

A NEW PROOF FOR THE NON-DEGENERACY OF THE FREY-RÜCK PAIRING AND A CONNECTION TO ISOGENIES OVER THE BASE FIELD

EDWARD F. SCHAEFER

ABSTRACT. Frey and Rück have described a non-degenerate bilinear pairing on the Jacobians of curves; this includes elliptic curves. We present a new mathematical foundation for this pairing and use it to give a different proof of its non-degeneracy. We then present yet another method of looking at this pairing using isogenies.

1. INTRODUCTION

In this article, we will provide a new mathematical foundation for a pairing, first described by Frey and Rück in [2], on the Jacobians of curves over finite fields. This pairing has cryptographic applications. It is used to give a fast translation of the discrete logarithm problem in a Jacobian to the discrete logarithm problem in the multiplicative group of a finite field. It is also used in pairing-based cryptography. We note that an elliptic curve is an example of a Jacobian.

In Section 4, we present a new proof of the non-degeneracy of this pairing. We will use Galois cohomology and Weil reciprocity over finite fields. The proof of non-degeneracy will stem from the non-degeneracy of the Weil pairing.

The pairing of Frey and Rück pairs two groups of prime exponent l . In order to use this pairing, the base field, over which the curve is defined, is always enlarged so as to include the l -th roots of unity. We pair the kernel and co-kernel of the multiplication by l map on the points of the Jacobian over this extended field.

For encryption and decryption, the group in which the computations take place is a subgroup of the Jacobian of a curve over the base field. Typically the base field does not include the l -th roots of unity. So it should not be necessary to always have to consider the Jacobian over the extension of the base field gotten by adjoining the l -th roots of unity.

In Section 5, we will use isogenies other than the multiplication by l map in order to consider the Jacobian over the base field. Perhaps this reinterpretation will lead to new insights into this pairing, as in Section 6.

2. OVERVIEW OF MATHEMATICAL METHODS

In this section, we will review the Galois cohomology and arithmetic geometry that will be used throughout this article. References for the results on cohomology that we simply state are [1, 5, 6]. A reference for results on curves that we simply state is [6].

Let G be a Galois group, finite or infinite, and let M be a G -module. A cocycle from G to M is a map $\xi : G \rightarrow M$ with the property that $\xi(\sigma\tau) = {}^\sigma\xi(\tau) + \xi(\sigma)$ for all $\sigma, \tau \in G$. If $m \in M$ then we can associate to it the cocycle $\sigma \mapsto {}^\sigma m - m$; such a cocycle is called a coboundary.

Key words and phrases. elliptic curve, Jacobian, discrete logarithm problem.

The author is grateful to Joseph Wetherell for useful conversations. The author is supported by a National Security Agency Standard MDA904-03-1-0030.

The quotient of the cocycles by the coboundaries is a group denoted $H^1(G, M)$. If G is an infinite Galois group, we just use continuous cocycles. If $0 \rightarrow \ker(f) \rightarrow M_1 \xrightarrow{f} M_2 \rightarrow 0$ is an exact sequence of G -modules then we get a long exact sequence $0 \rightarrow \ker(f)^G \rightarrow M_1^G \rightarrow M_2^G \xrightarrow{\delta_f} H^1(G, \ker(f)) \rightarrow H^1(G, M_1) \xrightarrow{f} H^1(G, M_2)$. Here M^G denotes the G -invariants of M . The maps between H^1 's are induced by the maps between the modules. Let us define δ_f . If $m \in M_2^G$ and $n \in M_1$ is a preimage, then $\delta_f(m)$ is the class including the cocycle $\sigma \mapsto {}^\sigma n - n$.

Let K be a field and \overline{K} a separable closure. If M is a $\text{Gal}(\overline{K}/K)$ -module, then we use $H^1(K, M)$ to denote $H^1(\text{Gal}(\overline{K}/K), M)$ and $M(K)$ to denote $M^{\text{Gal}(\overline{K}/K)}$. Let K^* denote the multiplicative group of units in K ; as a set, $K^* = K \setminus 0$. Hilbert's Theorem 90 tells us $H^1(K, \overline{K}^*) = 0$. Let $l \in \mathbb{Z}$, $l \geq 2$. Raising to the l -th power gives us a short exact sequence of $\text{Gal}(\overline{K}/K)$ -modules: $1 \rightarrow \mu_l \rightarrow \overline{K}^* \xrightarrow{l} \overline{K}^* \rightarrow 1$, where μ_l is the group of l -th roots of unity in \overline{K} . From above, we have a long exact sequence $1 \rightarrow \mu_l(K) \rightarrow K^* \xrightarrow{l} K^* \xrightarrow{\delta_l} H^1(K, \mu_l) \rightarrow 0$. So we get the Kummer isomorphism $K^*/K^{*l} \xrightarrow{\delta_l} H^1(K, \mu_l)$ by $k \in K^* \mapsto [\sigma \mapsto \sigma^l k / k]$.

