A Novel Proof on Weil Pairing

Sutirtha Sanyal
ssanyal77@gmail.com

Abstract

In this paper we will prove a basic property of weil pairing which helps in evaluating its value. We will show that the weil pairing value as computed from the definition is equivalent with the ratio formula based on the miller function. We prove a novel theorem (Theorem 2) and use it to establish the equivalence. We further validate our claims with Sage codes.

I. Introduction and Preliminaries

We will use basic concepts and usual notations from [1].

In general case, the equation of the elliptic curve E, defined over a finite field K and given in the Weierstrass form, is $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where $a_i \in K$. We consider two points in it, S and T of order n, co-prime to $char(K)$. The weil pairing $e_n(S,T)$ can be defined in the following manner. Let the function $f_T^{\mathcal{O}} \in \bar{K}(E)$ has the divisor $n(T) - n(\mathcal{O})$ ($\bar{K}(E)$ is the function field associated with E and $\mathcal{O}$ is the point at infinity). This is the usual miller function [2]. One can choose an arbitrary point X and define another similar function f_T^X with divisor $n(T+X) - n(X)$ (f_T^X= c$f_T^{\mathcal{O}} \circ \tau_{-X}$ where τ_{-X} is the translation by $-X$ map and $c \in K^*$ is some constant).

It is possible to find another point T' in a suitable algebraic closure $\bar{K}$ with the property that $[n]T' = T$, i.e., $T' \in E(\bar{K})[n^2]$. It is clear that once we find one such T', a total of n^2 such points can be found. All the points $T' + R$ where $R \in E[n]$ gives T when multiplied by n. Since we have $E[n] \subset E(\bar{K})$, we are already at the embedding degree.

We can find another function g whose divisor is $\sum((T'+R) - R)$ where $R \in E[n]$. The divisor is principal since $[n^2]T' = \mathcal{O}$. Next we observe that g^n and $f_T^{\mathcal{O}} \circ [n]$ have the same divisor where $[n]$ is the multiplication by n map. So, they are equal (upto multiplication by a constant from K^*). Then the weil pairing is defined as

$$e_n(S,T) = \frac{g(X+S)}{g(X)} \tag{1}$$

It is easy to check that $e_n(S,T)^n = 1$.

Another way of calculating weil pairing is as follows. Choose any other arbitrary point Y and compute

$$e_n(S,T)' = \frac{\frac{f_T^Y(X+S)}{f_T^Y(X)}}{\frac{f_S^X(Y+T)}{f_S^X(Y)}} \tag{2}$$

We prove that $e_n(S,T) = e_n(S,T)'$. During the course of proof we prove and use a novel property, Theorem 2 in section III.

II. Related Work

There are different previous works([3], [1], [4], [5], [6]). In [1], chapter III, section 8, remark 8.5 and in exercise 3.16.(c), the equivalence relationship is stated as

$$\mathit{weil\_pairing}(S,T) = \frac{g(X+S)}{g(X)} = \frac{\frac{f_S^X(Y+T)}{f_S^X(Y)}}{\frac{f_T^Y(X+S)}{f_T^Y(X)}}$$

This is not true as the correct relationship between (1) and (2) is the inverse of it. Both the examples in section IV serve as counterexamples. Now, obviously, inverse of a weil pairing is also another valid weil pairing with all the properties. Therefore, from application point of view, either one can be used. However, as a mathematical formula, if we use the definition of g and $f_T^{\mathcal{O}}$ as stated in [1] and restated in the previous section, then the above equivalence relationship is incorrect. The right hand side of the formula needs to be inverted [7].

In [6], the equivalence relation is stated as

$$\frac{g(X+S)}{g(X)} = (-1)^n \frac{\frac{f_S^X(Y+T)}{f_S^X(Y)}}{\frac{f_T^Y(X+S)}{f_T^Y(X)}}$$

This is incorrect because then for odd n, $(\frac{g(X+S)}{g(X)})^n = -1$, which is incorrect.

The equivalence relationship stated between (1) and (2) is true for all n, whether n is even or odd.

