ABSTRACT

Title of dissertation: Triviality and Nontriviality of Tate-Lichtenbaum Self Pairings

Susan L. Schmoyer
Doctor of Philosophy, 2007

Dissertation directed by: Professor Lawrence C. Washington
Department of Mathematics

Let E be an elliptic curve defined over $\mathbf{F}_q$ and suppose that $E[n] \subset E(\mathbf{F}_q)$. For attacking the elliptic curve discrete logarithm problem it is useful to know when points pair with themselves nontrivially under the Tate-Lichtenbaum pairing. In this thesis we characterize when all points in $E[n]$ have trivial self pairings. This result is expressed in terms of the action of the Frobenius endomorphism on $E[n^2]$. We then generalize this result to Jacobians of algebraic curves of arbitrary genus.

Triviality and Nontriviality of Tate-Lichtenbaum Self Pairings

by

Susan L. Schmoyer

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2007

Advisory Committee:
Professor Lawrence C. Washington, Chair/Advisor
Professor Niranjan Ramachandran
Professor Jeffrey Adams
Professor Thomas Haines
Professor William Gasarch

To Mom and Dad

Acknowledgments

I thank my advisor, Lawrence Washington, for all of the patience, guidance, and assistance he has given me while at the University of Maryland. He is a wonderful and hard-working mentor from whom I have learned a great deal. Niranjan Ramachandran has also been very helpful to me and I am especially grateful for the advice he gave me during the early stages of this project. I would also like to thank Bill Goldman for his guidance and mentoring throughout my time at Maryland.

I would like to recognize the financial support that I received through the VIGRE grant and from the Mathematics Department at the University of Maryland. I thank Julie Daberkow for advising me in my job as a teacher. I have enjoyed working with her during my many semesters of teaching Math 110.

Paul Irwin and Martha Dasef gave me valuable guidance when I was a student at Randolph-Macon Woman's College. I would like to give them special thanks for their mentoring and friendship. I also thank my professors at Virginia Tech.

I have been fortunate to have many friends throughout the years. I thank them all for the support they have given me.

I am especially thankful to Bobby Bhattacharjee for his friendship and support, through good times and bad. He has been there for me throughout my entire graduate education. He has helped me in many ways, both academically and personally, throughout the years and for that I will always be grateful.

Reinier Bröker has been my inspiration during the past five months. I thank him for all of the motivation and the happiness he has given me and for making my final months at Maryland very special.

I thank my grandparents, my sister, and the rest of my family for their love and support. Finally, I thank my parents for a lifetime of love and friendship. They have always believed in me and have given me everything I needed to succeed. I cannot adequately express how much I appreciate everything they have done for me.

Table of Contents

List of Abbreviations and Notation

$\mathbf{F}_q$	finite field of order q
$\overline{\mathbf{F}}_q$	an algebraic closure of $\mathbf{F}_q$
$J(\mathbf{F}_q)$	$\mathbf{F}_q$-rational elements of J
$J[n]$	full n-torsion subgroup of J
$J(\mathbf{F}_q)[n]$	$\mathbf{F}_q$-rational elements of $J[n]$
e_n	Weil pairing on n-torsion
div	divisor of a function
Div^0	class group of degree zero divisors
∞	point at infinity
id_J	identity element in J
Gal	Galois group
$\langle \cdot, \cdot \rangle_n$	Tate-Lichtenbaum pairing
τ_n	modified Tate-Lichtenbaum pairing
μ_n	nth roots of unity
ϕ	qth power Frobenius endomorphism
$\mathrm{End}(E)$	endomorphism ring of E
$\left(\frac{\cdot}{\cdot}\right)_n$	nth power residue symbol
I_n	$n \times n$ identity matrix
σ_i	sign of i
$N(f = g)$	number of $\mathbf{F}_q$-solutions to $f = g$
N_q	number of points on a curve over $\mathbf{F}_q$

Chapter 1

Introduction

1.1 Tate-Lichtenbaum Self Pairings

It is well-known that all self pairing are trivial for the Weil pairing (i.e., $e_n(P, P) = 1$ for all n-torsion points P). In this thesis we study self pairings for the Tate-Lichtenbaum pairing. We address the question,

Question 1. *Given an elliptic curve E defined over $\mathbf{F}_q$ and an integer n relatively prime to q, when does the Tate-Lichtenbaum pairing have only trivial self pairings for all points in $E[n]$?*

If E is an elliptic curve with cyclic n-torsion over $\mathbf{F}_q$, then nondegeneracy of the Tate-Lichtenbaum pairing implies that there exist points with nontrivial self pairings. Thus, we turn our attention to the case that all n-torsion points are defined over $\mathbf{F}_q$. In this case the existence of a point with a nontrivial self pairing is sometimes possible, but not guaranteed [2].

In this thesis we consider elliptic curves which have all of their n-torsion points defined over $\mathbf{F}_q$. We characterize when these curves have only trivial Tate-Lichtenbaum self pairings on their n-torsion points. This characterization depends on the action of the Frobenius endomorphism on the n^2-torsion points.

Theorem 1. *Let E be an elliptic curve defined over $\mathbf{F}_q$ and let n be an integer with*

gcd$(n, q) = 1$. *Assume that* $E[n] \subset E(\mathbf{F}_q)$. *Then* $\tau_n(Q, Q) = 1$ *for all* $Q \in E[n]$ *if and only if there exists an integer* a *such that* $\phi(R) = aR$ *for all* $R \in E[n^2]$. *If such an integer exists, then* $a \equiv 1 \bmod n$.

For certain elliptic curves, it is easy to recognize when this condition on the Frobenius endomorphism is realized. As an example, we study curves of the form $y^2 = x^3 + d^2$ for nonzero integers d and find the following characterization.

Theorem 2. *Let* E *be defined by* $y^2 = x^3 + d^2$ *over* $\mathbf{F}_p$ *with* $p \equiv 1 \bmod 3$ *and let* $n \geq 3$ *be an odd integer such that* $E[n] \subset E(\mathbf{F}_p)$. *Then* $\tau_n(P, P) = 1$ *for all* $P \in E[n]$ *if and only if* $4p = A^2 + 3B^2$ *for some integers* A *and* B *with* $B \equiv 0 \bmod n^2$.

When $n = 3$, this theorem, together with explicit calculations of the Tate-Lichtenbaum pairing, yields the following classical result due to Jacobi.

Corollary 3. *Let* $p \equiv 1 \bmod 3$. *Then 3 is a cubic residue mod p if and only if there exist integers* A *and* B *with* $4p = A^2 + 243B^2$.

The Weil pairing and Tate-Lichtenbaum pairing can be defined for more general abelian varieties. Although many of the results of this thesis can be restated for principally polarized abelian varieties, we restrict to Jacobians for simplicity. We consider the problem,

Question 2. *Given the Jacobian,* J, *of a genus* g *curve defined over* $\mathbf{F}_q$ *and an integer* n *relatively prime to* q, *can we characterize when all Tate-Lichtenbaum self pairings on* $J[n]$ *are trivial?*

We give a partial answer to this question. Like the characterization for elliptic curves, the result for Jacobians is also given in terms of the action of the Frobenius endomorphism on the n^2-torsion elements. We state the result below.

Theorem 4. *Let* $\{Q_1, Q_2, \ldots, Q_g, Q_{-1}, \ldots, Q_{-g}\}$ *be a basis for* $J[n^2]$ *such that* $\{nQ_{\pm i}\}_{i=1}^{g}$ *is an* e_n*-symplectic basis of* $J[n]$*. The Tate-Lichtenbaum pairing on* $J[n]$ *is then antisymmetric if and only if the Frobenius endomorphism restricted to* $J[n^2]$ *(with respect to this basis) is given by a matrix mod* n^2 *of the form* $\begin{bmatrix} M & N_1 \\ N_2 & M^\top \end{bmatrix}$ *where* M *is a* $g \times g$ *matrix such that* $M \bmod n$ *is the identity matrix and* M *has constant diagonal mod* n^2 *if* n *is odd and mod* $\frac{n^2}{2}$ *if* n *is even; and* N_i $(i = 1, 2)$ *is an antisymmetric* $g \times g$ *matrix such that* $N_i \bmod n$ *is the zero matrix.*

In addition, $\tau_n(P, P) = 1$ *for all* $P \in J[n]$ *if and only if each* N_i *has zero diagonal.*

We conclude this thesis by giving examples for Tate-Lichtenbaum self pairings on the 2-torsion of the Jacobians of some genus 2 curves.

1.1.1 Motivation: Pairings and Cryptography

Properties of the Tate-Lichtenbaum pairing are of practical interest due their use in cryptography. Security of elliptic curve cryptosystems is based on the difficulty of computing discrete logarithms. In certain circumstances, bilinear pairings can be used to reduce the problem of finding discrete logarithms in an elliptic curve to finding discrete logarithms in a multiplicative group (such as $\mathbf{F}_q^\times$). This reduced problem can then be solved more quickly than the original one.

The reduction works as follows. Suppose we are given two elements, P and Q, in $E[n]$, the group of n-torsion elements (defined over $\overline{\mathbf{F}}_q$). Also suppose that $Q = aP$ for some unknown integer a. The problem of finding a is known as the *discrete logarithm problem*. Let G be a multiplicative group and let $e : E[n] \times E[n] \to G$ be a bilinear nondegenerate pairing. For simplicity, we assume that G has prime order. Choose an element R such that $e(P, R)$ is nontrivial. Then,

$$e(Q, R) = e(aP, R) = e(P, R)^a. \tag{1.1}$$

Both $e(Q, R)$ and $e(P, R)$ are elements of G. We now have the problem of finding a discrete logarithm in the multiplicative group G. Subexponential attacks yield the solution for a, and this is also a solution to the original problem. When e is the Weil pairing, this reduction is called the MOV attack [10] and when e is the Tate-Lichtenbaum pairing, it is known as the Frey-Müller-Rück attack [7].

Sometimes $e(P, P)$ is nontrivial. In these cases one may simply choose $R = P$ and the reduction simplifies to

$$e(Q, P) = e(aP, P) = e(P, P)^a. \tag{1.2}$$

Hence, it is of interest to understand which pairings and which elliptic curves have this property. Since these cryptosystems can be generalized to Jacobian varieties, we also want to understand pairings and self pairings in this generalized setting.

In [3], Boneh and Franklin use bilinear pairings to create an Identity Based cryptosystem. They require the existence of a pairing and a point that pairs non-

trivially with itself. This provides additional motivation for wanting to recognize when this situation occurs.

1.2 Outline of Thesis

This thesis is structured as follows. In Chapter 2 we define the Weil pairing, e_n, and discuss its properties. We then define the Tate-Lichtenbaum pairing, τ_n, in terms of the Weil pairing and discuss properties of the Tate-Lichtenbaum pairing. Lastly, we show that this definition is equivalent to the standard definition of the pairing.

In Chapter 3 the definition of the Tate-Lichtenbaum pairing is used to find conditions that force all self pairings on n-torsion to be trivial. We then apply these conditions to the special case of elliptic curves and show that τ_n has only trivial self pairings if and only if the Frobenius endomorphism acts as multiplication by an integer on the n^2-torsion subgroup.

In Chapter 4 we apply the elliptic curve results from Chapter 3 to the elliptic curve given by $E : y^2 = x^3 - d^2x$ defined over $\mathbf{F}_p$. We also characterize when self pairings are always trivial by explicitly computing Tate-Lichtenbaum pairings using Miller's algorithm. These results combine to yield the classical reciprocity result that for primes $p \equiv 1 \bmod 3$ we have that 3 is a cubic residue mod p if and only if $4p = A^2 + 243B^2$ for some integers A and B.

In Chapter 5 we apply our results to Tate-Lichtenbaum self pairings on the 2-torsion points of the elliptic curve given by $E : y^2 = x^3 - d^2x$ and obtain a result

about primes congruent to 1 mod 8. We also apply our results to the 4-torsion points of the same curve and obtain a result about the octic residuacity of -2.

In Chapter 6 we use a result from Chapter 3 to study when Tate-Lichtenbaum self pairings are always trivial on the n-torsion subgroup of a Jacobian defined over a finite field. This result is similarly given in terms of the action of the Frobenius endomorphism on n^2-torsion and generalizes the elliptic curve case.

In Chapter 7 we apply the results of Chapter 6 to the Jacobian of the genus 2 curve given by $y^2 = x(x^2 - 1)(x^2 - 4)(x - 3)$. We also apply the results to the Jacobian of the genus 2 curve given by $y^2 = x^5 + 1$ and give examples of how Jacobi sums can be used to analyze the triviality and nontriviality of Tate-Lichtenbaum self pairings on the 2-torsion subgroup.

Chapter 2

Background

We now turn the discussion to the most commonly used pairings, the Weil pairing and the Tate-Lichtenbaum pairing. In Section 2.1 we define the Weil pairing and discuss its properties. In Section 2.2 we define the Tate-Lichtenbaum pairing in terms of the Weil pairing and discuss its properties. In Section 2.3 we explain the construction of the Tate-Lichtenbaum pairing as a cup product map and show that this construction is equivalent to the standard definition of the pairing.

2.1 The Weil Pairing

Let J be the Jacobian variety of a curve C defined over a finite field $\mathbf{F}_q$ where $q = p^k$ for some prime p and some positive integer k. Let μ_n represent the nth roots of unity in $\overline{\mathbf{F}}_q$. Let $J[n] = \{P \in J(\overline{\mathbf{F}}_q) | nP = \mathrm{id}_J\}$ be the group of n-torsion elements of J. If $p \nmid n$, then there exists a map

$$e_n : J[n] \times J[n] \to \mu_n$$

called the *Weil pairing*.

In order to define the Weil pairing, we need some notation for divisors. Recall that a divisor D is a formal sum of points, i.e., $D = \sum_{P \in C(\overline{\mathbf{F}}_q)} n_P[P]$. We use Div to denote the set of divisors. Let $\deg : \mathrm{Div}(C) \to \mathbf{Z}$ be the degree map, given

by $\deg(D) = \sum_{P \in C} n_P$. The set of divisors of degree zero is denoted by $\mathrm{Div}^0(C)$. The divisor of a function f is a formal sum of the zeros and poles of f, counting multiplicities:

$$\mathrm{div}(f) = \sum_{P \in C(\mathbf{F}_q)} \mathrm{ord}_P(f)[P], \tag{2.1}$$

where $\mathrm{ord}_P(f)$ is the order of vanishing of f at the point P. These are called *principal divisors*.

Define the *divisor class group* of C to be the group Div^0 mod principal divisors. Hence, two divisors D_1 and D_2 are said to be equivalent if $D_1 - D_2$ is a principal divisor. This group is isomorphic to J. If P is an element of J, we will use D_P to denote a divisor with the property that $P = [D_P]$, the divisor class of D_P.

Definition 2.1. *If $p \nmid n$ then the Weil Pairing is a map*

$e_n : J[n] \times J[n] \to \mu_n$ defined by

$$e_n(P, Q) = \frac{g(D_R + D_P)}{g(D_R)}, \tag{2.2}$$

where $g^n = f \circ n$, $div(f) = nD_Q$ and R is any point in $J(\overline{\mathbf{F}}_q)$.

It is important to note that the value of $e_n(P, Q)$ is independent of the choice of R (see [15] and [12] for proofs). Furthermore, the Weil pairing can be efficiently computed using Miller's algorithm (see [11] and Appendix B).

One can also define the Weil pairing as

$$e_n(P_1, P_2) = \frac{h_1(D_2)}{h_2(D_1)} \tag{2.3}$$

where $P_i \in J[n]$, D_i is a degree zero divisor such that $P_i = [D_i]$, D_1 and D_2 have disjoint supports, and h_i is a function such that $\mathrm{div}(h_i) = nD_i$.

Theorem 2.2. *The Weil pairing has the following properties:*

1. *Bilinearity:* $e_n(P+Q,R) = e_n(P,R) \cdot e_n(Q,R)$ *and*

   $e_n(P,Q+R) = e_n(P,Q) \cdot e_n(P,R)$ *for all* $P,Q,R \in J[n]$*;*

2. *Nondegeneracy: if* $e_n(P,Q) = 1$ *for all* $P \in J[n]$*, then* $Q = id_J$*; if* $e_n(P,Q) = 1$ *for all* $Q \in J[n]$*, then* $P = id_J$*;*

3. *Antisymmetry:* $e_n(P,Q) = e_n(Q,P)^{-1}$ *for all* $P,Q \in J[n]$*;*

4. *Alternating:* $e_n(P,P) = 1$ *for all* $P \in J[n]$*.*

5. *Compatibility: If* $P \in J[n]$ *and* $Q \in J[nm]$*, then* $mQ \in J[n]$ *and*

   $e_{nm}(P,Q) = e_n(P,mQ)$*;*

   $e_{nm}(Q,P) = e_n(mQ,P)$*.*

6. *Galois invariance: if* $\sigma \in Gal(\overline{\mathbf{F}}_q/\mathbf{F}_q)$*, then* $e_n(\sigma(P),\sigma(Q)) = \sigma e_n(P,Q)$*.*

Proof. See [14], Proposition 8.1(e) for the proof of the elliptic curve case and [12] for the general case for abelian varieties. □

When J is an elliptic curve, the Weil pairing has the following additional property [15]:

Proposition 2.3. *Let* E *be an elliptic curve defined over* $\mathbf{F}_q$ *and let* n *be a positive integer such that* n *is relatively prime to the characteristic of* $\mathbf{F}_q$*. Let* P_1 *and* P_2 *generate* $E[n]$*. Then* $e_n(P_1,P_2)$ *is a primitive* n*th root of unity.*

2.2 The Tate-Lichtenbaum Pairing

The Tate-Lichtenbaum pairing is a bilinear nondegenerate pairing on Jacobian varieties and it is related to the Weil Pairing.

