Bounding the number of rational points on certain curves of high rank

Joseph Loebach Wetherell

Dissertation for Ph.D.
Department of Mathematics
University of California
Berkeley, CA 94720

Currently (July 98) affiliated with
University of Southern California

Permanent Email Address:
`jlwether@alum.mit.edu`

Author address:

DEPARTMENT OF MATHEMATICS, DRB-155, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CA 90089-1113

ABSTRACT. Let K be a number field and let C be a curve of genus $g > 1$ defined over K. In this dissertation we describe techniques for bounding the number of K-rational points on C.

In Chapter I we discuss Chabauty techniques. This is a review and synthesis of previously known material, both published and unpublished. We have tried to eliminate unnecessary restrictions, such as assumptions of good reduction or the existence of a known rational point on the curve. We have also attempted to clearly state the circumstances under which Chabauty techniques can be applied. Our primary goal is to provide a flexible and powerful tool for computing on specific curves.

In Chapter II we develop a technique which, given a K-rational isogeny to the Jacobian of C, produces a positive integer n and a collection of covers of C with the property that the set of K-rational points in the collection is in n-to-1 correspondence with the set of K-rational points on C. If Chabauty is applicable to every curve in the collection, then we can use the covers to bound the number of K-rational points on C.

The examples in Chapters I and II are taken from problem VI.17 in the Arabic text of the *Arithmetica*. Chapter III is devoted to the background calculations for this problem. When we assemble the pieces, we discover that the solution given by Diophantus is the only positive rational solution to this problem.

Contents

1. Preface

This work was motivated by a problem from the *Arithmetica* of Diophantus. In problem 17 of book 6 of the Arabic manuscript, Diophantus poses a problem which comes down to finding positive rational solutions to $y^2 = x^6 + x^2 + 1$. This equation describes a genus 2 curve which we will call C. Diophantus provides the solution $(1/2,\ 9/8)$ and a natural question is whether there are any other positive rational solutions. It clearly will suffice to find all rational points on C. In addition to the solution given by Diophantus and the 3 obvious variations obtained by negating the x and y-coordinates, we have the 4 trivial solutions $(0, 1)$, $(0, -1)$, ∞^+, and ∞^-. Here ∞^+ and ∞^- are the points on the non-singular curve which lie over the point at infinity in the hyperelliptic plane model for C.

There are several reasons why C is intriguing. First, it appears to be the only curve of genus greater than one in the ten known books of the *Arithmetica*. Since the genus is greater than one, we know by Faltings' theorem that C has only finitely many rational points. So it makes sense to ask if Diophantus had found all of the positive rational solutions. In other words, are the 8 solutions we have described the only rational points on C?

Second, while C has many pleasant properties, it is just outside of reach for the usual methods of determining the set of rational points on a genus 2 curve. In particular, C covers two elliptic curves:

$$E_1 : y^2 = x^3 + x + 1,$$
$$E_2 : y^2 = x^3 + x^2 + 1.$$

If either of these elliptic curves had only finitely many rational points, it would be a short calculation to find the set of rational points on C; however, both E_1 and E_2 have rank 1. Along the same lines, if $J = \mathrm{Jac}(C)$ had rank 0, then it would be a finite calculation to determine $C(\mathbb{Q})$. If J had rank 1, then it would be possible to bound the number of points in $C(\mathbb{Q})$ by using Flynn's explicit description of Chabauty calculations on genus 2 curves [**2, 8**]. But J is isogenous to the product $E_1 \times E_2$, so that J has rank 2.

The methods of Chapter II were developed in order to reduce the question of finding the rational points on C to that of finding the rational points on curves to which Chabauty techniques could be applied. This was successful, leading us to the question of determining the set of rational points on two curves of genus 3. One of these curves has rank 0, and is therefore easily handled. The other genus 3 curve has rank 1, so Chabauty techniques are required.

Flynn's method of applying Chabauty is convenient for genus 2 curves, but requires a significant amount of work to generalize. Other authors have not addressed the question of computing bounds for specific curves. In Chapter I we discuss very general techniques for computing bounds on specific curves. An extended example at the end of the chapter determines the set of rational points on our genus 3 curve of rank 1, although certain calculations related to the Mordell-Weil group $J(\mathbb{Q})$ are assumed.

In Chapter III we present the details of the Mordell-Weil calculations. When we integrate the results from all three chapters, we conclude that the solution given by Diophantus is the only positive rational solution to problem VI.17.

We end on a note about the order of the chapters. The goal of Chapter II is to produce curves to which Chabauty can be applied. The goal of Chapter III is to produce information which will be used in Chabauty calculations. It therefore seems prudent to discuss Chabauty techniques first, in Chapter I, as motivation for the other two chapters. Unfortunately, in the context of determining the set of rational points on C, the natural order of the chapters would be II, III, I. We hope that no confusion results.

CHAPTER 1

Chabauty bounds

1. Introduction

Let K be a number field and let C be a complete non-singular curve of genus $g > 1$ defined over K. Let v be a non-archimedean valuation on K. In this chapter we will define a quantity $\mathrm{Chab}(C, K, v)$ which we call the **Chabauty rank** of C over K at v. The Chabauty rank of a curve is a non-negative integer less than or equal to the genus. If we know that the strict inequality $\mathrm{Chab}(C, K, v) < g$ holds, then we can effectively bound the number of K-rational points on C.

The idea of using the above inequality to show the there are only finitely many K-rational points on C dates back to a 1941 paper of Chabauty [**3**], while the details needed for obtaining an effective bound in the case of good reduction were provided by Coleman [**4**] in 1985. McCallum [**14**] and Flynn [**8**] have developed Coleman's techniques for Fermat and genus 2 curves. We will call any technique for computing a bound on $\#C(K)$ using $\mathrm{Chab}(C, K, v) < g$ a Chabauty technique and any bound so obtained a Chabauty bound.

Our emphasis will be on computation, especially on refining the bounds we obtain in specific situations. While the computations we will describe are generally quite straightforward, a certain amount of theory will be required in order to set up our calculations. An overview of the theoretical framework follows.

Let M be a complete non-archimedean field and let J be an abelian variety of dimension g defined over M. Let Tan_J and Cot_J be the tangent and cotangent spaces to J at the identity. The valuation topology on M induces natural M-analytic group structures on the sets $J(M)$, $\mathrm{Tan}_J(M)$, and $\mathrm{Cot}_J(M)$. The logarithm map on $J(M)$ is an analytic homomorphism to $\mathrm{Tan}_J(M)$. More specifically, the logarithm is a local isomorphism and combining it with the duality between Tan_J and Cot_J we obtain a natural analytic pairing

$$\lambda : \ \mathrm{Cot}_J(M) \times J(M) \longrightarrow M$$

which is non-degenerate on the left. For any given cotangent vector ω we define $\lambda_\omega = \lambda(\omega, \cdot)$.

We are interested in the case where M is the completion of K at v and J is the Jacobian of C. In this case $J(K)$ is a finitely generated subgroup of $J(M)$ and we consider the M-linear subspace of $\mathrm{Tan}_J(M)$ spanned by the logarithms of generators of $J(K)$; the dimension of this subspace is defined to be the Chabauty rank $\mathrm{Chab}(C, K, v)$ of C.

The dimension of $\mathrm{Tan}_J(M)$ is g. If $\mathrm{Chab}(C, K, v) < g$ then there exists a non-zero cotangent vector $\omega \in \mathrm{Cot}_J(M)$ such that λ_ω kills $J(K)$. Choosing a K-rational divisor D of positive degree r, we define $\lambda_{\omega,D} : C(M) \to M$ by $\lambda_{\omega,D}(P) = \lambda_\omega([rP - D])$. On the one hand, $\lambda_{\omega,D}(P) = 0$ for every $P \in C(K)$. On the other hand, $C(M)$ is compact and $\lambda_{\omega,D}$ is analytic, so there is a finite covering of $C(M)$ by open balls on which $\lambda_{\omega,D}$ is represented by a converging power series. A standard Newton polygon argument allows us to bound the number of zeros of $\lambda_{\omega,D}$ in each ball, thereby bounding the number of K-rational points on C.

Note that we have not required C to have good reduction at v. While certain difficulties could be avoided by assuming good reduction, we prefer to leave this possibility open. For example, in some cases it may be worth the added effort in order to take advantage of a small residue field.

Note also that we have not required the K-rational divisor D used in defining $\lambda_{\omega,D}$ to be effective of degree 1. Because of this, we are able to work with curves on which we do not know any K-rational points. We will show that every K-rational divisor of positive degree leads to the same bound, so we can let D be any divisor which is convenient. This generalizes Flynn's use of the map $P \mapsto [2P - \infty^+ - \infty^-]$ when doing similar calculation on genus 2 curves.

We end this introduction with a caveat. Chabauty techniques tend to hide a difficult and currently ineffective calculation in the assumption that $\mathrm{Chab}(C, K, v)$ is less than g. This assumption is often verified in the literature by calculating the free rank of $J(K)$, since the Chabauty rank of C is at most the free rank of J. One exception is McCallum's work on Fermat curves [**14**], in which he discusses a technique for directly bounding the Chabauty rank. In any case, it is appropriate to keep this computationally difficult prerequisite in mind when evaluating the difficulty of calculating or refining a Chabauty bound.

2. Notation

Throughout this chapter, K will be a number field with non-archimedean valuation v of residue characteristic p. We assume that v is normalized so that $v(p) = 1$. Let $|x| = p^{-v(x)}$ be the absolute value on K corresponding to the valuation v. We let $M = K_v$ be the completion of K at v and let $R = \{x \in M : v(x) \geq 0\}$ be the ring of integers in M. R is a complete DVR with maximal ideal $\mathfrak{m}$ and residue field k. We recall that if e and f are the absolute ramification index and residue field degree of $M/\mathbb{Q}_p$, then $[k : \mathbb{F}_p] = f$, $\mathfrak{m}^e = pR$, and $[M : \mathbb{Q}_p] = ef$. Note that $\mathfrak{m}$ is principal and that if π is a uniformizing parameter, then $v(\pi) = 1/e$. Finally, we assume that all algebraic extensions of M are subextensions of a fixed algebraic closure $\overline{M}$.

Let X be a non-singular algebraic variety of dimension n defined over M. The set of M-valued points $X(M)$ has a natural M-analytic manifold structure. Note that if X is complete, then $X(M)$ is compact under this topology. If $x \in X(M)$, let $\mathcal{O}_x$ be the ring of germs of algebraic functions at x and let $\mathfrak{m}_x$ be its maximal ideal. We similarly define $\mathcal{O}_x^{\mathrm{an}}$ and $\mathfrak{m}_x^{\mathrm{an}}$ to be the ring of germs of analytic functions at x and its maximal ideal. If $z_1, \ldots, z_n$ form a basis for $\mathfrak{m}_x/\mathfrak{m}_x^2$, then they also form a basis for $\mathfrak{m}_x^{\mathrm{an}}/(\mathfrak{m}_x^{\mathrm{an}})^2$ and the function $(z_1, \ldots, z_n) : X \to M^n$ is a local analytic isomorphism. We call $z_1, \ldots, z_n$ a **local coordinate system** for X at x. We note that there is a natural inclusion of local rings $\mathcal{O}_x \subset \mathcal{O}_x^{\mathrm{an}}$ and the adic completion of either is the completed local ring $\widehat{\mathcal{O}}_x \cong M[[z_1, \ldots, z_n]]$. An **open ball** about x on the manifold $X(M)$ is an open neighborhood B of x which is analytically isomorphic, via a local coordinate system at x, to an open polydisk on M^n about 0 We will be more specific about choosing specific balls and local coordinate systems when we introduce the arithmetic notions of models and residue classes in section 7.

3. Logarithms and Integrals on J

Let A be an abelian variety of dimension g defined over M. We begin this section by reviewing the connection between cotangent vectors and global differential 1-forms on A.

LEMMA 3.1. *The map which sends every global 1-form to its section at 0 induces a natural isomorphism* $\Gamma(A, \Omega^1_{A/M}) \cong \mathrm{Cot}_A(M)$.

PROOF. For any $a \in A$, the translation-by-a map t_a induces a natural isomorphism between the cotangent spaces at a and 0. This isomorphism yields a global trivialization of the cotangent bundle. Thus, we can consider any global differential 1-form to be a map from A to Cot_A. Since A is complete and Cot_A is affine, any such map must be constant; that is, every global differential 1-form must be translation invariant. The converse is trivial. $\square$

We next define the logarithm map and the pairing λ mentioned in the introduction. This is a summary of material from [**4**], [**10**], [**19**], and [**20**].

LEMMA 3.2. *Let $\omega \in \Gamma(A, \Omega^1_{A/M})$ be a global 1-form. There is a unique analytic homomorphism $\lambda_\omega : A(M) \to M$ such that $d(\lambda_\omega) = \omega$.*

PROOF. By the proof of lemma 3.1 we see that $d\omega = 0$, so we can express ω as the derivative of a convergent power series at 0. In particular, let $z_1, \dots, z_g$ be a local coordinate system for A at 0 and let $\lambda_\omega \in M[[z_1, \dots, z_g]]$ to be the unique power series such that $\lambda_\omega(0) = 0$ and $d(\lambda_\omega) = \omega$ on some open ball B about 0. There is a basis for the topology of $A(M)$ consisting of open subgroups, so we can also assume that B is a subgroup of $A(M)$.

Since λ_ω was obtained by formal integration of a converging power series, λ_ω satisfies the formal properties of an integral on B. This justifies writing $\int_a^b \omega = \lambda_\omega(b) - \lambda_\omega(a)$ for $a, b \in B$. Since ω is translation invariant, have the identity

$$\int_0^{a+b} \omega \quad = \quad \int_0^a \omega + \int_a^{a+b} \omega \quad = \quad \int_0^a \omega + \int_0^b t_a^* \omega \quad = \quad \int_0^a \omega + \int_0^b \omega$$

In other words, λ_ω defines a homomorphism from B to M. Since $A(M)$ is compact, B is a subgroup of finite index; we can extend λ_ω to a homomorphism on $A(M)$ by the rule $\lambda_\omega(a) = \lambda_\omega(na)/n$ where $n = [A(M) : B]$. □

It is clear that the map $\omega \mapsto \lambda_\omega$ is M-linear and injective. From this we obtain a pairing

$$\lambda : \Gamma(A, \Omega^1_{A/M}) \times A(M) \longrightarrow M$$

which is non-degenerate on the left. We use the duality between tangent and cotangent spaces and the natural isomorphism between the cotangent space and the space of global 1-forms to define the logarithm map $\log : A(M) \longrightarrow \mathrm{Tan}_A(M)$ by

$$\log(x) = (\omega \longmapsto \lambda_\omega(x)).$$

The logarithm is a local isomorphism; since $A(M)$ is compact, it follows that the kernel of the logarithm is finite. Moreover, $\mathrm{Tan}_A(M)$ is torsion free, so the kernel of the logarithm is exactly the set of torsion points on $A(M)$. In other words,

$$0 \longrightarrow A(M)_{\mathrm{tors}} \longrightarrow A(M) \xrightarrow{\log} \mathrm{Tan}_A(M)$$

is exact and

$$\log : A(M) \otimes \mathbb{Q} \xrightarrow{\sim} \mathrm{Tan}_A(M)$$

is an isomorphism.

REMARK 3.3. In general, the concept of integration on a variety defined over M is complicated by the fact that anti-derivatives are only well defined up to locally-constant functions. We have avoided this problem (for global 1-forms on abelian varieties) by requiring the indefinite integral to be a homomorphism. In the notation of this section, the integral

$$\int_a^b \omega = \lambda_\omega(b) - \lambda_\omega(a)$$

is uniquely determined and is functorial with respect to maps between abelian varieties, since any such map is the translation of a homomorphism.

We can similarly define integration and the logarithm map on A for any finite field extension N of M. It is easy to see that these integrals satisfy all of the usual formal properties: they are linear in the integrand, switch signs when the limits are switched, etc. Furthermore, the integrals and logarithm map are independent of any choices made in the above construction and respect the action of $\mathrm{Gal}(\overline{M}/M)$.

4. Integrals on C

It is quite easy to determine whether $C(M)$ is empty. If it is empty, we have a trivial bound on $C(K)$, so we assume that $C(M)$ is not empty. Let $P \in C(M)$ be an M-rational point on C and define $f_P : C \longrightarrow J$ by $Q \mapsto [Q-P]$. Let D be an M-rational divisor of degree r on C and define $f_D : C \longrightarrow J$ by $Q \mapsto [rQ - D]$. Let $\omega \in \Gamma(J, \Omega^1_{J/M})$ be a global 1-form on J and note that both $f_P^*\omega$ and $f_D^*\omega$ are global 1-forms on C.

Lemma 4.1. *$f_D^*\omega = r \cdot f_P^*\omega$.*

Proof. Note that f_D is equal to the composition

$$C \xrightarrow{f_P} J \xrightarrow{[r]} J \xrightarrow{t_{[rP-D]}} J.$$

But ω is translation invariant and $[r]^*\omega = r\omega$; the statement follows. □

Lemma 4.2. *The map $f^* = f_P^* : \Gamma(J, \Omega^1_{J/M}) \longrightarrow \Gamma(C, \Omega^1_{C/M})$ is a natural isomorphism and is independent of P.*

Proof. From [**16**] we know that $f_P^* : \Gamma(J, \Omega^1_{J/\overline{M}}) \longrightarrow \Gamma(C, \Omega^1_{C/\overline{M}})$ is an isomorphism over the algebraic closure. By the previous lemma we see that this isomorphism does not depend on the choice of P, and it is clearly defined over M. □

Let $\eta \in \Gamma(C, \Omega^1_{C/M})$ be a global 1-form on C and let $\omega = f^{*-1}\eta$ be the corresponding 1-form on J. For any M-rational divisor D of degree r, define

$$\lambda_{\eta,D}(Q) = \lambda_\omega([rQ - D]).$$

Note that $\lambda_{\eta,D} = \lambda_\omega \circ f_D$; abusing notation we define $\lambda_{\omega,D} = \lambda_{\eta,D}$. We see that $\lambda_{\eta,D}$ is an analytic function on C whose differential is $r\eta$. Indeed, fix $Q_0 \in C(M)$ and let u be a local coordinate function on a ball B about Q_0. Since η is global, we can express η as $F(u)du$, where $F(u) \in M[[u]]$ converges on B. The formal integral G of $rF(u)$ is also a converging power series on B and is equal to the function $\lambda_{\eta,D}$ up to an additive constant. Note that if $D = P$ is effective of degree 1 and if P is in the ball B, then this constant of integration is $-G(P)$, since $\lambda_{\eta,P}(P) = 0$. The question of calculating the constant of integration for other balls will be considered in section 8.

Remark 4.3. We can define integration on C of global 1-forms by

$$\int_P^Q \eta = \lambda_{\eta,P}(Q); \quad \text{in other words,} \quad \int_P^Q \eta = \int_0^{[Q-P]} f^{*-1}\eta.$$

In [**5**], Coleman gives a canonical definition of integration on affinoids of good reduction using rigid analysis and Dwork's principle of analytic continuation along Frobenius. The crux of Coleman's definition is to show that there is a canonical choice for the constant of integration on any ball. Our definitions of integration on algebraic curves and abelian varieties agrees with Coleman's when both are applicable; however, even in the case of good reduction the logarithmic approach seems to be computational simpler. Coleman's integrals satisfy all of the usual formal properties of integrals, are functorial with respect to maps between varieties, and respect the action of $\mathrm{Gal}(\overline{M}/M)$.

Remark 4.4. Note that we can calculate integrals on J in terms of integrals on C. Extending the base field if necessary, we can write any degree 0 divisor class $a \in J(M)$ as $a = [\sum Q_i - \sum P_i]$, where repeats are allowed. We then have

$$\int_0^a \omega = \sum \int_{P_i}^{Q_i} f^*\omega.$$

The interplay between integrals on C and integrals on J is a useful tool when performing explicit Chabauty calculations.

