The Tate Pairing via Elliptic Nets

Katherine E. Stange

Brown University, Providence, RI 02912, USA

Abstract. We derive a new algorithm for computing the Tate pairing on an elliptic curve over a finite field. The algorithm uses a generalisation of elliptic divisibility sequences known as elliptic nets, which are maps from $\mathbb{Z}^n$ to a ring that satisfy a certain recurrence relation. We explain how an elliptic net is associated to an elliptic curve and reflects its group structure. Then we give a formula for the Tate pairing in terms of values of the net. Using the recurrence relation we can calculate these values in linear time. Computing the Tate pairing is the bottleneck to efficient pairing-based cryptography. The new algorithm has time complexity comparable to Miller's algorithm, and should yield to further optimisation.

Key words: Tate pairing, elliptic curve, elliptic divisibility sequence, elliptic net, Miller's algorithm, pairing-based cryptography.

1 Introduction

The use of pairings in elliptic curve cryptography was originally suggested as a means of reducing the discrete logarithm problem on an elliptic curve to the discrete logarithm problem on a finite field [1, 2], but considerable excitement and research has since been generated by public-key cryptographic applications such as Sakai, Ohgishi and Kasahara's key agreement and signature schemes [3], Joux's tri-partite Diffie-Hellman key exchange [4], and Boneh and Franklin's identity-based encryption scheme [5]. Good overviews of the research include [6, 7], while a very up-to-date research bibliography can be found at [8].

The bottleneck to pairing-based cryptographic implementations is the costly computation of the pairing, which is most frequently the Tate or Weil pairing, the former usually being more efficient. Currently, the only polynomial time algorithm is due to Victor Miller [9] (for an overview of implementions, see [10, 11]).

In this paper, we propose a new method of computing of the Tate pairing, arising from the theory of elliptic nets.

Elliptic nets are a generalisation of elliptic divisibility sequences, which were first studied by Morgan Ward in 1948 [12]. These are integer sequences h_0, h_1, h_2, …, h_n, … satisfying the following two properties:

1. For all positive integers $m > n$,

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \ . \tag{1}$$

2. h_n divides h_m whenever n divides m.

Ward demonstrates that an elliptic divisibility sequence arises from any choice of elliptic curve and rational point on that curve.

Theorem 1 (M. Ward, 1948, [12]). *Suppose E is an elliptic curve defined over $\mathbb{Q}$, $\sigma : \mathbb{C} \to \mathbb{C}$ is its Weierstrass sigma function, and $u \in \mathbb{C}$ corresponds to a rational point on E. Then there exists an integer k such that the sequence*

$$h_n := k^{n^2-1} \frac{\sigma(nu)}{\sigma(u)^{n^2}}$$

forms an elliptic divisibility sequence.

For an overview of research on elliptic divisibility sequences, see [13].

Given an integral domain R and a finitely generated free abelian group A, an *elliptic net* is a map $W : A \to R$ satisfying the following recurrence relation for $p, q, r, s \in A$:

$$\begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &\qquad + W(q+r+s)W(q-r)W(p+s)W(p) \\ &\qquad\qquad + W(r+p+s)W(r-p)W(q+s)W(q) = 0 \ . \end{aligned}$$

When $A = R = \mathbb{Z}$ and $W(1) = 1$, the positive terms of an elliptic net satisfy Ward's equation (1) above. Under the further conditions that $W(2)|W(4)$ and $W(0) = 0$, these terms form an elliptic divisibility sequence.

Theorem 2 in Sect. 2 relates elliptic nets over $R = \mathbb{C}$ to elliptic curves, generalising Theorem 1. However, for cryptographic applications it is desired to work over finite fields: Theorem 3 allows results over $\mathbb{C}$ to be carried over to the finite field case. Theorem 4 is the statement of the curve-net relationship over finite fields.

According to these results, we can associate to any choice of curve E defined over a finite field K and n points $P_i \in E(K)$ an elliptic net

$$W_{E,P_1,\ldots,P_n} : \mathbb{Z}^n \to K \ .$$

This net can then be used to compute the Tate pairing: the main result can be stated as follows.

Theorem (Introductory Version of Theorem 6). *Fix a positive $m \in \mathbb{Z}$. Let E be an elliptic curve defined over a finite field K containing the m-th roots of unity. Let P, $Q \in E(K)$, with $[m]P = \mathcal{O}$. Choose $S \in E(K)$ such that $S \notin \{\mathcal{O}, -Q\}$. Then there exists an elliptic net $W : \mathbb{Z}^n \to K$ and $\mathbf{p}, \mathbf{q}, \mathbf{s} \in \mathbb{Z}^n$ such that the quantity*

$$T_m(P,Q) = \frac{W(\mathbf{s} + m\mathbf{p} + \mathbf{q})W(\mathbf{s})}{W(\mathbf{s} + m\mathbf{p})W(\mathbf{s} + \mathbf{q})}$$

is exactly the Tate pairing $T_m = \tau_m : E(K)[m] \times E(K)/mE(K) \to K^*/(K^*)^m$.

From Theorem 6, to calculate the Tate pairing efficiently only requires an efficient method of calculating the terms of an elliptic net. Rachel Shipsey's thesis provides a double-and-add method of calculating the n-th term of an elliptic divisibility sequence in $\log n$ time [14]. We generalise her algorithm to elliptic nets in Sect. 4.

This application is an example of doing arithmetic on elliptic curves via the arithmetic of elliptic nets. Rachel Shipsey's work made use of this approach to solve the elliptic curve discrete logarithm problem in certain cases. Her paradigm may have many other fruitful applications.

The Elliptic Net Algorithm and Miller's algorithm are both $log(n)$ algorithms; the difference is in the constants. In this nascent form, the Elliptic Net Algorithm is only somewhat slower than an optimised Miller's, especially at higher embedding degrees. This note should be considered a call to further research.

Guide to the Reader. I give substantial mathematical background in Sect. 2, which is currently unavailable elsewhere, and will be necessary for any improvements and new applications. The entirely theory-averse can skip the preliminaries. For most, a suggested path is Sect. 2.2 with reference to Definition 1, followed by Sect. 2.4 and 2.5. The proof of Theorem 3 is omitted for lack of space: for this and more details, see [15].

In Sect. 3, we prove Theorem 6 and a corollary relating elliptic nets and the Tate pairing. In Sect. 4, we describe the algorithms necessary to compute elliptic nets, and therefore the Tate pairing, efficiently. In Sect. 5, we make some brief remarks on optimisation of the algorithms and the efficiency as compared with Miller's algorithm. Finally, we make some concluding remarks in Sect. 6.

2 Mathematical Preliminaries

2.1 Elliptic Functions $\Psi_{\mathbf{v}}$

Elliptic Curves over $\mathbb{C}$. We begin with some complex function theory which will be necessary for the definition of elliptic nets over $\mathbb{C}$. This material is covered in, for example, [16, 17]. For a complex lattice Λ, define the Weierstrass sigma function $\sigma : \mathbb{C} \to \mathbb{C}$ by

$$\sigma(z;\Lambda) = z \prod_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(1 - \frac{z}{\omega}\right) e^{z/\omega + (1/2)(z/\omega)^2} \quad ,$$

and the Weierstrass zeta function $\zeta : \mathbb{C} \to \mathbb{C}$ by

$$\zeta(z;\Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \quad .$$

Recall that the quantity

$$\zeta(z+\omega;\Lambda)-\zeta(z;\Lambda)$$

is independent of z, and we call this $\eta(\omega)$. The map $\eta : \Lambda \to \mathbb{C}$ is called the quasi-period homomorphism. Define $\lambda : \Lambda \to \{\pm 1\}$ by

$$\lambda(\omega) = \begin{cases} 1 & \text{if } \omega \in 2\Lambda \ , \\ -1 & \text{if } \omega \notin 2\Lambda \ . \end{cases}$$

Recall that the Weierstrass sigma function $\sigma : \mathbb{C} \to \mathbb{C}$ satisfies the following transformation formula for all $z \in \mathbb{C}$ and $\omega \in \Lambda$:

$$\sigma(z+\omega;\Lambda) = \lambda(\omega)e^{\eta(\omega)(z+\frac{1}{2}\omega)}\sigma(z;\Lambda) \ . \tag{2}$$

Functions $\boldsymbol{\Psi}_{\mathbf{v}}$. We now define the functions which will be used to obtain an elliptic net from an elliptic curve, and collect a few basic results for later reference.