Theorem 2.4. *Let $J = J(\mathbf{F}_q)$ be a Jacobian variety defined over $\mathbf{F}_q$ and let $n|q-1$. Assume that there is a nontrivial point of order n defined over $\mathbf{F}_q$. Then there exists a bilinear nondegenerate pairing*

$$\langle \cdot, \cdot \rangle_n : J(\mathbf{F}_q)[n] \times J(\mathbf{F}_q)/nJ(\mathbf{F}_q) \to \mathbf{F}_q^\times/(\mathbf{F}_q^\times)^n. \tag{2.4}$$

Much like the Weil pairing, the Tate-Lichtenbaum pairing can be efficiently computed using Miller's algorithm. For computational purposes, we want the Tate-Lichtenbaum pairing to have a unique value, rather than a coset. Thus, one often uses the *modified Tate-Lichtenbaum pairing*:

$$\tau_n : J(\mathbf{F}_q)[n] \times J(\mathbf{F}_q)/nJ(\mathbf{F}_q) \to \mu_n \tag{2.5}$$

defined by $\tau_n(P, Q) = \langle P, Q \rangle_n^{(q-1)/n}$.

Remark: Requiring $n|q-1$ forces the group μ_n to be contained in $\mathbf{F}_q^\times$. Note also the slight abuse of notation — an element of $J(\mathbf{F}_q)/nJ(\mathbf{F}_q)$ should really be represented as $Q + nJ(\mathbf{F}_q)$.

Schaefer shows that the Tate-Lichtenbaum pairing can be defined using the Weil pairing ([13]).

Theorem 2.5. *Given points $P_1 \in J(\mathbf{F}_q)[n]$ and $P_2 \in J(\mathbf{F}_q)$, let $R_i \in J(\overline{\mathbf{F}}_q)$ be such that $nR_i = P_i$ for $i = 1, 2$. Let ϕ denote the qth power Frobenius map. Then*

$$\tau_n(P_1, P_2) = e_n(P_1, \phi(R_2) - R_2) = e_{n^2}(R_1, \phi(R_2) - R_2).$$

In Section 2.3 we show that this definition does not depend on the choice of R_i. The last equality follows from the compatibility of the Weil pairing (Theorem 2.2). Furthermore, the bilinearity and alternating properties of the Weil pairing give the following corollary.

Corollary 2.6. *For any $P \in J(\mathbf{F}_q)[n]$, let $R \in J(\overline{\mathbf{F}}_q)$ be such that $nR = P$. Then $\langle P, P \rangle_n = e_{n^2}(R, \phi(R))$.*

The Tate-Lichtenbaum pairing can also be defined in a manner similar to that of the Weil pairing. Let $P \in J(\mathbf{F}_q)[n]$ and let $Q \in J(\mathbf{F}_q)$. We require that D_P and D_Q have no points of C in common. If necessary, we replace D_P or D_Q by equivalent elements to make this so. There exists a function f_P such that $\mathrm{div}(f_P) = nD_P$. The Tate-Lichtenbaum pairing is defined to be

$$\langle P, Q \rangle_n := f_P(D_Q). \tag{2.6}$$

In Section 2.3 we show that these two definitions yield the same bilinear pairing.

Note that both the Weil Pairing and the Tate-Lichtenbaum pairing can be efficiently computed using Miller's algorithm [11] to construct the functions in the definitions. This makes them practical for use in cryptography.

Theorem 2.7. *The Tate-Lichtenbaum pairing has the following properties:*

1. *Bilinearity: For all $P, Q \in J[n]$ and all $R \in J(\mathbf{F}_q)/nJ(\mathbf{F}_q)$ we have that $\tau_n(P+Q, R) = \tau_n(P, R) \cdot \tau_n(Q, R)$; for all $P \in J[n]$ and all $Q, R \in J(\mathbf{F}_q)/nJ(\mathbf{F}_q)$ we have that $\tau_n(P, Q + R) = \tau_n(P, Q) \cdot \tau_n(P, R)$;*

2. *Nondegeneracy: If* $\tau_n(P,Q) = 1$ *for all* $P \in J[n]$*, then* $Q \in nJ(\mathbf{F}_q)$*. If* $\tau_n(P,Q) = 1$ *for all* $Q \in J(\mathbf{F}_q)$*, then* $P = id_J$*;*

Proof. Bilinearity of the Tate-Lichtenbaum pairing follows directly from bilinearity of the Weil pairing.

When the n-torsion is defined over $\mathbf{F}_q$, nondegeneracy of the Tate-Lichtenbaum pairing follows from nondegeneracy of the Weil pairing. Suppose that $\tau_n(P,Q) = 1$ for all $P \in J[n]$. If we write $Q = nR$ for some $R \in J[n^2]$, then $e_n(P, \phi(R) - R) = 1$ for all $P \in J[n]$. Nondegeneracy of the Weil pairing now implies that $\phi(R) - R = \mathrm{id}_J$, hence R is rational over $\mathbf{F}_q$. Therefore $Q = nR \in nJ(\mathbf{F}_q)$. The following lemma implies nondegeneracy in the remaining variable.

Lemma 2.8. *Let* V *and* W *be finite* $\mathbf{Z}/n\mathbf{Z}$*-modules with equal orders. If the pairing* $e : V \times W \to \mu_n$ *is nondegenerate in one variable, then it is also nondegenerate in the second variable.*

Proof. Suppose that the pairing $V \times W \to \mu_n$ is nondegenerate in V (i.e. that if $e(v,w) = 1$ for all $w \in W$, then $v = 1$). Then the pairing defines an injection $V \hookrightarrow \mathrm{Hom}(W, \mu_n)$. By assumption, $\#V = \#W = \#\mathrm{Hom}(W, \mu_n)$, so this is actually an isomorphism. Suppose that $e(v,w) = 1$ for all $v \in V$. Then we have that $\mathrm{Hom}(W, \mu_n) = \mathrm{Hom}(W/\langle w \rangle, \mu_n)$. This then implies that $\#W = \#W/\langle w \rangle$, so we must have $w = 1$. □

For the proof of nondegeneracy in general, see Section 2.3.3. □

Recall that the Weil pairing is antisymmetric and alternating. The Tate-

Lichtenbaum pairing does not necessarily have these properties. The goal of this thesis is to characterize when the Tate-Lichtenbaum pairing is alternating when restricted to $J[n] \times J[n]$ (i.e., when self–pairings are trivial). This property depends on when the pairing is antisymmetric.

There are other well–known relationships between the Weil pairing and the Tate–Lichtenbaum pairing. One often uses the relation

$$e_n(P,Q) = \frac{\langle Q, P\rangle_n}{\langle P, Q\rangle_n}$$

to compute the Weil pairing in practice. This together with Theorem 2.5 implies the following corollary.

Corollary 2.9. *If E is an elliptic curve such that the Tate–Lichtenbaum pairing is antisymmetric, then $e_n(P,Q) = \langle Q, P\rangle_n^2$ up to nth powers.*

2.3 Schaefer's Construction of the Tate-Lichtenbaum Pairing

Recall that in [13], Schaefer shows that the Tate–Lichtenbaum pairing can be defined from the Weil pairing as

$$\tau_n(P_1, P_2) = e_n(P_1,\ \phi(R_2) - R_2) = e_{n^2}(R_1,\ \phi(R_2) - R_2)$$

where ϕ denotes the qth power Frobenius map. This result is derived by constructing a cup product map induced by the Weil pairing on cohomology groups.

2.3.1 Construction of the pairing

Let G be the Galois group $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$. Note that the qth power Frobenius map fixes $\mathbf{F}_q$. Let n be a positive integer such that $n|q-1$. Then $\mu_n \subset \mathbf{F}_q$ and the Weil pairing $e_n : J[n] \times J[n] \to \mu_n$ induces a cup-product pairing on cohomology groups

$$H^i(G, J[n]) \times H^j(G, J[n]) \to H^{i+j}(G, \mu_n) \tag{2.7}$$

for nonnegative integers i and j.

Recall that for a group M, $H^0(G, M)$ is the subgroup of elements in M that are fixed by G. By hypothesis, $\mu_n \subset \mathbf{F}_q$. Thus, we have that $H^0(G, \mu_n) = \mu_n$ and $H^0(G, J[n]) = J(\mathbf{F}_q)[n]$. We now see that when $i = j = 0$, and when $J[n] \subset J(\mathbf{F}_q)$, then the pairing in (2.7) is precisely the Weil pairing.

When $i = 0$ and $j = 1$, the map in (2.7) becomes

$$H^0(G, J[n]) \times H^1(G, J[n]) \to H^1(G, \mu_n). \tag{2.8}$$

Hence, we must understand the group $H^1(G, M)$. A *cocycle* is a map $\xi : G \to M$ such that for all σ and τ in G, $\xi(\sigma\tau) = \sigma\xi(\tau) + \xi(\tau)$. A cocycle of the form $\sigma \mapsto \sigma(m) - m$ where $m \in M$ is called a *coboundary*. The group $H^1(G, M)$ is the quotient of cocycles modulo coboundaries.

The Kummer isomorphism $k : \mathbf{F}_q^\times/(\mathbf{F}_q^\times)^n \to H^1(G, \mu_n)$ is defined as follows. The Kummer sequence $1 \to \mu_n \to \overline{\mathbf{F}}_q^\times \to \overline{\mathbf{F}}_q^\times \to 1$ induces an exact sequence

$$1 \to \mu_n \to \mathbf{F}_q^\times \xrightarrow{n} \mathbf{F}_q^\times \xrightarrow{k} H^1(G, \mu_n) \to H^1(G, \overline{\mathbf{F}}_q^\times).$$

By Hilbert's Theorem 90, we have that $H^1(G, \overline{\mathbf{F}}_q^\times) = 0$. For any element $x \in \mathbf{F}_q^\times$,

fix an element y in $\overline{\mathbf{F}}_q$ such that $y^n = x$. Then k maps x to the class $(\sigma \mapsto \frac{\sigma(y)}{y}) \in H^1(G, \mu_n)$. The map k is well-defined. Suppose that y_0 is another element such that $y_0^n = x$. Then $\frac{y}{y_0} = \zeta$ is an nth root of unity and

$$\frac{\sigma(y_0)}{y_0} = \frac{\sigma(\zeta y)}{\zeta y} = \frac{\sigma(y)}{y}.$$

Hence, any choice of an nth root of x yields the same class. Since σ is in G, it fixes all elements of $\mathbf{F}_q$ and thus we have that the kernel of this map contains $(\mathbf{F}_q^\times)^n$. We also have that $\mu_n \subset \mathbf{F}_q^\times$, and this shows that coboundaries are zero. Thus, the kernel of k equals $(\mathbf{F}_q^\times)^n$.

There is a similar isomorphism $\delta_n : J(\mathbf{F}_q)/nJ(\mathbf{F}_q) \to H^1(G, J[n])$ which is defined as follows. The Kummer sequence for J is

$$\mathrm{id}_J \to J(\mathbf{F}_q)[n] \to J \xrightarrow{n} J \to \mathrm{id}_J$$

and it induces the long exact sequence

$$\mathrm{id}_J \to J(\mathbf{F}_q)[n] \to J(\mathbf{F}_q) \xrightarrow{n} J(\mathbf{F}_q) \xrightarrow{\delta_n} H^1(G, J[n]) \to H^1(G, J(\overline{\mathbf{F}}_q)).$$

Given an element $Q \in J(\mathbf{F}_q)$, fix an element $R \in J(\overline{\mathbf{F}}_q)$ such that $nR = Q$. Then δ_n maps Q to the cocycle $(\sigma \mapsto \sigma(R) - R)$ in $H^1(G, J[n])$. The exact sequence shows that the kernel of this map is $nJ(\mathbf{F}_q)$, since σ fixes all elements defined over $\mathbf{F}_q$ and since $Q = nR$. Note that this map is well defined. If we were to choose a different element R' with $nR' = Q$, then R' differs from R by an n-torsion element S (since $n(R - R') = \mathrm{id}_J$). Therefore, we have that

$$\sigma(R') - R' = \sigma(R + S) - (R + S) = \sigma(R) - R + \sigma(S) - S = \sigma(R) - R$$

since the n-torsion points are $\mathbf{F}_q$-rational and fixed by σ.

The pairing from (2.8) now yields a pairing

$$\langle \cdot, \cdot \rangle_n^* : J(\mathbf{F}_q)[n] \times J(\mathbf{F}_q)/nJ(\mathbf{F}_q) \to \mathbf{F}_q^\times/(\mathbf{F}_q^\times)^n$$

which is defined as follows. Let $P \in J(\mathbf{F}_q)[n]$, let $Q \in J(\mathbf{F}_q)/nJ(\mathbf{F}_q)$, and let $Q = nR$. Let $\omega_n : H^1(G, J[n]) \to H^1(G, \mu_n)$ be the map (depending on P) that sends the element $(\sigma \mapsto \zeta(\sigma))$ to $(\sigma \mapsto e_n(P, \zeta(\sigma)))$. Then

$$\langle P, Q \rangle_n^* = k^{-1} \circ \omega_n \circ \delta_n(Q). \tag{2.9}$$

Evaluating at $\sigma = \phi$, the qth power Frobenius map, yields the following theorem from [13].

Theorem 2.10. *Let J be the Jacobian of a curve defined over $\mathbf{F}_q$. Let n be an integer such that $n|q-1$. Then the Weil pairing induces a cup product map that yields a bilinear nondegenerate pairing*

$$\langle \cdot, \cdot \rangle_n^* : J(\mathbf{F}_q)[n] \times J(\mathbf{F}_q)/nJ(\mathbf{F}_q) \to \mathbf{F}_q^\times/(\mathbf{F}_q^\times)^n.$$

It is defined by $(\langle P, Q \rangle_n^*)^{\frac{q-1}{n}} = e_n(P, \phi(R) - R)$ where $nR = Q$ and ϕ is the qth power Frobenius map.

In Section 2.3.2, we prove that this pairing is the same as the standard definition of the Tate-Lichtenbaum pairing given by (2.6).

2.3.2 Equivalence to the Tate-Lichtenbaum pairing

We have seen that the Weil pairing induces a cup product pairing $H^0(G, J[n]) \times H^1(G, J[n]) \to H^1(G, \mu_n)$ and that this yields the pairing

$$\langle \cdot, \cdot \rangle_n^* : J(\mathbf{F}_q)[n] \times J(\mathbf{F}_q)/nJ(\mathbf{F}_q) \to \mathbf{F}_q^\times/(\mathbf{F}_q^\times)^n \tag{2.10}$$

defined by $(\langle P, Q \rangle_n^*)^{\frac{q-1}{n}} = e_n(P, \phi(R) - R)$ where $nR = Q$.

Theorem 2.11. *The Tate-Lichtenbaum pairing as defined in Theorem 2.5 is the same as the standard definition given in (2.6). That is,*

$$f_P(D_Q)^{\frac{q-1}{n}} = e_n(P, \phi(R) - R).$$

Proof. Let $P \in J[n]$ and let $Q \in J(\mathbf{F}_q)/nJ(\mathbf{F}_q)$ have disjoint supports. Let $R \in J(\overline{\mathbf{F}}_q)$ be such that $nR = Q$. Let D_P and D_Q be disjoint divisors of degree zero, defined over $\mathbf{F}_q$, with the property that $P = [D_P]$, and $Q = [D_Q]$.

Lemma 2.12. *Let J be the Jacobian of a curve C and let Q_0 be an element in $J(\mathbf{F}_q)$. It is possible to represent the class Q_0 by a divisor, D, with the property that $\phi(D) = D$.*

Proof. Let $\overline{\mathbf{F}}_q(C)^\times$ represent the functions on C defined over $\overline{\mathbf{F}}_q$. Since $[D]$ is in $J(\mathbf{F}_q)$, we know that $\phi[D] = [D]$. Hence, we have $\phi(D) = D + \mathrm{div}(F)$ for some function $F \in \overline{\mathbf{F}}_q(C)^\times$. Then F is an element of $\mathbf{F}_{q^n}(C)$ for some n. We have that $\phi(D) - D = \mathrm{div}(F)$, so the cocycle such that $\phi \mapsto \mathrm{div}(F)$ is an element of $H^1(H, P)$. The following claim shows that this cocycle is actually a coboundary.