5. Chabauty rank

Let A be an abelian variety defined over K. Consider the image $\log(A(K))$ of $A(K)$ under the logarithm. Let W be the M-linear subspace of $\mathrm{Tan}_A(M)$ spanned by elements of $\log(A(K))$. We define the Chabauty rank of A over K at v to be the dimension of W as a vector space over M:

$$\mathrm{Chab}(A, K, v) = \dim_M(W).$$

LEMMA 5.1.
(i) $0 \leq \mathrm{Chab}(A, K, v) \leq \dim A$.
(ii) $\mathrm{Chab}(A, K, v) \leq \mathrm{rank}(A(K))$.
(iii) $\mathrm{Chab}(A, K, v) = 0$ *if and only if* $\mathrm{rank}(A(K)) = 0$.
(iv) *If A is K-isogenous to a product* $\prod A_i$ *then* $\mathrm{Chab}(A, K, v) = \sum \mathrm{Chab}(A_i, K, v)$.

PROOF. These statements are obvious from the definitions. □

For convenience, we define the Chabauty rank of a curve to be the Chabauty rank of its Jacobian, so that $\mathrm{Chab}(C, K, v) = \mathrm{Chab}(J, K, v)$.

Let $V = \mathrm{Ann}(J(K))$ be the annihilator of $J(K)$ under the pairing λ. In other words,

$$V = \{\omega \in \Gamma(J, \Omega^1_{J/M}) : \lambda_\omega(a) = 0 \text{ for all } a \in J(K)\}.$$

Note that $\dim_M(W) + \dim_M(V) = g$; thus, V is non-trivial if and only if $\mathrm{Chab}(C, K, v) < g$. From this point forward we will assume that $V = \mathrm{Ann}(J(K))$ is non-trivial.

REMARK 5.2. The easiest way to show that V is non-trivial is for the rank of $J(K)$ to be less than g. Another relatively simple possibility is for some K-rational factor of J to have K-rank less than its dimension; this will be important in Chapter II when considering covering collections.

6. Common zeros

Recall that we want to bound the number of K-rational points on C. Let D be an M-rational divisor of positive degree r whose divisor class $[D]$ is K-rational. (In the introduction we assumed that D was K-rational; here we are slightly more general.) Since we have assumed that $C(M)$ is not empty, any K-rational divisor class will contain an M-rational divisor. Define

$$Z = \{P \in C(M) : \lambda_{\omega,D}(P) = 0 \text{ for all } \omega \in V\}.$$

Since f_D is K-rational and $\lambda_{\omega,D} = \lambda_\omega \circ f_D$, we see that $C(K) \subseteq Z$. Suppose D' is another M-rational divisor of positive degree whose divisor class is K-rational, and let r' be the degree of D'. We find that for any $P \in C(M)$,

$$r'\lambda_{\omega,D}(P) = r\lambda_{\omega,D'}(P) + \lambda_\omega([rD' - r'D]).$$

If $\omega \in V$ then $\lambda_\omega([rD' - r'D]) = 0$, in which case $\lambda_{\omega,D}(P) = 0$ if and only if $\lambda_{\omega,D'}(P) = 0$. It follows that the set Z does not depend on the choice of D. Note that, in addition to $C(K)$, Z contains any point $P \in C(M)$ which differs from a K-rational degree 1 divisor class by a torsion element in $J(M)$. This is not a complete list of points in Z, but it is the easiest subset to describe.

As we shall see, if $\mathrm{Chab}(C, K, v) < g$, then Z is finite and its size can be effectively bounded. If, in addition, we know a basis for the vector space V, then this bound takes the form of a set of congruences which exhaust the possibilities for points in Z. In order to make this explicit we will need to have better control over the power series which locally represent $\lambda_{\omega,D}$ and the balls on which these power series converge.

7. Models and residue classes

In this section we introduce some arithmetic theory with the goal of explicitly describing a set of balls on which our power series converge.

Let X be a non-singular algebraic variety of dimension n defined over M. Suppose that $\mathcal{X}$ is a model for X over R; that is, $\mathcal{X}$ is a reduced, irreducible scheme over R whose generic fiber is X. Let $\overline{\mathcal{X}}$ be the special fiber of $\mathcal{X}$. We will call the natural map from $\mathcal{X}(R)$ to $\mathcal{X}(k) = \overline{\mathcal{X}}(k)$ the **reduction map**. As usual, we define a **residue class** to be a fiber of the reduction map.

We make two assumptions about $\mathcal{X}$:

(i) the natural map $\mathcal{X}(R) \to X(M)$ is bijective, and

(ii) every $x \in \mathcal{X}(R)$ reduces to a non-singular point $\overline{x} \in \overline{\mathcal{X}}(k)$.

The first assumption allows us to transport the notions of reduction and residue class to $X(M)$. The second assumption says that at every $x \in X(M)$ there is a system $z_1, \dots, z_n$ of local coordinates which reduces to a basis for $\mathfrak{m}_{\overline{x}}/\mathfrak{m}_{\overline{x}}^2$. (In other words, $z_1, \dots, z_n$ is a basis for $\mathfrak{m}_{\mathcal{X},x}/\mathfrak{m}_{\mathcal{X},x}^2$). This system of local coordinates gives an analytic isomorphism of the residue class of x with the open polydisk of radius 1 in M^n; in this case we will call $z_1, \dots, z_n$ a system of local coordinates on the residue class at x. We also note that if $g \in \mathcal{O}_x$ reduces to an element of $\mathcal{O}_{\overline{x}}$ (equivalently, $g \in \mathcal{O}_{\mathcal{X},x}$), then g is represented by a power series in $R[[z_1, \dots, z_n]]$. Under these two assumptions we can identify the residue classes of $X(M)$ with the non-singular points of $\overline{\mathcal{X}}(k)$. Residue classes will be the most important examples of open balls on $X(M)$ whenever $\mathcal{X}$ satisfies both of these assumptions.

We are particularly interested in the curve C and its Jacobian J. Let $\mathcal{C}$ be a minimal regular proper model for C over R and let $\overline{\mathcal{C}}$ be its special fiber. (See, for example, Chapter IV in [**22**].) Since $\mathcal{C}$ is proper over R, $\mathcal{C}(R) = C(M)$; since $\mathcal{C}$ is regular over R, every M-rational point in $C(M)$ reduces to a non-singular point on $\overline{\mathcal{C}}$ [**22**, Cor IV.4.4]. Thus, both assumptions hold for $\mathcal{C}$.

Let $\mathcal{J}$ be the Néron model for J over R and let $\overline{\mathcal{J}}$ be its special fiber. (For a discussion of Néron models, see [**1**].) We note that the connected components of $\mathrm{Pic}^0(\mathcal{C}/R)$ and $\mathcal{J}$ are canonically isomorphic [**1**, Prop 1.20]. The Néron property tells us that $\mathcal{J}(R) = J(M)$. By definition, $\mathcal{J}$ is smooth over R, so every point on $\overline{\mathcal{J}}(k)$ is non-singular. This verifies both assumptions for $\mathcal{J}$. The reduction map is a homomorphism of abstract groups $J(M) \to \overline{\mathcal{J}}(k)$ and the residue class of the identity is called the kernel of reduction, denoted by $J_1(M)$. Note that $J_1(M)$ is an open subgroup of $J(M)$.

By a lattice in a vector space V over M we mean a free R-submodule of rank equal to the dimension of V which generates V over M. The R-modules $\mathrm{Tan}_{\mathcal{J}}(R)$, $\mathrm{Cot}_{\mathcal{J}}(R)$, $\Gamma(\mathcal{J}, \Omega^1_{\mathcal{J}/R})$, and $\Gamma(\mathcal{C}, \Omega^1_{\mathcal{C}/R})$ form natural lattices for the vector spaces $\mathrm{Tan}_J(M)$, $\mathrm{Cot}_J(M)$, $\Gamma(J, \Omega^1_{J/M})$, and $\Gamma(C, \Omega^1_{C/M})$ over M. These lattices are compatible with the natural maps discussed in the preceding sections.

PROPOSITION 7.1.

(i) *The map which sends each global 1-form to its section at 0 induces a natural isomorphism*

$$\Gamma(\mathcal{J}, \Omega^1_{\mathcal{J}/R}) \cong \mathrm{Cot}_{\mathcal{J}}(R).$$

(ii) f^* *induces a natural isomorphism*

$$\Gamma(\mathcal{J}, \Omega^1_{\mathcal{J}/R}) \cong \Gamma(\mathcal{C}, \Omega^1_{\mathcal{C}/R}).$$

(iii) *Let* $\overline{\mathcal{J}}^0$ *be the connected component of* $\overline{\mathcal{J}}$. *Restriction to* $\overline{\mathcal{J}}^0$ *induces an isomorphism*

$$\Gamma(\mathcal{J}, \Omega^1_{\mathcal{J}/R})/\mathfrak{m}\Gamma(\mathcal{J}, \Omega^1_{\mathcal{J}/R}) \xrightarrow{\ \sim\ } \Gamma(\overline{\mathcal{J}}^0, \Omega^1_{\overline{\mathcal{J}}^0/R}).$$

(iv) *Restriction to $\overline{\mathcal{C}}$ induces an isomorphism*

$$\Gamma(\mathcal{C}, \Omega^1_{\mathcal{C}/R})/\mathfrak{m}\Gamma(\mathcal{C}, \Omega^1_{\mathcal{C}/R}) \xrightarrow{\sim} \Gamma(\overline{\mathcal{C}}, \Omega^1_{\overline{\mathcal{C}}/R}).$$

PROOF. We refer the reader to section 2.1 of [**14**] for a discussion of these lattices and isomorphisms. □

We note that all of the open balls encountered thus far in our discussion can be assumed to be residue classes.

LEMMA 7.2. *At each point $a \in J(M)$ ($P \in C(M)$) there is a power series which converges on the residue class of a (of P) and is equal to λ_ω (to $\lambda_{\omega,D}$) as a function on that residue class.*

PROOF. We start by considering λ_ω at 0. Let $\omega \in \Gamma(J, \Omega^1_{J/M})$ and let $z_1, \dots, z_g$ be a local coordinate system for $J_1(M)$ at 0. We can multiply ω by a non-zero constant without affect convergence of ω or λ_ω, so we may assume that $\omega \in \Gamma(\mathcal{J}, \Omega^1_{\mathcal{J}/R})$. Thus, we can write ω at 0 as $\sum F_i dz_i$, where $F_i \in R[[z_1, \dots, z_g]]$. Let $G \in M[[z_1, \dots, z_g]]$ be the formal integral of $\sum F_i dz_i$. Since each coefficient of dG is in R, we see that the denominator of the coefficient of $z_1^{a_i} \dots z_g^{a_g}$ in G is bounded by the greatest common divisor of the integers $a_i, \dots, a_g$. In particular, G converges on $J_1(M)$. But G is equal to λ_ω as a function on $J_1(M)$, so our result is proven in this case. Since the above objects can be translated to any point of $J(M)$, we see that λ_ω can be represented by a converging power series on every residue class of $J(M)$.

A similar argument shows that for any M-rational divisor D, the function $\lambda_{\omega,D}$ on $C(M)$ can be represented by a converging power series on each residue class of $C(M)$. □

We end this section with some useful information regarding the kernel of reduction. Let $z_1, \dots, z_g$ be a local coordinate system for $J_1(M)$ at 0. This local coordinate system identifies $J_1(M)$ with the set $\mathfrak{m} \times \cdots \times \mathfrak{m}$. Define $J_n(M)$ to be the subgroup corresponding to $\mathfrak{m}^n \times \ldots \times \mathfrak{m}^n$; note that this subgroup is independent of the choice of local coordinates.

PROPOSITION 7.3.

(i) *If $v(\mathfrak{m}^n) > 1/(p-1)$, then the logarithm map induces an isomorphism*

$$\log : J_n(M) \xrightarrow{\sim} \mathfrak{m}^n \operatorname{Tan}_J(R)$$

(ii) *If $n \le m \le 2n$ then taking local coordinates induces an isomorphism of additive groups*

$$(z_1, \dots, z_g) : J_n(M)/J_m(M) \xrightarrow{\sim} (\mathfrak{m}^n/\mathfrak{m}^m)^g.$$

PROOF. This follows from [**14**, Lem 2.3.1] and [**19**, Thm IV.9.2]. □

Among other things, the first item in the above proposition tells us that if the ramification degree e of $M/\mathbb{Q}_p$ is less that $p-1$ then there is no torsion in the kernel of reduction. In other words, if $e < p-1$, then the reduction map restricted to torsion points is injective.

8. Bounding the number of zeros

Let D be an M-rational divisor of positive degree r whose divisor class $[D]$ is K-rational and let $\eta \in \frac{1}{r}\Gamma(\mathcal{C}, \Omega^1_{\mathcal{C}/R})$ be a differential on C such that $r\eta$ is integral. Fix a point $Q \in C(M)$ and let u be a local coordinate on the residue class at Q. Our goal in this section is to bound the number of zeros of $\lambda_{\eta,D}$ on the residue class of Q.

As we have indicated in the previous section, $r\eta$ can be expanded in the residue class of Q as

$$r\eta = \sum_{i=0}^{\infty} c_i u^i du$$

where each $c_i \in R$. Let π be a generator for $\mathfrak{m}$. Since $\lambda_{\eta,D}$ is obtained by integrating $r\eta$, we find that

$$\begin{aligned}\lambda_{\eta,D} &= b_0 + \sum_{i=0}^{\infty} \frac{c_i}{i+1} u^{i+1} \\ &= b_0 + \sum_{i=0}^{\infty} \frac{c_i \pi^{i+1}}{i+1} \left(\frac{u}{\pi}\right)^{i+1} \\ &= \sum_{i=0}^{\infty} b_i X^i\end{aligned}$$

where $b_0 = \lambda_{\eta,D}(Q)$ is the constant of integration at Q, $X = u/\pi$, and $b_i = c_{i-1}\pi^i/i$ for $i \geq 1$. Since we are restricting our attention to the residue class of Q, we see that u takes values in $\mathfrak{m}$ and X takes values in R. Using the theory of Newton polygons we obtain the following estimate on the number of possible zeros to such a series.

THEOREM 8.1 (Strassman). *Let $F(X) = b_0 + b_1 X + \cdots \in M[[X]]$ satisfy $b_n \to 0$ in M. Define m uniquely by $|b_m| \geq |b_i|$ $\forall i \geq 0$ and $|b_m| > |b_i|$ $\forall i > m$. Then $F(X)$ has at most m zeros in R.* □

Let $F(X) = \sum_{i=0}^{\infty} b_i X^i$ be the power series for $\lambda_{\eta,D}$ in terms of X calculated above and let $F_1(X) = F(X) - b_0 = \sum_{i=1}^{\infty} b_i X^i$ be the power series obtained by omitting the constant term. Let e be the ramification degree of the extension $M/\mathbb{Q}_p$. Note that $|1/i| \leq \log_p i$ and $|\pi^i| = p^{-i/e}$. Thus $|b_i| \leq p^{-i/e} \log_p i$, which gives us an upper bound on the size of each coefficient. Given the size of the any non-zero term b_k we can easily determine N such that $|b_n| < |b_k|$ for all $n > N$. Then the Strassman bound is at most N. It is a finite amount of work to calculate the Strassman bound in any given situation.

The Strassman bound will be our basic tool for bounding the number of zeros of $\lambda_{\eta,D}$ on the residue class of Q. We next consider some refinements and simplifications of this bound.

Approximate zeros. If we know η then formal integration gives us every coefficient of $F(X)$ except the constant of integration $b_0 = \lambda_{\eta,D}(Q)$. Suppose that we know b_0 to some given accuracy. Multiplying $F(X)$ by a constant, if necessary, we may assume that $F(X) \in R[[X]]$ and that $F(x) \notin \mathfrak{m}[[X]]$. Suppose that after this rescaling we know every coefficient of $F(X)$ modulo π^n. Then we can calculate all possible values of R/π^n which satisfy $F(X)$; call this our set of approximate zeros. The number of these solutions (counting multiplicities) is a refinement on the Strassman bound. If $\dim_M(V) > 1$ then we further refine our bound on the number of elements of Z which lie in this residue class by only accepting approximate zeros which are common to every $\eta \in V$. The values of the approximate zeros may also help in searching for new K-rational points on C.

Ignoring the constant of integration. Let m and m' be the Strassman bounds for $F(X)$ and $F_1(X)$, respectively. Note that $m' \geq 1$ and either $m = m'$ or $m = 0$. In either case, m' gives an upper bound for the number of zeros of $F(X)$ in R. Since m' ignores the constant of integration, it can be computed directly from η. When using a bound which ignores the constant of integration, keep in mind that the bound is always at least 1, so it cannot be used to rule out a residue class. Also, since we do not have approximate zeros, when estimating the number of elements of Z which lie in this residue class we must use the minimum of the bounds coming from some $\eta \in V$.

Reduction info only. Recall that Q reduces to a non-singular point $\overline{Q}$ of $\overline{\mathcal{C}}$. Let $\overline{r\eta}$ be the reduction of $r\eta$. Note that if $e < p-1$ and $\overline{r\eta}$ has order zero at $\overline{Q}$ (i.e.: $|c_0| = 1$), then $|b_1| = p^{-1/e}$ and $|b_i| \leq p^{-2/e}$ for $i \geq 2$; in other words, $\lambda_{\omega,D}$ has at most one zero in this residue class. More generally, assume that $\mathrm{ord}_{\overline{Q}}(\overline{r\eta}) = k-1$ and let $n(\overline{r\eta}, \overline{Q}) = \max\{n : |\pi|^n/|n| \geq |\pi|^k/|k|\}$. Looking at the Strassman bound we see that $\lambda_{\eta,D}$ has at most $n(\overline{r\eta}, \overline{Q})$ zeros in the residue class of Q. (See [**4**].) Note that the order of $\overline{r\eta}$ at $\overline{Q}$ is at most $2g-2$, so $n(\overline{r\eta}, \overline{Q})$ can be bounded strictly in terms of e and g. While $n(\overline{r\eta}, \overline{Q})$ may not give as sharp a bound as the Strassman estimate, it is generally much easier to determine. Since we have not used the constant of integration, the limitations discussed in the previous paragraph apply to this estimate also.

Effective Chabauty. The sum $N(\overline{r\eta}) = \sum n(\overline{r\eta}, \overline{P})$ over the residue classes $\overline{P}$ of $C(M)$ gives an upper bound on the number of zeros of $\lambda_{\eta,D}$ on $C(M)$. Note that $N(\overline{r\eta})$ depends only on the divisor $(\overline{r\eta})$. In fact, it only depends on that part of the divisor which is supported on non-singular k-rational points of $\overline{\mathcal{C}}$; call this restricted divisor $(\overline{r\eta})'$. There are only finitely many divisors on $\overline{\mathcal{C}}$ which are of the form $(\overline{\alpha})'$ for some differential $\overline{\alpha} \in \Gamma(\mathcal{C}, \Omega^1_{\mathcal{C}/R})$. Taking the maximum of the $N(\overline{\alpha})$ gives an estimate for the maximum number of zeros on $C(M)$ of any α. This is the approach taken in [**4**]. This bound depends only on knowing that $\mathrm{Chab}(C, K, v)$ is less than g; in particular, it does not require that we know any $\eta \in V$ nor any generators for $J(K)$.

Explicit Chabauty. Here we go to the other extreme. Suppose that we know generators for a subgroup G of finite index in $J(K)$. The M-linear spaces spanned by $\log(G)$ and $\log(J(K))$ are identical, so we will often be able to determine generators for $V = \mathrm{Ann}(J(K))$. (As a practical matter, we will only calculate $\log(G)$ to finite accuracy. If the space spanned by $\log(G)$ appears to have lower dimension than expected, it may be difficult to determine V.)

