ARITHMETIC OF SUPERSINGULAR KOBLITZ CURVES IN CHARACTERISTIC THREE

ROBERTO MARIA AVANZI, CLEMENS HEUBERGER, AND HELMUT PRODINGER

Abstract. We consider digital expansions of scalars for supersingular Koblitz curves in characteristic three. These are positional representations of integers to the base of τ, where τ is a zero of the characteristic polynomial $T^2 \pm 3\,T + 3$ of a Frobenius endomorphism. They are then applied to the improvement of scalar multiplication on the Koblitz curves.

A simple connection between τ-adic expansions and balanced ternary representations is given.

Windowed non-adjacent representations are considered whereby the digits are elements of minimal norm. We give an explicit description of the elements of the digit set, allowing for a very simple and efficient precomputation strategy, whereby the rotational symmetry of the digit set is also used to reduce the memory requirements. With respect to the current state of the art for computing scalar multiplications on supersingular Koblitz curves we achieve the following improvements: (i) speed-ups of up to 40%, (ii) a reduction of memory consumption by a factor of three, (iii) our methods apply to all window sizes without requiring operation sequences for the precomputation stage to be determined offline first.

Additionally, we explicitly describe the action of some endomorphisms on the Koblitz curve as a scalar multiplication by an explicitly given integer.

1. Introduction

Let m be a natural number coprime to 6, $\mu \in \{\pm 1\}$ and $\mathcal{E}_{3,\mu}$ be the elliptic curve

$$\mathcal{E}_{3,\mu} : Y^2 = X^3 - X - \mu \tag{1}$$

defined over $\mathbb{F}_3$. Koblitz [18] studied this curve for cryptographic applications, where one is interested in the group $\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$ of rational points over a field extension $\mathbb{F}_{3^m}$ of $\mathbb{F}_3$.

In this paper we study the question of computing scalar multiplications on this family of curves.

The motivation comes from pairing-based cryptography, as pairing-based protocols also call for the use of scalar multiplication, often in computationally restricted environments

This paper was in part written while R. Avanzi and C. Heuberger were visiting the Department of Mathematical Sciences, Stellenbosch University. R. Avanzi's research described in this paper has been partly supported by the European Commission through the IST Programme under Contract ICT-2007-216676 ECRYPT II.

C. Heuberger is supported by the Austrian Science Foundation FWF, project S9606, that is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory."

H. Prodinger is supported by the NRF grant 2053748 of the South African National Research Foundation and by the Center of Experimental Mathematics of the University of Stellenbosch.

(an important example being Direct Anonymous Attestation [9]). Indeed, the curves (1) are known to be supersingular with embedding degree 6. This makes them less secure than ordinary curves for purely discrete logarithm-based application, but it makes them attractive for pairing-based cryptography. Indeed, most of the current research about these curves is devoted to the optimization of the pairing operation: some recent references are [1, 7, 5, 6].

Now, whereas it used to be common to evaluate the performance of a pairing-based protocol by simply counting the number of required pairings, the recent algorithmic advancements in pairings imply that the performance of the two primitives is now similar. Therefore there is still need for more efficient, streamlined, and memory-saving scalar multiplication algorithms for the curves (1).

In this paper we provide a comprehensive answer to this question.

Our approach, following Koblitz, consists in using a τ-adic expansion of the scalar, where τ is a root of the characteristic polynomial of the Frobenius endomorphism of the curve, and then use a Horner scheme to perform the actual scalar multiplication. A similar approach is used for Koblitz curves in characteristic two as well [24, 25, 4].

The following is a summary of our results:

(i) We describe a method to immediately derive some τ-adic expansions from balanced ternary representations (Theorem 1 on page 6).

(ii) A compact and explicit representation of digit sets formed by elements of minimal norm is given in Theorem 2 on page 8. This guarantees that windowed expansions terminate and at the same time yields a very simple precomputation strategy for the scalar multiplication (Remark 4.4 on page 9). Our precomputation strategy is general in the sense that it works for all window sizes, whereas the previous methods require ad-hoc operation sequences for each window size to be determined offline.
This is also a stark difference with respect to the case of Koblitz curves in characteristic two, where no explicit description of a minimal norm digit set is currently available.

(iii) We reduce the memory requirements by a factor three with respect to all the previously published techniques based on windowed τ-adic expansions. This follows from the rotational symmetry of the minimal norm digit sets that we build (Remark 4.2 on page 7) and Algorithm 3 on page 8 shows how to use this fact.

(iv) The computational cost of scalar multiplication for some cryptographically relevant parameters is analyzed in Section 5. Performance gains between 12 % and 40 % with respect to previously known scalar multiplication algorithms for the same types of curves are common (see Remarks 5.2, 5.3 and 5.4).

(v) In Theorem 3 on page 18 (Section 6) we provide explicit expressions for the eigenvalues of the Frobenius operation and of an endomorphism of $\mathcal{E}_{3,\mu}$ corresponding to a sixth root of unity in $\mathbb{Z}[\tau]$. In particular we give values of the scalar t such that $\tau(P) = t \cdot P$ for a point in a large prime order subgroup on $\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$.

Acknowledgements. We thank Christiaan van de Woestijne for his comments which led to Remark 3.3.

2. Background

We collect some known facts on the curves that are the object of our investigation. From [18] we know that the cardinality N_m of $\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$ is given by

$$N_m := |\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})| = 3^m + \mu \cdot \left(\frac{m}{3}\right) (-3)^{\frac{m+1}{2}} + 1$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol. (Koblitz used a Jacobi symbol instead and obtained the slightly more complex expression $N_m := |\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})| = 3^m - \mu \cdot \left(\frac{3}{m}\right) 3^{\frac{m+1}{2}} + 1$.) In particular it is

$$\left(\frac{m}{3}\right) = \begin{cases} 1 \ , & \text{if } m \equiv \ \ 1 \pmod 3 \ , \\ -1 \ , & \text{if } m \equiv -1 \pmod 3 \ . \end{cases}$$

The Frobenius endomorphism

$$\tau \ : \ \mathcal{E}_{3,\mu}(\mathbb{F}_{3^m}) \to \mathcal{E}_{3,\mu}(\mathbb{F}_{3^m}) \ , \quad (x, y) \mapsto (x^3, y^3)$$

can be evaluated very efficiently because cubing is a linear operation in $\mathbb{F}_{3^m}$ and thus its evaluation takes only a fraction of the time required for a field multiplication (cf. for instance [11, 1]). Furthermore, it satisfies the relation

$$\tau^2 - 3\,\mu\,\tau + 3 = 0 \ . \tag{2}$$

It is an easy consequence of (2) that $\tau^6 = -3^3$. Indeed, τ may be identified with the imaginary quadratic number

$$\frac{3\mu + \sqrt{-3}}{2} = \sqrt{-3} \cdot \frac{1 - \mu\sqrt{-3}}{2} \ , \tag{3}$$

which we will also call τ. This identification induces a ring isomorphism between $\mathbb{Z}[\tau]$ and the endomorphism ring of $\mathcal{E}_{3,\mu}$. Hence, if an integer n can be written in the form $\sum_{i=0}^{\ell} d_i \tau^i$, the scalar multiple $n \cdot P$ can be computed by evaluating $\sum_{i=0}^{\ell} d_i \tau^i(P)$ via a Horner scheme.

Let

$$\zeta := \frac{1 - \mu\sqrt{-3}}{2} \ , \tag{4}$$

such that $\zeta \in \mathbb{Z}[\tau]$ is a primitive sixth root of unity and

$$\tau = \sqrt{-3}\,\zeta \ . \tag{5}$$

The set $\{\zeta^k : 0 \leqslant k < 6\}$ of sixth roots of unity is denoted by $\mathcal{U}_6$. Note that multiplication by ζ corresponds to a rotation of the complex plane by $\pi/3$ that leaves $\mathbb{Z}[\tau]$ globally invariant.

The ring $\mathbb{Z}[\tau]$ is factorial with τ prime. The complex conjugate of τ will be denoted by $\bar{\tau}$. We list a few useful relations between τ, $\bar{\tau}$ and ζ:

$$\tau = 2\,\mu - \mu\zeta \ , \tag{6}$$

$$\bar{\tau} = 3\,\mu - \tau = \tau\zeta \ , \tag{7}$$

$$\tau\bar{\tau} = \tau^2\zeta = 3 \ , \tag{8}$$

where (5) and (6) are easy consequences of (3) and (4), whereas (7) and (8) follow from the minimal polynomial (2).

