SYMMETRIC DIGIT SETS FOR ELLIPTIC CURVE SCALAR MULTIPLICATION WITHOUT PRECOMPUTATION

CLEMENS HEUBERGER AND MICHELA MAZZOLI

Abstract. We describe a method to perform scalar multiplication on two classes of ordinary elliptic curves, namely $E : y^2 = x^3 + Ax$ in prime characteristic $p \equiv 1 \bmod 4$, and $E : y^2 = x^3 + B$ in prime characteristic $p \equiv 1 \bmod 3$. On these curves, the 4-th and 6-th roots of unity act as (computationally efficient) endomorphisms. In order to optimise the scalar multiplication, we consider a width-w-NAF (non-adjacent form) digit expansion of positive integers to the complex base of τ, where τ is a zero of the characteristic polynomial $x^2 - tx + p$ of the Frobenius endomorphism associated to the curve. We provide a precomputationless algorithm by means of a convenient factorisation of the unit group of residue classes modulo τ in the endomorphism ring, whereby we construct a digit set consisting of powers of subgroup generators, which are chosen as efficient endomorphisms of the curve.

1. Introduction

In the last decades the use of elliptic curves in public key cryptography (ECC) has gained more and more attention. The operation that dominates the execution time of ECC algorithms is the scalar multiplication, i.e. $nP = P + \cdots + P$, where P is an elliptic curve point and $n \in \mathbb{Z}$. The need of time-saving implementations has led to the development of various scalar multiplication methods.

In analogy with the square-and-multiply method for modular integer exponentiation, one can consider the binary expansion of n, that is $n = \sum_{j=0}^{l-1} d_j 2^j$, with $d_j \in \{0, 1\}$; and then one can compute nP with a so-called *Horner scheme* or *double-and-add method*:

$$nP = \sum_{j=0}^{l-1} d_j 2^j (P) = d_0 P + 2(d_1 P + 2(d_2 P + 2(\cdots + 2(d_{l-1} P) \cdots))) \,.$$

It is clear that the fewer nonzero digits in the recoding of n, the fewer additions in the Horner scheme. As Morain and Olivos first proposed in [11], one can also take negative digits, i.e. $d_j \in \{0, \pm 1\}$, since point subtraction on elliptic curves is as easy as addition.

However, the scalar n can be expanded in a more convenient complex base. Indeed, for every elliptic curve over a finite field of prime characteristic p, there is a quadratic algebraic number, often denoted as τ, that represents the Frobenius endomorphism on the curve, namely

$$\tau(x, y) = (x^p, y^p) \,.$$

Key words and phrases. Elliptic curve scalar multiplication, Frobenius endomorphism, integer digit expansions, digit sets, τ-adic expansion, width-w non-adjacent form, Gaussian integers, Eisenstein integers.

The authors are supported by the Austrian Science Fund (FWF): P 24644-N26.

Since τ requires only two field exponentiations, its computational cost is very low in comparison with point doubling.

In his seminal work [13, 14], Solinas developed a *τ-and-add method* where the integer n is expanded in basis τ. In this way, in the Horner scheme, point doubling is replaced by the (faster) Frobenius endomorphism. Solinas applied this idea to Koblitz curves [8] in characteristic 2. Moreover, Solinas' integer expansion is a non-adjacent form (NAF), i.e. in every two consecutive digits there is at least one zero, which is a desirable property that reduces the number of additions in the Horner scheme.

Koblitz [9] suggested a NAF τ-and-add algorithm for a family of supersingular curves in characteristic 3; this method was later improved by Blake, Murty and Xu [4]. Avanzi, Heuberger and Prodinger [2] exploited the existence of the 6-th roots of unity in $\mathbb{Z}[\tau] = \{a + b\tau \mid a, b \in \mathbb{Z}\}$ to create a sixpartite digit set that decreased memory consumption by a factor three; Avanzi and Heuberger [1] also provided a precomputationless factored digit set. A similar study was undertaken by Kleinrahm [7], examining a curve in characteristic 5 where the 4-th roots of unity belong to $\mathbb{Z}[\tau]$.

In this paper, we study the use of elliptic curves where 4-th and 6-th roots of unity act on the curve as (computationally cheap) endomorphisms. In particular,

- we study w-NAF integer expansions whose digit sets are invariant under the action of the roots of unity and therefore reduce the precomputation effort (Section 3);
- we study the minimal norm representative digit sets and show that these are w-NADS, i.e. every element of the endomorphism ring admits a finite w-NAF expansion (Theorem 4.4);
- we study the use of factored digit sets for precomputationless efficient scalar multiplication (Section 6);
- we explain how to construct such factored digit sets in characteristic p with $p \equiv 7 \mod 36$ or $p \equiv 31 \mod 36$ or $p \equiv 5 \mod 8$ (Section 9, in particular Theorem 9.3);
- we provide explicit factored digit sets in characteristics 5, 7, 13, 29, 31, 37, 53, 61 leading to finite recoding (Tables 1 and 2).

The paper is organised as follows. In Section 2 we shall describe two families of elliptic curves with special endomorphism rings, which will come in handy for our purpose. In Section 3 we shall discuss w-NAF integer expansions to the base τ; a necessary and sufficient condition that guarantees finite recoding of integers will be provided. In Section 4 minimal norm representative digit sets are introduced. After giving some examples of suitable elliptic curves (Section 5), in Section 6 we shall study the structure of the unit group of the quotient ring $\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta]$, where $\mathbb{Z}[\delta]$ is one of the endomorphism rings of Section 2. In Sections 7 and 8 scalar multiplication algorithms will be provided for curves in characteristic 7 and 5 respectively. A deeper analysis for curves in characteristic $p \geq 13$ will be carried out in Section 9.

2. Elliptic curves with special endomorphism ring

Recent work by Avanzi and Heuberger [1], Avanzi, Heuberger and Prodinger [2], and Kleinrahm [7] point out that for certain elliptic curves over finite fields,

some roots of unity appear in $\mathbb{Z}[\tau]$ where τ is the Frobenius endomorphism of the curve. These roots of unity can be used to create a digit set for a τ-adic expansion of integers, leading to a very efficient elliptic curve scalar multiplication with reduced number of precomputations. In [1, 2] a primitive 6-th root of unity ζ occurs in $\mathbb{Z}[\tau]$ for a supersingular Koblitz curve in characteristic 3; ζ is used to create a digit set which noticeably speeds up scalar multiplication and decreases memory requirements at the same time. In [7] a curve in characteristic 5 with $i \in \mathbb{Z}[\tau]$ is analysed; the digit set built with the help of i needs no precomputation at all.

Moreover, in [7] a necessary and sufficient condition for either $i \in \mathbb{Z}[\tau]$ or $\zeta \in \mathbb{Z}[\tau]$ is given. Recall that the Frobenius endomorphism τ satisfies the characteristic equation

$$\tau^2 - t\tau + p = 0$$

where p is the field characteristic and $t = p+1-|E(\mathbb{F}_p)|$ is the trace of the Frobenius endomorphism. Then τ can be identified with

$$\tau = \frac{t \pm \sqrt{t^2 - 4p}}{2} \,. \tag{1}$$

Proposition 2.1 ([7], c. 4)**.** *Let p be a prime number, E an elliptic curve defined over the finite field $\mathbb{F}_p$, τ the Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$ of E and t the trace of τ. Then*

- *$\mathbb{Z}[\tau]$ includes the 4-th roots of unity if and only if $t^2 - 4p = -4$;*
- *$\mathbb{Z}[\tau]$ includes the 6-th roots of unity if and only if $t^2 - 4p = -3$.*

Nevertheless, with respect to our goal of creating an effective integer τ-adic expansion, we shall prove that this condition is not essential: provided that the 4-th (resp. 6-th) roots of unity belong to the endomorphism ring $\mathrm{End}\,(E)$ of the curve, but not necessarily to $\mathbb{Z}[\tau]$, we can still exploit their action on the points of E, an operation that will turn out to require negligible time.

Consider the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ and the ring of Eisenstein integers $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ where $\omega = (-1 + \sqrt{-3})/2$ is a primitive third root of unity. Clearly, the former contains the 4-th roots of unity, the latter includes the 6-th's.

Actually, let $\zeta = -\overline{\omega} = (1 + \sqrt{-3})/2$ be a primitive sixth root of unity; then $\mathbb{Z}[\omega] = \mathbb{Z}[\zeta]$. We prefer to adopt the latter notation $\mathbb{Z}[\zeta]$ instead of the standard $\mathbb{Z}[\omega]$ for the ring of Eisenstein integers, as it will better serve our purpose.

There is a tight relationship between the rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta]$, and certain elliptic curves in prime characteristic $p \neq 2, 3$.

The following theorem is a well-known often-mentioned fact, although the authors could not find a self-contained proof in the literature. However, the result can be derived from [12, III.9.3, III.10.1, V.4.1].

Theorem 2.2. *Let p be a prime number such that $p \equiv 1$ mod 4, and consider the family of elliptic curves over $\mathbb{F}_p$*

$$E : y^2 = x^3 + Ax, \text{ with } A \in \mathbb{F}_p,\ A \neq 0 \,. \tag{2}$$

Then the endomorphism ring of E is isomorphic to $\mathbb{Z}[i]$.

