{III}(A/K)_{\text{red}}$  is a square; or
2.  $\langle c, c \rangle = 1/2$ , and  $\text{III}(A/K)_{\text{red}} \simeq \mathbb{Z}/2\mathbb{Z} \times T \times T$ , where  $T$  is a finite abelian group, and hence the order of  $\text{III}(A/K)_{\text{red}}$  is twice a square.

In the first case, we say  $A/K$  is even, and in the second case, we say it is odd.

In the case where  $A$  is the jacobian of a curve  $X$  of genus  $g$ , they give the following criterion:

**Theorem 4.2.30.** *If  $A$  is the canonically polarized jacobian of a genus  $g$  curve  $X$  over a global field  $K$ , then the element  $c$  in  $\text{III}(A/K)[2]$  is*

$\text{Pic}^{g-1}X$ , and  $\langle c, c \rangle = N/2 \in \mathbb{Q}/\mathbb{Z}$ , where  $N$  is the number of places of  $\pi \in S$  where  $\text{Pic}^{g-1}X(K_\pi)^+ = \emptyset$ .

We call the  $\pi \in S$  deficient for the curve  $X$  iff  $\text{Pic}^{g-1}(X)(K_\pi)^+ = \emptyset$

### 3. Shimura curve quotients with odd jacobians

In [JL3], Jordan and Livne constructed the first known family of non-hyperelliptic curves with genus going to infinity, all of whose jacobians are odd. The family they construct is a family of quotients of Shimura curves. They used curves coming from quaternion algebras whose discriminant is the product of two primes  $pq$ . By setting up appropriate congruence conditions on  $p$  and  $q$ , they showed that  $V_{\mathbf{B}}(pq)/w_q$  has odd jacobian over  $\mathbb{Q}$ .

**Example 4.3.31.**  $V_{\mathbf{B}(85)}^G/w_{17}$  has odd jacobian.

In order to decide which quotients  $V^G/\mathbb{Q}$  of a Shimura curve  $V_{\mathbf{B}}$  can have odd jacobian, we will use the Poonen-Stoll criteria. Clearly, we need to count the number of places  $p|D$  at which  $\text{Pic}^{g-1}(V^G)(\mathbb{Q}_p)^+ = \emptyset$ . We know that  $\text{Pic}^2(V^G)(\mathbb{Q}_p)^+ \neq \emptyset$  for every place  $p$  (see proposition 4.2.21). Clearly we can have  $\text{Pic}^{g-1}(V^G)(\mathbb{Q}_p)^+ = \emptyset$  only if  $g-1$  is odd, and then we need to look for places  $p$  where  $\text{Pic}^1(V^G)(\mathbb{Q}_p)^+ = \emptyset$ . Now, by proposition 4.2.21, we know that  $\text{Pic}^1(V^G)(\mathbb{Q}_p)^+ = \emptyset$  if and only if  $V^G(\mathbb{Q}_p) = \emptyset$  when  $w_p \notin G$  and  $\text{Pic}^1(V^G)(\mathbb{Q}_p)^+ \neq \emptyset$  otherwise. Therefore, we have the following

**Observation 4.3.32.**  $V^G$  has odd jacobian if and only the genus  $g(V^G)$  is even and the number of places  $p$  so that  $\text{Pic}^1(V^G)(\mathbb{Q}_p)^+ = \emptyset$  is odd.

The first thing we need to do is figure out when the genus of  $V^G$  is even. The Eichler mass formula tells us the genus of  $V_{\mathbf{B}}$ :

$$(4.3.33) \quad g(V_{\mathbf{B}}) = 1 + \frac{1}{12} \prod_{p|Disc(\mathbf{B})} (p-1) - \frac{1}{4} \prod_{p|Disc(\mathbf{B})} \left(1 - \left(\frac{-4}{p}\right)\right) - \frac{1}{3} \prod_{p|Disc(\mathbf{B})} \left(1 - \left(\frac{-3}{p}\right)\right).$$

To get to the genus of  $V^G$ , we need to use the Riemann-Hurwitz theorem. Recall that if we have two curves  $X$  and  $Y$ , and  $Y$  covers  $X$  by a degree  $d$  map, then

$$(4.3.34) \quad g(Y) = dg(X) - d + 1 + \frac{1}{2} \sum_i e_i$$

, where  $e_i$  are the ramification degrees of the ramification loci. Hence,

$$(4.3.35) \quad g(X) = \frac{g(Y) + d - 1}{d} - \frac{\sum_i e_i}{2d}$$

**Lemma 4.3.36.**  $g(V^G)$  is even only if  $[W_{\mathbf{B}} : G] \leq 2$ .

**Proof.** Clearly the degree of the quotient map from  $V_{\mathbf{B}}$  to  $V^G$  is just the order of  $G$ . If  $Disc \mathbf{B}$  is divisible by  $N$  primes, then  $W_{\mathbf{B}} = 2^N$ , and so  $\#G = 2^n$ , where  $G$  is generated by  $n$  involutions. Hence, clearly,

$$(4.3.37) \quad g(V^G) = \frac{g(V_{\mathbf{B}}) + 2^n - 1}{2^n} - \frac{\sum_i e_i}{2^{n+1}}$$