These complex numbers correspond to functions in the endomorphism ring of $\mathcal{E}_{3,\mu}$, that act on the curve as follows

$$\zeta \,:\, (x,y) \mapsto (x+\mu, -y) \ ,$$
$$\bar{\tau} \,:\, (x,y) \mapsto (x^3+\mu, -y^3) \ .$$

These operations, as well as tripling

$$3 \,:\, (x,y) \mapsto (x^9+\mu, -y^9)$$

can thus be computed efficiently.

3. Digit Sets

We shall denote by $\mathbf{N}(\,)$ the norm from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}$. This function is equal to to the square of the absolute value of its argument and on $\mathbb{Z}[\tau]$ it takes integer values.

Definition 3.1. Let $\mathcal{D}$ be a finite subset of $\mathbb{Z}[\tau]$ and w a positive integer. A word $\eta_{\ell-1}\dots\eta_0 \in \mathcal{D}^*$ is called a $\mathcal{D}$-w-NAF of a $z \in \mathbb{Z}[\tau]$, if

(1) $\mathsf{value}(\eta_{\ell-1}\dots\eta_0) := \sum_{j=0}^{\ell-1} \eta_j \tau^j = z$,
(2) Each factor $\eta_{j+w-1}\dots\eta_j$, i.e., each block of length w, contains at most one non-zero.

A $\mathcal{D}$-2-NAF is also simply called a $\mathcal{D}$-NAF.

We call $\mathcal{D}$ a w-Non-Adjacent-Digit-Set (w-NADS), if every integer $z \in \mathbb{Z}[\tau]$ admits a $\mathcal{D}$-w-NAF.

Definition 3.2. A *reduced residue system* modulo τ^w is a set containing exactly one representative for each residue class of $\mathbb{Z}[\tau]$ modulo τ^w that is not divisible by τ.

Now, suppose that the digit set $\mathcal{D}$ consists of the zero and a reduced residue system modulo τ^w. Since τ is a prime element of $\mathbb{Z}[\tau]$, each $z \in \mathbb{Z}[\tau]$ is either divisible by τ or congruent modulo τ^w to exactly one element d of the digit set $\mathcal{D}$. From this it is easy to conclude that if $\mathcal{D}$ contains the zero and $\mathcal{D} \setminus \{0\}$ is a reduced residue system, then the $\mathcal{D}$-w-NAF of an integer, if it exists, is uniquely determined. Furthermore, a simple algorithm to compute it is given by Algorithm 1 (for some details, such as the implementation of the division by τ, see [8]).

Just using a digit set which consists of 0 and a reduced residue system does not imply that Algorithm 1 terminates. This has been observed in the binary case for NAF-like expansions of rational integers to the base of 2 by Muir and Stinson [21] and for τ-adic

Algorithm 1. General windowed integer recoding

INPUT: An element z from $\mathbb{Z}[\tau]$, an integer $w \geqslant 1$ and a reduced residue system $\mathcal{D}'$ modulo τ^w.
OUTPUT: A $\mathcal{D}$-w-NAF $\varepsilon_{\ell-1}\varepsilon_{\ell-1}\ldots\varepsilon_0$ of the integer z, if it exists. Otherwise, the algorithm does not terminate.

1. $j \leftarrow 0, u \leftarrow z$
2. **while** $u \neq 0$ **do**
3. **if** $\tau \mid u$ **then**
4. $\varepsilon_j \leftarrow 0$ [Output 0]
5. **else**
6. Let $\varepsilon_j \in \mathcal{D}'$ s.t. $\varepsilon_j \equiv z \pmod{\tau^w}$ [Output ε_j]
7. $u \leftarrow u - \varepsilon_j$
8. $u \leftarrow u/\tau$
9. $j \leftarrow j + 1$
10. $\ell \leftarrow j$
11. **return** $\varepsilon_{\ell-1}\varepsilon_{\ell-1}\ldots\varepsilon_0$

expansions for Koblitz curves in characteristic 2 by [4]. As pointed out by Blake, Kumar Murty and Xu [8], the set $\{0, 1, -1\}$ is not even a 1-NADS: Indeed, we have

$$\zeta(\tau^2 - 1) = \mu\tau + 1 \ ,$$

which implies that ζ does not admit a $\{0, 1, -1\}$-1-NAF, cf. the characterization of digit sets by Matula [20].

Remark 3.3 (due to Christiaan van de Woestijne). For $\mu = -1$, $\{0, 1, 2\}$ is a 1-NADS, as τ is a basis of a canonical number system in the sense of Kátai and Szabó [15], cf. the characterisation of quadratic integers which are bases of canonical number systems by Kátai and Kovács [14] and by Gilbert [10].

For $\mu = 1$, τ is not a basis of a canonical number system. Even worse, there exists no 1-NADS of the "right" cardinality, i.e., containing one representative for every residue class modulo τ: To see this, we use an argument used by Kátai and Kovács [14]: The crucial observation is that $\mathbf{N}(1 - \tau) = 1$. Assume that $\mathcal{D}$ is a 1-NADS. For some $d \in \mathcal{D} \setminus \{0\}$, we consider the $\mathcal{D}$-1-NAF $\eta_{\ell-1}\ldots\eta_0$ of $d(1 - \bar{\tau})$. Multiplying by $(1 - \tau)$ yields

$$d = d(1-\tau)(1-\bar{\tau}) = \sum_{j=0}^{\ell-1} \eta_j \tau^j (1-\tau) = \eta_0 + \sum_{j=1}^{\ell-1} (\eta_j - \eta_{j-1})\tau^j - \eta_{\ell-1}\tau^\ell.$$

Considering this equation modulo τ^k for $k = 1, \ldots, \ell$, we obtain $\eta_0 = d$, $\eta_1 = \eta_0 = d, \ldots,$ $\eta_{\ell-1} = d$. This results in

$$0 = -d\tau^\ell,$$

a contradiction.

However, allowing the non-integer digits $\mathcal{D} = \{-1/2, 1/2, 3/2\}$, every element of $\mathbb{Z}[\tau]$ can be represented by a $\mathcal{D}$-1-NAF whose length is divisible by 3. All these $\mathcal{D}$-1-NAFs of length divisible by 3 indeed have a value in $\mathbb{Z}[\tau]$.

On the other hand, Koblitz [18] proved the following result. We set $\mathcal{D}_2 = \mathcal{U}_6 \cup \{0\}$, which can also be seen as the set of all integers in $\mathbb{Z}[\tau]$ of norm at most 1.

Theorem (Koblitz [18])**.** *$\mathcal{D}_2$ is a 2-NADS, i.e., every element in $\mathbb{Z}[\tau]$ admits a $\mathcal{D}_2$-NAF.*

Our first result concerns a connection between balanced ternary expansion and $\mathcal{D}_2$-NAFs of rational integers.

About balanced ternary integer representations, Knuth [17, § 4.1] wrote: *Perhaps the prettiest number system of all is the balanced ternary notation, which consists of radix-3 representation using -1, 0, and $+1$ as "trits" (ternary digits) instead of 0, 1, and 2.*

It turns out that a $\mathcal{D}_2$-NAF of an integer can be constructed directly from its balanced ternary expansion, it is not necessary to use any complex computations.

Theorem 1. *Let n be a rational integer given by its balanced ternary expansion $n = \sum_{j=0}^{\ell-1} x_j 3^j$ for $x_j \in \{0, 1, -1\}$. Then the $\mathcal{D}_2$-NAF of n is given by $\eta_{2\ell-2} \dots \eta_0$, where*

$$\eta_j = \begin{cases} 0 \ , & \text{if } j \text{ is odd} \ , \\ x_{j/2}\zeta^{(j/2) \bmod 6} \ , & \text{if } j \text{ is even} \ . \end{cases} \tag{9}$$

Proof. By (8), we have $n = \sum_{j=0}^{\ell-1} (x_j \zeta^j) \tau^{2j}$. Since $\zeta^6 = 1$, we simply obtain (9). □

We refer to Knuth's book for many further properties of the balanced ternary number system and references.