Claim 2.13. *Let P be the principal divisors from $\mathbf{F}_{q^n}(C)^\times$. Let $H = Gal(\mathbf{F}_{q^n}/\mathbf{F}_q)$. Then we have $H^1(H, P) = 0$.*

Proof. The exact sequence

$$1 \to \mathbf{F}_{q^n}^{\times} \to \mathbf{F}_{q^n}(C)^{\times} \to P \to 1$$

induces the exact sequence

$$H^1(H, \mathbf{F}_{q^n}^{\times}) \to H^1(H, \mathbf{F}_{q^n}(C)^{\times}) \to H^1(H, P) \to H^2(H, \mathbf{F}_{q^n}^{\times}).$$

By Hilbert's Theorem 90, we have that $H^1(H, \mathbf{F}_{q^n}^{\times}) = 0$. Hilbert's Theorem 90 also gives us $H^1(H, \mathbf{F}_{q^n}(C)^{\times}) = 0$ since H is also the Galois group $\mathrm{Gal}(\mathbf{F}_{q^n}(C)/\mathbf{F}_{q^n})$.

Since H is cyclic, we have the isomorphism $H^2(H, \mathbf{F}_{q^n}^{\times}) \simeq \widehat{H}^0(H, \mathbf{F}_{q^n}^{\times})$, where $\widehat{H}^0(H, \mathbf{F}_{q^n})$ is the group of elements of $\mathbf{F}_{q^n}^{\times}$ that are fixed by H, mod norms. Since H fixes $\mathbf{F}_q$ and since the norm map is surjective on finite fields, this group is trivial. Therefore we also have that $H^1(H, P) = 0$. □

Claim 2.13 shows that $\mathrm{div}(F) = \phi(\mathrm{div}(F_1)) - \mathrm{div}(F_1)$ for some $F_1 \in \mathbf{F}_{q^n}(C)$. Rearranging gives us $\phi(D_Q - \mathrm{div}(F_1)) = D_Q - \mathrm{div}(F_1)$. Thus, we can replace D_Q by the equivalent divisor $D_Q - \mathrm{div}(F_1)$. This divisor is fixed by ϕ, as desired.

□

Lemma 2.12 shows that we may choose D_Q such that $\phi(D_Q) = D_Q$. Let g be a function on the curve with $\mathrm{div}(g) = nD_R - D_Q$. Then $\mathrm{div}(g^{\phi}) = nD_R^{\phi} - D_Q$ and $\mathrm{div}(g^{\phi}/g) = n(D_R^{\phi} - D_R)$. Also let f_P be a function on the curve such that $\mathrm{div}(f_P) = nD_P$.

Then the definition of the Weil pairing (in Equation 2.3) gives

$$e_n(P, \phi(R) - R) = \frac{f_P(D_R^{\phi} - D_R)}{(g^{\phi}/g)(D_P)} = \frac{\beta^{\phi}}{\beta}, \tag{2.11}$$

where $\beta = \frac{f_P(D_R)}{g(D_P)}$, since the following lemma tells us that we may assume that $f_P(D_R^\phi) = \phi f_P(D_R)$.

Lemma 2.14. *The function f_P can be chosen so that it commutes with ϕ.*

Proof. Recall that P is defined over $\mathbf{F}_p$. Hence, $\mathrm{div}(f_P^\phi) = \phi(nD_P) = nD_P$ and we see that $\frac{f_P^\phi}{f_P}$ is a constant element of $\overline{\mathbf{F}}_p$.

Then $(\sigma \mapsto \frac{f_P^\sigma}{f_P})$ is trivial since $H^1(G, \overline{\mathbf{F}}_p^\times) = 0$ by Hilbert's Theorem 90. This shows that $\frac{f_P^\phi}{f_P} = \frac{\alpha^\phi}{\alpha}$ for some $\alpha \in \overline{\mathbf{F}}_p^\times$. Therefore, $(\frac{f_P}{\alpha})^\phi = \frac{f_P}{\alpha}$ and we see that $\frac{f_P}{\alpha}$ is defined over $\mathbf{F}_p$. This means that $\phi \circ \frac{f_P}{\alpha} = \frac{f_P}{\alpha} \circ \phi$. Thus, replacing f_P by $\frac{f_P}{\alpha}$ gives the desired result. □

The lemma implies that $\beta^n = \frac{f_P(nD_R)}{g(D_P)^n}$ is an element of $\mathbf{F}_q$ since the nth power of the Weil pairing is always 1. Recall that $\omega_n : H^1(G, J[n]) \to H^1(G, \mu_n)$ is the map that sends the element $(\sigma \mapsto \zeta(\sigma))$ to $(\sigma \mapsto e_n(P, \zeta(\sigma)))$. Recall that we also have the Kummer isomorphism $k : \mathbf{F}_q^\times/(\mathbf{F}_q^\times)^n \to H^1(G, \mu_n)$. Evaluating at $\sigma = \phi$ yields

$$\begin{aligned} k^{-1} \circ \omega_n \circ \delta_n(Q) &\equiv \beta^n \bmod (\mathbf{F}_q^\times)^n && (2.12) \\ &\equiv \frac{f_P(nD_R)}{g(nD_P)} \bmod (\mathbf{F}_q^\times)^n. && (2.13) \end{aligned}$$

This is equivalent to $\frac{f_P(nD_R)}{f_P(nD_R - D_Q)} \bmod (\mathbf{F}_q^\times)^n$ because

$$g(nD_P) = g(\mathrm{div}(f_P)) = f_P(\mathrm{div}(g)) = f_P(nD_R - D_Q),$$

where the second equality is Weil Reciprocity.

Furthermore, we have that $\frac{f_P(nD_R)}{f_P(nD_R - D_Q)} \equiv f_P(D_Q) \bmod (\mathbf{F}_q^\times)^n$, which is simply $\langle P, Q \rangle_n$ as given by the classical definition of the pairing. We now have that

$$\beta^n \equiv k^{-1} \circ \omega_n \circ \delta_n \equiv \langle P, Q \rangle_n,$$

as in Equation 2.9. Raising to the power $(q-1)/n$ gives an isomorphism from $\mathbf{F}_q^\times / (\mathbf{F}_q^\times)^n$ to μ_n, and it gives us that

$$\beta^{q-1} = \langle P, Q \rangle_n^{\frac{q-1}{n}} = \tau_n(P, Q).$$

We also have that $\beta^{q-1} = \frac{\beta^\phi}{\beta} = e_n(P, \phi(R) - R)$ by Equation 2.11. Hence, we obtain the relation

$$\tau_n(P, Q) = e_n(P, \phi(R) - R),$$

where $nR = Q$. Throughout the proof, we used a fixed choice of R. In Section 2.3.1 we saw that the value of the pairing is independent of this choice. □

2.3.3 Nondegeneracy of the Tate-Lichtenbaum pairing

In Theorem 2.7 we proved that the Tate-Lichtenbaum pairing is nondegenerate in the special case that $J[n] \subset J(\mathbf{F}_q)$. We now prove nondegeneracy in general.

Let $\{Q_1, \ldots, Q_b\}$ generate $J(\mathbf{F}_q)[n]$. Let $\Omega_n : J[n] \to (\mu_n)^b$ be defined by

$$Q \mapsto (e_n(Q_1, Q), e_n(Q_2, Q), \ldots, e_n(Q_b, Q)).$$

Then we have that

$$\begin{aligned}\Omega_n(\phi(Q)) &= (e_n(Q_1,\phi(Q)),\dots,e_n(Q_b,\phi(Q)))\\ &= (e_n(\phi(Q_1),\phi(Q)),\dots,e_n(\phi(Q_b),\phi(Q))\\ &= (e_n(Q_1,Q)^{\phi},\dots,e_n(Q_b,Q)^{\phi})\\ &= \Omega_n(Q)\end{aligned} \tag{2.14}$$

since every generator Q_i is defined over $\mathbf{F}_q$ and since $\mu_n \subset \mathbf{F}_q^{\times}$. This shows that $\Omega_n((\phi-1)(Q)) = 1$ for all $Q \in J[n]$. Therefore Ω_n induces a surjective map

$$\widetilde{\Omega_n} : J[n]/(\phi-1)J[n] \to \mathrm{Im}\Omega_n.$$

We analyze the orders of these groups using the following lemmas.

Lemma 2.15. *Let M be a finite abelian group on which ϕ acts and let $M[\phi-1]$ denote the kernel of $\phi-1$. Then $\#M[\phi-1] = \#M/(\phi-1)M$.*

Proof. The map $\phi - 1$ gives the exact sequence

$$0 \to M[\phi-1] \to M \xrightarrow{\phi-1} M \to M/(\phi-1)M \to 0.$$

Since the sequence is exact, the alternating product of group orders is one. This implies the result. □

It is clear that $\#J(\mathbf{F}_q)[n] = \#J[n][\phi-1]$. By Lemma 2.15, this implies that $\#J(\mathbf{F}_q)[n] = \#J[n]/(\phi-1)J[n]$.

Lemma 2.16. *Suppose that A and B are finite $\mathbf{Z}/n\mathbf{Z}$-modules and that there is a bilinear nondegenerate pairing $\langle\cdot,\cdot\rangle : B \times A \to \mu_n$. Let C be a subgroup of B and let C be generated by the set $S = \{g_i\}_{i=1}^{s}$. Let $\Omega_n : A \to \prod_S \mu_n$ be defined by $a \mapsto (\dots,\langle g_i, a\rangle,\dots)$. Then $\#\Omega_n(A) = \#C$.*

Proof. Nondegeneracy of the pairing implies that $A = \mathrm{Hom}(B, \mu_n)$. This says that $\ker(\Omega_n) = \{f \in \mathrm{Hom}(B, \mu_n) | f(C) = \{1\}\}$. But this is the group $\mathrm{Hom}(B/C, \mu_n)$. Thus, we have that $\#\Omega_n(A) = \frac{\#A}{\#\ker\Omega_n} = \frac{\#A}{\#(B/C)} = \#C$. □

Lemma 2.16 tells us that $\#\mathrm{Im}\Omega_n = \#J(\mathbf{F}_q)[n]$, and so we have $\#\mathrm{Im}\Omega_n = \#J[n]/(\phi - 1)J[n]$. Thus, $\widetilde{\Omega_n}$ is a surjective map between groups of the same order, and hence it is an isomorphism. We now show that this implies nondegeneracy.

Let Q be an element in $J(\mathbf{F}_q)$ and let $Q = nR$ for some element $R \in J(\overline{\mathbf{F}}_q)$. Suppose that we know that $\tau_n(P, Q) = 1$ for all $P \in J(\mathbf{F}_q)[n]$. Then we have $e_n(P, \phi(R) - R) = 1$ for all $P \in J(\mathbf{F}_q)[n]$. In particular, we have $e_n(Q_i, \phi(R) - R) = 1$ for every generator Q_i of $J(\mathbf{F}_q)[n]$. This shows that $\widetilde{\Omega_n}(\phi(R) - R) = 1$. Injectivity of $\widetilde{\Omega_n}$ implies that $(\phi - 1)(R) \in (\phi - 1)J[n]$. Let $(\phi - 1)(R) = (\phi - 1)(T)$ for some element $T \in J[n]$. Then we have $\phi(R - T) = R - T$, so $R - T$ is in $J(\mathbf{F}_q)$. Since $Q = nR = n(R - T)$, we now have that $Q \in nJ(\mathbf{F}_q)$. This proves that the pairing

$$\tau_n : J(\mathbf{F}_q)[n] \times J(\mathbf{F}_q)/nJ(\mathbf{F}_q) \to \mu_n$$

is nondegenerate in the second variable. Lemma 2.8 implies that it is also nondegenerate in the first variable.

Chapter 3

Tate-Lichtenbaum Self Pairings

It is well–known that the Weil pairing always has trivial self pairings (i.e., that $e_n(P, P) = 1$ for all n-torsion points P). In this chapter we study Tate-Lichtenbaum self pairings on n-torsion. If E is an elliptic curve with cyclic n-torsion over $\mathbf{F}_q$, then nondegeneracy of the Tate-Lichtenbaum pairing implies that there exist points with nontrivial self pairings. An interesting case is when all n-torsion points are defined over $\mathbf{F}_q$. In this case the existence of a point with a nontrivial self pairing is sometimes possible, but not guaranteed.

In Section 3.1 we discuss the restriction of the Tate-Lichtenbaum pairing to n-torsion. In Section 3.2 (and throughout the remainder of the thesis) we restrict to the case that the n-torsion is $\mathbf{F}_q$-rational. Under this restriction, we determine conditions that make Tate-Lichtenbaum self pairings trivial for each element of $J[n]$. In Section 3.3 we apply the results of the previous section to Tate-Lichtenbaum pairings on elliptic curves. This yields a characterization of the triviality of self pairings in terms of the action of the Frobenius endomorphism on the n^2-torsion elements.

3.1 Restriction to n-torsion

The Tate-Lichtenbaum pairing can always be restricted to a map on $J[n]\times J[n]$. We first consider when this restriction yields a nondegenerate pairing. However, this property will not be required for the rest of the thesis.

Suppose that we had the situation that $J[n^2] \subset J(\mathbf{F}_q)$. Then any $P \in J(\mathbf{F}_q)[n]$ can be written as $P = nQ$ for some $Q \in J[n^2] \bigcap J(\mathbf{F}_q)$, so $P \in nJ(\mathbf{F}_q)$. In this case, we have that $\tau_n(P,P) = \tau_n(P,Q)^n = 1$. Therefore, if all n^2-torsion points are $\mathbf{F}_q$-rational, we have that all self pairings are trivial.

The following lemma addresses the opposite extreme case, namely when no n^2-torsion point is defined over $\mathbf{F}_q$.

Lemma 3.1. *Suppose that $J[n] \subset J(\mathbf{F}_q)$ and that $J[n] \bigcap nJ(\mathbf{F}_q) = \{id_J\}$. Then the natural map $J[n] \xrightarrow{\sim} J(\mathbf{F}_q)/nJ(\mathbf{F}_q)$ is an isomorphism. As a result, the Tate-Lichtenbaum pairing restricts to a nondegenerate pairing $\tau_n : J[n] \times J[n] \to \mu_n$.*

Proof. The natural map $J[n] \to J(\mathbf{F}_q)/nJ(\mathbf{F}_q)$ comes from the exact sequence

$$\mathrm{id}_J \to J[n] \to J(\mathbf{F}_q) \xrightarrow{n} J(\mathbf{F}_q) \to J(\mathbf{F}_q)/nJ(\mathbf{F}_q) \to \mathrm{id}_J.$$

It has kernel $J[n] \bigcap nJ(\mathbf{F}_q)$, which is $\{\mathrm{id}_J\}$ by hypothesis. The group $J(\mathbf{F}_q)$ is finite and so $J[n]$ and $J(\mathbf{F}_q)/nJ(\mathbf{F}_q)$ have the same orders. Therefore injectivity implies surjectivity, so the map is an isomorphism.

□

Bilinearity of the Tate-Lichtenbaum pairing also implies that for an element $P \in J(\mathbf{F}_q)[n] \bigcap nJ(\mathbf{F}_q)$ we have that $\tau_n(Q,P) = 1$ for all $Q \in J[n]$. Therefore, if we

want τ_n to be nondegenerate on $J(\mathbf{F}_p)[n]$, then we need to have $J(\mathbf{F}_q)[n] \bigcap nJ(\mathbf{F}_q) = \{\mathrm{id}_J\}$. The next lemma tells us that this condition is equivalent to having all n^2-torsion elements irrational over $\mathbf{F}_q$.

Lemma 3.2. *Let J be the Jacobian of a curve defined over $\mathbf{F}_q$ and let n be a positive integer. Then $J(\mathbf{F}_q)[n] \bigcap nJ(\mathbf{F}_q) = \{id_J\}$ if and only if $J[n^2] \bigcap J(\mathbf{F}_q) = J(\mathbf{F}_q)[n]$.*

Proof. Suppose that $J(\mathbf{F}_q)[n] \bigcap nJ(\mathbf{F}_q) = \{\mathrm{id}_J\}$. We clearly have that $J(\mathbf{F}_q)[n] \subset J[n^2] \bigcap J(\mathbf{F}_q)$. Let P be an element in $J[n^2] \bigcap J(\mathbf{F}_q)$. Then $nP \in J(\mathbf{F}_q)[n] \bigcap nJ(\mathbf{F}_q)$ and so $nP = \mathrm{id}_J$ by hypothesis. Thus, P is in $J(\mathbf{F}_q)[n]$.

Conversely, suppose that $J[n^2] \bigcap J(\mathbf{F}_q) = J(\mathbf{F}_q)[n]$. Let P be an element of $J(\mathbf{F}_q)[n] \bigcap nJ(\mathbf{F}_q)$. Write $P = nQ$ for some $Q \in J(\mathbf{F}_q)$. Then we have that $n^2Q = nP = \mathrm{id}_J$, so Q is in $J[n^2] \bigcap J(\mathbf{F}_q)$. Therefore Q is an element of $J(\mathbf{F}_q)[n]$ by our hypothesis, and $P = nQ = \mathrm{id}_J$. □

From now on we restrict to the case $J[n] \subset J(\mathbf{F}_q)$. There are now two possibilities. Sometimes there exists a point $P \in J[n]$ such that $\tau_n(P, P) \neq 1$. Sometimes all n-torsion points have trivial self pairings. The remainder of this thesis investigates when these situations occur.