Let p be a prime number such that $p \equiv 1 \bmod 3$, and consider the family of elliptic curves over $\mathbb{F}_p$

$$E : y^2 = x^3 + B, \text{ with } B \in \mathbb{F}_p,\ B \neq 0\,. \tag{3}$$

Then the endomorphism ring of E is isomorphic to $\mathbb{Z}[\zeta]$.

Henceforth p will always be a prime number such that $p \equiv 1 \bmod 3$ or $p \equiv 1 \bmod 4$. We shall denote the endomorphism ring as $\mathbb{Z}[\delta]$, where δ is either i or ζ depending on whether the elliptic curve belongs to the family (2) or (3).

Furthermore, the endomorphisms defined by the 4-th (resp. 6-th) roots of unity turn out to be very efficient to compute, as they require one field multiplication only (cf. for instance [12, III §10]).

More precisely, consider an elliptic curve of family (3). Then the endomorphisms defined by the primitive 6-th roots of unity ζ and its complex conjugate $\overline{\zeta}$ are given by

$$\begin{aligned}[\zeta](x, y) &= (u^2 x, -y)\,,\\ [\overline{\zeta}](x, y) &= (ux, -y)\end{aligned}$$

where $u \in \mathbb{F}_p$ is an element of order 3. We can also determine the endomorphisms defined by the third primitive roots of unity ω and $\overline{\omega}$:

$$\begin{aligned}[\omega](x, y) &= [-\overline{\zeta}](x, y) = (ux, y)\,,\\ [\overline{\omega}](x, y) &= [-\zeta](x, y) = (u^2 x, y)\,.\end{aligned}$$

In the case of family (2), the 4-th primitive roots of unity i and $-i$ define the following endomorphisms:

$$\begin{aligned}[i](x, y) &= (-x, -vy)\,,\\ [-i](x, y) &= (-x, vy)\end{aligned}$$

where $v \in \mathbb{F}_p$ is an element of order 4.

Recall that, in any $\mathbb{F}_p$, if $m \in \mathbb{Z}$ is such that $m \mid p - 1$ then there are $\varphi(m)$ elements of order m, where φ is Euler's totient function. In our case there are two possible values for the coefficient u (idem for v). One can find the right coefficient by testing each value on some points of $E(\mathbb{F}_p)$ or $E(\mathbb{F}_{p^2})$, as the action of the Frobenius endomorphism is known to be $\tau(x, y) = (x^p, y^p)$ and τ can be represented in terms of ζ or i, once a branch of the root in (1) is chosen.

3. Integer expansion to the base τ

In order to find a τ-adic expansion for integers, we shall work in the whole endomorphism ring $\mathbb{Z}[\delta]$, instead of $\mathbb{Z}[\tau]$. Recall that $\mathbb{Z}[\tau] \subseteq \mathbb{Z}[\delta]$, but equality does not necessarily hold. We regard an integer n as an element of $\mathbb{Z}[\delta]$, and the digits of its τ-adic expansion belong to $\mathbb{Z}[\delta]$, but not necessarily to $\mathbb{Z}[\tau]$. In other words, our digit set will be a finite subset $\mathcal{D}$ of $\mathbb{Z}[\delta]$, containing 0 and other convenient endomorphisms.

This larger digit set recoding is admissible for scalar multiplication. Indeed, let n be a positive integer and suppose $n = \sum_{j=0}^{l-1} \kappa_j \tau^j$ is a τ-adic recoding with digit

set $\mathcal{D} \subseteq \mathbb{Z}[\delta]$. Let P be a point of the elliptic curve E; computation of nP can be done with a so-called *Horner scheme*:

$$\begin{aligned} nP &= \sum_{j=0}^{l-1} \kappa_j \tau^j(P) \\ &= \tau(\ldots(\tau(\tau(\kappa_{l-1}P) + \kappa_{l-2}P) + \cdots + \kappa_1 P) + \kappa_0 P\,. \end{aligned}$$

For $0 \le j \le l-1$, κ_j is an endomorphism that is not necessarily a scalar multiplication. Of course, κ_j applies to the point $P \in E$, and $\kappa_j P$ is still a point of E. It may also be convenient to precompute κP for all $\kappa \in \mathcal{D}$ and store these values.

We state some useful definitions about digit sets to the basis τ (cf. [3, §2]).

Definition 3.1. Let $w \in \mathbb{N}$, $w \ge 1$ and $\eta \in \mathbb{Z}[\delta]$. A τ-adic recoding $\eta = \sum_{j=0}^{l-1} \kappa_j \tau^j$ is called *width-w Non-Adjacent Form* (*w-NAF*) if every block of w consecutive digits has at most one nonzero digit, i.e. for all $j = 0, \ldots, l-2$

$$\kappa_j \neq 0 \;\Rightarrow\; \kappa_{j+1} = \cdots = \kappa_{j+w-1} = 0\,.$$

Definition 3.2. Let $w \in \mathbb{N}$, $w \ge 1$. A digit set $\mathcal{D}_w \subseteq \mathbb{Z}[\delta]$ for w-NAF τ-adic recoding consisting of 0 and exactly one representative of each residue class modulo τ^w not divisible by τ in $\mathbb{Z}[\delta]$ is called *reduced residue system modulo τ^w*.

Definition 3.3. A digit set $\mathcal{D}_w \subseteq \mathbb{Z}[\delta]$ for τ-adic recoding is called *width-w Non-Adjacent Digit Set (w-NADS)* if every element $\eta \in \mathbb{Z}[\delta]$ has a finite recoding

$$\eta = \sum_{j=0}^{l-1} \kappa_j \tau^j$$

with $\kappa_j \in \mathcal{D}$ and this recoding is w-NAF.

Algorithm 1 (cf. [3, Alg. 1]) shows how to construct a w-NAF τ-adic recoding.

Algorithm 1 w-NAF τ-adic recoding of integers

Input: n, $w \in \mathbb{N}$, digit set $\mathcal{D}_w$, basis τ
Output: $n = \sum_{j=0}^{l-1} d_j \tau^j$ with $d_j \in \mathcal{D}_w$ and with w-NAF property, if such recoding exists; otherwise, the algorithm will enter an infinite loop.

1: $z := n$
2: $l := 0$
3: **while** $z \neq 0$ **do**
4: **if** $z \equiv 0 \bmod \tau$ **then**
5: $d_l := 0$
6: **else**
7: let $d_l \in \mathcal{D}_w$ s.t. $d_l \equiv z \bmod \tau^w$ ▷ guarantees $w-1$ zeros
8: **end if**
9: $z := \frac{z - d_l}{\tau}$
10: $l := l + 1$
11: **end while**
12: **return** $(\langle d_{l-1}, \ldots, d_0 \rangle, l)$

The next theorem provides a necessary and sufficient condition for a digit set to be w-NADS. It is based on [3, Thm 1] and [10].

Before stating the theorem, we recall that $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta]$ are Euclidean domains with their respective norms

$$\mathrm{N}(a+bi) = a^2+b^2 = |a+bi|^2 ,$$
$$\mathrm{N}(a+b\zeta) = a^2+ab+b^2 = |a+b\zeta|^2 ,$$

where $|\cdot|$ denotes the usual absolute value of a complex number. Also, $\mathrm{N}(\tau) = p$, the base field characteristic.

Theorem 3.1. *Let $\mathcal{D}_w$ be a reduced residue system for w-NAF recoding to the basis τ, with $w \in \mathbb{N}$, $w \geq 1$. Let $d_{max} = \max\{\mathrm{N}(d) \mid d \in \mathcal{D}_w\}$. Then $\mathcal{D}_w$ is a w-NADS if and only if for all $z \in \mathbb{Z}[\delta]$ such that*

$$\mathrm{N}(z) \leq \frac{d_{max}}{(|\tau^w|-1)^2} , \tag{4}$$

z has a finite $\mathcal{D}_w$-τ-adic expansion.

Proof. $\Rightarrow$) obvious.

$\Leftarrow$) Consider Algorithm 1. The crucial step is how the algorithm chooses the least significant digit of the input z.

If z is divisible by τ, then the least significant digit is 0 and the remaining digits are those of z/τ, which has smaller norm than z.

Otherwise, a digit $d \in \mathcal{D}_w$ is chosen in such a way that $d \equiv z \mod \tau^w$. Then the w least significant digits of z are $00\ldots0d$ ($w-1$ zeros); the remaining digits are those of $\frac{z-d}{\tau^w}$. As long as

$$\mathrm{N}\left(\frac{z-d}{\tau^w}\right) < \mathrm{N}(z) , \tag{5}$$

the norms $\mathrm{N}(z)$ yield a strictly decreasing sequence of non-negative integers, that must be finite. Thus Algorithm 1 must terminate or (5) must be violated.