Let $\overline{G}$ and $\overline{J(K)}$ be images of G and $J(K)$ under the reduction map. If the index of G in $J(K)$ is coprime to the order of $\overline{\mathcal{J}}(k)$, then $\overline{G} = \overline{J(K)}$. Let $P \in C(M)$ and let $\overline{P} \in \overline{\mathcal{C}}(k)$ be its reduction. If $P \in C(K)$ then clearly $[r\overline{P} - \overline{D}] \in \overline{J(K)}$; conversely, if $[r\overline{P} - \overline{D}] \notin \overline{J(K)}$ then there is no K-rational point in the residue class of P. This is a very effective way to rule out entire residue classes; in fact, this is one way to eliminate points of Z which are not in $C(K)$. As an added benefit, if the residue class of $Q \in C(M)$ is not ruled out then we know that the residue class of $[rQ - D]$ contains a K-rational divisor class; knowledge of this K-rational divisor class can be used to calculate the constant of integration at Q.

Calculating the constant of integration. In theory, it is always possible to calculate $b_0 = \lambda_\omega([rQ-D])$ by the method discussed in sections 3 and 7: find an integer n such that $n[rQ-D]$ is in the kernel of reduction, expand λ_ω as a power series at 0, and evaluate $b_0 = \lambda_\omega(n[rQ-D])/n$. Unfortunately, calculating $n[rQ-D]$ can be difficult if n is large. Fortunately, we can sometimes find a shortcut for calculating b_0. We will assume $\omega \in V$.

Recall that $F_1(X)$ is the formal integral of $r\eta = f_D^*\omega$ on the residue class at Q. If we know a K-rational point P in the residue class of Q, then $b_0 = -F_1(P)$. Alternatively, set $Q = P$ so that $b_0 = 0$.

If we know a K-rational divisor class a in the residue class of $[rQ-D]$, then we can make use of the fact that $\lambda_\omega(a) = 0$. Note that to be useful, we will want degree 0 divisors D_1 and D_2 representing the divisor classes $[rQ-D]$ and a such that D_1 and D_2 reduce to the same divisor over k. If we have D_1 and D_2, then $b_0 = \lambda_\omega([rQ-D]) = \lambda_\omega([D_1 - D_2])$ can be evaluated as a sum of integrals on C, where the limits of each integral are in the same residue class.

If we know an M-rational torsion point a in the residue class of $[rQ-D]$, then we proceed as in the previous paragraph. Note that if the order n of $[rQ-D]$ in $\overline{\mathcal{J}}$ is coprime to p, then we know that the residue class contains an M-rational n-torsion point. In fact, if we know a function $\overline{f}$ on $\overline{\mathcal{C}}$ whose divisor is $n(r\overline{Q} - \overline{D})$, then we can use Hensel's lemma to calculate (to any given accuracy) a divisor in the divisor class of a whose reduction is $r\overline{Q} - \overline{D}$.

9. Example

Let C be the non-singular curve over $\mathbb{Q}$ which is birational to the plane curve

$$\begin{aligned} y^2 = f(x) &= (x^4 - 2x^2 - 8x + 1)(x^3 + x + 1) \\ &= x^7 - x^5 - 7x^4 - x^3 - 10x^2 - 7x + 1. \end{aligned}$$

Note that C is a genus 3 hyperelliptic curve. Let $\rho : C \longrightarrow C$ be the hyperelliptic involution. Since $f(x)$ has odd degree, we see that C has a single point at infinity, which we call ∞. Note that ∞, $(0,1)$, and $(0,-1)$ are rational points on C; we would like to show that these 3 points are the only rational points on C.

The primes of bad reduction of C are 2 and 31. We choose to work with the prime $p = 3$ of good reduction. In the terminology of this chapter we let $K = \mathbb{Q}$, $M = \mathbb{Q}_3$, $R = \mathbb{Z}_3$, etc. Let $\mathcal{C}$ be the minimal regular proper model for C over $\mathbb{Z}_3$ given by $y^2 = f(x)$ on the affine plane. Let J be the Jacobian of C and let $\mathcal{J}$ be the Néron model of J. We note that $\mathcal{J} = \mathrm{Pic}^0(\mathcal{C}/R)$.

There are 6 residue classes on $C(\mathbb{Q}_3)$, corresponding to the 6 points $\overline{\infty}$, $\overline{(0,1)}$, $\overline{(0,2)}$, $\overline{(1,0)}$, $\overline{(2,1)}$, and $\overline{(2,2)}$ in $C(\mathbb{F}_3)$.

Let D_3 be the effective $\mathbb{Q}$-rational degree 3 divisor on C which is supported on points whose x-coordinates satisfy $x^3 + x + 1 = 0$ and whose y-coordinates are zero. Let $\overline{D_2}$ be the effective $\mathbb{F}_3$-rational degree 2 divisor on $\overline{\mathcal{C}}$ which is supported on points whose x-coordinates satisfy $x^2+x+2 = 0$ and whose y-coordinates are zero. Note that the reduction of D_3 is $\overline{D_2} + \overline{(1,0)}$.

As we will show in a chapter III, $J(\mathbb{Q}) \approx \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The divisor class $T = [D_3 - 3\infty]$ is the non-trivial 2-torsion point in $J(\mathbb{Q})$. The divisor class $U = [\infty - (0,1)] \in J(\mathbb{Q})$ has infinite order. Let $\overline{T}$ and $\overline{U}$ be the reductions of T and U at 3. The group $\overline{\mathcal{J}}(\mathbb{F}_3)$ has order 48 while $\overline{T}$ has order 2 and $\overline{U}$ has order 12. Let $G = \langle T, U\rangle$ be the subgroup of $J(\mathbb{Q})$ generated by T and U. We will show that U is neither a double nor a triple in $J(\mathbb{Q})$, so the index of G in $J(\mathbb{Q})$ is coprime to 48. Thus, $\overline{G} = \overline{J(\mathbb{Q})} \subsetneqq \overline{\mathcal{J}}(\mathbb{F}_3)$.

The power series. Note that x is a local coordinate on the residue class at $(0,1)$. A basis for the global differentials on C is given by $\eta_0 = (1/y)dx$, $\eta_1 = (x/y)dx$, and $\eta_2 = (x^2/y)dx$. Expanding $1/y$ in terms of x we get

$$\frac{1}{y} = \frac{1}{\sqrt{f(x)}} = 1 + \frac{7}{2}x + \frac{187}{8}x^2 + \frac{2563}{16}x^3 + \frac{148755}{128}x^4 + \frac{2210457}{256}x^5 + \frac{66888879}{1024}x^6 + \cdots$$

in the residue class of $(0,1)$; from this we easily calculate power series expansions for the η_i. Elementary information regarding roots of power series shows that $1/y \in \mathbb{Z}_3[[x]]$; thus, the power series for the η_i are in $\mathbb{Z}_3[[x]] \cdot dx$, as predicted.

Let λ_0, λ_1, λ_2 be defined by $\lambda_i = \lambda_{\eta_i, D}$, or in other words

$$\lambda_i(P) = \int_{(0,1)}^{P} \eta_i.$$

The series for the λ_i are

$$\begin{aligned} \lambda_0 &= x + \tfrac{7}{4}x^2 + \tfrac{187}{24}x^3 + \tfrac{2563}{64}x^4 + \tfrac{29751}{128}x^5 + \tfrac{736819}{512}x^6 + \tfrac{66888879}{7168}x^7 + \cdots, \\ \lambda_1 &= \tfrac{1}{2}x^2 + \tfrac{7}{6}x^3 + \tfrac{187}{32}x^4 + \tfrac{2563}{80}x^5 + \tfrac{49585}{256}x^6 + \tfrac{2210457}{1792}x^7 + \cdots, \\ \lambda_2 &= \tfrac{1}{3}x^3 + \tfrac{7}{8}x^4 + \tfrac{187}{40}x^5 + \tfrac{2563}{96}x^6 + \tfrac{148755}{896}x^7 + \cdots. \end{aligned}$$

Let $\omega_i = f^{*-1}\eta_i$ be the differential on J corresponding to η_i on C, and let $\lambda_i' = \lambda_{\omega_i}$ be the homomorphism from $J(\mathbb{Q}_3)$ to $\mathbb{Q}_3$ obtained by integrating ω_i. We calculate λ_i' explicitly on the kernel of reduction. Let $a \in J_1(\mathbb{Q}_3)$. The divisor class a can be represented $a = [P_1+P_2+P_3-3(0,1)]$ where $P_i \in C(\overline{\mathbb{Q}_3})$ and $\overline{P_i} = \overline{(0,1)}$. Let $s_j = \sum_{i=1}^{3} x(P_i)^j$. From the expression

$$\int_0^a \omega_i = \sum_j \int_{(0,1)}^{P_j} \eta_i$$

we see that

$$\begin{aligned}
\lambda_0 &= s_1 + \tfrac{7}{4}s_2 + \tfrac{187}{24}s_3 + \tfrac{2563}{64}s_4 + \tfrac{29751}{128}s_5 + \tfrac{736819}{512}s_6 + \tfrac{66888879}{7168}s_7 + \cdots, \\
\lambda_1 &= \tfrac{1}{2}s_2 + \tfrac{7}{6}s_3 + \tfrac{187}{32}s_4 + \tfrac{2563}{80}s_5 + \tfrac{49585}{256}s_6 + \tfrac{2210457}{1792}s_7 + \cdots, \\
\lambda_2 &= \tfrac{1}{3}s_3 + \tfrac{7}{8}s_4 + \tfrac{187}{40}s_5 + \tfrac{2563}{96}s_6 + \tfrac{148755}{896}s_7 + \cdots.
\end{aligned}$$

The annihilator. We want to calculate $V = \operatorname{Ann}(J(K))$. The span of $\log(J(\mathbb{Q}))$ is 1-dimensional, so the annihilator V will be 2-dimensional. Note that the divisor class $12U$ is in the kernel of reduction, and that a 1-form kills $J(K)$ if and only if it kills $12U$. Using the obvious generalization of methods in [**2**], we calculate that the divisor class $12U$ is represented by a divisor of the form $[P_1 + P_2 + P_3 - 3(0,1)]$ where the first 3 elementary symmetric functions in the $x(P_i)$ are

$$\begin{aligned}
\sigma_1 &= -\tfrac{711098862585431048203628054718792792}{1791388989232843315879537625475772081} = 3^2 \cdot 17 \pmod{3^5} \\
\sigma_2 &= \tfrac{2724451266300892942794426898300957680}{1791388989232843315879537625475772081} = 3^2 \cdot 14 \pmod{3^5} \\
\sigma_3 &= -\tfrac{1176445915710480852653316703575738240}{1791388989232843315879537625475772081} = 3^4 \cdot 1 \pmod{3^5}.
\end{aligned}$$

The decision to use a precision of 3^5 is somewhat arbitrary. We will find, however, that it is more than adequate.

Note that the valuation of every $x(P_i)$ is at least $\min\{v(\sigma_i)/i\} = \min\{2, 1, 4/3\} = 1$; consequently, the valuation of each s_j is at least j. Note that in the power series for λ'_i the valuation of the coefficient of s_j is at least $v(1/j)$. One easily checks that every term of $\lambda_i(12U)$ beyond $j = 4$ is 0 modulo 3^5.

We can calculate each s_j in terms of the σ_i; the values we get are

$$\begin{aligned}
s_1 &= \sigma_1 &&= 3^2 \cdot 17 \pmod{3^5} \\
s_2 &= \sigma_1^2 - 2\sigma_2 &&= 3^2 \cdot 8 \pmod{3^5} \\
s_3 &= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 &&= 0 \pmod{3^6} \\
s_4 &= \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2 &&= 3^4 \cdot 14 \pmod{3^7}.
\end{aligned}$$

Substituting these values into the series for the λ'_i, we find that

$$\begin{aligned}
\lambda'_0(12U) &= 3^2 \cdot 22 \pmod{3^5} \\
\lambda'_1(12U) &= 3^2 \cdot 13 \pmod{3^5} \\
\lambda'_2(12U) &= 3^4 \cdot 1 \pmod{3^5}.
\end{aligned}$$

Since integration is linear in the integrand we conclude that there are differentials $\alpha', \beta' \in V$ such that $\alpha' = 13\omega_1 - 22\omega_0 \pmod{3^3}$, and $\beta' = \omega_2 - 9\omega_0 \pmod{3^3}$. Let the corresponding differentials on C be α and β.

Bounding each residue class. We know that any rational point $P \in C(\mathbb{Q})$ must satisfy both $\int_{(0,1)}^{P} \alpha = 0$ and $\int_{(0,1)}^{P} \beta = 0$. Recall that we can give at least a preliminary bound on the number of zeros of these integrals by considering the order of vanishing of the reductions $\overline{\alpha}$ and $\overline{\beta}$ of α and β modulo 3. Note that $\overline{\alpha} = (x-1)/y\,dx$ and $\overline{\beta} = x^2/y\,dx$. We list the order of vanishing of these differentials at each residue class in table 1.

	$\overline{\alpha} = \frac{x-1}{y}dx$	$\overline{\beta} = \frac{x^2}{y}dx$
$\overline{(0,1)}$	0	2
$\overline{(0,2)}$	0	2
$\overline{\infty}$	2	0
$\overline{(1,0)}$	2	0
$\overline{(2,1)}$	0	0
$\overline{(2,2)}$	0	0

TABLE 1. Order of vanishing of $\overline{\alpha}$ and $\overline{\beta}$

n	$n\overline{U} \quad + 3[\overline{(0,1)}]$	$n\overline{U} + \overline{T} \quad + 3[\overline{(0,1)}]$
0	$3\overline{(0,1)}$	$2\overline{(2,1)} + 1\overline{(0,1)}$
1	$1\overline{\infty} + 2\overline{(0,1)}$	$2\overline{(2,1)} + 1\overline{\infty}$
2	$2\overline{\infty} + 1\overline{(0,1)}$	$2\overline{(2,1)} + 1\overline{(0,2)}$
3	$3\overline{\infty}$	$1\overline{D_2} + 1\overline{(1,0)}$
4	$2\overline{\infty} + 1\overline{(0,2)}$	$2\overline{(2,2)} + 1\overline{(0,1)}$
5	$1\overline{\infty} + 2\overline{(0,2)}$	$2\overline{(2,2)} + 1\overline{\infty}$
6	$3\overline{(0,2)}$	$2\overline{(2,2)} + 1\overline{(0,2)}$
7	$1\overline{(1,0)} + 2\overline{(0,1)}$	$2\overline{(2,1)} + 1\overline{(1,0)}$
8	$1\overline{(1,0)} + 1\overline{(0,1)} + 1\overline{\infty}$	$1\overline{D_2} + 1\overline{(0,1)}$
9	$3\overline{(1,0)}$	$1\overline{D_2} + 1\overline{\infty}$
10	$1\overline{(1,0)} + 1\overline{(0,2)} + 1\overline{\infty}$	$1\overline{D_2} + 1\overline{(0,2)}$
11	$1\overline{(1,0)} + 2\overline{(0,2)}$	$2\overline{(2,2)} + 1\overline{(1,0)}$

TABLE 2. Reduction of $J(\mathbb{Q})$, offset by $3[\overline{(0,1)}]$

Note that either $\overline{\alpha}$ or $\overline{\beta}$ has order zero at each residue class. Since order 0 implies a bound of 1, there is at most one common zero in each residue class. In particular, the points ∞, $(0,1)$, and $(0,-1)$ are the only rational points in their residue classes.

Using Hensel's Lemma, we find that the residue class of $\overline{(1,0)}$ contains a Weierstrass point W which is defined over $\mathbb{Q}_3$ but is not rational. Since $[W-\infty]$ is torsion, W is a zero of both integrals. By the previous paragraph, W must be the only common zero in its residue class, so the residue class $\overline{(1,0)}$ does not contain any rational points. We will be finished if we can show that there are no rational points in the residue classes $\overline{(2,1)}$ and $\overline{(2,2)}$.

Ruling out residue classes. We want to show that there are no rational points in the residue classes $\overline{(2,1)}$ and $\overline{(2,2)}$. We proceed by showing that neither $[3\overline{(2,1)} - 3\overline{(0,1)}]$ nor $[3\overline{(2,2)} - 3\overline{(0,1)}]$ is in $\overline{J(\mathbb{Q})}$. As noted in the introduction of this example, we know generators for $\overline{J(\mathbb{Q})}$, so this calculation is straightforward.

The group $\overline{J(\mathbb{Q})} \subset \overline{\mathcal{J}}(\mathbb{F}_3)$ is shown in table 2. Each entry in this table is an effective divisor $\overline{E}$ of degree three in the specified divisor class. We interpret this divisor as an element of $\overline{J(\mathbb{Q})}$ by subtracting $3\overline{(0,1)}$. (For example, $0\overline{U} = [3\overline{(0,1)} - 3\overline{(0,1)}]$.) Except for the cases $3\overline{U} + [3\overline{(0,1)}] = [3\overline{\infty}]$ and $9\overline{U} + [3\overline{(0,1)}] = [3\overline{(1,0)}]$, every entry in table 2 is the unique effective divisor in its divisor class.

The complete linear system containing $3\overline{\infty}$ has dimension 1; it consist of divisors of the form $\overline{\infty}+\overline{P}+\rho(\overline{P})$. Likewise, the complete linear system containing $3\overline{(1,0)}$ has dimension 1 and consists of divisors of the form $\overline{(1,0)}+\overline{P}+\rho(\overline{P})$. Taking table 2 together with these two families of divisors gives us an exhaustive list of effective divisors $\overline{E}$ over $\mathbb{F}_3$ such that $[\overline{E}-3\overline{(0,1)}]$ is in the reduction of $J(\mathbb{Q})$. The point we want to make is that $3\overline{(2,1)}$ does not appear in this list. Hence there are no rational points in the residue class of $\overline{(2,1)}$. Likewise, there are no rational points in the residue class of $\overline{(2,2)}$.

We conclude that the set of rational points on C is exactly $\{(0,1),(0,-1),\infty\}$. This completes the example.

CHAPTER 2

Covering Collections

1. Introduction

Let C be a curve defined over K with Jacobian J. We define a **covering collection** for C over K to be a set $\{D_i \to C\}$ of K-rational covers of C in a single $\overline{K}$-isomorphism class, and such that every point in $C(K)$ is hit by a point in some $D_i(K)$. Given a covering collection, the question of determining or bounding the set of rational points on C is reduced to determining or bounding the set of rational points on each of the covers. In fact, it is not difficult to construct a covering collection for C. Assuming that $C(K)$ is not empty, we will show that there are infinitely many unramified abelian covering collections for C over K, and that they can be described explicitly and effectively in terms of isogenies to J. We also have what appears to be a new result on the relationship between the number of rational points on C and the covering collection $\mathcal{D}_\varphi$ associated to an isogeny φ.

PROPOSITION. *Let $n = \#A(K)[\varphi]$ be the number of K-rational points in the kernel of φ. Then the natural map*

$$\bigcup_{D\in\mathcal{D}_\varphi} D(K) \longrightarrow C(K)$$

is n-to-1 and onto.

While it may seem pointless to pass from a single curve to several curves of higher genus, there are circumstances where this is a productive strategy. For example, the curves in a covering collection may cover elliptic curves of rank 0; Coombes and Grant [**6**] use this technique to bound the set of rational points on certain classes of hyperelliptic curves.