Definition 1. *Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E. For $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$, define a function $\Psi_{\mathbf{v}}$ on $\mathbb{C}^n$ in variables $\mathbf{z} = (z_1, \ldots, z_n)$ as follows:*

$$\Psi_{\mathbf{v}}(\mathbf{z};\Lambda) = \frac{\sigma(v_1z_1+\ldots+v_nz_n;\Lambda)}{\displaystyle\prod_{i=1}^{n}\sigma(z_i;\Lambda)^{2v_i^2-\sum_{j=1}^{n}v_iv_j}\prod_{1\le i<j\le n}\sigma(z_i+z_j;\Lambda)^{v_iv_j}} \ .$$

In particular, we have for each $n \in \mathbb{Z}$, a function Ψ_n on $\mathbb{C}$ in the variable z:

$$\Psi_n(z;\Lambda) = \frac{\sigma(nz;\Lambda)}{\sigma(z;\Lambda)^{n^2}} \ ,$$

and for each pair $(m,n) \in \mathbb{Z}\times\mathbb{Z}$, a function $\Psi_{m,n}$ on $\mathbb{C}\times\mathbb{C}$ in variables z and w:

$$\Psi_{m,n}(z,w;\Lambda) = \frac{\sigma(mz+nw;\Lambda)}{\sigma(z;\Lambda)^{m^2-mn}\sigma(z+w;\Lambda)^{mn}\sigma(w;\Lambda)^{n^2-mn}} \ .$$

From the general theory of elliptic functions, the divisor of $\Psi_{\mathbf{v}}$ as a function of z_1 is

$$\left(\sum_{j=2}^{n}[-v_j]z_j\right) - \sum_{j=2}^{n}v_1v_j(-z_j) - \left(v_1^2 - \sum_{j=2}^{n}v_1v_j\right)(0) \ . \tag{3}$$

Proposition 1. *The functions $\Psi_{\mathbf{v}}$ are elliptic functions in each variable.*

Proof. Let $\omega \in \Lambda$. We show the function is elliptic in the first variable. Let $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$ and $\mathbf{z} = (z_1, \ldots, z_n), \mathbf{w} = (\omega, 0, \ldots, 0) \in \mathbb{C}^n$. Using (2), we calculate

$$F = \frac{\Psi_{\mathbf{v}}(\mathbf{z}+\mathbf{w};\Lambda)}{\Psi_{\mathbf{v}}(\mathbf{z};\Lambda)} = \frac{\lambda(v_1\omega)}{\lambda(\omega)^{v_1^2}} \ .$$

If $\omega, v_1\omega \notin 2\Lambda$, then v_1 is odd, and $F = 1$. If $\omega \notin 2\Lambda$ but $v_1\omega \in 2\Lambda$, then v_1 must be even, and so $F = 1$ again. Finally, if $\omega \in 2\Lambda$, then $v_1\omega \in 2\Lambda$, and $F = 1$. Thus $\Psi_{\mathbf{v}}$ is invariant under adding a period to the variable z_1. Similarly $\Psi_{\mathbf{v}}$ is elliptic in each variable on $\mathbb{C}^n$. □

In view of this proposition, we will use the same notation $\Psi_{\mathbf{v}}$ for the associated map $E^n \to \mathbb{C}$, and write, for example, $\Psi_{m,n}(P_1, P_2; E)$.

Proposition 2. *Fix a lattice $\Lambda \subset \mathbb{C}$ corresponding to an elliptic curve. Let $\mathbf{v} \in \mathbb{Z}^n$ and $\mathbf{z} \in \mathbb{C}^n$. Let T be an $n \times n$ matrix with entries in $\mathbb{Z}$ and transpose T^{tr}. Then*

$$\Psi_{\mathbf{v}}(T^{tr}(\mathbf{z}); \Lambda) = \frac{\Psi_{T(\mathbf{v})}(\mathbf{z}; \Lambda)}{\prod_{i=1}^{n} \Psi_{T(\mathbf{e}_i)}(\mathbf{z}; \Lambda)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \le i < j \le n} \Psi_{T(\mathbf{e}_i + \mathbf{e}_j)}(\mathbf{z}; \Lambda)^{v_i v_j}} \ . \quad (4)$$

Proof. A straightforward calculation using (2). □

2.2 Elliptic Nets from Elliptic Curves

Definition 2. *Let A be a finitely generated free abelian group, and R be an integral domain. An* elliptic net *is any map $W : A \to R$ such that the following recurrence holds for all p, q, r, $s \in A$:*

$$\begin{aligned} W(p+q+s)W(p-q)W(r+s)W(r) \\ + W(q+r+s)W(q-r)W(p+s)W(p) \\ + W(r+p+s)W(r-p)W(q+s)W(q) = 0 \ . \quad (5) \end{aligned}$$

The set of such nets is denoted $\mathcal{EN}(A, R)$. If B is a subgroup of A, then W restricted to B is also an elliptic net and is called an elliptic subnet *of A.*

Proposition 3. *Let $W : A \to R$ be an elliptic net. Then $W(-z) = -W(z)$ for any $z \in A$. In particular $W(0) = 0$.*

Proof. If $W(-z) = W(z) = 0$, we are done. If not, then without loss of generality, assume $W(z) \neq 0$. Then setting $p = q = z, r = s = 0$ in (5), we obtain $0 + W(z)^4 + W(z)^3 W(-z) = 0$, whence $W(-z) = -W(z)$. □

Work of Christine Swart [18] and van der Poorten [19] on translated elliptic divisibility sequences provided the clues that the theory of elliptic nets existed. It has recently come to my attention that the possibility of such a definition was briefly discussed in correspondence by Noam Elkies, James Propp and Michael Somos in 2001 [20].

We will now see that the $\Psi_{\mathbf{v}}$ form an elliptic net as a function of $\mathbf{v} \in \mathbb{Z}^n$ when the curve E and points $P_1, \ldots, P_n$ are fixed. Let the standard basis of $\mathbb{Z}^n$ be denoted $\mathbf{e}_1, \ldots, \mathbf{e}_n$. As a means of fixing n points P_i, we specify a homomorphism $\phi : \mathbb{Z}^n \to E$.

Definition 3. *Fix an elliptic curve E. Suppose $\phi : \mathbb{Z}^n \to E$ is a homomorphism such that the images of $\pm\mathbf{e}_i$ under ϕ are all distinct and nonzero. Define $W_\phi : \mathbb{Z}^n \to \mathbb{C}$ by*

$$W_\phi(\mathbf{v}) = \Psi_{\mathbf{v}}(\phi(\mathbf{e}_1), \phi(\mathbf{e}_2), \ldots, \phi(\mathbf{e}_n); E) \ .$$

Theorem 2. *W_ϕ is an elliptic net.*

We will prove Theorem 2 in the next section.

Suppose we choose n points P_i of an elliptic curve E, such that the $\pm P_i$ are all distinct and nonzero. Define $\phi : \mathbb{Z}^n \to E$ by $\phi(\mathbf{e}_i) = P_i$. We call $W_\phi \in \mathcal{EN}(\mathbb{Z}^n, \mathbb{C})$ the *elliptic net associated to* $E, P_1, \ldots, P_n$. In fact, $W_\phi \in \mathcal{EN}(\mathbb{Z}^n, L)$ where L is the field of definition of the P_i. Part of the first quadrant of such an example net is shown in Fig. 1 at left. In this example, $E : y^2 + y = x^3 + x^2 - 2x$, $P = (0,0)$, $Q = (1,0)$, and $L = \mathbb{Q}$. For example, $W(3,2) = -13$.