Note that

$$\frac{|z-d|}{|\tau^w|} \leq \frac{|z|+|d|}{|\tau^w|} \leq \frac{|z|+\sqrt{d_{max}}}{|\tau^w|} .$$

Then the inequality (5) is true if

$$\frac{|z|+\sqrt{d_{max}}}{|\tau^w|} < |z| ,$$

or equivalently,

$$|z| > \frac{\sqrt{d_{max}}}{|\tau^w|-1} .$$

Therefore, as long as

$$\mathrm{N}(z) > \frac{d_{max}}{(|\tau^w|-1)^2} ,$$

(5) is true. All other z admit a finite expansion by assumption, so Algorithm 1 cannot enter an infinite loop. Hence $\mathcal{D}_w$ is a w-NADS. □

In other words, for all those elements $z \in \mathbb{Z}[\delta]$ such that (4) does hold, we have to check whether they have a finite recoding or not. In fact, these are the only values of z whereby Algorithm 1 may enter an infinite loop.

4. Minimal Norm Representatives

In order to guarantee that a finite w-NAF τ-adic recoding exists for every integer, one option is to choose $\mathcal{D}_w$ as a *Minimal Norm Representative (MNR)* digit set, i.e. $\mathcal{D}_w$ consists of 0 and exactly one representative of minimal norm of each residue class modulo τ^w not divisible by τ.

Definition 4.1. Let $\alpha \in \mathbb{Z}[\delta]$ be not divisible by τ. Then α is a *representative of minimal norm of its residue class* modulo τ^w if

$$\mathrm{N}(\alpha) \leq \mathrm{N}(\beta) \quad \text{for all } \beta \in \mathbb{Z}[\delta] \text{ s.t. } \beta \equiv \alpha \mod \tau^w .$$

Note that a representative of minimal norm needs not to be unique. Clearly,

$$\mathrm{N}(\alpha) \leq \mathrm{N}(\beta) \;\Leftrightarrow\; |\alpha| \leq |\beta| .$$

Lemma 4.1. *Suppose $|\tau| > 2$, let $u, v \in \mathbb{Z}[\delta]$ be two distinct units. Then $u \not\equiv v \mod \tau^w$ for all $w \geq 1$.*

Proof. Since u and v are units, $|u| = |v| = 1$. If $u \equiv v \mod \tau^w$ for some $w \geq 1$, then $u \equiv v \mod \tau$. Thus $\tau \mid u - v$, and therefore $\mathrm{N}(\tau) \mid \mathrm{N}(u - v) = |u - v|^2 \leq (|u| + |v|)^2 = 4$, but $\mathrm{N}(\tau) = |\tau|^2 > 4$. □

In other words, when $|\tau| > 2$ (or equivalently $p > 4$), all elements of $\mathbb{Z}[\delta]$ having norm equal to 1 belong to different residue classes modulo τ^w, for all $w \geq 1$.

Note that Lemma 4.1 does not hold for Koblitz curves in characteristic 3 [9]; in that case the units of $\mathbb{Z}[\zeta]$ are not distinct in the quotient ring.

It is clear that if $u \in \mathbb{Z}[\delta]$ has norm 1, then u is a representative of minimal norm of its residue class. Lemma 4.1 also implies that, if $|\tau| > 2$, then u is the *only* element of norm 1 in its residue class. Therefore we have the following

Corollary 4.2. *Suppose $|\tau| > 2$ and $u \in \mathbb{Z}[\delta]$ is a unit. If $\mathcal{D} \subseteq \mathbb{Z}[\delta]$ is an MNR digit set, then $u \in \mathcal{D}$.*

Lemma 4.3. *Let $p = \mathrm{N}(\tau) = |\tau|^2$ and suppose $p = 5$ or $p = 7$, and $w = 1$. If $\mathcal{D}_1$ is an MNR digit set for 1-τ-adic recoding, then*

$$\text{for } p = 5 , \; \mathcal{D}_1 = \{0, \pm 1, \pm i\} ;$$
$$\text{for } p = 7 , \; \mathcal{D}_1 = \{0, \pm 1, \pm \zeta, \pm \zeta^2\} .$$

Proof. Let $p = 5$ (the other case is analogous). Since $\mathcal{D}_1$ is an MNR digit set, by Corollary 4.2 $\mathcal{D}_1$ must contain, along with 0, all the units of $\mathbb{Z}[\delta] = \mathbb{Z}[i]$, i.e. 0, ± 1, $\pm i \in \mathcal{D}_1$.

In addition, $\mathcal{D}_1$ is a reduced residue system modulo τ. The number of residue classes modulo τ not divisible by τ is precisely $\varphi(\mathrm{N}(\tau)) = \varphi(5) = 4$. Therefore $\mathcal{D}_1 = \{0, \pm 1, \pm i\}$. □

Theorem 4.4. *Suppose $|\tau| > 2$, let $w \in \mathbb{N}$, $w \geq 1$. Let $\mathcal{D}_w$ be an MNR reduced residue system modulo τ^w. Then $\mathcal{D}_w$ is a w-NADS.*

Proof. We apply Theorem 3.1. Let $z \in \mathbb{Z}[\delta]$ be such that (4) does not hold, namely

$$\mathrm{N}(z) \leq \frac{d_{max}}{\left(|\tau^w| - 1\right)^2}\,. \tag{6}$$

Since $\mathbb{Z}[\delta]$ is a Euclidean domain with the norm N, for any $z \in \mathbb{Z}[\delta]$ there exist q, $r \in \mathbb{Z}[\delta]$ such that $z = q\tau^w + r$ and $\mathrm{N}(r) < \mathrm{N}(\tau^w)$. So the residue class of z mod τ^w can be represented by r. Due to the MNR condition on $\mathcal{D}_w$, the digit $d \equiv z \bmod \tau^w$ must be such that $\mathrm{N}(d) \leq \mathrm{N}(r) < \mathrm{N}(\tau^w) = p^w$.

Therefore $d_{max} < p^w$. In addition, if $w \geq 2$, or $w = 1$ and $p > 7$, then

$$\mathrm{N}(z) < \frac{p^w}{\left(\sqrt{p^w} - 1\right)^2} < 2\,, \tag{7}$$

which yields $\mathrm{N}(z) \leq 1$, as $\mathrm{N}(z)$ is an integer. Thus either $z = 0$ or z is a unit; in the latter case, since $\mathcal{D}_w$ is an MNR digit set, $z \in \mathcal{D}_w$ by Corollary 4.2.

Finally, if $p = 5$ or $p = 7$, and $w = 1$, then (7) does not hold, but in both cases $d_{max} = 1$ (cf. Lemma 4.3). So from (6) we have that $z = 0 \in \mathcal{D}_w$. □

5. Some curves in small characteristic

We give some examples of elliptic curves belonging to the families (2) and (3) in characteristic $p = 5$, 7, 13.

Example 5.1. Let $p = 5 \equiv 1 \mod 4$

Let $E : y^2 = x^3 + Ax$, $A \neq 0$; then $\mathrm{End}(E) \cong \mathbb{Z}[i]$.

A	t	τ	
1	2	$1 \pm 2i$	$\mathbb{Z}[\tau] \subsetneq \mathbb{Z}[i]$
2	4	$2 \pm i$	$\mathbb{Z}[\tau] = \mathbb{Z}[i]$
3	-4	$-2 \pm i$	$\mathbb{Z}[\tau] = \mathbb{Z}[i]$
4	-2	$-1 \pm 2i$	$\mathbb{Z}[\tau] \subsetneq \mathbb{Z}[i]$

Example 5.2. Let $p = 7 \equiv 1 \mod 3$

Let $E : y^2 = x^3 + B$, $B \neq 0$; then $\mathrm{End}(E) \cong \mathbb{Z}[\zeta]$.

B	t	τ	$\tau = a + b\zeta$	
1	-4	$-2 \pm \sqrt{-3}$	$-3 + 2\zeta,\ -1 - 2\zeta$	$\mathbb{Z}[\tau] \subsetneq \mathbb{Z}[\zeta]$
2	-1	$-\frac{1}{2} \pm \frac{3\sqrt{-3}}{2}$	$-2 + 3\zeta,\ 1 - 3\zeta$	$\mathbb{Z}[\tau] \subsetneq \mathbb{Z}[\zeta]$
3	-5	$-\frac{5}{2} \pm \frac{\sqrt{-3}}{2}$	$-3 + \zeta,\ -2 - \zeta$	$\mathbb{Z}[\tau] = \mathbb{Z}[\zeta]$
4	5	$\frac{5}{2} \pm \frac{\sqrt{-3}}{2}$	$2 + \zeta,\ 3 - \zeta$	$\mathbb{Z}[\tau] = \mathbb{Z}[\zeta]$
5	1	$\frac{1}{2} \pm \frac{3\sqrt{-3}}{2}$	$-1 + 3\zeta,\ 2 - 3\zeta$	$\mathbb{Z}[\tau] \subsetneq \mathbb{Z}[\zeta]$
6	4	$2 \pm \sqrt{-3}$	$1 + 2\zeta,\ 3 - 2\zeta$	$\mathbb{Z}[\tau] \subsetneq \mathbb{Z}[\zeta]$

Example 5.3. Let $p = 13 \equiv 1 \bmod 4$ and $\bmod 3$.

Let $E : y^2 = x^3 + Ax$, $A \neq 0$. The trace t can be equal to ± 4 or ± 6, and in each case the Frobenius endomorphism is one of the roots $\tau_{(4)} = 2 \pm 3i$, $\tau_{(-4)} = -2 \pm 3i$, $\tau_{(6)} = 3 \pm 2i$, and $\tau_{(-6)} = -3 \pm 2i$. For all these curves $\mathbb{Z}[\tau] \subsetneq \mathbb{Z}[i]$.

