Non-Adjacent Forms and their Playground

Daniel Krenn

Graz University of Technology, Austria

March 18, 2011

Introduction

Problem

- Let P be an element of a group, $n \in \mathbb{N}_0$.
- Calculate

$$nP = P + \cdots + P$$

as efficient as possible.

- double-and-add algorithm, e.g., $27 = (11011)_2$,

$$27P = 2(2(2(2(1P) + 1P) + 0) + 1P) + 1P$$

- double-add-and-subtract algorithm, e.g., $27 = (100\bar{1}0\bar{1})_2$,

$$27P = 2(2(2(2(1P) + 0) + 0) - 1P) + 0) - 1P$$

Introduction

Problem

- Let P be an element of a group, $n \in \mathbb{N}_0$.
- Calculate

$$nP = P + \cdots + P$$

as efficient as possible.

- double-and-add algorithm, e.g., $27 = (11011)_2$,

$$27P = 2(2(2(2(1P) + 1P) + 0) + 1P) + 1P$$

- double-add-and-subtract algorithm, e.g., $27 = (100\bar{1}0\bar{1})_2$,

$$27P = 2(2(2(2(2(1P) + 0) + 0) - 1P) + 0) - 1P$$

Introduction

Problem

- Let P be an element of a group, $n \in \mathbb{N}_0$.
- Calculate

$$nP = P + \cdots + P$$

as efficient as possible.

- double-and-add algorithm, e.g., $27 = (11011)_2$,

$$27P = 2(2(2(2(1P) + 1P) + 0) + 1P) + 1P$$

- double-add-and-subtract algorithm, e.g., $27 = (100\bar{1}0\bar{1})_2$,

$$27P = 2(2(2(2(2(1P) + 0) + 0) - 1P) + 0) - 1P$$

Non-Adjacent Form: Existence and Uniqueness

Theorem (Reitwiesner 1960)

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

$$z = \sum_{j \in \mathbb{N}_0} \xi_j 2^j, \quad (\xi \text{ is a binary expansion of } z),$$

and for all $j \geq 0$

$$\xi_j \xi_{j+1} = 0.$$

It is called the Non-Adjacent Form (NAF) of z.