III. The Proof

We start with the following lemma,

Lemma 1. *$e_n(S,T)'$ value as computed in (2) is independent of the choice of X and Y.*

Proof. We will show the independence w.r.t Y (independence w.r.t X holds in similar manner). Specifically we will show,

$$\frac{\frac{f_T^Y(X+S)}{f_T^Y(X)}}{\frac{f_S^X(Y+T)}{f_S^X(Y)}} = \frac{\frac{f_T^{\mathcal{O}}(X+S)}{f_T^{\mathcal{O}}(X)}}{\frac{f_S^X(T)}{f_S^X(\mathcal{O})}} \tag{3}$$

Now, f_T^Y has divisor $n(Y+T) - n(Y) = n(T) - n(\mathcal{O}) + n((Y+T) - (Y) - (T) + (\mathcal{O})) = div(f_T^{\mathcal{O}}) + n(div(h))$, because $(Y+T) - (Y) - (T) + (\mathcal{O})$ is principle, hence there exists a corresponding $h \in \bar{K}(E)$. So, $f_T^Y = cf_T^{\mathcal{O}} h^n$.

So,

$$\frac{\frac{f_T^Y(X+S)}{f_T^Y(X)}}{\frac{f_S^X(Y+T)}{f_S^X(Y)}} = \frac{\frac{f_T^{\mathcal{O}}(X+S)}{f_T^{\mathcal{O}}(X)} \frac{h^n(X+S)}{h^n(X)}}{\frac{f_S^X(Y+T)}{f_S^X(Y)}} = \frac{\frac{f_T^{\mathcal{O}}(X+S)}{f_T^{\mathcal{O}}(X)} \frac{f_S^X(Y+T) f_S^X(\mathcal{O})}{f_S^X(Y) f_S^X(T)}}{\frac{f_S^X(Y+T)}{f_S^X(Y)}} = \frac{\frac{f_T^{\mathcal{O}}(X+S)}{f_T^{\mathcal{O}}(X)}}{\frac{f_S^X(T)}{f_S^X(\mathcal{O})}}$$

Here we have used weil-reciprocity in the following way: $\frac{h^n(X+S)}{h^n(X)} = h(div(f_S^X)) = f_S^X(div(h))$ (weil reciprocity can be applied since f_S^X and h have disjoint support set).

□

Essentially, we have set $Y = \mathcal{O}$ in (2). However, we cannot set X to $\mathcal{O}$ as well because g and $f_T^{\mathcal{O}}$ has a pole (of order 1 and n respectively) at $\mathcal{O}$ hence both (1) and (2) cannot be evaluated. With $Y = \mathcal{O}$, X can be set to any other value (except that $X \notin div(g)$ which contains n^2 $n - torsion$ points, including $\mathcal{O}$, as poles of order 1) giving the same value for $e_n(S,T)'$.

Next, we re-arrange the divisor of g as follows:

$$div(g) = \sum_{R \in E[n]} (T' + R) - (R) = \overbrace{n^2(T') - n^2(\mathcal{O})} + \overbrace{\sum_{R \in E[n] \backslash \{\mathcal{O}\}} (T' + R) - (R) - (T') + (\mathcal{O})}$$

Now, the divisor under the first brace is of $f_{T'}^{\mathcal{O}}$. Each divisor under the second brace is of the form $(T' + R) - (R) - (T') + (\mathcal{O})$. Each one of them is principle.

If we denote a line passing through two points A and B as $l_{(A,B)}$, then it is clear that $\frac{l_{(-R,-T')}}{l_{(R,-R)} l_{(T',-T')}}$ has the divisor $(T' + R) - (R) - (T') + (\mathcal{O})$. This is because $div(l_{(-R,-T')}) = (-R) + (-T') + (T' + R) - 3(\mathcal{O})$ and $div(l_{(R,-R)}) = (R) + (-R) - 2(\mathcal{O})$.

Therefore,

$$g = cf_{T'}^{\mathcal{O}} \prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(-R,-T')}}{l_{(R,-R)} l_{(T',-T')}} \tag{4}$$

Next we re-arrange the divisor of $f_{T'}^{\mathcal{O}}$ as follows:

$$div(f_{T'}^{\mathcal{O}}) = \overbrace{n(T) - n(\mathcal{O})} + n \overbrace{(n(T') - (T) - (n-1)(\mathcal{O}))}$$

The divisor under first brace is of $f_T^{\mathcal{O}}$. The divisor under second brace is principle (since $[n]T' = T$). Hence there exists a function w whose divisor it corresponds.