4335	5959	12016	-55287	23921	1587077	-7159461
94	479	919	-2591	13751	68428	424345
-31	53	-33	-350	493	6627	48191
-5	8	-19	-41	-151	989	-1466
1	3	-1	-13	-36	181	-1535
1	1	2	-5	7	89	-149
0	1	1	-3	11	38	249

$\uparrow$ Q $P \rightarrow$ over $\mathbb{Q}$

0	4	4	3	1	2	4
4	4	4	4	1	3	0
4	3	2	0	3	2	1
0	3	1	4	4	4	4
1	3	4	2	4	1	0
1	1	2	0	2	4	1
0	1	1	2	1	3	4

$\uparrow$ Q $P \rightarrow$ over $\mathbb{F}_5$

Fig. 1. Portion of the elliptic net of $E : y^2 + y = x^3 + x^2 - 2x$, $P = (0,0)$, $Q = (1,0)$

Let E be an elliptic curve defined over $\mathbb{Q}$, and $P \in E(\mathbb{Q})$. Then if the positive terms of the elliptic net associated to E, P are integers, they form an elliptic divisibility sequence as described by Ward. In particular, the recurrence relation (5) implies Ward's relation (1). For example, in Fig. 1, the bottom row is the elliptic divisibility sequence associated to P: 0, 1, 1, -3, 11, 38, 249, ...

A word of caution: it is not appropriate to think of elliptic nets as maps on the points of the curve. This can lead to two misconceptions. First, although it is tempting in this example to think of -13 as the "number associated to $3P+2Q$", this depends on the choice of "basis" P, Q of the net. That is to say, if we consider instead the net W' associated to $E, P+Q, P$, then $W'(2,1)$ is **not** equal to $W(3,2)$. The relationship between the nets relative to different bases on a single curve is the content of Proposition 2. Further, even having restricted our attention to exactly one net we may be surprised. Suppose W is an elliptic net associated to E, P where P is an m-torsion point. We cannot expect $W(m+k)$ to equal $W(k)$ in general. We will address these crucial issues in Sect. 2.5.

2.3 Proof of Theorem 2

Proof. We will make use of the well-known elliptic function identity

$$\wp(a) - \wp(b) = -\frac{\sigma(a+b)\sigma(a-b)}{\sigma(a)^2\sigma(b)^2} \quad . \tag{6}$$

First, we show that

$$\zeta(x+a) - \zeta(a) - \zeta(x+b) + \zeta(b) = \frac{\sigma(x+a+b)\sigma(x)\sigma(a-b)}{\sigma(x+a)\sigma(x+b)\sigma(a)\sigma(b)} \quad . \tag{7}$$

Denote by f and g the left and right side of (7) respectively. Suppose that $a, b \notin \Lambda$. The functions f and g are elliptic in x. Both f and g have single poles at $-a$ and $-b$ only. The zeroes of g are at $-a-b$ and 0. These are also zeroes of f, since ζ is an odd function. Hence we have $f = cg$ for some c not depending on x. Now define instead

$$\begin{aligned} F &= (\zeta(x+a) - \zeta(a) - \zeta(x+b) + \zeta(b))\,\sigma(x+a)\sigma(x+b) \ , \\ G &= \sigma(x+a+b)\sigma(x) \ . \end{aligned}$$

We have $F = c'G$ for some constant c' independent of x. Taking derivatives and evaluating at $x = 0$, we have

$$(\wp(a) - \wp(b))\,\sigma(a)\sigma(b) = c'\sigma(a+b)\sigma'(0) \ .$$

We have $\sigma'(0) = 1$. By (6),

$$c' = -\frac{\sigma(a-b)}{\sigma(a)\sigma(b)} \ .$$

which proves (7).

Fix $\mathbf{z} \in \mathbb{C}^n$. We will show that the values $\Psi_{\mathbf{v}}(\mathbf{z};\Lambda)$ for $\mathbf{v} \in \mathbb{Z}^n$ form an elliptic net. For notational simplicity, we drop the arguments $(\mathbf{z};\Lambda)$ and also write $\sigma(\mathbf{v})$, $\wp(\mathbf{v})$ and $\zeta(\mathbf{v})$ for $\sigma(\mathbf{v}\cdot\mathbf{z})$, $\wp(\mathbf{v}\cdot\mathbf{z})$ and $\zeta(\mathbf{v}\cdot\mathbf{z})$. We observe that $\mathbf{v} = \mathbf{0}$ if and only if $\Psi_{\mathbf{v}} \equiv 0$.

If any of $\mathbf{p}$, $\mathbf{q}$, $\mathbf{r}$, $\mathbf{p}+\mathbf{s}$, $\mathbf{q}+\mathbf{s}$, or $\mathbf{r}+\mathbf{s}$ are zero, then the recurrence relation (5) holds trivially. So we may assume none of $\Psi_{\mathbf{p}}$, $\Psi_{\mathbf{q}}$, $\Psi_{\mathbf{r}}$, $\Psi_{\mathbf{p}+\mathbf{s}}$, $\Psi_{\mathbf{q}+\mathbf{s}}$, or $\Psi_{\mathbf{r}+\mathbf{s}}$ is identically zero.

For any quadratic form f defined on $\mathbb{Z}^n$, we have the following relation for all $\mathbf{p}, \mathbf{q}, \mathbf{s} \in \mathbb{Z}^n$:

$$f(\mathbf{p}+\mathbf{q}+\mathbf{s}) + f(\mathbf{p}-\mathbf{q}) + f(\mathbf{s}) - f(\mathbf{p}+\mathbf{s}) - f(\mathbf{p}) - f(\mathbf{q}+\mathbf{s}) - f(\mathbf{q}) = 0 \ . \tag{8}$$

Suppose that $\mathbf{s} \neq \mathbf{0}$ and so $\Psi_{\mathbf{s}} \not\equiv 0$. By (8) and (7),

$$\frac{\Psi_{\mathbf{p}+\mathbf{q}+\mathbf{s}}\Psi_{\mathbf{p}-\mathbf{q}}\Psi_{\mathbf{s}}}{\Psi_{\mathbf{p}+\mathbf{s}}\Psi_{\mathbf{p}}\Psi_{\mathbf{q}+\mathbf{s}}\Psi_{\mathbf{q}}} = \frac{\sigma(\mathbf{p}+\mathbf{q}+\mathbf{s})\sigma(\mathbf{p}-\mathbf{q})\sigma(\mathbf{s})}{\sigma(\mathbf{p}+\mathbf{s})\sigma(\mathbf{p})\sigma(\mathbf{q}+\mathbf{s})\sigma(\mathbf{q})} = \zeta(\mathbf{p}+\mathbf{s}) - \zeta(\mathbf{p}) - \zeta(\mathbf{q}+\mathbf{s}) + \zeta(\mathbf{q}) \ .$$

Therefore, we have

$$\frac{\Psi_{\mathbf{p}+\mathbf{q}+\mathbf{s}}\Psi_{\mathbf{p}-\mathbf{q}}\Psi_{\mathbf{s}}}{\Psi_{\mathbf{p}+\mathbf{s}}\Psi_{\mathbf{p}}\Psi_{\mathbf{q}+\mathbf{s}}\Psi_{\mathbf{q}}} + \frac{\Psi_{\mathbf{q}+\mathbf{r}+\mathbf{s}}\Psi_{\mathbf{q}-\mathbf{r}}\Psi_{\mathbf{s}}}{\Psi_{\mathbf{q}+\mathbf{s}}\Psi_{\mathbf{q}}\Psi_{\mathbf{r}+\mathbf{s}}\Psi_{\mathbf{r}}} + \frac{\Psi_{\mathbf{r}+\mathbf{p}+\mathbf{s}}\Psi_{\mathbf{r}-\mathbf{p}}\Psi_{\mathbf{s}}}{\Psi_{\mathbf{r}+\mathbf{s}}\Psi_{\mathbf{r}}\Psi_{\mathbf{p}+\mathbf{s}}\Psi_{\mathbf{p}}} = 0 \ ,$$

or, more simply,

$$\Psi_{\mathbf{p}+\mathbf{q}+\mathbf{s}}\Psi_{\mathbf{p}-\mathbf{q}}\Psi_{\mathbf{r}+\mathbf{s}}\Psi_{\mathbf{r}} + \Psi_{\mathbf{q}+\mathbf{r}+\mathbf{s}}\Psi_{\mathbf{q}-\mathbf{r}}\Psi_{\mathbf{p}+\mathbf{s}}\Psi_{\mathbf{p}} + \Psi_{\mathbf{r}+\mathbf{p}+\mathbf{s}}\Psi_{\mathbf{r}-\mathbf{p}}\Psi_{\mathbf{q}+\mathbf{s}}\Psi_{\mathbf{q}} = 0 \ ,$$

which is what was required to prove.

