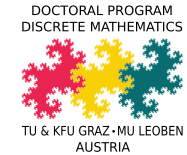
Counting Digits in Non-adjacent Forms in Conjunction with Hyperelliptic Curve Cryptography

Daniel Krenn

June 1, 2012



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

Introduction

- Abelian group $\mathcal{G}$, e.g.
  - point group of elliptic curve over a finite field
  - Jacobian of hyperelliptic curve over a finite field

Problem

For $P \in \mathcal{G}$ and $m \in \mathbb{N}_0$ calculate

$$mP = P + \cdots + P$$

as efficient as possible.

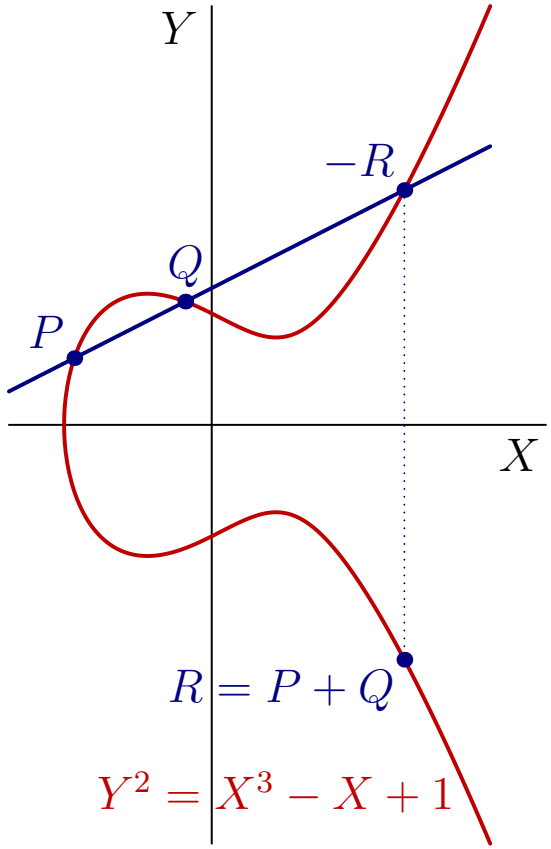


Figure: Elliptic curve $Y^2 = X^3 - X + 1$ over $\mathbb{R}$.

Scalar Multiplication

Problem

Calculate $mP = P + \cdots + P$ as efficient as possible.

Scalar Multiplication

Problem

Calculate $mP = P + \cdots + P$ as efficient as possible.

- double-and-add algorithm, e.g. $30 = (11110)_2$,

$$30P = 2(2(2(2(1P) + 1P) + 1P) + 1P) + 0$$

Scalar Multiplication

Problem

Calculate $mP = P + \cdots + P$ as efficient as possible.

- double-and-add algorithm, e.g. $30 = (11110)_2$,

$$30P = 2(2(2(2(1P) + 1P) + 1P) + 1P) + 0$$

- adding more digits, e.g. $30 = (3030)_2$ with $\mathcal{D} = \{0, \pm 1, \pm 3\}$,

$$30P = 2(2(2(3P) + 0) + 3P) + 0$$

$\rightsquigarrow$ windowing methods, non-adjacent form

Scalar Multiplication

Problem

Calculate $mP = P + \cdots + P$ as efficient as possible.

- double-and-add algorithm, e.g. $30 = (11110)_2$,

$$30P = 2(2(2(2(1P) + 1P) + 1P) + 1P) + 0$$

- adding more digits, e.g. $30 = (3030)_2$ with $\mathcal{D} = \{0, \pm 1, \pm 3\}$,

$$30P = 2(2(2(3P) + 0) + 3P) + 0$$

  $\rightsquigarrow$ windowing methods, non-adjacent form

- replace doublings (by something "cheaper")
  $\rightsquigarrow$ Frobenius-and-add method

Endomorphism-and-Add Method

- "cheap" endomorphism φ in group $\mathcal{G}$ which satisfies a characteristic polynomial χ
- e.g. Frobenius endomorphism on Jacobian $\rightsquigarrow$ Frobenius-and-add method
- φ corresponds to a zero τ of χ
- $z \in \mathbb{Z}[\tau]$, $P \in \mathcal{G}$