Therefore,

$$f_{T'}^{\mathcal{O}} = cf_T^{\mathcal{O}} w^n \tag{5}$$

Now, we replace (5) in (4) and replace g in (1) to obtain:

$$\frac{g(X+S)}{g(X)} = \frac{f_T^{\mathcal{O}}(X+S) w^n(X+S) \prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(-R,-T')}(X+S)}{l_{(R,-R)}(X+S) l_{(T',-T')}(X+S)}}{f_T^{\mathcal{O}}(X) w^n(X) \prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(-R,-T')}(X)}{l_{(R,-R)}(X) l_{(T',-T')}(X)}} \tag{6}$$

Now, w has divisor $n(T') - (T) - (n-1)(\mathcal{O})$. Applying weil reciprocity (weil reciprocity can be applied since f_S^X and w have disjoint support set),

$$\frac{w^n(X+S)}{w^n(X)} = w(div(f_S^X)) = f_S^X(div(w)) = \frac{(f_S^X(T'))^n}{f_S^X(T)(f_S^X(\mathcal{O}))^{n-1}} \tag{7}$$

Putting back (7) in (6) and comparing it with (3) we see that it is sufficient to prove,

$$\frac{\prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(-R,-T')}(X+S)}{l_{(R,-R)}(X+S) l_{(T',-T')}(X+S)}}{\prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(-R,-T')}(X)}{l_{(R,-R)}(X) l_{(T',-T')}(X)}} = \left(\frac{f_S^X(\mathcal{O})}{f_S^X(T')} \right)^n \tag{8}$$

We further note that, for any two points A and B, $l_{(A,B)} l_{(-A,-B)} = cl_{(A,-A)} l_{(B,-B)} l_{(A+B,-(A+B))}$, because divisors on the left and right are same.

Using this fact, in place of (8), we prove the following,

$$\frac{\prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(R,T')}(X+S)}{l_{(T'+R,-(T'+R))}(X+S)}}{\prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(R,T')}(X)}{l_{(T'+R,-(T'+R))}(X)}} = \left(\frac{f_S^X(T')}{f_S^X(\mathcal{O})} \right)^n \tag{9}$$

This is the main part of the proof and, we will prove it with the following stronger theorem,

Theorem 2. *For a point $S \in E[n], S \neq \mathcal{O}$, a fixed point $X(\notin E[n])$ and for any other point Z (except $Z \notin X + E[n]$),*

$$\frac{\displaystyle\prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(R,Z)}(X+S)}{l_{(R+Z,-(R+Z))}(X+S)}}{\displaystyle\prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(R,Z)}(X)}{l_{(R+Z,-(R+Z))}(X)}} = \left(\frac{f_S^X(Z)}{f_S^X(\mathcal{O})}\right)^n$$

Proof. First note that, $\frac{l_{(R,Z)}}{l_{(R+Z,-(R+Z))}}$ has divisor $(Z) + (R) - (Z+R) - (\mathcal{O})$.

Let

$$\psi = c \prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(R,Z)}}{l_{(R+Z,-(R+Z))}} \tag{10}$$

Then $div(\psi) = \sum_{R \in E[n] \backslash \{\mathcal{O}\}} (Z) + (R) - (Z+R) - (\mathcal{O})$.

The divisor of ψ can be partitioned as follows:

$$div(\psi) = div(\phi) - div(\phi \circ \tau_{-Z})$$

, where function ϕ has the divisor

$$div(\phi) = \sum_{(R,-R) \in E[n] \backslash \{\mathcal{O}\}} (R) + (-R) - 2(\mathcal{O}) = \sum_{(R,-R) \in E[n] \backslash \{\mathcal{O}\}} (R) + ([n-1]R) - 2(\mathcal{O}) \tag{11}$$

if n is odd. If n is even,

$$div(\phi) = \sum_{(R,-R) \in E[n] \backslash \{\mathcal{O}\}, R \neq -R} (R) + ([n-1]R) - 2(\mathcal{O}) + \sum_{[2]A_i = \mathcal{O}} (A_i) - (\mathcal{O}) \tag{12}$$

This is because, if n is even, $E[n]$ will contain three $2-torsion$ points, denoted as A_i in (12).