The case $\mathbf{s} = 0$ is done similarly, using

$$\frac{\Psi_{\mathbf{p}+\mathbf{q}}\Psi_{\mathbf{p}-\mathbf{q}}}{\Psi_{\mathbf{p}}^2\Psi_{\mathbf{q}}^2} = \frac{\sigma(\mathbf{p}+\mathbf{q})\sigma(\mathbf{p}-\mathbf{q})}{\sigma(\mathbf{p})^2\sigma(\mathbf{q})^2} = \wp(\mathbf{q}) - \wp(\mathbf{p}) \ .$$

□

2.4 Moving to Finite Fields

Some Notation Now is a good moment to collect the relevant notation for the next section and the remainder of the paper.

L	number field contained in $\mathbb{C}$
E_L	elliptic curve defined over L
R	ring of integers of L
$\mathfrak{p}$	prime of R of good reduction for E_L
$k_\mathfrak{p}$	residue field of $\mathfrak{p}$
$E_{k_\mathfrak{p}}$	E_L reduced modulo $\mathfrak{p}$
$\delta : E_L(L) \to E_{k_\mathfrak{p}}(k_\mathfrak{p})$	reduction map modulo $\mathfrak{p}$
$\delta : \mathbb{P}^1(L) \to \mathbb{P}^1(k_\mathfrak{p})$	reduction map modulo $\mathfrak{p}$

Reduction Modulo $\mathfrak{p}$ We wish to extend the relationship between nets and curves to finite fields, but we can no longer use Weierstrass' sigma function to define appropriate functions. The following theorem allows us to push results on number fields L over to residue fields $k_\mathfrak{p}$. It says that we can find the appropriate functions $\Omega_\mathbf{v}$ for $E_{k_\mathfrak{p}}$ by simply considering the net $\Psi_\mathbf{v}$ modulo $\mathfrak{p}$. These $\Omega_\mathbf{v}$ will also form an elliptic net.

Theorem 3. *Consider points $P_1, \ldots, P_n \in E_L(L)$ such that the reductions modulo $\mathfrak{p}$ of the $\pm P_i$ are all distinct and nonzero. Then for each $\mathbf{v} \in \mathbb{Z}^n$ there exists a function $\Omega_\mathbf{v}$ such that the following diagram commutes:*

$$\begin{array}{ccc} E_L^n(L) & \xrightarrow{\Psi_\mathbf{v}} & \mathbb{P}^1(L) \\ \delta\downarrow & & \downarrow\delta \\ E_{k_\mathfrak{p}}^n(k_\mathfrak{p}) & \xrightarrow{\Omega_\mathbf{v}} & \mathbb{P}^1(k_\mathfrak{p}) \end{array}$$

Furthermore $\operatorname{div}(\Omega_\mathbf{v}) = \delta^* \operatorname{div}(\Psi_\mathbf{v})$.

Proof (Sketch). Consider E^n as a scheme over $\operatorname{Spec} R$. The proof requires extending the function on the generic fibre to the special fibres. The difficulty lies in showing that the resulting function does not have any vertical fibres in the support of its divisor. This reduces to a statement about the form of the $\Psi_{\mathbf{v}}$ as polynomials in the structure sheaf. It relies on a number of nested and complicated inductive proofs. See [15]. □

In light of this, we extend Definition 3 and Theorem 2.

Definition 4. *Let $\phi : \mathbb{Z}^n \to E_{k_\mathfrak{p}}$ be a homomorphism such that the images of $\pm\mathbf{e}_i$ under ϕ are all distinct and nonzero. Let $\Omega_{\mathbf{v}}$ be defined according to Theorem 3. Define $W_\phi : \mathbb{Z}^n \to k_\mathfrak{p}$ by*

$$W_\phi(\mathbf{v}) = \Omega_{\mathbf{v}}(\phi(\mathbf{e}_1), \phi(\mathbf{e}_2), \ldots, \phi(\mathbf{e}_n)) \enspace .$$

Theorem 4. *Suppose K is either a number field or a finite field, and E is an elliptic curve defined over K. Let $\phi : \mathbb{Z}^n \to E(K)$ be a homomorphism. Then W_ϕ is an elliptic net.*

Proof. If K is a number field, this is Theorem 2. If K is a finite field, then this statement follows from Theorem 3: an elliptic net postcomposed with a homomorphism is still an elliptic net. □

Figure 1 illustrates the relationship between an example elliptic net associated to E, P, Q over $\mathbb{Q}$ and the elliptic net associated to their reductions modulo 5.

2.5 Equivalence of Nets

In this section, we restrict ourselves to finite fields.

Definition 5. *Let $W_1, W_2 \in \mathcal{EN}(A, K)$. Suppose $\alpha, \beta \in K^*$, and $f : A \to \mathbb{Z}$ is a quadratic form. If*

$$W_1(\mathbf{v}) = \alpha\beta^{f(\mathbf{v})} W_2(\mathbf{v})$$

for all $\mathbf{v}$, then we say W_1 is equivalent *to W_2 and write $W_1 \sim W_2$.*

Clearly this definition gives an equivalence relation, and it is easily verified that an equivalence applied to an elliptic net gives another elliptic net. We write

$$\mathcal{EN}_0(A, K) = \mathcal{EN}(A, K)/\sim \enspace .$$

If W_1 is a subnet of W_2, then we may, by abuse of language, say that the equivalence class $[W_1]$ is a subnet of the equivalence class $[W_2]$, since then any $W_1' \in [W_1]$ will be equivalent to some subnet of any $W_2' \in [W_2]$.

Recall the discussion at the end of Sect. 2.2. There, we encountered two reasons that we cannot consider an elliptic net W to be a map on the group $E(K)$ itself. The first is that a basis must be chosen, and the second is that the net may take different values at two vectors $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{Z}^n$ even when $\phi(\mathbf{v}_1) = \phi(\mathbf{v}_2) \in E(K)$.[1]

All is not lost, however. We can define elliptic nets on a free abelian cover of $E(K)$, and we shall see that, at least up to equivalence, we can do this in a canonical way.

Proposition 2 gives a "basis transformation formula" for elliptic nets. This formula holds in the finite field case by Theorem 3. We will see that it provides an equivalence of nets. This allows us to define a net on a free abelian cover of $E(K)$ whose equivalence class is unique.

Choose a free abelian group of finite rank with a quotient map

$$\pi : \hat{E}_K \to E_K(K) \ .$$

Let $\hat{\Gamma} \cong \mathbb{Z}^n$ be a subgroup of $\hat{E}_K$. Let $\Gamma = \pi(\hat{\Gamma})$. For any surjective homomorphism $\phi : \mathbb{Z}^n \to \Gamma$ there exists a lift $\hat{\phi} : \mathbb{Z}^n \to \hat{\Gamma}$ which is an isomorphism.