Now, the ramification locus of the quotient map is easy to describe: it

is clearly the set of fixed points for the involutions  $w_d \in G$ , we have

(4.3.38)

$$g(V^G) = \frac{g(V_B) + 2^n - 1}{2^n} - \frac{1}{2^{n+1}} \sum_{1 \neq w_d \in G} e(w_d)$$

where  $e(w_d)$  denotes the number of fixed points of the involution  $w_d$  on  $V_B$ .

Now, in proposition 2.4.5, we studied exactly the number  $e(w_d)$ , and we saw that it is divisible by  $2^N$ . Therefore, if  $n \leq N - 2$ ,  $e(w_d)/2^{n+1}$  is even always. Hence, for  $n \leq N - 2$ ,  $V^G$  can be even only if  $(g(V_B) + 2^n - 1)/2^n$  is even, or  $(g(V_B) - 1)/(2^n)$  is odd.

The analysis proceeds as follows:

(4.3.39)

$$\frac{g(V_B) - 1}{2^n} = \frac{1}{12 \cdot 2^n} \left( \prod_{p|DiscB} (p - 1) - 3 \prod_{p|DiscB} \left(1 - \left(\frac{-4}{p}\right)\right) - 4 \prod_{p|DiscB} \left(1 - \left(\frac{-3}{p}\right)\right) \right)$$

(4.3.40)

$$= \frac{1}{3 \cdot 2^{n+2}} \left( \prod_{p|DiscB} (p - 1) - 3 \prod_{p|DiscB} \left(1 - \left(\frac{-4}{p}\right)\right) - 4 \prod_{p|DiscB} \left(1 - \left(\frac{-3}{p}\right)\right) \right)$$

Clearly all three product terms are divisible by  $2^N$ , and hence if  $n \leq N - 3$ , clearly  $(g(V_B) - 1)/(2^n)$  is even (an extra factor of 2 remains in the numerator), and hence  $g(V^G)$  is odd.

In the case  $n = N - 2$ , we look at 2 possibilities:

- 1) One of the primes  $p|DiscB$  is of the form  $4t + 1$ . Then, clearly  $(1 - (\frac{-4}{p})) = 0$ , and so all that remain are the first and third product terms, both divisible by  $2^{N+1}$ . Hence, again  $g(V^G)$  turns out to be odd.

2) If all the primes  $p|\text{Disc}\mathbf{B}$  are of the form  $4t + 3$ , then the first two product terms are exactly divisible by  $2^N$ , but not by  $2^{N+1}$ . Hence, their sum is divisible by  $2^{N+1}$ , the third product term is always divisible by  $2^{N+1}$  and again  $g(V^G)$  turns out to be odd. This proves the lemma.

Now that we know which subgroups can give even genus curves, we need to eliminate the ones which have points at every completion of  $\mathbb{Q}$ . The case of  $n = N$  is easily eliminated- Notice that when  $n = N$ ,  $G = W_{\mathbf{B}}$ . Hence,  $G$  contains  $w_p$  for all primes  $p|\text{Disc}\mathbf{B}$ . Thus,  $\text{Pic}^1(V^G)(\mathbb{Q}_p)^+ \neq \emptyset$ , by proposition 4.2.22. Now, to check if  $V^G(\mathbb{R}) \neq \emptyset$ , we use theorem 4.2.18, clearly if  $D = \text{Disc}\mathbf{B}$ ,  $w_D$  satisfies the conditions of the proposition. Thus  $\text{Pic}^1(V^G)(\mathbb{Q}_p)^+ \neq \emptyset$  for all primes  $p \leq \infty$ , hence  $V^G$  has even jacobian.

This reduces the set of possible quotients  $V^G$  to those with  $G \subset W_{\mathbf{B}}$  of index 2. The argument in the previous section generalizes easily, and we get the following theorem

**Theorem 4.3.41.** *The curve  $V^G/\mathbb{Q}$  of genus  $g$  has odd jacobian only if the index of  $G$  in  $W_{\mathbf{B}}$  is 2, and  $w_D \notin G$ , where  $D = \text{Disc}\mathbf{B}$ .*

**Proof.** The first part of the theorem follows from all of the above. what remains is to show that  $V^G$  cannot have odd jacobian if  $w_D \in G$ . Clearly if  $w_D \in G$ , then  $V^G(\mathbb{R}) \neq \emptyset$ , and hence  $\text{Pic}^1(V^G)(\mathbb{R})^+ \neq \emptyset$ , and  $\text{Pic}^{g-1}(V^G)(\mathbb{R})^+ \neq \emptyset$ . This takes care of the case  $p = \infty$ .