Now let $E : y^2 = x^3 + B$, $B \neq 0$. For these curves the trace t can be ± 2, ± 5 or ± 7, and $\mathbb{Z}[\tau] = \mathbb{Z}[\zeta]$ if and only if $t = \pm 7$. For example, with $\tau_{(5)} = \frac{5}{2} \pm \frac{3\sqrt{-3}}{2} = 1 + 3\zeta$,

$\mathbb{Z}[\tau] = \mathbb{Z}[3\zeta] \subsetneq \mathbb{Z}[\zeta]$.

As we can see from the examples above, in each family of curves all values of τ are associated up to complex conjugation. The next theorem follows from the results in [6, c. 18 Thm 4, Thm 5].

Theorem 5.1. *Let $p \geq 5$ be a prime integer. Consider the family (2) (resp. (3)) of elliptic curves over $\mathbb{F}_p$, whose endomorphism ring is isomorphic to $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[\zeta]$).*

Then in $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[\zeta]$) there are exactly 4 (resp. 6) different complex numbers representing the Frobenius endomorphism of precisely $\frac{p-1}{4}$ (resp. $\frac{p-1}{6}$) curves of the family (2) (resp. (3)).

Furthermore, if τ_1 and τ_2 represent the Frobenius endomorphisms for some elliptic curves of type (2) (or type (3)), then either τ_1 is associated to τ_2, or τ_1 is associated to $\overline{\tau}_2$.

6. The unit group of $\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta]$

The unit group $(\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta])^*$ of the quotient ring $\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta]$ consists of all residue classes modulo τ^w that are not divisible by τ in $\mathbb{Z}[\delta]$. Therefore we can obtain a reduced residue system modulo τ^w by choosing, along with 0, one representative of each residue class modulo τ^w not divisible by τ. This reduced residue system modulo τ^w can serve as a digit set for a w-NAF τ-adic recoding of integers.

In this section we shall study the structure of $(\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta])^*$.

First of all, we notice that for fixed p, due to Theorem 5.1, the values of the Frobenius endomorphism of different curves in the same family give rise to the same (up to isomorphism) quotient ring $\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta]$, for any $w \geq 1$.

In general, if α and β are associated in $\mathbb{Z}[\delta]$, then $\alpha\mathbb{Z}[\delta] = \beta\mathbb{Z}[\delta]$ and therefore

$$\mathbb{Z}[\delta]/\alpha\mathbb{Z}[\delta] = \mathbb{Z}[\delta]/\beta\mathbb{Z}[\delta]\,.$$

This applies precisely to our case, where τ represents one of the two complex solutions of the characteristic equation $\tau^2 - t\tau + p = 0$. It makes no difference which root we choose as basis for integer expansion. Thus we can select τ's in such a way that they are all associated to one another. In this way, the quotient ring $\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta]$, and thus the resulting digit set, is the same (up to isomorphism) for all curves in the same family (2) or (3) and the same characteristic.

Furthermore, since $\mathrm{N}(\tau) = p$ is a prime integer, τ is prime in $\mathbb{Z}[\delta]$, i.e. if $\tau \mid cd$ then $\tau \mid c$ or $\tau \mid d$ for all $c, d \in \mathbb{Z}[\delta]$.

Lemma 6.1. *Let $n \in \mathbb{Z}$. Then $\tau \mid n$ in $\mathbb{Z}[\delta]$ if and only if $p \mid n$ in $\mathbb{Z}$.*

Proof. Since $\tau\overline{\tau} = p$, we have that $\tau \mid p$ in $\mathbb{Z}[\delta]$. Therefore, if $p \mid n$ in $\mathbb{Z}$, then $\tau \mid n$ in $\mathbb{Z}[\delta]$.

Conversely, suppose $\tau \mid \alpha$ with $\alpha \in \mathbb{Z}[\delta]$. Then $\alpha = \tau\beta$ for some $\beta \in \mathbb{Z}[\delta]$. Thus $\mathrm{N}(\alpha) = \mathrm{N}(\tau) \cdot \mathrm{N}(\beta)$, and therefore $\mathrm{N}(\tau) \mid \mathrm{N}(\alpha)$ in $\mathbb{Z}$. In particular, suppose $n \in \mathbb{Z}$ and $\tau \mid n$ in $\mathbb{Z}[\delta]$. Then $p = \mathrm{N}(\tau) \mid \mathrm{N}(n) = n^2$. Hence $p \mid n$ in $\mathbb{Z}$. □

Lemma 6.2. *We have $\tau \nmid \overline{\tau}$ in $\mathbb{Z}[\delta]$.*

Proof. Let $\tau = a + b\delta$ for some a, $b \in \mathbb{Z}$. First, we notice that $b \not\equiv 0 \mod p$. In fact, suppose $b = pk$ for some $k \in \mathbb{Z}$. Then

$$0 \equiv \tau = a + pk\delta \equiv a \mod \tau .$$

Since $a \in \mathbb{Z}$, $a \equiv 0 \mod p$, say $a = ph$ for some $h \in \mathbb{Z}$. Thus we have a contradiction:

$$p = \mathrm{N}(\tau) = \mathrm{N}(ph + pk\delta) = \mathrm{N}(p)\,\mathrm{N}(h + k\delta) \geq p^2 .$$

Now consider $\overline{\tau} = a + b\overline{\delta}$. Then

$$\begin{aligned} \overline{\tau} = \tau - b\delta + b\overline{\delta} \equiv 0 \mod \tau \Leftrightarrow \\ -b\delta + b\overline{\delta} = b(\overline{\delta} - \delta) \equiv 0 \mod \tau . \end{aligned}$$

But $b \not\equiv 0 \mod p$, and then $b \not\equiv 0 \mod \tau$ by Lemma 6.1. Also, $\delta \not\equiv \overline{\delta} \mod \tau$ by Lemma 4.1. Since τ is prime, $b(\overline{\delta} - \delta) \not\equiv 0 \mod \tau$. Hence $\tau \nmid \overline{\tau}$. □

Lemma 6.3. *Let $n \in \mathbb{Z}$. For any $w \in \mathbb{N}$,*

$$p^w \mid n \text{ in } \mathbb{Z} \;\Leftrightarrow\; \tau^w \mid n \text{ in } \mathbb{Z}[\delta] .$$

Proof. Since $p^w = \tau^w \overline{\tau}^w$, we have $\tau^w \mid p^w$ in $\mathbb{Z}[\delta]$. Suppose $n \in \mathbb{Z}$ and $p^w \mid n$. Then $\tau^w \mid n$ in $\mathbb{Z}[\delta]$.

Conversely, we proceed by induction on w.

$w = 1$: already proved in Lemma 6.1.

Suppose that $\tau^w \mid n \;\Rightarrow\; p^w \mid n$ for some $w > 1$.

If $\tau^{w+1} \mid n$, then $\tau^w \mid n$, and therefore $p^w \mid n$ in $\mathbb{Z}$ by induction hypothesis. If w is *not* the maximal power of p that divides n, then clearly $p^{w+1} \mid n$. Suppose w is the maximal power of p that divides n. Since $\tau^{w+1} \mid n$ and $\tau^{w+1} \mid p^{w+1}$, it follows that

$$\tau^{w+1} \mid \gcd(n, p^{w+1}) = p^w = \tau^w \overline{\tau}^w .$$

Then it must be $\tau \mid \overline{\tau}$, but this is impossible by Lemma 6.2.

□

Lemma 6.3 yields an injective ring homomorphism

$$\mathbb{Z}/p^w\mathbb{Z} \hookrightarrow \mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta] .$$

These rings have the same cardinality, because the number of residue classes modulo τ^w in $\mathbb{Z}[\delta]$ is $\mathrm{N}(\tau^w) = p^w$. Hence we obtain a ring isomorphism

$$\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta] \cong \mathbb{Z}/p^w\mathbb{Z} ,$$

and then an isomorphism of unit groups

$$(\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta])^* \cong (\mathbb{Z}/p^w\mathbb{Z})^* \tag{8}$$

for any $w \in \mathbb{N}$, $w \geq 1$.

The unit group is cyclic and has order $\varphi(p^w) = (p-1)p^{w-1}$, where φ is Euler's totient function. Note that for $w = 1$, $\mathbb{Z}[\delta]/\tau\mathbb{Z}[\delta] \cong \mathbb{Z}/p\mathbb{Z}$ is a field with p elements.

Consider $p = 7$. The unit group $(\mathbb{Z}[\zeta]/\tau^w\mathbb{Z}[\zeta])^*$ has order $6 \cdot 7^{w-1}$ and we can split it into the direct product of a cyclic subgroup of order 6 and a cyclic subgroup

of order 7^{w-1}. We want to find a generator for each subgroup. Actually, we already know an element of order 6: one of the two primitive 6-th roots of unity ζ or $\overline{\zeta}$.

Similarly, let $p = 5$. The unit group $(\mathbb{Z}[i]/\tau^w\mathbb{Z}[i])^*$ has order $4 \cdot 5^{w-1}$. Again, we want to split it into the direct product of a cyclic subgroup of order 4, namely $\langle i \rangle$, and a cyclic subgroup of order 5^{w-1}.