We define

$$V_\phi = W_\phi \circ \hat{\phi}^{-1} \ .$$

Theorem 5. *$V_\phi \in \mathcal{EN}(\hat{\Gamma}, K)$ and the equivalence class of V_ϕ is independent of the choice of the surjective map $\phi : \mathbb{Z}^n \to \Gamma$.*

Proof. The linearity of ϕ^{-1} shows that V_ϕ is an elliptic net.

Suppose $T : \mathbb{Z}^n \to \mathbb{Z}^n$ is a homomorphism. Then a restatement of Proposition 2 translated to finite fields via Theorem 3 is that $W_{\phi \circ T} \sim W_\phi \circ T$ (note that every finite field has a primitive element).

Now choose another surjective $\phi' : \mathbb{Z}^n \to \Gamma$. Then there exists an isomorphism $T : \mathbb{Z}^n \to \mathbb{Z}^n$ such that $\hat{\phi} \circ T = \hat{\phi}'$ and $\phi \circ T = \phi'$. Then

$$V_{\phi'} = W_{\phi'} \circ \hat{\phi}'^{-1} = W_{\phi \circ T} \circ T^{-1} \circ \hat{\phi}^{-1} \sim W_\phi \circ \hat{\phi}^{-1} = V_\phi \ .$$

The equivalence holds since $T^{-1} \circ \hat{\phi}^{-1}$ is linear. So we have defined a unique class $[V_\phi] \in \mathcal{EN}_0(\hat{\Gamma}, K)$. ◻

Definition 6. *Let $\mathcal{W}_{\hat{E}_K}$ denote the class $[V_\phi] \in \mathcal{EN}_0(\hat{E}_K, K)$ defined in Theorem 5.*

This equivalence class is in some sense the "abstract" elliptic net. Just as one writes an abstract linear transformation as a matrix with respect to a basis in order to do calculations, we must choose a basis in order to do calculations with nets. This choice of basis is for us the choice of homomorphism $\phi : \mathbb{Z}^n \to E(K)$. Theorem 6 gives a formula for the Tate pairing independent of the equivalence class chosen in $\mathcal{W}_{\hat{E}_K}$. Later, we will exploit this freedom to choose an appropriate ϕ for efficient calculations.

We note one useful proposition.

Proposition 4. *Let $W \in \mathcal{W}_{\hat{E}_K}$. Then $W(p) = 0$ implies $\pi(p) = \mathcal{O}$.*

Proof. If $W(p) = 0$ then by definition $\Omega_{\mathbf{v}}(\mathbf{P}) = 0$ for some $\mathbf{v}$ and $\mathbf{P}$ such that $\mathbf{v} \cdot \mathbf{P} = \pi(p)$. But the zeroes $\mathbf{P}$ of $\Psi_{\mathbf{v}}$ are exactly those $\mathbf{P}$ such that $\mathbf{v} \cdot \mathbf{P} = 0$. ◻

[1] An examination of the statement of Theorem 6 reveals that the difference in these values is in some sense what the Tate pairing measures.

2.6 The Tate Pairing

Choose $m \in \mathbb{Z}^+$. Let E be an elliptic curve defined over a field K containing the m-th roots of unity. Suppose $P \in E(K)[m]$ and $Q \in E(K)/mE(K)$. Since P is an m-torsion point, $m(P) - m(\mathcal{O})$ is a principal divisor, say $\operatorname{div}(f_P)$. Choose another divisor D_Q defined over K such that $D_Q \sim (Q) - (\mathcal{O})$ and with support disjoint from $\operatorname{div}(f_P)$. Then, we may define the Tate pairing

$$\tau_m : E(K)[m] \times E(K)/mE(K) \to K^*/(K^*)^m$$

by

$$\tau_m(P, Q) = f_P(D_Q) \ .$$

This pairing is well-defined, bilinear and Galois invariant. For cryptographic applications, the Tate pairing is usually considered over finite fields, where it is non-degenerate. For details, see [21, 22].

3 Tate Pairing Using Elliptic Nets

Theorem 6. *Fix a positive $m \in \mathbb{Z}$. Let E be an elliptic curve defined over a finite field K containing the m-th roots of unity. Let P, $Q \in E(K)$, with $[m]P = \mathcal{O}$. Choose $S \in E(K)$ such that $S \notin \{\mathcal{O}, -Q\}$. Choose p, q, $s \in \hat{E}_K$ such that $\pi(p) = P$, $\pi(q) = Q$ and $\pi(s) = S$. Let $W \in \mathcal{W}_{\hat{E}_K}$. Then the quantity*

$$T_m(P, Q) = \frac{W(s + mp + q)W(s)}{W(s + mp)W(s + q)} \tag{9}$$

is a well-defined function $T_m : E(K)[m] \times E(K)/mE(K) \to K^*/(K^*)^m$. Further, $T_m(P, Q) = \tau_m(P, Q)$, the Tate pairing.

Proof. By Proposition 4 and the assumptions on the choice of S, any W in the equivalence class of $\mathcal{W}$ is non-vanishing at the four arguments in (9). To verify that T_m is independent of choice of representative of $\mathcal{W}$, suppose that W_1 and W_2 are in the equivalence class of $\mathcal{W}$. Then $W_2(\mathbf{v}) = \alpha\beta^{f(\mathbf{v})}W_1(\mathbf{v})$ for some $\alpha, \beta \in K^*$ and quadratic form f. Then

$$\begin{aligned}
&\frac{W_1(s + mp - q)W_1(s)W_2(s + mp)W_2(s - q)}{W_1(s + mp)W_1(s - q)W_2(s + mp - q)W_2(s)} \\
&= \beta^{f(s+mp)+f(s-q)-f(s+mp-q)-f(s)} \\
&= \beta^{f(mp+q)-f(mp)-f(q)} = \beta^{m[f(p+q)-f(p)-f(q)]} \in (K^*)^m \ .
\end{aligned}$$

Let $\Gamma \subset E_K(K)$ be the subgroup generated by S, P, and Q. Let

$$f_P = \frac{\Omega_{1,0,0}(-S, P, Q)}{\Omega_{1,m,0}(-S, P, Q)} \ .$$

Therefore, we may compute the divisor of f_P as a function of S (by equation (3)):

$$(f_P) = -([m]P) + (1 - m)(\mathcal{O}) + m(P) = m(P) - m(\mathcal{O}) \ .$$

Let D_Q be the divisor $(-S) - (-S - Q)$.

Then, using Proposition 2 and Theorem 3, in $K^*/(K^*)^m$,

$$\begin{aligned} f_P(D_Q) &= \frac{\Omega_{1,0,0}(S,P,Q)\Omega_{1,m,0}(S+Q,P,Q)}{\Omega_{1,m,0}(S,P,Q)\Omega_{1,0,0}(S+Q,P,Q)} \\ &= \frac{\Omega_{1,0,0}(S,P,Q)\Omega_{1,m,1}(S,P,Q)}{\Omega_{1,m,0}(S,P,Q)\Omega_{1,0,1}(S,P,Q)} \ . \end{aligned}$$

By a choice of $\phi : \mathbb{Z}^3 \to \Gamma$ such that $\phi(1,0,0) = S$, $\phi(0,1,0) = P$, and $\phi(0,0,1) = Q$, we have $W_\phi(\mathbf{v}) = \Omega_{\mathbf{v}}(S,P,Q) \in \mathcal{EN}(\mathbb{Z}^3, K)$. Therefore

$$\tau_m(P,Q) = f_P(D_Q) = \frac{V_\phi(s+mp+q)V_\phi(s)}{V_\phi(s+mp)V_\phi(s+q)} = T_m(P,Q) \ .$$