If  $p$  is a finite prime, then we just need to check in the cases where  $p|\text{Disc}\mathbf{B}$ . If  $w_D \in G$ , we know that  $V^G(\mathbb{Q}_p) \neq \emptyset \forall p \leq \infty$ . Thus  $\text{Pic}^{g-1}(V^G)(\mathbb{Q}_p)^+ \neq \emptyset \forall p \leq \infty$ . By the observation 5.3.32,  $V^G$  must have even jacobian. This completes the proof of the theorem.

The next chapter deals with generating examples of quotients with odd jacobians. I calculate a certain set of examples in the case where  $N = 4$ , and extend the set of families in [JL3] in the case  $N = 2$ . I also define an invariant  $\mathbf{N}(V^G)$  which takes in a  $V$  and  $G$  and produces an integer, which has the property that  $V^G$  has odd jacobian if and only if  $\mathbf{N}(V^G)$  is odd.

## CHAPTER 5

### Families of quotients with odd jacobians

I will outline the construction of two families of curves with odd jacobians. One of these families is constructed from Shimura curves whose discriminant is a product of two primes, and the second family is constructed from Shimura curves with discriminant a product of four primes.

#### 1. Families from $\mathbf{B}(pq)$

To construct families of odd quotients, I will use theorem 5.3.41. I will also frequently use Hasse's theorem to check if a particular quadratic field splits a given quaternion algebra. We will construct our families of curves by forcing congruence conditions on the primes dividing  $D$ .

Suppose we let  $D = p \cdot q$ , where  $p$  and  $q$  are odd primes. Furthermore, let

a)  $p \equiv 5 \pmod{8}$ ;

b)  $q \equiv 3 \pmod{4}$ ;

c)  $\left(\frac{p}{q}\right) = 1$

Since  $N = 2$ , the only possible index 2 subgroups in  $W_{\mathbf{B}}$  are  $(1, w_p)$ ,  $(1, w_q)$ ,  $(1, w_{pq})$ . Clearly, from theorem [5.3.45], the third subgroup is not "good", we let  $G = (1, w_q)$ . We let  $V = V_{\mathbf{B}}$ , where  $\mathbf{B}$  is ramified exactly at  $p$  and  $q$ , and consider  $V^G$ . From observation 5.3.32, we need

to count the number of places  $r$  in  $p, q, \infty$  so that  $\text{Pic}^1(V^G)(\mathbb{Q}_r)^+ = \emptyset$ .

(i)  $r = \infty$ . Since  $\left(\frac{q}{p}\right) = +1$ ,  $\mathbb{Q}(\sqrt{q})$  doesn't split  $\mathbf{B}$ . Hence, by theorem 4.1.18,  $V^G(\mathbb{R}) = \emptyset$ , and hence  $\text{Pic}^d(V^G)(\mathbb{R})^+ = \emptyset$

(ii)  $r = q$ . By lemma 4.2.20, clearly  $\text{Pic}^1(V^G)(\mathbb{Q}_q)^+ \neq \emptyset$ .

(iii)  $r = p$ . We use proposition 4.2.21, and see that we need to check if  $V^G(\mathbb{Q}_p) \neq \emptyset$ .

We observe that  $\mathbf{B}^{p-int} \simeq \mathbf{B}(-p, -q)$ , because  $\left(\frac{-p}{q}\right) = -1$ , and  $\left(\frac{-q}{p}\right) = +1$ . Now, by theorem 3.1.16,  $V^G(\mathbb{Q}_p) \neq \emptyset$ , and hence so is  $\text{Pic}^d(V^G)(\mathbb{Q}_p)^+$  for any  $d$ .

From the formula in 5.3.38, we have

(5.1.42)

$$g(V^G) = 1 + \frac{(p-1)(q-1) - 16}{24} + \frac{e(w_q)}{4}$$

If -3 is not a residue modulo either  $p$  or  $q$ , and

(5.1.43) 
$$g(V^G) = 1 + \frac{(p-1)(q-1)}{24} + \frac{e(w_q)}{4}$$

otherwise, where  $e(w_q)$  is the number of fixed points of  $w_p$  on  $V$ . Since  $\left(\frac{-q}{p}\right) = +1$ ,  $\mathbb{Q}(\sqrt{-q})$  doesn't split  $\mathbf{B}$ , and hence, by corollary 2.4.4,  $e(w_p) = 0$ . By the congruence conditions on  $p$  and  $q$ , clearly  $g(V^G)$  is even.