In both cases it is possible to obtain a direct product because the orders of the subgroups are coprime. Our next goal is finding an element of order p^{w-1}. We shall prove that $\tau + 1$ is a canonical choice suitable for every p and every w.

Proposition 6.4. *For any integer $w \geq 1$, $\tau + 1$ is an element of order p^{w-1} in $(\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta])^*$.*

The proof of this proposition follows the idea of the proof that $p + 1$ has order p^{w-1} modulo p^w, for any $w \geq 1$ (cf. [6, c. 4 Cor. 2] for instance).

Proof. By induction on w.

For $w = 1$, clearly $\tau + 1 \equiv 1 \mod \tau$ and has order 1.

Suppose that for some $w \geq 1$

$$(\tau + 1)^{p^{w-1}} = 1 + a(w)\tau^w$$

for some $a(w) \in \mathbb{Z}[\delta]$ such that $\tau \nmid a(w)$.

Then

$$\begin{aligned}
(\tau + 1)^{p^w} &= (1 + a(w)\tau^w)^p \\
&= 1 + pa(w)\tau^w + \binom{p}{2} a(w)^2\tau^{2w} + \cdots + a(w)^p\tau^{pw} \\
&= 1 + pa(w)\tau^w + ph_2a(w)^2\tau^{2w} + \cdots + a(w)^p\tau^{pw} \\
&= 1 + \overline{\tau}a(w)\tau^{w+1} + \overline{\tau}h_2a(w)^2\tau^{2w+1} + \cdots + a(w)^p\tau^{pw} \\
&= 1 + \tau^{w+1}\left(a(w)\overline{\tau} + h_2a(w)^2\overline{\tau}\tau^w + \cdots + a(w)^p\tau^{(p-1)w-1}\right) .
\end{aligned}$$

Here $h_2 = \frac{p-1}{2}$ is such that $p \cdot h_2 = \binom{p}{2}$.

Let $a(w+1) = a(w)\overline{\tau} + h_2a(w)^2\overline{\tau}\tau^w + \dots$. Then

$$(\tau + 1)^{p^w} = 1 + a(w+1)\tau^{w+1} \equiv 1 \mod \tau^{w+1}$$

and

$$a(w+1) \equiv a(w)\overline{\tau} \mod \tau .$$

But $\tau \nmid a(w)$ and $\tau \nmid \overline{\tau}$ (cf. Lemma 6.2). Since τ is prime in $\mathbb{Z}[\delta]$, we conclude that $\tau \nmid a(w+1)$.

This proves that the order of $\tau + 1 \bmod \tau^{w+1}$ is p^b with $b \leq w$, that implies

$$1 \equiv (\tau + 1)^{p^b} \mod \tau^{w+1} .$$

Suppose $b < w$. Then

$$\begin{aligned}
1 &\equiv \left((\tau + 1)^{p^b}\right)^{p^{w-1-b}} \mod \tau^{w+1} \\
&= (\tau + 1)^{p^{w-1}} \\
&\equiv 1 + a(w)\tau^w \mod \tau^{w+1} .
\end{aligned}$$

Then $a(w)\tau^w \equiv 0 \mod \tau^{w+1}$, but $\tau \nmid a(w)$, so we have a contradiction. □

Remark. As an elliptic curve endomorphism, $\tau + 1$ is quite efficient to compute, as it requires only one elliptic curve addition, along with one application of the Frobenius endomorphism, which takes negligible time.

Hence, we have just obtained the following

Theorem 6.5. *For any integer $w \geq 1$*

$$(\mathbb{Z}[i]/\tau^w\mathbb{Z}[i])^* = \langle i \rangle \times \langle \tau + 1 \rangle \quad \text{for } p = 5\,,$$
$$(\mathbb{Z}[\zeta]/\tau^w\mathbb{Z}[\zeta])^* = \langle \zeta \rangle \times \langle \tau + 1 \rangle \quad \text{for } p = 7\,.$$

For $w = 1$, the subgroup $\langle \tau + 1 \rangle$ is trivial.

With the help of this theorem, we will now proceed with the construction of a digit set for a w-NAF τ-adic integer recoding in characteristic 7 and 5 (actually, they work quite similarly). In both cases we will also give an algorithm for elliptic curve scalar multiplication.

7. Characteristic $p = 7$

Let $p = 7$ and let us begin with a τ-adic expansion of window size $w = 1$.

In order to build a digit set $\mathcal{D}_1$, in addition to 0, we have to choose a representative for each nonzero residue class mod τ, i.e. elements of the unit group

$$(\mathbb{Z}[\zeta]/\tau\mathbb{Z}[\zeta])^* = \{\pm 1, \pm\zeta, \pm\zeta^2\} = \langle \zeta \rangle\,,$$

or equivalently $(\mathbb{Z}[\zeta]/\tau\mathbb{Z}[\zeta])^* = \{\pm 1, \pm\omega, \pm\omega^2\}$. Hence the digit set will be

$$\mathcal{D}_1 = \{0, \pm 1, \pm\zeta, \pm\zeta^2\}\,.$$

One advantage of using roots of unity as digits is that they all have norm equal to 1, and they are the only elements of $\mathbb{Z}[\zeta]$ with such a property. Hence, the 6-th roots of unity provide (unique) representatives of minimal norm for each nonzero residue class modulo τ. This implies that $\mathcal{D}_1$ is a (unique) MNR (Minimal Norm Representative) digit set, and thus it yields a finite τ-adic recoding for every integer, or equivalently $\mathcal{D}_1$ is a 1-NADS (cf. Theorem 4.4).

Another advantage of $\mathcal{D}_1$ is that, as elliptic curve endomorphisms, the 6-th roots of unity are very efficient to compute, as each of them requires one field multiplication only (see Section 2).

Now we wish to construct a w-NAF integer recoding for any window size $w \geq 1$. By Theorem 6.5, we know that

$$(\mathbb{Z}[\zeta]/\tau^w\mathbb{Z}[\zeta])^* = \langle \zeta \rangle \times \langle \tau + 1 \rangle$$

where $\tau + 1$ has order 7^{w-1}.

Then the digit set will be

$$\mathcal{D}_w = \{0\} \cup \{\, \zeta^r(\tau + 1)^s \mid 0 \leq r < 6,\ 0 \leq s \leq 7^{w-1} - 1 \,\}\,.$$

It follows that if an element $\eta \in \mathbb{Z}[\zeta]$ has a finite $\mathcal{D}_w$-τ-adic recoding, then η can be written as

$$\eta = \sum_{j=0}^{l-1} \varepsilon_j (\tau + 1)^{s_j} \tau^j$$

where $\varepsilon_j = 0$ or $\varepsilon_j = \zeta^r$ for $0 \le r < 6$ and $0 \le s_j \le 7^{w-1} - 1$.

However, for $w > 1$ we cannot ensure that every element in $\mathbb{Z}[\zeta]$ has a finite τ-adic recoding. In other words, we do not know whether $\mathcal{D}_w$ is w-NADS or not. To overcome this problem, in [3, §3.2.1] the authors suggest to step down the window size w in Algorithm 1 for the rest of the computation, whenever the following holds:

$$|z| \le \frac{|z| + |d_l|}{|\tau^w|} ,$$

or equivalently,

$$|d_l| \ge |z| \left(|\tau^w| - 1\right) . \tag{9}$$

In order to apply this workaround, $\mathcal{D}_w$ must fulfil the following requirements: for some $1 \le k < w$

- there exists a sequence of reduced residue systems $\mathcal{D}_k \subseteq \mathcal{D}_{k+1} \subseteq \cdots \subseteq \mathcal{D}_w$ modulo $\tau^k, \tau^{k+1}, \ldots, \tau^w$ respectively;
- $\mathcal{D}_k$ is a k-NADS.

It is clear that in our case $\mathcal{D}_v \subseteq \mathcal{D}_{v+1}$ for all $v = 1, \ldots, w-1$. Moreover, $\mathcal{D}_1 = \{0, \pm 1, \pm\zeta, \pm\zeta^2\}$ is a 1-NADS.

Algorithm 2 is a modified version of Algorithm 1 where a control step has been added (cf. [3, §3.2.1, Alg.6] with small adjustments): if (9) holds, the algorithm reduces the window size w and tries again until (9) is false, or $v = k$; at this point we use the fact that $\mathcal{D}_k$ is a k-NADS.

