Symmetric Digit Sets for Elliptic Curve Scalar Multiplication

Clemens Heuberger   Michela Mazzoli

Alpen-Adria-Universität Klagenfurt, Austria

Linz, 2013-11-15

Outline

1. Introduction
2. Complex Base
3. Symmetry

Elliptic Curve Cryptography

- Elliptic Curve E
- For $P \in E$ and $n \in \mathbb{Z}$, nP can be calculated easily.
- No efficient algorithm to calculate n from P and nP?
- Fast calculation of nP desirable!

Double-and-Add Algorithm

Calculating $27P$ via a doubling and adding scheme using the standard binary expansion of 27:

$$27 = (11011)_2 = 1 \cdot 16 + 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 \cdot 1,$$
$$27P = (11011)_2 P = 2(2(2(2(P) + P) + 0) + P) + P.$$

- Number of additions $\sim$ Hamming weight of the binary expansion (Number of nonzero digits)
- Number of doublings $\sim$ length of the expansion

Double, Add, and Subtract Algorithm

Subtraction is as cheap as addition!

$$27 = (100\bar{1}0\bar{1})_2, \qquad (\bar{1} := -1)$$

$$27P = (100\bar{1}0\bar{1})_2 P = 2(2(2(2(2(P) + 0) + 0) - P) + 0) - P.$$

- $\Longrightarrow$ Use of signed digit expansions
- Number of additions/subtractions $\sim$ Hamming weight of the binary expansion
- Number of multiplications $\sim$ length of the expansion

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT I WIEN GRAZ

Computation of the Standard Binary Expansion

Recall how to compute the standard unsigned binary expansion of 27 from right to left (least significant to most significant digit):

$$
\begin{aligned}
27 &\equiv 1 \pmod 2 & \varepsilon_0 &= 1\\
(27-1)/2 = 13 &\equiv 1 \pmod 2 & \varepsilon_1 &= 1\\
(13-1)/2 = 6 &\equiv 0 \pmod 2 & \varepsilon_2 &= 0\\
(6-0)/2 = 3 &\equiv 1 \pmod 2 & \varepsilon_3 &= 1\\
(3-1)/2 = 1 &\equiv 1 \pmod 2 & \varepsilon_4 &= 1\\
(1-1)/2 = 0 &\equiv 0 \pmod 2 & \varepsilon_j &= 0, \quad j \geq 5
\end{aligned}
$$

$$27 = (\ldots 011011)_2$$

Computation of Signed Expansion

Compute a signed binary expansion of 27 with many zeros:

$$
\begin{aligned}
27 &\equiv -1 \pmod 4 & \varepsilon_0 &= -1\\
(27-(-1))/2 = 14 &\equiv 0 \pmod 2 & \varepsilon_1 &= 0\\
(14-0)/2 = 7 &\equiv -1 \pmod 4 & \varepsilon_2 &= -1\\
(7-(-1))/2 = 4 &\equiv 0 \pmod 2 & \varepsilon_3 &= 0\\
(4-0)/2 = 2 &\equiv 0 \pmod 2 & \varepsilon_4 &= 0\\
(2-0)/2 = 1 &\equiv 1 \pmod 4 & \varepsilon_5 &= 1\\
(1-1)/2 = 0 &\equiv 0 \pmod 2 & \varepsilon_j &= 0, \quad j \geq 6
\end{aligned}
$$

$$27 = (\ldots 0100\bar{1}0\bar{1})_2$$

If n is odd, we use information modulo 4 instead of modulo 2 in order to guarantee a digit 0 in the next step. (Greedy!)

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Non-Adjacent Form

Theorem (Reitwiesner 1960)

Let $n \in \mathbb{Z}$, then there is exactly one signed binary expansion $\varepsilon \in \{-1, 0, 1\}^{\mathbb{N}_0}$ of n such that

$$n = \sum_{j \geq 0} \varepsilon_j 2^j, \qquad (\varepsilon \text{ is a binary expansion of } n),$$

$$\varepsilon_j \varepsilon_{j+1} = 0 \qquad \text{for all } j \geq 0.$$

It is called the Non-Adjacent Form (NAF) of n.
It minimises the Hamming weight amongst all signed binary expansions with digits $\{0, \pm 1\}$ of n.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

w-NAF

- Let $w \geq 2$. Consider digit set

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

- Binary digit expansion of $n \in \mathbb{Z}$ with digits in $\mathcal{D}_w$.
- Precompute ηP for $\eta \in \mathcal{D}_w$, $\eta > 0$.
- Minimise weight, i.e., number of nonzero digits.
- Choose expansion such that each block of w consecutive digits contains at most one non-zero digit ("w-NAF").
- NAF is special case $w = 2$.
- If n is even, take digit 0.
- If n is odd, take unique digit $\eta \in \mathcal{D}_w$ such that $n \equiv \eta \pmod{2^w}$.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT I WIEN GRAZ

