THE BRAUER-MANIN OBSTRUCTION ON FAMILIES OF HYPERELLIPTIC CURVES

BY THOM TYRRELL

A dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Mathematics

Written under the direction of

Jerrold Tunnell

and approved by

_____

_____

_____

_____

New Brunswick, New Jersey

January, 2015

ABSTRACT OF THE DISSERTATION

The Brauer-Manin Obstruction on Families of Hyperelliptic Curves

by Thom Tyrrell

Dissertation Director: Jerrold Tunnell

In [19], Manin introduced a way to explain the failure of the Hasse principle for algebraic varieties over a number field. For curves, the problem of whether all such failures can be explained by this method is open. In this thesis, we construct unramified quaternion algebras that obstruct the existence of rational points on families of curves admitting maps to elliptic curves.

In Chapter 1, we introduce the Brauer group of a projective variety. For curves, we relate the Brauer group to torsors over the Jacobian of the curve, and establish some properties of the Brauer group over local fields that will simplify later computations.

In Chapter 2, we define the Brauer-Manin obstruction and show that it explains all failures of the Hasse principle for genus 1 curves and curves without a degree 1 rational divisor. After reviewing a topological and more computational characterization of the obstruction, we note that it suffices to consider curves that admit maps to positive rank abelian varieties. Having established the obstruction, we introduce the motivating example for this thesis - a construction by D.Quan [21] of a genus 11 hyperelliptic curve and an unramified quaternion algebra that obstructs the existence of rational points on it.

The next two chapters may be roughly described as the "global" and "local" components of this thesis. In Chapter 3, we review the geometry of split Jacobians and ruled surfaces. We then use recent work of Doerksen and Bruin [2] on the characterization of (4,4)-split Jacobians to analyze the ramification of the algebra introduced by Quan.

In Chapter 4, we apply the results of the previous chapter to construct quaternion algebras on a family of hyperelliptic curves of genus 5. With the local results of Chapter 1, we give a new analysis of Quan's example, and show these quaternion algebras obstruct the existence of rational points in the family.

In Chapter 5, we briefly describe a conjecture of Poonen concerning the topological characterization of the Brauer-Manin obstruction given in the second chapter. With code executed in `sage`, we provide additional computational evidence for the conjecture that all failures of the Hasse principle for curves are explained by the obstruction.

Acknowledgements

I thank my advisor Jerrold Tunnell for sticking with me through this long process, and also for the many semesters of number theory seminars he organized.

I would like to thank Charles Weibel, Lev Borisov, and Bianca Viray for serving on my committee and aiding me in the preparation of this dissertation.

I am grateful to Stephen Miller, whose lectures on Fourier analysis over number fields led me to study number theory.

I am grateful to Henryk Iwaniec for his support during my third year.

This work was partially supported by the GAANN fellowship.

Dedication

To Nasya: Thank you for all of your inspiration and love. I could not have done this without you.

To my family: Thank you for your endless love and support.

Table of Contents

Abstract ii

Acknowledgements iv

Dedication v

1. The Brauer Group and Cyclic Algebras on Hyperelliptic Curves . . 1

1.1. The Brauer Group of a Field 1

1.2. The Brauer Group of a Scheme 4

1.3. Curves and Arithmetic 7

2. The Brauer-Manin Obstruction for Curves 11

2.1. The Brauer-Manin Obstruction Sets 12

2.2. Computing the Obstruction Set mod l 15

3. Hyperelliptic Curves with Split Jacobian 19

3.1. Decomposable Jacobians 20

3.2. (4,4)-splittings 22

4. Obstructions on Curves with Split Jacobian 27

4.1. Global Construction 27

4.2. The curve $dy^2 = x^3 - 1$ 31

5. Computations with `Sage` 39

5.1. Algorithms 40

5.2. Examples 41

Appendix A. Code 43

References 46

Chapter 1

The Brauer Group and Cyclic Algebras on Hyperelliptic Curves

1.1 The Brauer Group of a Field

The material in this section is classical. For a reference, see [10] and [26]. Let K be a perfect field of characteristic not 2 with algebraic closure $\overline{K}$, absolute Galois group $G_K = Gal(\overline{K}/K)$ and let A be a finite-dimensional K-algebra. A is *central* if its center is exactly the field K, and *simple* if it has no non-trivial two-sided ideals. The canonical example is $A = \mathrm{M}_n(K)$ - the ring of $n \times n$ matrices with coefficients in K. If L/K is a field extension, and A is a central simple algebra, then $A \otimes_K L$ is again central simple over L. The tensor product of two central simple algebras is again central simple. As the dimension of A over K is always a square, we may define the *degree* of A as $\sqrt{\dim_K A}$. There exists a finite extension K'/K for which $A \otimes_K K' \cong \mathrm{M}_d(K')$, for d equal to the degree of A.

Two central simple algebras A, B are said to be *equivalent* if there are matrix algebras $\mathrm{M}_r(K), \mathrm{M}_s(K)$ for which $A \otimes \mathrm{M}_r(K) \cong B \otimes \mathrm{M}_s(K)$. To A we associate the opposite algebra A^{op} with the same elements and addition but with multiplication done in the opposite order. As $A \otimes A^{\mathrm{op}}$ is a matrix algebra, the set of central, simple algebras up to equivalence, $\mathrm{Br}(K)$, becomes a group under the operation of tensor product. By the Wedderburn-Artin Theorem, every central simple algebra over K is isomorphic to a matrix algebra over a division ring; hence every equivalence class in the Brauer Group may be represented by a division algebra.

By the Skolem-Noether Theorem every automorphism of a central simple algebra is inner - i.e. given by conjugation. In particular, $\mathrm{Aut}(\mathrm{M}_n) = \mathrm{PGL}_n$, so we may identify central simple algebras of degree n with the classes of the cohomology set

$H^1(G_K, \mathrm{PGL}_n)$. From the exact sequence of algebraic groups over K,

$$1 \to \mathbb{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 1$$

we obtain by Hilbert's Theorem 90 an injection

$$0 \longrightarrow H^1(G_K, \mathrm{PGL}_n) \xrightarrow{\delta_n} H^2(K, \mathbb{G}_m).$$

Combining these injections for all n we may identify $\mathrm{Br}(K)$ with a subgroup of $H^2(K, \mathbb{G}_m)$, but these groups are in fact isomorphic [26, X.5.9].

To construct elements of $\mathrm{Br}(K)$ we form the *cup product* [10, 4.7.3]. From the natural pairing

$$\begin{aligned} \mu_n \times \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mu_n \\ (\mu, a) &\longmapsto \mu^a \end{aligned}$$

we obtain a pairing on cohomology

$$\cup : H^1(G_K, \mu_n) \times H^1(G_K, \mathbb{Z}/n\mathbb{Z}) \longrightarrow H^2(K, \mu_n)$$

Combining the long exact sequence associated to the Kummer sequence

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \longrightarrow 0,$$

with Hilbert's Theorem 90, it follows that $H^1(G_K, \mu_n) \cong K^*/(K^*)^n$ and $H^2(K, \mu_n) \cong \mathrm{Br}(K)[n]$, and as the action of G_K on $\mathbb{Z}/n\mathbb{Z}$ is trivial, we have $H^1(G_K, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cont}}(G_K, \mathbb{Z}/n\mathbb{Z})$. Given $\chi \in \mathrm{Hom}_{\mathrm{cont}}(G_K, \mathbb{Q}/\mathbb{Z})$ and $a \in K^*/(K^*)^n$ we then write $(\chi, a) \in \mathrm{Br}(K)$ to denote the image of the pair under the cup product, and we call (χ, a) the *cyclic algebra* associated to χ and a. It is trivial if and only if a is a norm from the Galois extension defined by χ [10, 4.7.5]. In the case $n = 2$, $\mu_2 \cong \mathbb{Z}/2\mathbb{Z}$, and given a pair of elements $a, b \in K^*/(K^*)^2$ the central simple algebra (a, b) associated to this pair is the quaternion algebra generated over K by i, j with relations $i^2 = a, j^2 = b, ij = -ji$.

To (a, b) we associate a conic curve $ax^2 + by^2 = z^2$; (a, b) is trivial if and only if the conic has a rational point.

Next we recall some fundamental examples.

Example 1.1.1. By Wedderburn's little theorem, every finite division algebra is a field; that is, the Brauer group of a finite field is trivial [26, VIII.8]. Indeed, every finite extension of a finite field is cyclic, and the norm map on finite fields is surjective.

Example 1.1.2. Frobenius showed that the quaternions are the only nontrivial central simple algebra over the real numbers; $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ [26, VIII.4]. As $\mathbb{C}$ is the only nontrivial algebraic extension of $\mathbb{R}$, the only nontrivial cyclic algebra over $\mathbb{R}$ is the quaternion algebra $(-1, -1)$.

Example 1.1.3. For K a number field and ν a place of K, Hasse proved that $\mathrm{Br}(K_\nu) \cong \mathbb{Q}/\mathbb{Z}$; this holds more generally for any field complete with respect to a discrete valuation with finite residue field [26, XIII.6]. Given $A \in \mathrm{Br}(K_\nu)$, we write $\mathrm{inv}_\nu A$ to denote the class of A in $\mathbb{Q}/\mathbb{Z}$.

Example 1.1.4 (Brauer-Hasse-Noether-Albert Theorem)**.** For K a number field we have an exact sequence

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \oplus_\nu \mathrm{Br}(K_\nu) \xrightarrow{\Sigma \mathrm{inv}_\nu} \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \tag{1.1}$$

where ν runs over the places of K and $\Sigma \mathrm{inv}_\nu$ denotes the sum of local invariants (cf. [30, XIII.6]).

We will need to compute the local invariants of quaternion algebras over completions of $\mathbb{Q}$. Let ν be a place of $\mathbb{Q}$. The class of a quaternion algebra $(a, b)_\nu \in \mathrm{Br}(\mathbb{Q}_\nu)[2]$ in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ is easily computed in terms of Legendre symbols $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Theorem 1.1.5. *[26, XIV.4] If ν is the infinite place, $inv_\nu(a, b)_\nu = 1$ if and only if a or b is positive. Otherwise, ν is a finite place associated to a prime p, and we may write*

$a = p^\alpha u$ and $b = p^\beta v$, where $\alpha, \beta \in \mathbb{Z}$ and u, v are p-adic units. We have

$$inv_\nu(a,b)_\nu = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \quad \text{if } p \neq 2$$

$$inv_\nu(a,b)_\nu = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)} \quad \text{if } p = 2$$

where $\epsilon(t) = \frac{t-1}{2}$ mod 2 and $\omega(t) = \frac{t^2-1}{8}$ mod 2.

In particular, given $a, b \in \mathbb{Q}$, at a prime p for which a, b are p-adic units, the algebra $(a,b)_p \in \mathrm{Br}(\mathbb{Q}_p)$ is trivial. When a is a unit and b is a uniformizer, we have that $\mathrm{inv}_p(a,b)_p = \left(\frac{a}{p}\right)$.

For Laurent series fields we have

Proposition 1.1.6. *[10, 6.3.7] For K a perfect field, there is a split exact sequence*

$$0 \longrightarrow Br(K) \longrightarrow Br(K((t))) \xrightarrow{r_t} H^1(G_K, \mathbb{Q}/\mathbb{Z}) \longrightarrow 0.$$

Every central simple algebra $\mathcal{A}$ over $K((t))$ is a tensor product of a central simple algebra over K and a cyclic algebra of the form (χ, t) over $K((t))$. The map r_t is called a *residue map*. The image of $\mathcal{A}$ under r_t is χ (see [10, 6.3.8]).

1.2 The Brauer Group of a Scheme

We first recall the definition of the Brauer group of a scheme and review some fundamental examples; see [20, Chapter IV] for details. Let X/K be a projective variety. If L/K is a field extension, we will write X_L for $X \times_{\mathrm{Spec}\ K} \mathrm{Spec}\ L$ the base change of X from K to L and $\overline{X}$ for $X_{\overline{K}}$. We let $k(X)$ denote the function field of X, and for a point $x \in X(\overline{K})$ we let $k(x)$ denote the residue field at x.[1]

Definition 1.2.1. [20, IV.2.1] Let $\mathcal{O}_X$ be the structure sheaf on X. An *Azumaya algebra* over X is an $\mathcal{O}_X$-algebra $\mathcal{A}$ which is locally free as an $\mathcal{O}_X$-module and for which $\mathcal{A}_x \otimes k(x)$ is a central simple algebra over $k(x)$ for all x in X.

[1] The k here refers to the German *körper* for field, and not the field of definition.

Equivalently, an Azumaya algebra is an $\mathcal{O}_X$-algebra which is of finite-type as an $\mathcal{O}_X$-module and locally isomorphic (for the étale topology) to a matrix algebra. We may define an equivalence relation on the set of Azumaya algebras of X - two Azumaya algebras $\mathcal{A}, \mathcal{A}'$ are similar if there exist locally free $\mathcal{O}_X$-modules $\mathcal{E}, \mathcal{E}'$ of finite rank such that

$$\mathcal{A} \otimes \mathrm{End}_{\mathcal{O}_X}(\mathcal{E}) \approx \mathcal{A}' \otimes \mathrm{End}_{\mathcal{O}_X}(\mathcal{E}')$$

Under the operation of tensor product, we define the *Brauer group* $\mathrm{Br}(X)$ to be the group of equivalence classes of Azumaya algebras on X. We call an algebra *trivial* if it belongs to the equivalence class of $\mathcal{O}_X$.

