Symmetric Digit Sets for Elliptic Curve Scalar Multiplication

Clemens Heuberger    Michela Mazzoli

Alpen-Adria-Universität Klagenfurt, Austria

Istanbul, July 14, 2014
Outline

1. Introduction

2. Scalar multiplication and integer digit expansions

3. Symmetric digit sets
1 Introduction

2 Scalar multiplication and integer digit expansions

3 Symmetric digit sets
Elliptic Curves

An elliptic curve over the field $\mathbb{K}$ is a smooth algebraic curve with equation (in projective coordinates):

$$E : Y^2Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2Z + a_4 XZ^2 + a_6 Z^3$$

with coefficients $a_1, a_3, a_2, a_4, a_6 \in \mathbb{K}$.

There is only one point on the line at infinity: $\mathcal{O} = [0 : 1 : 0]$.

In affine coordinates (i.e. by substituting $x = X/Z$ and $y = Y/Z$):

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

$E(\mathbb{K})$ is the set of points $(x, y) \in \mathbb{K} \times \mathbb{K}$ that satisfy the equation of $E$, together with $\mathcal{O}$. 
Addition of points

Let \( P, Q \in E \). Let \( \ell \) be the line through \( P \) and \( Q \) (or the tangent line to \( E \) if \( P = Q \)), let \( R \) be the third intersection point of \( \ell \) with \( E \). Let \( \ell' \) be the line through \( R \) and \( O \). 

\( P + Q \) is the third intersection point of \( \ell' \) with \( E \).

- with point addition \( E(\mathbb{K}) \) is an Abelian group
- the neutral element is \( O \)
- if \( P = (x, y) \), then \( -P = (x, -y) \)
Addition and doubling formulae

If $\mathbb{K}$ has characteristic $p \geq 5$,

$$E : y^2 = x^3 + Ax + B \quad A, B \in \mathbb{K}$$

Let $P = (x_1, y_1), Q = (x_2, y_2) \in E \setminus \{O\}$ s.t. $Q \neq \pm P$ and $P \neq -P$

$$P + Q : \quad \tilde{x} = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2$$

$$\tilde{y} = -y_1 + \left( \frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - \tilde{x})$$

$$2P : \quad \tilde{x} = \left( \frac{3x_1^2 + A}{2y_1} \right)^2 - 2x_1$$

$$\tilde{y} = -y_1 + \left( \frac{3x_1^2 + A}{2y_1} \right) (x_1 - \tilde{x})$$
1 Introduction

2 Scalar multiplication and integer digit expansions

3 Symmetric digit sets
Fast elliptic curve scalar multiplication

Let $E$ be an elliptic curve over the finite field of prime characteristic $p$ used in discrete-logarithm-like public key cryptography.

Problem: given a positive integer $n$ and a point $P \in E$, find a fast algorithm to compute the scalar multiplication $nP = P + \cdots + P$.

One possible approach: take the binary expansion of $n$, then use a Horner scheme:

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

- number of additions: $\sim$ weight of expansion
- number of doublings: $\sim$ length of expansion
$w$-NAF expansion

Idea: reduce the number of additions by reducing the weight of the integer expansion.

A $w$-NAF (Non-Adjacent Form) expansion of $n \in \mathbb{Z}$ is an expansion s.t. in every block of $w$ consecutive digits there is at most one non-zero digit.

Example: standard binary expansion: $15 = (1, 1, 1, 1)$
2-NAF binary expansion: $15 = (1, 0, 0, 0, -1)$

Digit set for binary $w$-NAF:

$$D = \{0, \pm 1, \pm 3, \ldots, \pm (2^{w-1} - 1)\}$$

- if $n \equiv 0 \mod 2$, then $d = 0$
- else choose $d \in D$ s.t. $d \equiv n \mod 2^w \leadsto$ ensures $w - 1$ zeros
- repeat for $n := \frac{n-d}{2}$
Frobenius endomorphism

Idea: avoid (expensive) point doublings by using another base.

Every elliptic curve over a finite field of prime characteristic $p$ is equipped with the Frobenius endomorphism

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

$\tau$ requires only two field exponentiations $\sim$ very cheap!

Again, compute the scalar multiplication with Horner scheme

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

Some precomputation may be required ($d_j P$).
Computational cost of $\tau$-based Horner scheme

Suppose: $n \in \mathbb{Z}$ has a finite $\tau$-adic $w$-NAF expansion.