Frobenius Endomorphism

- Let E be an elliptic curve defined over $\mathbb{F}_q$.
- The Frobenius endomorphism

$$\varphi : E(\mathbb{F}_{q^m}) \to E(\mathbb{F}_{q^m}); (x, y) \mapsto (x^q, y^q)$$

fulfils

$$\varphi^2 - t\varphi + q = 0$$

where $t = q + 1 - \#E(\mathbb{F}_q)$.

- As $|t| \leq 2\sqrt{q}$ (Hasse), φ can be identified with an imaginary quadratic integer τ.

τ-Expansions and Scalar Multiplication

- Assume that a digit expansion of n to the base of τ is known, e.g., $n = \sum_{j=0}^{\ell-1} c_j \tau^j$.
- Then

$$(c_{\ell-1}\tau^{\ell-1} + c_{\ell-2}\tau^{\ell-2} + c_{\ell-3}\tau^{\ell-3} + \cdots + c_1\tau + c_0)P = \varphi(\varphi(\varphi(\varphi(\varphi(c_{\ell-1}P) + c_{\ell-2}P) + c_{\ell-3}P) \cdots) + c_1 P) + c_0 P$$

- Frobenius-and-Add-Algorithm
- Frobenius endomorphism φ much faster than doubling
- Number of (fast) Frobenius applications: length of the expansion.
- Number of Additions/Subtractions: Hamming weight (number of nonzero digits) of the expansion (minus one).

$\mathcal{D}$-w-NAF with Base τ

- Aim: Generalise w-NAF to base τ.
- Digit set: $\mathcal{D} = \{0\} \cup \mathcal{D}^\bullet$ where $\mathcal{D}^\bullet$ consists of one representative of minimal norm from every residue class modulo τ^w which is not divisible by τ ("digit set of minimal norm representatives").
- A $\mathcal{D}$-w-NAF is an expansion of $z \in \mathbb{Z}[\tau]$ such that every block of w consecutive digits contains at most one non-zero digit.
- Questions:
  - Existence: Does every $z \in \mathbb{Z}[\tau]$ admit a $\mathcal{D}$-w-NAF?
  - Optimality: Does the $\mathcal{D}$-w-NAF minimise the weight over all expansions over the same digit set?
  - Analysis: Expected weight?

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

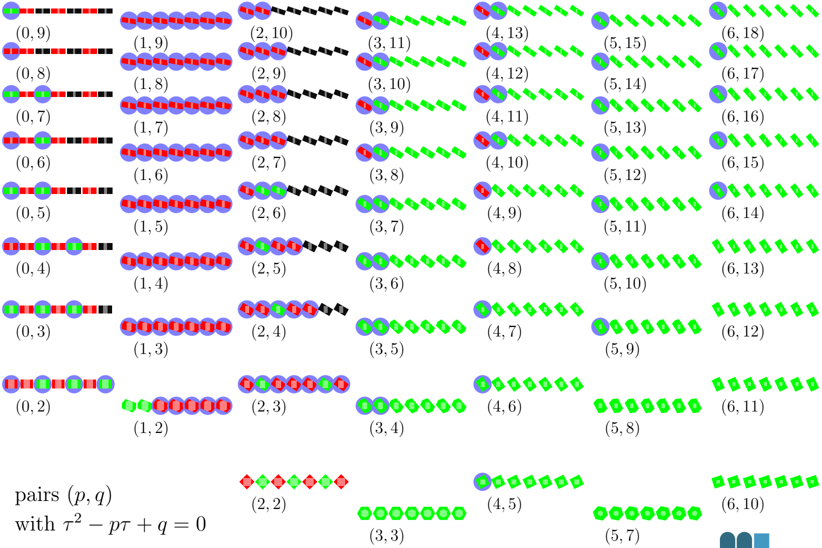
Existence of the w-NAF

Theorem (CH, Daniel Krenn 2013)

Let τ be an imaginary quadratic integer, $w \geq 2$ and $\mathcal{D}$ be a digit set of minimal norm representatives.
Then every element in $\mathbb{Z}[\tau]$ admits a w-NAF to the base of τ with digits in $\mathcal{D}$.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Optimality Results for Quadratic Integer Bases



pairs (p, q)
with $\tau^2 - p\tau + q = 0$

Digit Counting in w-NAFs to Imaginary Quadratic Bases

Theorem (CH, Daniel Krenn 2013)