3.2 Alternating Tate-Lichtenbaum Pairings

Assume that $J[n] \subset J(\mathbf{F}_q)$. The following theorem gives conditions for the Tate-Lichtenbaum pairing to be alternating.

Theorem 3.3. *Let n be a positive integer. Let $\{Q_i\}_{i=1}^{2g}$ be generators of $J[n]$. The*

Tate-Lichtenbaum pairing has the property that $\tau_n(Q,Q) = 1$ *for all* $Q \in J[n]$ *if and only if*

1. $\tau_n(Q_i, Q_i) = 1$ *for all* i*;*

2. $\tau_n(Q_i, Q_j) = \tau_n(Q_j, Q_i)^{-1}$ *for all* i*.*

Proof. Suppose that Conditions 1 and 2 hold. Since every point of J can be written as a linear combination of generators, we need to verify that $\sum_{i=1}^{2g} a_i Q_i$ (where $a_i \in \mathbf{Z}$) pairs trivially with itself. Bilinearity implies that

$$\tau_n\left(\sum_{i=1}^{2g} a_i Q_i, \sum_{i=1}^{2g} a_i Q_i\right) = \prod_{i=1}^{2g}\prod_{j=1}^{2g} \tau_n(Q_i, Q_j)^{a_i a_j}.$$

Condition 1 allows us to remove factors of the form $\tau_n(Q_i, Q_i)^{a_i^2}$ and Condition 2 tells us that the remaining factors cancel since $\tau_n(Q_i, Q_j)^{a_i a_j}\tau_n(Q_j, Q_i)^{a_i a_j} = 1$ when $i \neq j$. Hence, every n-torsion point pairs trivially with itself.

Conversely, suppose that $\tau_n(Q,Q) = 1$ for every $Q \in J[n]$. In particular, this is true for the generators of $J[n]$, so Condition 1 holds. Let $Q = Q_i + Q_j$. Then

$$\begin{aligned} 1 &= \tau_n(Q,Q) \\ &= \tau_n(Q_i + Q_j, Q_i + Q_j) \\ &= \tau_n(Q_i, Q_i) \cdot \tau_n(Q_i, Q_j) \cdot \tau_n(Q_j, Q_i) \cdot \tau_n(Q_j, Q_j) \\ &= \tau_n(Q_i, Q_j) \cdot \tau_n(Q_j, Q_i). \end{aligned}$$

This is Condition 2. □

Remark: Note that when n is even, then Condition 2 for $i = j$ is slightly weaker than Condition 1. When Condition 2 holds, bilinearity implies that τ_n is antisym-

metric since:

$$\begin{aligned}\tau_n\left(\sum_i a_iQ_i, \sum_j b_jQ_j\right) &= \prod_i\prod_j \tau_n(Q_i,Q_j)^{a_ib_j} \\ &= \prod_i\prod_j \tau_n(Q_j,Q_i)^{-b_ja_i} \\ &= \tau_n\left(\sum_j b_jQ_j, \sum_i a_iQ_i\right)^{-1}.\end{aligned}$$

3.3 Tate-Lichtenbaum Self Pairings in Elliptic Curves

Throughout this section we restrict to the special case of genus 1 curves. Let E be an elliptic curve defined over a finite field $\mathbf{F}_q$, where q is a prime power, and assume that $E[n] \subset E(\mathbf{F}_q)$. Let ϕ represent the qth-power Frobenius endomorphism given by $\phi(x,y) = (x^q, y^q)$, where (x,y) is a point on E. The following theorem characterizes when all self pairings are trivial.

Theorem 3.4. *Let E be an elliptic curve defined over $\mathbf{F}_q$ and let n be an integer with $gcd(n,q) = 1$. Assume that $E[n] \subset E(\mathbf{F}_q)$. Then $\tau_n(Q,Q) = 1$ for all $Q \in E[n]$ if and only if there exists an integer a such that $\phi(R) = aR$ for all $R \in E[n^2]$. If such an integer exists, then $a \equiv 1 \bmod n$.*

Proof. Let a be an integer and suppose $\phi(R) = aR$ for all R in $E[n^2]$. For any point Q in $E[n]$, let $R \in E(\overline{\mathbf{F}}_q)$ be such that $nR = Q$. Then, by Theorem 2.5,

$$\tau_n(Q,Q) = e_{n^2}(R,\phi(R)) = e_{n^2}(R,aR) = e_{n^2}(R,R)^a = 1.$$

Conversely, suppose that $\tau_n(Q,Q) = 1$ for all Q in $E[n]$. According to Theorem 3.3 , we know that the Tate-Lichtenbaum pairing is antisymmetric on $E[n]$.

Let $\{R_1, R_2\}$ generate $E[n^2]$. Then multiplication by n yields generators $P_i = nR_i$ of $E[n]$ for $i = 1, 2$.

The Frobenius endomorphism restricted to $E[n^2]$ can be represented by a 2×2 matrix with coefficients mod n^2 acting on the generators of $E[n^2]$ (expressed as column vectors). Thus,

$$\phi = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod n^2$$

expresses the relations that $\phi(R_1) = aR_1 + cR_2$ and $\phi(R_2) = bR_1 + dR_2$. Condition 1 of Theorem 3.3 now says that

$$1 = \tau_n(P_1, P_1) = e_{n^2}(R_1, \phi(R_1)) = e_{n^2}(R_1, aR_1 + cR_2) = e_{n^2}(R_1, R_2)^c = \zeta^c,$$

where $\zeta = e_{n^2}(R_1, R_2)$ is a primitive n^2th root of unity. (Note that ζ is primitive by Proposition 2.3.) The above relation occurs if and only if $c \equiv 0 \mod n^2$. Likewise, $\tau_n(P_2, P_2) = 1$ implies that $b \equiv 0 \mod n^2$.

We now have ϕ represented by a diagonal matrix on the n^2-torsion points, so that $\phi(R_1) = aR_1$ and $\phi(R_2) = dR_2$. By Theorem 2.5,

$$\tau_n(P_1, P_2) = e_{n^2}(R_1, \phi(R_2) - R_2) = e_{n^2}(R_1, dR_2 - R_2) = e_{n^2}(R_1, R_2)^{d-1},$$

and

$$\begin{aligned} \tau_n(P_2, P_1) &= e_{n^2}(R_2, \phi(R_1) - R_1) &&= e_{n^2}(R_2, aR_1 - R_1) \\ &= e_{n^2}(R_2, R_1)^{a-1} &&= e_{n^2}(R_1, R_2)^{1-a}. \end{aligned}$$

Condition 2 of Theorem 3.3 says that $\tau_n(P_1, P_2) \cdot \tau_n(P_2, P_1) = 1$. Thus we have that

$$1 = e_{n^2}(R_1, R_2)^{d-1} e_{n^2}(R_1, R_2)^{1-a} = e_{n^2}(R_1, R_2)^{d-a},$$

which occurs if and only if $a \equiv d \mod n^2$. Hence we have shown that $\phi(R) = aR$ for all $R \in E[n^2]$. Furthermore, note that since $E[n] \subset E[n^2]$ and since ϕ acts trivially on $E[n]$, then restriction to $E[n]$ implies that $a \equiv 1 \bmod n$. $\square$

Chapter 4

The Curve $E : y^2 = x^3 + d^2$

In this chapter, we consider the elliptic curve given by $E_d : y^2 = x^3 + d^2$ defined over a field $\mathbf{F}_p$ for some prime p and some nonzero integer d. In Section 4.1 we outline some properties of $E_d[3]$. In Section 4.2 we use Miller's algorithm to explicitly calculate the Tate-Lichtenbaum pairing on generators of $E_d[3]$ and we analyze the conditions that yield trivial self-pairings. In Section 4.3 we use complex multiplication to simplify the condition that ϕ is integer multiplication on $E_d[n^2]$ for arbitrary integers n. In Section 4.4 we combine the results of the previous sections to obtain a classical reciprocity theorem.

4.1 Properties of $E : y^2 = x^3 + d^2$

Let $E_d : y^2 = x^3 + d^2$ be defined over $\mathbf{F}_p$ where $p \geq 5$ is prime and d is a nonzero integer. We restrict to the case where $E_d[3] \subset E_d(\mathbf{F}_p)$ (hence $p \equiv 1 \bmod 3$ and E_d is ordinary). Under this restriction, $\mathbf{F}_p$ contains μ_3, the cube roots of unity. Since $E_d[3]$ is generated by the points $P = (0, d)$ and $Q = (-\alpha^2, d\sqrt{-3})$ where $2d \equiv \alpha^3 \bmod p$, we conclude that our restriction forces $2d$ to be a cubic residue. (Note that -3 is automatically a quadratic residue mod p since $p \equiv 1 \bmod 3$.) The simplest case is $E_4 : y^2 = x^3 + 16$ since $E_4[3]$ is generated by $(0, 4)$ and $(-4, 4\sqrt{-3})$. From now on, we let $E = E_d$.

4.2 Explicit Calculations of the Tate-Lichtenbaum Pairing

Explicit calculations of the Tate-Lichtenbaum pairing using Miller's algorithm yield the following result.

Theorem 4.1. *Let E be the elliptic curve defined by $y^2 = x^3 + d^2$ over $\mathbf{F}_p$ where p is prime such that $p \equiv 1 \bmod 3$. Assume that $2d$ is a cube mod p (so that $E[3] \subset E(\mathbf{F}_p)$). Then the following are equivalent:*

1. *$\tau_3(R, R) = 1$ for all $R \in E[3]$;*

2. *3 is a cubic residue p.*

Proof. Let α be such that $\alpha^3 = 2d$ and note that $E[3]$ is rational mod p since $p \equiv 1 \bmod 3$. Let ζ be a primitive cube root of unity in $\mathbf{F}_p$. By Theorem 3.3, we only need to explicitly compute the Tate-Lichtenbaum pairing on the generators. We use Miller's algorithm to do so. Let $r = \sqrt{-3}$, let $f_P(x, y) = y - d$, and let $f_Q(x, y) = y\sqrt{-3} - 3(\alpha x + d)$. Then $\operatorname{div}(f_P) = 3[P] - 3[\infty]$ and $\operatorname{div}(f_Q) = 3[Q] - 3[\infty]$.

1. Let $D_P = [(-\zeta\alpha^2, dr)] + [(-\zeta^2\alpha^2, dr)] - [(0, -d)] - [(-\alpha^2, -dr)]$ be a divisor on E. Then $[P] - [\infty]$ is equivalent to D_P modulo principal divisors and

$$\langle P, P\rangle_3 = f_P(D_P) \equiv \frac{d^2(2\zeta)^2}{(2d^2)(-2\zeta^2)} \equiv 1 \bmod (\mathbf{F}_p^\times)^3.$$

2. To calculate $\langle P, Q\rangle_3$, choose β such that $\beta^3 = 3 - d^2$ and let $D_Q = [(\beta, -r)] + [(\beta\zeta, -r)] + [(\beta\zeta^2, -r)] - [(1, \sqrt{1 + d^2})] - [(1, -\sqrt{1 + d^2})] - [(-\alpha^2, -dr)]$ be a divisor on E. Then $[Q] - [\infty]$ is equivalent to D_Q modulo principal divisors and

$$\langle P, Q\rangle_3 = f_P(D_Q) \equiv \frac{1}{(2d)\zeta^2} \equiv \zeta \bmod (\mathbf{F}_p^\times)^3.$$

We also calculate

$$\langle Q, P\rangle_3 = f_Q(D_P) \equiv \frac{9d^2 \cdot 4(1-\zeta)(1-\zeta^2)}{(6d^2\sqrt{-3})(2\zeta)} \equiv \zeta^{-1} \bmod (\mathbf{F}_p^\times)^3$$

since P is equivalent to D_P in the divisor class group and since -3 is a quadratic residue mod p. Thus we see that $\langle P, Q\rangle_3\langle Q, P\rangle_3 \equiv 1 \bmod (\mathbf{F}_p^\times)^3$.

3. Let $D'_Q = [(-\alpha^2\zeta, dr)] + [(-\alpha^2\zeta^2, dr)] - 2[(-\alpha^2, -dr)]$ be a divisor on E. Then $[Q] - [\infty]$ is also equivalent to D'_Q and

$$\langle Q, Q\rangle_3 = f_Q(D'_Q) \equiv \frac{9d^2 \cdot 4(1-\zeta)(1-\zeta^2)}{4 \cdot 9d^2} \equiv 3 \bmod (\mathbf{F}_p^\times)^3.$$

Thus, in order for self pairings to be trivial, we need 3 to be a cube mod p.

Therefore by Theorem 3.3, we see that 3 is a cube mod p if and only if all elements of $E[3]$ have trivial self pairings. □

4.3 Complex Multiplication

We can use the fact that elliptic curves defined over finite fields have complex multiplication to restate Theorem 3.4 as follows.

Theorem 4.2. *Let E be an ordinary elliptic curve defined over $\mathbf{F}_p$ for some prime p and let n be a positive integer such that $E[n] \subset E(\mathbf{F}_p)$. Assume that End$(E)$ is the ring of integers in an imaginary quadratic field $\mathbf{Q}(\sqrt{-D})$ for some squarefree integer D.*

(A) *If $D \equiv 3 \bmod 4$, then we can write $4p = A^2 + DB^2$ for some integers A and B with $n|B$. Moreover, $\tau_n(P, P) = 1$ for all $P \in E[n]$ if and only if $n^2|B$.*

(B) *If $D \equiv 1, 2 \bmod 4$, then we can write $p = A^2 + DB^2$ for some integers A and B with $n|B$. Moreover, $\tau_n(P, P) = 1$ for all $P \in E[n]$ if and only if $n^2|B$.*

Proof. For Case A, we have $D \equiv 3 \bmod 4$. This gives us that $\mathrm{End}(E) = \mathbf{Z}\left[\frac{1+\sqrt{-D}}{2}\right]$. We can view the Frobenius endomorphism, ϕ, as an element of this ring. We write $\phi = a + b\left(\frac{1+\sqrt{-D}}{2}\right) = \frac{(2a+b)+b\sqrt{-D}}{2}$. Since we know that $\phi\overline{\phi} = p$, we have that $4p = (2a+b)^2 + b^2D$. The assumption that $E[n]$ is defined over $\mathbf{F}_p$ forces $\phi \equiv 1 \bmod n$, so we have that $a \equiv 1 \bmod n$ and that $n|b$.

If $D > 3$, then a and b depend on p up to sign since ± 1 are the only units in $\mathrm{End}(E)$. By Theorem 3.4, $\tau_n(P, P) = 1$ for all $P \in E[n]$ if and only if ϕ is an integer mod n^2. This occurs if and only if $n^2|b$.

Now suppose that $D = 3$. By the above, we have $4p = A^2 + 3B^2$ for some integers A and B with $n|B$. The units in $\mathrm{End}(E)$ are generated by $u = \frac{1+\sqrt{-3}}{2}$, a sixth root of unity. Thus we have

$$\begin{aligned} \phi &= u^k\left(\tfrac{A \pm B\sqrt{-3}}{2}\right) \\ &= u^k\left(\tfrac{A \mp B}{2} \pm B\left(\tfrac{1+\sqrt{-3}}{2}\right)\right) \\ &= u^k\left(\tfrac{A \mp B}{2}\right) \pm u^{k+1}B, \end{aligned}$$

for some integer k. Since ϕ must be congruent to 1 mod n and $n|B$, we must have that $\alpha u^k \equiv 1 \bmod n$ for some integer α. Thus, we see that $u^k = \pm 1$. We now have $\phi = x \pm B\left(\frac{1+\sqrt{-3}}{2}\right)$ for some integer x. Therefore ϕ is congruent to an integer mod n^2 if and only if $n^2|B$.

In Case B, we have $D \equiv 1, 2 \bmod 4$ and so $\mathrm{End}(E) = \mathbf{Z}[\sqrt{-D}]$. We view the Frobenius endomorphism as an element $\phi = a + b\sqrt{-D}$ in this ring. Since $\phi\overline{\phi} = p$, we have that $p = a^2 + Db^2$. The assumption that $E[n] \subset E(\mathbf{F}_p)$ gives us that

$a \equiv 1 \bmod n$ and $n|b$. As before, if $D > 1$, then a and b depend on p up to sign since ± 1 are the only units. As above, we have that all Tate-Lichtenbaum self pairings are trivial on $E[n]$ if and only if $n^2|b$.

