# Non-adjacent Forms and their Playground

Daniel Krenn

Graz University of Technology, Austria

February 29, 2012

DOCTORAL PROGRAM DISCRETE MATHEMATICS

TU & KFU GRAZ · MU LEOBEN AUSTRIA

Supported by the Austrian Science Fund (FWF), projects W1230 and S9606.

# Overview

## Numbers

$$z = \sum_{j=0}^{\ell-1} \xi_j \tau^j$$

with base $\tau \in \mathbb{C}$ and digits $\xi_j$ in a digit set $\mathcal{D}$.

- digit set too large $\rightsquigarrow$ redundant representations
- want syntax on digits of $z$ to gain uniqueness

# Overview

## Numbers

$$z = \sum_{j=0}^{\ell-1} \xi_j \tau^j$$

with base $\tau \in \mathbb{C}$ and digits $\xi_j$ in a digit set $\mathcal{D}$.

- digit set too large $\rightsquigarrow$ redundant representations
- want syntax on digits of $z$ to gain uniqueness
- Questions:
  - Existence of representations?
  - How often does a digit occur?
  - Is the syntax the best possible syntax?

# Introduction

## Problem

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

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

as efficient as possible.

# Introduction

## Problem

- Let $P$ be an element of an Abelian group, $n \in \mathbb{N}_0$.
- Calculate
$$nP = P + \cdots + P$$
as efficient as possible.

- double-and-add algorithm, e.g., $29 = (11101)_2$,
$$29P = 2(2(2(2(1P) + 1P) + 1P) + 0) + 1P$$

# Introduction

## Problem

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

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

as efficient as possible.

- double-and-add algorithm, e.g., $29 = (11101)_2$,

$$29P = 2(2(2(2(1P) + 1P) + 1P) + 0) + 1P$$

- double-add-and-subtract algorithm, e.g., $29 = (100\bar{1}01)_2$,

$$29P = 2(2(2(2(2(1P) + 0) + 0) - 1P) + 0) + 1P$$

# Elliptic Curves over Finite Fields

## Elliptic Curve

$$E\colon y^2 = x^3 + ax + b$$

- Example. Koblitz curve

$$E_3\colon Y^2 = X^3 - X - 1$$

  defined over $\mathbb{F}_3$

- interested in the group

$$E(\mathbb{F}_{q^m})$$

  of rational points of $E$

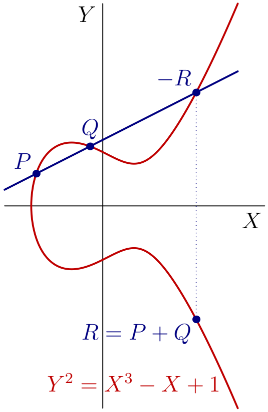



Figure: Elliptic curve $Y^2 = X^3 - X + 1$ over $\mathbb{R}$.

# Frobenius-and-Add Method

- $E(\mathbb{F}_{q^m})$ group of rational points of elliptic curve $E$ over a finite field
- Frobenius endomorphism

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

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

**Computation of the Action $zP$**

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

# Non-Adjacent Form: General Definition

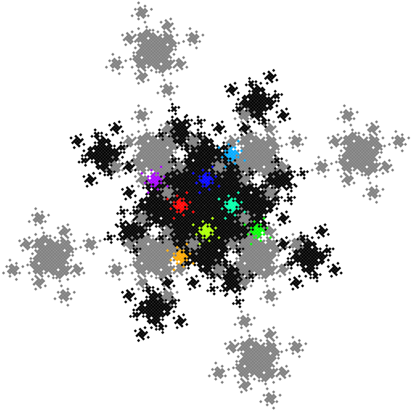


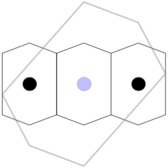
Figure: Values of 4-NAFs with MNR digit set and $\tau = 1 + i$.

- base $\tau$, digit set $\mathcal{D}$
- numbers

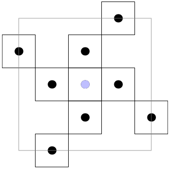
$$z = \sum_{j \in \mathbb{N}_0} \xi_j \tau^j =: (\boldsymbol{\xi})_\tau$$

  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.

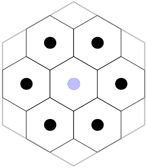
# Digit Sets



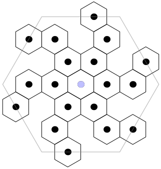
$\tau = \frac{1}{2} + \frac{1}{2}\sqrt{-7}$, $w = 2$



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



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



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

Figure: Some MNR digit sets.