Now,  $V^G$  has even genus, and has divisors of degree  $g(V^G) - 1$  over all completions of  $\mathbb{Q}$  excepts for  $\mathbb{R}$ . Thus, by the Poonen-Stoll criterion,  $V^G$  has odd jacobian.

**Example** Let  $p = 5$ ,  $q = 11$ . then  $p$  and  $q$  satisfy the consitions listed

above, and hence  $V_{\mathbf{B}(55)}/w_{11}$  has odd jacobian. This curve has genus 2, and is clearly the smallest genus curve that we get using the above construction.

**Example** let  $p = 13$ ,  $q = 23$ , then  $p$  and  $q$  work as above, and we have  $V_{\mathbf{B}(299)}/w_{23}$ , which has genus 12, has odd jacobian.

**Example** Let  $p = 13$ ,  $q = 3$ , then  $V_{\mathbf{B}(39)}/w_3$  has genus 2 and odd jacobian.

From the formula for the genus of  $V^G$ , clearly we can produce curves of arbitrarily high genus with odd jacobians.

## 2. Families from $\mathbf{B}(pqrs)$ .

As in the previous section, We will force congruence conditions on the four primes, and this will give us the families with odd quotients. Let  $\mathbf{B}$  be ramified at four primes,  $p, q, r$  and  $s$ , and let

$$\text{a) } p \equiv r \equiv s \equiv 3 \pmod{4};$$

$$\text{b) } q \equiv 5 \pmod{8};$$

$$\text{c) } \left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = \left(\frac{p}{s}\right) = -1;$$

$$\text{d) } \left(\frac{-r}{q}\right) = \left(\frac{-s}{q}\right) = \left(\frac{r}{s}\right) = +1.$$

Let  $V = V_{\mathbf{B}}$ , and let  $G$  be the subgroup of  $W_{\mathbf{B}}$  generated by  $\langle w_p, w_q, w_r \rangle$ . Then  $G$  is clearly of index 2, and does not contain  $w_{pqrs}$ , hence  $V^G$  potentially has odd jacobian. We show that it does:

(i) Clearly  $\text{Pic}^1(V^G)(\mathbb{Q}_p)^+ \neq \emptyset$ ,  $\text{Pic}^1(V^G)(\mathbb{Q}_q)^+ \neq \emptyset$ ,  $\text{Pic}^1(V^G)(\mathbb{Q}_r)^+ \neq \emptyset$ , by proposition 4.2.22, and hence  $p, q, r$  cannot be deficient for  $V^G$ .

(ii)  $V^G(\mathbb{R}) \neq \emptyset$ , because  $\mathbb{Q}(\sqrt{p})$  splits  $\mathbf{B}$ , and hence  $\infty$  cannot be deficient for  $V^G$ .

(iii)  $V^G(\mathbb{Q}_s) = \emptyset$  This is easy to see, because the condition in theorem 3.4.16 fails for every try of  $d_1, d_2 \in G$ . So  $r$  is deficient for  $V^G$ .

Now for the genus of  $V^G$ : from the formula in 5.3.48, we have

$$(5.2.44) \quad g(V^G) = 1 + \frac{\prod_{n=p,q,r,s} (n-1) - 4 \prod_{n=p,q,r,s} (1 - (\frac{-3}{n}))}{96} - \frac{\sum_{w_d \in G} e(w_d)}{16}$$

Now, clearly, the numerator in the first fraction is divisible by 32 but not 64, and hence the fraction is odd. I claim that the second fraction is 0, and hence the total is even.

To show that  $e(w_d) = 0 \forall w_d \in G$ , we just check that  $\mathbb{Q}(\sqrt{-d})$  doesn't split  $\mathbf{B}$  for each eligible  $d$ . This is easy to do.

Hence  $g(V^G)$  is even, and it has exactly one deficient prime. So, by the Poonen-Stoll criteria, its jacobian is odd. Simple examples are

**Example.** Let  $p = 7, q = 5, r = 11, s = 79$ . Then,  $p, q, r, s$  satisfy the conditions above, and so  $V^G$ , which has genus 196, has odd jacobian.

**Example.** let  $p = 107, q = 5, r = 11, s = 19$ . Then, by the above,  $g(V^G) = 796$ , and the jacobian of  $V^G$  is odd.

### 3. The invariant $N(V^G)$

We define an invariant  $N(V^G)$  which has the following property:  $N(V^G)$  is odd if and only if  $V^G$  has odd jacobian. This invariant is easy to

calculate, and using this, we can calculate all Shimura curve quotients with odd Jacobians. In the next section, I give the code for a program which calculates all quotients of  $V$  which have odd Jacobian.

To define  $N(V^G)$ , we need to define the *deficiency terms*  $n_p$ , where  $p$  varies through primes of bad reduction and  $\infty$ .