Our intended application is to extend the range of curves to which Chabauty techniques can be applied. Let v be a valuation on K and suppose that $\mathrm{Chab}(C, K, v) = g$, so that Chabauty techniques cannot be applied directly to C. (See Chapter I of this work for details.) Let g' be the genus of the curves in the covering collection. Note that $\mathrm{Jac}(D_i)$ is isogenous over K to the product $J \times A_i$ for some K-rational abelian variety of dimension $g' - g$. Using additivity of the Chabauty rank, the question of whether Chabauty can be applied to D_i is precisely the question of whether the Chabauty rank of A_i is less than $g' - g$. No matter how large the rank of $J(K)$ is, it does not rule out the possibility of applying Chabauty on each of the D_i.

Thus, it may be possible to obtain a bound on C by applying Chabauty to each curve D_i in a covering collection. Unfortunately, the Chabauty rank of each D_i is difficult to predict, and requires extensive (and ineffective) computation to determine. In this chapter we will describe the determination of a covering collection; we leave questions of Chabauty techniques to Chapter I and rank calculations to Chapter III.

This chapter starts by developing a theory of covering collections applicable to any curve. This is not essentially new material. We then provide a detailed treatment of the bielliptic genus 2 case, which has several agreeable properties including an explicitly computable rational subcover of genus 3 and elimination of the requirement of a known rational point. Finally, we apply these techniques to a bielliptic genus 2 curve with rank 2. We are able to completely determine the set of rational points on this curve.

In the following, all curves will be assumed to be complete and nonsingular. We fix a choice of number field K and curve C (of genus $g > 1$) defined over K. The Jacobian of C will be denoted by $J = \operatorname{Jac} C$; it is also defined over K. We will assume that $C(K)$ is not empty, and fix a choice of $P \in C(K)$. Finally, we fix a Galois closure $\overline{K}$ of K and let $G_K = \operatorname{Gal}(\overline{K}/K)$ be the absolute Galois group of K.

2. Covering Collections

Recall that a (connected) cover of C is a surjective map from a curve D onto C. (We shall assume that all covers are connected.) We write a cover as $D \to C$, D/C, or even just D if the map to C is understood, but we shall always intend the map and not just the curve D.

Covers have an obvious notion of morphism. If $D \to C$ is defined over K, then by $\operatorname{Aut}_K(D/C)$ we will mean the group of K-automorphisms of the cover; $\operatorname{Aut}_{\overline{K}}(D/C)$ or simply $\operatorname{Aut}(D/C)$ will denote the G_K-module of $\overline{K}$-automorphisms of the cover. If the number of $\overline{K}$-automorphisms is equal to the degree of the cover, we say that $D \to C$ is a Galois cover with Galois group $\operatorname{Gal}(D/C) = \operatorname{Aut}(D/C)$. An abelian cover is a Galois cover with abelian Galois group.

Our goal in studying a K-rational cover $D \to C$ is to use $D(K)$ to discover information about $C(K)$. With that in mind it is useful to introduce the following terminology. We will say that the cover $D \to C$ **hits** the point $Q \in C(K)$ if Q is in the image of $D(K)$. If D hits at least one point of $C(K)$, then we will say that $D \to C$ is **productive**. Note that $D \to C$ is productive exactly when $D(K)$ is not empty.

We now come to our main definition. Let $\mathcal{D} = \{D_i \to C\}_{i \in I}$ be a set of K-isomorphism classes of covers of C. We will say that $\mathcal{D}$ is a (K-rational) **covering collection** for C if

(i) all of the covers in $\mathcal{D}$ are $\overline{K}$-isomorphic, and
(ii) every point of $C(K)$ is hit by some cover in $\mathcal{D}$.

We will often abuse notation by saying that a cover $D \to C$ is in $\mathcal{D}$ when the K-isomorphism class of $D \to C$ is in $\mathcal{D}$; we will say that it is in the class of $\mathcal{D}$ when it is in the $\overline{K}$-isomorphism class of $\mathcal{D}$.

THEOREM 2.1. *An unramified Galois covering collection contains every productive cover in its class.*

PROOF. Let $\mathcal{D}$ be an unramified Galois K-rational covering collection for C, and let $f : D \to C$ be a productive K-rational cover in the class of $\mathcal{D}$. By assumption, $D(K)$ is not empty; fix an element $R \in D(K)$. Since $\mathcal{D}$ is a covering collection we can find a cover $f' : D' \to C$ in $\mathcal{D}$ and a point $R' \in D'(K)$ with $f'(R') = f(R)$.

Since D/C is in the class of $\mathcal{D}$, there is a $\overline{K}$-isomorphism $g : D'/C \to D/C$; since D/C is Galois we can choose g so that R' maps to R. Then for every $\sigma \in G_K$, $g^\sigma(R') = g(R')^\sigma = g(R')$. Since the non-trivial automorphisms of an unramified cover contain no fixed-points, we see that $g^\sigma = g$. Thus D/C is in $\mathcal{D}$. □

By the proof of theorem 2.1 we see that if $\mathcal{D}$ is an unramified Galois covering collection, then every rational point of C is hit by exactly one cover in $\mathcal{D}$. This means that we can characterize a productive cover in the class of $\mathcal{D}$ by any rational point it hits.

3. Unramified Abelian Covers

Our main subject of study in the remainder of this chapter will be unramified abelian covering collections for C. As we shall see, these have an intimate connection with J, the Jacobian of C.

Recall that we have fixed the choice of a point $P \in C(K)$. For every rational divisor class $b \in J(K)$, we define a K-rational map $f_{P,b} : C \to J$ which is given on geometric points by

$Q \mapsto [Q-P]-b$. Note that the classical Abel-Jacobi map with basepoint P is given by $Q \mapsto [Q-P]$; we will write $f_P = f_{P,0}$ for this map. Let t_b be the K-rational map $a \mapsto a+b$ (translation by b) on J; then $f_{P,b} = t_{-b} \circ f_P$. It follows that many of the properties of the Abel-Jacobi map carry over to $f_{P,b}$; in particular, $f_{P,b}$ is a closed embedding.

Define $C_{P,b} = f_{P,b}(C)$. As previously noted, $f_{P,b}$ defines an isomorphism between C and $C_{P,b}$. In case C has automorphisms, the notation $C_{P,b}$ will always refer to the particular identification of $C_{P,b}$ with C given by $f_{P,b}$. Note that $C_{P,b}(K) \subset J(K)$.

Now suppose we are given an abelian variety A/K and a K-rational isogeny $\varphi : A \to J$ of degree d. Since an isogeny is a finite connected abelian cover, the pullback of $C_{P,b}$ to A via φ is a finite connected abelian cover of C; let us call it $D_{P,b}$.

$$\begin{array}{ccc} C_{P,b} \times_J A = D_{P,b} & \longrightarrow & C_{P,b} \\ \downarrow & & \downarrow \\ A & \xrightarrow{\varphi} & J \end{array}$$

$D_{P,b}$ is a curve of genus $d(g-1)+1$. The embedding $D_{P,b} \hookrightarrow A$ induces an isomorphism $\mathrm{Aut}(D_{P,b}/C) \cong A[\varphi]$ of G_K-modules. The notation $D_{P,b} \to C$ will always denote the cover of C given by $D_{P,b} \to C_{P,b} \to C$.

LEMMA 3.1. *The K-isomorphism class of the cover $D_{P,b} \to C$ is determined by the point $P \in C(K)$ and the class of b in $J(K)/\varphi(A(K))$.*

PROOF. Let $a \in A(K)$ and consider the following diagram.

$$\begin{array}{ccc} D_{P,b} & \underset{t_{-a}}{\xrightarrow{\approx}} & D_{P,b+\varphi(a)} \\ \downarrow & & \downarrow \\ C_{P,b} & \underset{t_{\varphi(-a)}}{\xrightarrow{\approx}} & C_{P,b+\varphi(a)} \end{array}$$

$\square$

DEFINITION 3.2. We define $\mathcal{D}_\varphi$ to be the set of isomorphism classes of covers

$$\mathcal{D}_\varphi = \{D_{P,b} \to C\}_{b \in J(K)/\varphi(A(K))}.$$

THEOREM 3.3. *$\mathcal{D}_\varphi$ is a covering collection for C, and $\mathcal{D}_\varphi$ does not depend on the choice of $P \in C(K)$.*

PROOF. Let $Q \in C(K)$ and let $b = f_P(Q)$. Since the image of Q in $C_{P,b}(K)$ is 0_J, we see that 0_A is in $D_{P,b}(K)$; thus, $D_{P,b}$ hits Q. In other words, f_P induces a map $C(K) \to J(K)/\varphi(A(K))$ which sends every $Q \in C(K)$ to the unique cover which hits it.

Suppose $P, P' \in C(K)$ are two rational points on C. Then for any $b \in J(K)$, we have $D_{P',b} = D_{P,b+[P'-P]}$. It follows that the set of K-isomorphism classes of covers in $\mathcal{D}_\varphi$ is independent of the choice of P. Note, however, that the implied map from $J(K)/\varphi(A(K))$ to $\mathcal{D}_\varphi$ does depend on P. $\square$

The next result gives us the exact relationship between the number of rational points on C and the number of rational points in an unramified abelian covering collection.

PROPOSITION 3.4. *Let $n = \#A(K)[\varphi]$ be the number of K-rational points in the kernel of φ. Then the natural map*

$$\bigcup_{D\in\mathcal{D}_\varphi} D(K) \longrightarrow C(K)$$

is n-to-1 and onto.

PROOF. $A(K)\xrightarrow{\varphi}\varphi(A(K))$ is n-to-1, and $D_{P,b}(K) = \varphi^{-1}(C_{P,b}(K)) \cap A(K)$. □

3.1. Galois Cohomology. Consider the exact sequence of G_K-modules

$$0 \to A[\varphi] \to A \to J \to 0.$$

Taking Galois cohomology gives us a long exact sequence from which we can extract the short exact sequence

$$(*) \qquad 0 \to J(K)/\varphi(A(K)) \to H^1(G_K, A[\varphi]) \to H^1(G_K, A)[\varphi] \to 0.$$

Now suppose that D/C is an arbitrary K-rational cover in the class of $\mathcal{D}_\varphi$, and let $g : D/C \to D_{P,0}/C$ be an isomorphism over $\overline{K}$. The class of the cocycle

$$\xi_{D/C}(\sigma) = g^\sigma g^{-1} \in H^1(G_K, \mathrm{Aut}(D_{P,0}/C)) \cong H^1(G_K, A[\varphi])$$

is independent of the choice of isomorphism g. Thus, we can identify the middle term in $(*)$ with the set $\mathrm{Twist}(D_{P,0}/C)$ of K-isomorphism classes of covers of C in the class of $\mathcal{D}_\varphi$.

Next consider the last term in $(*)$. We can identify $H^1(G_K, A)$ with the set of principal homogeneous spaces for A defined over K; in this interpretation, $H^1(G_K, A)[\varphi]$ is the set of principal homogeneous spaces for A which can be provided with a K-rational map to J which is $\overline{K}$-isomorphic to φ.

The map $H^1(G_K, A[\varphi]) \to H^1(G_K, A)[\varphi]$ sends a twist of $D_{P,0}/C$ to the principal homogeneous space in which it is naturally embedded. Thus, $J(K)/\varphi(A(K))$ is identified with the set of twists which lie on A. Also, since non-trivial principal homogeneous spaces do not contain any rational points, we have a second proof of the fact that $\mathcal{D}_\varphi$ contains all of the productive covers in its class.

On the other hand, suppose $H \subset H^1(G_K, A[\varphi])$ is a finite cohomology subgroup containing the image of $J(K)/\varphi(A(K))$. Then we can define a covering collection

$$\mathcal{D}_H = \{D^\xi_{P,0}\}_{\xi\in H},$$

where $D^\xi_{P,0}$ is the twist of $D_{P,0}$ associated to the cocycle ξ. In particular, if we let H be the φ-Selmer group $S^{(\varphi)}(A/K)$, this leads (at theory, at least) to an effectively computable covering collection for C. See also Coombes and Grant [**6**], where the set of cohomology classes that are unramified outside of the primes over 2, the infinite places, and the primes of bad reduction of C are used to analyze hyperelliptic curves whose Jacobians have a rational 2-torsion point.

4. Bielliptic Genus 2

Having laid out a general framework which is applicable to any curve, we now work out a detailed description of the curves and maps in the V_4 covering collection associated to a bielliptic genus 2 curve C. For each genus 5 cover in the collection, we also examine a genus 3 quotient associated to the hyperelliptic involution on C. In many applications, use of the genus 3 curve has both practical and theoretical advantages.

We will use the following naming convention for curves:

L_* genus 0
E_* genus 1
C_* genus 2
F_* genus 3
D_* genus 5

The case of genus 0 curves bears special attention. Whenever we consider a genus 0 curve defined over K, it will be K-isomorphic to $\mathbb{P}^1_K$, but not canonically. Thus we will give specific names to the roles played by various genus 0 curves. In particular, L_X will frequently denote the quotient of a hyperelliptic curve X by its hyperelliptic involution; one exception to this rule is the genus 0 curve L_0, which is the terminal object in the set of maps we will be considering. On the other hand, if we simply wish to indicate that some genus 0 curve occupies a particular place in a diagram, we may on occasion refer to it as $\mathbb{P}^1$ rather than giving it a specific name.

4.1. Description of Bielliptic Genus 2.

DEFINITION 4.1. A curve is called **bielliptic** if it has a degree 2 map to an elliptic curve.

We start by summarizing results from the literature which provide a description of K-rational bielliptic genus 2 curves.

THEOREM 4.2. *Suppose C is a genus 2 curve with a K-rational degree 2 map to a curve of genus 1.*

(i) *C has degree 2 maps to two genus 1 curves E_1 and E_2.*
(ii) *There is a polynomial $r(x) \in K[x]$ such that C, E_1, and E_2 have equations of the form*

$$\begin{aligned} C : y^2 &= \quad r(x^2) &&= r_3x^6 + r_2x^4 + r_1x^2 + r_0 \\ E_1 : y^2 &= \quad r(x) &&= r_3x^3 + r_2x^2 + r_1x + r_0 \\ E_2 : y^2 &= x^3 \cdot r(x^{-1}) &&= r_0x^3 + r_1x^2 + r_2x + r_3. \end{aligned}$$

With this choice of coordinates, there are degree 2 maps $\varphi_1 : C \to E_1$ and $\varphi_2 : C \to E_2$ given by $\varphi_1(x, y) = (x^2, y)$ and $\varphi_2(x, y) = (1/x^2, y/x^3)$. In particular, both E_1 and E_2 have a K-rational point at infinity, and we will consider each of them to be an elliptic curve with this choice of identity element.
(iii) *The maps φ_1 and φ_2 induce V_4 isogenies*

$$E_1 \times E_2 \xrightarrow{{\varphi_1}^* + {\varphi_2}^*} J \xrightarrow{{\varphi_1}_* \times {\varphi_2}_*} E_1 \times E_2$$

whose composition is multiplication by 2. If the roots of r are α, β, and γ, then the kernel of the first isogeny is

$$\{0\times 0,\ (\alpha, 0)\times(1/\alpha, 0),\ (\beta, 0)\times(1/\beta, 0),\ (\gamma, 0)\times(1/\gamma, 0)\}$$

and the kernel of the second isogeny is

$$\{0,\ [(\sqrt[+]{\alpha}, 0) - (\sqrt[-]{\alpha}, 0)],\ [(\sqrt[+]{\beta}, 0) - (\sqrt[-]{\beta}, 0)],\ [(\sqrt[+]{\gamma}, 0) - (\sqrt[-]{\gamma}, 0)]\}.$$

(iv) *With the choice of coordinates above, we obtain a commutative diagram of K-rational maps:*

$$\begin{tikzcd} & E_1 \arrow[dr, "x"] & \\ C \arrow[ur, "\varphi_1"] \arrow[r, "\varphi_2"] \arrow[dr, "x"'] & E_2 \arrow[r, "1/x"] & L_0 \\ & L_C \arrow[ur, "x^2"'] & \end{tikzcd}$$

PROOF. See Frey and Kani [**11**], or Kuhn [**13**]. □

NOTE. Since our intended application is to bound the number of rational points on C, we will assume that neither E_1 nor E_2 has rank 0. If it were that case that, say, E_1 had rank 0, then it would be relatively straightforward to completely determine the set of rational points on C by examining the preimages of the set of rational torsion points on E_1.

Set $A = E_1 \times E_2$ and $\varphi = {\varphi_1}^* + {\varphi_2}^*$, and assume the existence of a rational point $P \in C(K)$, which we fix. (But note that we will eventually be able to remove this restriction.) Then for every rational $b \in J(K)$ we obtain a genus 5 cover $D_{P,b} \to C$ with V_4 Galois group. We now focus on this cover.

We start by introducing two important values related to the cover $D_{P,b}$:

$$e_1 = \varphi_1(P) + \varphi_{1*}(b) \in E_1(K),$$
$$e_2 = \varphi_2(P) + \varphi_{2*}(b) \in E_2(K).$$

The definition of e_1 is motivated by the observation that when we are working with the cover $D_{P,b}$ we have two different "natural" maps from C to E_1. The first is $\varphi_1 : C \to E_1$ and the second is the composition

$$\begin{array}{ccc} C \cong C_{P,b} \hookrightarrow J \xrightarrow{\varphi_{1*}} E_1 \\ Q \quad \mapsto \quad \varphi_1(Q) - \varphi_1(P) - \varphi_{1*}(b). \end{array}$$

Note that this second map is equal to $t_{-e_1} \circ \varphi_1$. We shall often depend on the notation $C \to E_1$ and $C_{P,b} \to E_1$ to distinguish these maps; a similar convention holds for maps to E_2.

REMARK 4.3. The connection between E_1 and E_2 is arithmetic rather than geometric. If C is bielliptic to the elliptic curves E_1 and E_2, then $E_1[2]$ is G_K-isomorphic to $E_2[2]$. Conversely, for any two elliptic curves E_1 and E_2 over K and any G_K-module isomorphism $g : E_1[2] \to E_2[2]$, either we obtain a genus 2 bielliptic curve over K or E_1 is $\overline{K}$-isomorphic to E_2 and g is induced by this isomorphism. For example, if E_1 and E_2 have different j-invariants and $K(E_1[2]) = K(E_2[2])$, then E_1 and E_2 are degree 2 subcovers of respectively 6, 2, 3, or 6 different bielliptic genus 2 curves depending on whether the degree of the extension $K(E_1[2])/K$ is 1, 2, 3, or 6.

4.2. Involutions. Because of the prominent role played by degree 2 and V_4 maps, it is convenient to examine various involutions on $D_{P,b}$. As we shall see, this analysis is greatly facilitated if the involution on $D_{P,b}$ is **carried by** an involution on $E_1 \times E_2$; by this we mean that there is an involution of the variety $E_1 \times E_2$ which sends the embedded curve $D_{P,b}$ into itself and induces the desired involution on $D_{P,b}$. We will also talk about involutions on $D_{P,b}$ which **lie over** an involution on C (or equivalently on $C_{P,b}$). This means that the involutions commute with the covering map; since $D_{P,b}/C$ is Galois, it is clear that if there are any $\overline{K}$-defined involutions of $D_{P,b}$ lying over a given involution of C, then there are exactly 4 such. For notational convenience, we will generally write $[n, m]$ for the endomorphism on $E_1 \times E_2$ that is $[n]$ on E_1 and $[m]$ on E_2.

Consider the map $D_{P,b} \to E_1$ obtained by projecting $D_{P,b} \hookrightarrow E_1 \times E_2$ onto the first coordinate. This map sits in a commutative diagram

$$\begin{array}{ccc} D_{P,b} & \xrightarrow{\varphi} & C_{P,b} \\ \downarrow & & \downarrow \\ E_1 & \xrightarrow{[2]} & E_1 \end{array}$$

and checking degrees shows that both vertical maps are degree 2. Thus the vertical maps correspond to involutions $\rho_{1,D}$ and $\rho_{1,C}$ on $D_{P,b}$ and $C_{P,b}$, respectively. Furthermore, the commutativity of the diagram implies that $\rho_{1,D}$ lies over $\rho_{1,C}$. We similarly define the involutions $\rho_{2,D}$ and $\rho_{2,C}$ relative to $D_{P,b} \to E_2$ and $C_{P,b} \to E_2$.