- base $\tau$ imaginary quadratic, algebraic integer
- $w \geq 2$
- minimal norm representatives digit set modulo $\tau^w$
  - 0
  - exactly one representative of each residue class modulo $\tau^w$ not divisible by $\tau$ which has minimal norm

# Existence and Uniqueness

$\exists!$

Existence and uniqueness of the $w$-NAFs, $w \geq 2$, for

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

  (Reitwiesner 1960, Solinas 2000, Muir–Stinson 2006)
- - base $\tau$ is solution of $\tau^2 \pm \tau + 2 = 0$
  - minimal norm representatives digit set modulo $\tau^w$

  (Solinas 2000, Blake–Murty–Xu 2005)
- - base $\tau$ is solution of $\tau^2 \pm 3\tau + 3 = 0$
  - minimal norm representatives digit set modulo $\tau^w$

  (Koblitz 1998, Blake–Murty–Xu 2005)
- - base $\tau$ coming from Euclidean imaginary quadratic number field,
  - minimal norm representatives digit set modulo $\tau^w$

  (Blake–Murty–Xu 2008)

# Existence and Uniqueness

- base $\tau$ imaginary quadratic, algebraic integer with $|\tau| > 1$
- minimal norm representatives digit set modulo $\tau^w$, $w \geq 2$

**Theorem (Heuberger–K. 2010)**

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

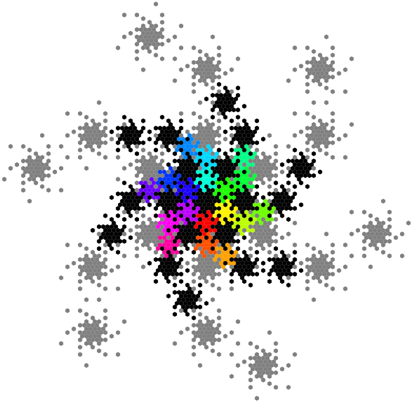


Figure: Values of 3-NAFs with MNR digit set and $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$.

# Occurences of a non-zero Digit in a Region

**Theorem (Heuberger–K. 2010)**

- *base $\tau$ 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 $\eta$ in all $w$-NAFs 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

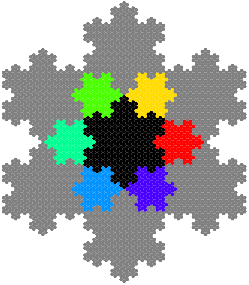


Figure: $W_\eta$ for 2-NAFs with $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$.

- based on Delange's method
- 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 $W_\eta$, approximations $W_{\eta,j}$
- equivalent conditions
  - $j$th digit of $\mathbf{n}$ equals $\eta$
  - $\left\{\tau^{-(j+w)} n\right\}_{\mathbb{Z}[\tau]} \in W_{\eta,j}$
- 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 $\tau$, 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 $\mathcal{D}$

# Optimality

- base $\tau$, 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–Stinson 2004)**

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

# Optimality

- base $\tau$ is solution of $\tau^2 - \mu\tau + 2 = 0$, $\mu \in \{-1, 1\}$
- minimal norm representatives digit set modulo $\tau^w$, $w \geq 2$

**Theorem (Avanzi–Heuberger–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 $\tau$ 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 $\tau^w$, $w \geq 2$

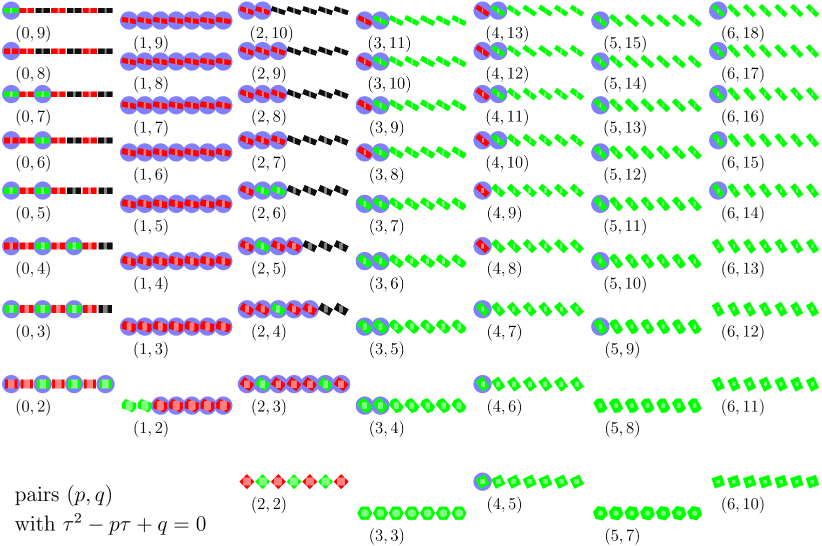
**Theorem (Heuberger–K. 2011)**

*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




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