Algorithm 2 Windowed τ-adic recoding with guaranteed termination

Input: n, $w \in \mathbb{N}$, basis τ, reduced residue systems $\mathcal{D}_k \subseteq \mathcal{D}_{k+1} \subseteq \cdots \subseteq \mathcal{D}_w$ modulo $\tau^k, \tau^{k+1}, \ldots, \tau^w$ respectively s.t. $\mathcal{D}_k$ is a k-NADS for some $1 \le k < w$.
Output: $n = \sum_{j=0}^{l-1} d_j \tau^j$

1: $z := n$
2: $l := 0$
3: $v := w$
4: **while** $z \neq 0$ **do**
5: **if** $z \equiv 0 \bmod \tau$ **then**
6: $d_l := 0$
7: **else**
8: let $d_l \in \mathcal{D}_v$ s.t. $d_l \equiv z \bmod \tau^v$
9: **if** $|d_l| \ge |z|(|\tau^v| - 1)$ and $v > k$ **then**
10: $v := v - 1$
11: go to step 8
12: **end if**
13: **end if**
14: $z := \frac{z - d_l}{\tau}$
15: $l := l + 1$
16: **end while**
17: **return** $(\langle d_{l-1}, \ldots, d_0 \rangle, l)$

Now we are ready to implement an efficient algorithm for scalar multiplication. Let $E : y^2 = x^3 + B$, $B \neq 0$, be an elliptic curve over $\mathbb{F}_7$. We can regard E as a curve over $\mathbb{F}_{7^m}$ for any $m \geq 1$. Let n be an integer, $P \in E(\mathbb{F}_{7^m})$; suppose n has the following w-NAF τ-adic recoding:

$$n = \sum_{j=0}^{l-1} \varepsilon_j (\tau + 1)^{s_j} \tau^j \,.$$

Algorithm 3 shows how to compute nP; it is a variant of [7, Alg. 4], with small modifications. It consists of two nested Horner schemes: the outer one loops on the exponent of $\tau + 1$, whilst the inner one loops on the exponent of τ. For window size $w = 1$, the outer loop vanishes. It is worth noting that this algorithm requires no precomputation at all.

Algorithm 3 Scalar multiplication ($p = 7$)

Input: curve E, point $P = (x, y)$, scalar $n = \sum_{j=0}^{l-1} \varepsilon_j (\tau + 1)^{s_j} \tau^j$
Output: nP

$R := O$
for $j = 7^{w-1} - 1$ down to 0 **do**
  $R := (\tau + 1)R$
  $S := O$
  for $k = l - 1$ down to 0 **do**
    $S := \tau S$
    if $\varepsilon_k \neq 0$ and $s_k = j$ **then** ▷ $\varepsilon_k = \zeta^r$ with $0 \leq r \leq 5$
      switch r
      case 0: $S := S + (x, y)$
      case 1: $S := S + (u^2 x, -y)$
      case 2: $S := S + (v^2 x, y)$
      case 3: $S := S + (x, -y)$
      case 4: $S := S + (u^2 x, y)$
      case 5: $S := S + (v^2 x, -y)$
    end if
  end for
  $R := R + S$
end for
return R

Example 7.1. Let $\mathcal{E}$ be an elliptic curve in characteristic 7 defined over $\mathbb{F}_{7^m}$ and given by the equation

$$\mathcal{E} : y^2 = x^3 - 1 \,,$$

whose endomorphism ring is isomorphic to $\mathbb{Z}[\zeta]$. The Frobenius endomorphism of $\mathcal{E}$

$$\tau : (x, y) \mapsto \left(x^7, y^7\right)$$

has trace $t = 4$ and satisfies the characteristic equation $\tau^2 - 4\tau + 7 = 0$. Therefore

$$\tau = 2 + \sqrt{-3} = 1 + 2\zeta \,.$$

The actions on $\mathcal{E}$ of the 6-th roots of unity are

$$[\zeta] : (x, y) \mapsto (4x, -y) \qquad [\overline{\zeta}] : (x, y) \mapsto (2x, -y)$$
$$[\omega] : (x, y) \mapsto (2x, y) \qquad [\overline{\omega}] : (x, y) \mapsto (4x, y) .$$

By Theorem 6.5 we have that for any $w \geq 1$

$$(\mathbb{Z}[\zeta]/\tau^w\mathbb{Z}[\zeta])^* = \langle\zeta\rangle \times \langle\tau + 1\rangle .$$

For instance,

$$\mathcal{D}_1 = \{0, \pm 1, \pm\zeta, \pm\zeta^2\}$$
$$\mathcal{D}_2 = \{0,\ \pm 1,\ \pm\zeta,\ \pm\zeta^2,\ \pm(\tau+1),\ \pm\zeta(\tau+1),\ \pm\zeta^2(\tau+1), \ldots$$
$$\ldots,\ \pm(\tau+1)^6,\ \pm\zeta(\tau+1)^6,\ \pm\zeta^2(\tau+1)^6\} .$$

As an example, consider $n = 10$. A base-τ expansion of n with digit set $\mathcal{D}_1$ is

$$10 = \zeta + \zeta^2\tau + \zeta^2\tau^2 + \zeta^4\tau^3 ,$$

whilst a 2-NAF τ-adic recoding of n with digit set $\mathcal{D}_2$ is

$$10 = \zeta(\tau + 1)^3 - \tau^2 - \tau^4 .$$

8. Characteristic $p = 5$

Let $p = 5$. The discussion is analogous to the case $p = 7$.

By Theorem 6.5, for any $w \geq 1$

$$(\mathbb{Z}[i]/\tau^w\mathbb{Z}[i])^* = \langle i\rangle \times \langle\tau + 1\rangle$$

where $\tau + 1$ has order 5^{w-1}.

In particular, for window size $w = 1$, $(\mathbb{Z}[i]/\tau\mathbb{Z}[i])^* = \langle i\rangle$.

Therefore the digit set will be

$$\mathcal{D}_w = \{0\} \cup \{\, i^r(\tau+1)^s \mid\ 0 \leq r < 4,\ 0 \leq s \leq 5^{w-1} - 1 \,\} .$$

It follows that if an element $\eta \in \mathbb{Z}[i]$ admits a finite $\mathcal{D}_w$-τ-adic recoding, then η can be written as

$$\eta = \sum_{j=0}^{l-1} \varepsilon_j(\tau+1)^{s_j}\tau^j$$

where $\varepsilon_j = 0$ or $\varepsilon_j = i^r$ for $0 \leq r < 4$, and $0 \leq s_j \leq 5^{w-1} - 1$.

We cannot guarantee that every element in $\mathbb{Z}[i]$ has a finite w-NAF τ-adic recoding, i.e. we do not know if $\mathcal{D}_w$ is a w-NADS. However, $\mathcal{D}_w$ satisfies the requirements of Algorithm 2, hence we can step down the window size whenever it is necessary; eventually $\mathcal{D}_1 = \{0, \pm 1, \pm i\}$ is a 1-NADS.

Finally, let us turn to scalar multiplication. Let $E : y^2 = x^3 + Ax$, $A \neq 0$, be an elliptic curve over $\mathbb{F}_5$. We can regard E as a curve over $\mathbb{F}_{5^m}$ for any $m \geq 1$.

Algorithm 4 describes how to compute nP for any point $P \in E(\mathbb{F}_{5^m})$ and any integer n with w-NAF τ-adic recoding: $n = \sum_{j=0}^{l-1} \varepsilon_j(\tau+1)^{s_j}\tau^j$.

Basically, this algorithm works as Algorithm 3 and as [7, Alg. 4] with minor adjustments; no precomputation is required.

Algorithm 4 Scalar multiplication ($p = 5$)

Input: curve E, point $P = (x, y)$, scalar $n = \sum_{j=0}^{l-1} \varepsilon_j (\tau + 1)^{s_j} \tau^j$
Output: nP

$R := O$
for $j = 5^{w-1} - 1$ down to 0 **do**
  $R := (\tau + 1)R$
  $S := O$
  for $k = l - 1$ down to 0 **do**
    $S := \tau S$
    if $\varepsilon_k \neq 0$ and $s_k = j$ **then** ▷ $\varepsilon_k = i^r$ with $0 \leq r \leq 3$
      switch r
      case 0: $S := S + (x, y)$
      case 1: $S := S + (-x, uy)$
      case 2: $S := S + (x, -y)$
      case 3: $S := S + (-x, -uy)$
    end if
  end for
  $R := R + S$
end for
return R

9. Characteristic $p \geq 13$

Now we consider prime numbers larger than 7, thus we will work in characteristic $p \geq 13$ (note that $11 \not\equiv 1 \mod 3$ and $11 \not\equiv 1 \mod 4$).

As before, we wish to split the unit group $(\mathbb{Z}[\delta]/\tau^w \mathbb{Z}[\delta])^*$ into a direct product of some convenient cyclic subgroups, whose orders must be coprime.

Recall that the order of the unit group is $(p-1)p^{w-1}$. It is clear that $p - 1$ and p^{w-1} are coprime, so we can always split the unit group into the direct product of a subgroup of order $p - 1$ and a subgroup of order p^{w-1}. We have already proven that the latter is $\langle \tau + 1 \rangle$ (cf. Proposition 6.4).

Furthermore, if $p \equiv 1 \mod 3$ (resp. $p \equiv 1 \mod 4$), then $p - 1 = 6 \cdot k$ (resp. $p - 1 = 4 \cdot k$) for some $k \in \mathbb{N}$, $k \geq 1$. This means that the subgroup of order $p - 1$ contains a subgroup of order 6 (resp. 4) generated by ζ (resp. i). For $p = 5$ and $p = 7$ the description of the unit group is complete at this point (i.e. $k = 1$). Instead, for larger primes, we also have a non-trivial subgroup of order $k > 1$.

Let us begin with $p \equiv 1 \mod 3$.