Once we know the τ-adic $\mathcal{D}_2$-NAF of a scalar n, we can perform the corresponding scalar multiplication on a curve $\mathcal{E}_{2,\mu}$ by means of Algorithm 2.

The following lemma characterizes divisibility by τ, cf. for instance Blake, Kumar Murty and Xu [8].

Lemma 3.4. *Let $\alpha \in \mathbb{Z}[\tau]$ be written as $\alpha = a + b\tau$ for some rational integers a and b. Then α is divisible by τ if and only if 3 divides a.*

4. Minimal Norm Representatives and Scalar Multiplication

In what follows $w \geqslant 2$ is an integer.

Definition 4.1. Let $\alpha \in \mathbb{Z}[\tau]$ be not divisible by τ and assume that

$$\mathbf{N}(\alpha) \leqslant \mathbf{N}(\beta) \text{ for all } \beta \in \mathbb{Z}[\tau] \text{ with } \beta \equiv \alpha \pmod{\tau^w}. \tag{10}$$

Then α is called a *representative of minimum norm of its residue class.*

In analogy to Solinas [24, 25], Blake, Kumar Murty and Xu [8] propose to choose one representative of minimal norm from each residue class modulo τ^w which is not divisible by τ. They show that such representatives (together with 0) form a w-NADS, which we denote by $\mathcal{D}_w$. The purpose of this section is to better understand this digit set and give explicit formulæ.

Algorithm 2. Scalar Multiplication on Koblitz curves in characteristic 3 using the $\mathcal{D}_2$-NAF

INPUT: A point $P \in \mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$ and an integer $n = \sum_{i=0}^{\ell} \eta_i \tau^i$ where $\eta_i = 0$ or $\eta_i = \zeta^{j(i)}, 0 \leqslant j(i) < 6$
OUTPUT: The point $Q = n \cdot P = \sum_{i=0}^{\ell} \eta_i \tau^i P$

1. $Q \leftarrow 0 \in \mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$
2. **for** $i = \ell$ **downto** 0 **do**
3. $\quad Q \leftarrow \tau\, Q$
4. $\quad$ **if** $\eta_i \neq 0$ **then**
$\quad\quad$ Write $\eta_i = \zeta^{j(i)}, 0 \leqslant j(i) < 6$
5. $\quad\quad$ **let** $(x, y) \leftarrow P$
6. $\quad\quad$ **switch** $j(i)$
7. $\quad\quad\quad$ **case** 0: $Q \leftarrow Q + (x, y)$
8. $\quad\quad\quad$ **case** 1: $Q \leftarrow Q + (x + \mu, -y)$
9. $\quad\quad\quad$ **case** 2: $Q \leftarrow Q + (x - \mu, y)$
10. $\quad\quad\quad$ **case** 3: $Q \leftarrow Q + (x, -y)$
11. $\quad\quad\quad$ **case** 4: $Q \leftarrow Q + (x + \mu, y)$
12. $\quad\quad\quad$ **case** 5: $Q \leftarrow Q + (x - \mu, -y)$
13. **return** Q

Remark 4.2. An important observation is that *any reduced residue system modulo τ^w and thus also the corresponding digit set $\mathcal{D}$ can be constructed to be invariant under multiplication by ζ.*

To prove this, we first observe that for each $d \neq 0$ with $\tau \nmid d$, the elements $\zeta^\ell d$ with $0 \leqslant \ell \leqslant 5$, are pairwise *not* congruent to each other modulo τ^w. In fact, suppose that $\ell < \ell'$ and τ^w divides $d^\ell - d^{\ell'} = d\big(1 - \zeta^{\ell'-\ell}\big)\zeta^\ell$. Since the norm of $1 - \zeta^{\ell'-\ell}$ is at most 4 it follows that τ can divide $1 - \zeta^{\ell'-\ell}$ at most once, and since $w \geqslant 2$, we must have $\tau \mid d$, a contradiction.

Now, when an element d is chosen to represent its residue class, it suffices to include the elements $\zeta^\ell d$ for $1 \leqslant \ell \leqslant 5$ in the reduced residue system to represent their respective residue classes.

Remark 4.3. As a consequence of the previous remark, if there were a unique representative of minimal norm in each residue class modulo τ^w, like in the characteristic two case, we would have that the digit set $\mathcal{D}_w$ formed by taking the zero and a reduced residue system of minimal norm representatives has a rotational symmetry. In fact, all the $\zeta^\ell d$ have the same norm, hence one of these element has minimal norm in its class if and only if all of them satisfy the same property.

It turns out that in some cases there are two elements of minimal norm in a residue class modulo τ^w coprime to τ, hence one must decide which orbits of minimal norm elements under the action of $\langle\zeta\rangle$ to include in the digit set.

Algorithm 3. Scalar Multiplication on Koblitz curves in characteristic 3 with a sixpartite digit set

INPUT: A point $P \in \mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$ and an integer $n = \sum_{i=0}^{\ell} \eta_i \tau^i$ where $\eta_i = \zeta^{j(i)} d_i, 0 \leqslant j(i) < 6$, and $d_i \in \mathcal{D}_{w,0}$
OUTPUT: The point $Q = n \cdot P = \sum_{i=0}^{\ell} \eta_i \tau^i P$

1. **for all** $d_i \in \mathcal{D}_{w,0}$
2. Precompute $d_i \cdot P$ [store in a table]
3. $Q \leftarrow 0 \in \mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$
4. **for** $i = \ell$ **downto** 0 **do**
5. $Q \leftarrow \tau\, Q$
6. **if** $\eta_i \neq 0$ **then**
7. **let** $(x, y) \leftarrow d_i \cdot P$ [Retrieve from precomputed table]
8. **switch** $j(i)$
9. **case** 0: $Q \leftarrow Q + (x, y)$
10. **case** 1: $Q \leftarrow Q + (x + \mu, -y)$
11. **case** 2: $Q \leftarrow Q + (x - \mu, y)$
12. **case** 3: $Q \leftarrow Q + (x, -y)$
13. **case** 4: $Q \leftarrow Q + (x + \mu, y)$
14. **case** 5: $Q \leftarrow Q + (x - \mu, -y)$
15. **return** Q

The following theorem gives an explicit description of such a digit set with rotational symmetry in all cases. Its proof explains when in a given residue class modulo τ^w the minimum with respect to the norm may not be unique.

Theorem 2. *Let $w \geqslant 2$ and set*

(11)
$$\mathcal{D}_{w,0} = \left\{ a + b\mu\tau : a \in \mathbb{Z}, b \in \mathbb{Z}, 3 \nmid a, 1 \leqslant a \leqslant 3^{w/2} - 2 \text{ and } -\frac{a}{3} < b < 3^{w/2-1} - \frac{2a}{3} \right\}$$

if w is even and

(12)
$$\mathcal{D}_{w,0} = \left\{ a + b\mu\tau : a \in \mathbb{Z}, b \in \mathbb{Z}, 3 \nmid a, -3^{\lfloor \frac{w}{2} \rfloor} + 2 \leqslant b \leqslant 0, 1 - 2b \leqslant a \leqslant 3^{\lfloor \frac{w}{2} \rfloor} - b - 1 \right\} \cup \left\{ (3^{\lfloor \frac{w}{2} \rfloor} - b) + b\mu\tau : b \in \mathbb{Z}, 3 \nmid b, -\frac{3^{\lfloor \frac{w}{2} \rfloor} - 1}{2} \leqslant b \leqslant 0 \right\}$$

if w is odd. Set

$$\mathcal{D}_w := \{0\} \cup \bigcup_{0 \leqslant k < 6} \zeta^k \mathcal{D}_{w,0} \ .$$

Then $\mathcal{D}_w$ consists of 0 and exactly one representative of minimum norm of every residue class modulo τ^w. In particular, $\mathcal{D}_w$ is a w-NADS.

Before giving a proof of Theorem 2, we briefly discuss its practical implications.