Computation of the Action zP

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

- calculation via a Horner scheme

The Non-Adjacent Form

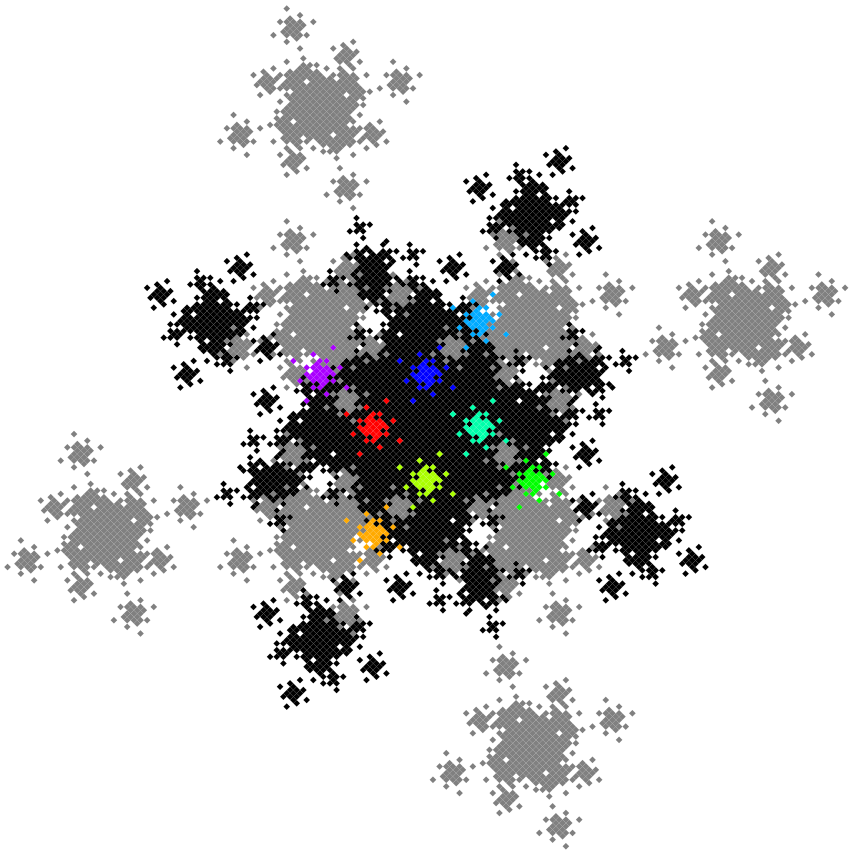


Figure: Values of 4-NAFs with MNR digit set and $\tau = 1 + i$.

- numbers

$$z = (z_J \dots z_1 z_0)_\tau$$

with digits $z_j \in \mathcal{D}$

- w positive integer
- $z_J \dots z_1 z_0$ is a width-w non-adjacent form (short w-NAF), if each block of length w contains at most one non-zero.

Typical Questions

Numbers

$$z = \sum_{j=0}^{J} z_j \tau^j = (z_J \dots z_1 z_0)_\tau$$

with τ algebraic integer, digits $z_j \in \mathcal{D}$, w-NAF $z_J \dots z_1 z_0$

- Existence of representations?
- Is the syntax the best possible syntax?
  $\rightsquigarrow$ optimal (minimal) expansions of z
- How often does a digit occur?
  $\rightsquigarrow$ runtime of scalar multiplication

Existence and Uniqueness

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 τ coming from Euclidean imaginary quadratic number field,
  - minimal norm representatives digit set modulo τ^w

  (Koblitz 1998, Solinas 2000, Blake–Murty–Xu 2005, Blake–Murty–Xu 2008)
- - base τ imaginary quadratic algebraic integer,
  - minimal norm representatives digit set modulo τ^w

  (Heuberger–DK 2010)

Lattices

- τ algebraic integer (zero of monic polynomial of degree n)
- order $\mathbb{Z}[\tau]$, number field $K = \mathbb{Q}[\tau]$
- $\sigma_1, \ldots, \sigma_s$ real embeddings of K,
  $\sigma_{s+1}, \overline{\sigma_{s+1}}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}}$ non-real complex embeddings,
- Minkowski map $\Sigma\colon K \to \mathbb{R}^n$ maps $\alpha \in K$ to

  $$(\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \Re\sigma_{s+1}(\alpha), \Im\sigma_{s+1}(\alpha), \ldots, \Re\sigma_{s+t}(\alpha), \Im\sigma_{s+t}(\alpha))$$

- lattice $\Lambda = \Sigma(\mathbb{Z}[\tau])$ in $\mathbb{R}^n$

Lattices

- τ algebraic integer (zero of monic polynomial of degree n)
- order $\mathbb{Z}[\tau]$, number field $K = \mathbb{Q}[\tau]$
- $\sigma_1, \ldots, \sigma_s$ real embeddings of K,
  $\sigma_{s+1}, \overline{\sigma_{s+1}}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}}$ non-real complex embeddings,
- Minkowski map $\Sigma\colon K \to \mathbb{R}^n$ maps $\alpha \in K$ to

$$(\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \Re\sigma_{s+1}(\alpha), \Im\sigma_{s+1}(\alpha), \ldots, \Re\sigma_{s+t}(\alpha), \Im\sigma_{s+t}(\alpha))$$