Similarly, let A be an abelian variety defined over the field K . Abelian varieties include Jacobian varieties. By A we mean $A(\overline{K})$, the set of points with coordinates in \overline{K} . Let $A[l]$ denote the kernel of the multiplication by l map. This is the l -torsion on A . We have the short exact sequence of $\text{Gal}(\overline{K}/K)$ -modules $0 \rightarrow A[l] \rightarrow A(\overline{K}) \xrightarrow{l} A(\overline{K}) \rightarrow 0$. This gives us the long exact sequence $0 \rightarrow A[l](K) \rightarrow A(K) \xrightarrow{l} A(K) \xrightarrow{\delta_l} H^1(K, A[l]) \rightarrow H^1(K, A)$. From this we get an injection $A(K)/lA(K) \xrightarrow{\delta_l} H^1(K, A[l])$. If $P \in A(K)$ and $Q \in A(\overline{K})$ has the property that $lQ = P$ then $\delta_l(P) = [\sigma \mapsto {}^\sigma Q - Q]$.

If L is a normal extension of K and M is a $\text{Gal}(\overline{K}/K)$ -module then there is a restriction map $H^1(K, M) \xrightarrow{\text{res}} H^1(L, M)$ induced by $\text{Gal}(\overline{K}/L) \subseteq \text{Gal}(\overline{K}/K)$. If $[\xi] \in H^1(\text{Gal}(L/K), M(L))$ then ξ induces a cocycle $\text{inf}(\xi) : \text{Gal}(\overline{K}/K) \rightarrow \text{Gal}(L/K) \xrightarrow{\xi} M(L) \subseteq M$, where the first map is simply the quotient map on Galois groups. This induces an inflation map from $H^1(\text{Gal}(L/K), M(L))$ to $H^1(K, M)$. We get an exact sequence $0 \rightarrow H^1(\text{Gal}(L/K), M(L)) \xrightarrow{\text{inf}} H^1(K, M) \xrightarrow{\text{res}} H^1(L, M)^{\text{Gal}(L/K)} \rightarrow H^2(\text{Gal}(L/K), M(L))$. For the purposes of this article, we will not need to understand the structure of nor the map to $H^2(\text{Gal}(L/K), M(L))$.

If G is a group with exponent n and M has exponent m and $\text{gcd}(m, n) = 1$, then $H^i(G, M) = 0$ for all i .

Proposition 2.1. *Let K be a finite field of characteristic p and let $l \neq p$ be a prime. Let M be a finite dimensional \mathbb{F}_l -vector space on which $\text{Gal}(\overline{K}/K)$ acts. Then $\dim_{\mathbb{F}_l} H^1(K, M) = \dim_{\mathbb{F}_l} M(K)$.*

Proof. Let L be the field of definition of all elements of M . Let L_l be the extension of L of degree l . We have the exact sequence $0 \rightarrow H^1(\text{Gal}(L_l/K), M) \xrightarrow{\text{inf}} H^1(K, M) \xrightarrow{\text{res}} H^1(L_l, M)$. The restriction map from $H^1(K, M)$ to $H^1(L_l, M)$ can be factored as $H^1(K, M) \xrightarrow{\text{res}} \text{Hom}(\text{Gal}(\overline{K}/L), M) \xrightarrow{\text{res}} \text{Hom}(\text{Gal}(\overline{K}/L_l), M) = H^1(L_l, M)$. Since M is an \mathbb{F}_l -vector space and L_l is the degree l extension of L , we see that the latter restriction map is trivial. Thus the inflation map induces an isomorphism of $H^1(\text{Gal}(L_l/K), M)$ and $H^1(K, M)$.

Since $\text{Gal}(L_l/K)$ is a finite cyclic group, we have $H^1(\text{Gal}(L_l/K), M) \cong \hat{H}^1(\text{Gal}(L_l/K), M)$, the Tate-cohomology group. Since M is finite, we have $\#\hat{H}^1(\text{Gal}(L_l/K), M) = \#\hat{H}^0(\text{Gal}(L_l/K), M)$. Let σ generate $\text{Gal}(L_l/K)$ and N_σ be the norm from L_l to K . The group $\hat{H}^0(\text{Gal}(L_l/K), M)$

is isomorphic to the quotient of the kernel of $\sigma - 1$ on M by the image of N_σ on M . Since N_σ on M is the same as the composition of the norm from L to K and the multiplication by l map, we see that the image of N_σ on M is trivial. So $\hat{H}^0(\text{Gal}(L_l/K), M) \cong M(K)$. \square

Let C be a curve defined over the field K . When we write C we mean the set of points $C(\bar{K})$. A divisor on C is a formal finite sum of points on C ; it could be denoted $\sum_{P \in C} n_P P$, with $P \in C$, $n_P \in \mathbb{Z}$, and where all but finitely many n_P are 0. The set of P 's for which $n_P \neq 0$ is the support of the divisor. The degree of $\sum n_P P$ is $\sum n_P$. There is a natural action of $\text{Gal}(\bar{K}/K)$ on divisors of C . A divisor fixed by $\text{Gal}(\bar{K}/K)$ will be called a divisor over K . For example, the divisor $(\sqrt{3}, 0) + (-\sqrt{3}, 0) - 2(1, 1)$ would be a divisor over \mathbb{Q} of degree 0 on a curve containing those three points.