Non-Adjacent Form: General Definition

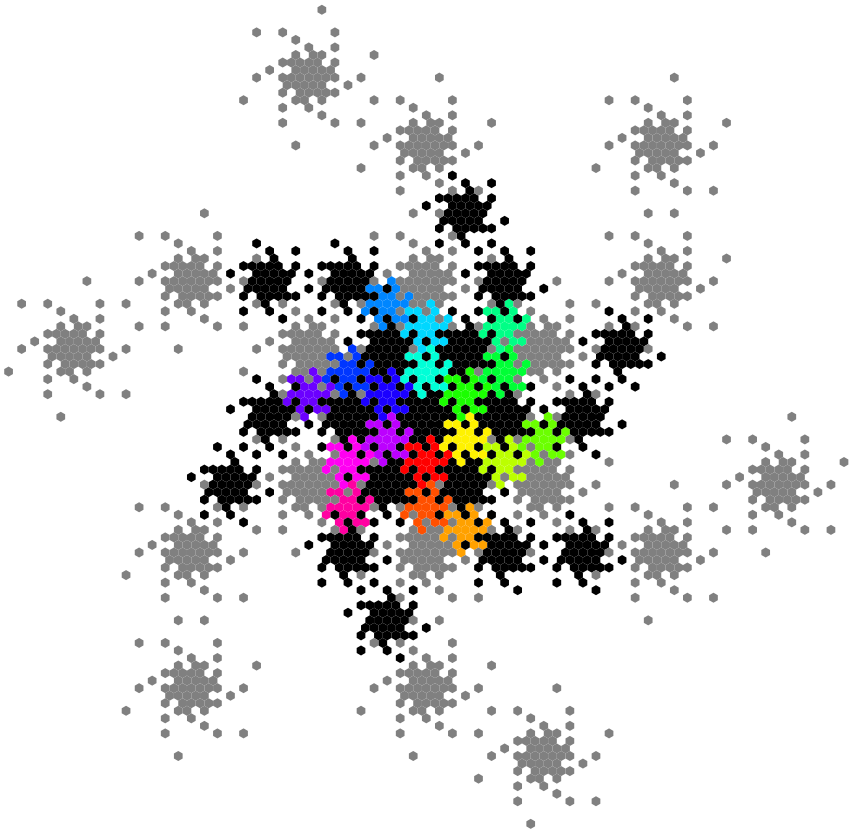


Figure: Values of 3-NAFs with MNR digit set and $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$.

- base τ
- digit set $\mathcal{D}$
- numbers

$$z = \sum_{j \in \mathbb{N}_0} \xi_j \tau^j =: (\boldsymbol{\xi})_\tau$$

  with digits $\xi_j \in \mathcal{D}$
- $w \in \mathbb{N}$ with $w \geq 2$
- $\boldsymbol{\xi}$ is a width-w non-adjacent form (short w-NAF), if each block of length w contains at most one non-zero.

Some Properties of w-NAFs

- base $\tau = 2$
- w-NAFs with digit set $\mathcal{D} = \{0, \pm 1, \pm 3, \ldots, \pm 2^{w-2}\}$

Theorem

Each integer has a unique w-NAF.

Proposition

The length of the w-NAF-expansion of an integer is at most one digit longer than its binary representation.

Optimality

- base τ, digit set $\mathcal{D}$
- expansions with digits out of $\mathcal{D}$
- (Hamming-)weight of an expansion is the number of its non-zero digits
- expansion of z is optimal, if it minimizes the weight among all expansions of z with digits out of $\mathcal{D}$

Theorem (Reitwiesner 1960)

Let $\tau = 2$ and $\mathcal{D} = \{-1, 0, 1\}$, then the 2-NAF of each integer is optimal.

Theorem (Avanzi 2004, Muir and Stinson 2004)

Let $\tau = 2$, $w \geq 2$ and $\mathcal{D} = \{0, \pm 1, \pm 3, \ldots, \pm 2^{w-2}\}$, then the w-NAF of each integer is optimal.

Optimality

- base τ, digit set $\mathcal{D}$
- expansions with digits out of $\mathcal{D}$
- (Hamming-)weight of an expansion is the number of its non-zero digits
- expansion of z is optimal, if it minimizes the weight among all expansions of z with digits out of $\mathcal{D}$