Now suppose that $D = 1$. We write $p = A^2 + B^2$ for some integers A and B with $n|B$. The units in $\mathrm{End}(E)$ are generated by i, where $i^2 = -1$. Thus, we have $\phi = i^k(A \pm Bi) = i^k A \pm i^{k+1} B$ for some integer k. Since ϕ is congruent to 1 mod n and $n|B$, we must have $i^k = \pm 1$. Thus, ϕ is congruent to an integer mod n^2 if and only if $n^2|B$. □

In particular, we can use the fact that $E : y^2 = x^3 + d^2$ has complex multiplication by the ring $\mathbf{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ to restate Theorem 3.4 as follows.

Theorem 4.3. *Let E be defined by $y^2 = x^3 + d^2$ over $\mathbf{F}_p$ with $p \equiv 1 \bmod 3$ and let n be a positive integer such that $E[n] \subset E(\mathbf{F}_p)$. Then $\tau_n(P, P) = 1$ for all $P \in E[n]$ if and only if $4p = A^2 + 3B^2$ for some integers A and B with $B \equiv 0 \mod n^2$.*

Proof. This follows from Theorem 4.2. □

Remark: Observe that when $n > 2$, we need only consider the case that $p \equiv 1 \bmod 3$, since otherwise E would be supersingular and thus have $p + 1$ points over $\mathbf{F}_p$. Since $E[n] \subset E(\mathbf{F}_p)$, we have $n^2|p + 1$ and so $n|p + 1$. However, the definition of the Tate-Lichtenbaum pairing requires that $n|p - 1$, hence $n|2$, a contradiction.

We now have the following corollary.

Corollary 4.4. *Let E be the elliptic curve defined by $y^2 = x^3 + d^2$ over $\mathbf{F}_p$ where p is a prime such that $p \equiv 1 \bmod 3$. Suppose that $E[3] \subset E(\mathbf{F}_p)$. Then the following*

are equivalent:

1. $\tau_3(P,P) = 1$ *for all* $P \in E[3]$*;*

2. $4p = A^2 + 243B^2$ *for some integers* A *and* B*.*

Note that it is a classical result that if $p \equiv 1 \bmod 3$, then there are integers A and B such that $4p = A^2 + 27B^2$. Moreover, A is unique if we require that $A \equiv 1 \bmod 3$.

As an example of the above result, consider the elliptic curve defined by $E := y^2 = x^3 + 1$ over $\mathbf{F}_{307}$. Since we can write $4(307) = 16^2 + 243(2^2)$ and since $3|6$, we conclude that $\tau_3(P,P) = 1$ for all 3-torsion points P. However, the same curve defined over $\mathbf{F}_{283}$ has nontrivial self-pairings on $E[3]$ since $4(283) = 16^2 + 27(4^2)$ and 4 is not divisible by 3. In particular, the 3-torsion point $S = (37, 194)$ pairs nontrivially with itself and $\tau_3(S,S) = 238$, a cube root of unity in $\mathbf{F}_{283}$.

4.4 Consequences

The following classical result due to Jacobi ([1], Corollary 2.6.10) now follows from Corollary 4.4 and Theorem 4.1 applied to the case $d = 4$.

Theorem 4.5. *Let* $p \equiv 1 \bmod 3$*. Then 3 is a cubic residue mod* p *if and only if there exist integers* A *and* B *with* $4p = A^2 + 243B^2$*.*

Since 3 is a cubic residue for one-third of all primes p such that $p \equiv 1 \bmod 3$, we obtain the following.

Theorem 4.6. *Let E be the elliptic curve defined by $y^2 = x^3 + 16$ over $\mathbf{F}_p$. For one third of all primes $p \equiv 1 \bmod 3$, $\tau_3(P, P) = 1$ for all $P \in E[3]$.*

Chapter 5

The Curve: $E : y^2 = x^3 - d^2x$

In this chapter, we consider the elliptic curve given by $E : y^2 = x^3 - d^2x$ defined over a field $\mathbf{F}_p$ for some prime p and some nonzero integer d. In Section 5.1 we give an overview of the properties of E. In Section 5.2 we analyze Tate-Lichtenbaum self pairings on $E[2]$. We use Miller's algorithm to explicitly calculate the Tate-Lichtenbaum pairing on generators of $E[2]$ and we analyze the conditions that yield trivial self-pairings. We also use complex multiplication to simplify the condition that ϕ is integer multiplication on $E[4]$. We then combine these results to obtain a theorem about primes congruent to $1 \bmod 8$. In Section 5.3 we analyze Tate-Lichtenbaum self pairings on $E[4]$ in the same manner. Complex multiplication is used to characterize self pairings in terms of the action of the Frobenius map on $E[16]$. Combining this with explicit calculations of pairings yields a classical reciprocity result.

5.1 Properties of $E : y^2 = x^3 - d^2x$

Let $E_d : y^2 = x^3 - d^2x$ be defined over $\mathbf{F}_p$ where p is an odd prime. We again restrict to the case where $E[n] \subset E(\mathbf{F}_p)$ (hence $p \equiv 1 \bmod n$). Under this restriction, $\mathbf{F}_p$ contains μ_n, the nth roots of unity. When n is even, we further restrict to the case where $p \equiv 1 \bmod 4$. This guarantees that in addition to nth

roots of unity, $\mathbf{F}_p$ also contains the 4th roots of unity. From now on we let $E = E_d$.

The torsion subgroup $E[2]$ is generated by the $\mathbf{F}_p$-rational points $R = (0, 0)$ and $S = (d, 0)$. If d is a quadratic residue mod p and $d \equiv \delta^2 \bmod p$, then $E[4]$ is generated by the $\mathbf{F}_p$-rational points $P = (i\delta^2, (1-i)\delta^3)$ and $Q = (\delta^2(1-\sqrt{2}), (\sqrt{2}-2)\delta^3)$ where $i^2 = 1$. Observe that $2P = R$ and $2Q = S$. Also note that $E[4]$ is rational over $\mathbf{F}_p$ if and only if both -1 and 2 are quadratic residues mod p. This occurs if and only if $p \equiv 1 \bmod 8$.

5.2 Self pairings on $E[2]$

We now characterize when Tate-Lichtenbaum self pairings are trivial on $E[2]$ using Theorem 3.3 and Theorem 4.2.

5.2.1 Explicit Calculations of the Tate-Lichtenbaum pairing on $E[2]$

Explicit calculations of the Tate-Lichtenbaum pairings for $E[2]$ yield the following theorem.

Theorem 5.1. *Let $p > 2$ be prime and let $E : y^2 = x^3 - d^2x$ be defined over $\mathbf{F}_p$. Then the following are equivalent:*

1. *$\tau_2(P, P) = 1$ for all $P \in E[2]$;*
2. *$p \equiv 1 \bmod 8$.*

Proof. By Theorem 3.3, all self pairings are trivial if and only if generators of $E[2]$ pair both trivially and antisymmetrically. Let $f_R = x$ and let $f_S = x - d$. Let $T = (-d, 0)$ and notice that $R + S + T = \infty$.

1. Let $D_R = [R+T]-[T] = [S]-[T]$. Then $\langle R,R\rangle_2 = f_R(D_R) = \frac{f_R(S)}{f_R(T)} = \frac{d}{-d} = -1$. Therefore we need -1 to be a square mod p, which is equivalent to $p \equiv 1 \bmod 4$.

2. Let $D_S = [S+T]-[T] = [R]-[T]$. Then $\langle S,S\rangle_2 = f_S(D_S) = \frac{f_S(R)}{f_S(T)} = \frac{-d}{-2d} = \frac{1}{2}$. Therefore we need 2 to be a square mod p. Since -1 must also be a square, this occurs if and only if $p \equiv 1 \bmod 8$.

3. It remains to characterize when $\langle R,S\rangle_2 \cdot \langle S,R\rangle_2 = 1$. Let $D'_R = [-P]-[P]$ and let $D'_S = [-Q]-[Q]$. Then

$$\langle R,S\rangle_2 \cdot \langle S,R\rangle_2 = f_R(D'_S)\cdot f_S(D'_R) = \frac{f_R(-Q)}{f_R(Q)}\cdot\frac{f_S(-P)}{f_S(P)} = 1.$$

   This shows that the Tate-Lichtenbaum pairing is antisymmetric on $E[2]$.

Thus, Tate-Lichtenbaum self pairings are trivial for all 2-torsion points if and only if $p \equiv 1 \bmod 8$. □

5.2.2 Complex Multiplication

Complex multiplication can be used to recognize when the Frobenius endomorphism acts like integer multiplication on $E[n^2]$.

Theorem 5.2. *Let p be an odd prime and let $n > 2$. Define E to be the elliptic curve given by $y^2 = x^3 - d^2x$ over $\mathbf{F}_p$. Assume that $E[n] \subset E(\mathbf{F}_p)$. Then $p \equiv 1 \bmod 4$. Moreover, $\tau_n(P,P) = 1$ for all $P \in E[n]$ if and only if we can express $p = A^2 + B^2$ for some integers A and B with $n^2|A$.*

Proof. If $p \equiv 3 \bmod 4$, then E_d is supersingular and has $p+1$ points over $\mathbf{F}_p$. Thus we have that $n^2 | p+1$ since $E[n] \subset E(\mathbf{F}_p)$. We also have that $n|(p-1)$, and so n divides $(p+1)-(p-1) = 2$. This is a contradiction since we assume $n > 2$. Thus, $p \equiv 1 \bmod 4$. The second half of the theorem follows directly from Theorem 4.2. □

When $n = 2$, we have the following proposition.

Proposition 5.3. *Let $p \equiv 1 \bmod 4$ be a prime. Define E to be the elliptic curve given by $y^2 = x^3 - d^2x$ over $\mathbf{F}_p$. Then $\tau_2(P,P) = 1$ for all $P \in E[2]$ if and only if we can express $p = A^2 + 16B^2$ for some integers A and B.*

Proof. In Theorem 5.2, we used the hypothesis that $n > 2$ to show that p must be congruent to $1 \bmod 4$. We now assume that $p \equiv 1 \bmod 4$, and hence we have $p = A^2 + B^2$ for some odd integer A and some even integer B. The remainder of the proof is identical to that of Theorem 4.2. □

5.2.3 Consequences

Putting together Proposition 5.3 and Theorem 5.1 now yields the following result.

Theorem 5.4. *Let p be prime. Then $p \equiv 1 \bmod 8$ if and only if $p = x^2 + 16y^2$ for some integers x and y.*

We can also prove this directly. If $p = x^2 + 16y^2$ for some integers x and y, then it is clear that $p \equiv 1 \bmod 8$. Conversely, if we have $p \equiv 1 \bmod 8$, then p is also congruent to $1 \bmod 4$, so there are integers u and v such that $p = u^2 + v^2$. Since p

is odd, we take u to be odd and v to be even. This implies that $u^2 \equiv 1 \bmod 8$, and hence $v^2 \equiv 0 \bmod 8$. Therefore, we have $4|v$.

5.3 Self pairings on $E[4]$

In this section we characterize when Tate-Lichtenbaum self pairings are trivial on 4-torsion points.

5.3.1 Explicit Calculations of the Tate-Lichtenbaum Pairing on $E[4]$

Explicit calculations of the Tate-Lichtenbaum pairing for $E[4]$ yield the following theorem.

Theorem 5.5. *Let $p \equiv 1 \bmod 8$ be prime and let $E : y^2 = x^3 - d^2x$ be defined over $\mathbf{F}_p$. Suppose that d is a quadratic residue mod p. Then the following are equivalent:*

1. *$\tau_4(T, T) = 1$ for all $T \in E[4]$;*

2. *-2 is an octic residue mod p.*

Proof. Recall that $E[4]$ is rational over $\mathbf{F}_p$ if and only if d is a quadratic residue mod p. Let $d \equiv \delta^2 \bmod p$ and let i be a primitive fourth root of unity. Then $P = (i\delta^2, (1-i)\delta^3)$ and $Q = (\delta^2(1-\sqrt{2}), (\sqrt{2}-2)\delta^3)$ generate $E[4]$. These points are rational over $\mathbf{F}_p$ since $p \equiv 1 \bmod 8$.

We use Miller's algorithm to find a function whose divisor is $4[P] - 4[\infty]$. The function $f_P = \frac{(-(i+1)\delta x - y)^2}{x}$ has this property. We also use Miller's algorithm to find the function $f_Q = \frac{((\sqrt{2}-1)\delta(x-\delta^2)-y)^2}{x-\sqrt{2}}$ whose divisor is $\mathrm{div}(f_Q) = 4[Q] - 4[\infty]$.

By Theorem 3.3, we need only check pairings on the generators. Self pairings are trivial if and only if (1) $\langle P, P\rangle_4 \equiv 1 \bmod (\mathbf{F}_p)^4$; (2) $\langle Q, Q\rangle_4 \equiv 1 \bmod (\mathbf{F}_p)^4$; and (3) $\langle P, Q\rangle_4\langle Q, P\rangle_4 \equiv 1 \bmod (\mathbf{F}_p)^4$. We explicitly compute these Tate-Lichtenbaum pairings.

1. Let $D'_P = [P+S]-[S] = [(-i\delta^2, (-i-1)\delta^3)]-[(\delta^2, 0)]$. Then D'_P is equivalent to $[P]-[\infty]$ modulo principal divisors and

$$\begin{aligned}\langle P, P\rangle_4 &= f_P(D'_P)\\ &= \tfrac{f_P(P+S)}{f_P(S)}\\ &= -2.\end{aligned}$$

   Therefore, in order for self pairings to be trivial we require that 2 be a fourth power mod p (since $p \equiv 1 \bmod 8$ guarantees that -1 is a quartic residue).

2. To calculate $\langle P, Q\rangle_4$, let $D_Q = [Q+S]-[S] = [((1-\sqrt{2})\delta^2, -(\sqrt{2}-2)\delta^3)]-[(\delta^2, 0)]$. (Notice that $Q+S = -Q$.) Then D_Q is equivalent to $[Q]-[\infty]$ modulo principal divisors and

$$\begin{aligned}\langle P, Q\rangle_4 &= f_P(D_Q)\\ &= \tfrac{f_P(-Q)}{f_P(S)}\\ &= -(\sqrt{2}-1)^2(i-1).\end{aligned}$$

   To calculate $\langle Q, P\rangle_4$, let $D_P = [P+R]-[R] = [(i\delta^2, -(1-i)\delta^3)]-[(0,0)]$. (Notice that $P+R = -P$.) Then D_P is equivalent to $[P]-[\infty]$ modulo

principal divisors and

$$\begin{aligned}\langle Q, P\rangle_4 &= f_Q(D_P) \\ &= \tfrac{f_Q(-P)}{f_Q(R)} \\ &= 2(i-1).\end{aligned}$$

In order for self pairings to be trivial, we need $\langle P, Q\rangle_4 \cdot \langle Q, P\rangle_4 \equiv 1 \bmod (\mathbf{F}_p)^4$ by Theorem 3.3. Hence, we need $-2(\sqrt{2}-1)^2(i-1)^2 = 4i(\sqrt{2}-1)^2$ to be a fourth power. By hypothesis, 4 is already a fourth power. Therefore trivial self pairings require that $i(\sqrt{2}-1)^2$ be a quartic residue.

3. Let $D'_Q = [Q+R] - [R] = [(\delta^2(\sqrt{2}+1), -(\sqrt{2}+2)\delta^3)] - [(0,0)]$. Then D'_Q is equivalent to $[Q] - [\infty]$ modulo principal divisors and

$$\begin{aligned}\langle Q, Q\rangle_4 &= f_Q(D'_Q) \\ &= \tfrac{f_Q(Q+R)}{f_Q(R)} \\ &= \tfrac{8\sqrt{2}}{-(\sqrt{2}-1)^2}.\end{aligned}$$

In order for self pairings to be trivial, we need $\frac{8\sqrt{2}}{-(\sqrt{2}-1)^2}$ to be a fourth power mod p. By hypothesis, -8 is already a quartic residue, hence we require that $\frac{\sqrt{2}}{(\sqrt{2}-1)^2}$ is a fourth power mod p.

Suppose that $p \equiv 1 \bmod 16$. Then i is a quartic residue mod p. We then have that $\langle T, T\rangle_4 \equiv 1 \bmod (\mathbf{F}_p)^4$ for all $T \in E[4]$ if and only if 2, $(\sqrt{2}-1)^2$, and $\frac{\sqrt{2}}{(\sqrt{2}-1)^2}$ are all fourth powers mod p. This occurs if and only if $\sqrt{2}-1$ is a quadratic residue and 2 is an octic residue mod p. The following supplement to Scholz's reciprocity law [1] proves that for $p \equiv 1 \bmod 16$, the second condition implies the first (note that $(\sqrt{2}-1)(\sqrt{2}+1) = 1$).

Lemma 5.6. *Let $q \equiv 1 \bmod 8$ be a prime. Define*

$$\left(\frac{q}{2}\right)_4 = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 16 \\ -1 & \text{if } p \equiv 9 \bmod 16. \end{cases}$$

Then $\left(\frac{2}{q}\right)_4 \left(\frac{q}{2}\right)_4 = \left(\frac{\sqrt{2}+1}{q}\right)_2$, where $\left(\frac{\cdot}{q}\right)_n$ is the nth-power residue symbol mod q.