Note that we can easily give formulas for $\rho_{1,C}$ and $\rho_{2,C}$:

$$\rho_{1,C}(x,y) = (-x,y),$$
$$\rho_{2,C}(x,y) = (-x,-y).$$

It follows that $\rho_{1,C}$ commutes with $\rho_{2,C}$, and that their product $\rho_{0,C} = \rho_{1,C} \circ \rho_{2,C}$ is the hyperelliptic involution on C. We also note that the fixed points for $\rho_{1,C}$ are $(0,1)$ and $(0,-1)$, while the fixed points for $\rho_{2,C}$ are the two points over infinity on C, which we will call ∞^+ and ∞^-.

THEOREM 4.4. *Let $e_1 \in E_1$ and $e_2 \in E_2$ be defined as above.*

Then $\rho_{1,D}$ is carried by the involution $[1,-1] \circ t_{0\times e_2}$ on $E_1 \times E_2$, and $\rho_{2,D}$ is carried by the involution $[-1,1] \circ t_{e_1 \times 0}$.

PROOF. First we show that $[1,-1] \circ t_{0\times e_2}$ induces an involution which lies over $\rho_{1,C}$. Note that $\rho_{1,C}$ induces an automorphism $\rho_{1,J} = {\rho_{1,C}}^*$ on J. The automorphism $[1,-1]$ on $E_1 \times E_2$ lies over $\rho_{1,J}$ and one easily verifies that

$$\begin{aligned}
\rho_{1,J}(\varphi(0\times e_2)) &= -{\varphi_2}^*(e_2) \\
&= -{\varphi_2}^* \circ \varphi_2(P) - {\varphi_2}^* \circ \varphi_{2*}(b) \\
&= -[\rho_{2,C}(P) + P] - [\rho_{2,J}(b) + b] \\
&= [\rho_{1,C}(P) - P] + [\rho_{1,J}(b) - b].
\end{aligned}$$

In particular, if we apply $\rho_{1,J} \circ t_{\varphi(0\times e_2)}$ to a point in $C_{P,b}$, we see that

$$\rho_{1,J} \circ t_{\varphi(0\times e_2)}([Q-P] - b) = [\rho_{1,C}(Q) - P] - b \in C_{P,b}.$$

Since $\rho_{1,J} \circ t_{\varphi(0\times e_2)}$ carries $C_{P,b}$ to itself and induces $\rho_{1,C}$, we find that $[1,-1] \circ t_{0\times e_2}$ carries $D_{P,b}$ to itself and induces an involution which lies over $\rho_{1,C}$.

Now, $\rho_{1,J}$ lies under the 4 involutions $[1,-1] \circ t_{T_1 \times T_2}$, $T_1 \times T_2 \in E_1 \times E_2[\varphi]$. It follows that $\rho_{1,D}$ is carried by one of the 4 involutions $[1,-1] \circ t_{T_1 \times (e_2 - T_2)}$. Riemann-Hurwitz tells us that $D_{P,b} \to E_1$ is ramified, so $\rho_{1,D}$ must be carried by an involution with fixed points. But $[1,-1] \circ t_{T_1 \times (e_2 - T_2)}$ acts by t_{T_1} on the E_1 coordinate; it can only have fixed points if $T_1 = 0$. Since $T_1 = 0$ implies $T_2 = 0$, we conclude that $\rho_{1,D}$ is carried by $[1,-1] \circ t_{0\times e_2}$.

A similar argument shows that $\rho_{2,D}$ is carried by $[-1,1] \circ t_{e_1 \times 0}$. □

Since $\rho_{1,D}$ and $\rho_{2,D}$ are carried by morphisms on $E_1 \times E_2$, we easily verify that they commute with each other and with the automorphisms from $\mathrm{Aut}(D_{P,b}/C)$. In particular, we see that the product $\rho_{0,D} = \rho_{1,D} \circ \rho_{2,D}$ is an involution on $D_{P,b}$ which lies over the hyperelliptic involution $\rho_{0,C} = \rho_{1,C} \circ \rho_{2,C}$ on C. Note that $\rho_{0,D}$ is carried by $[-1,-1] \circ t_{e_1 \times e_2}$.

Define $F_{P,b}$ to be the quotient of $D_{P,b}$ by $\rho_{0,D}$.

THEOREM 4.5. *$F_{P,b}$ is a K-rational genus 3 curve.*

PROOF. Define L_F to be the quotient of $D_{P,b}$ by the V_4 group of automorphisms generated by $\rho_{1,D}$ and $\rho_{2,D}$. We then obtain a commutative diagram

$$\begin{tikzcd}
 & E_1 \arrow[dr] & \\
D_{P,b} \arrow[ur] \arrow[r] \arrow[dr] & E_2 \arrow[r] & L_F \\
 & F_{P,b} \arrow[ur] &
\end{tikzcd}$$

where all of the maps are induced by involutions, and in fact the first three maps are induced by $\rho_{1,D}$, $\rho_{2,D}$, and $\rho_{0,D}$, and the second three maps are induced by the residues of these involutions.

By Riemann-Hurwitz we know that $D_{P,b} \to E_1$ and $D_{P,b} \to E_2$ are each ramified at 8 points; since the fixed points for $\rho_{1,D}$ and $\rho_{2,D}$ must lie over the fixed points for $\rho_{1,C}$ and $\rho_{2,C}$, we see that these two fixed point sets do not intersect. One consequence is that the map $E_1 \to L_F$ is ramified, so L_F has genus 0.

Using Riemann-Hurwitz again, we find that map $D_{P,b} \to L_F$ has 16 ramification points; since this must include all of the fixed points of $\rho_{1,D}$, $\rho_{2,D}$, and $\rho_{0,D}$, we find that the fixed point set of $\rho_{0,D}$ must be a subset of the union of the fixed point sets of $\rho_{1,D}$ and $\rho_{2,D}$. But writing $\rho_{0,D} = \rho_{2,D} \circ \rho_{1,D}$ we see that none of the fixed points for $\rho_{1,D}$ are fixed by $\rho_{0,D}$, and switching the order we see that in fact $\rho_{0,D}$ does not have any fixed points. Thus $D_{P,b} \to F_{P,b}$ is unramified, from which it follows by Riemann-Hurwitz that $F_{P,b}$ is of genus 3. □

REMARK 4.6. Since any rational point on $D_{P,b}$ will map to a rational point on $F_{P,b}$, it will suffice to bound the set of rational points on $F_{P,b}$. As we shall see, working with $F_{P,b}$ instead of $D_{P,b}$ has at least three distinct advantages. First, the difference between genus 3 and genus 5 is significant in terms of computational difficulty. Second, $F_{P,b}$ is hyperelliptic while $D_{P,b}$ is not; this also affects computational difficulty. Third, the rank of $D_{P,b}$ is the sum of the ranks of C and $F_{P,b}$. Since by assumption C has rank at least 2, we see that it is never a disadvantage, and frequently an advantage, to attempt to apply Chabauty to $F_{P,b}$ instead of $D_{P,b}$. In the extreme case, if the rank of C is at least 5 it will never be possible to apply Chabauty to $D_{P,b}$, while there is no *a priori* reason to believe Chabauty on $F_{P,b}$ will be impossible.

COROLLARY 4.7. *$F_{P,b}$ is hyperelliptic.*

PROOF. This is implicit in the degree 2 map $F_{P,b} \to L_F$ found in the previous theorem. The hyperelliptic involution on $F_{P,b}$ is given by $\rho_{1,D} \pmod{\rho_{0,D}}$, which is equivalent to $\rho_{2,D} \pmod{\rho_{0,D}}$. □

LEMMA 4.8. *$D_{P,b}$ is not hyperelliptic.*

PROOF. If $D_{P,b}$ were hyperelliptic, then the hyperelliptic involution on $D_{P,b}$ would necessarily lie over the hyperelliptic involution on $C_{P,b}$. (Consider that $[-1]$ commutes with the Albanese map from the Jacobian of $D_{P,b}$ to $E_1 \times E_2$.)

Working over $\overline{K}$, the 4 involutions on $D_{P,b}$ lying over $\rho_{0,C}$ are carried by the 4 maps $[-1,-1] \circ t_{(e_1+T_1)\times(e_2+T_2)}$, $T_1 \times T_2 \in (E_1 \times E_2)[\varphi]$. Direct calculation shows that the fixed points of these involutions on $E_1 \times E_2$ intersect $D_{P,b}$ in respectively 0,8,8,8 points; thus, these involutions on $D_{P,b}$ correspond to maps to $F_{P,b}$ and 3 elliptic curves. In particular, none of these involutions is hyperelliptic. □

Our next step is to describe the decomposition of the Jacobians of $D_{P,b}$ and $F_{P,b}$. It will be useful to have the following technical lemma.

LEMMA 4.9. *Suppose H is a V_4 group of automorphisms on a curve X, inducing a commutative diagram*

$$\begin{tikzcd} & Y \arrow[dr] & \\ X \arrow[ur] \arrow[r] \arrow[dr] & Y' \arrow[r] & W \\ & Y'' \arrow[ur] & \end{tikzcd}$$

Let J_X be the Jacobian of X, J_Y the Jacobian of Y, etc. Then J_X/J_W is isogenous to $J_Y/J_W \times J_{Y'}/J_W \times J_{Y''}/J_W$.

PROOF. Let ρ, ρ', and ρ'' be the involutions on X associated to Y, Y', and Y'', respectively. Let $\sim$ denote isogeny. We start by making 3 observations:

(i) The image of J_Y in J_X is $(1+\rho_*)J_X$; hence $J_Y \sim (1+\rho_*)J_X$.
(ii) Since ρ and ρ' commute, ρ'_* operates on both J_Y and $(1+\rho_*)J_X$.
(iii) If ι is any involution on an abelian variety A, then $A \sim (1+\iota)A \times (1-\iota)A$.

Applying these observations to J_Y, we see that

$$\begin{aligned} J_Y &\sim (1+\rho_*)J_X \\ &\sim (1+\rho'_*)(1+\rho_*)J_X \times (1-\rho'_*)(1+\rho_*)J_X \\ &\sim (1+\rho_*+\rho'_*+\rho''_*)J_X \times (1+\rho_*-\rho'_*-\rho''_*)J_X. \end{aligned}$$

Similar calculations show that

$$\begin{aligned} J_{Y'} &\sim (1+\rho_*+\rho'_*+\rho''_*)J_X \times (1-\rho_*+\rho'_*-\rho''_*)J_X, \\ J_{Y''} &\sim (1+\rho_*+\rho'_*+\rho''_*)J_X \times (1-\rho_*-\rho'_*+\rho''_*)J_X, \\ J_W &\sim (1+\rho_*+\rho'_*+\rho''_*)J_X, \end{aligned}$$

and finally,

$$\begin{aligned} J_X \sim\ & (1+\rho_*+\rho'_*+\rho''_*)J_X \times (1+\rho_*-\rho'_*-\rho''_*)J_X \\ & \times (1-\rho_*+\rho'_*-\rho''_*)J_X \times (1-\rho_*-\rho'_*+\rho''_*)J_X. \end{aligned}$$

The result now follows easily. □

THEOREM 4.10. *$\mathrm{Jac}(D_{P,b})$ is K-isogenous to $E_1 \times E_2 \times \mathrm{Jac}(F_{P,b})$, and $\mathrm{Jac}(F_{P,b})$ is $\overline{K}$-isogenous to a product of 3 elliptic curves.*

PROOF. The first statement is clear from the preceding corollary and the definitions of $\rho_{1,D}$, $\rho_{2,D}$, and $\rho_{0,D}$. For the second statement, note that $D_{P,b} \to C$ is a V_4 unramified cover. Thus over $\overline{K}$ there are 3 intermediate unramified subcovers, which must have genus 3. The result follows from either of the following diagrams.

$$\begin{tikzcd} & F_\alpha \arrow[dr] & & & & E_\alpha \arrow[dr] & \\ D_{P,b} \arrow[ur] \arrow[r] \arrow[dr] & F_\beta \arrow[r] & C & & F_{P,b} \arrow[ur] \arrow[r] \arrow[dr] & E_\beta \arrow[r] & L_C \\ & F_\gamma \arrow[ur] & \arrow[rr, "\text{quotient by } \rho_{0,D}"] & & & E_\gamma \arrow[ur] & \end{tikzcd}$$

□

REMARK 4.11. In the proof of lemma 4.8 it was mentioned that the $\overline{K}$-involutions on $D_{P,b}$ lying over $\rho_{0,C}$ induce maps to $F_{P,b}$ and "three elliptic curves". In fact, these curves are 2-isogenous to the elliptic curves E_α, E_β, and E_γ mentioned above; let us call them E'_α, E'_β, and E'_γ. Then over $\overline{K}$ these elliptic curves can be characterized in the following way: The map $D_{P,b} \to L_0$ is ramified over 5 points on L_0. These points are $\{0, \alpha, \beta, \gamma, \infty\}$. Now, $E_1 \to L_0$ is ramified over $\{\alpha, \beta, \gamma, \infty\}$ and $E_2 \to L_0$ is ramified over $\{0, \alpha, \beta, \gamma\}$. We claim that the elliptic curves E'_α, E'_β, and E'_γ are ramified over $\{0, \beta, \gamma, \infty\}$, $\{0, \alpha, \gamma, \infty\}$, and $\{0, \alpha, \beta, \infty\}$, and that E_α, E_β, and E_γ are 2-isogenous to respectively E'_α, E'_β, and E'_γ by the isogeny which identifies 0 and ∞ on each of these curves.

4.3. Explicit Equations. The involutions $\rho_{0,D}$, $\rho_{1,D}$, and $\rho_{2,D}$, and the group of involutions corresponding to $\mathrm{Aut}(D_{P,b}/C)$ are K-rational and commute. Taking the quotient of $D_{P,b}$ by the various combinations of these K-rational automorphism subgroups give us a large diagram of K-rational maps:

$$
(**) \qquad
\begin{tikzcd}
D_{P,b} \arrow[rrr, "\varphi"] \arrow[drr] \arrow[ddr] \arrow[ddd] & & & C_{P,b} \arrow[drr, "t_{-e_1} \circ \varphi_1"] \arrow[ddr] \arrow[ddd] & & \\
& & E_1 \arrow[rrr, "{[2]}"] \arrow[ddd] & & & E_1 \arrow[ddd, "x \circ t_{e_1}"] \\
& E_2 \arrow[rrr, "{[2]}"] \arrow[ddr] & & & E_2 \arrow[ddr] & \\
F_{P,b} \arrow[rrr, "Y"] \arrow[drr, "Z"'] & & & L_C \arrow[drr, "Y^2"] & & \\
& & L_F \arrow[rrr, "h"] & & & L_0
\end{tikzcd}
$$

In this diagram we introduce labels h, Y, Z for maps that will be important in the sequel.

Let $[x]$ and $[y]$ be the x and y coordinate maps on E_1. As mentioned earlier, the map $C_{P,b} \to E_1$ is $t_{-e_1} \circ \varphi_1$; the corresponding map $E_1 \to L_0$ is $[x] \circ t_{e_1}$. With this convention, the map $L_C \to L_0$ is still the squaring map, which we have labeled as Y^2 to be compatible with the map Y.

So far we have chosen a specific isomorphism to $\mathbb{P}^1$ for every genus 0 curve in this diagram except L_F. Ignoring the $\mathrm{PGL}(2, K)$ ambiguity for the moment, we can take Z to be the coordinate system for L_F. The diagram suggests the following proposition:

Proposition 4.12. *The plane curve $Y^2 = h(Z)$ on $L_C \times L_F$ is birational to $F_{P,b}$.*

From the diagram it is clear that $F_{P,b}$ covers $Y^2 = h(Z)$, so it will suffice to show that $Y^2 = h(Z)$ is genus 3. The remainder of this section will be devoted to proving this result; along the way we also provide an explicit description of the map h.

As noted above, we need to choose an isomorphism $L_F \cong \mathbb{P}^1$. The map $E_1 \to L_F$ is induced by the involution $\rho_{2,D}$ (mod $\rho_{1,D}$); this gives the involution $[-1] \circ t_{e_1}$ on E_1. If $d \in E_1(\overline{K})$ is a point whose double is e_1, then the $\overline{K}$-defined function $[x] \circ t_d$ is $\overline{K}$-isomorphic to the desired map $E_1 \to L_F$, and there is a fractional linear transformation $g \in \mathrm{PGL}(2, \overline{K})$ such that $g \circ [x] \circ t_d$ is K-rational. The choice of g is well-defined up to $\mathrm{PGL}(2, K)$.

We now demonstrate a method for explicitly constructing an appropriate choice of g. By assumption, the rank of E_1 is positive; choose points $R_0, R_1, R_\infty \in E_1(K)$ which are in distinct orbits under the involution $[-1] \circ t_{e_1}$. Define $x_0 = [x](R_0 + d)$, $x_1 = [x](R_1 + d)$, $x_\infty = [x](R_\infty + d)$. Then we can define

$$g(Z) = g(d, R_0, R_1, R_\infty; Z) = \frac{x_1 - x_\infty}{x_1 - x_0} \left(\frac{Z - x_0}{Z - x_\infty} \right).$$

Note that $g \circ [x] \circ t_d$ sends R_0, R_1, and R_∞ to 0, 1, and ∞, respectively.

Lemma 4.13. *With the given choice of R_0, R_1, R_∞, and for any choice of point $d \in E_1(\overline{K})$ with $[2]d = e_1$, the map $g(d, R_0, R_1, R_\infty; \cdot) \circ [x] \circ t_d$ is K-rational and is independent of the choice of d.*

Proof. Let d and d' be any two points whose doubles are e_1, and let g and g' be given by the above formula. Both $[x] \circ t_d$ and $[x] \circ t_{d'}$ are degree two functions which induce the involution $[-1] \circ t_{e_1}$; thus, they both induce degree one functions on the quotient curve L_F. It follows that there is a transformation $\eta \in \mathrm{PGL}(2, \overline{K})$ such that $[x] \circ t_{d'} = \eta \circ [x] \circ t_d$. Thus,

$$g' \circ [x] \circ t_{d'} = g' \circ \eta \circ [x] \circ t_d.$$

But both $g' \circ \eta$ and g are in $\mathrm{PGL}(2, \overline{K})$; since they send the same three points to 0, 1, and ∞, they must be identical. Thus the given map does not depend on the choice of d. K-rationality follows. $\square$

NOTE. The above formula only gives one possible choice for g. If there is a rational point whose double is e_1, it will generally be much more convenient to choose this point for d, in which case we can choose $g = \mathrm{Id}$. Note that this set of choices will not necessarily result in any rational point on E_1 being sent to 0, 1, or ∞ on L_F.

We can now give an explicit formula for h in terms of our choices for d and g. Let $[2x]$ be the x-coordinate duplication formula for E_1. Then we have the following diagram, where the curve labeled $\mathbb{P}^1$ and the diagonal arrows to and from it are not necessarily defined over K.

$$\begin{tikzcd}
E_1 \arrow[rr, "{[2]}"] \arrow[dd, "g \circ [x] \circ t_d"'] \arrow[dr, "{[x] \circ t_d}"] & & E_1 \arrow[dd, "{[x] \circ t_{e_1}}"] \\
& \mathbb{P}^1 \arrow[dl, "g"'] \arrow[dr, "{[2x]}"] & \\
L_F \arrow[rr, "h = [2x] \circ g^{-1}"'] & & L_0
\end{tikzcd}$$

Now, the relationship $Y^2 = h(Z)$ holds on $F_{P,b}$. By the identity $h = [2x] \circ g^{-1}$ we see that h is a degree 4 map ramified exactly over the x-coordinates of the 3 non-trivial 2-torsion points on E_1. In particular, h is not ramified over 0 or ∞. Thus, $Y^2 = h(Z)$ gives the equation for a genus 3 hyperelliptic curve whose 8 Weierstrass points have Z-coordinates in $h^{-1}(0) \cup h^{-1}(\infty)$. Since $F_{P,b}$ covers this curve, they must be birational.