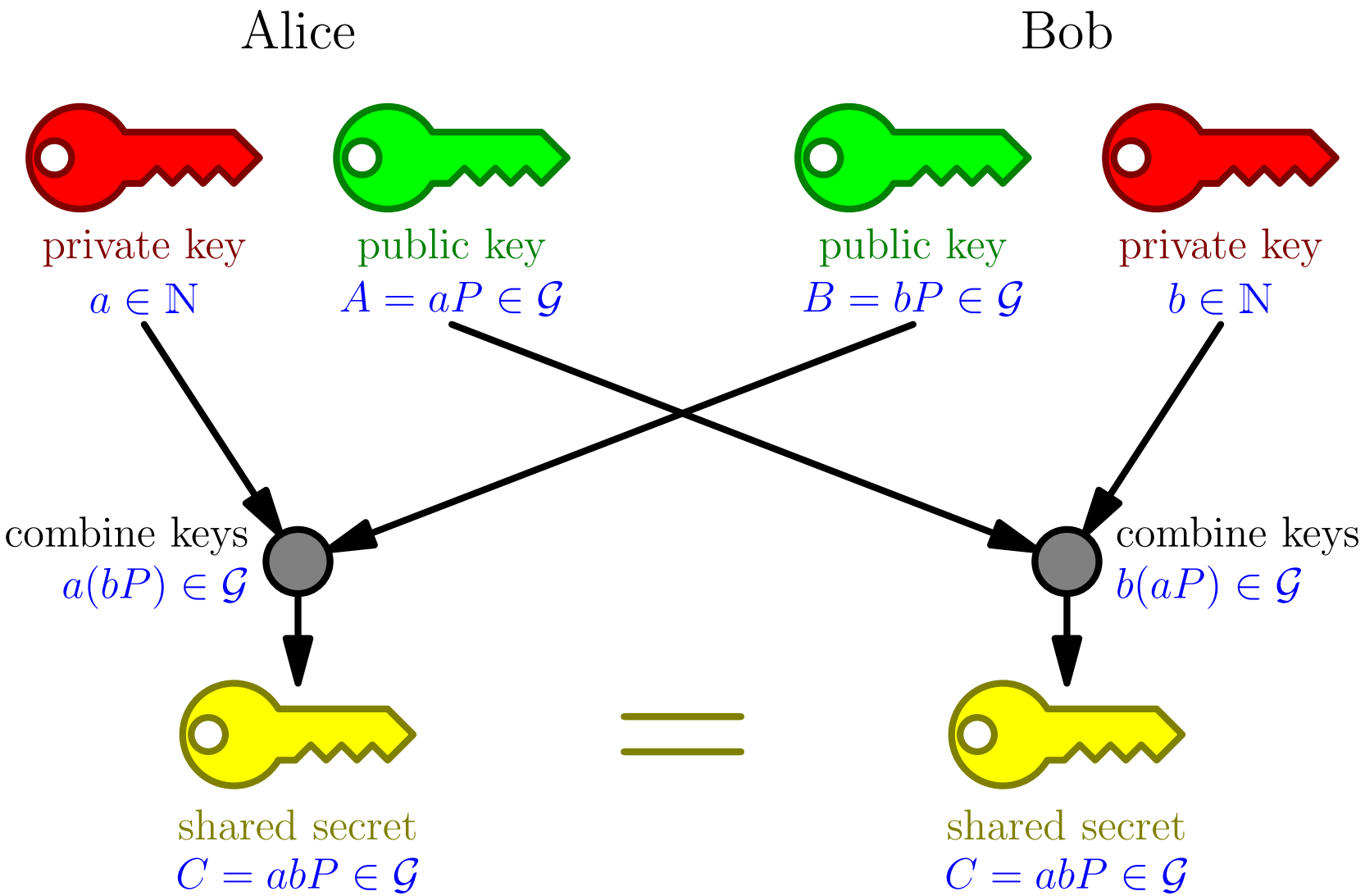
Theorem (Reitwiesner 1960)

Let $\tau = 2$ and $\mathcal{D} = \{-1, 0, 1\}$, then the 2-NAF of each integer is optimal.

Theorem (Avanzi 2004, Muir and Stinson 2004)

Let $\tau = 2$, $w \geq 2$ and $\mathcal{D} = \{0, \pm 1, \pm 3, \ldots, \pm 2^{w-2}\}$, then the w-NAF of each integer is optimal.

Application: Diffie-Hellman Key Exchange



Elliptic Curves over Finite Fields

Definition (Elliptic Curve $\mathcal{E}$)

- smooth algebraic curve of genus 1 defined over a field K
- together with a point $\mathbf{0}$ on the curve (identity)

- Example. Koblitz curve $\mathcal{E}_3 : Y^2 = X^3 - X - 1$ defined over $\mathbb{F}_3$
- interested in the group $\mathcal{E}(\mathbb{F}_{q^m})$ of rational points