Fix  $D = p_1 \cdot p_2 \cdot \dots \cdot p_{2n}$ , the discriminant of the given quaternion algebra, and let  $V$  be the corresponding Shimura curve. Let  $G$  be a subgroup of the Atkin-Lehner group.

We observe the following:

$\mathbb{Q}(\sqrt{-d})$  splits  $\mathbf{B}$  if and only if the quadratic residues

$$(5.3.45) \quad \left(\frac{d}{p}\right) \neq 1 \forall p|D$$

that is,

$$(5.3.46) \quad \prod_{p|D} \left(1 - \left(\frac{d}{p}\right)\right) \neq 0.$$

Thus, there exists  $w_d \in G$  so that  $\mathbb{Q}(\sqrt{-d})$  splits  $\mathbf{B}$  if and only if

$$(5.3.47) \quad \sum_{w_d \in G} \left(\prod_{p|D} \left(1 - \left(\frac{d}{p}\right)\right)\right) \neq 0$$

Thus, if we define

$$(5.3.48) \quad n_\infty = \sum_{w_d \in G} \left(\prod_{p|D} \left(1 - \left(\frac{d}{p}\right)\right)\right)$$

the  $n_\infty = 0$  if and only if  $V^G(\mathbb{R}) = \emptyset$ . Hence,  $n_\infty$  is a measure of the deficiency of  $V^G$  at  $\infty$ .

Similarly, for each prime of bad reduction  $p_i$ , we define

$$n_{p_i} = 1 \text{ if } w_{p_i} \in G$$

$$n_{p_i} = n_{p_i}^1 + n_{p_i}^2 \text{ if } w_{p_i} \notin G$$

where

$$(5.3.49) \quad n_p^1 = \sum_{w_d \in G, p|d} \left( \prod_{q|D/p} \left( 1 - \left( \frac{-pd}{q} \right) \right) \right)$$

and

$$(5.3.50) \quad n_p^2 = \sum_{w_{d_1}, w_{d_2} \in G, D|d_1 d_2 p, p \nmid d_2} \left( 1 + \left( \frac{-d_2}{p} \right) \right) \prod_{q|D/p} \left( 1 - \left( \frac{-pd_1}{q} \right) \right) \left( 1 - \left( \frac{-d_2}{q} \right) \right).$$

Then,  $n_p = 0$  if and only if  $n_p^1 = n_p^2 = 0$ , i.e., no component nor edge can give a  $\mathbb{F}_p$  rational point. Thus,  $n_p = 0$  if and only if  $\text{Pic}^1 V^G(\mathbb{Q}_p)^+ = \emptyset$  for  $p = p_i$  or  $\infty$ . To define the invariant  $\mathbf{N}(V^G)$ , we need to check how many  $n_p$ 's are 0, these are the deficient ones, and measure the parity. Clearly,  $2^{n_p}$  is odd if and only if  $n_p$  is 0, i.e.,  $\text{Pic}^1 V^G(\mathbb{Q}_p)^+ = \emptyset$ . Hence,  $\sum_p 2^{n_p}$  is odd if and only if the number of places where  $V^G$  is deficient is odd.

To meet the Poonen-Stoll criteria, we only need to make sure when  $g(V^G)$  is even, we can thus define

$\mathbf{N}(V^G) = (g(V^G) + 1)(\sum_p 2^{n_p})$  where  $p$  varies through  $p_i$  and  $\infty$ . Thus  $V^G$  has odd jacobian if and only if  $\mathbf{N}(V^G)$  is odd, by the Poonen-Stoll criteria.

## Appendix A - PARI code for calculating odd quotients

```
/*
Author: Florian Lengyel, Srinath Baba
Date: Sun, 07 Mar 1999 20:41:17 -0500 (EST)
Generate subgroups of index 2 in  $Z_2(+)$  ...  $(+)$   $Z_2$ 
Associate a prime with each summand...
/
/* Create empty set of index 2 subgroups of  $Z_2(+)$  ...  $(+)$   $Z_2$  that do
not contain the vector [1,1,1,1].
/
SetOfSubgroups = Set();
/*
Step 1: subgroup enumeration. Enumerate subgroups by enumerating
triples  $v_1, v_2, v_3$  of bit vectors modulo 2. Create the matrix  $m =$ 
 $(v_1, v_2, v_3, [1,1,1,1])$  and verify that  $\text{rank}(m) = 4$ . If so, compute the
group  $G$  generated over  $Z_2$  by  $v_1, v_2, v_3$ .  $G$  is represented in PARI as a
set of stringified bit vectors, which are sorted in ascending lexicographic
order by default. Once  $G$  is created,  $G$  itself is stringified and added
the union of the set of stringified subgroups of the direct sum. The set
union operation ensures that exactly one copy of  $G$  is enumerated in
the set of subgroups, even if  $G$  is generated by several  $Z_2$ -bases.
```