Let τ be an imaginary quadratic integer, $w \geq 2$, $\mathcal{D}$ be a digit set of minimal norm representatives, $0 \neq \eta \in \mathcal{D}$ and $N > 0$.
Let $z \in \mathbb{Z}[\tau]$ with $|z| \leq N$ be a random element (under equidistribution).
Then the expected number of occurrences of the digit η in the $\mathcal{D}$-w-NAF of z is

$$e_w \log_{|\tau|} N + \psi_\eta(\log_{|\tau|} N) + o(1),$$

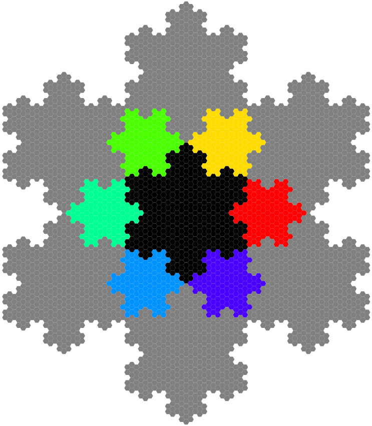
where

$$e_w = \frac{1}{|\tau|^{2(w-1)}((|\tau|^2 - 1)w + 1)},$$

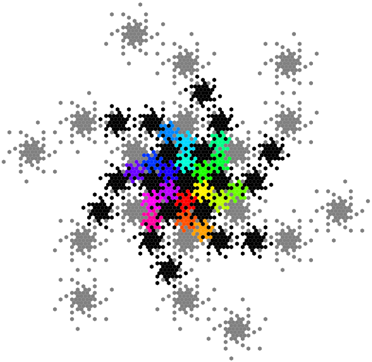
and $\psi_\eta(x)$ is a 1-periodic continuous function.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Characteristic Sets (1)

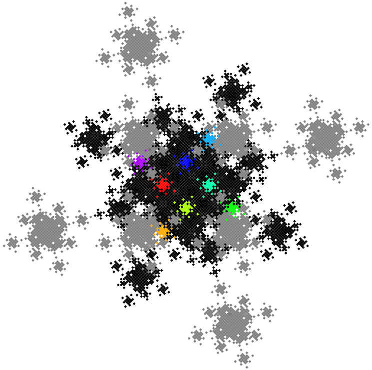


$\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$, $w = 2$

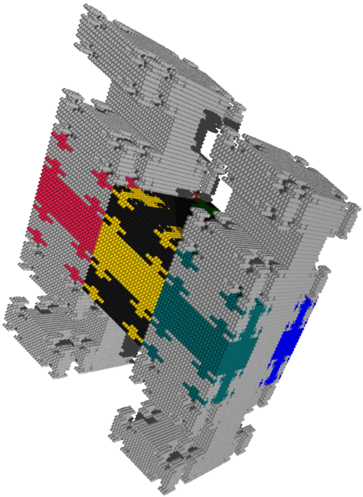


$\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$, $w = 3$

Characteristic Sets (2)



$\tau = 1 + i,\ w = 4$



$\tau = \sqrt[3]{-3},\ w = 2$

Curves

- $y^2 = x^3 + Ax$ over $\mathbb{F}_{p^m}$ with $p \equiv 1 \pmod 4$, $A \in \mathbb{F}_p^\times$.
  $\mathrm{End}(E) \simeq \mathbb{Z}[i]$.
- $y^2 = x^3 + B$ over $\mathbb{F}_{p^m}$ with $p \equiv 1 \pmod 6$, $B \in \mathbb{F}_p^\times$.
  $\mathrm{End}(E) \simeq \mathbb{Z}[\zeta]$ for a primitive sixth root of unity ζ.
- Ternary Koblitz curve: Defined over $\mathbb{F}_3$ by equation

  $$Y^2 = X^3 - X - \mu, \quad \text{with} \quad \mu \in \{\pm 1\}.$$

  Supersingular, hence interesting for pairing-based cryptography.
  Sixth roots of unity in endomorphism ring.

For this talk: focus on $y^2 = x^3 + Ax$.

Using Rotations to Reduce Precomputation

$y^2 = x^3 + Ax$ over $\mathbb{F}_{p^m}$, $p \equiv 1 \pmod 4$, $A \in \mathbb{F}_p^\times$.