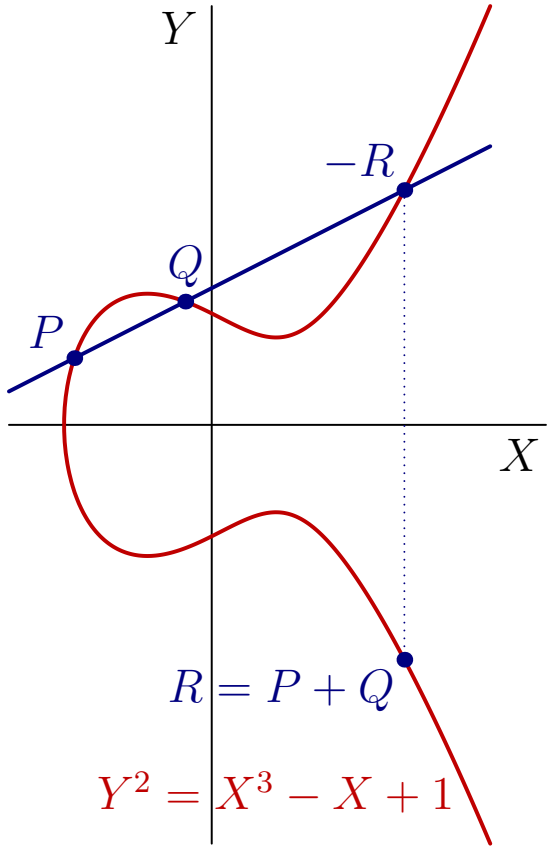


Figure: Elliptic curve $Y^2 = X^3 - X + 1$ over $\mathbb{R}$.

Frobenius-and-Add Method

- Frobenius endomorphism

$$\varphi : \mathcal{E}(\mathbb{F}_{q^m}) \longrightarrow \mathcal{E}(\mathbb{F}_{q^m}), \quad (x, y) \longmapsto (x^q, y^q)$$

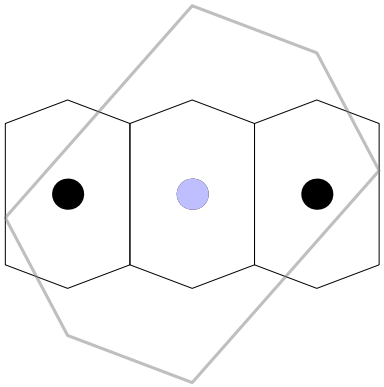
  satisfies a relation $\varphi^2 - p\varphi + q = 0$
- φ may be identified with an imaginary quadratic τ that is a solution of $\tau^2 - p\tau + q = 0$
- $z \in \mathbb{Z}[\tau]$, $P \in \mathcal{E}(\mathbb{F}_{q^m})$

Computation of the Action zP

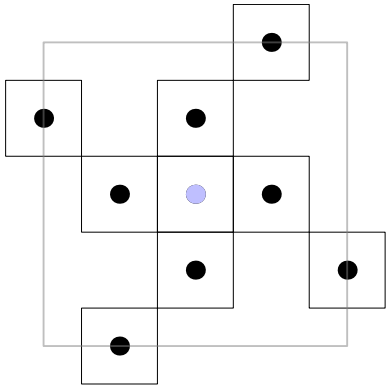
$$z = \sum_{j=0}^{\ell-1} z_j \tau^j \qquad \Longrightarrow \qquad zP = \sum_{j=0}^{\ell-1} z_j \, \varphi^j(P)$$

- calculation via a Horner scheme

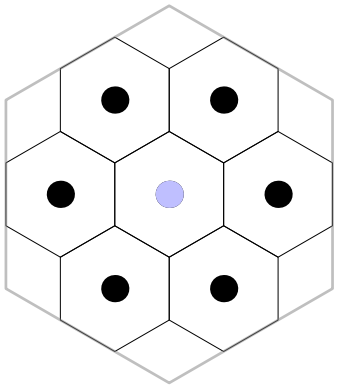
Digit Sets



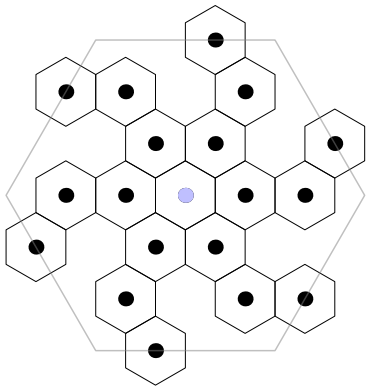
$\tau = \frac{1}{2} + \frac{1}{2}\sqrt{-7}$, $w = 2$



$\tau = 1 + \sqrt{-1}$, $w = 4$



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



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

Figure: Some digit sets modulo τ^w.