REMARK 4.14. The divisor $Z^*h^*([0-\infty])$ on $F_{P,b}$ gives a rational 2-torsion point on the Jacobian of $F_{P,b}$. Let B be the quotient of $\mathrm{Jac}(F_{P,b})$ by this 2-torsion element. Then the unramified abelian cover $D_{P,b} \to F_{P,b}$ is in the class of the covering collection given by the dual isogeny $B^\vee \to \mathrm{Jac}(F_{P,b})$.

REMARK 4.15. It is now quite easy to give equations for $D_{P,b}$. We can, for example, take the obvious relations given in the large diagram (**):

$$(x,y) \in E_1, \quad (Z,Y) \in F_{P,b}, \quad ([x] \circ t_{e_1} \circ [2])(x,y) = h(Z).$$

However, the last two equations collapse, giving us the more succinct formulation:

$$\begin{aligned} y^2 &= r_3x^3 + r_2x^2 + r_1x + r_0 \\ Y^2 &= ([x] \circ t_{e_1} \circ [2])(x,y). \end{aligned}$$

Given these equations for $D_{P,b}$, the maps to $F_{P,b}$ and C are:

$$\begin{aligned} D_{P,b} \to F_{P,b}&\colon\ (x,y,Y) \mapsto ((g \circ [x] \circ t_d)(x,y), Y) \\ D_{P,b} \to C\ \ &:\ (x,y,Y) \mapsto (Y, ([y] \circ t_{e_1} \circ [2])(x,y)) \end{aligned}$$

Note that the Y coordinate on $F_{P,b}$ agrees with the x coordinate on C. This means we can move points back and forth between C and $F_{P,b}$ with minimal ambiguity; there is no need to actually lift points to $D_{P,b}$ in order to determine the relationship between rational points on C and $F_{P,b}$.

4.4. Effective Computation. The alert reader will have noticed that we have constructed a bijection between elements $b \in J(K)/\varphi((E_1 \times E_2)(K))$ and certain covers $D_{P,b}$ of C, but that we have given explicit equation for $D_{P,b}$ in terms of a parameter $e_1 = e_1(P,b) \in E_1(K)/2E_1(K)$. This is no illusion: a quick check of theorem 4.2 shows that $E_1 \times E_2[\varphi]$ is G_K-isomorphic to both $E_1[2]$ and $E_2[2]$. Then from the diagram

$$\begin{tikzcd}
0 \arrow[r] & J(K)/\varphi((E_1 \times E_2)(K)) \arrow[r] \arrow[d, "\varphi_{1*}"] & H^1(G_K, E_1 \times E_2[\varphi]) \arrow[d, equal] \\
0 \arrow[r] & E_1(K)/2E_1(K) \arrow[r] & H^1(G_K, E_1[2])
\end{tikzcd}$$

we see that φ_{1*} induces injections from $J(K)/\varphi((E_1 \times E_2)(K))$ into $E_1(K)/2E_1(K)$ and from the Selmer group $S^{(\varphi)}(E_1 \times E_2/K)$ into $S^{(2)}(E_1/K)$. The map of sets e_1 is simply a translation of φ_{1*} by a factor in $E_1(K)$, so it, too, induces injections.

So far, the largest practical obstacle to the calculation of $\mathcal{D}_\varphi$ is the necessity of finding representatives for $J(K)/\varphi((E_1 \times E_2)(K))$. This can now be improved in several ways. First, the size of $J(K)/\varphi((E_1 \times E_2)(K))$ is limited by the smaller of $E_1(K)/2E_1(K)$ and $E_2(K)/2E_2(K)$. Second, the cohomology classes representing $J(K)/\varphi((E_1 \times E_2)(K))$ must be unramified outside the infinite places, the primes over 2, and the *intersection* of the primes of bad reduction of E_1 and E_2; this can restrict the search even further. Third, one can abandon $J(K)/\varphi((E_1 \times E_2)(K))$ altogether and use either $E_1(K)/2E_1(K)$ or the 2-Selmer group $S^{(2)}(E_1/K)$; in fact, one does not even need to know a rational point $P \in C(K)$ in order to use this option.

This last point deserves some emphasis. Given a curve C which is bielliptic and genus 2 over K, we readily calculate the genus 3 curve associated to $e_1 = 0$:

$$F_0 : Y^2 = [2x]_{E_1}(Z).$$

If we know a set of representatives for $E_1(K)/2E_1(K)$, we calculate the genus 3 curve F_{e_1} associated to each possible $e_1 \in E_1(K)/2E_1(K)$; otherwise, we use the cohomology twist F_0^ξ for each $\xi \in S^{(2)}(E_1/K)$. Note that $S^{(2)}(E_1/K)$ is effectively computable, and that good tools exist for calculating it. If we know a rational point $P \in C(K)$ we may be able to use it to limit the number of cases (as discussed above), but this is no longer a requirement.

5. Example

Problem VI.17 in Diophantus' *Arithmetica* (Arabic text) asks for positive rational solutions to

$$y^2 = x^8 + x^4 + x^2.$$

Removing the singularity at $(0,0)$ and generalizing to all rational solutions, we obtain the following bielliptic genus 2 curve:

$$C : y^2 = x^6 + x^2 + 1,$$

with associated elliptic curves:

$$E_1 : y^2 = x^3 + x + 1,$$
$$E_2 : y^2 = x^3 + x^2 + 1.$$

Let ∞^+ and ∞^- be the two points at infinity on C.

PROPOSITION 5.1. *$C(\mathbb{Q})$ consists of the 8 points* $\{(0, \pm 1), (\pm\frac{1}{2}, \pm\frac{9}{8}), \infty^+, \infty^-\}$.

E_1 and E_2 are 496A1 and 248A1 from Cremona's tables. Both E_1 and E_2 have rank 1 over $\mathbb{Q}$, generated by the points (0,1) and (0,1). Both elliptic curves have bad reduction at 2 and 31. Since $x^6 + x^2 + 1$ has no rational factors, $J(\mathbb{Q})$, $E_1(\mathbb{Q})$, and $E_2(\mathbb{Q})$ contain no 2-torsion. One also observes that

$$[(0,1) - (0,-1)] = \varphi((0,1) \times 0) \notin [2]J(\mathbb{Q})$$

and

$$\varphi_{1*} \times \varphi_{2*}([(0,1) - \infty^+]) = (0,1) \times (0,1) \notin 2(E_1 \times E_2)(\mathbb{Q}).$$

It follows that $J(\mathbb{Q})/\varphi((E_1 \times E_2)(\mathbb{Q}))$ has two elements, which can be represented by 0 and $[(0,1) - \infty^+]$.

Let us choose $P = \infty^+$ for our basepoint. Then our two embeddings of C in J are $C_{\infty^+,0}$ and $C_{(0,1),0} = C_{\infty^+,[(0,1)-\infty^+]}$; for notational convenience we will call these curves C_1 and C_2, and we carry this notation over to D_1, D_2, F_1, and F_2.

5.1. Equations for F_1. Note that $e_1(\infty^+, 0) = \varphi_1(\infty^+) - \varphi_{1*}(0) = 0_{E_1}$. Thus we can let $d = 0_{E_1}$ and $g = \mathrm{Id}$. Then

$$F_1 : Y^2 = h_1(Z) = [2x]_{E_1}(Z) = \frac{Z^4 - 2Z^2 - 8Z + 1}{4(Z^3 + Z + 1)}.$$

Note the rational Weierstrass point at infinity, as well as the solutions $(0, \pm\frac{1}{2})$. This curve has bad reduction at 2 and 31.

5.2. Equations for F_2. Note that $e_2((0,1), 0) = \varphi_2((0,1)) - \varphi_{2*}(0) = 0_{E_2}$. Switching the roles of E_1 and E_2 we can let $d = 0_{E_2}$ and $g = \mathrm{Id}$. Then

$$F_2 : Y^2 = h_2(Z) = [2x]_{E_2}(Z) = \frac{Z^4 - 8Z - 4}{4(Z^3 + Z^2 + 1)}.$$

Note the rational Weierstrass point at infinity. This curve has bad reduction at 2 and 31.

5.3. Bounding the rational points. We will defer certain calculations regarding Mordell-Weil groups until Chapter III. Other calculations have already been performed in Chapter I.

We start with the curve F_1. For convenience, we shift to the equation:

$$F_1' : Y'^2 = h'_1(Z) = (Z^4 - 2Z^2 - 8Z + 1)(Z^3 + Z + 1).$$

Note that this is the equation for the curve from the example at the end of Chapter I. We conclude that $F_1'(\mathbb{Q}) = \{(0,1), (0,-1), \infty\}$.

We tackle F_2 next. Let $\infty \in F_2(\mathbb{Q})$ be the rational Weierstrass point on F_2, and let J_2 be the Jacobian of F_2. We will consider F_2 to be embedded in J_2 by the map $Q \mapsto [Q - \infty]$. By lemma 4.2 we see that $J_2(\mathbb{Q}) \approx \mathbb{Z}/2\mathbb{Z}$. Thus, if $[Q - \infty] \in J_2(\mathbb{Q})$, then Q is a Weierstrass point of C. Since the only rational Weierstrass point is ∞, we find that $F_2(\mathbb{Q}) = \{\infty\}$.

Finally, note that the maps $D_1 \to F_1$, $D_2 \to F_2$ are degree 2 maps. Thus, the 3 rational points on F_1 and the 1 rational point on F_2 tell us that there are at most 6 rational points on D_1 and 2 rational points on D_2. It follows that there are at most 8 rational points on C. But we have named 8 rational points on C. This completes the proof of Proposition 5.1.

CHAPTER 3

The Mordell-Weil group

1. Introduction

In Chapters I and II we quoted results concerning the structure of the Mordell-Weil groups of the Jacobians of the curves

$$F_1 : \; y^2 = (x^4 - 2x^2 - 8x + 1)(x^3 + x + 1),$$
$$F_2 : \; y^2 = (x^4 - 8x - 4)(x^3 + x^2 + 1).$$

Our goal in this chapter is to prove these results.

2. Background

Let K be a number field, the completion of a number field at a finite or infinite valuation, or a finite field of odd characteristic. Choose an algebraic closure $\overline{K}$ of K. Let F/K be a complete non-singular hyperelliptic curve of genus g. For our purposes it will suffice to assume that F has a plane model $y^2 = f(x)$ where $f(x) \in K[x]$ is a separable polynomial of degree $2g+1$. A model of this form is non-singular in the affine plane and we identify affine points (x, y) in this model with the corresponding points of F. In addition to the affine points there is one $\overline{K}$-valued point at infinity, which we will call ∞; the point ∞ is a K-rational Weierstrass point on F. Note that the hyperelliptic involution ρ on F takes an affine point $P = (x, y) \in F(\overline{K})$ to the point $\rho(P) = (x, -y)$ and that the affine Weierstrass points in $F(\overline{K})$ are exactly those points for which $y = 0$.

Let $J = \mathrm{Jac}(F)$ be the Jacobian of F. Since F has a K-rational point, every K-rational divisor class contains a K-rational divisor. In fact, for every divisor class $a \in J(K)$ we can write $a = [D - g\infty]$, where D is an effective K-rational divisor of degree g. Note that $P + \rho(P) \sim 2\infty$ for any point $P \in F(\overline{K})$. We will call an effective K-rational divisor D **standard** if $D - P - \rho(P)$ is not effective for every $P \neq \infty$; a simple application of the Riemann-Roch theorem shows that in every K-rational divisor class of degree g there is a unique standard divisor. In particular, every divisor class in $J(K)$ has a unique representation of the form $[D - d\infty]$ where D is a standard affine divisor of degree $d \leq g$.

The set of K-rational effective affine divisors on F can be identified with the set of non-zero ideals of $K[x, y]/(y^2 - f(x))$. Under this identification, maximal ideals correspond to the sum over galois conjugates $\sum P^\sigma$ of a single point $P \in F(\overline{K})$ where each point in the sum occurs only once; furthermore, depending on whether $y(P) \in \overline{K}$ is contained in the field $K(x(P))$ or not, the maximal ideal associated to $\sum P^\sigma$ can be written in either the form $(h(x), y - k(x))$ or $(h(x), y^2 - k(x))$. Note that the corresponding divisor is standard in the first case and not standard in the second. In either case, if $(h(x), y^n - k(x))$ is maximal then h is irreducible. We will call a divisor **maximal** if it is K-rational, effective, affine, and corresponds to a maximal ideal.

We are primarily interested in ideals of the form $(h(x), y^n - k(x))$ and will write $\{h(x), y^n - k(x)\}$ for the corresponding divisor. The degree of $(h(x), y^n - k(x))$ is $n \deg(h)$. To fix representations we will always assume that $h(x)$ is a monic polynomial. The polynomial $k(x)$ is only defined up to elements of the radical of the ideal generated by $h(x)$; if we assume $h(x)$ is separable then we can fix $k(x)$ by requiring that its degree be less than that of $h(x)$. If $h(x)$ is separable, it is clear that $\{h(x), y-k(x)\}$ is a standard divisor; conversely, any standard affine divisor can be written as $\{h(x), y-k(x)\}$ for some separable polynomial $h(x)$. In fact, if D is a standard affine divisor, then

$$h(T) = \prod_{P \in D} (T - x(P))$$

and the polynomial $k(x)$ can be determined by the Chinese Remainder Theorem. Note that for the more general divisor $D = \{h(x), y^n - k(x)\}$, the above product yields $h(T)^n$.

2.1. 2-torsion. Suppose $f(x)$ factors over K as $f(x) = h(x)h'(x)$ and let d be the degree of h. Since the divisor of h is

$$(h) = 2\{h(x), y\} - 2d\infty,$$

the divisor class $[\{h(x), y\} - d\infty]$ is an element of $J(K)[2]$; furthermore, since

$$(y) = \{f(x), y\} - (2g+1)\infty,$$

we see that $[\{h(x), y\} - d\infty]$ represents the same 2-torsion point as $[\{h'(x), y\} - (2g+1-d)\infty]$.

On the other hand, let $a \in J(K)[2]$ and let $[D - d\infty]$ be the unique representation such that D is a standard affine divisor of degree $d \leq g$. Since a is 2-torsion and since ρ_* acts as -1 on J, we conclude that $\rho_*(D) = D$. Thus, for every point P in the support of D, $\rho(P)$ must also be in the support of D. Given the restrictions on D, this means that D is supported on affine Weierstrass points, each of which occurs with multiplicity at most 1. We see that, up to a constant factor, we can express any K-rational 2-torsion point in the form $[\{h(x), y\} - d\infty]$ for exactly one polynomial $h(x)$ dividing $f(x)$ of degree less than or equal to g. In particular, $\#J(K)[2]$ is equal to half the total number of (monic) factors of $f(x)$ over K and the dimension of $J(K)[2]$ as an $\mathbb{F}_2$-vector space is one less than the number of irreducible factors of $f(x)$ over K.

3. The (x-T) map

We next describe an efficient method for determining whether a point $a \in J(K)$ is contained in $2J(K)$. This algorithm is specific to the case of a hyperelliptic curve with K-rational Weierstrass point.

Fix the plane model $y^2 = f(x)$ for F, and write $f = \prod_{i=1}^{r} f_i$ where each f_i is irreducible over K. By choosing a root $\alpha_i \in \overline{K}$ for each f_i, we can identify the algebra $K[T]/f(T)$ with the product of fields $\prod K(\alpha_i)$ by the homomorphism

$$T \longmapsto (\alpha_1, \ldots, \alpha_r).$$

For convenience, we define $L = K[T]/f(T)$ and $K_i = K(\alpha_i)$. We also give a name to the Weierstrass point $W_i = (\alpha_i, 0) \in F(K_i)$ whose x-coordinate is our chosen root of f_i.

Let D be a divisor on F which is rational over K. If, in addition, the support of D avoids the Weierstrass points of F, we will call D a good divisor. The set of good divisors forms a group under addition and the good maximal divisors are a generating set.

Next we define a homomorphism from the group of good divisors to L^* known as the $(x-T)$ map. Let $D = \{h(x), y^n - k(x)\}$ be a good maximal divisor where h is monic of degree d. Define $(x-T)(D)$ to be the element of L^* given by

$$(x-T)\left(\{h(x), y^n - k(x)\}\right) = (-1)^{dn} h(T)^n.$$

We extend the $(x-T)$ map to the entire group of good divisors by linearity. Note that we can rewrite the right hand side of the previous equation as

$$(-1)^{dn} h(T)^n = (-1)^{dn} \prod_{P \in D} (T - x(P)) = \prod_{P \in D} (x(P) - T),$$

where the product takes place in $\overline{K}[T]/f(T)$. Thus, we have the alternate definition

$$(x-T)\left(\sum m_i P\right) = \prod (x(P)-T)^{m_i}$$

from which the $(x-T)$ map gets its name. In general, the first definition is more convenient for computation, since one can work entirely in L^*.

LEMMA 3.1. *The $(x-T)$ map on good divisors induces a well-defined homomorphism*

$$(x-T) : \mathrm{Pic}(F)(K) \longrightarrow L^*/L^{*2}.$$

PROOF. See [**17**, lemma 2.1]. Since the proof is instructive, we repeat it for the reader.

Every K-rational divisor is linearly equivalent to a K-rational divisor which misses any given finite set. It follows that every K-rational divisor class contains a good divisor.

Next, let M be a field extension of K and let s be a function on F defined over M. We can extend s to divisors whose support avoids the zeros and poles of s by

$$s\left(\sum m_i P\right) = \prod s(P)^{m_i} \in \overline{M}^*.$$

If D is an M-rational divisor then $s(D) \in M^*$. Furthermore, if s and s' are two functions on F whose divisors are supported on disjoint sets, then Weil reciprocity tells us that $s((s')) = s'((s))$. (See, for example [**21**, ex. II.11])

If we follow the $(x-T)$ map on good divisors by projection onto the i^{th} factor we get the map $(x-\alpha_i)$ as defined above. Note that $(x-\alpha_i)$ is defined over K_i. Suppose D and D' are linearly equivalent good divisors, say $D-D' = (s)$, then

$$(x-\alpha_i)(D-D') = (x-\alpha_i)((s)) = s((x-\alpha_i)) = s(2W_i - 2\infty) = s(W_i-\infty)^2 \in K_i^{*2}.$$

It follows that $(x-T)(D-D') \in L^{*2}$; this shows that the $(x-T)$ map is well-defined on K-rational divisor classes. □

We end this section by quoting some useful results from [**17**].

PROPOSITION 3.2. *The $(x-T)$ map induces an injective homomorphism*

$$(x-T) : J(K)/2J(K) \longrightarrow L^*/L^{*2}.$$

PROOF. See [**17**, theorem 1.2]. □

PROPOSITION 3.3.