(See [9], Proposition 5.8 for a proof.)

Hence, all self pairings are trivial if and only if 2 is an octic residue mod p. Since $p \equiv 1 \bmod 16$, this is equivalent to -2 being an octic residue mod p.

Now consider the case that $p \equiv 9 \bmod 16$. Suppose that $\langle T, T \rangle_4 = 1$ for all $T \in E[4]$. As before, the above conditions imply that $2, i(\sqrt{2}-1)^2$, and $\frac{\sqrt{2}}{(\sqrt{2}-1)^2}$ are all fourth powers mod p. Putting the last two conditions together yields that $\sqrt{-2}$ is a fourth power, hence -2 is an octic residue. Hence, the condition that 2 is a fourth power is redundant since $p \equiv 1 \bmod 8$ implies that -1 is a fourth power mod p.

Conversely, suppose that -2 is an octic residue mod p. Since for $p \equiv 9 \bmod 16$ we have that -1 is not an octic residue, this implies that 2 is also not an octic residue. We want to show that this implies that the following:

1. 2 is a quartic residue mod p;
2. $i(\sqrt{2}-1)^2$ is a quartic residue mod p;
3. $\frac{\sqrt{2}}{(\sqrt{2}-1)^2}$ is a quartic residue mod p.

We automatically have that 2 is a quartic residue since $p \equiv 1 \bmod 8$. By Lemma 5.6, we see that $\sqrt{2}-1$ is not a quadratic residue, hence $(\sqrt{2}-1)^2$ is a

quadratic residue, but not a quartic residue. Likewise, $p \equiv 9 \bmod 16$ implies that i is a quadratic residue but not a quartic residue. We conclude that $i(\sqrt{2}-1)^2$ is a fourth power. Similarly, $\frac{\sqrt{2}}{(\sqrt{2}-1)^2}$ is a fourth power since neither $\sqrt{2}$ nor $(\sqrt{2}-1)^2$ are fourth powers. Thus, all three of the conditions above hold, and we conclude that $\langle R, R\rangle_4 = 1$ for all $R \in E[4]$. □

5.3.2 Consequences

When $n = 4$, we have the following corollary to Theorem 5.2.

Corollary 5.7. *Let $p \equiv 1 \bmod 4$ be a prime. Define E to be the elliptic curve given by $y^2 = x^3 - d^2x$ over $\mathbf{F}_p$ and assume that d is a quadratic residue mod p. Suppose that $E[4] \subset E(\mathbf{F}_p)$. Then $\tau_4(P, P) = 1$ for all $P \in E[4]$ if and only if we can express $p = A^2 + 256B^2$ for some integers A and B.*

Recall that $p \equiv 1 \bmod 8$ implies that -1 is a quartic residue mod p. Putting together Corollary 5.7 and Theorem 5.5 now yields the following result.

Theorem 5.8. *Let $p \equiv 1 \bmod 8$ be prime. Then -2 is an octic residue mod p if and only if $p = x^2 + 256y^2$ for some integers x and y.*

Furthermore, for $p \equiv 1 \bmod 16$, this yields the well-known fact that 2 is an octic residue mod p if and only if $p = x^2 + 256y^2$ for some integers x and y (see [1], Corollary 7.5.8).

Chapter 6

Tate-Lichtenbaum Self Pairings on Jacobians of Curves

In Chapter 3 we saw how alternating Tate-Lichtenbaum self pairings relate to the Frobenius endomorphism for elliptic curves. In this chapter we generalize this result to Jacobians of higher genus curves.

In Section 6.1 we present the generalized result. The remainder of the chapter is dedicated to the proof. In Section 6.2 we analyze the conditions on the Frobenius map (on n^2-torsion) that make the Tate-Lichtenbaum pairing antisymmetric. In Section 6.3 we analyze the conditions that make self pairings trivial on generators of n-torsion.

6.1 Self Pairings on Higher Genus Jacobians

Let C be a genus g algebraic curve defined over a finite field $\mathbf{F}_q$ where q is a prime power. Let J represent the Jacobian of C. As before, let ϕ represent the qth power Frobenius endomorphism. Let n be an integer with $\gcd(n, q) = 1$. We assume that $J[n] \subset J(\mathbf{F}_q)$

Since J is the Jacobian of a genus g curve, the torsion group $J[n]$ is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^{2g}$. Let $\{Q_{\pm i}\}_{i=1}^{g}$ denote generators of $J[n^2]$. The following lemma specifies

a choice of generators and is a convenient way of expressing the nondegeneracy of the Weil pairing, e_n. Let I_k denote the $k \times k$ identity matrix.

Lemma 6.1. *Let ζ be a fixed primitive nth root of unity. Define $f_n : J[n] \times J[n] \to \mathbf{Z}/n\mathbf{Z}$ by $e_n(Q,R) = \zeta^{f_n(Q,R)}$. Then there is a choice of generators*

$$\{Q_1, Q_2, \ldots, Q_g, Q_{-1}, \ldots, Q_{-g}\}$$

such that the matrix associated to $f_n(Q_i, Q_j)$ is $\begin{bmatrix} 0 & I_g \\ -I_g & 0 \end{bmatrix} \bmod n$, *with respect to the above ordering of the generators.*

Proof. First notice that f_n inherits nondegeneracy and bilinearity from the Weil pairing. Antisymmetry of the Weil pairing implies that $f_n(P,Q) \equiv -f_n(Q,P) \bmod n$, so f_n is antisymmetric. We show that $J[n]$ has a symplectic basis

$$\{Q_1, Q_2, \ldots, Q_g, Q_{-1}, \ldots, Q_{-g}\}$$

such that $f_n(Q_i, Q_j) \equiv \delta_{i,-j} \bmod n$ for $i > 0$ (where δ is the Kronecker delta function).

Let $\{P_1, \ldots P_{2g}\}$ be any basis for $J[n]$ and let $Q_1 = P_1$. Let $a_i = f_n(P_1, P_i)$. If $d = \gcd(a_1, \ldots, a_{2g}, n)$, then

$$e_n\left(\frac{n}{d}P_1, P_i\right) = e_n(P_1, P_i)^{n/d} = (\zeta^{a_i/d})^n = 1$$

for all i. Nondegeneracy of the Weil pairing then implies that $\frac{n}{d}P_1 = \mathrm{id}_J$ which implies that $d = 1$ since P_1 is a generator of the n-torsion. Therefore $\sum x_i a_i + xn = 1$ for some integers x_i and x. Now $P = \sum x_i P_i$ has the property that $f_n(P_1, P) = 1$. Define $Q_{-1} = P$.

We proceed by induction on g and assume that $g > 1$. Let

$$W = \{P \in J[n] \mid f_n(Q_1, P) \equiv f_n(Q_{-1}, P) \equiv 0 \bmod n\},$$

and let $Q \in J[n]$ be any point. Set $Q' = Q - f_n(Q, Q_{-1})Q_1 + f_n(Q, Q_1)Q_{-1}$. Then Q' is in W. Hence, we see that $J[n] = (\mathbf{Z}/n\mathbf{Z})Q_1 \oplus (\mathbf{Z}/n\mathbf{Z})Q_{-1} \oplus W$.

We claim that f_n remains nondegenerate when restricted to W. Let $P \in W$ be nontrivial. Then nondegeneracy of f_n on $J[n]$ implies that there is a point $Q \in J[n]$ such that $f_n(P, Q) \not\equiv 0$. As above, let $Q' = Q - f_n(Q, Q_{-1})Q_1 + f_n(Q, Q_1)Q_{-1}$. Then $e_n(P, Q') = e_n(P, Q)$ since $P \in W$. Thus, $f_n(P, Q') \equiv f_n(P, Q) \not\equiv 0 \bmod n$ and $Q' \in W$ by the argument given above. This proves nondegeneracy of f_n restricted to W.

By induction, there exists a symplectic basis $\{Q_2, \ldots, Q_g, Q_{-2}, \ldots, Q_{-g}\}$ for W Inclusion of Q_1 and Q_{-1} in this basis gives the desired basis for $J[n]$. □

Let $\{Q_1, Q_2, \ldots, Q_g, Q_{-1}, \ldots, Q_{-g}\}$ be a basis of $J[n^2]$ such that $\{nQ_{\pm i}\}_{i=1}^g$ is the basis of $J[n]$ given by Lemma 6.1. Let σ_i be the sign of i. The importance of this lemma is that we now have that

$$e_n(nQ_i, nQ_j) = \begin{cases} \zeta^{\sigma_i} & \text{if } i = -j \\ 1 & \text{otherwise.} \end{cases} \tag{6.1}$$

With respect to this basis, we now have the following theorem.

Theorem 6.2. *Let $\{Q_1, Q_2, \ldots, Q_g, Q_{-1}, \ldots, Q_{-g}\}$ be a basis for $J[n^2]$ such that $\{nQ_{\pm i}\}_{i=1}^g$ is a basis of $J[n]$ as given by Lemma 6.1. The Tate-Lichtenbaum pairing on $J[n]$ is then antisymmetric if and only if the Frobenius endomorphism re-*

stricted to $J[n^2]$ *(with respect to this basis) is given by a matrix mod* n^2 *of the form* $\begin{bmatrix} M & N_1 \\ N_2 & M^\top \end{bmatrix}$ *where* M *is a* $g \times g$ *matrix such that* $M \bmod n$ *is the identity matrix and* M *has constant diagonal mod* n^2 *when* n *is odd and mod* $\frac{n^2}{2}$ *when* n *is even; and* N_i $(i = 1, 2)$ *is an antisymmetric* $g \times g$ *matrix such that* $N_i \bmod n$ *is the zero matrix.*

In addition, $\tau_n(P, P) = 1$ *for all* $P \in J[n]$ *if and only if each* N_i *has zero diagonal.*

Remark: If the Tate-Lichtenbaum pairing is antisymmetric (or, more specifically, has all trivial self pairings on $J[n]$), then there exists a basis for $J[n^2]$ such that the Frobenius map on $J[n^2]$ is a matrix of the form given in Theorem 6.2 (namely, an e_n-symplectic basis). However, if there is some basis such that the Frobenius map on $J[n^2]$ has the form given in Theorem 6.2, then we cannot conclude anything about self pairings. The converse is only true if we fix an e_n-symplectic basis as in Lemma 6.1. As a result, we can use Theorem 6.2 to show the existence of an element that has a nontrivial self pairing, but we cannot use the theorem to show that all self pairings on $J[n]$ are trivial.

Our proof of Theorem 6.2 relies on Theorem 3.3, which states that the Tate-Lichtenbaum pairing has the property that $\tau_n(P, P) = 1$ for all $P \in J[n]$ if and only if self-pairings are trivial for the n-torsion generators and τ_n is antisymmetric on the generators. The proof of Theorem 6.2 addresses each condition separately.

6.2 Antisymmetry of the Tate-Lichtenbaum Pairing

Since all of the n-torsion points are rational, the Frobenius endomorphism ϕ acts trivially on $J[n]$. Therefore the matrix corresponding to the action of ϕ on $J[n^2]$ is congruent to the identity matrix mod n. Write $\phi(Q_i) = \sum_{k=-g}^{g}{}' a_{k,i}Q_k$ (where the prime denotes summation over $k \neq 0$). Since $i \neq k$ implies that $n \mid a_{k,i}$, we write $a_{k,i} = n\ b_{k,i}$ for some integer $b_{k,i}$. Similarly, we can write $a_{i,i} - 1 = nA_i$ for some integer A_i since $a_{i,i} \equiv 1 \bmod n$.

Combining this with Theorem 2.5 gives the following lemma (recall that $\sigma_i = \text{sign}(i)$).

Lemma 6.3. *For $i \neq j$,*

$$\tau_n(nQ_i, nQ_j) = \begin{cases} \zeta^{\sigma_i A_{-i}} & \text{if } j = -i \\ \zeta^{\sigma_i b_{-i,j}} & \text{otherwise.} \end{cases} \tag{6.2}$$

Proof. Assume that $i \neq j$. By bilinearity, we see that

$$\begin{aligned} \tau_n(nQ_i, nQ_j) &= e_{n^2}(Q_i, \phi(Q_j) - Q_j) \\ &= e_{n^2}\left(Q_i, \sum_{k=-g}^{g}{}' a_{k,j}Q_k - Q_j\right) \\ &= e_{n^2}(Q_i, Q_j)^{a_{j,j}-1} \cdot \prod_{\substack{k=-g \\ k\neq j}}^{g}{}' e_{n^2}(Q_i, Q_k)^{a_{k,j}} \\ &= e_n(nQ_i, nQ_j)^{A_j} \cdot \prod_{\substack{k=-g \\ k\neq j}}^{g}{}' e_n(nQ_i, nQ_k)^{b_{k,j}}. \end{aligned} \tag{6.3}$$

By Equation 6.1, all factors but one vanish. If $j = -i$, then $\tau_n(nQ_i, nQ_{-i}) = e_n(nQ_i, nQ_{-i})^{A_{-i}}$. Otherwise, we get $\tau_n(nQ_i, nQ_j) = e_n(nQ_i, nQ_{-i})^{b_{-i,j}}$. □

As a result of Lemma 6.3 we get that $\tau_n(nQ_i, nQ_j) = \tau_n(nQ_j, nQ_i)^{-1}$ if and only if:

$$\begin{cases} \zeta^{\sigma_i A_{-i}} = \zeta^{-\sigma_{-i} A_i} & \text{if } j = -i \\ \zeta^{\sigma_i b_{-i,j}} = \zeta^{-\sigma_j b_{-j,i}} & \text{otherwise.} \end{cases}$$

Hence, when $j = -i$, then $\tau_n(nQ_i, nQ_{-i}) = \tau_n(nQ_{-1}, nQ_i)^{-1}$ if and only if $\zeta^{A_{-i}} = \zeta^{A_i}$, which occurs if and only if $A_{-i} \equiv A_i \bmod n$. Since $nA_k = a_{k,k} - 1$, we obtain the relations $a_{i,i} \equiv a_{-i,-i} \mod n^2$.

If $j \neq -i$, then $\tau_n(nQ_i, nQ_j) = \tau_n(nQ_j, nQ_i)$ if and only if

$$e_n(nQ_i, nQ_{-i})^{b_{-i,j}} = e_n(nQ_j, nQ_{-j})^{-b_{-j,i}}.$$

By Equation 6.1, $e_n(nQ_k, nQ_{-k}) = \zeta$ when $k > 0$ and equals ζ^{-1} otherwise. This shows that antisymmetry holds for $j \neq i$ if and only if

$$\begin{aligned} \zeta^{b_{-i,j}} &= \zeta^{-b_{-j,i}} \quad \text{for } i, j > 0 \qquad \text{or} \quad i, j < 0 \\ \zeta^{b_{-i,j}} &= \zeta^{b_{-j,i}} \quad \text{for } i > 0 > j \quad \text{or} \quad i < 0 < j. \end{aligned}$$

Since $a_{i,j} = n\, b_{i,j}$ (for $i \neq j$), we find that antisymmetry holds if and only if

$$\begin{aligned} a_{-i,j} &\equiv -a_{-j,i} \mod n^2 \quad \text{for } i, j > 0 \qquad \text{or} \quad i, j < 0 \\ a_{-i,j} &\equiv a_{-j,i} \mod n^2 \quad \text{for } i < 0 < j \quad \text{or} \quad i > 0 > j. \end{aligned} \tag{6.4}$$

It remains to prove that $a_{i,i} \equiv a_{j,j} \bmod \frac{n^2}{2}$ for all $i, j \in \{1, \ldots g, -1, ..., -g\}$. (If n is odd, this is the same as showing equivalence mod n^2.) Galois invariance of the Weil pairing implies that $e_{n^2}(\phi(Q_i), \phi(Q_j)) = \phi(e_{n^2}(Q_i, Q_j)) = e_{n^2}(Q_i, Q_j)^q$. Recall that we write $\phi(Q_i) = \sum_{k=1}^{2g} a_{k,i} Q_k$. Consider the case that $j = -i$. We get

that

$$\begin{aligned} e_{n^2}(\phi(Q_i), \phi(Q_{-i})) &= e_{n^2}\left(\sum_{k=-g}^{g}{}' a_{k,i}Q_k, \sum_{\ell=-g}^{g}{}' a_{\ell,-i}Q_\ell\right) \\ &= \prod_{k=-g}^{g}{}' \prod_{\ell=-g}^{g}{}' e_n(a_{k,i}Q_k, a_{\ell,-i}Q_\ell). \end{aligned}$$

We separate the product into factors that allow us to deal with the diagonal entries $a_{k,k}$ separately. Recall that $a_{i,j} = nb_{i,j}$ for $i \neq j$. Then $e_{n^2}(\phi(Q_i), \phi(Q_{-i}))$ becomes

$$\begin{aligned} & e_{n^2}(Q_i, Q_{-i})^{a_{i,i}a_{-i,-i}} \times \prod_{\substack{\ell=-g \\ \ell\neq -i}}^{g}{}' e_n(nQ_i, nQ_\ell)^{a_{i,i}b_{\ell,-i}} \\ \times \prod_{\substack{k=-g \\ k\neq i}}^{g}{}' e_n(nQ_k, nQ_{-i})^{b_{k,i}a_{-i,-i}} & \times \prod_{\substack{k=-g \\ k\neq i}}^{g}{}' \prod_{\substack{\ell=-g \\ \ell\neq -i}}^{g}{}' e_{n^2}(Q_k, Q_\ell)^{a_{k,i}a_{\ell,-i}}. \end{aligned}$$

The double product evaluates to 1 because $n|a_{k,i}$ and $n|a_{\ell,j}$. Similarly, the single products are 1. The equation now collapses to

$$e_{n^2}(Q_i, Q_{-i})^q = e_{n^2}(\phi(Q_i), \phi(Q_{-i})) = e_{n^2}(Q_i, Q_{-i})^{a_{i,i}a_{-i,-i}}.$$

As we have seen, antisymmetry implies that $a_{i,i} \equiv a_{-i,-i} \mod n^2$. Thus, we get the congruences

$$q \equiv a_{i,i}^2 \mod n^2 \quad \text{for all } i. \tag{6.5}$$

Let $i, j \leq g$ be distinct integers. Then $a_{i,i}^2 \equiv q \equiv a_{j,j}^2 \mod n^2$. Recall that we also know that $a_{i,i} \equiv 1 \equiv a_{j,j} \bmod n$. We conclude that $a_{i,i} \equiv a_{j,j} \bmod (n^2/2)$. If we order the generators $Q_1, Q_2, \ldots, Q_g, Q_{-1}, \ldots, Q_{-g}$, then this proves that ϕ is a matrix of the form stated in Theorem 6.2.