Remark 4.4. The explicit constructions (11) and (12) make it easy to give an efficient precomputation strategy for a scalar multiplication algorithm. Such an algorithm would be similar to Algorithm 2 but would be based on a $\mathcal{D}$-w-NAF of the scalar. Hence, the first step would be to precompute dP for $d \in \mathcal{D}_w$. In fact, it is only necessary to precompute dP for $d \in \mathcal{D}_{w,0}$, as all other dP for $d \in \mathcal{D}_w$ follow from this by multiplication by ζ – similarly to Steps 5 to 12 of Algorithm 2. The result is Algorithm 3.

The remaining question is how to compute $\mathcal{D}_{w,0}$ in general. First, we observe that 1, 2, and $4 - \mu\tau$ are in $\mathcal{D}_{w,0}$ for all $w \geqslant 3$.

It is easy to observe that all elements of $\mathcal{D}_{w,0}$, $w \geqslant 4$ can be reached from 1 by repeatedly adding 1 or 2 or $\pm\tau$. It is trivial to see this in the case of even w, but still easy in the case of odd w, where we must consider the two sets in (12) separately. Hence, let $w \geqslant 5$ be odd. Consider the first set: for any two consecutive values of b with $-3^{\lfloor \frac{w}{2} \rfloor} + 2 \leqslant b \leqslant 0$ the a-ranges, i.e. the intervals $1 - 2b \leqslant a \leqslant 3^{\lfloor \frac{w}{2} \rfloor} - b - 1$ overlap, even if we remove the values of a that are multiples of 3. The elements of the second set just add another element at the "end" of the a-range for about a half of the values of b already considered. The only exception to this latter fact takes place for $w = 3$, where the set consists just of the element $4 - \mu\tau$ (for $b = -1$) whereas the first set contains 1 and 2 (corresponding to the a-range for $b = 0$) – but we are considering $w \geqslant 5$ here.

Hence one doubling and one application of τ are needed, and then $3^{w-2} - 2$ group additions.

Proof of Theorem 2. We set

$$V = \{z \in \mathbb{C} : |z| \leqslant |z - u| \text{ for all } u \in \mathbb{Z}[\tau]\} \ ,$$

i.e., V is the Voronoi cell for 0 corresponding to the set $\mathbb{Z}[\tau]$. The set V is shown in Figure 1 on the following page. It is a hexagon with vertices v_k, $k \in \{0, \ldots, 5\}$, where $v_0 = \frac{\sqrt{-3}}{3}$ and $v_k = v_0 \zeta^{-\mu k} = v_0 e^{k\pi i/3}$. This latter fact mirrors the fact that $\mathbb{Z}[\tau]$ is invariant under multiplication by ζ (i.e., invariant under rotation by $\pi/3$), thus V also has to be invariant under multiplication by ζ. We have $|v_k| = 1/\sqrt{3}$, which implies that $|z| \leqslant 1/\sqrt{3}$ for all $z \in V$.

Consider now an $\alpha \in \mathbb{Z}[\tau]$ which is not divisible by τ. Condition (10) can be rewritten as

$$\left|\frac{\alpha}{\tau^w}\right| \leqslant \left|\frac{\alpha}{\tau^w} - u\right| \text{ for all } u \in \mathbb{Z}[\tau] \ ,$$

which is equivalent to

$$\frac{\alpha}{\tau^w} \in V \ .$$

Thus α is a minimum norm representative if and only if $\alpha/\tau^w \in V$. It is the unique minimum norm representative of its residue class if and only if α/τ^w is in the interior of the region V.

Assume that α/τ^w equals one of the vertices of V. This means that $\alpha/\tau^w = \zeta^k v_0$ for an appropriate k. This is equivalent to

$$\alpha = \tau^{w-1}\zeta^k v_0 \tau = -\tau^{w-1}\zeta^{k+1}$$

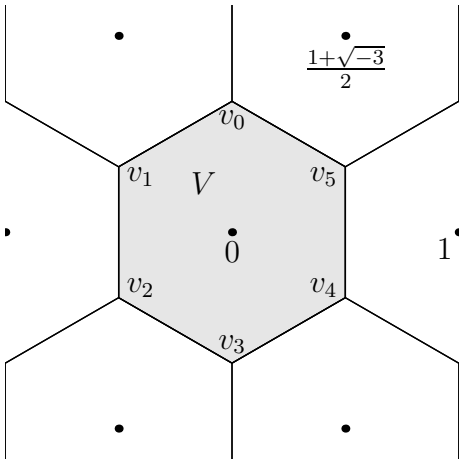

FIGURE 1. Voronoi cell V for 0 corresponding to the set $\mathbb{Z}[\tau]$

by (5). As we assume that $w \geqslant 2$, α is divisible by τ, contradiction.

Assume now that α/τ^w is on that part of the boundary of V which lies on the perpendicular bisector of the line segment from 0 to ζ^k for some k. After a rotation induced by multiplication by ζ^{-k}, we may assume without loss of generality that α/τ^w lies on the perpendicular bisector of the line segment from 0 to 1, i.e., $|\alpha/\tau^w| = |\alpha/\tau^w - 1|$ and $\operatorname{Re}(\alpha/\tau^w) = 1/2$ and $\alpha/\tau^w = 1/2 + iy$ for an appropriate $y \in \mathbb{R}$. We note that it cannot happen that $\alpha/\tau^w = 1/2$, because this would imply that $N(\alpha) = 3^w/4$, which is impossible. The other representative of minimum norm of the residue class of α is $\beta := \alpha - \tau^w$. We consider β/τ^w, which is given by $\beta/\tau^w = -1/2 + iy$.

We denote the midpoint of the line segment v_k, v_{k+1} by $v_{k+1/2}$ and adopt the convention that the indices of the points v_k are always meant modulo 6. We conclude that if there are two distinct representatives α and β of minimum norm of the same residue class modulo τ^w, then one of the "normalized points" α/τ^w and β/τ^w lies on the line segment v_k, $v_{k+1/2}$, i.e., the first half of v_k, v_{k+1}, for an appropriate integer k, whereas the other normalized point lies on the segment $v_{k+3+1/2}$, v_{k+4}, i.e., the second half of v_{k+3}, v_{k+4}.

To enforce uniqueness, we can therefore pass to a slightly smaller set $\widetilde{V}$, which consists of the interior of V and the line segments $v_{k+1/2}$ (excluded), v_{k+1} (included) for all integers k, as shown in Figure 2 on the next page (in the case $\mu = 1$, in the case $\mu = -1$ we take the complex conjugate in order to get results which can be written down without case distinction). We may now define

$$\mathcal{D}_w := \{0\} \cup \{\alpha \in \mathbb{Z}[\tau] : \alpha/\tau^w \in \widetilde{V} \text{ and } \tau \nmid \alpha\} \ .$$

Then $\mathcal{D}_w$ consists of 0 and exactly one minimum norm representative from every residue class modulo τ^w not divisible by τ.

The set $\widetilde{V}$ has been chosen in such a way that it is still invariant under rotation by $\pi/3$, i.e., multiplication by ζ. Therefore, the set $\mathcal{D}_w$ is also invariant under multiplication by ζ. We only need to construct one representative of every orbit under this action. This means

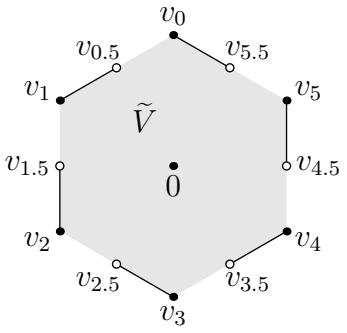

FIGURE 2. Restricted Cell $\widetilde{V}$ for $\mu = 1$

that we may restrict ourselves to the set $\widetilde{V}_0$ defined to be the interior of the triangle 0, v_4, v_5 plus the line segment $v_{4.5}$ (excluded), v_5 (included), 0 (excluded), cf. Figure 3 (again for $\mu = 1$, in the other case, we take the complex conjugate).