- base τ imaginary quadratic, algebraic integer
- $w \geq 2$
- reduced residue digit set
  - 0
  - exactly one representative for each residue class modulo τ^w not divisible by τ
- minimal norm digit set
  - taking minimal norm representatives

Existence and Uniqueness

- base τ imaginary quadratic, algebraic integer
- minimal norm representatives digit set modulo τ^w, $w \geq 2$

Theorem

Each element in $\mathbb{Z}[\tau]$ has a unique w-NAF-expansion.

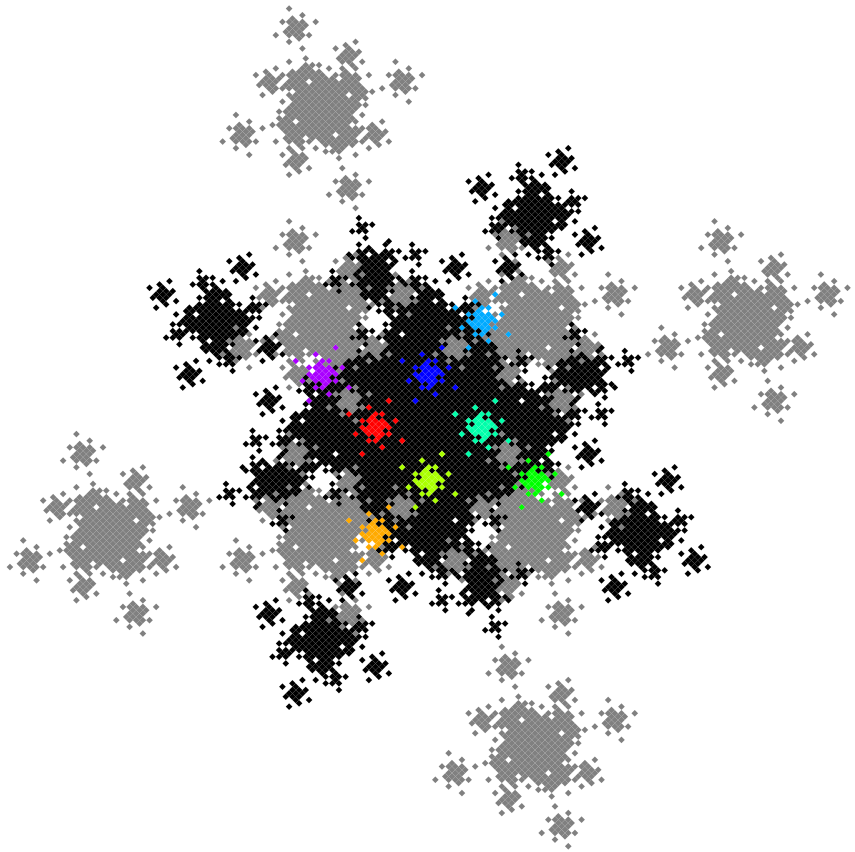


Figure: Values of 4-NAFs with MNR digit set and $\tau = 1 + i$.

Occurences of a non-zero Digit in a Region

Theorem (Heuberger and K. 2010)

- *base* τ *imaginary quadratic, algebraic integer with* $|\tau| > 1$
- *minimal norm representatives digit set* $\mathcal{D}$
- $0 \neq \eta \in \mathcal{D}$
- $N \in \mathbb{R}_{\geq 0}$
- *unit disc* $U := \mathcal{B}(0,1) \subseteq \mathbb{C}$

Then number of occurrences of the digit η *in the region* NU *is*

$$Z(N) = e_w \pi N^2 \log_{|\tau|} N + N^2 \psi\left(\log_{|\tau|} N\right) + o\left(N^2\right)$$