Conversely, suppose that the conditions given in Equation 6.4 hold and that $a_{i,i} \equiv a_{-i,-i} \mod n^2$ for all i. Recall that these must be congruent to 1 mod n since we assume that the n-torsion is rational over $\mathbf{F}_q$. As before, since $a_{i,j} \equiv 0 \bmod n$

when $i \neq j$, we write $a_{i,j} = nb_{i,j}$ for some integer $b_{i,j}$. Since $a_{i,i} \equiv 1 \bmod n$, we write $a_{i,i} - 1 = nA_i$ for some integer A_i. Suppose that $j = -i$. Then Lemma 6.3 implies that

$$\tau_n(nQ_i, nQ_{-i}) = \zeta^{\sigma_i A_{-i}} = \zeta^{-\sigma_{-i} A_{-i}} = \zeta^{-\sigma_{-i} A_i}$$

where the last equality holds because $a_{j,j} \equiv a_{-j,-j} \bmod n^2$ for all j. This is now just $\tau_n(nQ_{-i}, nQ_i)^{-1}$ by Lemma 6.3.

Now suppose that $j \neq -i$. Then by Lemma 6.3, $\tau_n(nQ_i, nQ_j) = \zeta^{\sigma_i b_{-i,j}}$. If i and j have the same signs, then the conditions in Equation 6.4 and Lemma 6.3 imply that this is $\zeta^{\sigma_j b_{-j,i}} = \tau_n(nQ_j, nQ_i)^{-1}$. If i and j have opposite signs, then the conditions in Equation 6.4 and Lemma 6.3 imply that this is $\zeta^{-\sigma_j b_{-j,i}} = \tau_n(nQ_j, nQ_i)^{-1}$. Hence, the Tate-Lichtenbaum pairing is antisymmetric under these assumptions.

6.3 Self Pairings of the Generators of $J[n]$

We have shown how antisymmetry relates to the matrix representing the Frobenius endomorphism. We now want to show how $\tau_n(P_i, P_i) = 1$ relates to the matrix. Recall that in the above proof of antisymmetry of τ_n, we need only deal with the cases that $i \neq j$. It is interesting to note that the congruences in (6.4) for $i = j$ give the conditions for trivial Tate-Lichtenbaum self-pairings of the generators of the n-torsion points except when n is even. However, we take a different approach for that proof which will work for any n.

Suppose that $\tau_n(nQ_i,\ nQ_i) = 1$ for all $i = 1, 2, ..., 2g$. As before, we represent the Frobenius map on $J[n^2]$ as the matrix $(a_{i,j})$ with $i, j \in \{1, \ldots, g, -1, \ldots, -g\}$

(with respect to the basis given by Lemma 6.1).

By Theorem 2.5, we get that $e_{n^2}(Q_i,\ \phi(Q_i)) = 1$. Also recall that $\phi(Q_i) = \sum_{k=-g}^{g}{}' a_{k,i}Q_k$, and so

$$e_{n^2}\left(Q_i,\ \sum_{k=-g}^{g}{}' a_{k,i}Q_k\right) = 1.$$

Since for $i \neq k$ we have that $n \mid a_{k,i}$, we write $a_{k,i} = nb_{k,i}$ for some $b_{k,i}$ (because $\phi \equiv I_{2g} \bmod n$). Bilinearity and compatibility yield the following

$$\begin{aligned} 1 &= e_{n^2}\left(Q_i, \sum_{k=-g}^{g}{}' a_{k,i}Q_k\right) = \prod_{\substack{k=-g \\ k\neq i}}^{g}{}' e_{n^2}(Q_i, n\ b_{k,i}Q_k) \\ &= \prod_{\substack{k=-g \\ k\neq i}}^{g}{}' e_n(nQ_i, n\ b_{k,i}Q_k) = \prod_{\substack{k=-g \\ k\neq i}}^{g}{}' e_n(nQ_i, nQ_k)^{b_{k,i}} \\ &= e_n(nQ_i, nQ_{-i})^{b_{-i,i}}. \end{aligned}$$

By Equation 6.1 we have that $\zeta^{\sigma_i b_{-i,i}} = 1$. These two cases imply that $b_{-i,i} \equiv 0 \bmod n$, hence

$$a_{-i,i} \equiv 0 \mod n^2 \text{ for all } i. \tag{6.6}$$

Conversely, we need to prove that if (6.6) holds, then $\tau_n(nQ_i, nQ_i) = 1$ for all i. This will complete the proof that if ϕ has the matrix form given in Theorem 6.2, then self pairings are trivial on $J[n]$. Recall that by Equation 6.3 we know

$$\tau_n(nQ_i, nQ_j) = e_n(nQ_i, nQ_j)^{A_j} \cdot \left(\prod_{\substack{k=-g \\ k\neq j}}^{g}{}' e_n(nQ_i, nQ_k)^{b_{k,j}}\right).$$

Letting $j = i$ gives

$$\begin{aligned} \tau_n(nQ_i, nQ_i) &= e_n(nQ_i, nQ_i)^{A_i} \cdot e_n(nQ_i, nQ_{-i})^{b_{-i,i}} \\ &= e_n(nQ_i, nQ_{-i})^{b_{-i,i}} \qquad (6.7) \\ &= \zeta^{\sigma_i b_{-i,i}}. \end{aligned}$$

Assuming that ϕ satisfies the condition in (6.6), then $\zeta^{\sigma_i b_{-i,i}} = 1$.

Thus, if the matrix corresponding to $\phi \mod n^2$ has the form given in Theorem 6.2, then self pairings are trivial on the generators of $J[n]$. This together with antisymmetry implies that all self-pairings on $J[n]$ are trivial.

Chapter 7

Examples of Self Pairings on Jacobians of Curves

In this chapter we give examples of the results in Chapter 6 for genus 2 curves. In Section 7.1 we apply Theorem 6.2 to Jacobians of genus 2 curves. In Section 7.2 we apply our results to the Jacobian of the curve $C_1 : y^2 = x(x^2-1)(x^2-4)(x-3)$. In Section 7.3 we apply our results to the Jacobian of the curve $C_2 : y^2 = x^5 + 1$. In this example, we determine the eigenvalues of the Frobenius endomorphism and show how they can be used to determine when all self pairings on $J[n]$ are trivial.

7.1 Overview of Self Pairings in Genus 2

Let J be the Jacobian of a curve defined over $\mathbf{F}_q$ and suppose that n is an odd integer such that $\gcd(n, q) = 1$. We work with respect to a basis

$$\{Q_1, Q_2, \ldots, Q_g, Q_{-1} \ldots, Q_{-g}\}$$

for the generators of $J[n^2]$ as described in Lemma 6.1. Suppose that J is the Jacobian of a genus 2 curve. Then Theorem 6.2 states that self-pairings on $J[n]$ are trivial if

and only if the Frobenius map on $J[n^2]$ has the form

$$\phi \equiv \begin{bmatrix} b & c & 0 & a \\ d & b & -a & 0 \\ 0 & f & b & d \\ -f & 0 & c & b \end{bmatrix} \mod n^2, \tag{7.1}$$

with respect to the e_n-symplectic basis $\{Q_1, Q_2, Q_{-1}, Q_{-2}\}$ (as in Lemma 6.1), where $b \equiv 1 \bmod n$ and $a, c, d, f \equiv 0 \bmod n$. If n is an even integer, we lose the restriction that the diagonal is constant, in which case ϕ has the form

$$\phi \equiv \begin{bmatrix} b & c & 0 & a \\ d & b' & -a & 0 \\ 0 & f & b & d \\ -f & 0 & c & b' \end{bmatrix} \mod n^2, \tag{7.2}$$

with respect to the above e_n-symplectic basis for $J[n]$, where $b, b' \equiv 1 \bmod n$ and $a, c, d, f \equiv 0 \bmod n$.

7.2 The Curve $C : y^2 = x(x^2 - 1)(x^2 - 4)(x - 3)$

Using MAGMA [4], we found examples of trivial self-pairings for the Jacobian of the genus 2 hyperelliptic curve $C : \ y^2 = x(x^2-1)(x^2-4)(x-3)$. Due to limitations in the computation of division points, we focused on examples of pairings of 2-torsion points. Hence, we chose to work with this curve because all of the Weierstrass points are known and are defined over any field $\mathbf{F}_q$. The smallest prime p such that the 2-torsion points of $J_C(\mathbf{F}_p)$ have trivial self pairings is $p = 41$. We found a symplectic

basis for the 2-torsion of the Jacobian of $C(\mathbf{F}_{41})$ (i.e., a basis such that the Weil pairing corresponds to a matrix as in Lemma 6.1). The associated Frobenius map for this particular basis is given by the matrix:

$$\phi = \begin{bmatrix} 3 & 2 & 0 & 2 \\ 0 & 3 & 2 & 0 \\ 0 & 2 & 3 & 0 \\ 2 & 0 & 2 & 3 \end{bmatrix} \bmod 4.$$

Observe that this satisfies Equation 7.2.

The prime $p = 43$ yielded nontrivial self pairings. Using a symplectic basis for the Jacobian of $C(\mathbf{F}_{43})$ we found that the Frobenius map is given by:

$$\phi = \begin{bmatrix} 3 & 0 & 2 & 2 \\ 0 & 3 & 2 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \bmod 4.$$

Observe that this does not satisfy Equation 7.2 because the upper right 2×2 block does not have zeros off of the diagonal. However, this matrix can be diagonalized. Let P be the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Then we have that

$$P^{-1}\phi P \equiv \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Although we have given the matrix the form described in Theorem 6.2, we have done so by changing the basis in such a way that the basis for $J[n]$ is no longer e_n-symplectic. As a result, we still have the existence of nontrivial self pairings. This shows that the converse of Theorem 6.2 only holds for a particular basis. It is not enough to be able to write the Frobenius in a certain form. However, if the matrix associated to the Frobenius endomorphism mod n^2 cannot be written in the form given in Theorem 6.2, we know that there must exist nontrivial self pairings.

7.3 The Curve $C : y^2 = x^5 + D$

Consider the genus 2 hyperelliptic curve $C : y^2 = x^5 + D$ defined over $\mathbf{F}_p$. This curve has a single point at infinity. Let J represent the Jacobian of C. Assume that $p \equiv 1 \bmod 5$. (Since p is odd, this implies that we really have $p \equiv 1 \bmod 10$.) Then we have the fifth roots of unity contained in $\mathbf{F}_p$. Let ζ be a primitive fifth root of unity. Assume that D is a fifth power mod p and let $D \equiv d^5 \bmod p$. Then the points $P_k = (d(-\zeta)^k, 0)$ with $k = 1, 3, 5, 7, 9$ are rational over $\mathbf{F}_p$.

Every element of J can be represented using a unique pair of points on C (see [6] for details). In particular, every element of $J[2]$ can be represented using the points P_k and the point at infinity, and hence $J[2] \subset J(\mathbf{F}_p)$.

We can count the points on C using Jacobi sums. Recall that if χ and λ are characters of $\mathbf{F}_p^\times$, then we define their Jacobi sum to be $J(\chi,\lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$. See [8] for details about Jacobi sums and point counting.

Let $N(f = g)$ represent the number of $\mathbf{F}_p$-solutions to the equation $f = g$. Then $N(y^2 = x^5 + D) = \sum_{u+v=D} N(y^2 = u) \cdot N(x^5 = -v)$. If u is a nonzero quadratic residue mod p then there are two solutions to $y^2 = u$. If it is a nonresidue, then there are no solutions. Hence, $N(y^2 = u) = 1 + \rho(u)$ where $\rho(u) = \left(\frac{u}{p}\right)$ is the Legendre symbol (extended to $\mathbf{F}_p$ by defining $\rho(0) = 0$).

Let ζ be a primitive fifth root of unity and let χ be a character of $\mathbf{F}_p^\times$ of order 5. We can extend χ to all of $\mathbf{F}_p$ by setting $\chi(0) = 0$. Since $p \equiv 1 \bmod 5$, we have $p = \pi_1\pi_2\pi_3\pi_4$ in $\mathbf{Z}[\zeta]$. Choose χ to be a fifth power residue symbol $\chi(a) = \left(\frac{a}{\pi_i}\right)_5$. Note that $\chi(-1) = 1$. Then $N(x^5 = -v) = 1 + \chi(-v) + \chi^2(-v) + \chi^3(-v) + \chi^4(-v)$ since $5|p-1$ (see [8], Proposition 8.15).

Thus, we have that

$$N(y^2 = x^5 + D) = \sum_{u+v=D} (1 + \rho(u))\,(1 + \chi(-v) + \chi^2(-v) + \chi^3(-v) + \chi^4(-v)).$$

Since $\sum_v \chi^i(-v) = 0$ for all i and $\sum_u \rho(u) = 0$, this simplifies to

$$N(y^2 = x^5 + D) = p + \sum_{i=1}^{4} \sum_{u+v=D} \rho(u)\chi^i(-v).$$

Letting $u = Du'$ and $v = Dv'$, we get

$$\begin{aligned} N(y^2 = x^5 + D) &= p + \sum_{i=1}^{4} \sum_{u'+v'=1} \rho(Du')\chi^i(-Dv') \\ &= p + \sum_{i=1}^{4} \rho(D)\chi^i(D) \sum_{u+v=1} \rho(u)\chi^i(v) \qquad (7.3) \\ &= p + \sum_{i=1}^{4} \rho(D)\chi^i(D)J(\rho,\chi^i). \end{aligned}$$

Since p is odd and ρ is an order 2 character, we have that [8]

$$J(\rho, \chi^i) = \chi^i(4)J(\chi^i, \chi^i).$$

Let N_q be the number of $\mathbf{F}_q$-points on C. Then, including the point at infinity, the number of points on C is

$$N_p = p + 1 + \sum_{i=1}^{4} \rho(D)\chi^i(4D)J(\chi^i, \chi^i).$$

Note that $\chi^4 = \overline{\chi}$ and $\chi^3 = \overline{\chi^2}$.

7.3.1 The Frobenius Endomorphism

We want to relate these Jacobi sums to the eigenvalues of the Frobenius endomorphism. We begin with the following proposition about the characteristic polynomial of the Frobenius map.

Proposition 7.1. *For a genus g hyperelliptic curve C defined over $\mathbf{F}_q$, the characteristic polynomial of the Frobenius endomorphism has the form*

$$f(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + \cdots a_1 q^{g-1} t + q^g$$

where $a_i \in \mathbf{Z}$.

See Theorem 14.16 in [6] for details.

The coefficients a_k can be defined using the number of points on $C(\mathbf{F}_{q^k})$. For a genus 2 curve defined over $\mathbf{F}_p$, the characteristic polynomial is $f(t) = t^4 + a_1 t^3 + a_2 t^2 + a_1 pt + p^2$ where $a_1 = N_p - p - 1$ and $2a_2 = (N_{p^2} - p^2 - 1 + a_1^2)$. We also have the following proposition concerning the roots of f.