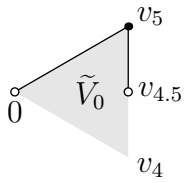

FIGURE 3. Representatives modulo rotation $\widetilde{V}_0$ for $\mu = 1$

We set $\widetilde{V}_k := \zeta^k \widetilde{V}_0$, where the indices are again meant modulo 6, thus $\widetilde{V} \setminus \{0\}$ is the disjoint union of the sets $\widetilde{V}_k$, $k \in \{0, \ldots, 5\}$. Similarly, we partition the set $\mathcal{D}_w$ into the six sets

$$\mathcal{D}_{w,k} := \left\{ \alpha \in \mathcal{D}_w : \frac{\alpha}{\tau^w} \in \widetilde{V}_{k+\lfloor w/2 \rfloor + [w \text{ is odd}]\frac{3\mu-1}{2}} \right\} \quad , \qquad k \in \{0, \ldots, 5\} \ .$$

Here, we use Iverson's notation [ ] for conditional expressions (1 if true, 0 if false). We required the quotient to be in $\widetilde{V}_{k+\lfloor w/2 \rfloor + [w \text{ is odd}]\frac{3\mu-1}{2}}$ instead of the more natural choice $\widetilde{V}_k$ in order to get $1 \in \mathcal{D}_{w,0}$ in the end. By construction, the sets $\mathcal{D}_{w,k}$ can be written as $\mathcal{D}_{w,k} = \zeta^k \mathcal{D}_{w,0}$, i.e., they are rotations of the set $\mathcal{D}_{w,0}$.

Now, we head for an explicit description of $\mathcal{D}_{w,0}$. Using (5), $\zeta^3 = -1$ and the definition of $\widetilde{V}_j$ gives

$$\begin{aligned}
\mathcal{D}_{w,0} &= \{\alpha \in \mathbb{Z}[\tau] \cap \tau^w \widetilde{V}_{\lfloor w/2 \rfloor + [w \text{ is odd}]\frac{3\mu-1}{2}} : \tau \nmid \alpha\} \\
&= \{\alpha \in \mathbb{Z}[\tau] \cap i^{[w \text{ is odd}]} 3^{w/2} \zeta^{w-3\lfloor w/2 \rfloor} \widetilde{V}_{\lfloor w/2 \rfloor + [w \text{ is odd}]\frac{3\mu-1}{2}} : \tau \nmid \alpha\} \\
&= \begin{cases} \{\alpha \in \mathbb{Z}[\tau] \cap 3^{w/2} \widetilde{V}_0 : \tau \nmid \alpha\} \ , & \text{if } w \text{ is even} \ , \\ \{\alpha \in \mathbb{Z}[\tau] \cap \mu i 3^{w/2} \zeta^2 \widetilde{V}_0 : \tau \nmid \alpha\} \ , & \text{if } w \text{ is odd} \ . \end{cases}
\end{aligned}$$

The set $3^{w/2}\widetilde{V}_0$ can be described as

$$3^{w/2}\widetilde{V}_0 = \left\{x+\sqrt{-3}y : 0 < x < \frac{3^{w/2}}{2} \text{ and } -\frac{x}{3} < \mu y \leqslant \frac{x}{3}\right\} \cup \\ \cup \left\{\frac{3^{w/2}}{2} + \sqrt{-3}y : 0 < \mu y \leqslant \frac{3^{w/2-1}}{2}\right\} \ .$$

We first consider the case of even w. Writing $\alpha = a + b\mu\tau$ for rational integers a and b yields

$$\mathcal{D}_{w,0} = \left\{a + b\mu\tau : a \in \mathbb{Z}, b \in \mathbb{Z}, 3 \nmid a, 0 < a \text{ and } -\frac{a}{3} < b < 3^{w/2-1} - \frac{2a}{3}\right\} \ . \tag{13}$$

We note that the equality case $\mathrm{Re}(a + b\mu\tau) = 3^{w/2}/2$ cannot occur, because $3 \nmid a$, which simplifies the formulæ in this case.

To see which values of a actually admit valid values of b, we reformulate the condition on b in (13) as

$$\left\lfloor -\frac{a}{3} \right\rfloor + 1 \leqslant b \leqslant 3^{w/2-1} + \left\lceil -\frac{2a}{3} \right\rceil - 1 \ .$$

Such b exist if and only if the upper bound is greater to or equal than the lower bound, which yields

$$-\left\lceil \frac{a}{3} \right\rceil + \left\lfloor \frac{2a}{3} \right\rfloor \leqslant 3^{w/2-1} - 2 \ .$$

If $a \equiv 1 \pmod 3$, we have $\lceil a/3 \rceil = (a+2)/3$ and $\lfloor 2a/3 \rfloor = (2a-2)/3$ and we obtain

$$-(a+2) + (2a-2) \leqslant 3^{w/2} - 6 \ ,$$

which is equivalent to $a \leqslant 3^{w/2} - 2$. If $a \equiv 2 \pmod 3$, we have $\lceil a/3 \rceil = (a+1)/2$ and $\lfloor 2a/3 \rfloor = (2a-1)/3$, which results in

$$-(a+1) + (2a-1) \leqslant 3^{w/2} - 6 \ ,$$

which is equivalent to $a \leqslant 3^{w/2} - 4$. Thus (13) is equivalent to (11).

Next, we consider the case of odd w. In this case, we have to deal with another rotation induced by the factor $\mu i \zeta^2$ and obtain (12). In this case, the second set in the union corresponds to points on the boundary of $\widetilde{V}$, i.e., residue classes modulo τ^w containing two representatives of minimum norm.

It has already been shown by Blake, Kumar Murty and Xu [8] that any set $\mathcal{D}$ consisting of 0 and one minimum norm representative of every residue class modulo τ^w not divisible by τ is a w-NADS, for convenience, we repeat the argument. Such a proof requires showing that the right-to-left Algorithm 1 constructing a $\mathcal{D}$-w-NAF terminates.

This algorithm is entirely determined by how it chooses the least significant digit(s) of its input. If the input z is divisible by τ, the least significant digit is 0 and the remaining digits are those of z/τ, that clearly has smaller norm than z. Otherwise, a digit $d \in \mathcal{D}$

is chosen which is congruent to z modulo τ^w and the w least significant digits of z are $0\,0\,\ldots\,0\,d$, with $w-1$ zeros; the most significant digits of z are those of $(z-d)/\tau^w$. Now

$$\mathbf{N}\left(\frac{z-d}{\tau^w}\right) = \left|\frac{z-d}{\tau^w}\right|^2 \leqslant \left(\frac{|z|}{|\tau^w|} + \frac{1}{\sqrt{3}}\right)^2 \leqslant |z|^2 \left(\frac{1}{3} + \frac{1}{\sqrt{3}}\right)^2 < |z|^2 = \mathbf{N}(z) \ ,$$

i.e. the norm is decreasing in this case as well. The norms yield thus a strictly decreasing sequence of non-negative integers. Hence the algorithm must terminate after finitely many iterations, and the proof of the NADS-property of $\mathcal{D}$ is complete. □

One of the frequently considered questions about w-NADS with respect to various bases is that of optimality. In the case of binary expansions, the digit set $\{-2^{w-1}+1, \ldots, -3, -1, 0, 1, 3, \ldots, 2^{w-1}-1\}$ is known to be a w-NADS and it minimizes the Hamming weight (i.e., the number of nonzero digits) over all expansions with the same digit set, but without the w-NAF condition, cf. [2, 22, 23].

In the case of expansions to the base of the Frobenius endomorphism of Koblitz curves in characteristic 2 and various digit sets, this optimality result is only true for $w \leqslant 3$; for larger values of w, optimal expansions cannot even be described as a regular language, cf. [12].

In our case, optimality is true for moderate values of w:

Proposition 4.5. *Let $w \in \{2, \ldots, 7\}$, $z \in \mathbb{Z}[\tau]$ and $\eta_{\ell-1} \ldots \eta_0$ be the $\mathcal{D}_w$-w-NAF of z. Then*

$$W(\eta_{\ell-1} \ldots \eta_0) = \min\{W(d_{k-1} \ldots d_0) : d_{k-1} \ldots d_0 \in \mathcal{D}_w^* \text{ with } \mathsf{value}(d_{k-1} \ldots d_0) = z\},$$

where $W(d_{k-1} \ldots d_0) = \#\{j : d_j \neq 0\}$ denotes the Hamming weight of $d_{k-1} \ldots d_0$.

The proof runs along the lines of [13, Lemma 19] and uses heavy symbolic calculations, cf. Kröll [19] for technical details.

For $w > 7$, no information on optimality is available yet.