Thus $p - 1 = 6 \cdot k$ for some $k \in \mathbb{N}$, $k > 1$. We wish to keep the subgroup $\langle \zeta \rangle$ of order 6, so that we do not lose the computational advantage of the 6-th roots of unity. Therefore we shall restrict ourselves to those primes such that k is coprime to 6. This means

$$p \not\equiv 1 \mod 4 \quad \text{and} \quad p \not\equiv 1 \mod 9\,,$$

which yields

$$p \equiv 31 \mod 36 \quad \text{or} \quad p \equiv 7 \mod 36\,. \tag{10}$$

Some prime numbers congruent to 31 modulo 36 are: 31, 67, 103, 139, 211.

Whereas some primes congruent to 7 modulo 36 are: 7, 43, 79, 151, 223.

Now consider $p \equiv 1 \mod 4$. Then $p - 1 = 4 \cdot k$ for some $k \in \mathbb{N}$, $k > 1$. As before, we shall restrict ourselves to those primes such that k is coprime to 4. In other words

$$p \not\equiv 1 \mod 8 ,$$

that leads to

$$p \equiv 5 \mod 8 . \tag{11}$$

Some prime numbers of this form are: 5, 13, 29, 37, 53, 61.

For the sake of simplicity, let $d = 4$ when $\delta = i$, or $d = 6$ when $\delta = \zeta$. Therefore $k = (p-1)/d$.

Let $w \in \mathbb{N}$, $w \geq 1$. Suppose that, for p as in (10) or (11), we have found an element $\sigma_w \in \mathbb{Z}[\delta]$ of order k modulo τ^w. Hence

$$(\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta])^* = \langle\delta\rangle \times \langle\sigma_w\rangle \times \langle\tau + 1\rangle .$$

In general, we may not find a canonical choice for σ_w, as we did with $\tau + 1$. In fact, fixed p, an element of order k modulo τ^w in general has not order k modulo τ^{w+1}. Therefore σ_w depends on both the characteristic p and the window size w.

The problem with the corresponding digit set

$$\mathcal{D}_w = \{0\} \cup \{\, \delta^r {\sigma_w}^s (\tau+1)^t \mid \ 0 \leq r < d,\ 0 \leq s < k,\ 0 \leq t < p^{w-1} \,\}$$

is that the requirements of Algorithm 2 are generally not satisfied:

(1) in general $\langle\sigma_v\rangle \not\subseteq \langle\sigma_{v+1}\rangle$, thus $\mathcal{D}_v \not\subseteq \mathcal{D}_{v+1}$;
(2) we cannot tell a priori if $\mathcal{D}_1$ is a 1-NADS.

The second problem can be dealt with by means of Theorem 3.1 on a case-by-case basis; cf. Tables 1 and 2 at the end of this section.

Concerning the first problem, we can solve it by providing a different factorisation of the unit group. The next proposition is a general case of [5, Lemma 1.4.5]; we partially follow the original proof.

Proposition 9.1. *Let p be an odd prime number, let $m \neq 1$ be an element of order d modulo p. Then m has order $d \cdot p^{a-1}$ modulo p^a for all $a \geq 1$, unless $m^d \equiv 1 \mod p^2$; in this case $m + p$ has order $d \cdot p^{a-1}$ modulo p^a for all $a \geq 1$.*

Proof. Suppose $m^d \not\equiv 1 \mod p^2$. We have to prove the following:

(1) $m^{dp^{a-1}} \equiv 1 \mod p^a$ for all $a \geq 1$;
(2) let l be a prime such that $l \mid d$; then $m^{\frac{d}{l}p^{a-1}} \not\equiv 1 \mod p^a$ for all $a \geq 1$;
(3) $m^{dp^{a-2}} \not\equiv 1 \mod p^a$ for all $a \geq 2$.

(1) By induction on a.

For $a = 1$, obviously $m^d \equiv 1 \mod p$.

Suppose $m^{dp^{a-2}} \equiv 1 \mod p^{a-1}$ for some $a \geq 2$, that is $m^{dp^{a-2}} = 1 + cp^{a-1}$ for some $c \in \mathbb{Z}$. Then

$$m^{dp^{a-1}} = (1 + cp^{a-1})^p = 1 + cp^a + \binom{p}{2} c^2 p^{2(a-1)} + \cdots \equiv 1 \mod p^a .$$

(2) Let g be a primitive root mod p. Then

$$m \equiv g^{\frac{p-1}{d}h} \mod p$$

for some $1 \le h \le d$ such that $\gcd(h,d) = 1$. Thus

$$m^{\frac{d}{l}p^{a-1}} \equiv g^{(p-1)\frac{h}{l}p^{a-1}} \equiv g^{(p-1)\frac{h}{l}} \not\equiv 1 \mod p$$

because h/l is not an integer. In fact, if $l \mid h$, since $l \mid d$, then $l \mid \gcd(h,d) = 1$. Therefore $m^{\frac{d}{l}p^{a-1}} \not\equiv 1 \mod p^a$ for all $a \ge 1$.

(3) By induction on a.
If $a = 2$, we already know that $m^d \not\equiv 1 \mod p^2$.

Suppose $m^{dp^{a-3}} \not\equiv 1 \mod p^{a-1}$ for some $a \ge 2$. It is easy to see that if p is an odd prime and $x^p \equiv 1 \mod p^a$, then $x \equiv 1 \mod p^b$ for all $b < a$. In our case, if $m^{dp^{a-2}} \equiv 1 \mod p^a$ for some $a \ge 2$, then $m^{dp^{a-3}} \equiv 1 \mod p^b$ for all $b < a$, which contradicts the induction hypothesis.

Lastly, suppose $m^d \equiv 1 \mod p^2$. Then

$$\begin{aligned}(m+p)^d &= m^d + dm^{d-1}p + \binom{d}{2}m^{d-2}p^2 + \dots \\ &\equiv 1 + dm^{d-1}p \not\equiv 1 \mod p^2\end{aligned}$$

since $p \nmid m$ and $p \nmid d$ (because $d < p$). It is immediate to see that (1)-(2)-(3) hold for $m + p$ in place of m.

□

As a consequence of Proposition 9.1 and the group isomorphism (8) we have

Corollary 9.2. *Let $\sigma \in \mathbb{Z}[\delta]$ be an element of order k modulo τ.*
If $\sigma^k \not\equiv 1 \mod \tau^2$, then σ is an element of order $k \cdot p^{w-1}$ modulo τ^w for all $w \ge 1$. Otherwise, if $\sigma^k \equiv 1 \mod \tau^2$, then $\sigma + \tau$ is an element of order $k \cdot p^{w-1}$ modulo τ^w for all $w \ge 1$.

Therefore we have obtained the following

Theorem 9.3. *Let $w \in \mathbb{N}$, $w \ge 1$. Let $\sigma \in \mathbb{Z}[\delta]$ be an element of order k modulo τ.*
If $\sigma^k \not\equiv 1 \mod \tau^2$, then

$$(\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta])^* = \langle\delta\rangle \times \langle\sigma\rangle\,. \tag{12}$$

In this case σ has order $k \cdot p^{w-1}$ modulo τ^w.

Otherwise $\sigma + \tau$ has order $k \cdot p^{w-1}$ modulo τ^w, and then

$$(\mathbb{Z}[\delta]/\tau^w\mathbb{Z}[\delta])^* = \langle\delta\rangle \times \langle\sigma+\tau\rangle\,. \tag{13}$$

It is worth noting that the generator σ (or $\sigma+\tau$) does not depend on the window size w. In the case (12), for any $w \ge 1$ the digit set is

$$\mathcal{D}_w = \{0\} \cup \{\, \delta^r\sigma^s \mid 0 \le r < d,\ 0 \le s \le kp^{w-1} - 1 \,\}\,.$$

If $\eta \in \mathbb{Z}[\delta]$ admits a finite $\mathcal{D}_w$-τ-adic recoding, then η can be written as

$$\eta = \sum_{j=0}^{l-1} \varepsilon_j \sigma^{s_j} \tau^j$$

where $\varepsilon_j = 0$ or $\varepsilon_j = \delta^r$ for $0 \le r < d$, and $0 \le s_j \le kp^{w-1} - 1$.

Whereas, in the case (13), we simply replace σ by $\sigma+\tau$. In both cases it is clear that $\mathcal{D}_v \subseteq \mathcal{D}_{v+1}$ for all $v \geq 1$.

Algorithm 5 shows how to compute nP when p satisfies (11), in particular $p \equiv 1 \bmod 4$, so that the 4-th roots of unity act as elliptic curve endomorphisms. It works basically like Algorithm 4; here σ is applied instead of $\tau+1$. When p satisfies (10), it suffices to change the switch routine with the one in Algorithm 3. Finally, if σ has not the desired order modulo τ^2, then we take $\sigma+\tau$ in place of σ (we still call it σ in the algorithm).

Algorithm 5 Scalar multiplication ($p \geq 13$)

Input: curve E, point $P=(x,y)$, scalar $n = \sum_{j=0}^{l-1} \varepsilon_j \sigma^{s_j} \tau^j$
Output: nP

$R := O$
for $j = kp^{w-1} - 1$ down to 0 **do**
  $R := \sigma R$
  $S := O$
  for $h = l-1$ down to 0 **do**
    $S := \tau S$
    if $\varepsilon_h \neq 0$ and $s_h = j$ **then** ▷ $\varepsilon_h = i^r$ with $0 \leq r \leq 3$
      switch r
      case 0: $S := S + (x, y)$
      case 1: $S := S + (-x, uy)$
      case 2: $S := S + (x, -y)$
      case 3: $S := S + (-x, -uy)$
    end if
  end for
  $R := R + S$
end for
return R

We still have to see whether $\mathcal{D}_1$ is a 1-NADS or not.