$E[n]$ has $n^2 - 1$ non-trivial $n-torsion$ points and hence if n is odd, $div(\phi)$ has $\frac{n^2-1}{2}$ number of terms in (11). In terms of straight lines, ϕ is just the product of vertical lines passing through a point and its inverse in $E[n] \backslash \{\mathcal{O}\}$, i.e,

$$\phi = \prod_{(R,-R) \in E[n] \backslash \{\mathcal{O}\}} (x - R[0]) \tag{13}$$

, where $R[0]$ is the x-coordinate of both R and $-R$.

If n is even, $div(\phi)$ has $\frac{n^2-4}{2} + 3$ number of terms in (12). Because $div(\phi)$ will contain three $2-torsion$ points. Summing over these three points will give a divisor of the form $(A_1) + (A_2) + (A_3) - 3(\mathcal{O})$ which is the divisor of the line $2y + a_1 x + a_3$, where a_1 and a_3 are coefficients of xy and y in the equation of E. ϕ is then product of vertical lines passing through a point and its inverse in $E[n] \backslash \{\mathcal{O}\}$ and $2y + a_1 x + a_3$, i.e,

$$\phi = (2y + a_1 x + a_3) \prod_{(R,-R) \in E[n] \backslash \{\mathcal{O}\}, R \neq -R} (x - R[0]) \tag{14}$$

Therefore, from (10), we have,

$$\frac{\psi(X+S)}{\psi(X)} = \frac{\displaystyle\prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(R,Z)}(X+S)}{l_{(R+Z,-(R+Z))}(X+S)}}{\displaystyle\prod_{R \in E[n] \backslash \{\mathcal{O}\}} \frac{l_{(R,Z)}(X)}{l_{(R+Z,-(R+Z))}(X)}} = \frac{\frac{\phi(X+S)}{\phi \circ \tau_{-Z}(X+S)}}{\frac{\phi(X)}{\phi \circ \tau_{-Z}(X)}} = \frac{\frac{\phi(X+S)}{\phi(X)}}{\frac{\phi \circ \tau_{-Z}(X+S)}{\phi \circ \tau_{-Z}(X)}} \tag{15}$$

We will focus on the numerator of (15).

Next, we know that the structure of $E[n]$ is a free module of rank 2. Lets denote its two basis as B_1 and B_2. The whole $E[n]$ can be generated by $[i]B_1 + [j]B_2$, where $i, j \in [0, \ldots, n-1]$. We are interested in all the points in $E[n]$ except $\mathcal{O}$, because $R \neq \mathcal{O}$ in (10). Hence i and j are not both 0. Let $S = [r_1]B_1 + [r_2]B_2$ for some $r_1, r_2 \in [0, \ldots, n-1]$. Obviously, $-S = [n-1]S = [n-r_1]B_1 + [n-r_2]B_2$.

Next, we consider the divisor of the function $\eta = \frac{\phi \circ \tau_S}{\phi}$.

The divisor is,

$$\begin{aligned} div(\eta) = & \underbrace{\sum_{i=0}^{i=n-1}\sum_{j=0}^{j=n-1}}_{i+j\neq 0}([i-r_1]B_1+[j-r_2]B_2) \\ & -\underbrace{\sum_{i=0}^{i=n-1}\sum_{j=0}^{j=n-1}}_{i+j\neq 0}([n-r_1]B_1+[n-r_2]B_2) \\ & -\underbrace{\sum_{i=0}^{i=n-1}\sum_{j=0}^{j=n-1}}_{i+j\neq 0}([i]B_1+[j]B_2) \\ & +\underbrace{\sum_{i=0}^{i=n-1}\sum_{j=0}^{j=n-1}}_{i+j\neq 0}(\mathcal{O}) \end{aligned} \tag{16}$$

or

$$\begin{aligned} div(\eta) & = \underbrace{\sum_{i=0}^{i=n-1}\sum_{j=0}^{j=n-1}}_{i+j\neq 0}([i-r_1]B_1+[j-r_2]B_2) - \underbrace{\sum_{i=0}^{i=n-1}\sum_{j=0}^{j=n-1}}_{i+j\neq 0}([i]B_1+[j]B_2) \\ & +(n^2-1)(\mathcal{O}) - (n^2-1)([n-r_1]B_1+[n-r_2]B_2) \end{aligned} \tag{17}$$