The reason for the data conversion is to take advantage of PARI's lexicographic ordering of sets of strings to represent groups, which obviates the need for sorting, and to use set union to eliminate duplicate groups.

```

/
  for ( i = 1,14,
for ( j = i+1, 14,
for (k = j+1, 14,
m = Mod(matid(4),2);
m[1, ] = Mod(vecextract(binary(16+i),"2..5"), 2);
m[2, ] = Mod(vecextract(binary(16+j),"2..5"), 2);
m[3, ] = Mod(vecextract(binary(16+k),"2..5"), 2);
m[4, ] = Mod(Vec([1,1,1,1]), 2);
if (matrank(m) == 4,
SubGroup = Set();
for (a = 1,7,
v = 0 * m[1, ];
for (b = 0, 2,
if (bittest(a, b) == 1,
v += m[b+1,];
);
);
SubGroup = setunion(SubGroup, Set(Str(v)));
);
SetOfSubgroups = setunion(SetOfSubgroups, Set(Str(SubGroup))); )
)

```

```

)
)
nGroups = length(SetOfSubgroups);
writel(out,"Number of subgroups: "); writel(out, nGroups);
print();
PrimeVector = [7,5,11,79];
writel(out,"List of primes: "); writel(out,Str(PrimeVector));
write(out, );
/* compute the preGenus (part that depends only on the given primes)

/
a = 1;
b = 1;
c = 1;
for (i = 1, 4,
a *= PrimeVector[i]-1;
b *= 1 - kronecker(-3,PrimeVector[i]);
c *= 1 - kronecker(-4,PrimeVector[i]);
)
preGenus = 1 + (a -3*c -4*b)/96;
/*
Step 2: genus sum computation.

```

This is where we need to unquote (more precisely, evaluate) a subgroup encoded as a stringified vector of stringified mod 2 bitvectors. Two levels of unquoting are required, the

first to recover the subgroup as a list of quoted bit vectors,  
the second to recover an individual bitvector.

```

FL
/
dVector=vector(7,i,0);
for (i = 1,nGroups,
n0 = 1;
nInvariant=vector(4,1,1);
GenusSum = 0;
e = vector(7,i,0);
eGenus = 0;
for (j = 1,7,
BitVector = eval(eval(SetOfSubgroups[i])[j]));
d = 1;
for (k = 1, 4,
if ( BitVector[k] == 1,
d *= PrimeVector[k];
);
);
kronprod= 1;
for (k = 1, 4,
kronprod *= 1-kronecker(-d,PrimeVector[k])
);
if (kronprod==0,
e[j] = 0;,
h = kronprod*qfbclassno(quaddisc(-d));

```

```

if (d
e[j] = h;
);
print1("e[");
print1(d);
print1( "]=");
print( e[j]);
eGenus += e[j];
kron= 1;
for (k = 1, 4,
kron *= 1-kronecker(d,PrimeVector[k])

);
if (kron != 0, n0=0);
for (k = 1, 4,
if (PrimeVector[k] == d, nInvariant[k]=0)
);
for (k = 1, 4,
if (nInvariant[k] == 1,
if (d
kron = 1;
for (kk = 1, 4,
if (kk != k,
kron *= 1- kronecker(-PrimeVector[k]*d,PrimeVector[kk]) ;
);
);
);

```



```

);
);
if (allneg1 == 1,
nInvariant[k] = 0;
);
);
);
);
);
);
);
);
);
);
genus = preGenus - eGenus/16;
writel(out,"genus for group "); writel(out, i); writel(out, " = "):
write(out, genus);
writel(out, "n[0] = "); write(out, n0);
parity = n0;
for (k = 1, 4,
writel(out, "n["); writel(out, k); writel(out, "] = ");
write(out, nInvariant[k]);
parity += nInvariant[k];
);
writel(out,"parity = "); write(out, parity
write(out," ");
)

```

## Appendix B - Some results from the program

Our conventions are:

If List of primes:  $[p, q, r, s]$ , then

group 1 =  $\langle q, r, s \rangle$ ;

group 2 =  $\langle p, r, s \rangle$ ;

group 3 =  $\langle p, q, s \rangle$ ;

group 4 =  $\langle pq, pr, s \rangle$ ;

group 5 =  $\langle p, q, r \rangle$ ;

group 6 =  $\langle pq, ps, r \rangle$ ;

group 7 =  $\langle q, pr, ps \rangle$ ;

group 8 =  $\langle p, qr, qs \rangle$  .

$n[0]$  (resp.  $n[1]$ ,  $n[2]$ ,  $n[3]$ ,  $n[4]$ ) = 1 if and only if  $\infty$  (resp.  $p, q, r, s$ ) is deficient.