The function field of C is denoted $\bar{K}(C)$ and its $\text{Gal}(\bar{K}/K)$ -invariants are denoted $K(C)$. If $f \in K(C)$ and $\sum n_P P$ is a divisor over K then we define $f(\sum n_P P) = \prod f(P)^{n_P}$. A priori, this is an element of \bar{K} ; however, given the Galois-actions on both f and the divisor, we see that $\prod f(P)^{n_P} \in K$. If $f \in \bar{K}(C)$ then $\text{div}(f) = \sum_{P \in C} \text{ord}_P(f) P$ is its divisor. The divisor of a function is called a principal divisor. If $f \in K(C)$ then $\text{div}(f)$ is a divisor over K . If $f, g \in \bar{K}(C)$ and their divisors have disjoint supports, then $f(\text{div}(g)) = g(\text{div}(f))$; this is called Weil reciprocity.

The degree 0 divisors of C form a group and the principal divisors form a subgroup. The quotient group is the Jacobian of C , which we will denote J . Here $J = J(\bar{K})$. We can give J the structure of an algebraic variety, but we will not need to do so in this article.

3. DESCRIPTION OF THE FIRST PAIRING

Let us recall the pairing of Frey and Rück. Let p be a prime, $q = p^s$ for some positive integer s and \mathbb{F}_q denote the finite field with q elements. Let C be a curve of genus greater than or equal to 1 over \mathbb{F}_q . (If C has genus 1, then J is just an elliptic curve.) Assume $C(\mathbb{F}_q)$ is non-empty. This is a safe assumption whenever the genus of C is small and q is sufficiently large, as is true in cryptographic applications. Let J be the Jacobian of C . If D is a degree 0 divisor, then we represent its divisor class in J by $[D]$. Since $C(\mathbb{F}_q)$ is non-empty, every divisor class in $J(\mathbb{F}_q)$ is represented by a degree 0 divisor over \mathbb{F}_q . Let $l \neq p$ be a prime dividing $\#J(\mathbb{F}_q)$. Here and in Section 4 we will make the assumption that the l -th roots of unity are contained in \mathbb{F}_q . In other words, we are assuming that $l|q - 1$.

There is a pairing from $J(\mathbb{F}_q)/lJ(\mathbb{F}_q) \times J[l](\mathbb{F}_q) \rightarrow \mathbb{F}_q^*/\mathbb{F}_q^{*l}$. Let $R \in J(\mathbb{F}_q)$ and $S \in J[l](\mathbb{F}_q)$. Choose degree 0 divisors D_1 and D_2 over \mathbb{F}_q , with disjoint supports, such that $R = [D_1]$ and $S = [D_2]$. Choose $f_{D_2} \in \mathbb{F}_q(C)$ where $\text{div}(f_{D_2}) = lD_2$. Then $\langle R, S \rangle = f_{D_2}(D_1)$. We will see in Section 4 that this pairing is bilinear, non-degenerate and does not depend on the choices of D_1, D_2 or f_{D_2} .

4. PROOF OF NON-DEGENERACY OF THE FIRST PAIRING

From Section 2 we have an injection $J(\mathbb{F}_q)/lJ(\mathbb{F}_q) \xrightarrow{\delta_l} H^1(\mathbb{F}_q, J[l])$.

Lemma 4.1. *The map δ_l induces an isomorphism of $J(\mathbb{F}_q)/lJ(\mathbb{F}_q)$ and $H^1(\mathbb{F}_q, J[l])$.*

Proof. Since $J(\mathbb{F}_q)$ is a finite abelian group, we have $\#J(\mathbb{F}_q)/lJ(\mathbb{F}_q) = \#J[l](\mathbb{F}_q)$. From Proposition 2.1, we have $\#J[l](\mathbb{F}_q) = \#H^1(\mathbb{F}_q, J[l])$. \square

Let $\mathcal{B} = \{[D_1], \dots, [D_b]\}$ be a basis of $J[l](\mathbb{F}_q)$. Let $w_l : J[l] \rightarrow (\mu_l)^b$ by $[D] \mapsto (e_l([D], [D_1]), \dots, e_l([D], [D_b]))$, where e_l is the l -Weil pairing. Let \hat{w}_l be the induced map from $H^1(\mathbb{F}_q, J[l])$ to $H^1(\mathbb{F}_q, (\mu_l)^b)$.