- lattice $\Lambda = \Sigma(\mathbb{Z}[\tau])$ in $\mathbb{R}^n$
- endomorphism Φ = multiplication by τ

Numeral Systems in Lattices

$$z = \sum_{j=0}^{J} \Phi^j(z_j) \in \Lambda$$

Theorem (Heuberger–DK 2012)

- *digit set* $\mathcal{D}$ *comes from tiling* T *of* $\mathbb{R}^n$ *w.r.t.* Λ, *i.e.*,
  - $\mathbb{R}^n = \bigcup_{z \in \Lambda} (z + T)$
  - $\mathcal{D} \subseteq \Phi^w(T) \cap \Lambda$
- $w \in \mathbb{N}$ *such that all eigenvalues* λ *of* Φ *fulfil* $|\lambda|^w > 1 + c_T$ *with* $c_T > 0$

Then each lattice element has a unique w*-NAF-expansion.*

Theorem (Heuberger–DK 2012)

- *digit set* $\mathcal{D}$ *of minimal norm representatives*
- $w \in \mathbb{N}$ *such that all eigenvalues* λ *of* Φ *fulfil* $|\lambda|^w > 2$

Then each lattice element has a unique w*-NAF-expansion.*

Occurences of a non-zero Digit in a Region

Theorem (Heuberger–DK 2010, DK 2012)

- *all eigenvalues of* Φ *have the same absolute value* $\rho > 1$
- *digit set* $\mathcal{D}$ *comes from tiling* T *of* $\mathbb{R}^n$ *w.r.t.* Λ, *i.e.*,
  - $\mathbb{R}^n = \bigcup_{z \in \Lambda} (z + T)$
  - $\mathcal{D} \subseteq \Phi^w(T) \cap \Lambda$
- *fix a non-zero digit* $\eta \in \mathcal{D}$
- $N \in \mathbb{R}_{\geq 0}$

Then the number of occurrences of the digit η
in all w*-NAFs in a ball with radius* N *around* 0 *is*

$$Z(N) = \frac{\pi^{n/2}}{\Gamma(n/2+1)} N^n E \log_\rho N + N^n \psi\big(\log_\rho N\big) + o(N^n)\,.$$

Sketch of Proof

- use Delange's method
- counting

$\bigcirc$ = ball with radius N around 0

$$Z(N) = \sum_{z \in \bigcirc \cap \Lambda} \sum_{j=0}^{J} \left[\begin{array}{c} j\text{th digit of} \\ w\text{-NAF of } z \text{ is } \eta \end{array} \right]$$