List of primes: [191, 61, 347, 59]

genus for group 1 = 2383053

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 2 = 2383029

$n[0] = 0$   $n[1] = 0$   $n[2] = 1$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 3 = 2383070

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 4 = 2383046

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 5 = 2383052, ODD CURVE!!

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 1$

parity = 1

genus for group 6 = 2383076

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 7 = 2383035

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 1$

parity = 1

genus for group 8 = 2383059

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

List of primes: [137, 113, 29, 149]

genus for group 1 = 657459

$n[0] = 0$   $n[1] = 1$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 2 = 657496

$n[0] = 0$   $n[1] = 0$   $n[2] = 1$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 3 = 657496

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 1$   $n[4] = 0$

parity = 1

genus for group 4 = 657459

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 5 = 657418 ODD CURVE!!!

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 1$

parity = 1

genus for group 6 = 657351

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 7 = 657351

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 8 = 657418

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

---

List of primes: [277, 281, 97, 73]

genus for group 1 = 5564093

$n[0] = 0$   $n[1] = 1$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 2 = 5564109

$n[0] = 0$   $n[1] = 0$   $n[2] = 1$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 3 = 5564112 ODD CURVE!!!

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 1$   $n[4] = 0$

parity = 1

genus for group 4 = 5564090

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 5 = 5564090 ODD CURVE!!!

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 1$

parity = 1

genus for group 6 = 5564112

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 7 = 5564109

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 8 = 5564093

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

---

List of primes: [179, 181, 307, 277]

genus for group 1 = 28187039

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 2 = 28187044

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 3 = 28186495

$n[0] = 1$   $n[1] = 0$   $n[2] = 0$   $n[3] = 1$   $n[4] = 0$

parity = 0

genus for group 4 = 28186452

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 5 = 28187092

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 6 = 28187155

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 7 = 28186404

$$n[0] = 0 \ n[1] = 0 \ n[2] = 0 \ n[3] = 0 \ n[4] = 0$$

$$\text{parity} = 0$$

$$\text{genus for group 8} = 28186379$$

$$n[0] = 1 \ n[1] = 0 \ n[2] = 0 \ n[3] = 1 \ n[4] = 0$$

$$\text{parity} = 0$$

List of primes: [5, 19, 11, 107]

$$\text{genus for group 1} = 773$$

$$n[0] = 0 \ n[1] = 0 \ n[2] = 0 \ n[3] = 0 \ n[4] = 0$$

$$\text{parity} = 0$$

$$\text{genus for group 2} = 796 \text{ ODD CURVE!!!}$$

$$n[0] = 0 \ n[1] = 0 \ n[2] = 1 \ n[3] = 0 \ n[4] = 0$$

$$\text{parity} = 1$$

$$\text{genus for group 3} = 783$$

$$n[0] = 0 \ n[1] = 0 \ n[2] = 0 \ n[3] = 1 \ n[4] = 0$$

$$\text{parity} = 1$$

$$\text{genus for group 4} = 774$$

$$n[0] = 0 \ n[1] = 0 \ n[2] = 0 \ n[3] = 0 \ n[4] = 0$$

$$\text{parity} = 0$$

$$\text{genus for group 5} = 796$$

$$n[0] = 0 \ n[1] = 0 \ n[2] = 0 \ n[3] = 0 \ n[4] = 0$$

$$\text{parity} = 0$$

genus for group 6 = 773

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 7 = 774

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 8 = 783

$n[0] = 0$   $n[1] = 0$   $n[2] = 1$   $n[3] = 1$   $n[4] = 0$  parity = 0

---

List of primes: [5, 19, 23, 31]

genus for group 1 = 478 ODD CURVE!!!

$n[0] = 0$   $n[1] = 1$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 2 = 496

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 3 = 484

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 4 = 466 ODD CURVE!!!

$n[0] = 0$   $n[1] = 1$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 5 = 492

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 6 = 474 ODD CURVE!!!

$n[0] = 0$   $n[1] = 1$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 7 = 470 ODD CURVE!!!

$n[0] = 0$   $n[1] = 1$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 8 = 488

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

---

List of primes: [3, 7, 11, 13]

genus for group 1 = 14

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 2 = 14

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 3 = 13

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 4 = 13

$$n[0] = 0 \quad n[1] = 0 \quad n[2] = 0 \quad n[3] = 0 \quad n[4] = 0$$

$$\text{parity} = 0$$

genus for group 5 = 16

$$n[0] = 0 \quad n[1] = 0 \quad n[2] = 0 \quad n[3] = 0 \quad n[4] = 0$$

$$\text{parity} = 0$$

genus for group 6 = 12 ODD CURVE!!!