$\mathrm{Br}(X)$ canonically injects into the *cohomological* Brauer group $H^2_{\acute{e}t}(X, \mathbb{G}_m)$, but in general, unlike the case with fields, these groups do not coincide[2]. The Skolem-Noether Theorem yields an exact sequence of group schemes for the étale topology

$$1 \to \mathbb{G}_m \to GL_n \to PGL_n \to 1,$$

and from the associated long exact sequence we obtain a map $H^1(X, PGL_n) \to H^2(X, \mathbb{G}_m)$ with image annihilated by n. We may identify the Azumaya algebras of rank n^2 with the elements of the cohomology set $H^1(X, PGL_n)$; if X has finitely-many connected components, $\mathrm{Br}(X)$ is a torsion group [20, IV.2.7].

Example 1.2.2. For a local Henselian ring R with maximal ideal $\mathbf{m}$, $\mathrm{Br}(R) \cong \mathrm{Br}(R/\mathbf{m})$ [20, IV.2.13]. Thus, if R is strictly Henselian or if R has finite residue field, $\mathrm{Br}(R)$ is trivial.

Example 1.2.3. For a smooth, projective conic $C/K : ax^2 + by^2 = z^2$, $\mathrm{Br}(C) \cong \mathrm{Br}(K)/\{(a, b)\}$ [10, 6.9]. If C has a rational point so that $C \cong \mathbb{P}^1$, we have that (a, b) is trivial and hence $\mathrm{Br}(\mathbb{P}^1) = \mathrm{Br}(K)$.

We now consider the case of curves more closely. That the Brauer group of a curve is related to arithmetic can be first seen in the vanishing of the geometric Brauer group. For function fields of curves, geometrically we have

[2]For smooth projective curves over a field they are isomorphic (cf. [20, IV.2.18(c)]).

Theorem 1.2.4 (Tsen's theorem)**.** *The Brauer group of a transcendence degree 1 extension over an algebraically closed field is trivial.*

Tsen's original proof has two components - that the functions in this field satisfy a Chevalley-Warning-like condition, and that the Brauer group of any such field is trivial. The first component is formalized in the following

Definition 1.2.5. A field k is called a *C^i-field* or simply C^i if, for any positive integer d, every homogeneous polynomial $f \in k[x_0, ..., x_n]$ of degree d in $n > d^i$ variables has a nontrivial solution in k^n.

The C^0 fields are precisely the algebraically closed fields. By the Chevalley-Warning Theorem, finite fields are C^1. As a transcendence degree 1 extension over an algebraically closed field is C^1 [10, 6.2.8], and the Brauer group of a C^1 field is trivial [10, 6.2.3], Tsen's theorem follows.

When X is regular and integral, the canonical map $\mathrm{Br}(X) \to \mathrm{Br}(k(X))$ is injective [20, IV.2.6]. When X is a curve over an algebraically closed field, Tsen's Theorem implies that $\mathrm{Br}(X)$ vanishes. In general, when X is a curve the question of which elements of $\mathrm{Br}(k(X))$ come from $\mathrm{Br}(X)$ is addressed by Grothendieck [11, V.1.7] in the exact sequence

$$0 \longrightarrow \mathrm{Br}(X) \longrightarrow \mathrm{Br}(k(X)) \longrightarrow H^2(X, \underline{\mathrm{Div}}),$$

where $\underline{\mathrm{Div}} = \bigoplus_{x \in X} x_* \mathbb{Z}$ with the sum taken over the prime divisors of X, and the map $\mathrm{Br}(k(X)) \to H^2(X, \underline{\mathrm{Div}})$ is induced by the map $k(X)^* \to \mathrm{Div}(X)$ sending a rational function to its associated divisor. We say an algebra $\mathcal{A} \in \mathrm{Br}(k(X))$ is *unramified* when it belongs to the kernel of the last map, and hence, extends to an element of $\mathrm{Br}(X)$. $\mathrm{Div}(\overline{X})$ is a free abelian group over the prime divisors of $\overline{X}$, and using the fact that $H^2(X, \mathbb{Z}) = H^1(X, \mathbb{Q}/\mathbb{Z})$, we may instead write

$$0 \longrightarrow \mathrm{Br}(X) \longrightarrow \mathrm{Br}(k(X)) \xrightarrow{\oplus r_x} \bigoplus_x H^1(G_{k(x)}, \mathbb{Q}/\mathbb{Z}).$$

where $G_{k(x)} = \mathrm{Gal}(\overline{K}/k(x))$ [11, VI.2.1]. The maps $r_x : \mathrm{Br}(k(X)) \to H^1(G_{k(x)}, \mathbb{Q}/\mathbb{Z})$ are called *residue maps*, and we say an algebra $\mathcal{A} \in \mathrm{Br}(k(X))$ is *unramified at x* when it

belongs to the kernel of r_x. To compute the residue maps r_x, we may apply Proposition 1.1.6 after passing to the completion of the local ring at x, which is isomorphic to a power series ring $k(x)[[t]]$.

Proposition 1.2.6. *[10, 6.4.3] Let K be a perfect field and x be a closed point of X over $\overline{K}$. Then the following diagram commutes*

$$\begin{array}{ccc} Br(k(X)) & \xrightarrow{r_P} & H^1(G_{k(x)}, \mathbb{Q}/\mathbb{Z}) \\ \Big\downarrow{\scriptstyle res_x} & & \Big\uparrow{\scriptstyle r_t} \\ Br(k(X_{k(x)})) & \longrightarrow & Br(k(x)((t))) \end{array}$$

where r_t is the residue map of Proposition 1.1.6.

The case where X is the projective line is originally due to Faddeev. The closed points of $\mathbb{P}^1$ (up to linear equivalence) are zeros of monic, irreducible polynomials, and as $\mathrm{Br}(\mathbb{P}^1) = \mathrm{Br}(K)$, in this case we may write [10, 6.4.6]

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \mathrm{Br}(k(\mathbb{P}^1)) \xrightarrow{\oplus r_x} \bigoplus_{x \in \mathbb{P}^1} H^1(G_{k(x)}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\Sigma \mathrm{Cor}_{k(x)}} H^1(G, \mathbb{Q}/\mathbb{Z}) \longrightarrow 0. \tag{1.2}$$

where $\mathrm{Cor}_{k(x)}$ denotes corestriction.

1.3 Curves and Arithmetic

For the remainder of this section we assume that X is a curve of positive genus with a rational point over K, and we let J denote the Jacobian of X. We now introduce a map $\kappa : \mathrm{Br}(X) \to H^1(G, \overline{J})$ in order to relate the Brauer group of X to the arithmetic of its Jacobian J; there is an exact sequence

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \mathrm{Br}(X) \xrightarrow{\kappa} H^1(G, \overline{J}) \longrightarrow 0. \tag{1.3}$$

The map $\mathrm{Br}(K) \to \mathrm{Br}(X)$ is defined by extension of scalars; we refer to the image of these algebras as *constant algebras.*

We give a direct construction of κ; see [5], [17], or [11, 2.5b]. Let $A \in \mathrm{Br}(X)$; via

the injection $\mathrm{Br}(X) \subset \mathrm{Br}(k(X)) = H^2(G, k(\overline{X}))$ we regard A as an algebra over the function field of X. Writing $\mathrm{P}(X) = k(X)^*/K^*$ for the group of principal divisors on X and $\mathrm{Pic}(X) = \mathrm{Div}(X)/\mathrm{P}(X)$ for the Picard group, we write A' for the image of A in $H^2(G, \mathrm{P}(\overline{X}))$. From the exact sequence of Galois modules

$$0 \longrightarrow \mathrm{P}(\overline{X}) \longrightarrow \mathrm{Div}(\overline{X}) \longrightarrow \mathrm{Pic}(\overline{X}) \longrightarrow 0$$

we obtain an exact sequence in cohomology

$$H^1(G, \mathrm{Div}(\overline{X})) \longrightarrow H^1(G, \mathrm{Pic}(\overline{X})) \xrightarrow{\partial} H^2(G, \mathrm{P}(\overline{X})) \longrightarrow H^2(G, \mathrm{Div}(\overline{X}))$$

As $A \in \mathrm{Br}(X)$, the image of A' in $H^2(G, \mathrm{Div}(\overline{X}))$ is 0, and hence there exists an element a' such that $\partial(a') = A'$. As $H^1(G, \mathrm{Div}(\overline{X}))$ vanishes (it splits as a direct sum of terms $H^1(\mathrm{Gal}(\overline{K}/L), \mathbb{Z})$ for L/K Galois), the connecting homomorphism ∂ is injective and a' is unique. As $X(K) \neq \emptyset$ the exact sequence

$$0 \longrightarrow \mathrm{Pic}^0(\overline{X}) \longrightarrow \mathrm{Pic}(\overline{X}) \xrightarrow{deg} \mathbb{Z} \to 0$$

splits, and since $H^1(G, \mathbb{Z}) = \mathrm{Hom}_{cont}(G, \mathbb{Z}) = 0$, we have

$$H^1(G, \mathrm{Pic}(\overline{X})) = H^1(G, \mathrm{Pic}^0(\overline{X})) = H^1(G, \overline{J}).$$

We define $\kappa(A) = a'$. To see that κ is surjective we use the exact sequence

$$0 \longrightarrow \overline{K}^* \longrightarrow k(\overline{X})^* \longrightarrow \mathrm{P}(\overline{X}) \longrightarrow 0$$

and part of the associated long exact sequence

$$\mathrm{Br}(K) \longrightarrow H^2(G, k(\overline{X})) \longrightarrow H^2(G, \mathrm{P}(\overline{X})) \longrightarrow H^3(G, \overline{K}^*).$$

The H^3 term vanishes when K is a local or number field [28], so the map $H^2(G, k(\overline{X})) \to H^2(G, \mathrm{P}(\overline{X}))$ is surjective. Given $a' \in H^1(G, \overline{J}) = H^1(G, \mathrm{Pic}(\overline{X}))$, $\partial(a') \in H^2(G, \mathrm{P}(\overline{X}))$

and lifts to an element of $H^2(G, k(\overline{X}))$. As $\partial(a')$ maps to 0 in $H^2(G, \mathrm{Div}(\overline{X}))$, the surjectivity of κ follows.

A higher powered derivation of the same sequence proceeds via a Hochschild-Serre spectral sequence $H^p(G, H^q(\overline{X}, \mathbb{G}_m)) \Rightarrow H^{p+q}(X, \mathbb{G}_m)$:

$$\mathrm{Pic}(X) \to H^0(G, \mathrm{Pic}(\overline{X})) \to \mathrm{Br}(K) \to \mathrm{Br}(X) \to H^1(G, \mathrm{Pic}(\overline{X})) \to H^3(G, \overline{K}^*).$$

As X has a K-rational point we have $\mathrm{Pic}(X) = H^0(G, \mathrm{Pic}(\overline{X}))$, yielding

$$0 \to \mathrm{Br}(K) \to \mathrm{Br}(X) \to H^1(G, \mathrm{Pic}(\overline{X})) \to H^3(G, \overline{K}^*)$$

As above, $H^3(G, \overline{K}^*)$ vanishes and $H^1(G, \mathrm{Pic}(\overline{X})) = H^1(G, \overline{J})$, so again we obtain the short exact sequence.

A K-rational point P on X defines an evaluation map $\mathrm{Br}(X) \to \mathrm{Br}(K)$ and hence a splitting of (1.3). We write $\mathcal{A}(P)$ for the image of $\mathcal{A} \in \mathrm{Br}(X)$ under this map; more generally, if $\Delta = P_1 + \cdots + P_m - Q_1 - \cdots - Q_n$ is a K-rational divisor we write $\mathcal{A}(\Delta)$ for the product

$$\mathcal{A}(P_1) \otimes \cdots \otimes \mathcal{A}(P_m) \otimes \mathcal{A}^{-1}(Q_1) \otimes \cdots \otimes \mathcal{A}^{-1}(Q_n).$$

We thus have a split exact sequence on n-torsion

$$0 \longrightarrow \mathrm{Br}(K)[n] \longrightarrow \mathrm{Br}(X)[n] \xrightarrow{\kappa} H^1(G, \overline{J})[n] \longrightarrow 0.$$

Writing $[n]J(K)$ for the image of $J(K)$ under the multiplication by n map, from the Kummer exact sequence for n-torsion we have

$$0 \longrightarrow J(K)/[n]J(K) \longrightarrow H^1(G, J[n]) \xrightarrow{\theta} H^1(G, \overline{J})[n] \longrightarrow 0$$

and combining the surjection with a section of κ we define

$$\eta_P : H^1(G, J[n]) \to \mathrm{Br}(X)[n] \tag{1.4}$$

The above map allows us to describe quaternion algebras on X in terms of principal homogeneous spaces for J.

Lemma 1.3.1. *[5, 4.1] Let K be a local, non-archimedean field of odd residue characteristic such that $X(K) \neq \emptyset$ and J has good reduction over K. If $\alpha \in K^*/(K^*)^2$ is a nonsquare unit and $F \in k(X)$ is a rational function such that the quaternion algebra $\mathcal{A} = (\alpha, F) \in Br(k(X))[2]$ is unramified, then $\mathcal{A}$ is a constant algebra.*

Proof. Let $P \in X(K)$, K_{nr}/K be the maximal unramified extension over K, and let $G_{nr} = \mathrm{Gal}(\overline{K}/K_{nr})$. Without loss of generality, we suppose $\mathcal{A}(P) \in \mathrm{Br}(K)$ is trivial and we show that $\mathcal{A}$ is trivial. Let $A \in H^1(G, J[2])$ belong to the pre-image of $\mathcal{A}$ under η_P. As η_P factors through θ, it suffices to show that $A \in \ker(\theta)$.