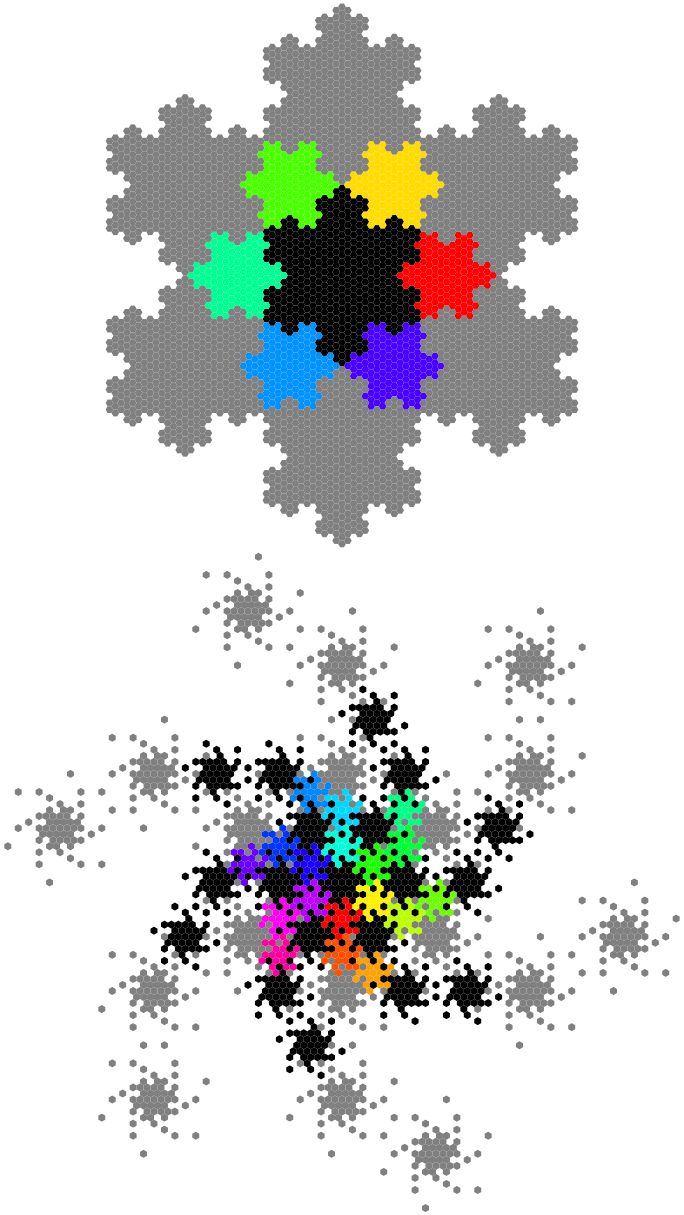
- rewriting the sum as integral

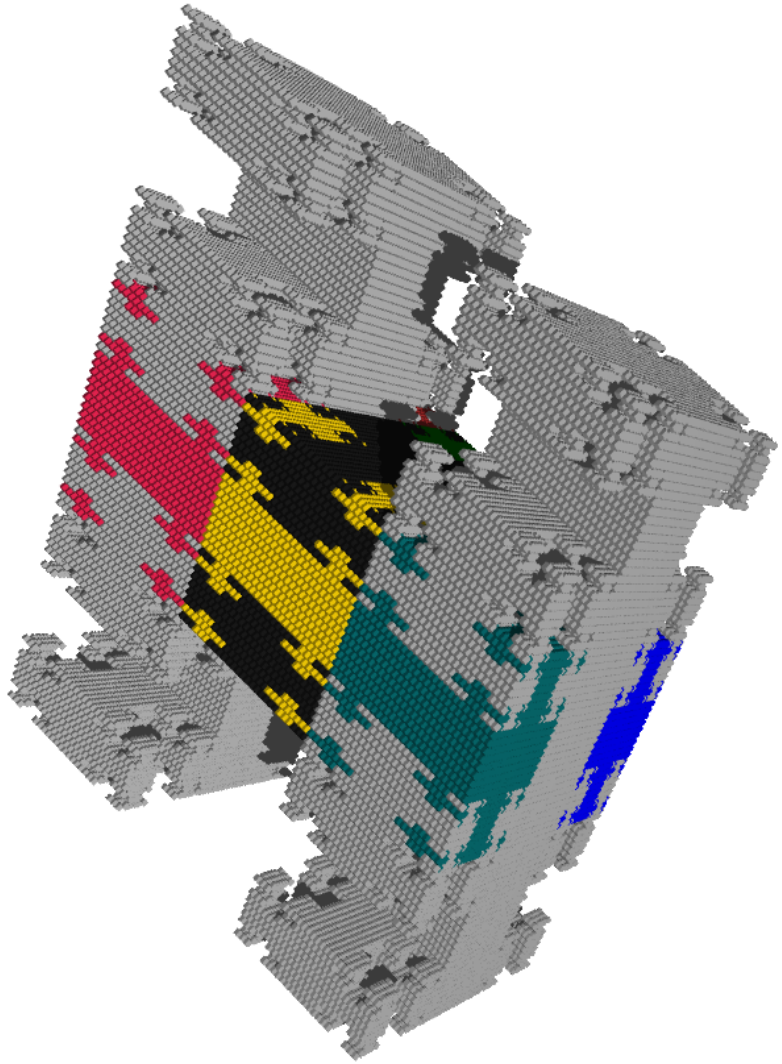
$$Z(N) = \frac{1}{d(\Lambda)} \sum_{j=0}^{\log_\rho N} \int_{z \in \bigcirc} \mathbb{1}_{W_{\eta,j}}\left(\left\{\Phi^{-j-w} z\right\}\right) \, \mathrm{d}z \; + \; \begin{array}{c} \text{“small”} \\ \text{error terms} \end{array}$$

- splitting up the integral

$$\int_{\bigcirc} \mathbb{1}_{W_{\eta,j}} = \int_{\bigcirc} \lambda(W_\eta) + \int_{\bigcirc} \left(\mathbb{1}_{W_\eta} - \lambda(W_\eta)\right) + \int_{\bigcirc} \left(\mathbb{1}_{W_{\eta,j}} - \mathbb{1}_{W_\eta}\right)$$

Characteristic Sets





Figures: different characteristic sets