- $$[\tau](x, y) = \varphi(x, y) = (x^p, y^p),$$
  $$[i](x, y) = (-x, -vy)$$
  where $v \in \mathbb{F}_p$ is an element of order 4.
- Choose digit set $\mathcal{D}$ such that $i\eta \in \mathcal{D}$ for each $\eta \in \mathcal{D}$, i.e., $\mathcal{D}$ is invariant under rotation.
- Only precompute ηP for one representative η of each orbit of $\mathcal{D}$ under rotation by i, generate $i^k \eta P$ on the fly.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Structural Digit Set

- Replace minimum norm digit set by a "structurally defined" digit set.
- Aim: Reduce precomputation/storage.
- Assume that $p \equiv 5 \pmod 8$.
- Write
$$(\mathbb{Z}[i]/\tau^w\mathbb{Z}[i])^\times \simeq \langle i \rangle \times \langle \sigma \rangle.$$
Here, σ is an element of order $(p-1)p^{w-1}/4$.
- σ can be determined modulo τ^2.
- Choose digit set
$$\mathcal{D} = \{0\} \cup \left\{ i^a \sigma^b \mid 0 \leq a < 4, 0 \leq b < \frac{(p-1)p^{w-1}}{4} \right\}.$$

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Structural Digit Set

- Is $\mathcal{D}$ a valid digit set, i.e., does every $z \in \mathbb{Z}[\tau]$ admit an expansion

$$z = \sum_{i=0}^{\ell} d_i \tau^i$$

  with $d_i \in \mathcal{D}$ and fulfilling the width-w non-adjacency condition?
- Algorithmically, this is not important:
- For the last "few" positions, we can simply relax the non-adjacency condition, dropping back to the case $w = 1$.
- This does not alter the asymptotic behaviour of the algorithms.

Using the Structural Digit Set

- Write $[\alpha]$ for the action of $\alpha \in \mathbb{Z}[i]$ as an endomorphism of E.
- Consider expansion

$$z = \sum_{j=0}^{\ell} \varepsilon_j \sigma^{b_j} \tau^j$$

of $z \in \mathbb{Z}[i]$ with $\varepsilon_j \in \{0, \pm 1, \pm i\}$.

- Write scalar multiplication as

$$zP = \sum_{j=0}^{\ell} \varepsilon_j \sigma^{b_j} \tau^j]P = \sum_{b=0}^{\frac{(p-1)p^{w-1}}{4}-1} \sum_{\substack{j=0 \\ b_j=b}}^{\ell} [\varepsilon_j][\tau]^j[\sigma]^b P.$$

- Here, $[\sigma]^b P$ is stored.

ALPEN-ADRIA UNIVERSITÄT
KLAGENFURT | WIEN GRAZ

Using the Structural Digit Set — Algorithm 1

Input: $P = (x, y) \in E(\mathbb{F}_{p^m})$, scalar $z = \sum_{j=0}^{\ell} \varepsilon_j \sigma^{b_j} \tau^j$
Output: zP

$Q \leftarrow 0$
for $b = (p-1)p^{w-1}/4 - 1$ **to** 0 **do**
  $Q \leftarrow [\sigma]Q$, $R \leftarrow 0$
  for $j = \ell$ **to** 0 **do**
    $R \leftarrow [\tau]R$
    if $\varepsilon_j \neq 0$ **and** $b_j = b$ **then**
      $R \leftarrow R + [\varepsilon_j](P)$
  $Q \leftarrow Q + R$
return Q

Algorithm 1: Comments

- No storage for precomputed points
- Many applications of τ
  - no problem when normal bases are used
  - for polynomial bases, we use the following variant (Algorithm 2)

Using the Structural Digit Set — Algorithm 2 (Variant)

Input: $P = (x, y) \in E(\mathbb{F}_{p^m})$, scalar $z = \sum_{j=0}^{\ell} \varepsilon_j \sigma^{b_j} \tau^j$
Output: zP

$Q \leftarrow 0$, $\hat{P} \leftarrow$ normal_basis(P)
for $b = (p-1)p^{w-1}/4 - 1$ **to** 0 **do**
  $Q \leftarrow [\sigma]Q$, $R \leftarrow 0$
  for $j = 0$ **to** ℓ **do**
    if $\varepsilon_j \neq 0$ **and** $b_j = b$ **then**
      $R \leftarrow R + [\varepsilon_j]$polynomial_basis$(\tau^j \hat{P})$
  $Q \leftarrow Q + R$
return Q

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Examples

p	τ	unit group	bound	MNR	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