By our assumption on α, $\mathcal{A} \otimes_K K_{nr}$ is trivial. Applying the restriction map

$$\mathrm{Res}^G_{G_{nr}} : H^1(G, \overline{J}) \longrightarrow H^1(G_{nr}, \overline{J}),$$

it follows that $\mathrm{Res}^G_{G_{nr}} \circ \theta(A) = 0$. If k is the residue field of K, write j for the reduction of J. From [15, Lemma 5, p.675] and [14, Theorem 2 p.557], we have, respectively, that

$$H^1(\mathrm{Gal}(K_{nr}/K), J(K_{nr})) = H^1(\mathrm{Gal}(\overline{k}/k), j(\overline{k})) = 0$$

and from the inflation-restriction sequence it follows that $\mathrm{res}^G_{G_{nr}}$ is injective. □

Under the hypotheses of the lemma, for $R \in X(K)$ we have $\mathcal{A}(R) \in \mathrm{Br}(K)$, and as K is local the lemma implies $\mathrm{inv}\mathcal{A}(R) \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ is independent of R.

Chapter 2

The Brauer-Manin Obstruction for Curves

Let K be a number field and $\mathbb{A}_K$ be the ring of adeles over K. For each place ν of K, let $G_\nu = \mathrm{Gal}(\overline{K}_\nu/K_\nu)$. We say that a smooth, projective curve X over K *satisfies the Hasse principle* if the implication

$$X(\mathbb{A}_K) \neq \emptyset \Longrightarrow X(K) \neq \emptyset \tag{2.1}$$

holds. That is, X satisfies the Hasse principle if whenever it has points everywhere locally, it has a rational point. All genus 0 curves satisfy the Hasse principle; the anticanonical bundle gives an embedding of the curve as a conic, and the classical Hasse-Minkowski Theorem applies. The situation changes for curves of higher genus. One of the first counterexamples, discovered independently in the 1940s by Lind [18] and Reichardt [23], is given by the genus 1 plane curve $2y^2 = x^4 - 17$ over $\mathbb{Q}$. The genus 2 curve $y^2 = 5x^6 - 29$ over $\mathbb{Q}$, studied by Bremner [1], is also a counterexample. In both cases, the failure of the Hasse principle can be verified directly by reducing the local computations to a finite set of primes via the Hasse-Weil bound and, for the global computations, by working over $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-29})$, respectively.

From now on, we assume that $X(\mathbb{A}_K) \neq \emptyset$. If, nevertheless, $X(K)$ is empty, we now describe work of Manin [19] that explains the failure of the Hasse principle in some cases. The implication (2.1) is false in general, but by pairing the Brauer group of X with the exact sequence (1.1) of Brauer groups

$$0 \to \mathrm{Br}(K) \to \bigoplus_\nu \mathrm{Br}(K_\nu) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0,$$

we filter the adelic points to obtain a necessary condition for the existence of rational

points on X. This is motivated by the following observation - if $P \in X(K)$ is a rational point and $\mathcal{A} \in \mathrm{Br}(X)$, then as $\mathcal{A}(P) \in \mathrm{Br}(K)$ the sum of its local invariants is 0.

2.1 The Brauer-Manin Obstruction Sets

For each subset $B \subseteq \mathrm{Br}(X)$, we define the *Brauer-Manin obstruction* sets $X(\mathbb{A}_K)^B \subseteq X(\mathbb{A}_K)$. Let $(P_\nu) \in X(\mathbb{A}_K)$ be an adelic point. Each P_ν defines a K-morphism $\mathrm{Spec}\ K_\nu \to X$ and in turn a group homomorphism $\mathrm{Br}(X) \to \mathrm{Br}(K_\nu)$; we write the image of $\mathcal{A} \in \mathrm{Br}(X)$ under this morphism as $\mathcal{A}(P_\nu)$. By applying these homomorphisms and summing local invariants we define a pairing

$$X(\mathbb{A}_K) \times \mathrm{Br}(X) \longrightarrow \mathbb{Q}/\mathbb{Z}. \tag{2.2}$$

$$(P_\nu), \mathcal{A} \longmapsto \sum_\nu \mathrm{inv}_\nu \mathcal{A}(P_\nu) \tag{2.3}$$

The kernel of this pairing on the left will be denoted by $X(\mathbb{A}_K)^{\mathrm{Br}}$. This set consists of the adelic points of X that are orthogonal to every element of $\mathrm{Br}(X)$; in general, for any subset $B \subseteq Br(X)$, we define $X(\mathbb{A}_K)^B$ as the left kernel of the pairing when restricted on the right to B. By functoriality,

$$X(K) \subseteq X(\mathbb{A}_K)^{\mathrm{Br}} \subseteq X(\mathbb{A}_K)^B \subseteq X(\mathbb{A}_K),$$

so if $X(\mathbb{A}_K)^B = \emptyset$ then $X(K)$ is empty as well. If $X(\mathbb{A}_K) \neq \emptyset$ but $X(\mathbb{A}_K)^B = \emptyset$, we say that the failure of the Hasse principle is *explained by* the Brauer-Manin obstruction, and we say that B *obstructs* the existence of K-points.

Example 2.1.1. Following Creutz and Viray [7, 1.2], consider the curve $X : 2y^2 = x^4 - 17$ and the quaternion algebra $\mathcal{A} = (-x^2 - 4, -2)$ over its function field. Note that when the rational function $x^2 + 4$ vanishes $2y^2 + 1$ vanishes as well, so -2 is a square, and the poles of $x^2 + 4$ are of even order. It follows that $\mathcal{A}$ is unramified everywhere and extends to an element of $\mathrm{Br}(X)$.

For an l-adic point P_l on the curve, the local invariant $\mathrm{inv}_l \mathcal{A}(P_l)$ is independent of P_l. Indeed, at the infinite place $x^2 + 4 > 0$ and $\mathcal{A}(P)$ ramifies for all real points P. If l

is odd and x^2+4 vanishes at a point (x_l, y_l) over $\mathbb{Q}_l$, then $-2y_l^2 = 1$ and -2 is a square modulo l. Modulo 8, a point (x, y) on the curve must satisfy $x^2 \equiv 1$, but the algebra $(-5,-2)_2 = (3,-2)_2$ is trivial over $\mathbb{Q}_2$. The sum of local invariants is thus independent of the chosen adelic point, and the class of $\mathcal{A} \in \mathrm{Br}(X)$ obstructs the existence of rational points.

Let $J \cong \mathrm{Pic}^0(X)$ denote the Jacobian of X and Ш(J) denote the Tate-Shafarevich group:

$$\ker\left(H^1(G_K, J) \to \bigoplus_{\nu} H^1(G_\nu, J)\right).$$

The *index* δ of X is the smallest positive degree of a rational divisor on X. We may reduce to the index 1 case with the following

Proposition 2.1.2. *Suppose that* Ш(J) *is finite. Then there exists a subset* $B' \subseteq Br(X)$ *such that* X *has index 1 if and only if* $X(\mathbb{A}_{\mathbb{Q}})^{B'} \neq \emptyset$.

Proof. See Scharaschkin, [24, 1.1]. □

If $\delta > 1$ then $X(K)$ is necessarily empty, and as $X(\mathbb{A}_K)^{\mathrm{Br}} \subseteq X(\mathbb{A}_K)^{B'}$, the proposition implies that the Brauer-Manin obstruction explains the failure of the Hasse principle for such curves. Restricting then to the case of $\delta = 1$, for genus 1 curves the existence of a rational divisor of degree 1 is equivalent to the existence of a rational point. Thus, assuming the finiteness of Ш(J), the failure of the Hasse principle for genus 1 curves is explained by the Brauer-Manin obstruction.

Having explained all failures of the Hasse principle for curves with $\delta > 1$, and for genus 1 curves, from now on we will primarily be interested in curves of genus at least 2 with a degree 1 rational divisor. It is currently open as to whether the Brauer-Manin obstruction explains all counterexamples to the Hasse principle for such curves.

From section 2 of [21] we state

Theorem 2.1.3. *Let* $p \equiv 17 \pmod{24}$ *be prime and* $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$ *be an*

integer point on the threefold

$$\begin{cases} B^2 - C^2 + 2pEF = 0 \\ 2AB - 2CD + pF^2 = 0 \\ A^2 - D^2 + pG^2 = 0 \end{cases} \tag{2.4}$$

satisfying the following conditions:

(1) *Let l be any odd prime such that* $\gcd(l,3) = \gcd(l,p) = 1$ *and l divides E. Then p is a square in $\mathbb{Q}_l^\times$ or $\nu_l(E) - \nu_l(G) < 6n$.*

(2) $\gcd(A, D, G) = 1$, $E, G \not\equiv 0 \pmod p$

(3) *Let l be any odd prime such that* $\gcd(l,3) = \gcd(l,p) = 1$ *and*

$$\gcd(AC - BD, DE - CF, AE - BF) \equiv 0 \pmod l.$$

Then p is a square in $\mathbb{Q}_l^\times$.

(4) *There exists an integer H such that $G - EH^6 \equiv 0 \pmod p$ and $A + \zeta BH^4$ is a quadratic non-residue in $\mathbb{F}_p^\times$ for any cube root of unity ζ in $\mathbb{F}_p^\times$.*

Then for the curve $\mathcal{C} : py^2 = E^2x^{24} - G^2$, $\mathcal{C}(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.

Proof. Combine Lemma 2.1 and Theorem 2.2 of [21], with $n = 2$. The quaternion algebra $(A + Bx^4 + py, p)$ extends to an element of $\mathrm{Br}(\mathcal{C})$ and obstructs the existence of rational points. □

Quan then parameterizes a family of solutions to (2.4) satisfying $E = 27\kappa^3 G$ for $\kappa \in \mathbb{Z}$ [21, 3.1]; the curve $\mathcal{C}$ becomes, up to isomorphism, $\mathcal{C}_t : py^2 = x^{24} - t^6$, for $t \in \mathbb{Q}$.

While the method of proof in [21] is ad hoc - the ramification locus and local invariants associated to the algebra are all computed explicitly from the definitions - we generalize the computations in two ways. In Chapter 3 we construct the quaternion algebra of Example 2.1.3 by realizing the rational points on the threefold (2.4) as solutions to a 2-descent associated to an elliptic factor of the Jacobian of $\mathcal{C}_t$. The conditions

(1)-(4) are needed to compute the pairing (2.2), but in Chapter 4 we simplify the computations by showing the quaternion algebra we construct is locally constant at primes of good reduction. To compute the local invariants at these primes, we utilize a degree 1 rational divisor on $\mathcal{C}_t$. With these generalizations we give new examples.

2.2 Computing the Obstruction Set mod l

Scharaschkin describes in [24] a topological method of computing $X(\mathbb{A}_K)^{\mathrm{Br}}$ as an intersection inside $J(\mathbb{A}_K)$. Let Δ be a rational divisor of degree 1 on X. Identifying $J(\overline{K})$ with $\mathrm{Pic}^0(\overline{X})$, Δ defines an injection

$$\begin{aligned} \xi_\Delta : X(\overline{K}) &\longrightarrow J(\overline{K}) \\ P &\longmapsto [P - \Delta] \end{aligned}$$

which is defined over K. From the commutative diagram

$$\begin{array}{ccc} X(K) & \xrightarrow{\xi_\Delta} & J(K) \\ \downarrow & & \downarrow \\ \prod_\nu X(K_\nu) & \xrightarrow{\xi_\Delta} & \prod_\nu J(K_\nu) \end{array}$$

it follows that $X(K) \cong \xi_\Delta\left(\prod_\nu X(K_\nu)\right) \cap J(K)$ inside $\prod_\nu J(K_\nu)$. Each factor $J(K_\nu)$ has a topology as a set of points in an affine space over K_ν, and giving $\prod_\nu J(K_\nu)$ the product topology, we have the

Theorem 2.2.1. *[24, 1.2] Suppose that $Ш(J)$ is finite and X has a rational divisor of degree 1 Δ. Then*

$$X(K) \cong \xi_\Delta\left(\prod_\nu X(K_\nu)\right) \cap J(K) \subseteq \xi_\Delta\left(\prod_\nu X(K_\nu)\right) \cap \overline{J(K)} \cong X(\mathbb{A}_K)^{\mathrm{Br}}$$

where the closure of $J(K)$ is taken inside the group $\prod_\nu J(K_\nu)$.

By a theorem of Serre [25, 1.3], the topology on $J(K)$ induced by the product coincides with that defined by the subgroups of $J(K)$ of finite index. In the case that J has rank 0 the closure of $J(K)$ is itself, hence as a corollary we have

Corollary 2.2.2. *[24, 1.3] Suppose that* $Ш(J)$ *and* $J(K)$ *are finite, and* X *has a rational divisor of degree 1* Δ*. If the Hasse principle fails for* X*, then it is explained by the Brauer-Manin obstruction.*

In some examples it is possible to show that $X(\mathbb{A}_K)^{\mathrm{Br}}$ is empty by by replacing J with abelian varieties A which admit maps from X. If $\psi : X \to A$ is a morphism, it follows from the universal property of the Jacobian that $\xi_\Delta\left(\prod_\nu X(K_\nu)\right) \cap \overline{J(K)}$ maps into $\psi\left(\prod_\nu X(K_\nu)\right) \cap \overline{A(K)}$. As in corollary 2.2.2, the closure of $A(K)$ is determined by its subgroups of finite index, so if A has rank 0 then we may conclude $X(\mathbb{A}_K)^{\mathrm{Br}} = \emptyset$.