Lemma 4.2. *The map \hat{w}_l induces an isomorphism of $H^1(\mathbb{F}_q, J[l])$ and $H^1(\mathbb{F}_q, (\mu_l)^b)$.*

Proof. The following is a short exact sequence of $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -modules

$$0 \rightarrow \ker(w_l) \rightarrow J[l] \xrightarrow{w_l} (\mu_l)^b \rightarrow 0.$$

That w_l maps surjectively follows from the non-degeneracy of the Weil-pairing. Taking $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -invariants gives

$$0 \rightarrow \ker(w_l)(\mathbb{F}_q) \rightarrow J[l](\mathbb{F}_q) \xrightarrow{w_l} (\mu_l)^b \rightarrow H^1(\mathbb{F}_q, \ker(w_l)) \rightarrow H^1(\mathbb{F}_q, J[l]) \xrightarrow{\hat{w}_l} H^1(\mathbb{F}_q, (\mu_l)^b).$$

Let $a = \dim_{\mathbb{F}_l} \ker(w_l)(\mathbb{F}_q)$. We know $b = \dim_{\mathbb{F}_l} J[l](\mathbb{F}_q) = \dim_{\mathbb{F}_l} (\mu_l)^b$. From Proposition 2.1, we see $\dim_{\mathbb{F}_l} H^1(\mathbb{F}_q, \ker(w_l)) = a$ and $\dim_{\mathbb{F}_l} H^1(\mathbb{F}_q, J[l]) = \dim_{\mathbb{F}_l} H^1(\mathbb{F}_q, (\mu_l)^b) = b$. The dimensions of the seven vector spaces in the long exact sequence are $0, a, b, b, a, b, b$, respectively; so the last two are isomorphic. \square

Let $\iota : H^1(\mathbb{F}_q, (\mu_l)^b) \rightarrow H^1(\mathbb{F}_q, \mu_l)^b$ be the canonical isomorphism. We have the inverse Kummer isomorphism $H^1(\mathbb{F}_q, \mu_l) \cong \mathbb{F}_q^*/\mathbb{F}_q^{*l}$. Let k denote the composition of ι with the product of b inverse Kummer isomorphisms. So $k : H^1(\mathbb{F}_q, (\mu_l)^b) \rightarrow (\mathbb{F}_q^*/\mathbb{F}_q^{*l})^b$ is an isomorphism.

For each $[D_i] \in \mathcal{B}$, choose $f_{D_i} \in \mathbb{F}_q(C)$ with the property that $\text{div}(f_{D_i}) = lD_i$. We call a divisor D of C a *good divisor* if D has degree 0, is defined over \mathbb{F}_q and its support does not intersect the supports of any of the D_i 's. Let $D = \sum n_P P$ be a good divisor. We note that f_{D_i} induces an evaluation homomorphism from the group of good divisors to \mathbb{F}_q^* .

Lemma 4.3. *The map f_{D_i} induces a well-defined homomorphism from $J(\mathbb{F}_q)/lJ(\mathbb{F}_q)$ to $\mathbb{F}_q^*/\mathbb{F}_q^{*l}$.*

Proof. Since $C(\mathbb{F}_q)$ is non-empty, every element of $J(\mathbb{F}_q)$ contains a good divisor (see [3, Lemma 3, p. 166]). Let T_1, T_2 be two linearly equivalent good divisors. Then $T_1 - T_2 = \text{div}(h)$ for some $h \in \mathbb{F}_q(C)$. We have $f_{D_i}(T_1 - T_2) = f_{D_i}(\text{div}(h)) = h(\text{div}(f_{D_i})) = h(lD_i) = h(D_i)^l \in \mathbb{F}_q^{*l}$. \square

We have a map $(f_{D_1}, \dots, f_{D_b})$ from $J(\mathbb{F}_q)/lJ(\mathbb{F}_q)$ to $(\mathbb{F}_q^*/\mathbb{F}_q^{*l})^b$.

Theorem 4.4. *The maps $(f_{D_1}, \dots, f_{D_b})$ and $k \circ \hat{w}_l \circ \delta_l$ are the same as maps from $J(\mathbb{F}_q)/lJ(\mathbb{F}_q)$ to $(\mathbb{F}_q^*/\mathbb{F}_q^{*l})^b$.*

Proof. Let $w_{l,i}$ be the map from $J[l] \rightarrow \mu_l$ given by $[U] \mapsto e_l([U], [D_i])$ and $\hat{w}_{l,i}$ be the map it induces on H^1 's. Let k_i be the inverse Kummer isomorphism from the i -th component of $H^1(\mathbb{F}_q, \mu_l)^b$ to the i -th component of $(\mathbb{F}_q^*/\mathbb{F}_q^{*l})^b$. It suffices to show that $f_{D_i} = k_i \circ \hat{w}_{l,i} \circ \delta_l$ on $J(\mathbb{F}_q)/lJ(\mathbb{F}_q)$. Let $[D] \in J(\mathbb{F}_q)$ where D is a good divisor. From Lemma 4.3, the choice of D is unimportant. From [3, Lemma 3, p. 166], we can choose a degree 0 divisor T over \overline{K} , whose support does not intersect the supports of the D_i 's, such that $[lT] = [D]$. The class of cocycles $\delta_l([D])$ includes the cocycle $(\sigma \mapsto \text{[}\sigma T - T\text{]})$ with $\sigma \in \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. So $\hat{w}_{l,i} \circ \delta_l([D])$ is the class of cocycles that includes $(\sigma \mapsto e_l(\text{[}\sigma T - T\text{]}, [D_i]))$. The e_l -Weil pairing can be defined as follows. If h_1 and h_2 are functions on C with divisors lU_1 and lU_2 respectively, with disjoint