Scalar multiplication $nP$ with Horner scheme requires at runtime

$$(\text{wt}(n) - 1)A + (\text{len}(n) - 1)F \approx \text{wt}(n)A$$

[A = addition, F = Frobenius endomorphism]

Weight of a $w$-NAF expansion of $n$:

$$\text{wt}(n) \approx \frac{p - 1}{(p - 1)w + 1} \cdot \text{len}(n)$$
Density of $\tau$-adic $w$-NAF expansion

\[
density = \frac{\text{weight}}{\text{length}} = \frac{p - 1}{(p - 1)w + 1}
\]

<table>
<thead>
<tr>
<th></th>
<th>$w = 1$</th>
<th>$w = 2$</th>
<th>$w = 3$</th>
<th>$w = 4$</th>
<th>$w = 5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p = 2$</td>
<td>0.5</td>
<td>0.33333</td>
<td>0.25</td>
<td>0.2</td>
<td>0.16666</td>
</tr>
<tr>
<td>$p = 3$</td>
<td>0.66666</td>
<td>0.4</td>
<td>0.28571</td>
<td>0.22222</td>
<td>0.18181</td>
</tr>
<tr>
<td>$p = 5$</td>
<td>0.8</td>
<td>0.44444</td>
<td>0.30769</td>
<td>0.23529</td>
<td>0.19047</td>
</tr>
<tr>
<td>$p = 7$</td>
<td>0.85714</td>
<td>0.46153</td>
<td>0.31578</td>
<td>0.24</td>
<td>0.19354</td>
</tr>
<tr>
<td>$p = 11$</td>
<td>0.90909</td>
<td>0.47619</td>
<td>0.32258</td>
<td>0.24390</td>
<td>0.19607</td>
</tr>
<tr>
<td>$p = 13$</td>
<td>0.92307</td>
<td>0.48</td>
<td>0.32432</td>
<td>0.24489</td>
<td>0.19672</td>
</tr>
</tbody>
</table>
Frobenius endomorphism satisfies the characteristic equation

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

where $t = p + 1 - \#E(\mathbb{F}_p)$ is called trace and $N(\tau) = p$. We can represent $\tau$ as a root of the characteristic equation:

$$\tau = \frac{t \pm \sqrt{t^2 - 4p}}{2}$$

which is a non-real quadratic algebraic integer.

[Solinas 1997, Koblitz 1998]
Goal: find a \(w\)-NAF integer expansion to the complex basis \(\tau\) with a digit set \(D \subseteq \mathbb{Z}[\tau]\) (we allow complex digits).

Questions...

1. How to find a suitable digit set?

A \(w\)-NAF digit set \(D \subseteq \mathbb{Z}[\tau]\) is a reduced residue system mod \(\tau^w\), i.e. a set containing 0 and exactly one representative of each residue class mod \(\tau^w\) not divisible by \(\tau\).

2. Given \(n \in \mathbb{Z}\), does a finite \(\tau\)-adic \(w\)-NAF expansion of \(n\) always exist?

No, in general. It depends on the choice of the digit set!
Existence of finite $w$-NAF expansions

**Theorem**

Let $D_w$ be a reduced residue system for $w$-NAF $\tau$-adic expansion with $w \geq 1$. Let $d_{\text{max}} = \max \{N(d) \mid d \in D_w\}$. Then every element of $\mathbb{Z}[\tau]$ admits a finite expansion with the digit set $D_w$ if and only if for all $z \in \mathbb{Z}[\tau]$ s.t.

$$N(z) \leq \frac{d_{\text{max}}}{(|\tau^w| - 1)^2}$$

$z$ has a finite $D_w$-$\tau$-adic expansion.
MNR digit sets

One good choice for the digit set are the Minimal Norm Representatives (MNR) of each residue class mod $\tau^w$ coprime to $\tau$.

Theorem

Suppose $|\tau| > 2$, let $w \geq 1$. Let $\mathcal{D}_w$ be an MNR reduced residue system mod $\tau^w$. Then every element of $\mathbb{Z}[\tau]$ admits a finite $w$-NAF $\tau$-adic expansion with the digit set $\mathcal{D}_w$. 
1 Introduction

2 Scalar multiplication and integer digit expansions

3 Symmetric digit sets
Symmetric digit sets

Idea: find $w$-NAF digit sets for $\tau$-adic expansion invariant under the action of roots of unity.

We use two families of ordinary elliptic curves:

- $E : y^2 = x^3 + Ax$ with $A \in \mathbb{F}_p$, $A \neq 0$ and $p \equiv 1 \mod 4$; then $\text{End}(E) \approx \mathbb{Z}[i]$

- $E : y^2 = x^3 + B$ with $B \in \mathbb{F}_p$, $B \neq 0$ and $p \equiv 1 \mod 3$; then $\text{End}(E) \approx \mathbb{Z}[\zeta]$

where $\zeta = \frac{1 + \sqrt{-3}}{2}$ is a primitive sixth root of unity.
Symmetric digit sets

Today we focus on $\text{End}(E) \cong \mathbb{Z}[i]$ only.