This observation allows us to analyze example 2.1.3 in a different fashion.

Example 2.2.3. The curve $\mathcal{C}_t : py^2 = x^2 4 - t^6$ admits a nonconstant map to the elliptic curve $E_p : pY^2 = X^3 - 1$ via $(x, y) \mapsto (t^{-2}x^8, t^{-3}y)$. E_p is the quadratic twist by the prime p of the elliptic curve $y^2 = x^3 - 1$ with complex multiplication by $\sqrt{-3}$, and we may use the theory of half-integral weight modular forms to relate the Fourier coefficients $a(p)$ of the L-function associated to E_{-1} to the ranks of the curves E_p over $\mathbb{Q}$. Indeed, the Mellin transform of $L(E_{-1}, s)$ is the weight 2 cusp form $\eta^4(6z)$, where

$$\eta(z) = e^{\frac{\pi i z}{12}} \prod_{n=1}^{\infty}(1 - q^n)$$

is Dedekind's eta function and $q = e^{2\pi i z}$. The weight $\frac{3}{2}$ eigenform

$$\eta^2(12z)\theta(z) = q + 2q^2 + 2q^5 + 2q^{10} - 2q^{13} - 4q^{14} - 2q^{17} - \cdots \in S_{\frac{3}{2}}(144, \chi_0)$$

corresponds under the Shimura lift to $\eta^4(6z)$, where

$$\theta(z) = \sum_{n \in \mathbb{Z}} q^{n^2}$$

is the classical theta function of Riemann. By a theorem of Waldspurger [29], if $a(p) \neq 0$ then $L(E_p, 1) \neq 0$, and as E_p has complex multiplication it follows from work of Coates and Wiles [6] that E_p has rank 0. Frey [9, Korollar 1] showed that for $p \equiv 5 \pmod{12}$ E_p has rank 0, so when $p \equiv 17 \pmod{24}$, the Jacobian $\mathcal{J}_t$ of $\mathcal{C}_t$ has a rank 0 quotient.

Thus, assuming the finiteness of $Ш(\mathcal{J}_t)$, the Brauer-Manin obstruction explains the lack of rational points on $\mathcal{C}_t$.

Remark 2.2.4. If $\psi : X \to A$ is a nonconstant map to an abelian variety A, then another reduction can be made by studying $\psi\left(\prod_\nu X(K_\nu)\right) \cap \overline{A(K)}$ after reduction at the places of good reduction for A. Indeed, if ν is a finite place and k_ν denotes the residue field of K_ν, by an abuse of notation we consider the sets $\psi\left(\prod_\nu X(k_\nu)\right) \cap A(K)$ and $\psi\left(\prod_\nu X(k_\nu)\right) \cap \overline{A(K)}$, where we reduce $A(K)$ at each finite place and consider its closure with respect to its subgroups of finite index. If an ordering of the places of K is fixed, then the latter set is nonempty if and only if there is a tuple of points $(p_i) \in \prod_i X(k_{\nu_i})$ and a sequence of points $Q_n \in A(K)$ such that for every $n > 1$, $\psi(p_i) = Q_n$ (as points in $A(k_{\nu_i})$) for $i < n$.

Example 2.2.5. Consider a smooth, projective model of the hyperelliptic curve $X : y^2 = 5x^6 - 29$. The curve can be constructed by glueing the two affine curves

$$\begin{cases} y^2 = 5x^6 - 29 \\ v^2 = -29u^6 + 5 \end{cases}$$

according to the relations $xu = 1, vx^3 = y$. We note that X has a degree 1 rational divisor and its Jacobian has positive rank, so the possible failure of the Hasse principle on this curve is not immediately explained by Corollary 2.2.2. Indeed, an ad-hoc approach suffices to construct the divisor - we need only consider the difference of any odd degree rational divisor with the appropriate multiple of a rational divisor of degree 2. X has rational points over $\mathbb{Q}(\sqrt{-29})$ that give rise to a degree 2 rational divisor, and X admits a map $(x, y) \mapsto (x^3, y)$ of degree 3 to the conic curve $Y^2 = 5X^2 - 29Z^2$ associated to the quaternion algebra $(5, -29)$. This algebra is unramified at 2 and infinity, and by Theorem 1.1.5, we compute

$$(5, -29)_5 = \left(\frac{-29}{5}\right) = \left(\frac{1}{5}\right) = 1$$
$$(5, -29)_{29} = \left(\frac{5}{29}\right) = \left(\frac{-1}{5}\right) = 1$$

and it follows that the quaternion algebra is trivial and the conic curve has a rational point. Pulling any such rational point back along the degree 3 map yields a rational divisor on X of degree 3, and thus a rational divisor of degree 1.

Bremner's proof [1] that X has no rational points relies on the fact that the class number of $K = \mathbb{Q}(\sqrt{-29})$ is 6; if $(x_0, y_0) \in X(\mathbb{Q})$, factoring over K we have

$$5x_0^6 = y_0^2 + 29 = (y_0 + \sqrt{-29})(y_0 - \sqrt{-29}),$$

and while it follows that the primes that lie over 5 are principal in K, a norm computation shows that this is impossible. That X has points everywhere locally is seen by direct computation; by the Weil bounds we need only check the primes of bad reduction and $p \leq 13$.

Alternatively, we may show $X(\mathbb{Q})$ is empty using the preceding Remark 2.2.4. X admits a map to the elliptic curve $E : y^2 = x^3 + 5^2(-29)$ given by $\psi : (x, y) \mapsto (5x^2, 5y)$. Following [24, 4.3], we search for a prime p at which $\psi(X(\mathbb{F}_p)) \cap E(\mathbb{Q})$ is empty, from which it follows $\prod_p \psi(X(\mathbb{F}_p)) \cap \overline{E(\mathbb{Q})}$ and $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$ are empty as well. Computations in `sage` reveal that $E(\mathbb{Q})$ has rank 1 and is generated by the point $P = (3^2, 2)$, which at $p = 13$ has order 3. Thus, we check whether the points $P, 2P = (2^{-4}3^2 6529, -2^{-6}14244059)$ or the point at infinity are in the image of ψ modulo 13. The point at infinity pulls back to the points on X with $u = 0$, and it follows that $\psi(X(\mathbb{F}_p)) \cap E(\mathbb{Q})$ is non-empty if and only if 5 or $5 \cdot 6529$ is a square modulo 13. By quadratic reciprocity

$$\left(\frac{6529}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{1}{3}\right) = 1$$
$$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$$

so we conclude that $X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$ is empty.

Chapter 3

Hyperelliptic Curves with Split Jacobian

As we saw in Corollary 2.2.2, we may conclude that the Brauer group obstructs the Hasse principle on a smooth curve when its Jacobian has finite Tate-Shafarevich group and admits a map to an abelian variety of Mordell-Weil rank 0. In general, if $\phi : A \to B$ is a surjective homomorphism of abelian varieties, A is isogenous to the direct sum of B with the connected component of the identity in $\ker \phi$. If B and $\ker \phi$ are of positive dimension, we say A is *decomposable*. Thus, in order to produce nontrivial examples of curves violating the Hasse principle for which Corollary 2.2.2 does not apply, we will study how their Jacobians decompose. The simplest nontrivial case occurs when B is an elliptic curve, and we say that an abelian variety is *split* if it is isogenous to a product of elliptic curves. The study of hyperelliptic curves with split Jacobian began with the study of hyperelliptic integrals and their reduction to elliptic integrals. Legendre studied some of the first examples. In Volume 2 of his *Traité* (1826) he considers the integrals

$$\int \frac{\mathrm{d}x}{\sqrt{1-x^n}}$$

for $n = 6, 8, 12$. He resolves each case by reducing the integral to a (sum of) elliptic integrals of the first kind; indeed, geometrically the Jacobian of these curves is isogenous to a power of an elliptic curve. Bolza in 1887 gave a family of genus 2 curves with split Jacobian and degree 4 maps to elliptic curves. We will utilize the description of the degree 4 case by Bruin and Doerksen [2, 1.1] in the construction of quaternion algebras on hyperelliptic curves of genus 5.

3.1 Decomposable Jacobians

If X is a curve with Jacobian J_X, we may use the automorphism group of the curve to decompose its Jacobian.

Theorem 3.1.1. *[12, B] Let $G \subseteq Aut(X)$ be a subgroup such that $G = H_1 \cup H_2 \cup \ldots \cup H_t$, where the subgroups $H_i \subseteq G$ satisfy $H_i \cap H_j = \{1\}$ for $i \neq j$. Then we have the isogeny relation*

$$J_X^{t-1} \times J_{X/G}^{|G|} \sim J_{X/H_1}^{h_1} \times \cdots \times J_{X/H_t}^{h_t}$$

where $h_i = |H_i|$ and J^n is the n-fold product of J with itself.

Based on the partition of the group G we initially only deduce an isogeny with a power of J_X, but as any abelian variety is isogenous to a direct product of simple abelian varieties, it is possible to decompose the Jacobian itself. We apply the theorem to a hyperelliptic curve with an extra involution.

Example 3.1.2. A hyperelliptic curve of the form $X : y^2 = a_{2g+2}x^{2g+2} + a_{2g}x^{2g} + \cdots + a_2x^2 + a_0$ with genus g has at least two involutions - the hyperelliptic involution i and the involution j sending $x \mapsto -x$ - hence has automorphism group containing $\langle i, j\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The quotient by the hyperelliptic involution is a projective line and has trivial Jacobian, thus applying Theorem 3.1.1, we find

$$J_X^2 \times J_{X/\langle i,j\rangle}^4 \sim J_{X/\langle i\rangle}^2 \times J_{X/\langle j\rangle}^2 \times J_{X/\langle ij\rangle}^2$$
$$J_X^2 \sim J_{X/\langle j\rangle}^2 \times J_{X/\langle ij\rangle}^2$$

and it follows that $J_X \sim J_{X/\langle j\rangle} \times J_{X/\langle ij\rangle}$. Applying Riemann-Hurwitz to the quotients $X/\langle j\rangle$ and $X/\langle ij\rangle$ of X, if g is odd then these curves have genera $\frac{g-1}{2}$ and $\frac{g+1}{2}$, respectively, and if g is even then they both have genus $\frac{g}{2}$.

Note that in the genus 2 case, the Jacobian of X splits as product of two elliptic curves. We consider this case in more detail.

A *polarization* on an abelian variety A is an isogeny $\lambda : A \to \check{A}$ with the dual abelian variety to A which, over $\overline{K}$, arises from an ample line bundle on $\overline{A}$. An abelian variety

together with a polarization is called a *polarized abelian variety.* A polarization is called *principal* when it is an isomorphism.

Definition 3.1.3. Let $(A, \lambda_A), (B, \lambda_B)$ be principally-polarized abelian varieties of dimension g. We say that an isogeny $\Phi : A \to B$ is a *polarized* $(n_1, \ldots, n_g)$*-isogeny* if $\ker(\Phi)(\overline{K}) \simeq \bigoplus_{i=1}^{g} \mathbb{Z}/n_i\mathbb{Z}$ and $\Phi^\vee \circ \lambda_B \circ \Phi = n^g \lambda_A$ where $n^g = \prod_{i=1}^{g} n_i$.

For a genus 2 curve X with Jacobian J, we say that J is (n, n)-split if J admits a polarized (n, n)-isogeny to a product of elliptic curves.

The existence of an (n, n) splitting of J is equivalent to the existence of a dominant map of degree n from X to an elliptic curve; we call the (n, n) splitting *optimal* if the map from X to the elliptic curve has minimal degree. Conversely, given two elliptic curves E and F, we can produce a genus 2 curve defined over $\overline{K}$ with degree n maps to E and F; identifying $E[n](\overline{K})$ and $F[n](\overline{K})$ with the trivial Galois-module $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, J is isomorphic to the quotient of $E \times F$ by the subgroup $E[n](\overline{K}) \oplus F[n](\overline{K})$. For the resulting curve to be defined over K, we need only a Galois-module isomorphism $\phi' : E[n] \to F[n]$ that is an *anti-isometry* for the Weil pairing; if $e_{E[n]}, e_{F[n]}$ denote the respective Weil pairings on n-torsion, ϕ' is an anti-isometry if, for $P, Q \in E[n]$, we have $e_{E[n]}(P, Q) = e_{F[n]}(\phi'(P), \phi'(Q))^{-1}$. The kernel of the desired isogeny $\phi : E \times F \to J$ is the graph of ϕ'.

We quote from [2] a description of (2,2)-split Jacobians. In this case, any anti-isometry is automatically an isometry.

Lemma 3.1.4 ([2], 3.1)**.** *Let K be a field with char$(K) \neq 2$ and let $E_1 : V^2 = f(U)$ be an elliptic curve over K, where $f(U) \in K[U]$ is a monic square-free cubic. Specifying (E_2, α), where E_2 is an elliptic curve over K and $\alpha : E_1[2] \to E_2[2]$ is an anti-isometry is equivalent to specifying $a \in K \cup \{\infty\}$ with $f(a) \neq 0$ and $d \in K^*$ representing an element in $K^*/(K^*)^2$ such that*

$$E_2 : \begin{cases} W^2 = -df(U) & \text{if } a = \infty \\ W^2 = d(U - a)f(U) & \text{otherwise} \end{cases}$$

where $0_{E_2} \in E_2(K)$ is the unique point with $U(0_{E_2}) = a$ and the anti-isometry is given by $\alpha(0_{E_1}) = 0_{E_2}$ and $\alpha((u,0)) = (u,0)$ for any $(u,0) \in E_1[2] - \{0_{E_1}\}$.