It can be further simplified. The terms in the first two summations cancel each other except two. When $i = r_1$ and $j = r_2$, the first summation gives a zero at $\mathcal{O}$ which does not get canceled by the second summation. Likewise, the second summation gives a pole at $[n-r_1]B_1 + [n-r_2]B_2$ for $i = n-r_1$ and $j = n-r_2$ which does not get canceled by the first summation. Adding these two with the rest, the divisor takes the final form,

$$div(\eta) = n^2(\mathcal{O}) - n^2([n-r_1]B_1+[n-r_2]B_2) = n^2(\mathcal{O}) - n^2([n-1]S) \tag{18}$$

However, this is the divisor of function $\left(\frac{1}{f^{\mathcal{O}}_{[n-1]S}}\right)^n$.

Therefore, we have,

$$\eta(X)(f^{\mathcal{O}}_{[n-1]S}(X))^n = \frac{\phi(X+S)}{\phi(X)}(f^{\mathcal{O}}_{[n-1]S}(X))^n = c,\ \forall X \notin div(\phi) \tag{19}$$

Returning back to (15), we have ,

$$\begin{aligned} \frac{\psi(X+S)}{\psi(X)} = & \frac{\prod\limits_{R\in E[n]\backslash\{\mathcal{O}\}} \frac{l_{(R,Z)}(X+S)}{l_{(R+Z,-(R+Z))}(X+S)}}{\prod\limits_{R\in E[n]\backslash\{\mathcal{O}\}} \frac{l_{(R,Z)}(X)}{l_{(R+Z,-(R+Z))}(X)}} = \frac{\frac{\phi(X+S)}{\phi\circ\tau_{-Z}(X+S)}}{\frac{\phi(X)}{\phi\circ\tau_{-Z}(X)}} \\ & = \frac{\frac{\phi(X+S)}{\phi(X)}}{\frac{\phi\circ\tau_{-Z}(X+S)}{\phi\circ\tau_{-Z}(X)}} = \frac{\frac{\phi(X+S)}{\phi(X)}}{\frac{\phi(X-Z+S)}{\phi(X-Z)}} = \left(\frac{f^{\mathcal{O}}_{[n-1]S}(X-Z)}{f^{\mathcal{O}}_{[n-1]S}(X)}\right)^n \end{aligned} \tag{20}$$

Next, we prove,

$$\left(\frac{f^{\mathcal{O}}_{[n-1]S}(X-Z)}{f^{\mathcal{O}}_{[n-1]S}(X)}\right) = \frac{f^X_S(Z)}{f^X_S(\mathcal{O})}$$

We consider the divisor of function $\kappa = f^{\mathcal{O}}_{[n-1]S} \circ \tau_X \circ [-1]$.

The divisor is

$$n([-1]([n-1]S - X)) - n([-1](\mathcal{O} - X)) = n(X+S) - n(X)$$

However, f^X_S has the same divisor. So, we have

$$\frac{\kappa(Z)}{f^X_S(Z)} = \frac{f^{\mathcal{O}}_{[n-1]S}(X-Z)}{f^X_S(Z)} = c,\ \forall Z \neq X, X+S \tag{21}$$

The only thing left is to find the value of this constant. In general, in other equations like (19), finding the exact value of the constant is difficult, but for (21) it is straightforward. Putting $Z = \mathcal{O}$ in (21) (Z can be in $E[n]$ because restrictions are $X \notin E[n]$ and $Z \notin X + E[n]$) we have,

$$c = \frac{f^{\mathcal{O}}_{[n-1]S}(X)}{f^X_S(\mathcal{O})}$$

Therefore, we have,

$$\frac{f^{\mathcal{O}}_{[n-1]S}(X-Z)}{f^{\mathcal{O}}_{[n-1]S}(X)} = \frac{f^{X}_{S}(Z)}{f^{X}_{S}(\mathcal{O})} \tag{22}$$

□

IV. Implementation and Validation

We have used Sage [8] to validate claims made during the proof. We have used two elliptic curves to check our assertions on $n-torsion$ points, for even and odd n.