In general $\mathbb{Z}[\tau] \subseteq \text{End}(E)$, but we work in the whole endomorphism ring to include the roots of unity.

The action of $i$ and $-i$ is very efficient to evaluate:

\[
i(x, y) = (-x, -uy)
\]
\[
-i(x, y) = (-x, uy)
\]

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

If a digit set $\mathcal{D}$ is invariant under the action of $i$, then it is necessary to precompute $dP$ for only $1/4$ of the digits $d \in \mathcal{D}$. 
Residue classes mod $\tau^w$

Recall: a $w$-NAF digit set contains 0 and exactly one representative of each residue class mod $\tau^w$ i.e. an element of the unit group $(\mathbb{Z}[i]/\tau^w \mathbb{Z}[i])^*$ of the quotient ring $\mathbb{Z}[i]/\tau^w \mathbb{Z}[i]$.

We are interested in the structure of the unit group:

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

which is a cyclic group of order $\varphi(p^w) = (p - 1)p^{w-1}$.

Recall: $N(\tau) = p$
Factorization of \((\mathbb{Z}[i]/\tau^w\mathbb{Z}[i])^*\)

We have assumed \(p \equiv 1 \mod 4\). Then \((p - 1)p^{w-1} = 4 \cdot k \cdot p^{w-1}\).
Therefore \((\mathbb{Z}[i]/\tau^w\mathbb{Z}[i])^*\) contains a subgroup of order 4:

\[
\langle i \rangle = \{\pm 1, \pm i\}
\]

Assume: \(p \not\equiv 1 \mod 8\), so that 4 and \(k\) are coprime.

**Theorem**

Let \(w \geq 1\). Let \(\sigma \in \mathbb{Z}[i]\) be an element of order \(k\) mod \(\tau\).
If \(\sigma^k \not\equiv 1 \mod \tau^2\), then \(\sigma\) has order \(k \cdot p^{w-1}\) mod \(\tau^w\) and therefore

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

Otherwise \(\sigma + \tau\) has order \(k \cdot p^{w-1}\) mod \(\tau^w\).

Important: the subgroup generators do not depend on \(w\).
Factored digit sets

The corresponding factored $w$-NAF digit set

$$D_w = \{0\} \cup \{ \pm \sigma^s, \pm i \sigma^s \mid 0 \leq s \leq k \cdot p^{w-1} - 1 \}$$

has also the property that $D_v \subseteq D_{v+1}$ for any $v \geq 1$.

- integer expansion: use a step-down-$w$ algorithm $\leadsto$ weak $w$-NAF
- a finite expansion is guaranteed if there exists $1 \leq \nu \leq w$ s.t. $D_\nu$ provides finite $\nu$-NAF expansion for every element of $\mathbb{Z}[i]$
- scalar multiplication computed via two nested Horner schemes: one loops on the exponent of $\tau$ (basis), the other loops on the exponent of $\sigma$
- no precomputation required!
Digit sets $\mathcal{D}_1$ for 1-NAF $\tau$-adic integer expansion

\[ p \equiv 1 \mod 4, \ E : y^2 = x^3 + x \]

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\tau$</th>
<th>unit group</th>
<th>MNR digit set</th>
<th>finite expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>$1 + 2i$</td>
<td>$\langle i \rangle$</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>13</td>
<td>$-3 + 2i$</td>
<td>$\langle i \rangle \times \langle 1 + i \rangle$</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>29</td>
<td>$5 + 2i$</td>
<td>$\langle i \rangle \times \langle -1 - i \rangle$</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>37</td>
<td>$1 + 6i$</td>
<td>$\langle i \rangle \times \langle 1 + i \rangle$</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>53</td>
<td>$-7 + 2i$</td>
<td>$\langle i \rangle \times \langle 1 - i \rangle$</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>61</td>
<td>$5 + 6i$</td>
<td>$\langle i \rangle \times \langle 1 - i \rangle$</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>101</td>
<td>$1 + 10i$</td>
<td>$\langle i \rangle \times \langle 1 - i \rangle$</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>109</td>
<td>$-3 + 10i$</td>
<td>$\langle i \rangle \times \langle 2 + i \rangle$</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>149</td>
<td>$-7 + 10i$</td>
<td>$\langle i \rangle \times \langle -1 + i \rangle$</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>157</td>
<td>$-11 + 6i$</td>
<td>$\langle i \rangle \times \langle 2 + i \rangle$</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>