(i) $(x-T)([\infty]) = 1$.
(ii) *Suppose $f(x)$ factors over K as $f(x) = h(x)h'(x)$ where $h(x)$ is a polynomial of degree d. Then $(x-T)([\{h(x),y\}]) = (-1)^d h(T) + (-1)^{1-d} h'(T)$.*

PROOF. See [**17**, lemma 2.2]. □

EXAMPLE 3.4. We now do a few calculations which will be useful in the sequel. Let $K=\mathbb{Q}$ and let F_1 be the genus 3 curve $y^2 = (x^4-2x^2-8x+1)(x^3+x+1)$. Let $K_1 = \mathbb{Q}[T]/(T^4-2T^2-8T+1)$, $K_2 = \mathbb{Q}[T]/(T^3+T+1)$, and $L = K_1 \times K_2 = \mathbb{Q}[T]/((T^4-2T^2-8T+1)(T^3+T+1))$. Let $T_1 = [\{x^3+x+1, y\} - 3\infty]$, and let $U_1 = [(0,1)-\infty]$.

Using the preceding propositions, we calculate the image of T_1 and U_1.

$$\begin{aligned}
(x-T)(T_1) &= -(T^3+T+1)+(T^4-2T^2-8T+1) && \in L^*/L^{*2}\\
&= (\ -(T^3+T+1)\ ,\ (T^4-2T^2-8T+1)\ ) && \in {K_1}^*/{K_1}^{*2}\times {K_2}^*/{K_2}^{*2}\\
&= (\ -((T^3-T-1)/2)^2\ ,\ (3T^2+1)^2\ ) && \in {K_1}^*/{K_1}^{*2}\times {K_2}^*/{K_2}^{*2}\\
&= (-1,1). && \in {K_1}^*/{K_1}^{*2}\times {K_2}^*/{K_2}^{*2}\\
(x-T)(U_1) &= -T && \in L^*/L^{*2}\\
&= (-T,-T) && \in {K_1}^*/{K_1}^{*2}\times {K_2}^*/{K_2}^{*2}
\end{aligned}$$

EXAMPLE 3.5. Let $K=\mathbb{Q}$ and let F_2 be the genus 3 curve $y^2=(x^4-8x-4)(x^3+x^2+1)$. Let K_1, K_2, and L be defined as in the previous example. We note that $\mathbb{Q}[T]/(T^4-2T^2-8T+1)\cong\mathbb{Q}[R]/(R^4-8R-4)$ by the map $R=\frac{1}{2}T^2-\frac{1}{2}$. Similarly, $\mathbb{Q}[T]/(T^3+T+1)\cong\mathbb{Q}[R]/(R^3+R^2+1)$ by the map $R=-T^2-1$. Thus, the "$(x-R)$" map can also be interpreted as taking values in L^*. The image of $T_2=[\{x^3+x^2+1,y\}-3\infty]$ is

$$\begin{aligned}
(x-R)(T_2) &= -(R^3+R^2+1)+(R^4-8R-4) && \in L^*/L^{*2}\\
&= (\ -(R^3+R^2+1)\ ,\ (R^4-8R-4)\ ) && \in {K_1}^*/{K_1}^{*2}\times {K_2}^*/{K_2}^{*2}\\
&= (\ -(T^3+T+1)\ ,\ (10T^2-T+7)\ ) && \in {K_1}^*/{K_1}^{*2}\times {K_2}^*/{K_2}^{*2}\\
&= (\ -((T^3-T-1)/2)^2\ ,\ (T^2-3T+1)^2\ ) && \in {K_1}^*/{K_1}^{*2}\times {K_2}^*/{K_2}^{*2}\\
&= (-1,1). && \in {K_1}^*/{K_1}^{*2}\times {K_2}^*/{K_2}^{*2}
\end{aligned}$$

4. Summary of calculation

Terminology. Assume the following definitions.

$f_1(x)$ $= (x^4-2x^2-8x+1)(x^3+x+1)$.
F_1 = Nonsingular curve over $\mathbb{Q}$ birational to $y^2=f_1(x)$.
J_1 = Jacobian of F_1 over $\mathbb{Q}$.
T_1 $= [\{x^3+x+1,y\}-3\infty]\in J_1(\mathbb{Q})$.
U_1 $= [(0,1)-\infty]\in J_1(\mathbb{Q})$.

$f_2(x)$ $= (x^4-8x-4)(x^3+x^2+1)$.
F_2 = Nonsingular curve over $\mathbb{Q}$ birational to $y^2=f_2(x)$.
J_2 = Jacobian of F_2 over $\mathbb{Q}$.
T_2 $= [\{x^3+x^2+1,y\}-3\infty]\in J_2(\mathbb{Q})$.

K_1 $= \mathbb{Q}[T]/(T^4-2T^2-8T+1)$
K_2 $= \mathbb{Q}[T]/(T^3+T+1)$
L $= \mathbb{Q}[T]/f_1(T)\cong K_1\times K_2$
L_p $= \mathbb{Q}_p[T]/f_1(T)$ for any finite or infinite prime p of $\mathbb{Q}$

Summary of Results. We will show the following:

LEMMA 4.1 (Reduction information).

(i) *$J_1(\mathbb{Q})_{tor}\approx\mathbb{Z}/2\mathbb{Z}$ and is generated by T_1.*
(ii) *$J_2(\mathbb{Q})_{tor}\approx\mathbb{Z}/2\mathbb{Z}$ and is generated by T_2.*
(iii) *U_1 has infinite order, and U_1 is neither the double nor the triple of a point in $J_1(\mathbb{Q})$.*

LEMMA 4.2 (Rank information).

(i) $J_1(\mathbb{Q}) \approx \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(ii) $J_2(\mathbb{Q}) \approx \mathbb{Z}/2\mathbb{Z}$.

5. Reduction information

We can obtain a large amount of information by reducing J_1 and J_2 at various primes of good reduction. For both F_1 and F_2, the primes of bad reduction of the given hyperelliptic model are 2 and 31; the curves and their Jacobians have good reduction at all other primes.

In fact, we need only a little information to determine the torsion on J_1. The number of F_3-valued points of J_1 is $48 = 2^4 \cdot 3$ and the number of F_5-valued points is $112 = 2^4 \cdot 7$. The ramification degree of $\mathbb{Q}$ at any prime is 1; in particular, it is less than $p-1$ for any odd prime p. Thus the torsion of $J_1(\mathbb{Q})$ injects under the reduction map at both 3 and 5. Since the gcd of 48 and 112 is 2^4 we see that the torsion of $J_1(\mathbb{Q})$ must be 2-power order. But the only 2-torsion point in $J_1(\mathbb{Q})$ is T_1, and the $(x-T)$ map shows that it is not a double. So the only non-trivial torsion point in $J_1(\mathbb{Q})$ is T_1. This shows the first part of lemma 4.1.

A similar argument shows that the only non-trivial torsion point on $J_2(\mathbb{Q})$ is T_2; in this case, the number of F_3-valued points of J_2 is $24 = 2^3 \cdot 3$ while the number of F_5-valued points is again $112 = 2^4 \cdot 7$. This is the second part of lemma 4.1.

Finally, since U_1 is not in the torsion subgroup, it must be of infinite order. The reduction of U_1 at 3 has order 12. Since J_1 has 48 F_3-valued points, the reduction of U_1 is not a triple in $J_1(\mathbb{F}_3)$. It follows that U_1 is not a triple over $\mathbb{Q}$. The $(x-T)$ map calculation from the previous example shows that U_1 is not a double over $\mathbb{Q}$. This completes lemma 4.1.

NOTE. Let F be a genus 3 curve defined over the finite field $\mathbb{F}_q$ and let J be its Jacobian. A comparison of the zeta functions of F and J shows that

$$\#J(\mathbb{F}_q) = \frac{1}{6}a^3 + (\frac{1}{2}b - p) \cdot a + \frac{1}{3}c$$
$$\text{where } a = \#F(\mathbb{F}_q),\ b = \#F(\mathbb{F}_{q^2}),\ c = \#F(\mathbb{F}_{q^3}).$$

This is not the most efficient method for counting the number of points on J over a large finite field, but it suffices for small values of q.

6. Rank information

We want to verify that J_1 has rank 1 over $\mathbb{Q}$, and that J_2 has rank 0. Since we know the structure of the $\mathbb{Q}$-rational torsion, it will suffice to show that $J_1(\mathbb{Q})/2J_1(\mathbb{Q})$ is generated by U_1 and T_1 and that $J_2(\mathbb{Q})/2J_2(\mathbb{Q})$ is generated by T_2. In order to do this we will need to look somewhat more closely at the $(x-T)$ map.

First we will need a few definitions. Let $S = \{2, 31, \infty\}$; as with the proof of the weak Mordell-Weil theorem for $J(K)/nJ(K)$, the set S is chosen to include the primes of bad reduction (2 and 31) and the primes dividing $n = 2$ and infinity. Define $({K_1}^*/{K_1}^{*2})_S$ to be the subgroup of ${K_1}^*/{K_1}^{*2}$ consisting of classes which are unramified outside of S; that is, for every class $[\beta] \in ({K_1}^*/{K_1}^{*2})_S$, the field extension $K_1(\sqrt{\beta})/K_1$ is unramified outside of primes of K_1 lying over primes of S. Note that there are only finitely many quadratic extensions of K_1 with the given ramification restriction, so $({K_1}^*/{K_1}^{*2})_S$ is finite. Similarly, we define $({K_2}^*/{K_2}^{*2})_S$ to be the subgroup of ${K_2}^*/{K_2}^{*2}$ consisting of classes which are unramified outside of S and we let $(L^*/L^{*2})_S$ be the subgroup of $L^*/L^{*2} = {K_1}^*/{K_1}^{*2} \times {K_2}^*/{K_2}^{*2}$ corresponding to $({K_1}^*/{K_1}^{*2})_S \times ({K_2}^*/{K_2}^{*2})_S$. The groups $({K_2}^*/{K_2}^{*2})_S$ and $(L^*/L^{*2})_S$ are also finite. Finally, note that the norm maps from K_1 and K_2 to $\mathbb{Q}$ induce a norm map from $(L^*/L^{*2})_S$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

PROPOSITION 6.1. *The image of the injective map*

$$(x - T) : J(\mathbb{Q})/2J(\mathbb{Q}) \longrightarrow L^*/L^{*2}$$

is contained in the kernel of the norm from $(L^*/L^{*2})_S$ *to* $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

PROOF. This follows from theorems 1.1 and 1.2 in [**17**]. □

Let H be the kernel of the norm from $(L^*/L^{*2})_S$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ and let v be a valuation of $\mathbb{Q}$. Consider the diagram

$$\begin{array}{ccccc} 0 \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \xrightarrow{(x-T)} & H \subset (L^*/L^{*2})_S \\ & \downarrow & & \downarrow \beta_v \\ 0 \longrightarrow & J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) & \xrightarrow{(x-T)_v} & {L_v}^*/{L_v}^{*2} \end{array}$$

In this diagram β_v is the restriction to H of the natural map from L^*/L^{*2} to ${L_v}^*/{L_v}^{*2}$ and $(x-T)_v$ is the $(x-T)$ map over $\mathbb{Q}_v$.

Let $\mathrm{Im}(x-T)_v$ denote the image of the $(x-T)_v$ map. It is clear that $J(\mathbb{Q})/2J(\mathbb{Q})$ is contained in $\beta_v^{-1}(\mathrm{Im}(x-T)_v)$ for each v. In order to show that a given set of divisor classes generates $J(\mathbb{Q})/2J(\mathbb{Q})$, it will suffice to show that this same set generates the intersection

$$\bigcap_v \beta_v^{-1}(\mathrm{Im}(x-T)_v)$$

where v ranges over the set of all valuations of $\mathbb{Q}$. Since H is a finite group, the intersection is stable after a finite number of steps. In our case $\beta_2^{-1}(\mathrm{Im}(x-T)_2) \cap \beta_{31}^{-1}(\mathrm{Im}(x-T)_{31})$ will suffice.

Computing the group H and the maps β_v are both relatively straightforward. On the other hand, one generally has to search for generators of $J(\mathbb{Q}_v)/2J(\mathbb{Q}_v)$. The following proposition lets us know when the search is complete.

PROPOSITION 6.2. *Let K be a finite extension of $\mathbb{Q}_p$ and let A be an abelian variety of dimension g defined over K.*

(i) *If $p \neq 2$, then* $\#A(K)/2A(K) = \#A(K)[2]$.
(ii) *If $p = 2$, then* $\#A(K)/2A(K) = 2^{g[K:\mathbb{Q}_p]} \cdot \#A(K)[2]$.
(iii) $\#A(\mathbb{R})/2A(\mathbb{R}) = 2^{-g} \cdot \#A(\mathbb{R})[2]$.

PROOF. This is a special case of propositions 2.4 and 2.5 in [**18**]. □

REMARK 6.3. The intersection $\bigcap \beta_v^{-1}(\mathrm{Im}(x-T)_v)$ can be related to the 2-Selmer group $S^2(J,K)$. The process described above is a truncated version of the algorithm given in [**17**] for computing the 2-Selmer group on Jacobians of hyperelliptic curves with a rational Weierstrass point. For a description of a general approach to computing Selmer groups of Jacobians, see [**18**].

6.1. Computing modulo squares. Before we get into the actual rank calculations it would be appropriate to say a few words about computing in K^*/K^{*2} for some of the fields K we are working with. We will not add anything new to the topic, but hopefully it will be a useful discussion for the reader who is interested in performing actual computations.

Note that the groups K^*/K^{*2} and $J(K)/2J(K)$ have natural $\mathbb{F}_2$-vector space structures; this is the context in which we will discuss dimensions, generators, a basis, etc. We will also frequently use the notation $\langle b_1, \ldots, b_n \rangle$ to denote the subspace generated by the elements $b_1, \ldots, b_n$.

Finite Fields. Clearly the easiest case is when K is a finite field with q elements. If q is even then every element is a square. If q is odd then there is one non-trivial class modulo squares; $a \in K^*$ is a square if and only if $a^{(q-1)/2} = 1$.

Extensions of $\mathbb{Q}_p$, p odd. The case where K is a finite extension of $\mathbb{Q}_p$, p odd, is also straightforward. Fix a uniformizing element $\pi \in K$. Then $K^*/K^{*2} = \langle \pi, u\rangle$, where u is any non-square unit in K. Since all non-square units in K are equivalent class modulo squares, this basis is well-defined. On the other hand, each choice of uniformizing element modulo π^2 yields a different basis.

We can express an element $a \in K^*$ on the basis $\{\pi, u\}$ in the following way: let n be the valuation of a, so that $a = \pi^n \cdot a'$ for some unit a'. The class of π^n modulo squares is clearly determined by $n \pmod 2$, while the class of a' is determined by the image of a' in the residue field.

Extensions of $\mathbb{Q}_2$. When K is a finite extension of $\mathbb{Q}_2$ we must work a bit harder. Let k be the residue field of K and let (e,f) be the ramification index and residue field degree of K over $\mathbb{Q}_2$. Thus, $[K : \mathbb{Q}_2] = ef$ and $[k : \mathbb{F}_2] = f$. Fix a uniformizing element $\pi \in K^*$ and let $b_1, \ldots, b_f$ be a set of elements in K whose residues form a basis for k as a vector space over $\mathbb{F}_2$. We leave it as an exercise to the reader to show that K^*/K^{*2} has dimension $ef + 2$ and that the $ef + 1$ elements

$$\pi, \quad 1 + b_1\pi, \ldots, 1 + b_f\pi, \quad 1 + b_1\pi^3, \ldots, 1 + b_f\pi^3, \quad \ldots, \quad 1 + b_1\pi^{2e-1}, \ldots, 1 + b_f\pi^{2e-1}$$

are independent modulo squares. We complete this basis with a non-square element μ in $1+(\pi)^{2e} = 1 + (4)$. Note that if μ and μ' are two non-squares which are 1 mod 4 then μ and μ' are equivalent mod squares. In practice it is not necessary to choose a specific value for μ.

Let $a \in K^*$, and let $v(a)$ be the valuation of a. Let $q = 2^f$ be the size of the residue field. If $v(a - 1) = m > 0$, define $w(a) = (a - 1)/\pi^m$. The following algorithm can be used to recursively express any element $a \in K^*$ on the above basis. At each step we simplify a (generally by increasing the valuation of $a - 1$) and record the basis elements involved in the transformation, if any.

condition	action	result
$v(a) = n \neq 0$	Divide a by π^n and record change.	$v(a) = 0$
$v(a) = 0 = v(a-1)$	Divide a by a^q. (No change modulo squares.)	$v(a-1) > 0$
$0 < v(a-1) < 2e$, $m = v(a-1)$ even	Divide a by $(1 + w(a)^{q/2}\pi^{m/2})^2$. (No change modulo squares.)	$v(a-1) > m$
$0 < v(a-1) < 2e$, $m = v(a-1)$ odd	Find $\alpha_i \in \{0,1\}$ such that $w(a) \equiv \sum \alpha_i b_i \pmod{\pi}$. Divide a by $\prod(1 + b_i\pi^m)^{\alpha_i}$ and record change.	$v(a-1) > m$
$v(a-1) = 2e$	Let $b = (a-1)/4$. If $\sum_{i=1}^{f-1} b^i \equiv 0 \pmod{\pi}$ then a is a square, else divide a by μ and record change. In either case, a is now a square.	Done.
$v(a-1) > 2e$,	Note that a is a square.	Done.

We make two notes about the above algorithm. First, the condition "If $\sum_{i=1}^{f-1} b^i \equiv 0 \pmod{\pi}$ … " in the second-to-last case uses the fact that $b = (a-1)/4$; attempting to use the more general expression $b = (a-1)/\pi^{2e}$ would require a much more complex conditional.

Second, all of the computations except for the initial division by a power of π can be done modulo 4π (or modulo 8 if that is more convenient). In particular, we only need to specify π and $b_1, \ldots, b_f$ to this accuracy.

Number Fields. Finally, we consider the case where K is a number field. If K has class number 1 and if we know a basis of the fundamental units and roots of unity, then it is fairly straightforward to determine the class of an element $a \in K^*$: First factor the fractional ideal (a) as a product of (principal) prime ideals. Divide a by the corresponding product of prime elements to get a unit a'. Next, express a' as a product of powers of the fundamental units modulo roots of unity; this can be done using the logarithms of embeddings of K in $\mathbb{C}$. Finally, divide a' by this product of fundamental units and determine whether the resulting root of unity is a square.

For our present purposes it will suffice to assume that the class number is 1, and we will not discuss the alternative in detail. The calculation of fundamental units and roots of unity can be performed by PARI/GP for number fields of modest size, so this requirement will not introduce significant difficulty.