A. Weil Pairing on $10-torsion$ points

We use a finite field of F_{14347^4} with irreducible polynomial $x^4+3x^2+12043x+3$ and multiplicative generator denoted by a. We use the Elliptic Curve $E: y^2 = x^3+x+39$.

We compute weil pairing $e_{10}(S,T)$ between $S = E(1110a^3+10656a^2+5309a+1572, 13867a^3+584a^2+8409a+12362)$ and $T = E(13658a^3+9495a^2+6829a+2596, 6535a^3+2890a^2+13646a+2944)$.

Both S and T are of exact order 10. Moreover, $S \neq [i]T\, i \in (1,9)$, $[5]S \neq [5]T$, $[2]S \neq [2i]T\, i \in (1,4)$ and $T \neq [i]S\, i \in (1,9)$, $[2]T \neq [2i]S\, i \in (1,4)$. This means, S and T can be used as basis for $E[10]$.

T' corresponding to T is $T' = E(8545a^3+11397a^2+5701a+12822, 11533a^3+1070a^2+4865a+6859)$. T' has order 100 and $[10]T' = T$. We compute the whole $E[10]$ taking S and T as basis.

1) Results: The weil pairing value as computed in equation (1), from definition is: $4742a^3+8112a^2+772a+13716$, a primitive $10-th$ root of unity.

The same value can be obtained by equation (2) which calculates the pairing value using ratio of miller's functions. Also, as claimed in (3), Y can be eliminated from (2) without changing the pairing value.

Next we check assertions made in equation (19) and (22).

To check (19), we evaluate η at an arbitrary point X. As we noted η is the ratio of $\phi(X+S)$ and $\phi(X)$. We calculate ϕ as the product $2y \prod\limits_{R,-R\in E[n]\setminus\{\mathcal{O}\}, R\neq -R} (x-R[0])$, since a_1 and a_3 are 0 in this case. As claimed in (19), the product $\left(\frac{\phi(X+S)}{\phi(X)}\right)(f^{\mathcal{O}}_{[9]S}(X))^{10}$ is the constant $4753a^3+3499a^2+11277a+6205$.

Next we validate (22) with $X = E(10779a^3+10994a^2+6005a+8239, 12553a^3+203a^2+13682a+7415)$ and $Z = E(5080a^3+3076a^2+3943a+7238, 12713a^3+5248a^2+8673a+259)$. The value of $f^{X}_{S}(\mathcal{O})$ is the constant used for initialization before starting the iteration in the miller's algorithm. This constant is set to 1.

Value of $f^{\mathcal{O}}_{[9]S}(X-Z)$ is $499a^3+7310a^2+6418a+7484$. Value of $f^{\mathcal{O}}_{[9]S}(X)$ is $7729a^3+5487a^2+2724a+5255$. Their ratio is $4957a^3+9897a^2+11176a+5290$, same as the value of $\frac{f^X_S(Z)}{f^X_S(\mathcal{O})}$.

B. Weil Pairing on $17-torsion$ points

We use a finite field of F_{14347^6} with irreducible polynomial $x^6+4988x^5+10289x^4+12288x^3+8098x^2+11627x+2657$ and indeterminate denoted by a. We use the Elliptic Curve $E: y^2 = x^3+3x+192$. E has a point of order 17 in F_{14347} and $14347^6\, mod\, 17 = 1$.

Now, note that the embedding degree w.r.t $17-torsion$ points is not 6, but it is 2, because $14347^2\, mod\, 17 = 1$. However, we must go to a higher algebraic closure to find T' whose order is 289 and which gives T when multiplied by 17.