□

Corollary 1. *Let E be an elliptic curve defined over a finite field K, m a positive integer, $P \in E(K)[m]$ and $Q \in E(K)$. If W_P is the elliptic net associated to E, P, then we have*

$$\tau_m(P,P) = \frac{W_P(m+2)W_P(1)}{W_P(m+1)W_P(2)} \ . \tag{10}$$

Further, if $W_{P,Q}$ is the elliptic net associated to E, P, Q, then we have

$$\tau_m(P,Q) = \frac{W_{P,Q}(m+1,1)W_{P,Q}(1,0)}{W_{P,Q}(m+1,0)W_{P,Q}(1,1)} \ . \tag{11}$$

Proof. For the first formula, taking $q = p$ and $s = 2p$, we obtain

$$T_m(P,P) = \frac{W((m+2)p)W(p)}{W((m+1)p)W(2p)} \ .$$

For the second, take $s = p$, obtaining

$$T_m(P,Q) = \frac{W((m+1)p+q)W(p)}{W((m+1)p)W(p+q)} \ .$$

□

4 Tate Pairing Computation

4.1 Computing the Values of an Elliptic Net

Rachel Shipsey gives a double-and-add algorithm for computing terms of an elliptic divisibility sequence [14]. In the case of interest to us now, given the initial values of an elliptic divisibility sequence, the algorithm computes the n-th term of a sequence in $\log(n)$ time. Shipsey applied her more general algorithm (which allows beginning elsewhere in the sequence) to give a solution to the elliptic curve discrete logarithm problem in certain cases.

The algorithm described here is an adaptation and generalisation of Shipsey's algorithm to calculate terms $W(m, 0)$ and $W(m, 1)$ of an elliptic net. We define a *block centred on* k (shown in Fig. 2) to consist of a first vector of eight consecutive terms of the sequence $W(i, 0)$ centred on terms $W(k, 0)$ and $W(k + 1, 0)$ and a second vector of three consecutive terms $W(i, 1)$ centred on the term $W(k, 1)$. We define two functions:

1. **Double**(V)**:** Given a block V centred on k, returns the block centred on $2k$.
2. **DoubleAdd**(V)**:** Given a block V centred on k, returns the block centred on $2k + 1$.

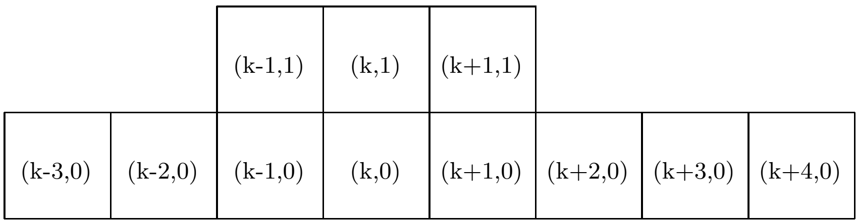

Fig. 2. A block centred on k

We assume the elliptic net satisfies $W(1, 0) = W(0, 1) = 1$. The first vectors of Double(V) and DoubleAdd(V) are calculated according to the following special cases of (5) (or (1)):

$$W(2i - 1, 0) = W(i + 1, 0)W(i - 1, 0)^3 - W(i - 2, 0)W(i, 0)^3 \ , \tag{12}$$

$$\begin{aligned} W(2i, 0) = (&W(i, 0)W(i + 2, 0)W(i - 1, 0)^2 \\ &- W(i, 0)W(i - 2, 0)W(i + 1, 0)^2)/W(2, 0) \ . \end{aligned} \tag{13}$$

The formulæ needed for the computations of the second vectors are instances of (5):[2]

$$\begin{aligned}
W(2k-1,1) &= (W(k+1,1)W(k-1,1)W(k-1,0)^2 \\
&\quad - W(k,0)W(k-2,0)W(k,1)^2)/W(1,1) \ , && (14) \\
W(2k,1) &= W(k-1,1)W(k+1,1)W(k,0)^2 \\
&\quad - W(k-1,0)W(k+1,0)W(k,1)^2 \ , && (15) \\
W(2k+1,1) &= (W(k-1,1)W(k+1,1)W(k+1,0)^2 \\
&\quad - W(k,0)W(k+2,0)W(k,1)^2)/W(-1,1) \ , && (16) \\
W(2k+2,1) &= (W(k+1,0)W(k+3,0)W(k,1)^2 \\
&\quad - W(k-1,1)W(k+1,1)W(k+2,0)^2)/W(2,-1) \ . && (17)
\end{aligned}$$

Equations (12) and (13), applied for $i = k-1, \ldots, k+3$, allow calculation of the first vectors of Double(V) and DoubleAdd(V) in terms of $W(2,0)$ and the terms of V. Equations (14)–(17) allow calculation of the second vectors in terms of $W(1,1)$, $W(-1,1)$, $W(2,-1)$ and the terms of V.

The algorithm to calculate $W(m,1)$ and $W(m,0)$ for any positive integer m is shown in Algorithm 1. The formula for the last term of the first vector of V in line 1 is from (1). Note that elliptic nets satisfy $W(-n,-m) = -W(n,m)$ by Proposition 3. In Sect. 5.1 we will consider possible optimisations.

Algorithm 1 Elliptic Net Algorithm

Input: Initial terms $a = W(2,0), b = W(3,0), c = W(4,0), d = W(2,1), e = W(-1,1), f = W(2,-1), g = W(1,1)$ of an elliptic net satisfying $W(1,0) = W(0,1) = 1$ and integer $m = (d_k d_{k-1} \ldots d_1)_2$ with $d_k = 1$

Output: Elliptic net elements $W(m,0)$ and $W(m,1)$

1: $V \leftarrow [[-a,-1,0,1,a,b,c,a^3c-b^3];[1,g,d]]$
2: **for** $i = k-1$ down to 1 **do**
3:     **if** $d_i = 0$ **then**
4:         $V \leftarrow$ Double(V)
5:     **else**
6:         $V \leftarrow$ DoubleAdd(V)
7:     **end if**
8: **end for**
9: **return** $V[0,3]$ and $V[1,1]$ // terms $W(m,0)$ and $W(m,1)$ respectively

[2] The values p,q,r,s substituted into (5) to obtain equations (14) - (17) are $[p,q,r,s] = [(k,0),(k-1,0),(1,0),(0,1)]$, $[(k+1,0),(k,0),(1,0),(-1,1)]$, $[(k+1,0),(k,0),(-1,0),(0,1)]$, and $[(k+2,0),(k,1),(1,0),(0,0)]$ respectively.

4.2 Computation of the Tate Pairing

We can now compute the Tate pairing via Corollary 1. Consider an elliptic curve E over a finite field $\mathbb{F}_q$ of characteristic not 2 or 3, in Weierstrass form

$$y^2 = x^3 + Ax + B$$

and points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on $E(\mathbb{F}_q)$ with $Q \neq \pm P$. We must calculate the values a, b, c, d, e, f, g required as input for the Elliptic Net Algorithm. These are terms of the elliptic net associated to E, P, Q. The necessary formulæ are given by the functions $\Psi_{m,n}$. In the case that $m = 0$, these are called *division polynomials* (see [16, p.105] and [17, p.477]). We have

$$W(1,0) = 1 \ , \tag{18}$$

$$W(2,0) = 2y_1 \ , \tag{19}$$

$$W(3,0) = 3x_1^4 + 6Ax_1^2 + 12Bx_1 - A^2 \ , \tag{20}$$

$$W(4,0) = 4y_1(x_1^6 + 5Ax_1^4 + 20Bx_1^3 - 5A^2x_1^2 - 4ABx_1 - 8B^2 - A^3) \ . \tag{21}$$

For the formulæ in case of characteristic 2 or 3, or the more general Weierstrass form, see [23, p.80]. Also using classical formulæ (see for example [24]), we have

$$W(0,1) = W(1,1) = 1 \ , \tag{22}$$

$$W(2,1) = 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \ , \tag{23}$$

$$W(-1,1) = x_1 - x_2 \ , \tag{24}$$

$$W(2,-1) = (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \ . \tag{25}$$

Suppose that P has order m. Then we use the Elliptic Net Algorithm, with input $m + 1$ and a, b, c, d, e, f, g given by (19)–(25).[3] The output is used to evaluate formula (11) of Corollary 1, giving the Tate pairing.