Theorem 3.1.5 ([2], 3.2)**.** *Let K be a field with $char(K) \neq 2$. Let E_1, E_2 be elliptic curves given by models*

$$E_1 : V^2 = f(U)$$
$$E_2 : W^2 = d(U-a)f(U)$$

and let $\alpha : E_1[2] \to E_2[2]$ be the isometry induced by the identification $U(E_1[2]-\{0_{E_1}\}) = E_2[2] - \{0_{E_2}\}$. If $a \neq \infty$ then the fiber product $C_2 = E_1 \times_{\mathbb{P}^1_U} E_2$ is a curve of genus 2 admitting a model $Y^2 = f(X^2/d + a)$ where the double covers $\phi_1 : C_2 \to E_1$ and $\phi_2 : C_2 \to E_2$ are induced by the relations

$$U = \frac{1}{d}X^2 + a, \qquad V = Y, \qquad W = XY.$$

Furthermore, the isogeny $\phi_1^* + \phi_2^* : E_1 \times E_2 \to Jac(C_2)$ is the (2,2)-splitting corresponding to α.

3.2 (4,4)-splittings

To motivate the considerations of this section, we first prove the following

Lemma 3.2.1. *Let $f(t) \in K[t]$ be an irreducible polynomial of odd degree n with splitting field L/K and leading coefficient -1. If the roots of f are squares in L, then the quaternion algebra $\mathcal{A} = (f(t), t) \in Br(k(\mathbb{P}^1))$ is unramified over K.*

Proof. Applying Faddeev's exact sequence (1.2) and Proposition 1.2.6, we check that the residue maps vanish at $0, \infty$, and the zeros of f. As f is irreducible and the roots of f are squares in L, the constant term of f is a square in K. It follows that f is a square in $K[[t]]$, so $\mathcal{A}$ is unramified at 0.

Over L, f factors as

$$(\alpha_1 - t)(\alpha_2 - t)\cdots(\alpha_n - t),$$

so we may write $\mathcal{A}_L$ as a product of quaternion algebras of the form $(\alpha_i - t, t)$. Each α_i is a square in L so $\alpha_i - t$ is a norm in $L(\sqrt{t})$. Thus, $\mathcal{A}$ is unramified at the places $t - \alpha_i$, for each i.

To find the residue at ∞, note that $-t$ is a norm in the quadratic extension generated by $\sqrt{t}$. As n is odd t^{n+1} is a square, so we may consider the equivalent quaternion algebra

$$\left(\frac{-tf(t)}{t^{n+1}}, \frac{t}{t^2}\right) = \left(\frac{-tf(t)}{t^{n+1}}, \frac{1}{t}\right).$$

At infinity $1/t$ is a uniformizer, and as $-tf(t)/t^{n+1}$ is a polynomial of degree n in $1/t$ with constant coefficient 1, it follows that $\mathcal{A}$ is unramified at ∞. □

The condition of the lemma on the splitting field L means that $f(t)$ and $g(t) = f(t^2)$ have the same splitting field.

To classify (4,4)-splittings on genus 2 curves, note that any such splitting factors through a (2,2)-splitting. Indeed, if $E_1 \times E_2 \to J$ is a (4,4)-splitting with kernel $\Delta_4 \subseteq E_1[4] \times E_2[4]$ coming from the graph of an anti-isometry $E_1[4] \to E_2[4]$, then since $E_i[2] \subseteq E_i[4]$, the anti-isometry restricts to an anti-isometry on the 2-torsion, and Δ_4 restricts to the graph Δ_2 of this anti-isometry. Setting $A = (E_1 \times E_2)/\Delta_2$, $E_1 \times E_2 \to A$ is a (2,2)-splitting. Every 2 dimensional abelian variety is the Jacobian of a genus 2 curve, and we may describe the curve associated to A explicitly.

Lemma 3.2.2. *[2, 6.1] Let K be a field with char$(K) \neq 2$. Let $\Phi_4 : E_1 \times E_2 \to J$ be an optimal (4,4)-splitting over K that factors through the (2,2)-splitting $\Phi_2 : E_1 \times E_2 \to A$. Suppose that $A = Jac(C_2)$ where C_2 is a curve of genus 2. Then C_2 admits a model of the form*

$$C_2 : Y^2 = g(X) = f(X^2) = c_3X^6 + c_2X^4 + c_1X^2 + c_0$$

such that $g(X)$ and $f(X)$ have the same splitting field and Gal(g) is isomorphic to $\widetilde{S}_3$, the subgroup $\langle (135)(246), (12)(36)(45) \rangle$ of S_6.

Let K be a number field, C be a curve with a (2,2)-split Jacobian J, and suppose C admits a degree 2 map to an elliptic curve E_1. E_1 has a model of the form $V^2 = f(U)$, where $f(U) = U^3 + bU + c$, and $b, c \in K$; we assume the Galois group of the splitting

field of f is S_3. C in turn has a model of the form

$$y^2 = g(x) := f\left(\frac{x^2}{d} + a\right),$$

where $a, d \in K$. Following lemma 3.2.2 above and computations in [2], we study when f and g have the same splitting field. Working over the extension $K[U]/f(U) := K(r)$, we may write

$$f(U) = (U - r)(U^2 + rU + (r^2 + b)) \tag{3.1}$$

$$g(x) = \frac{1}{d^3}(x^2 + ad - rd)h(x), \tag{3.2}$$

where $h(x) = x^4 + (dr + 2ad)x^2 + d^2(r^2 + ar + a^2 + b)$. As f splits over a quadratic extension of $K(r)$, for g to have the same splitting field as f, h must be reducible over $K(r)$. To factor h, we use

Lemma 3.2.3. *[13] Let $h(x) = x^4 + c_2x^2 + c_4$ be a polynomial over a field k of characteristic not 2. Then h is irreducible over k if and only if the following are not squares in k:*

$$(i) \quad c_2^2 - 4c_4$$

$$(ii) - c_2 + 2\sqrt{c_4}$$

$$(iii) - c_2 - 2\sqrt{c_4}$$

We apply the lemma with $k = K(r)$ and

$$c_2 = dr + 2ad$$

$$c_4 = d^2(r^2 + ar + a^2 + b),$$

so h is reducible if and only if one of

$$(i) \quad (dr+2ad)^2 - 4d^2(r^2+ar+a^2+b), \text{ or}$$
$$(ii) \quad -(dr+2ad) + 2d\sqrt{r^2+ar+a^2+b}, \text{ or}$$
$$(iii) \quad -(dr+2ad) - 2d\sqrt{r^2+ar+a^2+b},$$

is a square in $K(r)$. (i) is the discriminant of h as a quadratic polynomial and up to squares is equal to $-3r^2-4b$, which is the discriminant of the quadratic factor of f from (3.1) above. If this is a square then f splits over $K(r)$, which contradicts our assumption that the Galois group of f is S_3. For the remaining cases, suppose first $r^2+ar+a^2+b=t^2$ with $t \in K(r)$. Expressing t in terms of the basis $\{1, r, r^2\}$ for $K(r)/K$, we expand $t^2 = (t_2r^2+t_1r+t_0)^2$ and equate coefficients with r^2+ar+a^2+b. Treating a as a variable, this defines a reducible curve in $\mathbb{A}^4$ with solutions over K if and only if there exists $s \in K$ such that

$$a = \frac{s^4 - 2bs^2 - 8cs + b^2}{4f(s)}. \tag{3.3}$$

Replacing $\sqrt{r^2+ar+a^2+b}$ by $t = t_2r^2+t_1r+t_0$ and expanding (ii) and (iii), we have reduced to considering whether

$$d = -f(s) \cdot \square \tag{3.4}$$

where $\square$ is now a square in K. If $-d$ is a square, then condition (3.3) above leads to a relation of 2-divisibility between K-rational points on the elliptic curve E_1.

Lemma 3.2.4. *Let $E_1 : V^2 = f(U) = U^3 + bU + c$ be an elliptic curve over K such that $Gal(f) \cong S_3$ and $C : y^2 = g(x) = f(x^2/d + a)$ be a degree 2 cover over K. Suppose $d \equiv -1$ up to squares and there exists a K-rational point P on E_1 with $U(P) = a$. If $P \in [2]E_1(K)$ then f and g have the same splitting field.*

Proof. If $P = [2]Q$ with $U(Q) = s$, then (3.3) is satisfied by the definition of the multiplication by 2 map on E_1, and as Q is a K-rational point (3.4) is satisfied as well. As (ii) is then a square, by lemma 3.2.3 h is reducible over $K(r)$ and f, g have the same

splitting field over K. $\square$

We will not be interested in case (iii), but it is the principal case of interest in [2] for the characterization of (4,4)-split Jacobians.

Chapter 4

Obstructions on Curves with Split Jacobian

The main result of this chapter, Theorem 4.2.1, will be the construction of an infinite family of hyperelliptic curves of genus 5 for which the failure of the Hasse principle is explained by the Brauer-Manin obstruction. Generalizing the construction given in example 2.1.3, to each curve in the family we associate an Azumaya algebra which pairs nontrivially by (2.2) with every adelic point on the curve.

4.1 Global Construction

We consider an elliptic curve $E : y^2 = x^3 + bx + c$ over a number field K with a point $P \in E(\overline{K})$ such that $x([2]P) = 0$ and $x(P) \in K$. Recall for a point $P \in E(\overline{K})$,

$$x([2]P) = \frac{x^4 - 2bx^2 - 8cx + b^2}{4(x^3 + bx + c)},$$

hence if $x([2]P) = 0$ then $x(P)$ must satisfy $x^4 - 2bx^2 - 8cx + b^2 = 0$. If $\alpha \in K$ is a root of this polynomial, then writing the numerator of $x([2]P)$ as $(x - \alpha)(x^3 + \alpha x^2 + \beta x + \gamma)$ (note the coefficient of x^3 is 0), we find the following relations

$$-2b = \beta - \alpha^2$$

$$b^2 = -\alpha\gamma$$

$$-8c = \gamma - \alpha\beta$$

and a two-parameter family of curves satisfying this descent condition

$$E_{\alpha,\beta} : y^2 = x^3 + \frac{\alpha^2 - \beta}{2}x + \frac{(\alpha^2 + \beta)^2}{32\alpha}.$$

For convenience we write

$$c_4(\alpha,\beta) = \frac{\alpha^2-\beta}{2} \qquad\qquad c_6(\alpha,\beta) = \frac{(\alpha^2+\beta)^2}{32\alpha}.$$

Up to nonzero constant factors, the discriminant of this curve is

$$\frac{(11\alpha^4-26\alpha^2\beta+27\beta^2)(7\alpha^2-\beta)^2}{\alpha^2},$$

so excluding finitely-many $\alpha,\beta\in K$, $E_{\alpha,\beta}$ is an elliptic curve. A point P on $E_{\alpha,\beta}$ with $x(P)=\alpha$ has $x([2]P)=0$.

We construct a quaternion algebra of the form $\mathcal{A}' := (A+Bx+Cy,x)\in \mathrm{Br}(k(E_{\alpha,\beta}))$ that is invariant under the involution $[-1]$ induced by the map $(x,y)\to(x,-y)$ on $E_{\alpha,\beta}$. Since $\mathcal{A}'$ is a quaternion algebra, $\mathcal{A}'=[-1]\mathcal{A}'$ if and only if $\mathcal{A}'\otimes[-1]\mathcal{A}'$ is trivial. Towards satisfying this condition, we write $\mathbb{N}\mathcal{A}'$ for $\mathcal{A}'\otimes[-1]\mathcal{A}'$ and consider

$$\begin{aligned}\mathbb{N}\mathcal{A}' &= (A+Bx+Cy,x)\cdot(A+Bx-Cy,x)\\ &= ((A+Bx)^2-C^2y^2,x).\end{aligned}$$

Since $F=(A+Bx)^2-C^2y^2$ is a norm in the quadratic extension $k(E_{\alpha,\beta})/K(x)$, we may express F as a cubic polynomial in x with leading coefficient $-C^2$ and we have $\mathbb{N}\mathcal{A}'=(F,x)\in\mathrm{Br}(k(\mathbb{P}^1))$.

If we apply Faddeev's exact sequence (1.2), for (F,x) to be unramified at $x=0$ we require

$$A^2-\frac{(\alpha^2+\beta)^2}{32\alpha}C^2=D^2, \tag{4.1}$$

where $D\in K$. Computing residues at the zeros of F, we require the zeros to be squares over the splitting field of F. As we saw in Lemma 3.2.4, this condition on the splitting field of F is related to the $(4,4)$-splittings of a genus 2 curve. To apply Lemma 3.2.4, we make a linear change of variables, replacing x by $\frac{x-12B^2}{-36C^2}$ over $\mathbb{P}^1$, to write

$\mathbb{N}\mathcal{A}' = (x^3 + bx + c, d(x - a))$, where

$$\begin{aligned} a =& 12B^2 \\ b =& 1296\frac{\alpha^2 - \beta}{2}C^4 - 2592ABC^2 - 432B^4 \\ c =& -46656\frac{(\alpha^2 + \beta)^2}{32\alpha}C^6 - 15552\frac{\alpha^2 - \beta}{2}B^2C^4 + 46656A^2C^4 + 104AB^3C^2 + 3456B^6 \\ d =& -\frac{1}{36C^2}. \end{aligned}$$

Set $f(U) = F(\frac{U-12B^2}{-36C^2}) = U^3 + bU + c$, consider the elliptic curve $E_{A,B,C} : V^2 = f(U)$ and the genus 2 curve defined by $v^2 = g(u) = f(u^2/d + a)$. Then, by Lemma 3.2.4, f and g have the same splitting field if some K-rational point with $U = 12B^2$ is divisible by 2.