supports, then $e_l([U_1], [U_2]) = h_2(U_1)/h_1(U_2)$. Let $\text{div}(g) = lT - D$ with g defined over the field of definition of the divisor T . We have $\text{div}(\sigma g) = l\sigma T - D$. So $\text{div}(\sigma g/g) = l(\sigma T - T)$. Recall $\text{div}(f_{D_i}) = lD_i$. We have

$$e_l([\sigma T - T], [D_i]) = \frac{f_{D_i}(\sigma T - T)}{(\sigma g/g)(D_i)} = \frac{\sigma\beta}{\beta}$$

where $\beta = f_{D_i}(T)/g(D_i)$. So we have

$$k_i \circ \hat{w}_{l,i} \circ \delta_i([D]) \equiv \beta^l \equiv \frac{f_{D_i}(lT)}{g(lD_i)} \equiv \frac{f_{D_i}(lT)}{f_{D_i}(lT - D)} \equiv f_{D_i}(D) \pmod{\mathbb{F}_q^{*l}}.$$

□

This proof is essentially identical to that of [4, Thm 2.3]

Corollary 4.5. *The map $(f_{D_1}, \dots, f_{D_b})$ from $J(\mathbb{F}_q)/lJ(\mathbb{F}_q)$ to $(\mathbb{F}_q^*/\mathbb{F}_q^{*l})^b$ is an isomorphism.*

Proof. This follows from Lemmas 4.1, 4.2, the fact that k is an isomorphism and Theorem 4.4. □

Corollary 4.6. *The pairing from $J(\mathbb{F}_q)/lJ(\mathbb{F}_q) \times J[l](\mathbb{F}_q) \rightarrow \mathbb{F}_q^*/\mathbb{F}_q^{*l}$ given by $\langle [D], [D'] \rangle = f_{D'}(D)$ is bilinear and non-degenerate.*

Proof. Non-degeneracy follows from Corollary 4.5. We have linearity on the left from Corollary 4.5. Taking the divisor is a homomorphism from $\mathbb{F}_{q^m}(C)^*$ to $\text{Div}^0(C)(\mathbb{F}_{q^m})$; so we can extend this pairing to $J[l](\mathbb{F}_q)$ from its basis \mathcal{B} . This gives linearity on the right. □

5. MOTIVATION FOR THE PAIRING USING ISOGENIES OVER THE BASE FIELD

We start with the same set-up as before, except that we no longer assume that $l|q-1$. We will assume that $l^2 \nmid \#J(\mathbb{F}_q)$. For cryptographic purposes, l is usually taken to be a prime, such that $\frac{1}{l}\#J(\mathbb{F}_q)$ is very small compared to l ; so this is a reasonable assumption.

Let m be the order of q in \mathbb{F}_l^* . We note that $\mathbb{F}_{q^m} = \mathbb{F}_q(\mu_l)$. The q -Frobenius map raises elements of $\overline{\mathbb{F}_q}$ to the q -th power. This induces a map on points of C , and hence on divisors on C and then on elements of J . Let π_q denote the map induced on J by the q -Frobenius map. Let us first show the existence of a subgroup of $J[l]$ on which π_q acts as multiplication by q . If λ is an eigenvalue of π_q on $J[l]$ then we let $J[l]^{(\lambda)}$ denote the λ -eigenspace. Since $\dim_{\mathbb{F}_l} J[l](\mathbb{F}_q) = 1$, we see that $1 \pmod{l}$ is an eigenvalue of π_q on $J[l]$ and $J[l]^{(1)} = J[l](\mathbb{F}_q)$.

Proposition 5.1. *There is a subgroup of $J[l]$ of order l , which is isomorphic as a $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -module to μ_l .*

I thank Joseph Wetherell for suggesting the following proof.

Proof. The zeros of the characteristic polynomial of π_q come in complex conjugate pairs $\alpha, q/\alpha$. Since $1 \pmod{l}$ is an eigenvalue with a 1-dimensional eigenspace in $J[l]$, we see that $q \pmod{l}$ is an eigenvalue with a 1-dimensional eigenspace. So π_q acts on $J[l]^{(q)}$ by multiplying by q , which is the same as the action of π_q on μ_l . □

As a consequence of this proposition, we note that $J[l]^{(q)}$ is a subgroup of $J(\mathbb{F}_q(\mu_l)) = J(\mathbb{F}_{q^m})$.

We will describe a pairing γ from $J[l]^{(1)} \times J[l]^{(q)}$ to $\mathbb{F}_{q^m}^*/\mathbb{F}_{q^m}^{*l}$. Let D and D_1 be degree 0 divisors over \mathbb{F}_q and \mathbb{F}_{q^m} , respectively, with disjoint supports such that $[D] \in J[l]^{(1)}$ and $[D_1] \in J[l]^{(q)}$. Choose $f_{D_1} \in \mathbb{F}_{q^m}(C)$ such that $\text{div}(f_{D_1}) = lD_1$.

Let $\gamma([D], [D_1]) = f_{D_1}(D) \in \mathbb{F}_{q^m}^*/\mathbb{F}_{q^m}^{*l}$.

Theorem 5.2. *The pairing γ is bilinear and non-degenerate.*

Note that γ pairs two 1-dimensional \mathbb{F}_l -vector spaces, which is elegant.