$$n[0] = 0 \quad n[1] = 0 \quad n[2] = 0 \quad n[3] = 0 \quad n[4] = 1$$

$$\text{parity} = 1$$

genus for group 7 = 15

$$n[0] = 0 \quad n[1] = 0 \quad n[2] = 0 \quad n[3] = 0 \quad n[4] = 0$$

$$\text{parity} = 0$$

genus for group 8 = 11

$$n[0] = 0 \quad n[1] = 0 \quad n[2] = 0 \quad n[3] = 0 \quad n[4] = 1$$

$$\text{parity} = 1$$

---

List of primes: [7, 5, 11, 79]

genus for group 1 = 196

$$n[0] = 0 \quad n[1] = 0 \quad n[2] = 0 \quad n[3] = 0 \quad n[4] = 0$$

$$\text{parity} = 0$$

genus for group 2 = 182

$$n[0] = 0 \quad n[1] = 0 \quad n[2] = 0 \quad n[3] = 0 \quad n[4] = 0$$

$$\text{parity} = 0$$

genus for group 3 = 187

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 1$   $n[4] = 0$

parity = 1

genus for group 4 = 177

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 5 = 196 ODD CURVE!!!

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 1$

parity = 1

genus for group 6 = 182

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

genus for group 7 = 187

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 1$   $n[4] = 1$

parity = 0

genus for group 8 = 177

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

---

List of primes: [1109, 757, 449, 953]

genus for group 1 = 3721389569

$n[0] = 0$   $n[1] = 1$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 2 = 3721388069

$n[0] = 0$   $n[1] = 0$   $n[2] = 1$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 3 = 3721386897

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 1$   $n[4] = 0$

parity = 1

genus for group 4 = 3721383241

$n[0] = 0$   $n[1] = 1$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 5 = 3721389527

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 1$

parity = 1

genus for group 6 = 3721385715

$n[0] = 0$   $n[1] = 1$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 7 = 3721384717

$n[0] = 0$   $n[1] = 1$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 1

genus for group 8 = 3721383769

$n[0] = 0$   $n[1] = 0$   $n[2] = 0$   $n[3] = 0$   $n[4] = 0$

parity = 0

## Bibliography

- [AW] M. Atiyah and C. Wall, *Cohomology of Groups*, Algebraic Number Theory, London, 1967.
- [Dr] V. G. Drinfeld, *coverings of  $p$ -adic symmetric regions*, Functional Anal. i Pril. **10** 1976, 107 - 115.
- [GH] B. Gross, J. Harris *Real Algebraic Curves*. Ann. Scient. Ec. Norm. Sup. (4) **14**, 1981, 157 - 182.
- [Jo] B. W. Jordan, *Diophantine properties of Shimura curves*, Ph.D. Thesis, Harvard, 1982.
- [JL1] B. W. Jordan and R. Livne, *Local diophantine propoerties of Shimura curves*, Math. Ann. **270**, 1985, 235 - 248.
- [JL2] B. W. Jordan and R. Livne, *Divisor classes on Shimura curves rational over local fields*, J. Reine. Angew. Math. **378**, 1987, 46 - 52.
- [JL3] B. W. Jordan and R. Livne, *On Atkin-Lehner quotients of Shimura curves*, Preprint, 1998.
- [JLV] B. W. Jordan, R. Livne and Y. Varshavsky, *Local points on  $p$ -adically uniformised Shimura varities*, Preprint, 1999.
- [Ku] A. Kurihara, *On some examples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Univ. Tokyo, Sec 1A **25**, 1979, 277 - 301.

- [Ma] B. Mazur, *Rational points of abelian varieties with values in towers on number fields*, *Inventiones Math.* **18**, 1972, 183 - 266.
- [Mic] J-F. Michon, *Corbes de Shimura Hyperelliptique*, *Bull. Soc. Math. France*, **109**, 1981, 217 - 225.
- [Mil] J. S. Milne, *Arithmetic Duality Theorems*, Academic Press, 1985.
- [Mo] Y. Morita, *Ihara's conjectures and moduli spaces of abelian varieties*, Master's Thesis, Tokyo, 1970.
- [Ogg] A. Ogg, *Real points on Shimura curves*, in *Aritmetic and Geometry*, Volume I, Birkhauser, 1983.
- [PSt] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Preprint, 1997.
- [Ray] M. Raynaud, *Specialization du foncteur de Picard*, *Publ. Math. IHES*, 1970, 27 - 76.
- [Sh1] G. Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain*, *Math. Ann.* **215**, 1975, 135 - 164.
- [Sh2] G. Shimura, *Intro. to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.
- [Ta] J. Tate, *WC groups over p-adic fields*, *Sem. Bourbaki*, 10e annee, 1957-58.
- [Vig] M.-F. Vigneras, *Arithemetique des algebres de quaternions*, *Lecture Notes in Mathematics* **800**, Springer, 1980.