We consider the product abelian variety $E_{\alpha,\beta} \times E_{A,B,C}$ and the curve $X_{A,B,C}$ obtained via fibered product over the x-coordinate of $E_{\alpha,\beta}$ and the rational function $\frac{U-12B^2}{-36C^2}$ on $E_{A,B,C}$. Working over $\overline{K}$, the fiber over $x = 0$ contains the point

$$\left(0, \frac{(\alpha^2 + \beta)}{4\sqrt{2\alpha}}\right) \times (12B^2, D).$$

To divide the latter point by two, we view the conic (4.1) as a surface $\mathcal{S}$. By taking a linear section L of the surface, the family of curves given by points on $\mathcal{S}$ and L has a structure of an elliptic surface, and over the projective line with $\frac{U-12B^2}{-36C^2}$ as coordinate it becomes a birationally ruled surface[1] we denote by $\mathcal{E}_L$. Similarly, we write $\mathcal{X}_L$ for the family of fibered products (a ruled surface over $E_{\alpha,\beta}$) and the projection from the fibered product onto the second factor induces a double cover $\mathcal{X}_L \to \mathcal{E}_L$ of ruled surfaces.

Towards performing the 2-descent on $\mathcal{E}_L$, we will transfer the descent data from the elliptic curve to the surface by an appropriate choice of section L. If $Q \in E_{A,B,C}(K)$ satisfies $U([2]Q) = 12B^2$, the points on $E_{A,B,C}$ over $x = \alpha$ have U-coordinate $12B^2 - 36C^2\alpha$, so we will require $U(Q) = 12B^2 - 36C^2\alpha$. Computing $[2]Q$ and factoring $U([2]Q) - 12B^2 = 0$, we find that this occurs exactly when $(8\alpha A + (\alpha^2 + \beta)B)C = 0$.

[1] A surface fibered over a smooth curve is *birationally ruled* if the generic fiber is isomorphic to $\mathbb{P}^1$. Some authors (eg. Hartshorne) require *every* fiber to be a projective line.

As the fiber with $C = 0$ is degenerate, we choose

$$8\alpha A + (\alpha^2 + \beta)B = 0 \tag{4.2}$$

for the section L, and together with (4.1) above, the pair defines a smooth conic curve with a rational point $(A, C, D) = (1, 0, 1)$.

Theorem 4.1.1. *On the elliptic curve $E_{\alpha,\beta} : y^2 = x^3 + c_4(\alpha, \beta)x + c_6(\alpha, \beta)$, the quaternion algebras*

$$\mathcal{A}'_m = \left(1 - \frac{8\alpha}{\alpha^2 + \beta}x + \frac{2m}{c_6(\alpha, \beta) + m^2}y, x\right),$$

with $m \in K$ such that $c_6(\alpha, \beta) + m^2 \neq 0$, are invariant under $[-1]$.

Proof. Given a tuple $(A, B, C, D) \in K^4$, let $\mathcal{A}' = (A + Bx + Cy, x) \in \mathrm{Br}(k(E_{\alpha,\beta}))$ and $\mathbb{N}\mathcal{A}' = (F, x) \in \mathrm{Br}(k(\mathbb{P}^1))$ where F is a polynomial in x of degree 3 with leading coefficient $-C^2$, as above. If the tuple satisfies (4.1) $\mathbb{N}\mathcal{A}'$ is unramified at $x = 0$, and if the tuple satisfies (4.2) the roots of F are squares in its splitting field. Applying Lemma 3.2.1 to F/C^2, it follows $(F/C^2, x) = \mathbb{N}\mathcal{A}' \in \mathrm{Br}(k(\mathbb{P}^1))$ is unramified everywhere, hence belongs to $\mathrm{Br}(K)$. Evaluating at infinity on $E_{\alpha,\beta}$, $\mathbb{N}\mathcal{A}'$ is trivial, thus $\mathcal{A}'$ is invariant under the action of $[-1]$. Parameterizing the conic in (4.1) we may write

$$C = \frac{2m}{c_6(\alpha, \beta) + m^2}A$$

for $m \in K$, and solving for B in (4.2), we find that $\mathcal{A}'$ equals $\mathcal{A}'_m$ in $\mathrm{Br}(k(E_{\alpha,\beta}))$ up to the algebra (A, x) which is trivially invariant under $[-1]$. □

Corollary 4.1.2. *Suppose $\beta \neq -\alpha^2$. Then $\mathcal{A}'_m$ is unramified away from the point at infinity and the points with $x = 0$.*

Proof. If both

$$f_+ = 1 - \frac{8\alpha}{\alpha^2 + \beta}x + \frac{2m}{c_6(\alpha, \beta) + m^2}y$$
$$f_- = 1 - \frac{8\alpha}{\alpha^2 + \beta}x - \frac{2m}{c_6(\alpha, \beta) + m^2}y$$

vanish at a point, then both

$$f_+ + f_- = 2\left(1 - \frac{8\alpha}{\alpha^2+\beta}x\right)$$
$$f_+ - f_- = \frac{4m}{c_6(\alpha,\beta)+m^2}y$$

must vanish as well, which can only occur when $y = 0$ and $x = \frac{\alpha^2+\beta}{8\alpha}$. The points on $E_{\alpha,\beta}$ with $x = \frac{\alpha^2+\beta}{8\alpha}$ are 2-torsion exactly when $\beta = -\alpha^2$ (the curves with j-invariant 1728), so excluding these values of the parameters, f_+, f_- never vanish simultaneously. Thus, away from where $x = 0$ or the point at infinity, either xf_+ or xf_- will be regular and nonzero, hence $\mathcal{A}'_m$ can be represented by either (f_+, x) or (f_-, x) at all such points of $E_{\alpha,\beta}$. □

For later use we record some information about the valuations of the rational function occurring as the coefficient of y in $\mathcal{A}'_m$.

Lemma 4.1.3. *Let $\alpha, \beta, m \in \mathbb{Q}$ such that $(m, c_6(\alpha,\beta)) = 1$. For a prime ℓ, we have*

$$\nu_\ell\left(\frac{2m}{c_6(\alpha,\beta)+m^2}\right) = \nu_\ell(2) + \begin{cases} 0, & \text{if } \ell | c_6(\alpha,\beta) \\ \nu_\ell(m), & \text{if } \ell | m \\ -\nu_\ell(c_6(\alpha,\beta)+m^2), & \text{otherwise} \end{cases}$$

4.2 The curve $dy^2 = x^3 - 1$

We now apply the results of the previous section to construct unramified algebras on curves whose Jacobian contains a factor of the form $E_{\alpha,\beta}$. We will consider curves over $K = \mathbb{Q}$; for a prime l, let ν_l be the associated valuation. Let $d, t \in \mathbb{Z}$ be integers such that

(L1) d, t are square-free and relatively-prime.

(L2) t is odd, $t \equiv 0 \pmod 3$ and for each prime $l|t$, $l \equiv 3 \pmod 4$ and d is a non-square modulo l.

(L3) $d > 0$, and for each prime $l|d$, $l \equiv 1 \pmod 8$ and t is a square modulo l.

In this section we will prove

Theorem 4.2.1. *Given integers d, t satisfying (L1)-(L3), if d factors into a product of an odd number of primes l with $l \equiv 2 \pmod 3$, then for the curve $C : dy^2 = x^{12} - t^6$, $C(\mathbb{A}_{\mathbb{Q}})^{\{\mathcal{A}\}} = \emptyset$.*

Set $\alpha = -2d, \beta = 4d^2$ so that $E = E_{-2d,4d^2} : Y^2 = X^3 - d^3$ is the quadratic twist of the $j = 0$ curve $y^2 = x^3 - 1$ by d. We now construct a quaternion algebra on the hyperelliptic curve $C/\mathbb{Q}$ with affine model $dy^2 = x^{12} - t^6$ and show that it extends to an element of $\mathrm{Br}(C)$. The curve C is determined up to isomorphism by the class of $d, t \in \mathbb{Q}^*/\mathbb{Q}^{*2}$, so we assume $\nu_l(dt) = 1$ for each $l|dt$. An open cover of C is given by the affine varieties $dy^2 = x^{12} - t^6$ and $dv^2 = -t^6u^{12} + 1$, identified along $xu = 1, vx^6 = y$. Using the notation from the previous section, C maps to E via $\phi_1 : (x, y) \mapsto (dt^{-2}x^4, d^2t^{-3}y)$ and the genus 1 curve $F : dY^2 = X^4 - t^6$ via $\phi_2 : (x, y) \mapsto (x^3, y)$. As an illustration of the methods of the previous section, we will now exhibit an algebra $\mathcal{A} \in \mathrm{Br}(C)$ for which $C(\mathbb{A}_{\mathbb{Q}})^{\{\mathcal{A}\}} = \emptyset$.

From Theorem 4.1.1 we have a family of quaternion algebras for $m \in \mathbb{Q}$

$$\mathcal{A}'_m = (1 + \frac{2}{d}X + \frac{2m}{m^2 - d^3}Y, X) \in \mathrm{Br}(k(E))$$

that are invariant under the action of $[-1]$ and unramified outside of infinity and the points with $x = 0$. We pull back $\mathcal{A}'_m$ to C along ϕ_1.

$$\begin{aligned}
\mathcal{A}_m = \phi_1^*\mathcal{A}'_m &= (\phi_1^* f_+, \phi_1^* X) \\
&= \left(1 + 2t^{-2}x^4 + d^2t^{-3}\frac{2m}{m^2 - d^3}y, dt^{-2}x^4\right) \\
&= \left(1 + 2t^{-2}x^4 + d^2t^{-3}\frac{2m}{m^2 - d^3}y, d\right)
\end{aligned}$$

For simplicity we replace m by dn, to write

$$\begin{aligned}\mathcal{A}_{dn} &= \left(1 + 2t^{-2}x^4 + d^2t^{-3}\frac{2dn}{d^2n^2 - d^3}y, d\right)\\ &= \left(1 + 2t^{-2}x^4 + dt^{-3}\frac{2n}{n^2 - d}y, d\right)\\ &= (t, d) \otimes \left(t^3 + 2tx^4 + d\frac{2n}{n^2 - d}y, d\right)\\ &= (t, d) \otimes \left(t^3(n^2 - d) + 2t(n^2 - d)x^4 + 2ndy, d\right),\end{aligned}$$

where the last step follows as $n^2 - d$ is a norm in the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$.

Lemma 4.2.2. *$\mathcal{A}_{dn}$ is unramified, hence extends to an element of $Br(C)$.*

Proof. Dividing f_+ through by x^6, in a neighborhood of the points at infinity $u = 0$ we may express $\mathcal{A}_{dn}$ up to constant algebras as

$$\left(t^3(n^2 - d)u^6 + 2t(n^2 - d)u^2 + 2ndv, d\right).$$

The points at infinity, in (u, v) coordinates, are $(0, \pm\sqrt{d}^{-1})$. It follows that $\mathcal{A}_{dn}$ is unramified and extends to an element of $\mathrm{Br}(C)$. □

Towards applying Lemma 1.3.1 we will require a degree 1 rational divisor class.