In order to prove this theorem, we first present some lemmas. Let \hat{A} be the abelian variety $J/J[l]^{(q)}$ and let $\hat{\phi} : J \rightarrow \hat{A}$ be the natural quotient map (thus $J[\hat{\phi}]$, the kernel of $\hat{\phi}$ on $J(\overline{\mathbb{F}_q})$, is $J[l]^{(q)}$). We note $\hat{\phi}$ is an isogeny of degree l defined over \mathbb{F}_q . Let $\phi : A \rightarrow \hat{J}$ be the dual isogeny. Let $\lambda : J \rightarrow \hat{J}$ be the canonical principal polarization on J/\mathbb{F}_q coming from J being the Jacobian of C/\mathbb{F}_q . By abuse of notation, we denote the composition $\lambda^{-1} \circ \phi$ by $\phi : A \rightarrow J$.

Lemma 5.3. *We have $\#J(\mathbb{F}_q)/\phi A(\mathbb{F}_q) = l$.*

Proof. From Cartier duality, since $J[\hat{\phi}]$ is isomorphic to μ_l as a $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -module, we have that $A[\phi]$ is isomorphic to $\mathbb{Z}/l\mathbb{Z}$ as a $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -module. Thus $\#A[\phi](\mathbb{F}_q) = l$. The following sequence is exact

$$0 \rightarrow A[\phi](\mathbb{F}_q) \rightarrow A(\mathbb{F}_q) \xrightarrow{\phi} J(\mathbb{F}_q) \rightarrow J(\mathbb{F}_q)/\phi A(\mathbb{F}_q) \rightarrow 0.$$

Since A and J are isogenous over \mathbb{F}_q , we have $\#A(\mathbb{F}_q) = \#J(\mathbb{F}_q)$. Thus $\#A[\phi](\mathbb{F}_q)$ and $\#J(\mathbb{F}_q)/\phi A(\mathbb{F}_q)$ are the same. \square

From this lemma we see that the quotient map $J[l]^{(1)} = J[l](\mathbb{F}_q) \rightarrow J(\mathbb{F}_q)/\phi A(\mathbb{F}_q)$ is an isomorphism. As we will see, γ should really be thought of as a pairing on $J(\mathbb{F}_q)/\phi A(\mathbb{F}_q) \times J[l]^{(q)}$.

The following is an exact sequence of $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -modules

$$0 \rightarrow A[\phi] \rightarrow A(\overline{\mathbb{F}_q}) \xrightarrow{\phi} J(\overline{\mathbb{F}_q}) \rightarrow 0.$$

Taking $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -invariants gives us $J(\mathbb{F}_q)/\phi A(\mathbb{F}_q) \xrightarrow{\delta_\phi} H^1(\mathbb{F}_q, A[\phi])$.

Lemma 5.4. *The restriction map induces an isomorphism of $H^1(\mathbb{F}_q, A[\phi])$ and $H^1(\mathbb{F}_{q^m}, A[\phi])$.*

We let r_ϕ denote this restriction map.

Proof. We have the following inflation/restriction exact sequence

$$\begin{aligned} 0 \rightarrow H^1(\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q), A[\phi](\mathbb{F}_{q^m})) &\xrightarrow{\text{inf}} H^1(\mathbb{F}_q, A[\phi]) \xrightarrow{r_\phi} H^1(\mathbb{F}_{q^m}, A[\phi])^{\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} \\ &\rightarrow H^2(\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q), A[\phi]). \end{aligned}$$

Since m is the order of q in the group \mathbb{F}_l^* , we see $m \mid l - 1$. So $\text{gcd}(m, l) = 1$. Since m and l are the exponents of the groups $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ and $A[\phi]$, respectively, we have $H^i(\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q), A[\phi]) = 0$ for all i . In addition, since $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ acts trivially on $A[\phi]$ we have $H^1(\mathbb{F}_{q^m}, A[\phi])^{\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)} = H^1(\mathbb{F}_{q^m}, A[\phi])$. \square

We now create an isomorphism of $H^1(\mathbb{F}_{q^m}, A[\phi])$ with another cohomology group. Let D_1 be a degree 0 divisor on C over \mathbb{F}_{q^m} , with the property that the divisor class $[D_1]$ generates $J[l]^{(q)} = J[\hat{\phi}]$.

Define the map $w_\phi : A[\phi] \rightarrow \mu_l$ by $w_\phi(R) = e_\phi(R, [D_1])$, where e_ϕ denotes the ϕ -Weil pairing. The map w_ϕ is an isomorphism of $\text{Gal}(\overline{\mathbb{F}_{q^m}}/\mathbb{F}_{q^m})$ -modules. Let \hat{w}_ϕ be the map induced on cohomology.