5 Analysis

5.1 Some Implementation Considerations

For an integer m and finite field $\mathbb{F}_q$, we define the *embedding degree* k to be the least integer such that $m|(q^k - 1)$, thus ensuring the m-th roots of unity are contained in $\mathbb{F}_{q^k}^*$. In cryptographic applications of the Tate pairing, it is usual to use a curve defined over $\mathbb{F}_q$ of embedding degree $k > 1$, and points $P \in E(\mathbb{F}_q)$, $Q \in E(\mathbb{F}_{q^k})$: throughout what follows we make this assumption.

First, note that no inversions are actually needed in equations (12)–(17), since the inverses of $W(2,0)$, $W(2,1)$, $W(-1,1)$ and $W(2,-1)$ may be precomputed

[3] In this case, $g = 1$. However, in Sect. 5.1 we will replace this elliptic net with an equivalent one for which $W(1,1) \neq 1$. For this reason, it is convenient to state Algorithm 1 in sufficient generality and include a variable g.

before the double-and-add loop is begun. Therefore these inversions are replaced by multiplications.

Now we consider optimisations in the functions Double and DoubleAdd. The largest savings can be gained by first computing a number of products which appear frequently in the formulæ:

$$\begin{aligned} W(i,0)^2 \text{ and } W(i-1,0)W(i+1,0) \quad \text{for } i = k-2, \ldots, k+3 \ , \\ W(k,1)^2 \text{ and } W(k-1,1)W(k+1,1) \ . \end{aligned}$$

With these 14 computations, each term of the 11 to be calculated requires only two multiplications and an addition (plus multiplications by $W(2,0)^{-1}$, $W(2,-1)^{-1}$, $W(1,1)^{-1}$ and $W(-1,1)^{-1}$). The resulting Double and DoubleAdd algorithms are shown in Algorithm 2.

Algorithm 2 Double and DoubleAdd

Input: Block V centred at k of an elliptic net satisfying $W(1,0) = W(0,1) = 1$, values $A = W(2,0)^{-1}, E = W(-1,1)^{-1}, F = W(2,-1)^{-1}, G = W(1,1)^{-1}$ and boolean *add*

Output: Block centred at $2k$ if $add == 0$ and centred at $2k+1$ if $add == 1$

$S \leftarrow [0,0,0,0,0,0]$
$P \leftarrow [0,0,0,0,0,0]$
$S_0 \leftarrow V[1,1]^2$
$P_0 \leftarrow V[1,0]V[1,2]$
for $i = 0$ to 5 **do**
    $S[i] \leftarrow V[0,i+1]^2$
    $P[i] \leftarrow V[0,i]V[0,i+2]$
end for
if $add == 0$ **then**
    for $i = 1$ to 4 **do**
        $V[0,2i-2] \leftarrow S[i]P[i+1] - S[i+1]P[i]$
        $V[0,2i-1] \leftarrow (S[i]P[i+2] - S[i+2]P[i])A$
    end for
    $V[1,0] \leftarrow (S_0P[3] - S[3]P_0)G$
    $V[1,1] \leftarrow S[3]P_0 - S_0P[3]$
    $V[1,2] \leftarrow (S[4]P_0 - S_0P[4])E$
else
    for $i = 1$ to 4 **do**
        $V[0,2i-2] \leftarrow (S[i]P[i+2] - S[i+2]P[i])A$
        $V[0,2i-1] \leftarrow S[i+1]P[i+2] - S[i+2]P[i+1]$
    end for
    $V[1,0] \leftarrow S[3]P_0 - S_0P[3]$
    $V[1,1] \leftarrow (S[4]P_0 - S_0P[4])E$
    $V[1,2] \leftarrow (S_0P[5] - S[5]P_0)F$
end if
return V

Finally, we may try to avoid some of these extra multiplications by $W(2,0)^{-1}$, $W(1,1)^{-1}$, $W(2,1)^{-1}$ and $W(2,-1)^{-1}$ entirely. Recall that by Theorem 6, applying an equivalence to the net will not alter the Tate pairing result. Let $\eta = W(-1,1)$. Apply the equivalence given by $\alpha = 1$, $\beta = \eta$ and $f(n,m) = mn$. Clearly, this preserves the conditions[4] that $W(1,0) = W(0,1) = 1$ (and leaves terms $W(n,0)$ unchanged, so they are still in $\mathbb{F}_q$), but changes $W(-1,1)$ to 1, which saves one multiplication in $\mathbb{F}_{q^k}$ per iteration. If $W(2,0)$ has a cube root ν in $\mathbb{F}_q$, then the equivalence $\alpha = \nu^{-1}, \beta = \nu$ and $f(n,m) = m^2 + n^2 + mn$ will change $W(2,0)$ to 1, while preserving $W(1,0) = W(0,1) = W(-1,1) = 1$, saving four $\mathbb{F}_q$ multiplications per iteration. Note that these equivalences may result in $W(1,1) \neq 1$.

Finally, we consider the applicability of some of the usual optimisations of Miller's algorithm. In Miller's algorithm, a final exponentiation is applied, in order to compute a unique value for the Tate pairing; the same exponentiation must be applied here. In the case of Miller's, this exponentiation eliminates multiplicative factors living in the base field $\mathbb{F}_q$. In our case, the $\mathbb{F}_q$ computations do not give rise to strictly multiplicative factors (the algorithm requires much addition and subtraction), and so we cannot use this final exponentiation as a justification for the saving of $\mathbb{F}_q$ computations. Windowing methods (as in [25] and [26]) may lead to improvement. A triple-and-add adaptation (as in [11] and [27]) does not seem promising, by the nature of the recurrence relation. However, efficiency improvements are likely to be found by studying the characteristic 2 and 3 cases.

5.2 Complexity

Since the algorithm involves a fixed number of precomputations, and a double-and-add loop with a fixed number of computations per step, the algorithm is linear time in the size of m, as is Miller's algorithm. Miller's algorithm also consists of a double-and-add loop, and we call the two internal steps Double and DoubleAdd, as for the Elliptic Net Algorithm. In Miller's algorithm the cost of DoubleAdd is almost twice that of Double. By contrast, in the Elliptic Net Algorithm these steps take the same time, so the complexity is independent of Hamming weight. This makes the choice of appropriate curves for cryptographical implementations somewhat easier [6], and may help discourage side channel attacks.

Denote squaring and multiplication in $\mathbb{F}_q$ by S and M. Denote squaring and multiplication in $\mathbb{F}_{q^k}$ by S_k and M_k. Assume that multiplying an element of $\mathbb{F}_q$ by one of $\mathbb{F}_{q^k}$ takes k multiplications in $\mathbb{F}_q$. Recall that E is defined over $\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$, and $Q \in E(\mathbb{F}_{q^k})$. Then any term $W(n,0)$, being a term in the elliptic divisibility sequence associated to E, P, has a value in $\mathbb{F}_q$. Under the optimisations discussed in Sect. 5.1, each Double or DoubleAdd step requires $6S + (6k+26)M + S_k + 2M_k$. Furthermore, under the condition that $2y_P \in \mathbb{F}_q$

[4] These were needed to derive formulæ (12)–(17).

is a cube, then precomputing its cube root will save four multiplications in $\mathbb{F}_q$ per step.

The Elliptic Net Algorithm requires no inversions. Miller's algorithm in affine coordinates requires one or two $\mathbb{F}_q$ inversion per step. In situations where inversions are costly (depending on implementation, they may cost anywhere from approximately 4 to 80 multiplications [28]), one may implement Miller's algorithm in homogeneous coordinates.