5. Evaluation of Costs for simple τ-adic Scalar Multiplication

We do not discuss here how to reduce a given scalar modulo $\tau^m - 1$ or the details of the computation of a τ-adic expansion: for these details we refer the reader to [8]. From now on we shall thus assume that an arbitrary scalar is *first* reduced modulo $\tau^m - 1$ and *then* expanded as a w-NAF.

5.1. **Choosing the Coordinate System.** Similarly to elliptic curves over fields of characteristic two or of large characteristic, different coordinate systems can be used to represent an elliptic curve over a field of characteristic three, its points, and to describe explicit computations on it (see for instance [3, Ch. 13] as a reference).

Affine coordinates use equation (1) and a point is represented by a pair of elements (x, y) from $\mathbb{F}_{3^m}$.

Koblitz [18] has suggested to use *projective coordinates*, whereas a point (x, y) is represented by a triple $[X{:}Y{:}Z]$ with $x = X/Z$ and $y = Y/Z$. The corresponding homogenized curve equation is $\mathcal{E}_{3,\mu} : Y^2Z = X^3 - XZ^2 - \mu Z^3$.

Coordinates → / ↓ Operation	Affine	Projective	Jacobian	Modified Jacobian
ADD	1 I + 3 M	14 M + 1 C	12 M + 4 C	11 M + 4 C
mixADD	—	9 M + 2 C	8 M + 3 C	7 M + 3 C
DBL	1 I + 2 M	11 M + 1 C	7 M + 2 C	6 M + 4 C
TPL	4 C	6 C	1 M + 6 C	8 C
τ	2 C	3 C	3 C	4 C

TABLE 1. Costs of various group operations in terms of field multiplications

Harrison, Page and Smart in [11] have proposed a different kind of projectivisation of the curve, whereby the affine point (x, y) is represented as $\langle X{:}Y{:}Z\rangle = (x, y)$, where $x = X/Z^2$ and $y = Y/Z^3$. Their curve equation is $\mathcal{E}_{3,\mu} : Y^2 = X^3 - XZ^4 - \mu Z^6$. In order to distinguish these coordinates from those described by Koblitz and in accordance with the rest of the literature on elliptic curves we call them instead *Jacobian coordinates*.

Finally, Kim and Negre [16] observe that some computational time can be saved if $T = Z^2$ is saved along with the Jacobian coordinates. They therefore introduce a *modified Jacobian* coordinate system, in which an affine point (x, y) on $\mathcal{E}_{3,\mu}$ is represented by the quadruple $\langle X{:}Y{:}Z{:}T\rangle$, where $x = X/Z^2$, $y = Y/Z^3$, and $T = Z^2$.

In Table 1 the costs of several operations on an elliptic curve $\mathcal{E}_{3,\mu}$ in these coordinate systems are given. There, ADD, DBL, TPL, and τ denote addition of two different points, doubling, tripling, and computation of the Frobenius image of a point, respectively. mixADD is used to denote a *mixed* addition of a point given in affine coordinates to a point in another coordinate system (i.e. $Z_2 = 1$), with a result expressed in the same coordinate system of the second point. M, I and C denote a field multiplication, inversion and cubing, respectively.

We did not find gains with *repeated additions*, i.e. when a given point is added to several inputs, except with standard Jacobian coordinates, where one M can be saved in the ADD. In Jacobian and modified Jacobian coordinates we save a cubing for the generic addition and nothing for the mixed addition.

Remark 5.1. The modified Jacobian coordinate system seems to be the fastest system, as long as a field inversion is slow. In fact, according to [11] and [1], a field inversion is in excess of ten field multiplication already for relatively small fields, if an efficient representation of the field is used.

5.2. **Operation Counts for Scalar Multiplication.** In order to estimate the cost of a scalar multiplication, we therefore use modified Jacobian coordinates system for the curve, but we keep the base point P in affine coordinates in order to exploit mixed additions. Note that for any point Q in affine coordinates, the point $\zeta^\ell Q$ can be computed in essentially no time and is also given in affine coordinates.

We shall determine the cost of a scalar multiplication on $\mathcal{E}_{3,\mu}$ in terms of field multiplications in $\mathbb{F}_{3^m}$. We assume that the expected length of a w-NAF is approximately m.

By an easy generalization of Koblitz' arguments (cf. the end of the proof of Theorem 1 in [18]) it can be proved that the expected density of a w-NAF expansion is $\frac{2}{2w+1}$.

In our notation, Koblitz' τ-adic expansion is a $\mathcal{D}_2$-NAF. A τ-adic Horner scheme based on the $\mathcal{D}_2$-NAF, i.e. Algorithm 2, takes

$$\left(\frac{2}{5}\,m-1\right)\mathtt{mixADD}+(m-1)\tau=\left(\frac{14}{5}\,m-7\right)\mathtt{M}+\left(\frac{26}{5}\,m-7\right)\mathtt{C}$$

to compute a scalar multiplication.

With $w=3$ we consider the digit set

$$\mathcal{D}_3:=\{0\}\cup\bigcup_{0\leqslant k<6}\zeta^k\{1,2,4-\mu\tau\}$$

so we need to precompute $2P$ and $(4-\mu\tau)P$ in affine coordinates. This takes two doublings (the first one being of an affine point, with a modified Jacobian result), an application of τ to an affine point and a mixed addition. Now, the Kim-Nègre's DBL takes the form

$$Z_3=-Y_1Z_1^3\ ,\quad T_3=Z_3^2\ ,\quad X_3=(T_1^3)^2+(X_1^3-Y_1^2)Y_1^2-\mu T_3\ ,\quad Y_3=T_1^9+Y_1^2T_3\ .$$

and, assuming $Z_1=T_1=1$ the cost becomes $4\,\mathtt{M}+1\,\mathtt{C}$. We do not need to compute the T-coordinate of $(4-\mu\tau)P$, so we save a M here. We then need to invert two Z-coordinates in order to convert $2P$ and $(4-\mu\tau)P$ to affine coordinates, and using Montgomery's trick this costs $1\,\mathtt{M}+7\,\mathtt{M}$ in total. So we have

$$\Big(\text{“first” }\mathtt{DBL}+\mathtt{DBL}+2\,\mathtt{C}+\mathtt{mixADD}-\mathtt{M}+(1\,\mathtt{I}+7\,\mathtt{M})\Big)+(m-1)\tau+\left(\frac{2}{7}\,m-1\right)\mathtt{mixADD}=$$
$$=(2\,m+16)\,\mathtt{M}+\mathtt{I}+\left(\frac{34}{7}\,m+3\right)\mathtt{C}\ .$$

For larger w, i.e. $w\geqslant 4$, we have to devise a precomputation strategy. As already observed, the triangular "slices" of the hexagon containing the minimal norm digits contain 1 and 2, and then we can compute all other digits simply by further additions of 1, 2 and $\pm\tau$. So we perform an affine doubling to get $2P$, a single application of τ to obtain $\tau(P)$ and $(3^{w-2}-2)$ further mixADDs.

At this stage we can decide whether to convert these $(3^{w-2}-2)$ points to affine coordinates as well, or to leave them in modified Jacobian coordinates.