Lemma 4.2.3. *The genus 1 curve $dY^2 = X^4 - t^6$ has a rational point if and only if $-d$, up to square factors in $\mathbb{Q}^*$, is the x-coordinate of a rational point on the elliptic curve $y^2 = x^3 - 4d^2t^6x$.*

Proof. We employ a descent via two-isogeny. On the elliptic curve $E : y^2 = x^3 + 4d^2t^6x$ with identity O, the quotient by the subgroup $\{O, (0, 0)\}$ of E defines an isogeny $\phi : E \to E'$, where $E' : y^2 = x^3 - 4d^2t^6x$. If S denotes a finite set of places including the archimedean places, 2, and the places of bad reduction, and we set

$$\mathbb{Q}(S, 2) = \{q \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : \nu(d) \equiv 0 \pmod 2 \text{ for all } \nu \notin S\}$$

then there is an exact sequence

$$0 \longrightarrow E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\delta} \mathbb{Q}(S,2) \longrightarrow WC(E/\mathbb{Q})[\phi]$$

where $WC(E/\mathbb{Q})$ is the Weil-Chatelet group of principal homogeneous spaces under E, $\delta(x,y) = x$, and $q \in \mathbb{Q}(S,2)$ maps to the genus 1 curve

$$C_q : qw^2 = q^2 - 16d^2t^6z^4$$

under the last map [27, Proposition X.4.9]. In particular, the image of $-dt^4$ under this map is

$$C_{-dt^4} : -dt^4w^2 = d^2t^8 - 16d^2t^6z^4$$
$$\frac{1}{d}w^2 = -t^2 + 16z^4$$

which is isomorphic to $dY^2 = X^4 - t^6$. If $-d$ is, up to square factors in $\mathbb{Q}$, the x-coordinate of a $\mathbb{Q}$-rational point on E', then it is in the image of δ, and hence $C_{-dt^4} \in WC(E/\mathbb{Q})[\phi]$ is trivial and has a $\mathbb{Q}$-rational point. □

On the genus 1 curve $F : dY^2 = X^4 - t^6$, suppose then $Q \in F(\mathbb{Q})$ and set

$$\Delta = \phi_2^* Q - \{x = 0\} \in \mathrm{Pic}^1_{\mathbb{Q}}(C).$$

As $\mathcal{A}_{dn}$ is invariant under [-1], $\mathcal{A}_{dn}(\{x = 0\}) = 0$. If Q has coordinates (X_0, Y_0), we have $dY_0^2 = X_0^4 - t^6$ and fixing a third root χ_0 of X_0 and a primitive third root of unity

ζ_3, we have

$$\begin{aligned}\mathcal{A}_{dn}(\Delta) = \mathcal{A}_{dn}(\phi_2^* Q) &= (t,d) \otimes \prod_{i=0}^{2} \left(t^3(n^2-d) + 2t(n^2-d)(\zeta^i \chi_0)^4 + 2ndY_0, d \right) \\ &= (t,d) \otimes \prod_{i=0}^{2} \left(t^3(n^2-d) + 2t(n^2-d)\zeta^i X_0 \chi_0 + 2ndY_0, d \right) \\ &= (t,d) \otimes \left(\prod_{i=0}^{2} \left(t^3(n^2-d) + 2t(n^2-d)\zeta^i X_0 \chi_0 + 2ndY_0 \right), d \right) \\ &= (t,d) \otimes \left((t^3(n^2-d) + 2ndY_0)^3 + (2t(n^2-d)X_0)^3 X_0, d \right) \in \mathrm{Br}(\mathbb{Q})\end{aligned}$$

Let $c_0 = (t^3(n^2-d) + 2ndY_0)^3 + (2t(n^2-d)X_0)^3 X_0$. We will employ Theorem 1.1.5 repeatedly in the proof of the following lemma.

Lemma 4.2.4. *Let n be an integer such that $\nu_2(n) = 0$, $(n,d) = 1$, and for all $l|t$ we have $\nu_l(n) = 2$, then we have*

$$inv_l(c_0, d) = \begin{cases} 0, & \text{if } l|2, d \\ \frac{1}{2}, & \text{if } l|t \end{cases}.$$

Proof. At $l = 2$, as $d \equiv 1 \pmod 8$ it follows the local invariant is trivial. For $l|t$, as d is a non-square modulo l and $dY_0^2 \equiv X_0^4 \pmod l$, we have $X_0 \equiv 0 \pmod l$ and $Y_0 \equiv 0 \pmod{l^2}$. Furthermore,

$$\begin{aligned}\nu_l(dY_0^2) &= \nu_l(X_0^4 - t^6) \\ \nu_l(d) + 2\nu_l(Y_0) &= 2 \cdot \min(2\nu_l(X_0), 3\nu_l(t)) \\ \nu_l(Y_0) &= \min(2\nu_l(X_0), 3).\end{aligned}$$

Since $\nu_l(n) = 2$ and $\nu_l(n^2 - d) = 0$ and we have

$$\begin{aligned}
\nu_l((t^3(n^2-d) + 2ndY_0)^3) &= 3 \cdot \min(\nu_l(t^3(n^2-d)), \nu_l(2ndY_0)) \\
&= 3 \cdot \min(3, \nu_l(n) + \nu_l(Y_0)) \\
&= 3 \cdot \min(3, 2 + \nu_l(Y_0)) \\
&= 9 \\
\nu_l((2t(n^2-d)X_0)^3 X_0) &= 3 + 4\nu_l(X_0).
\end{aligned}$$

It follows $\nu_l((t^3(n^2-d) + 2ndY_0)^3 + (2t(n^2-d)X_0)^3 X_0)$ is odd and hence the local invariant at l is nontrivial.

Lastly, for $l|d$ we have $X_0^4 \equiv t^6 \pmod{l}$ and hence modulo l

$$\begin{aligned}
(t^3(n^2-d) + 2ndY_0)^3 + (2t(n^2-d)X_0)^3 X_0 &\equiv t^9 n^6 + 8t^3 n^6 X_0^4 \\
&\equiv t^9 n^6 + 8t^9 n^6 \\
&\equiv 9t^9 n^6.
\end{aligned}$$

As t is a square modulo l, it follows the local invariant is trivial. □

Fixing a value for n according to the hypotheses of the previous lemma, we evaluate the algebra at Δ and define

$$\begin{aligned}
\mathcal{A} &= \mathcal{A}_{dn} \otimes \mathcal{A}_{dn}(\Delta) \\
&= \left(t^3(n^2-d) + 2t(n^2-d)x^4 + 2ndy, d \right) \otimes (c_0, d)
\end{aligned}$$

Lemma 4.2.5. *For all adelic points $(R_l)_l \in C(\mathbb{A}_Q)$ we have*

$$inv_l \mathcal{A}(R_l) = \begin{cases} 0, \textit{if } l \not| d \\ 0, \textit{if } l|d, l \equiv 1 \ (mod\ 3), l = a^2 + b^2 \textit{with } b \equiv 0 \ (mod\ 6) \\ \frac{1}{2}, \textit{if } l|d, l \equiv 2 \ (mod\ 3) \end{cases} .$$

Proof. Let l be a prime of $\mathbb{Q}$. By Lemma 1.3.1, if C has good reduction at l then $\mathcal{A} \otimes \mathbb{Q}_\ell$

is a constant algebra, and as Δ has degree 1, we have

$$\mathcal{A}(R_\ell) = \mathcal{A}(\Delta) = \mathcal{A}_{dn}(\Delta) \otimes \mathcal{A}_{dn}(\Delta)$$

which is trivial.

If $l = 2$, as $d \equiv 1 (\text{mod } 8)$, it follows again from Theorem 1.1.5 that $\text{inv}_2\mathcal{A}(R_2) = 0$ for all $R_2 \in C(\mathbb{Q}_2)$. As d is positive, $\mathcal{A}(R_\infty)$ is unramified at the infinite place for $R \in X(\mathbb{R})$.

For the primes $l|t$, having shown that $\text{inv}_l(c, d) = \frac{1}{2}$, it suffices to show that for each local point $R_l = (x_l, y_l) \in C(\mathbb{Q}_l)$ we have

$$\text{inv}_l\Big(t^3(n^2 - d) + 2t(n^2 - d)x_l^4 + 2mdy_l, d\Big) = \frac{1}{2}$$

We have $\nu_l(2t(n^2 - d)x_l^4 + 2mdy_l) \geq 5$ and as d is a nonsquare modulo l, the claim follows.

Lastly, for $l|d$ we have $x^{12} \equiv t^6 \pmod{l}$ hence $x^4 \equiv \zeta_3^i t^2 \pmod{l}$ for some $0 \leq i \leq 3$. Then

$$\begin{aligned}
\text{inv}_l\mathcal{A}(R_l) &= \left(\frac{t^3(n^2 - d) + 2t(n^2 - d)x_l^4 + 2ndy_l}{l}\right) \\
&= \left(\frac{t^3n^2 + 2\zeta_3^i n^2 t^3}{l}\right) \\
&= \left(\frac{t^3}{l}\right)\left(\frac{n^2}{l}\right)\left(\frac{1 + 2\zeta_3^i}{l}\right) \\
&= \left(\frac{1 + 2\zeta_3^i}{l}\right)
\end{aligned}$$

Note that

$$1 + 2\zeta_3^i = \begin{cases} 3, & \text{if } i = 0 \\ (-1)^{i-1}\sqrt{-3}, & \text{if } i = 1, 2. \end{cases}$$

If $l \equiv 1 \pmod 3$ the second case follows from quartic reciprocity [16, 6.2] and our assumptions on l. If $l \equiv 2 \pmod 3$ only the $i = 0$ case is possible, and then 3 is a nonsquare modulo l. $\square$

We may now give a proof of Theorem 4.2.1

Proof. Since there are an odd number of primes l dividing d with $l \equiv 2 \pmod 3$, the claim is immediate from Lemma 4.2.5. $\square$

Chapter 5

Computations with Sage

Recall our setup: X is a smooth curve of genus $g > 1$ over a number field K with Jacobian J and a degree 1 rational divisor class Δ. This divisor class defines an embedding $\eta_\Delta : X \to J$. Let T_X denote the set of places of good reduction for X.

Following Remark 2.2.4, with a morphism $\psi : X \to A$ we can show that $X(\mathbb{A}_K)^{\mathrm{Br}}$ is empty directly by showing $\psi\left(\prod_\nu X(k_\nu)\right) \cap \overline{A(K)}$ is empty. If $T \subset T_X$, we have the reverse inclusion

$$\psi\left(\prod_{\nu \in T_X} X(k_\nu)\right) \cap \overline{A(K)} \subset \psi\left(\prod_{\nu \in T} X(k_\nu)\right) \cap \overline{A(K)},$$

so in particular we may show $X(\mathbb{A}_K)^{\mathrm{Br}}$ is empty after computations at a finite set of primes. This leads to the following

Conjecture 5.0.6. *[22, 5.1] If $X(K) = \emptyset$, then there exists a finite set $T \subset T_X$ such that the images of $J(K)$ and $\prod_{\nu \in T} X(k_\nu)$ in $\prod_{\nu \in T} J(k_\nu)$ do not intersect.*

There is both data and heuristic to support this conjecture. Scharaschkin originally applied his method to a twist $3x^4 + 4y^4 = 19z^4$ of the Fermat quartic [24, 5.1] and the hyperelliptic curve $y^2 = 2(x^3 + 7)(x^3 - 7)$ [24, 5.3]. In both cases he used a map to an elliptic curve and a set S of one or two primes to show the sets of rational points for these curves are empty.

Flynn [8] considered 145 curves of genus 2 with local points at all places. Working with the full Jacobian of each curve he showed in most cases that the Brauer-Manin obstruction explains the lack of rational points.

Poonen [22] gave a heuristic argument for the above conjecture by modeling the image of $X(k_\nu)$ in $J(k_\nu)$ with subsets of $J(k_\nu)$ of the same size.

Bruin and Stoll [3] considered all the genus 2 curves

$$y^2 = f_6x^6 + f_5x^5 + \cdots + f_1x + f_0$$

with $f_i \in \{-3, -2, \ldots, 2, 3\}$, some of the curves having been considered but left unresolved by Flynn. After discarding the curves with obvious or easily found rational points (e.g. If f_6 is a square the points at infinity are rational) and those without rational points that could be treated by other means (e.g. 2-descent), they considered 1492 curves with local points and a degree 1 rational divisor class and were able to verify Conjecture 5.0.6 unconditionally for all but 42. More recently, they have implemented a general "Mordell-Weil Sieve" algorithm [4] and applied it to curves of genus 3. Implementation is limited by the often difficult computation of the Mordell-Weil group of J.

5.1 Algorithms

As further evidence for the conjecture, for curves defined over $\mathbb{Q}$, we implement an algorithm in Python/Sage to compute the intersection of the $\mathbb{Q}$-rational points of a suitable quotient of J and $X(\mathbb{F}_p)$ for $p \in T_X$. Given a curve X as above, an abelian variety A, a map $\psi : X \to A$, and a prime $p \in T_X$, we have the following diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{\psi} & A(\mathbb{Q}) \\ \downarrow & & \downarrow \\ X(\mathbb{F}_p) & \xrightarrow{\overline{\psi}} & A(\mathbb{F}_p) \end{array}$$

We compute as follows:

1. Compute generators $P_1, \ldots, P_n \in A(K)$ for the Mordell-Weil group of A.

2. For each P_i, compute its image $\overline{P_i}$ under the reduction map $A(\mathbb{Q}) \to A(\mathbb{F}_p)$ and the order m_i of each $\overline{P_i}$ as an element of the finite group $A(\mathbb{F}_p)$.

3. The image of $A(\mathbb{Q})$ in $A(\mathbb{F}_p)$ can be identified with a quotient of $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus$

$\mathbb{Z}/m_n\mathbb{Z}$. For each tuple $(a_1, \ldots, a_n)$ in the image, we compute

$$\overline{\psi}^{-1}(a_1\overline{P_1} \oplus \cdots \oplus a_n\overline{P_n}) \cap X(\mathbb{F}_p)$$

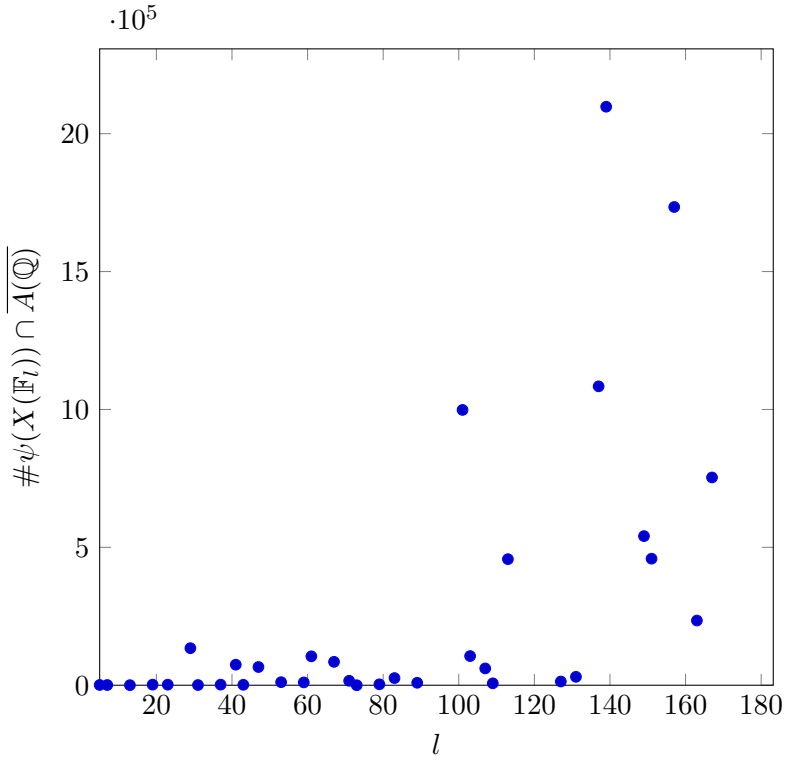
and count the tuples with nonempty intersection.