For the purpose of comparison, we consider an optimised implementation of Miller's algorithm in Jacobian coordinates analysed by Neal Koblitz and Alfred Menezes [29]. In their implementation, they assume $x(Q) \in E(\mathbb{F}_{q^{k/2}})$ (this is possible by using a twist of the curve, see for example [30]). Applying this additional assumption to the elliptic net algorithm, $W(1,1)$ will be an element of $\mathbb{F}_{q^{k/2}}$, reducing one of the multiplications in Double to one half the time. The comparison is summarised in Tables 1 and 2. In the latter, a squaring is assumed to be comparable to a multiplication (although it is more usually assumed to be 0.8 times as fast), and a multiplication in $\mathbb{F}_{q^k}$ is assumed to take $k^{1.5}$ multiplications in $\mathbb{F}_q$ (see [29]). The number of steps constitutes a range because the Double and DoubleAdd steps may differ in cost.

Table 1. Comparison of Operations for Double and DoubleAdd steps

Algorithm	Double	DoubleAdd
Optimised Miller's [29]	$4S + (k+7)M + S_k + M_k$	$7S + (2k+19)M + S_k + 2M_k$
Elliptic Net Algorithm	$6S + (6k+26)M + S_k + \frac{3}{2}M_k$	$6S + (6k+26)M + S_k + 2M_k$

Table 2. $\mathbb{F}_q$ Multiplications per Step

Embedding degree	2	4	6	8	10	12
Optimised Miller's	18-38	31-58	46-82	64-109	84-140	106-174
Elliptic Net	51-52	76-80	104-112	136-147	171-186	207-228

5.3 A Remark on Implementations

The elliptic net algorithm has been implemented by the author for PARI/GP (see [31]) and is available at [32]. It has also been implemented in C++ by Michael Scott and Augusto Jun Devegili for a pairing-friendly curve of degree 2. The implementation by Ben Lynn in the Pairing Based Cryptography Library

[33] is applicable to curves of various sizes and embedding degrees and includes a program to compare the Elliptic Net algorithm with Miller's. Preliminary data agree with the complexity analysis above.

6 Conclusions

The Elliptic Net Algorithm has no significant restrictions on the points, curves or finite fields to which it applies, and requires no inversions. The efficiency of the algorithm is comparable to Miller's algorithm. One expects that the Elliptic Net Algorithm will yield to further optimisation, possibly providing an efficient alternative to Miller's algorithm in many cases. The theory of elliptic nets here introduced may also yield other applications in the field of elliptic curve cryptography.

Acknowledgments. The author would like to thank Rafe Jones, Anna Lysyanskaya, Michelle Manes, Michael Scott, Joseph Silverman and Jonathan Wise for helpful discussions and editorial comments; and the anonymous referees for suggestions. This work was supported by NSERC Award PGS D2 331379-2006.

References

[1] Menezes, A.J., Okamoto, T., Vanstone, S.A.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inform. Theory **39**(5) (1993) 1639–1646
[2] Frey, G., Rück, H.G.: A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. Comp. **62**(206) (1994) 865–874
[3] Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: Symposium on Cryptography and Information Security, Okinawa, Japan (2000)
[4] Joux, A.: A one round protocol for tripartite Diffie-Hellman. In: Algorithmic number theory (Leiden, 2000). Volume 1838 of Lecture Notes in Comput. Sci. Springer, Berlin (2000) 385–393
[5] Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Advances in cryptology—CRYPTO 2001 (Santa Barbara, CA). Volume 2139 of Lecture Notes in Comput. Sci. Springer, Berlin (2001) 213–229
[6] Duquesne, S., Lange, T.: Pairing-based cryptography. In: Handbook of elliptic and hyperelliptic curve cryptography. Discrete Math. Appl. (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL (2006) 573–590
[7] Paterson, K.G.: Cryptography from pairings. In: Advances in elliptic curve cryptography. Volume 317 of London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge (2005) 215–251
[8] Barreto, P.S.L.M.: The pairing-based crypto lounge. (`http://planeta.terra.com.br/informatica/paulbarreto/pblounge.html`)
[9] Miller, V.: Short programs for functions on curves. (1986)
[10] Duquesne, S., Frey, G.: Implementation of pairings. In: Handbook of elliptic and hyperelliptic curve cryptography. Discrete Math. Appl. (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL (2006) 389–404

[11] Galbraith, S.D., Harrison, K., Soldera, D.: Implementing the Tate pairing. In: Algorithmic number theory (Sydney, 2002). Volume 2369 of Lecture Notes in Comput. Sci. Springer, Berlin (2002) 324–337
[12] Ward, M.: Memoir on elliptic divisibility sequences. Amer. J. Math. **70** (1948) 31–74
[13] Everest, G., Poorten, A.v.d., Shparlinski, I., Ward, T. In: Elliptic Divisibility Sequences. American Mathematical Society, Providence (2003) 163–175
[14] Shipsey, R.: Elliptic Divibility Sequences. PhD thesis, Goldsmiths, University of London (2001)
[15] Stange, K.E.: Elliptic Nets. PhD thesis, Brown University (in preparation)
[16] Silverman, J.H.: The arithmetic of elliptic curves. Volume 106 of Graduate Texts in Mathematics. Springer-Verlag, New York (1992) Corrected reprint of the 1986 original.
[17] Silverman, J.H.: Advanced topics in the arithmetic of elliptic curves. Volume 151 of Graduate Texts in Mathematics. Springer-Verlag, New York (1994)
[18] Swart, C.: Elliptic curves and related sequences. PhD thesis, Royal Holloway and Bedford New College, University of London (2003)
[19] van der Poorten, A.J.: Elliptic curves and continued fractions. J. Integer Seq. **8**(2) (2005) Article 05.2.5, 19 pp. (electronic)
[20] Propp, J.: Robbins forum. (`http://www.math.wisc.edu/~propp/about-robbins`)
[21] Duquesne, S., Frey, G.: Background on pairings. In: Handbook of elliptic and hyperelliptic curve cryptography. Discrete Math. Appl. (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL (2006) 115–124
[22] Galbraith, S.: Pairings. In: Advances in elliptic curve cryptography. Volume 317 of London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge (2005) 183–213
[23] Frey, G., Lange, T.: Background on curves and Jacobians. In: Handbook of elliptic and hyperelliptic curve cryptography. Discrete Math. Appl. (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL (2006) 45–85
[24] Chandrasekharan, K.: Elliptic functions. Volume 281 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin (1985)
[25] Blake, I.F., Seroussi, G., Smart, N.P.: Elliptic curves in cryptography. Volume 265 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge (2000) Reprint of the 1999 original.
[26] Hankerson, D., Hernandez, J.L., Menezes, A.: Software implementation of elliptic curve cryptography over binary fields. In: Proceedings of CHES 2000. Volume 1965 of Lecture Notes in Comput. Sci. Springer, Berlin (2000) 1–24
[27] Barreto, P.S.L.M., Kim, H.Y., Lynn, B., Scott, M.: Efficient algorithms for pairing-based cryptosystems. In: Advances in cryptology—CRYPTO 2002. Volume 2442 of Lecture Notes in Comput. Sci. Springer, Berlin (2002) 354–368
[28] Ciet, M., Joye, M., Lauter, K., Montgomery, P.L.: Trading inversions for multiplications in elliptic curve cryptography. Des. Codes Cryptogr. **39**(2) (2006) 189–206
[29] Koblitz, N., Menezes, A.: Pairing-based cryptography at high security levels. In: Cryptography and coding. Volume 3796 of Lecture Notes in Comput. Sci. Springer, Berlin (2005) 13–36
[30] Barreto, P.S.L.M., Lynn, B., Scott, M.: On the selection of pairing-friendly groups. In: Selected areas in cryptography. Volume 3006 of Lecture Notes in Comput. Sci. Springer, Berlin (2004) 17–25

[31] The PARI Group: Pari/gp development headquarters. (http://pari.math.u-bordeaux.fr/)
[32] Stange, K.E.: Pari/gp scripts for tate pairing via elliptic nets. (http://www.math.brown.edu/~stange/tatepairing/)
[33] Lynn, B.: Pairing-based cryptography library. (http://crypto.stanford.edu/pbc/)