Lemma 5.5. *The map \hat{w}_ϕ is an isomorphism from $H^1(\mathbb{F}_{q^m}, A[\phi])$ to $H^1(\mathbb{F}_{q^m}, \mu_l)$.*

Proof. Isomorphisms of $\text{Gal}(\overline{\mathbb{F}_{q^m}}/\mathbb{F}_{q^m})$ -modules induce isomorphisms on cohomology. \square

Let k denote the inverse Kummer isomorphism from $H^1(\mathbb{F}_{q^m}, \mu_l)$ to $\mathbb{F}_{q^m}^*/\mathbb{F}_{q^m}^{*l}$. Choose $f_{D_1} \in \mathbb{F}_{q^m}(C)$ such that $\text{div}(f_{D_1}) = lD_1$.

Lemma 5.6. *The map f_{D_1} induces a well-defined homomorphism from $J(\mathbb{F}_q)/lJ(\mathbb{F}_q)$ to $\mathbb{F}_{q^m}^*/\mathbb{F}_{q^m}^{*l}$.*

The proof of this lemma is essentially identical to that of Lemma 4.3.

Lemma 5.7. *The maps f_{D_1} and $k \circ \hat{w}_\phi \circ r_\phi \circ \delta_\phi$ are the same from $J(\mathbb{F}_q)/\phi A(\mathbb{F}_q)$ to $\mathbb{F}_{q^m}^*/\mathbb{F}_{q^m}^{*l}$.*

Proof. Let r_l be the restriction map from $H^1(\mathbb{F}_q, J[l])$ to $H^1(\mathbb{F}_{q^m}, J[l])$. From Theorem 4.4 we know that f_{D_1} and $k \circ \hat{w}_{l,1} \circ r_l \circ \delta_l$ are the same from $J(\mathbb{F}_q)/lJ(\mathbb{F}_q)$ to $\mathbb{F}_{q^m}^*/\mathbb{F}_{q^m}^{*l}$. There is an isogeny $\tau : J \rightarrow A$ with $\phi \circ \tau = l$. From the commutative diagram

$$\begin{array}{ccccccc} 0 & \rightarrow & J[l] & \rightarrow & J(\overline{\mathbb{F}_q}) & \xrightarrow{l} & J(\overline{\mathbb{F}_q}) \rightarrow 0 \\ & & \downarrow \tau & & \downarrow \tau & & \downarrow 1 \\ 0 & \rightarrow & A[\phi] & \rightarrow & A(\overline{\mathbb{F}_q}) & \xrightarrow{\phi} & J(\overline{\mathbb{F}_q}) \rightarrow 0 \end{array}$$

we get the following commutative diagram by taking $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -invariants

$$\begin{array}{ccc} J(\mathbb{F}_q)/lJ(\mathbb{F}_q) & \xrightarrow{\delta_l} & H^1(\mathbb{F}_q, J[l]) \\ \downarrow & & \downarrow \tau \\ J(\mathbb{F}_q)/\phi A(\mathbb{F}_q) & \xrightarrow{\delta_\phi} & H^1(\mathbb{F}_q, A[\phi]). \end{array}$$

From the compatibility of Weil pairings we have $e_l([D], [D_1]) = e_\phi(\tau([D]), [D_1])$. Thus the triangle of the following diagram commutes and so the whole diagram commutes

$$\begin{array}{ccccccc} J(\mathbb{F}_q)/lJ(\mathbb{F}_q) & \xrightarrow{\delta_l} & H^1(\mathbb{F}_q, J[l]) & \xrightarrow{r_l} & H^1(\mathbb{F}_{q^m}, J[l]) & \searrow \hat{w}_{l,1} & \\ \downarrow & & \downarrow & & \downarrow \tau & & H^1(\mathbb{F}_{q^m}, \mu_q) \xrightarrow{k} \mathbb{F}_{q^m}^*/\mathbb{F}_{q^m}^{*l}. \\ J(\mathbb{F}_q)/\phi A(\mathbb{F}_q) & \xrightarrow{\delta_\phi} & H^1(\mathbb{F}_q, A[\phi]) & \xrightarrow{r_\phi} & H^1(\mathbb{F}_{q^m}, A[\phi]) & \nearrow \hat{w}_\phi & \end{array}$$

From commutivity, f_{D_1} must factor through $\phi A(\mathbb{F}_q)$ and f_{D_1} and $k \circ \hat{w}_\phi \circ r_\phi \circ \delta_\phi$ are the same as maps from $J(\mathbb{F}_q)/\phi A(\mathbb{F}_q)$ to $\mathbb{F}_{q^m}^*/\mathbb{F}_{q^m}^{*l}$. \square

This proof is essentially identical to that of [4, Thm 2.3]

Lemma 5.8. *The map f_{D_1} from $J(\mathbb{F}_q)/\phi A(\mathbb{F}_q)$ to $\mathbb{F}_{q^m}^*/\mathbb{F}_{q^m}^{*l}$ is an isomorphism.*

Proof. The map δ_ϕ is an injection. From Lemmas 5.4 and 5.5 and the fact that k is an isomorphism, we see that the composition $k \circ \hat{w}_\phi \circ r_\phi \circ \delta_\phi$ is an injective homomorphism. From Lemma 5.3 we have $\#J(\mathbb{F}_q)/\phi A(\mathbb{F}_q) = l$ and since $\mathbb{F}_{q^m}^*$ is cyclic we have $\#\mathbb{F}_{q^m}^*/\mathbb{F}_{q^m}^{*l} = l$. Thus this injection must be an isomorphism. From Lemma 5.7, the composition is the same as f_{D_1} . \square

We can now finish the proof of Theorem 5.2.