Example 9.1. In characteristic $p = 13$ we obtain again an MNR digit set for window size $w = 1$.

Recall that the unit group of $\mathbb{Z}[i]/\tau\mathbb{Z}[i]$ has order 12 and splits as

$$(\mathbb{Z}[i]/\tau\mathbb{Z}[i])^* = \langle i \rangle \times \langle \sigma \rangle$$

where σ has order 3 modulo τ. A generator of the second subgroup is either $1+i$ (for $\tau = -3+2i$ and associates) or $1-i$ (for $\overline{\tau}$ and associates). For instance, let $\tau = -3+2i$ and $\sigma = 1+i$. Then the corresponding digit set is

$$\begin{aligned}\mathcal{D}_1 &= \{\, 0,\, \pm 1,\, \pm i,\, \pm(1+i),\, \pm i(1+i),\, \pm(1+i)^2,\, \pm i(1+i)^2 \,\} \\ &= \{\, 0,\, \pm 1,\, \pm i,\, \pm(1+i),\, \pm(1-i),\, \pm 2i,\, \pm 2 \,\}\,.\end{aligned}$$

It is worth noting that $\mathcal{D}_1$ contains exactly all the elements of norm 0, 1, 2, 4 (there are no elements of norm 3 in the Gaussian integers). Hence $\mathcal{D}_1$ is a (unique) MNR digit set and thus Theorem 4.4 guarantees that every element of $\mathbb{Z}[i]$ has a finite $\mathcal{D}_1$-τ-adic expansion, i.e. $\mathcal{D}_1$ is a 1-NADS.

p	τ	unit group	$\left\lceil \frac{d_{max}}{(\sqrt{p}-1)^2} \right\rceil$	MNR digit set	1-NADS
5	$1+2i$	$\langle i\rangle$	1	yes	yes
13	$-3+2i$	$\langle i\rangle \times \langle 1+i\rangle$	1	yes	yes
29	$5+2i$	$\langle i\rangle \times \langle -1-i\rangle$	4	no	yes
37	$1+6i$	$\langle i\rangle \times \langle 1+i\rangle$	10	no	yes
53	$-7+2i$	$\langle i\rangle \times \langle 1-i\rangle$	104	no	yes
61	$5+6i$	$\langle i\rangle \times \langle 1-i\rangle$	354	no	yes
101	$1+10i$	$\langle i\rangle \times \langle 1-i\rangle$	204850	no	no
109	$-3+10i$	$\langle i\rangle \times \langle 2+i\rangle$	huge	no	no
149	$-7+10i$	$\langle i\rangle \times \langle -1+i\rangle$	547186713	no	no
157	$-11+6i$	$\langle i\rangle \times \langle 2+i\rangle$	huge	no	no
173	$13+2i$	$\langle i\rangle \times \langle 1+i\rangle$	29778077114	no	no
181	$9+10i$	$\langle i\rangle \times \langle -1+i\rangle$	113430097979	no	??
197	$1+14i$	$\langle i\rangle \times \langle -1-i\rangle$	1656430250748	no	no

TABLE 1. Digit set $\mathcal{D}_1$ in characteristic $p \equiv 1 \mod 4$, $p \not\equiv 1 \mod 8$. All values of τ correspond to the curve $E : y^2 = x^3 + x$ over $\mathbb{F}_p$, where $\mathrm{End}\,(E) \cong \mathbb{Z}[i]$.

Furthermore, note that

$$(1+i)^3 = -2+2i = 1+(-3+2i) = 1+\tau \not\equiv 1 \mod \tau^2\,,$$

so $1+i$ has order $3 \cdot 13^{w-1} \mod \tau^w$ for all $w \geq 1$, by Corollary 9.2. Hence, by Theorem 9.3 we have that, for any $w \geq 1$

$$(\mathbb{Z}[i]/\tau^w\mathbb{Z}[i])^* = \langle i\rangle \times \langle 1+i\rangle\,.$$

Although for larger primes $p > 13$, $\mathcal{D}_1$ is no longer an MNR digit set, yet there are some cases in which it is a 1-NADS. This can be verified by means of Theorem 3.1.

Results are displayed in Table 1 for some digit sets in the case of $\mathrm{End}\,(E) \cong \mathbb{Z}[i]$, and in Table 2 when $\mathrm{End}\,(E) \cong \mathbb{Z}[\zeta]$.

Example 9.2. Let $p = 101$. In this case $\mathcal{D}_1$ is not a 1-NADS. An integer that does not have a finite expansion to the basis $\tau = 1+10i$ is for instance 3 (starting from the left with the least significant digit):

$$\begin{aligned} 3 = \langle\, & i(1-i)^{13},\, i(1-i)^{21},\, -1,\, i(1-i)^{14},\, -(1-i)^{17},\, -1,\, -(1-i)^{10}, \\ & -i(1-i)^{13},\, -i(1-i)^{21},\, 1,\, -i(1-i)^{14},\, (1-i)^{17},\, 1,\, (1-i)^{10}, \\ & i(1-i)^{13},\, i(1-i)^{21},\, \ldots \rangle\,. \end{aligned}$$

Example 9.3. For $p = 181$, the norm bound of Theorem 3.1 seems quite large to be tested efficiently. Nevertheless, we have computed the $\mathcal{D}_1$-τ-adic expansion of all integers up to 33055, and no infinite expansion has arisen so far.

p	τ	unit group	$\left\lceil \frac{d_{max}}{(\sqrt{p}-1)^2} \right\rceil$	MNR digit set	1-NADS
7	$-3+2\zeta$	$\langle\zeta\rangle$	1	yes	yes
31	$-5+6\zeta$	$\langle\zeta\rangle \times \langle 2-\zeta\rangle$	4	no	yes

TABLE 2. Digit set $\mathcal{D}_1$ in characteristic $p = 7$, 31 for the curve $E : y^2 = x^3 + 1$ over $\mathbb{F}_p$, where $\mathrm{End}\,(E) \cong \mathbb{Z}[\zeta]$.

REFERENCES

[1] R. Avanzi and C. Heuberger. Faster and lower memory scalar multiplication on supersingular curves in characteristic three. In Catalano et al., editors, *PKC 2011*, LNCS 6571, pages 109–127. Springer, 2011.

[2] R. M. Avanzi, C. Heuberger, and H. Prodinger. Arithmetic of supersingular Koblitz curves in characteristic three. Technical Report 2010-8, Graz University of Technology, 2010. available at `http://www.math.tugraz.at/fosp/pdfs/tugraz_0166.pdf`.

[3] R. M. Avanzi, C. Heuberger, and H. Prodinger. Redundant τ-adic expansions I: Non-adjacent digit sets and their applications to scalar multiplication. *Designs, Codes and Cryptography*, 58(2):173–202, 2011.

[4] I. F. Blake, V. K. Murty, and G. Xu. Efficient algorithms for Koblitz curves over fields of characteristic three. *Journal of Discrete Algorithms*, 3(1):113–124, 2005.

[5] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1993.

[6] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, 2 edition, 1990.

[7] A. Kleinrahm. Arithmetic of subfield elliptic curves in small characteristic. Master's thesis, Ruhr-Universität Bochum, 2011.

[8] N. Koblitz. CM-curves with good cryptographic properties. In *Advances in Cryptology - CRYPTO '91 (Santa Barbara, CA, USA)*, LNCS 576, pages 279–287. Springer, 1992.

[9] N. Koblitz. An elliptic curve implementation of the finite field digital signature algorithm. In *Advances in Cryptology - CRYPTO '98 (Santa Barbara, CA, USA)*, LNCS 1462, pages 327–337. Springer, 1998.

[10] D. W. Matula. Basic digit sets for radix representation. *Journal of the Association for Computing Machinery*, 29(4):1131–1143, 1982.

[11] F. Morain and J. Olivos. Speeding up the computations on an elliptic curve using addition-subtraction chains. *Inform. Theor. Appl.*, 24:531–543, 1990.

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

[13] J. A. Solinas. An improved algorithm for arithmetic on a family of elliptic curves. In Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97 (Santa Barbara, CA, USA)*, LNCS 1294, pages 357–371. Springer, 1997.

[14] J. A. Solinas. Efficient arithmetic on Koblitz curves. *Designs, Codes and Cryptography*, 19:195–249, 2000.

CLEMENS HEUBERGER, INSTITUT FÜR MATHEMATIK, ALPEN-ADRIA-UNIVERSITÄT KLAGENFURT, UNIVERSITÄTSSTRASSE 65–67, 9020 KLAGENFURT AM WÖRTHERSEE, AUSTRIA

E-mail address: `clemens.heuberger@aau.at`

MICHELA MAZZOLI, INSTITUT FÜR MATHEMATIK, ALPEN-ADRIA-UNIVERSITÄT KLAGENFURT, UNIVERSITÄTSSTRASSE 65–67, 9020 KLAGENFURT AM WÖRTHERSEE, AUSTRIA

E-mail address: `michela.mazzoli@aau.at`