Sketch of Proof

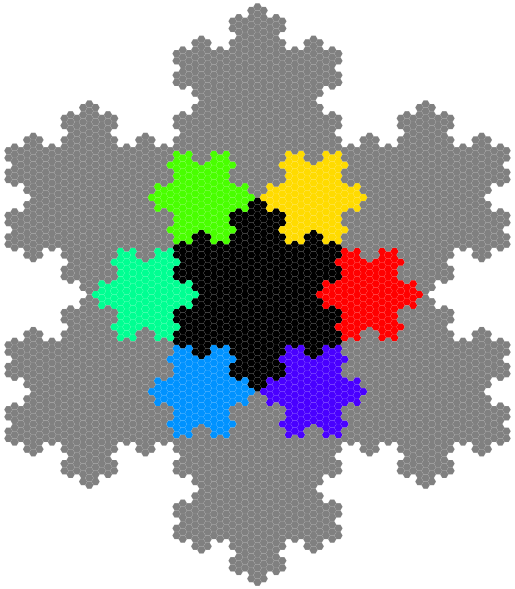


Figure: W_η for 2-NAFs with $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$.

- fixed digit η
- counting

$$Z(N) = \sum_{\substack{n \in NU \cap \mathbb{Z}[\tau] \\ \mathbf{n} = \mathrm{NAF}_w(n)}} \sum_{j \in \mathbb{N}_0} [\varepsilon_j(\mathbf{n}) = \eta]$$

- characteristic sets W_η, approximations $W_{\eta,j}$
- equivalent conditions
  - jth digit of $\mathbf{n}$ equals η
  - $\left\{\tau^{-(j+w)} n\right\}_{\mathbb{Z}[\tau]} \in W_{\eta,j}$
- rewriting the sum as integral

$$Z(N) = \frac{1}{\lambda(V)} \sum_{j=0}^{J} \int_{x \in NU} \mathbb{1}_{W_{\eta,j}} \left(\left\{ \frac{x}{\tau^{j+w}} \right\}_{\mathbb{Z}[\tau]} \right) \mathrm{d}x + \text{‘small’ error terms}$$

Optimality

- base τ is solution of $\tau^2 - \mu\tau + 2 = 0$, $\mu \in \{-1, 1\}$
- minimal norm representatives digit set modulo τ^w, $w \geq 2$
- (Hamming-)weight of an expansion is the number of its non-zero digits
- expansion of z is optimal, if it minimizes the weight among all expansions of z with digits out of $\mathcal{D}$

Theorem (Avanzi, Heuberger and Prodinger 2005, Gordon 1998)

Let $w \in \{2, 3\}$, then the w-NAF of each element of $\mathbb{Z}[\tau]$ is optimal.

Theorem (Heuberger 2010)

Let $w \in \{4, 5, 6\}$, then the w-NAF is not optimal.

Optimality

- base τ is solution of $\tau^2 - \mu\tau + 2 = 0$, $\mu \in \{-1, 1\}$
- minimal norm representatives digit set modulo τ^w, $w \geq 2$
- (Hamming-)weight of an expansion is the number of its non-zero digits
- expansion of z is optimal, if it minimizes the weight among all expansions of z with digits out of $\mathcal{D}$

Theorem (Avanzi, Heuberger and Prodinger 2005, Gordon 1998)

Let $w \in \{2, 3\}$, then the w-NAF of each element of $\mathbb{Z}[\tau]$ is optimal.

Theorem (Heuberger 2010)

Let $w \in \{4, 5, 6\}$, then the w-NAF is not optimal.

Optimality

- base τ is solution of $\tau^2 - p\tau + q = 0$, $p, q \in \mathbb{Z}$ with $q - p^2/4 > 0$
- minimal norm representatives digit set modulo τ^w, $w \geq 2$

Theorem (K. 2011)

If one of the conditions

- $w \geq 4$ *and* $|p| \geq 3$,
- $w = 3$ *and* $|p| \geq 5$

holds, then the w-NAF of each element of $\mathbb{Z}[\tau]$ *is optimal.*

Optimality-Map