Proof. We have linearity on the left from Lemma 5.8. Taking the divisor is a homomorphism from $\mathbb{F}_{q^m}(C)^*$ to $\text{Div}^0(C)(\mathbb{F}_{q^m})$. This gives linearity on the right. Non-degeneracy also follows from Lemma 5.8. \square

6. APPLICATIONS TO ELLIPTIC CURVES

An interesting corollary of Proposition 5.1 is the following.

Corollary 6.1. *Let E/\mathbb{F}_q be an elliptic curve. Let $l \nmid q$ be prime with $l \mid \#E(\mathbb{F}_q)$ and $l^2 \nmid \#E(\mathbb{F}_q)$. Assume $\mu_l \not\subseteq \mathbb{F}_q$ (i.e. $l \nmid q-1$). Then $E[l] \subseteq E(\mathbb{F}_q(\mu_l))$.*

Now let us explain what seems to be a surprising fact, which applies, for example, to trace 2 elliptic curves (i.e. where $\#E(\mathbb{F}_q) = \#\mathbb{F}_q^*$). Assume E is defined over \mathbb{F}_q , $l \mid \#E(\mathbb{F}_q)$, $l^2 \nmid \#E(\mathbb{F}_q)$ and $l \mid q-1$ (so $\mu_l \subseteq \mathbb{F}_q$). Let D be a degree 0 divisor of E over \mathbb{F}_q such that $[D]$ generates $E[l](\mathbb{F}_q)$. If $f_D \in \mathbb{F}_q(E)$ has divisor lD then f_D induces an isomorphism of $E[l](\mathbb{F}_q)$ (which is generated by $[D]$) and $\mathbb{F}_q^*/\mathbb{F}_q^{*l}$. At first glance, this might seem to contradict the fact that the l -Weil pairing of an element with itself is trivial. One might imagine that one needs to use $f_{D'}$ for some $[D'] \in E[l] \setminus E[l](\mathbb{F}_q)$. There is no contradiction, however. What is happening is better explained by considering isogenies.

Let $A = E/(E[l](\mathbb{F}_q))$ and $\hat{\phi}$ be the induced isogeny from E to A (note A is an elliptic curve also). So $E[\hat{\phi}] = E[l](\mathbb{F}_q)$. Let $\phi : A \rightarrow E$ be the dual isogeny (here we identify the elliptic curves with their dual abelian varieties as in [6]). Though $[D]$ is an element of $E[l](\mathbb{F}_q)$, it should be thought of as representing an element of $E(\mathbb{F}_q)/\phi A(\mathbb{F}_q)$. Let us show that $\#E(\mathbb{F}_q)/\phi A(\mathbb{F}_q) = l$. As $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -modules, we have $E[\hat{\phi}] \cong \mathbb{Z}/l\mathbb{Z}$; so by Cartier duality we have $A[\phi] \cong \mu_l$. But since $\mu_l \subseteq \mathbb{F}_q$ we have $\mu_l \cong \mathbb{Z}/l\mathbb{Z}$ as $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ -modules. Since $A[\phi] \cong \mathbb{Z}/l\mathbb{Z}$ we see that $E(\mathbb{F}_q)/\phi A(\mathbb{F}_q)$ has size l . Since $l^2 \nmid \#E(\mathbb{F}_q)$, we see that $[D]$ generates $E(\mathbb{F}_q)/\phi A(\mathbb{F}_q)$.

The image of $[D] \in E(\mathbb{F}_q)/\phi A(\mathbb{F}_q)$ under δ_ϕ lands in $H^1(\mathbb{F}_q, A[\phi])$ and is a class of cocycles including, say, ξ . The image of ξ in $A[\phi]$ is then ϕ -Weil paired with $[D]$, a chosen generator of $E[\hat{\phi}]$. Since $\dim_{\mathbb{F}_l} A[\phi] = \dim_{\mathbb{F}_l} E[\hat{\phi}] = 1$, the ϕ -Weil pairing of any two non-trivial elements is non-trivial. From Lemma 5.8, this gives the isomorphism of $E[l](\mathbb{F}_q)$ and $\mathbb{F}_q^*/\mathbb{F}_q^{*l}$ by f_D .

REFERENCES

- [1] Brown, K.S. *Cohomology of Groups*, Springer-Verlag, New York, 1982
- [2] Frey, G. and Rück, H.-G., *A remark concerning m -divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. **62**, (1994), 865–874.
- [3] Lang, S. *Abelian Varieties*, Interscience Publishers, New York, 1959.
- [4] Schaefer, E.F., *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310**, (1998), 447–471.
- [5] Serre, J.-P., *Cohomologie Galoisienne*, Springer-Verlag, New York, 1973.

[6] Silverman, J.H., *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

E-mail address: `eschaefe@math.scu.edu`

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, SANTA CLARA UNIVERSITY, SANTA CLARA,
CA 95053, USA.