Hence, for arbitrary $w>3$ we have the following cost

$$\Big(\text{affine}\,(\mathtt{DBL}+\tau)+1\,\mathtt{I}+(5\cdot 3^{w-2}-6)\,\mathtt{M}+(3^{w-2}-2)\,\mathtt{mixADD}\Big)+$$
$$+(m-1)\tau+\left(\frac{2}{2w+1}\,m-1\right)\mathtt{mixADD}=$$
$$=\left(\frac{14}{2w+1}\,m-32+4\cdot 3^{w-1}\right)\mathtt{M}+2\,\mathtt{I}+\left(\left(4+\frac{6}{2w+1}\right)m-11+3^{w-1}\right)\mathtt{C}$$

m	$w=2$	$w=3$	$w \geqslant 4$ Affine Pre.	$w \geqslant 4$ Mixed Pre.	gain
97	339.2	296.1	327.2 (w=4)	346.6 (w=4)	12.7 %
163	533.5	436.5	437.2 (w=4)	502.5 (w=4)	18.2 %
239	748.7	595.5	562.0 (w=4)	679.9 (w=4)	24.9 %
509	1537.0	1185.4	1035.4 (w=4)	1327.9 (w=5)	32.6 %
773	2305.9	1761.0	1498.4 (w=5)	1958.0 (w=5)	36.3 %
1223	3608.0	2720.3	2137.4 (w=5)	2921.4 (w=5)	40.7 %

TABLE 2. Cost (expressed in field multiplications) of scalar multiplication on curves over fields represented in polynomial basis

in the case we convert the last $3^{w-2}-2$ points to affine coordinates. If we leave these points in modified Jacobian coordinates, the cost is

$$\begin{aligned}\Big(\text{affine}\,(\mathtt{DBL}+\tau)+(3^{w-2}-2)\,\mathtt{mixADD}\Big)+\\ +(m-1)\tau+\left(\frac{2}{2w+1}\,m-1\right)\left(\frac{2}{3^{w-2}}\,\mathtt{mixADD}+\frac{3^{w-2}-2}{3^{w-2}}\,\mathtt{ADD}\right)=\\ =\left(\frac{2\,m}{2w+1}\left(11-\frac{8}{3^{w-2}}\right)-23+\frac{8}{3^{w-3}}+7\cdot 3^{w-2}\right)\mathtt{M}+\\ +\left(\frac{4\,m}{2w+1}\left(2+\frac{1}{3^{w-3}}\right)+4\,m-12+\frac{2}{3^{w-3}}+3^{w-1}\right)\mathtt{C}+\mathtt{I}\ .\end{aligned}$$

The probability that an addition in the Horner scheme is a mixed addition is taken into account, under the assumption that all non-zero digits occur with equal probability.

5.3. **Comparisons.** In Tables 2 and 3 on the facing page we express the costs of scalar multiplication for different values of w and m. In the first table it is assumed that a polynomial basis is used to represent the field, in the second table a normal basis.

In our comparisons we consider six field (and curve) sizes: $m = 97$, 163, 239, 509, 773 and 1223. We also consider two different representations of the fields: with a normal basis and with a polynomial basis. The first four are fields already considered in the literature, and the last two have been chosen to see how the various methods scale with the field size. We consider here the simple scalar multiplication Algorithms 2 and 3 with the precomputation strategies described in § 5.2 for $w \geqslant 3$.

The cost of a field inversion is taken to be equal to 15, 15, 20, 40, 60 and 80 multiplications, respectively for the six chosen values of m, and a cubing is equal to 0.15, 0.10, 0.07, 0.045, 0.037 and 0.03 multiplications, respectively. These values are approximate distillates of the values found in other scientific literature (for instance [11, 1]) and our own implementation experiments.

The optimal value of w in the case $w \geqslant 4$ is given in parentheses.

m	$w=2$	$w=3$	$w \geqslant 4$ Affine Pre.	$w \geqslant 4$ Mixed Pre.	gain
97	264.6	225.0	256.9 (w=4)	273.8 (w=4)	15.0 %
163	449.4	357.0	359.6 (w=4)	422.1 (w=4)	20.6 %
239	662.2	514.0	482.7 (w=4)	602.9 (w=4)	27.1 %
509	1418.2	1074.0	927.7 (w=4)	1216.9 (w=5)	34.5 %
773	2157.4	1622.0	1365.8 (w=5)	1820.7 (w=5)	36.7 %
1223	3417.4	2542.0	1988.5 (w=5)	2746.4 (w=5)	41.8 %

TABLE 3. Cost (expressed in field multiplications) of scalar multiplication on curves over fields represented in normal basis

Remark 5.2. The gains are significant and are between 20 % and 35 % for curves used in actual cryptographic applications. For larger curves, which could be interesting as security requirements increase, and are significant anyway for implementation in computer algebra systems, the gains are even higher. It is clear, as expected, that using a windowed representation of the scalar brings noticeable speed gains.

Remark 5.3. We note that in the comparison from [8] only the number of group additions is considered, whereas we consider all the costs. If we counted only the number of group operations, our results would be very similar to the ones in [8]. We note that the techniques described in [8] are not generic in the sense that for each value of w the precomputation sequence has to be determined anew, whereas our uniform description of the digit set yields a precomputation sequence for each w (Remark 4.4 on page 9).

Furthermore, our memory requirements are only *one third* of those in [8] because we explicitly make use of the rotational symmetry of the digit sets of minimal norm representatives, whereas Blake, Kumar and Xu just use a signed representation in [8, Section 4.2]. The explicit description of these digit sets (Theorem 2 on page 8) permits a very streamlined implementation of the scalar multiplication for all values of w, whereas in previously published results an ad-hoc operation sequence had to be devised for each w.

Remark 5.4. A comparison to expansions to the base of three, such as those used, for instance in [11], seems due.

(i) A tripling requires twice as many cubings as a Frobenius operation. Since the density of a simple base-three expansion is $1/2$ – higher than the $2/5$ of a $\mathcal{D}_2$-NAF – and its length is m, the method is slower than Koblitz' τ-adic method.
The nonary method from [11] uses a base 9 expansion, that has density $7/8$, hence yielding an expected $\frac{7}{16}\,m = 0.4375\,m$ group additions in the Horner scheme. This method requires 7 precomputations (and 7 operations).
For a τ-adic method the value of w giving the closest amount of precomputations to 7, is $w = 4$, which gives 9 precomputations. With this parameter we have about $\frac{2}{9}\,m =$

$0.\bar{2}\,m$ group additions in the Horner scheme. Taking $w = 3$, with 3 precomputations, already gives an expected $\frac{2}{7}\,m = 0.\overline{285714}\,m$ group operations in the Horner scheme.

(ii) With the exception of the derivation of the $\mathcal{D}_2$-NAF from the balanced ternary expansion (Theorem 1), in general computing the τ-adic expansion used in the methods by Koblitz [18], Blake, Kumar and Xu [8], and us is slightly more complex than computing a base three representation.

Hence, replacing a base-three $\{0, 1, 2\}$-expansion with a balanced ternary expansion or, even better, with the $\mathcal{D}_2$-NAF obtained from Theorem 1, brings already significant improvements. The methods studied in this paper further improve over the $\mathcal{D}_2$-NAF.

6. Eigenvalues

Let us assume in this section that the chosen Koblitz curve is good for cryptographic applications. In particular, the rational point group $\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$ contains a large cyclic subgroup G of prime order. The index of G in $\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$ should be as small as possible. Since $\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m}) > \mathcal{E}_{3,\mu}(\mathbb{F}_3)$, the order of $\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$ is always divisible by the order of $\mathcal{E}_{3,\mu}(\mathbb{F}_3)$, which is 1 if $\mu = 1$ and 7 if $\mu = -1$.

Furthermore, since N_m is divisible by $N_{m'}$ whenever $m' \mid m$, we may want to consider only m prime in order to increase the likelihood that N_m has a large prime factor. For example, when $\mu = 1$ we have that $N_{163} = 3^{163} + 3^{82} + 1$ is a prime of 259 bits; and when $\mu = -1$ we have that $N_{97} = 3^{97} + 3^{49} + 1$ is 7 times a prime of 154 bits.

Ideally, the index of G in $\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$ should be then as small as possible, however it suffices to assume that the order of G is a prime number ℓ and to require that ℓ divides the order of $\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$ only once – then G is also the only subgroup of order ℓ of $\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$. In particular, all endomorphisms of $\mathcal{E}_{3,\mu}(\mathbb{F}_{3^m})$ that operate non trivially on G map G onto itself.

Being G cyclic, τ, ζ, etc. operate on G by multiplication by a constant, i.e., there exist integers t, s such that

$$\tau P = t \cdot P \quad \text{and} \quad \zeta P = s \cdot P$$

for all $P \in G$. These integers are defined modulo ℓ.

In order to get a general expression, as we cannot make assumptions about ℓ, we compute here t and s modulo N_m instead, i.e., we find t such that

$$t^2 - 3\,\mu\,t + 3 \equiv 0 \bmod N_m \ , \quad \text{and} \quad t^m \equiv 1 \bmod N_m$$

and similarly for s. Then, to determine the eigenvalues s, t of ζ, τ operating on G, we shall reduce these integers modulo ℓ.