Proposition 7.2. *Let C be a genus g hyperelliptic curve defined over $\mathbf{F}_q$. Let $f(t) = \prod_{i=1}^{2g}(t - \tau_i)$ with $\tau_i \in \mathbf{C}$. Then*

1. *$|\tau_i| = \sqrt{q}$ for all i;*

2. *the roots can be ordered such that $\tau_i\tau_{i+g} = q$;*

3. *for any integer k, $N_{q^k} = q^k + 1 - \sum_{i=1}^{2g} \tau_i^k$.*

See Theorem 14.17 in [6] for more information. Let

$$\begin{aligned} \tau_1 &= -\rho(D)\chi(4D)J(\chi,\chi) \\ \tau_2 &= -\rho(D)\chi^2(4D)J(\chi^2,\chi^2) \end{aligned} \tag{7.4}$$

and let define τ_3 and τ_4 by $\tau_1\tau_3 = q = \tau_2\tau_4$. Then the algebraic integers τ_i satisfy Proposition 7.2 and are eigenvalues of the Frobenius endomorphism.

7.3.2 Matrix Representation of a Jacobi Sum

We want to represent the Frobenius endomorphism as a matrix and determine whether or not it can be put into the form given in Theorem 6.2. We use its eigenvalues to do so. The endomorphism ring is $\mathbf{Z}[\zeta]$ and the Frobenius is an element of this ring which is given by a τ_i. Let $\{\zeta, \zeta^2, \zeta^3, \zeta^4\}$ be a $\mathbf{Z}$-basis of $\mathbf{Z}[\zeta]$. Since the τ_i are Galois conjugates, it suffices to work with any one of them (since choosing a different τ_i would correspond to permuting the basis). Let $\tau = \tau_i = a\zeta + b\zeta^2 + c\zeta^3 + d\zeta^4$ for some integers a, b, c and d and for some fixed choice of i.

We can calculate a matrix for multiplication by τ on the elements of $\mathbf{Z}[\zeta]$. Writing $\tau\zeta^k$ in this basis for $k = 1, 2, 3, 4$ yields the following matrix representation.

$$M_i = \begin{bmatrix} -d & d-c & c-b & b-a \\ a-d & -c & d-b & c-a \\ b-d & a-c & -b & d-a \\ c-d & b-c & a-b & -a \end{bmatrix}. \tag{7.5}$$

Consider self pairings on $J[2]$. Since this matrix must be congruent to the identity matrix mod 2, we know that it can be written as $M_i \equiv 2X + I \bmod 4$ where I is the 4×4 identity matrix and X is a 4×4 matrix with entries in $\mathbf{F}_2$.

We wish to determine if a change of basis will convert M_i into the form given by Equation 7.2. We use MAGMA to run through all possibilities for X and to calculate their characteristic polynomials. They are all reducible mod 2. The possible characteristic polynomials are given below.

x^4	$x^4 + x^3$
$x^4 + x^2$	$x^4 + x^3 + x^2 + x$
$x^4 + 1$	$x^4 + x^3 + x + 1$
$x^4 + x^2 + 1$	$x^4 + x^3 + x^2$
$x^4 + x^3 + x$	$x^4 + x^3 + x^2 + 1$

7.3.3 $C : y^2 = x^5 + 1$ over $\mathbf{F}_{41}$

If $p = 41$, then $\rho(1)\chi(1)J(\rho, \chi) = 5\zeta + 3\zeta^2 + 7\zeta^3 + \zeta^4$ is an eigenvalue of the Frobenius endomorphism. We use Equation 7.5 to represent it as a matrix M. Then

M satisfies

$$M \equiv \begin{bmatrix} 3 & 2 & 0 & 2 \\ 0 & 1 & 2 & 2 \\ 2 & 2 & 1 & 0 \\ 2 & 0 & 2 & 3 \end{bmatrix} \bmod 4. \tag{7.6}$$

In this case, we have $M = 2X + I$ where

$$X \equiv \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \bmod 2 \tag{7.7}$$

and X has characteristic polynomial $x^4 + x^2 + 1$ which is reducible and one of the possible polynomials.

The change of basis matrix that puts M in the form given by Equation 7.2 is

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \bmod 4. \tag{7.8}$$

and we see that

$$A^{-1}MA \equiv \begin{bmatrix} 3 & 2 & 0 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 2 & 3 & 0 \\ 2 & 0 & 2 & 1 \end{bmatrix} \bmod 4. \tag{7.9}$$

Unfortunately, this does not imply that Tate-Lichtenbaum self-pairings are trivial

on the 2-torsion of the Jacobian of $y^2 = x^5 + 1$ defined over $\mathbf{F}_{41}$. This is because the matrix might not correspond to an e_n-symplectic basis of $J[2]$.

We can use MAGMA to do additional analysis. We find a basis for $J[4]$ such that the Frobenius endomorphism on $J[4]$ is

$$\phi_1 \equiv \begin{bmatrix} 1 & 0 & 0 & 2 \\ 2 & 1 & 2 & 2 \\ 0 & 2 & 3 & 2 \\ 2 & 0 & 0 & 3 \end{bmatrix} \bmod 4 \tag{7.10}$$

and the Weil pairing on $J[2]$ is given by

$$\begin{bmatrix} 1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 \end{bmatrix}. \tag{7.11}$$

The change of basis matrix

$$B = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{7.12}$$

yields an e_n-symplectic basis and gives the Frobenius map the form

$$\phi_2 \equiv B\phi_1 B^{-1} \equiv \begin{bmatrix} 3 & 2 & 0 & 2 \\ 0 & 1 & 2 & 0 \\ 0 & 2 & 3 & 0 \\ 2 & 0 & 2 & 1 \end{bmatrix} \bmod 4. \tag{7.13}$$

Observe that ϕ_2 is the same as $A^{-1}MA \bmod 4$. Since ϕ_2 is written in an e_n-symplectic basis and since it also has the form in Equation 7.2, we conclude that all self pairings on $J[2]$ are trivial.

7.3.4 $C : y^2 = x^5 + 1$ over $\mathbf{F}_{71}$

Now consider the prime $p = 71$. We now have that $\rho(1)\chi(1)J(\rho, \chi) = -\zeta - 7\zeta^2 + 3\zeta^3 + \zeta^4$ is an eigenvalue of the Frobenius endomorphism. We again use Equation 7.5 to represent it as a matrix, N. Then N satisfies

$$N \equiv \begin{bmatrix} 3 & 2 & 2 & 2 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 3 & 2 \\ 2 & 2 & 2 & 1 \end{bmatrix} \bmod 4. \tag{7.14}$$

Writing N as $2X + I$ for some 4×4 matrix X, we find that X has characteristic polynomial $x^4 + x + 1$. Since this polynomial is irreducible over $\mathbf{F}_2$, we see that N cannot be put in the form given by Theorem 6.2. This shows that even if we change to a basis for $J[n]$ that is symplectic for the Weil pairing, e_n, the matrix N would not have the form given by Equation 7.2 and hence there must exist an element of $J[2]$ that pairs nontrivially with itself.

Computations with MAGMA (for $p \leq 641$) suggest that Tate-Lichtenbaum self pairings are trivial on $J[2]$ if and only if $p \equiv 1 \bmod 20$. Since we already require that $p \equiv 1 \bmod 5$, this says that trivial self pairings are equivalent to the condition that $p \equiv 1 \bmod 4$.

Appendix A

Elliptic Curves and Jacobian Varieties

A.1 Elliptic Curves

This thesis deals with bilinear pairings on elliptic curves and Jacobians of higher genus curves. An *elliptic curve* E can be represented as a nonsingular projective curve of the form

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{A.1}$$

defined over a field K with the $a_i \in K$ being fixed constants. This equation is known as the *generalized Weierstraß equation*. We denote by $E(K)$ the set of all equivalence classes of solutions in K.

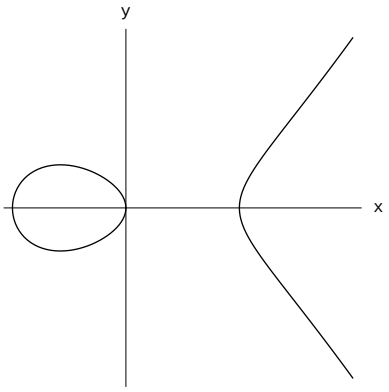
When $z = 0$ we get the solution $(0 : 1 : 0)$, called the "point at infinity" and often denoted by ∞. For $z \neq 0$, we work with the affine generalized Weierstraß equation,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{A.2}$$

When the characteristic of K is not 2 or 3, a simple change of variables can be used to convert Equation A.1 into one of the form $y^2 = x^3 + Ax + B$, where A and B are new constants in K. An equation of this form is called a Weierstraß equation for the elliptic curve E. In order for the elliptic curve to be nonsingular, we require that $x^3 + Ax + B$ have no multiple roots. This is equivalent to requiring

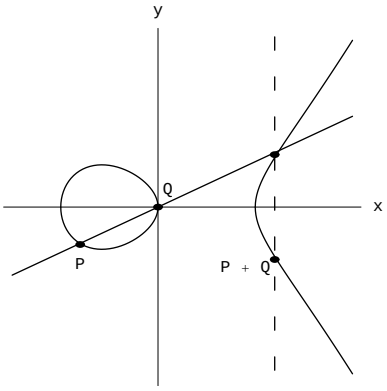
the discriminant $\Delta = 4A^3 + 27B^2$ to be nonzero.

Although in number theory we often work with elliptic curves defined over finite fields, it is often useful to be able to picture the graph of an elliptic curve. The picture we most often visualize is that of an elliptic curve defined over $\mathbf{R}$ in which $x^3 + Ax + B$ has three distinct real roots.

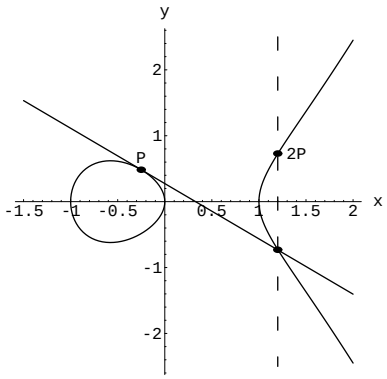


We picture the point at infinity as sitting at the top and bottom of the y-axis.

One can alternatively define an elliptic curve to be a nonsingular projective curve with a group structure defined by regular maps ([12]). This group structure forces the curve to have genus 1 (see [12], page 2). Traditionally, we often view the group structure geometrically in terms of chords and tangents. Hence, we momentarily return to the picture of an elliptic curve defined over $\mathbf{R}$. If we have two distinct points, P and Q, which we want to compose to form a third point, we begin by drawing the line that passes through P and Q. This line will intersect the graph of E in a third point. The reflection of this point across the x-axis is the sum, $P+Q$.



There are certain cases that require special attention. For example, if instead we wish to form the point $P + P$, which we denote by $2P$, we need to do a similar, but slightly different construction. In this case, we draw the line, ℓ, tangent to the graph of E at P. Since ℓ now intersects the graph of E with multiplicity 2 at P, there is again a third point of intersection. The reflection of this point across the x-axis is the sum $2P$.



In all cases, the composition law can be explicitly stated in terms of rational functions. The inverse of an element is simply its reflection across the y-axis. The point at infinity serves as the identity element. While this composition is easily seen to be commutative, it is not obvious that it should be associative. See [15] for a proof. Note that the group structure which we have described depends on our choice of ∞ as the identity element.

Alternatively, let $\mathrm{Pic}^0(E)$ be the group of divisor classes of degree 0 (where two divisors are defined to be equivalent if they differ by a principal divisor). Then the map $E(K) \to \mathrm{Pic}^0(E)$ defined by $P \mapsto [P] - [\infty]$ is a bijection and it gives the set of points $E(K)$ a canonical group structure which is easily seen to be commutative. This group structure agrees with the chord and tangent method outlined above.

A.2 Jacobians of Higher Genus Algebraic Curves

Jacobians are higher dimensional analogues to elliptic curves and much of the theory of elliptic curves can be generalized. In general, the definition of elliptic curves in terms of equations does not generalize to higher dimensions. The exception is the case of 2-dimensional abelian varieties, which are Jacobians of genus 2 projective curves of the form

$$y^2 z^4 = a_0 x^6 + a_1 x^5 z + \cdots + a_6 z^6 \tag{A.3}$$

(when defined over fields of characteristic not equal to 2 or 3). See [5] for details.

However, we can make the following generalization: abelian varieties can be defined as nonsingular connected projective varieties with a group structure defined by regular maps ([12]). Jacobian varieties are special examples of abelian varieties. Let C be a genus g curve defined over K and choose $Q \in C(K)$. Then the Jacobian variety, $J = \mathrm{Jac}(C)$, of C is an abelian variety that is canonically attached to C. It comes equipped with a regular map $\phi : C \to J$ which has the property that $\phi(Q) = 0$. It induces a map $\mathrm{Div}^0(C) \to J(K)$ defined by $\sum n_i P_i \mapsto \sum n_i \phi(P_i)$. This, in turn, induces an isomorphism $\mathrm{Pic}^0(C) \to J(K)$. Furthermore, the dimension of

J is the genus of C. If C is a genus 1 curve, then $\mathrm{Jac}(C) = C$ (assuming that C has a rational point over K).

Let n be a positive integer not divisible by the characteristic of K. Define $E[n] = \{P \in E(\overline{K}) | nP = \infty\}$ to be the subgroup of n-torsion points. Here $\overline{K}$ is an algebraic closure of K. Then $E[n] \simeq (\mathbf{Z}/n\mathbf{Z})^2$. If J is the Jacobian of a genus g curve, then we similarly define $J[n]$ to be the kernel of the multiplication by n map $J(\overline{K}) \xrightarrow{n} J(\overline{K})$. In this case, $J[n] \simeq (\mathbf{Z}/n\mathbf{Z})^{2g}$.

Appendix B

Miller's Algorithm

Computation of both the Weil pairing and the Tate-Lichtenbaum pairing requires finding a function with certain properties. In particular, if $P \in J[n]$, one needs a function f_P such that $\mathrm{div}(f_P) = P$. Victor Miller developed an algorithm for efficiently finding and evaluating such functions (see [15], [11]). It uses the idea of successive doubling. We present it in the case of elliptic curves.

Let E be an elliptic curve, let P be an element of $E[n]$, and let R be any point in E. We need to find a function f_P such that $\mathrm{div}(f_P) = n[P+R] - n[R]$ and evaluate $\frac{f_P(Q_1)}{f_P(Q_2)}$ for some points Q_1 and Q_2.

Let $D_j = j[P+R] - j[R] - [jP] + [\infty]$. Then $D_j = \mathrm{div}(f_j)$ for some function f_j. For example, D_1 arises from by the equation of the line through P, R, and $P+R$.

If f_j and f_k are known, one can find f_{j+k} as follows.

1. Compute the equation $ax + by + c = 0$ for the line passing through the points jP and kP. If these are the same points, use the tangent line.

2. Compute the equation $x+d = 0$ for the vertical line through the point $(j+k)P$.

3. The function f_{j+k} is defined to be $f_j f_k \frac{ax+by+c}{x+d}$, up to a constant.

4. Use successive doubling and addition of functions of the form f_j to build up the function f_n. Then $\mathrm{div}(f_n) = D_n = n[P+R] - n[R] - [nP] + [\infty] =$

$n[P+R]-n[R]$ since P is an n-torsion element. Hence, up to multiplication by a constant, $f_P = f_n$.

Note that the constant factor cancels when we evaluate f_P on a degree zero divisor. Also note that f_P depends on R (or more precisely, on the divisor used to represent P). However, it can be shown that the use of Miller's algorithm to compute pairings produces results independent of the choice of R. See [15] for details.

References

[1] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998, , A Wiley-Interscience Publication. MR MR1625181 (99d:11092)

[2] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart (eds.), *Advances in elliptic curve cryptography*, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005. MR MR2166105

[3] Dan Boneh and Matthew Franklin, *Identity-based encryption from the Weil pairing*, SIAM J. Comput. **32** (2003), no. 3, 586–615 (electronic). MR MR2001745 (2004m:94035)

[4] Wieb Bosma, John J. Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24** (1997), no. 3–4, 235–265, Computational algebra and number theory (London, 1993). MR 1 484 478

[5] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. MR MR1406090 (97i:11071)

[6] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006. MR MR2162716

[7] Gerhard Frey, Michael Müller, and Hans-Georg Rück, *The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems*, IEEE Trans. Inform. Theory **45** (1999), no. 5, 1717–1719. MR MR1699906 (2000c:11095)

[8] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR MR1070716 (92e:11001)

[9] Franz Lemmermeyer, *Reciprocity laws*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000, From Euler to Eisenstein. MR MR1761696 (2001i:11009)

[10] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Trans. Inform. Theory **39** (1993), no. 5, 1639–1646. MR MR1281712 (95e:94038)

[11] Victor S. Miller, *The Weil pairing, and its efficient calculation*, J. Cryptology **17** (2004), no. 4, 235–261. MR MR2090556 (2005g:11112)

[12] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150. MR MR861974

[13] Edward F. Schaefer and Joseph L. Wetherell, *Computing the Selmer group of an isogeny between abelian varieties using a further isogeny to a Jacobian*, J. Number Theory **115** (2005), no. 1, 158–175. MR MR2176488 (2006g:11116)

[14] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR MR817210 (87g:11070)

[15] Lawrence C. Washington, *Elliptic curves: Number theory and cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2003. MR MR1989729 (2004e:11061)