We compute weil pairing $e_{17}(S,T)$ between $S = E(4502a^5+3474a^4+2478a^3+4954a^2+3412a+313, 13914a^5+11132a^4+7990a^3+8829a^2+4656a+12436)$ and $T = E(11758, 1749a^5+11694a^4+8713a^3+9267a^2+2664a+6792)$.

Both S and T are of order 17. T' corresponding to T is $T' = E(13385a^5+6906a^4+4034a^3+12326a^2+9781a+8754, 5965a^5+9466a^4+9676a^3+4314a^2+2392a+9507)$. T' has order 289 and $[17]T' = T$. We compute the whole $E[17]$ taking S and another $17-torsion$ point $B = E(11653, 3018)$ as basis (we could have taken T in place of B as well).

1) Results: The weil pairing value as computed in equation (1), from definition is: $4725a^5+14341a^4+6017a^3+2395a^2+2472a+3604$, a $17-th$ root of unity.

The same value can be obtained by equation (2) which calculates the pairing value using ratio of miller's functions. Also, as claimed in (3), Y can be eliminated from (2) without changing the pairing value.

Next we check assertions made in equation (19) and (22).

To check (19), we evaluate η at an arbitrary point X. As we noted η is the ratio of $\phi(X+S)$ and $\phi(X)$. We calculate ϕ as the product $\prod\limits_{R,-R\in E[n]\setminus\{\mathcal{O}\}} (x-R[0])$, where $R[0]$ is the x-coordinate of both R and $-R$. As claimed in (19), the product $\left(\frac{\phi(X+S)}{\phi(X)}\right)(f^{\mathcal{O}}_{[16]S}(X))^{17}$ is the constant $6787a^5+2879a^4+13328a^3+10515a^2+4653a+11540$.

Next we check (22) with $X = E(8824a^5+8715a^4+9456a^3+7907a^2+9332a+6386, 6590a^5+10000a^4+2161a^3+6617a^2+6456a+42)$ and $Z = E(13084a^5+11849a^4+10647a^3+6290a^2+4913a+8692, 1142a^5+12161a^4+5317a^3+2010a^2+2851a+5636)$.

Value of $f^{\mathcal{O}}_{[16]S}(X-Z)$ is $5303a^5+12451a^4+13526a^3+13903a^2+13361a+6973$. Value of $f^{\mathcal{O}}_{[16]S}(X)$ is $646a^5+12955a^4+7680a^3+8279a^2+13854a+8563$. Their ratio is $571a^5+4974a^4+1934a^3+11933a^2+3839a+2060$, same as the value of $\frac{f^X_S(Z)}{f^X_S(\mathcal{O})}$.

V. Conclusion

In this paper we have contributed a novel proof of a fundamental property of weil pairing. The property says that the weil pairing value as computed from the definition is identical with the ratio of miller's functions evaluated at certain points. We state and prove a novel theorem (Theorem 2 in section III) related with the function field associated with the curve. Then we use this theorem to prove the equivalence. We have further verified claims made during the proof with the Sage codes (available at :
https://sites.google.com/site/weilpairingcode/software/weil_pairing.zip?attredirects=0&d=1).

REFERENCES

[1] J. H. Silverman, *The arithmetic of elliptic curves.* Springer, 2009, vol. 106.

[2] V. S. Miller, "Short programs for functions on curves," *Unpublished manuscript*, 1986. [Online]. Available: http://crypto.stanford.edu/miller/miller.pdf

[3] A. Weil, *Courbes algébriques et variétés abéliennes,(2nd Ed.).* Hermann & Cie., 1971.

[4] E. W. Howe, "The weil pairing and the hilbert symbol," *Mathematische Annalen*, vol. 305, pp. 387–392, 1996.

[5] V. S. Miller, "The weil pairing, and its efficient calculation," *Journal of Cryptology*, vol. 17, no. 4, pp. 235–261, 2004.

[6] L. JAIN, "Weil pairing." [Online]. Available: http://www.math.uwaterloo.ca/~djao/co690.2007/weil.pdf

[7] J. H. Silverman, "Errata and corrections to the arithmetic of elliptic curves." [Online]. Available: http://www.math.brown.edu/~jhs/AEC/AECErrata.pdf

[8] W. Stein *et al.*, "Sage: Software for algebra and geometry experimentation," 2006.