Theorem 3. *The two congruences*

$$\text{(i)} \quad t^2 - 3\,\mu\,t + 3 \equiv 0 \pmod{N_m} \ , \quad \textit{and} \quad \text{(ii)} \quad t^m \equiv 1 \pmod{N_m} \tag{14}$$

for $m \geqslant 5$ odd, integer, and coprime to 3, always admit a unique solution, namely

$$t \equiv (-3)^{\frac{m+1}{2}} + 3\,\mu\,[m \equiv 1 \pmod 3] \pmod{N_m} \ . \tag{15}$$

If

$$s \equiv \frac{3}{t^2} \pmod{N_m}$$

then

$$s \equiv 2 - \mu t \pmod{N_m} \ . \tag{16}$$

Proof. We use relation $t^6 \equiv (-3)^3 \pmod{N_m}$ that follows from (14,i) (without even using the actual value of N_m) to simplify (14,ii).

If $m \equiv 1 \pmod 3$ then it is necessarily $m \equiv 1 \pmod 6$ and

$$t^m \equiv 1 \equiv (-3)^{\frac{m-1}{2}} \cdot t \pmod{N_m} \ .$$

It is readily verified that this linear congruence admits the unique solution $t \equiv (-3)^{\frac{m+1}{2}} + 3\mu$.

If, on the other hand $m \equiv -1 \pmod 6$ then

$$t^m \equiv 1 \equiv (-3)^{\frac{m+1}{2}} \cdot t^{-1} \pmod{N_m}$$

whence it follows at once that $t \equiv (-3)^{\frac{m+1}{2}}$.

The statement (16) about s is a direct consequence of the fact that $\zeta = 2 - \mu\tau$, which is just another form of (6). □

Remark 6.1. In fact it can now be easily seen that Equation (14,i) has *two* distinct solutions mod N_m:

$$t_1 = (-3)^{\frac{m+1}{2}} + 3\mu[m \equiv 1 \pmod 3] \quad \text{and} \quad t_2 = -(-3)^{\frac{m+1}{2}} + 3\mu[m \equiv 2 \pmod 3] \ .$$

References

[1] Omran Ahmadi, Darrel Hankerson, and Alfred Menezes, *Software Implementation of Arithmetic in* $\mathbb{F}_{3^m}$, Arithmetic of Finite Fields, First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007, Proceedings, Lecture Notes in Computer Science, vol. 4547, 2007, pp. 85–102.

[2] Roberto Avanzi, *A Note on the Signed Sliding Window Integer Recoding and a Left-to-Right Analogue*, Selected Areas in Cryptography: 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers, Lecture Notes in Comput. Sci., vol. 3357, Springer-Verlag, Berlin, 2004, pp. 130–143.

[3] Roberto Avanzi, Henri Cohen, Christophe Doche, Gerhard Frey, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press Series on Discrete Mathematics and its Applications, vol. 34, Chapman & Hall/CRC, Boca Raton, FL, 2005.

[4] Roberto Avanzi, Clemens Heuberger, and Helmut Prodinger, *Redundant τ-adic Expansions I: Non-Adjacent Digit Sets and their Applications to Scalar Multiplication*, Des. Codes Cryptogr. (2010), To appear.

[5] Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, Eiji Okamoto, and Francisco Rodríguez-Henríquez, *A Comparison between Hardware Accelerators for the Modified Tate Pairing over F_{2^m} and F_{3^m}*, Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings (Steven D. Galbraith and Kenneth G. Paterson, eds.), Lecture Notes in Computer Science, vol. 5209, Springer, 2008, pp. 297–315.

[6] Jean-Luc Beuchat, Emmanuel López-Trejo, Luis Martínez-Ramos, Shigeo Mitsunari, and Francisco Rodríguez-Henríquez, *Multi-core Implementation of the Tate Pairing over Supersingular Elliptic Curves*, Cryptology and Network Security, 8th International Conference, CANS 2009, Kanazawa,

Japan, December 12-14, 2009. Proceedings (Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, eds.), Lecture Notes in Computer Science, vol. 5888, Springer, 2009, pp. 413–432.

[7] Jean-Luc Beuchat, Masaaki Shirase, Tsuyoshi Takagi, and Eiji Okamoto, *An Algorithm for the η_T Pairing Calculation in Characteristic Three and its Hardware Implementation*, ARITH '07: Proceedings of the 18th IEEE Symposium on Computer Arithmetic (Washington, DC, USA), IEEE Computer Society, 2007, pp. 97–104.

[8] Ian F. Blake, V. Kumar Murty, and Guangwu Xu, *Efficient algorithms for Koblitz curves over fields of characteristic three*, J. Discrete Algorithms **3** (2005), no. 1, 113–124.

[9] Ernie Brickell, Liqun Chen, and Jiangtao Li, *A New Direct Anonymous Attestation Scheme from Bilinear Maps*, Trusted Computing - Challenges and Applications, First International Conference on Trusted Computing and Trust in Information Technologies, Trust 2008, Villach, Austria, March 11-12, 2008, Proceedings, Lecture Notes in Computer Science, vol. 4968, Springer, 2008, pp. 166–178.

[10] William J. Gilbert, *Radix representations of quadratic fields*, J. Math. Anal. Appl. **83** (1981), no. 1, 264–274.

[11] Keith Harrison, Dan Page, and Nigel Smart, *Software Implementation of Finite Fields of Characteristic Three, for Use in Pairing Based Cryptosystems*, LMS JCM **5** (2002), 181–193.

[12] Clemens Heuberger, *Redundant τ-adic expansions II: Non-optimality and chaotic behaviour*, Math. Comput. Sci. **3** (2010), 141–157.

[13] Clemens Heuberger and Helmut Prodinger, *Analysis of alternative digit sets for nonadjacent representations*, Monatsh. Math. **147** (2006), 219–248.

[14] I. Kátai and B. Kovács, *Canonical Number Systems in Imaginary Quadratic Fields*, Acta Math. Hungar. **37** (1981), 159–164.

[15] I. Kátai and J. Szabó, *Canonical Number Systems for Complex Integers*, Acta Sci. Math. (Szeged) **37** (1975), 255–260.

[16] Kwang-Ho Kim and Christophe Nègre, *Point multiplication on supersingular elliptic curves defined over fields of characteristic 2 and 3*, SECRYPT, INSTICC Press, 2008, pp. 373–376.

[17] Donald E. Knuth, *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1997.

[18] Neal Koblitz, *An elliptic curve implementation of the finite field digital signature algorithm*, Advances in cryptology—CRYPTO '98 (Santa Barbara, CA, 1998), Lecture Notes in Comput. Sci., vol. 1462, Springer, Berlin, 1998, pp. 327–337.

[19] Markus Kröll, *Optimality of digital expansions to the base of the Frobenius endomorphism on Koblitz curves in characteristic three*, in preparation.

[20] David W. Matula, *Basic digit sets for radix representation*, J. Assoc. Comput. Mach. **29** (1982), no. 4, 1131–1143.

[21] James A. Muir and Douglas R. Stinson, *Alternative digit sets for nonadjacent representations*, SIAM J. Discrete Math. **19** (2005), 165–191.

[22] ———, *Minimality and other properties of the width-w nonadjacent form*, Math. Comp. **75** (2006), 369–384.

[23] Braden Phillips and Neil Burgess, *Minimal weight digit set conversions*, IEEE Trans. Comput. **53** (2004), 666–677.

[24] Jerome A. Solinas, *An improved algorithm for arithmetic on a family of elliptic curves*, Advances in Cryptology — CRYPTO '97. 17th annual international cryptology conference. Santa Barbara, CA, USA. August 17–21, 1997. Proceedings (B. S. Kaliski, jun., ed.), Lecture Notes in Comput. Sci., vol. 1294, Springer, Berlin, 1997, pp. 357–371.

[25] ———, *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249.

Faculty of Mathematics and Horst Görtz Institute for IT Security, Ruhr-University Bochum, Germany
E-mail address: roberto.avanzi AT ruhr-uni-bochum.de

Institut für Mathematik B, Technische Universität Graz, Austria
E-mail address: clemens.heuberger AT tugraz.at

Department of Mathematics, University of Stellenbosch, South Africa
E-mail address: hproding AT sun.ac.za