5.2 Examples

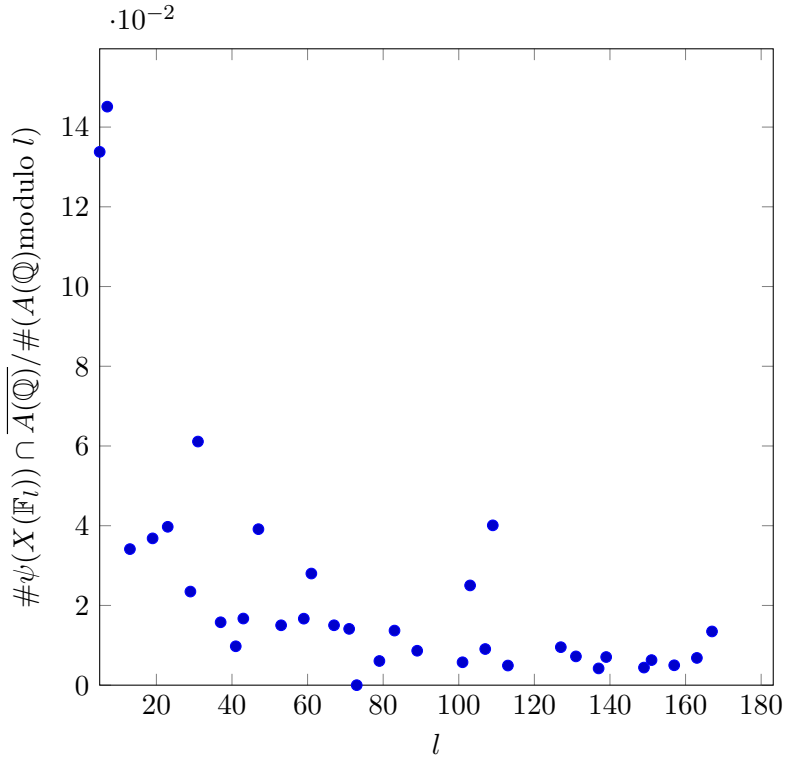
We retain the notation of section 4.2: $C/\mathbb{Q}$ is a genus 5 curve given by the equation $dy^2 = x^{12} - t^6$, where d, t satisfy the conditions (L1)-(L3).

As in [21], we first consider the case where $d = p$ is a prime congruent to 17 (mod 24). With $p \equiv 17 \equiv 5 \pmod{12}$, C has an elliptic curve quotient with rank 0 by Example 2.2.3, so it already follows from Corollary 2.2.2 that the Brauer-Manin obstruction explains the lack of rational points for these curves. With $d = 41$ and $t = 21$, the genus 1 curve $41Y^2 = X^4 - 21^6$ has a rational point $(\frac{4851}{50}, \frac{657531}{2500})$, so C has a $\mathbb{Q}$-rational divisor of degree 1.

With $d = 97 \cdot 17$ and $t = 33$, the genus 1 quotient of C $97 \cdot 17Y^2 = X^4 - 33^6$ has a rational point $(\frac{9801}{25}, \frac{2299968}{625})$, so C has a $\mathbb{Q}$-rational divisor of degree 1. C admits a degree 2 map to the genus 2 curve $C' : 97 \cdot 17Y^2 = X^6 - 33^6$, which in turn maps to an abelian variety A which is a sum of elliptic curves, and we apply the algorithm above to the composition of these maps. $\psi(X(\mathbb{F}_l)) \cap \overline{A(\mathbb{Q})}$ is empty for $l = 73$. If these sets are not empty, how large are they on average? A graph of our computations are below.



We may view the same data after dividing $\#\psi(X(\mathbb{F}_l)) \cap A(\mathbb{Q})$, for each l, by the number of rational points in $A(\mathbb{Q})$ modulo l.



Appendix A

Code

The Python code below defines a class that was used in the computations of the previous section. The code is available for download at the link

math.rutgers.edu/ ∼ ttyrrell/thesisCode.sage

```
def __init__(self,E,a,d):
    #Error Checking
    if d==0:
        print "Please choose a value for d not equal to 0";
        return false;
    elif a!=0:
        print "Not Implemented";
        return false;

    x,y = PolynomialRing(QQ,2,'xy').gens();
    self.f = (1/4)*E.torsion_polynomial(2,x);
    self.a = a;
    self.b = self.f.coefficient(x);
    self.c = self.f.subs(x=0)
    self.d = d;

    from sage.schemes.elliptic_curves.jacobian import Jacobian;
    self.eFactors = [E,Jacobian(y^2 - d*(x-a)*self.f)];

    self.badprimes = [p for (p,k) in list(factor(6*E.discriminant()*d))];

    self.ranks = [self.eFactors[k].rank(only_use_mwrank = false)
                  for k in range(2)];
    self.torsion = [self.eFactors[k].torsion_subgroup().points()
                  for k in range(2)];
    self.gens = [self.eFactors[k].gens() + self.torsion[k]
                  for k in range(2)];

    #see below for a definition.  We run this for initialization purposes.
    self._clear();

    self.data = dict();
    self.density = dict();

def _clear(self):
    self._p = None;   #a prime for use in computation
```

```
    self._K = None;
    self._eFactors1 = [None,None];
    self._ident1 = [None,None];

def _initialize(self,p):
    self._p = p;
    self._K = GF(p);
    self.cp = self._K(self.c);
    self.dp = self._K(self.d);
    self._eFactors1 = [self.eFactors[k].reduction(self._p)
                       for k in range(2)];
    self._ident1 = [self._eFactors1[k](0,1,0) for k in range(2)];

#reduceMWGroup(p):
#Given a prime p, this procedure will take the elements of self.gens,
#reduce them modulo p, and compute the (finite!) abelian group they
#generate.
def reduceMWGroup(self,p):
    self._initialize(p);
    mw = [[] for _ in range(2)];
    for k in range(2):
        for R in self.gens[k]:
            i=0;
            R1 = self._eFactors1[k](R);
            o1 = R1.order();
            genR1 = [self._ident1[k]];
            while i < o1:
                genR1.append(genR1[i]+R1);
                i=i+1;
            if len(mw[k]) == 0:
                mw[k] = genR1;
            else:
                mw[k] = map(lambda (R,S): R+S,
                            CartesianProduct(mw[k],genR1));
    return mw;

#Checks whether (R,S) lies on the image of X mod p.
def _isPointOnX(self,R,S):
    if R==self._ident1[0]:
        return S[0]==0 and S[2]!=0;
    elif S==self._ident1[1]:
        return R[0]==0 and R[2]!=0;
    else:
        return  R.xy()[0]*S.xy()[0] == self.dp*self.cp
                and is_quartic_residue(self.dp*R.xy()[0],self._p);

#Building off of the previous method numPointsOnX(...) counts for a
#given prime how many rational points are in the image of X mod p.
def numPointsOnX(self,p,verbose=true):
    mw = self.reduceMWGroup(p);
    mwE = mw[0];
    mwF = mw[1];
    l=0;
    for R in mwE:
        for S in mwF:
            if self._isPointOnX(R,S):
                l=l+1;
    self.data[p]=(l);
    self.density[p]=RR(l/(len(mwE)*len(mwF)));
```

```
    if verbose:
        if l==1:
            print "There is 1 point on X mod %d with density %f"
                % (p, self.density[p]);
        else:
            print "There are %d points on X mod %d with density %f"
                % (self.data[p],p,RR(self.density[p]));

#generateData() will run a sequence of computations, counting points at
#each prime p between L and U.
def generateData(self,L=0,U=500,verbose=true,zeroCount=false):
    for p in Primes():
        if p >= L and  p <= U and not(p in self.badprimes):
            self.numPointsOnX(p,verbose,zeroCount);
        elif p > U:
            self._clear();
            break;
    if verbose:
        print self.data

#displays data/densities
def printData(self,density=false):
    print "Printing data...";
    for p in self.data:
        print p, self.data[p];

    if density:
        print "Printing densities..."
        for p in self.density:
            print p, self.density[p];

#Given a quadratic residue a and a prime p, determines whether a is a
#biquadratic residue.  If p = 3 (mod 4) this is a given (if sqrt(a) is a
#nonsquare, -sqrt(a) is).  If p = 1 (mod 4) then we compute a^((p-1)/4).
def is_quartic_residue(a,p):
    if Mod(p,4)==3:
        return a.is_square();
    else:
        return a^((p-1)/4)==1

#Given an elliptic curve E: y^2 = f(x) = x^3 + bx + c and rational
#numbers a,d, this function computes and returns the complimentary curve
#E' - E x E' is isogeneous to the Jacobian of the genus 2 curve y^2 =
#f(x^2/d + a)
def compEllipticCurve(E,a,d):
    x,y = PolynomialRing(QQ,2,'xy').gens();
    from sage.schemes.elliptic_curves.jacobian import Jacobian;
    E1 = Jacobian(y^2 - d*(x-a)*self.f);
    del x,y;

    return E1;
```

References

[1] A. Bremner. Some interesting curves of genus 2 to 7. *J. Number Theory*, 67(2):277–290, 1997.

[2] N. Bruin and K. Doerksen. The arithmetic of genus two curves with (4,4)-split Jacobians. *Canad. J. Math. 63(2011), 992-1021*, 02 2009.

[3] N. Bruin and M. Stoll. Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17(2):181–189, 2008.

[4] N. Bruin and M. Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010.

[5] V. Chernousov and V. Guletskiĭ. 2-torsion of the Brauer group of an elliptic curve: generators and relations. In *Proceedings of the Conference on Quadratic Forms and Related Topics (Baton Rouge, LA, 2001)*, number Extra Vol., pages 85–120 (electronic), 2001.

[6] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Inventiones mathematicae*, 39:223–252, 1977.

[7] B. Creutz and B. Viray. Two torsion in the Brauer group of a hyperelliptic curve, 03 2014. `http://arxiv.org/abs/1403.2924`.

[8] E. V. Flynn. The Hasse principle and the Brauer-Manin obstruction for curves. *Manuscripta Math.*, 115(4):437–466, 2004.

[9] G. Frey. Der Rang der Lösungen von $Y^2 = X^3 \pm p^3$ über $\mathbf{Q}$. *Manuscripta Math.*, 48(1-3):71–101, 1984.

[10] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[11] A. Grothendieck. Le groupe de Brauer. III. Exemples et compléments. In *Dix Exposés sur la Cohomologie des Schémas*, pages 88–188. North-Holland, Amsterdam; Masson, Paris, 1968.

[12] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.

[13] L.-C. Kappe and B. Warren. An elementary test for the Galois group of a quartic polynomial. *Amer. Math. Monthly*, 96(2):133–137, 1989.

[14] S. Lang. Algebraic groups over finite fields. *Amer. J. Math.*, 78:555–563, 1956.

[15] S. Lang and J. Tate. Principal homogeneous spaces over abelian varieties. *Amer. J. Math.*, 80:659–684, 1958.

[16] F. Lemmermeyer. *Reciprocity laws.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[17] S. Lichtenbaum. Duality theorems for curves over p-adic fields. *Invent. Math.*, 7:120–136, 1969.

[18] C.-E. Lind. Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins. *Thesis, University of Uppsala,*, 1940:97, 1940.

[19] Y. I. Manin. Le groupe de Brauer-Grothendieck en géométrie diophantienne. In *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*, pages 401–411. Gauthier-Villars, Paris, 1971.

[20] J. S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series.* Princeton University Press, Princeton, N.J., 1980.

[21] D. Q. N. Nguyen. Generalized Mordell curves, generalized Fermat curves, and the Hasse principle, 2012. `http://arxiv.org/abs/1212.3400`.

[22] B. Poonen. Heuristics for the Brauer-Manin obstruction for curves. *Experiment. Math.*, 15(4):415–420, 2006.

[23] H. Reichardt. Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen. *J. Reine Angew. Math.*, 184:12–18, 1942.

[24] V. Scharaschkin. The Brauer-Manin obstruction for curves. 1998. Preprint.

[25] J.-P. Serre. Sur les groupes de congruence des variétés Abéliennes. II. *Izv. Akad. Nauk SSSR Ser. Mat.*, 35:731–737, 1971.

[26] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[27] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009.

[28] J. Tate. Duality theorems in Galois cohomology over number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 288–295. Inst. Mittag-Leffler, Djursholm, 1963.

[29] J.-L. Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl. (9)*, 60(4):375–484, 1981.

[30] A. Weil. *Basic number theory.* Springer-Verlag, New York-Berlin, third edition, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.