6.2. Rank verification for F_1. We would like to verify that $J_1(\mathbb{Q})/2J_1(\mathbb{Q})$ is generated by T_1 and U_1. Recall the definitions.

$$\begin{aligned}
f_1(x) &= (x^4 - 2x^2 - 8x + 1)(x^3 + x + 1).\\
F_1 &= \text{Nonsingular curve over } \mathbb{Q} \text{ birational to } y^2 = f_1(x).\\
J_1 &= \text{Jacobian of } F_1 \text{ over } \mathbb{Q}.\\
T_1 &= [\{x^3 + x + 1, y\} - 3\infty] \in J_1(\mathbb{Q}).\\
U_1 &= [(0,1) - \infty] \in J_1(\mathbb{Q}).
\end{aligned}$$

$$\begin{aligned}
K_1 &= \mathbb{Q}[T]/(T^4 - 2T^2 - 8T + 1)\\
K_2 &= \mathbb{Q}[T]/(T^3 + T + 1)\\
L &= \mathbb{Q}[T]/f_1(T) \cong K_1 \times K_2\\
L_p &= \mathbb{Q}_p[T]/f_1(T)
\end{aligned}$$

We start by recording various pieces of information about the number fields K_1 and K_2. The majority of this information comes from PARI/GP.

field	K_1	K_2
discriminant	-1984	-31
Minkowski bound	≈ 5.2	≈ 1.6
class number	1	1
(r_1, r_2)	$(2,1)$	$(1,1)$
rank of unit group	2	1
torsion in unit group	$\langle -1 \rangle$	$\langle -1 \rangle$
(e,f) for primes over 2	$(4,1)$	$(1,3)$
(e,f) for primes over 31	$(2,1),(1,2)$	$(2,1),(1,1)$

The fact that both K_1 and K_2 have trivial class group simplifies the computation of $({K_1}^*/{K_1}^{*2})_S$ and $({K_2}^*/{K_2}^{*2})_S$. In fact, we see that these groups are generated by -1, the fundamental units, and by generators for the primes over 2 and 31. Specifically, a basis for ${K_1}^*/{K_1}^{*2}$ is given by

name	element	norm	description
-1	-1	1	root of unity
u_1	T	1	fundamental unit
u_2	$(T^3 - T^2 - T - 3)/4$	-1	fundamental unit
$\mathfrak{p}_2$	$(T^3 + T^2 - T - 9)/4$	-2	$(e,f) = (4,1)$
$\mathfrak{p}_{31}$	$(-T^3 + T + 2)/2$	-31	$(e,f) = (2,1)$
$\mathfrak{p}'_{31}$	$-T^2 + 3T + 3$	31^2	$(e,f) = (1,2)$

	p_{31}	p'_{31}	q_{31}	q'_{31}
number field	K_1	K_1	K_2	K_2
completion	$\mathbb{Q}_{31}(\sqrt{31})$	$\mathbb{Q}_{31}(i)$	$\mathbb{Q}_{31}(\sqrt{-31})$	$\mathbb{Q}_{31}$
image of T	$14+(p_{31})$	$17+7i+(p'_{31})$	$14+(q_{31})$	$3+(q'_{31})$
basis mod squares	$-1, p_{31}$	$4+i, p'_{31}$	$-1, q_{31}$	$-1, q'_{31}$

TABLE 1. Description of L_{31}

	p_{31}	p'_{31}	q_{31}	q'_{31}
T_1	-1	1	1	1
U_1	-1	1	-1	1
$[(1,\sqrt{-24})-\infty]$	1	$4+i$	1	-1

TABLE 2. Image of $(x-T)_{31}$ for J_1

and a basis for ${K_2}^*/{K_2}^{*2}$ is given by

name	element	norm	description
-1	-1	-1	root of unity
v_1	T	-1	fundamental unit
2	2	8	$(e,f)=(1,3)$
q_{31}	T^2-3T+1	31	$(e,f)=(2,1)$
q'_{31}	$T-3$	-31	$(e,f)=(1,1)$

From the above bases for ${K_1}^*/{K_1}^{*2}$ and ${K_2}^*/{K_2}^{*2}$ we easily obtain a basis for L^*/L^{*2}. Examining the norm, we see that its kernel, H, has dimension 8 generated by the elements

$$\begin{array}{llll} h_1=-1\times 1, & h_2=-u_1\times -v_1, & h_3=u_1\times 1, & h_4=-u_2\cdot p_2\times 2, \\ h_5=u_2\times v_1, & h_6=1\times -q_{31}\cdot q'_{31}, & h_7=p'_{31}\times 1, & h_8=p_{31}\times q'_{31}. \end{array}$$

The h_i have been chosen to make the linear algebra which follows as transparent as possible. In particular, h_1 and h_2 are the images of T_1 and U_1 under the $(x-T)$ map.

Calculations at 31. From the prime decomposition of 31 in K_1 and K_2 we see that L_{31} is isomorphic to the product of four local fields, two of which are localizations of K_1 and two of K_2. These local fields are described in table 1. We use the chosen generator of each prime ideal lying over 31 as the uniformizing element in the corresponding local field. In each case, a basis for the multiplicative group modulo squares is given by a non-square unit and the uniformizing element. In order to aid any reader interested in following along with the computations, table 1 also specifies the value of T modulo the maximal ideal in each local field.

In order to calculate $\beta_{31}^{-1}(\mathrm{Im}(x-T)_{31})$ we will want to know the image of $(x-T)_{31}$ and of β_{31}. From the prime decomposition of 31 we see that $f_1(x)$ has 4 factors over $\mathbb{Q}_{31}$. Since the dimension of $J_1(\mathbb{Q}_{31})/2J_1(\mathbb{Q}_{31})$ equals the dimension of $J_1(\mathbb{Q}_{31})[2]$ (Proposition 6.2), we see that to specify $\mathrm{Im}(x-T)_{31}$ we will need 4-1=3 independent divisor classes. We find that T_1 and U_1 remain independent over $\mathbb{Q}_{31}$, and a small amount of searching uncovers $[(1,\sqrt{-24})-\infty]$. The image of these elements in ${L_{31}}^*/{L_{31}}^{*2}$ is described in table 2.

Note that table 3 describes the image of β_{31}. One easily checks that the subspace $\langle h_1,h_2,h_3,h_4,h_5\rangle$ maps onto the image of $(x-T)_{31}$ and that the kernel of β_{31} in H has dimension 2. Counting dimensions we find that the subspace generated by h_1 through h_5 is the full inverse image of $\mathrm{Im}(x-T)_{31}$ in H. From now on we will limit our attention to this subspace.

	p_{31}	p'_{31}	q_{31}	q'_{31}
$h_1 = -1 \times 1$	-1	1	1	1
$h_2 = -u_1 \times -v_1$	-1	1	-1	1
$h_3 = u_1 \times 1$	1	1	1	1
$h_4 = -u_2 \cdot p_2 \times 2$	1	1	1	1
$h_5 = u_2 \times v_1$	1	$4+i$	1	-1
$h_6 = 1 \times -q_{31} \cdot q'_{31}$	1	1	q_{31}	$-qc'$
$h_7 = p'_{31} \times 1$	1	p'_{31}	1	1
$h_8 = p_{31} \times q'_{31}$	p_{31}	1	-1	q'_{31}

TABLE 3. Image of β_{31}

	p_2	2
number field	K_1	K_2
completion	$\mathbb{Q}_2(p_2)$	$\mathbb{Q}_2(\zeta), \zeta^7 = 1$
image of T	$1 + p_2^3 + p_2^5 + p_2^6 + p_2^7 + p_2^8 + (p_2)^9$	$2 + 5\zeta + (2)^3$
$b_1, \ldots, b_f$	1	$1, \zeta, \zeta^2$
basis mod squares	$p_2, \eta_1, \eta_3, \eta_5, \eta_7, 5$	$2, 3, 1+2\zeta, 1+2\zeta^2, 5$

TABLE 4. Description of L_2

	p_2	2
T_1	$5\eta_7$	1
U_1	$5\eta_3\eta_5\eta_7$	$(1+2\zeta^2)$
$[\{x^2+2x+57, *\} - 2\infty]$	η_7	1
$[\{x^3+x^2+x+3, *\} - 3\infty]$	η_5	$5(1+2\zeta)(1+2\zeta^2)$

TABLE 5. Image of $(x-T)_2$ for J_1

Calculations at 2. From the prime decomposition of 2 in K_1 and K_2 we see that L_2 is isomorphic to the product of two local fields; these local fields are described in table 4. We use the chosen generator of each prime ideal lying over 2 as the uniformizing element in the corresponding local field. In addition, we define $\eta_i = 1 + p_2^i \in K_1$ and let ζ be a primitive 7^{th} root of unity in K_2. Since the ramification indices of K_1 and K_2 are 4 and 1, the class of units modulo squares is determined modulo $(4p_2) = (p_2)^9$ and $(4 \cdot 2) = (2)^3$, respectively. Table 4 specifies the image of T to this accuracy in both local fields. The residue field degrees of K_1 and K_2 are 1 and 3, respectively, and the reductions of the sets $\{1\}$ and $\{1, \zeta, \zeta^2\}$ form a basis for the corresponding residue field over $\mathbb{F}_2$. We use the basis modulo squares discussed in the section on computation modulo squares.

From the prime decomposition of 2 we see that $f_1(x)$ has 2 factors over $\mathbb{Q}_2$ and that the dimension of $J_1(\mathbb{Q}_2)[2]$ is 1. From proposition 6.2 the dimension of $J_1(\mathbb{Q}_2)/2J_1(\mathbb{Q}_2)$ is $g+1=4$. The divisor classes of T_1 and U_1 remain independent over $\mathbb{Q}_2$, so we need two more independent divisor classes. A computer-assisted search discovered independent $\mathbb{Q}_2$-rational divisors of the form $[\{x^2+2x+57, *\} - 2\infty]$ and $[\{x^3+x^2+x+3, *\} - 3\infty]$. The "$*$" in each of these divisors means a polynomial over $\mathbb{Q}_2$ of the form $y - k(x)$ which we choose not to specify since it is complicated and not relevant to the calculation. The image of $(x-T)_2$ in ${L_2}^*/{L_2}^{*2}$ is described in table 5.

From Table 6 we see that the map β_2 restricted to $\langle h_1, h_2, h_3, h_4, h_5 \rangle$ is injective. With a small amount of work one can verify that the intersection of the image of β_2 with the image of $(x-T)_2$

	p_2	2
$h_1 = -1 \times 1$	$5\eta_7$	1
$h_2 = -u_1 \times -v_1$	$5\eta_3\eta_5\eta_7$	$(1+2\zeta^2)$
$h_3 = u_1 \times 1$	$\eta_3\eta_5$	1
$h_4 = -u_2 \cdot p_2 \times 2$	$5\eta_1\eta_7 p_2$	2
$h_5 = u_2 \times v_1$	η_1	$3 \cdot 5(1+2\zeta^2)$

TABLE 6. Image of β_2

is generated by the images of $h_1 = (x-T)(T_1)$ and $h_2 = (x-T)(U_1)$. Since $\langle h_1, h_2, h_3, h_4, h_5\rangle$ is the inverse image of $\mathrm{Im}(x-T)_{31}$ restricted to H, and since $\langle h_1, h_2\rangle$ is the inverse image of $\mathrm{Im}(x-T)_2$ restricted to $\langle h_1, h_2, h_3, h_4, h_5\rangle$, we see that the intersection in H of $\beta_{31}^{-1}(\mathrm{Im}(x-T)_{31})$ with $\beta_2^{-1}(\mathrm{Im}(x-T)_2)$ is $\langle h_1, h_2\rangle = (x-T)(\langle T_1, U_1\rangle)$. But this is exactly what we wanted to demonstrate, so we are finished.

Unwinding all of the arguments which went into getting here, we see that we have now shown that $J_1(\mathbb{Q})/2J_1(\mathbb{Q})$ is generated by T_1 and U_1, that J_1 has rank 1, and that $J_1(\mathbb{Q}) \approx \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

6.3. Rank verification for F_2. We would like to verify that $J_2(\mathbb{Q})/2J_2(\mathbb{Q})$ is generated by T_2. Recall the definitions.

$f_2(x) \quad = (x^4 - 8x - 4)(x^3 + x^2 + 1)$.
$F_2 \quad$ = Nonsingular curve over $\mathbb{Q}$ birational to $y^2 = f_2(x)$.
$J_2 \quad$ = Jacobian of F_2 over $\mathbb{Q}$.
$T_2 \quad = [\{x^3 + x^2 + 1, y\} - 3\infty] \in J_2(\mathbb{Q})$.

$K_1 \quad = \mathbb{Q}[T]/(T^4 - 2T^2 - 8T + 1) \cong \mathbb{Q}[R]/(R^4 - 8R - 4) \qquad$ where $R = \frac{1}{2}T^2 - \frac{1}{2}$
$K_2 \quad = \mathbb{Q}[T]/(T^3 + T + 1) \cong \mathbb{Q}[R]/(R^3 + R^2 + 1) \qquad$ where $R = -T^2 - 1$
$L \quad = \mathbb{Q}[R]/f_2(R) \cong K_1 \times K_2$
$L_p \quad = \mathbb{Q}_p[R]/f_2(R) \cong (K_1 \times K_2) \otimes \mathbb{Q}_p$

As noted in the examples, the rings K_1, K_2, and L for J_2 are isomorphic to the corresponding rings for J_1. This means that we can use the same bases for L^*/L^{*2}, ${L_{31}}^*/{L_{31}}^{*2}$, and ${L_2}^*/{L_2}^{*2}$; in particular we can use the same basis $h_1, \ldots, h_8$ for the kernel of the norm from L^*/L^{*2} to $\mathbb{Q}^*/\mathbb{Q}^{*2}$. We also see that the maps β_{31} and β_2 are identical.

Calculations at 31. We recall that L_{31} is isomorphic to the product of four local fields, two of which are localizations of K_1 and two of K_2. We retain the choice of basis for ${L_{31}}^*/{L_{31}}^{*2}$ from the discussion of J_1.

From the prime decomposition of 31 we see that $f_2(x)$ has 4 factors over $\mathbb{Q}_{31}$. Since the dimension of $J_2(\mathbb{Q}_{31})/2J_2(\mathbb{Q}_{31})$ equals the dimension of $J_2(\mathbb{Q}_{31})[2]$ (Proposition 6.2), we see that to specify $\mathrm{Im}(x-T)_{31}$ we will need 4-1=3 independent divisor classes. We find that T_2 maps non-trivially, so we will need 2 more independent divisor classes. A small amount of searching uncovers $[(3, \sqrt{1961}) - \infty]$ and $[(2, \sqrt{-52}) - \infty]$. The image of $(x-T)_{31}$ is described in table 7.

Comparing the images of the $(x-T)_{31}$ maps for J_1 and J_2 (tables 2 and 7), we immediately see that they span the same subspace of ${L_{31}}^*/{L_{31}}^{*2}$. We conclude that $\langle h_1, h_2, h_3, h_4, h_5\rangle$ is the full inverse image of $\mathrm{Im}(x-T)_{31}$ in H. From now on we will limit our attention to this subspace.

Calculations at 2. We recall that L_2 is isomorphic to the product of two local fields, the first extending K_1 and the second extending K_2. We retain the choice of basis for ${L_2}^*/{L_2}^{*2}$ from the discussion of J_1.

	p_{31}	p'_{31}	q_{31}	q'_{31}
T_2	-1	1	1	1
$[(3, \sqrt{1961}) - \infty]$	1	$4+i$	1	-1
$[(2, \sqrt{-52}) - \infty]$	-1	$4+i$	-1	-1

TABLE 7. Image of $(x-T)_{31}$ for J_2

	p_2	2
T_2	$5\eta_7$	1
$[(3, \sqrt{1961}) - \infty]$	$\eta_3\eta_7$	5
$[\{x^2+2x+10, *\} - 2\infty]$	η_7	$(1+2\zeta)(1+2\zeta^2)$
$[\{x^2+3x+1, *\} - 2\infty]$	η_3	5

TABLE 8. Image of $(x-T)_2$ for J_2

From the prime decomposition of 2 we see that $f_2(x)$ has 2 factors over $\mathbb{Q}_2$ and that the dimension of $J_2(\mathbb{Q}_2)[2]$ is 1. From proposition 6.2 the dimension of $J_2(\mathbb{Q}_2)/2J_2(\mathbb{Q}_2)$ is $g+1=4$. The divisor class of T_2 maps non-trivially, so we need three more independent divisor classes. A small amount of searching uncovers $[(3, \sqrt{1961}) - \infty]$ and more extensive searching finds $[\{x^2+2x+10, *\} - 2\infty]$ and $[\{x^2+3x+1, *\} - 2\infty]$. Once again, "$*$" means a polynomial over $\mathbb{Q}_2$ of the form $y-k(x)$ which we choose not to specify. The image of $(x-T)_2$ is described in table 8.

We again note that the map β_2 restricted to $\langle h_1, h_2, h_3, h_4, h_5\rangle$ is injective. Comparing tables 6 and 8, one can verify that the intersection of the image of β_2 with the image of $(x-T)_2$ is generated by the image of $h_1 = (x-T)(T_2)$. Since $\langle h_1, h_2, h_3, h_4, h_5\rangle$ is the inverse image of $\mathrm{Im}(x-T)_{31}$ restricted to H, and since $\langle h_1\rangle$ is the inverse image of $\mathrm{Im}(x-T)_2$ restricted to $\langle h_1, h_2, h_3, h_4, h_5\rangle$, we see that the intersection in H of $\beta_{31}^{-1}(\mathrm{Im}(x-T)_{31})$ with $\beta_2^{-1}(\mathrm{Im}(x-T)_2)$ is $\langle h_1\rangle = (x-T)(\langle T_2\rangle)$. This shows that $J_2(\mathbb{Q})/2J_2(\mathbb{Q})$ is generated by T_2, that J_2 has rank 0, and that $J_2(\mathbb{Q}) \approx \mathbb{Z}/2\mathbb{Z}$. This completes the proof of lemma 4.2.

Bibliography

[1] Artin, M., Néron Models, in Cornell, G. & Silverman, J.H. (eds.), *Arithmetic Geometry*, 213–230, Springer-Verlag, New York, 1986.

[2] Cassels, J.W.S. & Flynn, E.V., *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Math. Soc., Lecture Notes, Cambridge Univ. Press, 1996.

[3] Chabauty, C., Sur les points rationnels des courbes algébriques de genre supérieur à l'unité, *Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris* **212** (1941), 882–885.

[4] Coleman, R., Effective Chabauty, *Duke Math. J.* **52** (1985), 765–770.

[5] Coleman, R., Torsion points on curves and p-adic Abelian integrals, *Annals of Mathematics* **121** (1985), 111–168.

[6] Coombes, K.R. & Grant, D.R., On heterogeneous Spaces, *J. London Math. Soc. (2)* **40** (1985), 385–397.

[7] Flynn, E.V., Descent via isogeny in dimension 2, *Acta Arith.* **66** (1994), 23–43.

[8] Flynn, E.V., A flexible method for applying Chabauty's theorem, *Compositio Mathematica* **105** (1997), 1: 79–94.

[9] Flynn, E.V., Poonen, B. & Schaefer, E.F., Cycles of quadratic polynomials and rational points on a genus-two curve, to appear in *Duke Math. J.* 1995.

[10] Freije, M.N., The formal group of the Jacobian of an algebraic curve, *Pacific Journal of Mathematics* **157** (1993), 2: 241–255.

[11] Frey, G. & Kani, E., Curves of genus 2 covering elliptic curves and an arithmetical application, in van der Geer, G., Oort, F. & Steenbrink, J. (eds.), *Arithmetic Algebraic Geometry*, 153–175, Progress in Mathematics **89** Birkh auser, Boston, 1991.

[12] Grant, D.R., A curve for which Coleman's effective Chabauty bound is sharp, *Proc. Amer. Math. Soc.* **122** (1994), 317–319.

[13] Kuhn, R.M., Curves of genus 2 with split Jacobian, *Trans. Amer. Math. Soc.* **307** (1988), 41-49.

[14] McCallum, W., On the method of Coleman and Chabauty, *Math. Ann.* **299** (1994), 3: 565–596.

[15] Milne, J.S., Abelian varieties, in Cornell, G. & Silverman, J.H. (eds.), *Arithmetic Geometry*, 103–150, Springer-Verlag, New York, 1986.

[16] Milne, J.S., Jacobian varieties, in Cornell, G. & Silverman, J.H. (eds.), *Arithmetic Geometry*, 167–212, Springer-Verlag, New York, 1986.

[17] Schaefer, E.F., 2-descent on the Jacobians of hyperelliptic curves, *J. Number Theory* **51** (1995), 219–232.

[18] Schaefer, E.F., Computing a Selmer group of a Jacobian using functions on the curve, to appear in Mathematische Annalen.

[19] Serre, J.-P., Lie Algebras and Lie Groups, *Lecture Notes in Mathematics* **1500** Springer-Verlag, Berlin, 1992.

[20] Shatz, S., Group Schemes, Formal Groups and p-Divisible Groups, in Cornell, G. & Silverman, J.H. (eds.), *Arithmetic Geometry*, 29–78, Springer-Verlag, New York, 1986.

[21] Silverman, J.H., *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

[22] Silverman, J.H., *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.