ANALYSIS OF DIGITAL EXPANSIONS IN CONJUNCTION WITH KOBLITZ CURVES IN CHARACTERISTIC THREE

DANIEL KRENN

Consider the elliptic curve

$$\mathcal{E}_3 : Y^2 = X^3 - X - 1$$

defined over $\mathbb{F}_3$. This curve was studied by Koblitz [3]. In cryptographic applications we are interested in the group $\mathcal{E}_3(\mathbb{F}_{3^m})$ of rational points over a field extension $\mathbb{F}_{3^m}$ of $\mathbb{F}_3$ for an $m \in \mathbb{N}$. The Frobenius endomorphism

$$\varphi : \mathcal{E}_3(\mathbb{F}_{3^m}) \longrightarrow \mathcal{E}_3(\mathbb{F}_{3^m}), \quad (x, y) \longmapsto \left(x^3, y^3\right)$$

satisfies the relation $\varphi^2 - 3\varphi + 3 = 0$, so φ may be identified with the imaginary quadratic number $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$, which is a solution of the mentioned relation. Thus we have an isomorphism between $\mathbb{Z}[\tau]$ and the endomorphism ring of $\mathcal{E}_3(\mathbb{F}_{3^m})$.

Let $z \in \mathbb{Z}[\tau]$ and $P \in \mathcal{E}_3(\mathbb{F}_{3^m})$. If we write the element z as $\sum_{j=0}^{\ell-1} z_j \tau^j$ for some digits z_j belonging to a digits set $\mathcal{D}$, then we can compute the action zP as $\sum_{j=0}^{\ell-1} z_j \, \varphi^j(P)$ via a Horner scheme. The resulting *Frobenius-and-add* method [2, 4, 5] is much faster than the classic double-and-add scalar multiplication.

So we are interested in a τ-adic expansion for an element of $\mathbb{Z}[\tau]$, such that the operation mentioned above is as efficient as possible. Let $w \in \mathbb{N}$ with $w \geq 2$ and suppose our digit set $\mathcal{D}$ consists of zero and all minimal norm representatives modulo τ^w not divisible by τ, cf. Solinas [4, 5]. We consider numbers $z = \sum_{j=0}^{\ell-1} z_j \tau^j$, where $z_j \in \mathcal{D}$ and $z_{\ell-1} \ldots z_0$ is a *width-w non-adjacent form*, or *w-NAF* for short, i.e. each block of length w contains at most one non-zero. Figure 1 shows two examples. There all w-NAFs of a given length ℓ are drawn.

Since a w-NAF can be described by the regular expression

$$\left(\varepsilon + \sum_{d \in \mathcal{D}\setminus\{0\}} \sum_{k=0}^{w-2} 0^k d\right) \left(0 + \sum_{d \in \mathcal{D}\setminus\{0\}} 0^{w-1} d\right)^*,$$

we can simply use a generating function to count the occurrences of a non-zero digit in all w-NAFs of length ℓ. We obtain

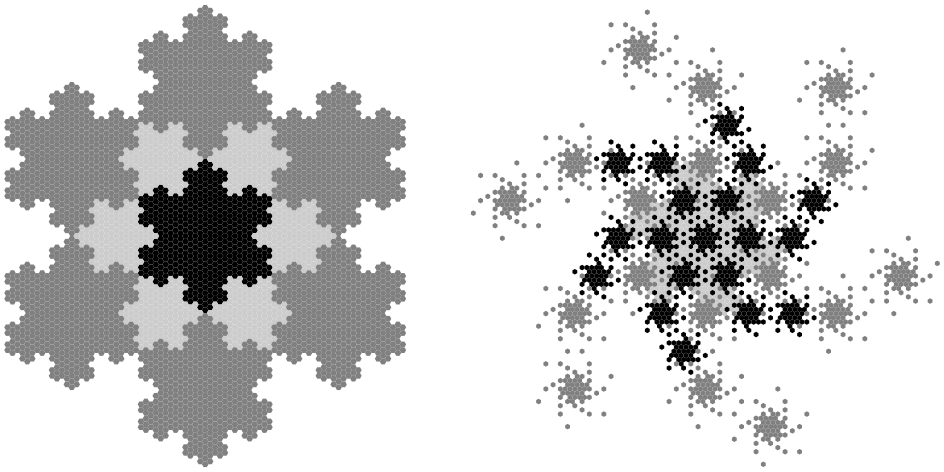
$$\frac{1}{(\mathcal{N}(\tau)-1)w+1} \, \mathcal{N}(\tau)^{\ell+w} + \mathcal{O}\Big(\big(\rho\,\mathcal{N}(\tau)\big)^{\ell}\Big),$$

where $\rho = (1 + \frac{1}{\mathcal{N}(\tau)w^3})^{-1} < 1$ and $\mathcal{N}(\tau)$ denotes the norm of τ. This result holds for a general algebraic integer τ, too.

A more general question is, what the number of occurrences of a non-zero digit η is, when we look at all w-NAFs with absolute value smaller than a given N. For imaginary quadratic τ with $|\tau| > 1$, the answer is given by the following theorem.

Key words and phrases. Koblitz curves, Frobenius endomorphism, tau-adic expansions, non-adjacent forms, sum of digits.

D. Krenn is supported by the Austrian Science Foundation FWF, project S9606, that is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory".



(a) $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$, $w = 2$ and $\ell = 7$ (b) $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$, $w = 3$ and $\ell = 6$

Figure 1: Values of w-NAFs of length ℓ.

Theorem. *Let $0 \neq \eta \in \mathcal{D}$, $U \subseteq \mathbb{C}$ be the unit disc and let $N \in \mathbb{R}_{\geq 0}$. Then the number of occurrences of the digit η in all w-NAFs with value in the region NU is*

$$Z_{\tau,w,\eta}(N) = e_w N^2 \, \lambda(U) \log_{|\tau|} N + N^2 \, \psi_\eta\Big(\log_{|\tau|} N\Big) + \mathcal{O}(N^\alpha)\,.$$

There $e_w = \Big(\mathcal{N}(\tau)^{w-1}\left((\mathcal{N}(\tau)-1)w+1\right)\Big)^{-1}$, the function ψ_η is 1-periodic and continuous, and α is a computable constant with $\alpha < 2$.

Instead of the unit disc, other bounded regions U can be used, but they possibly destroy the periodicity and continuity of ψ_η. The proof of the theorem follows the ideas of Delange [1].

References

1. H. Delange, *Sur la fonction sommatoire de la fonction "somme des chiffres"*, Enseignement Math. (2) **21** (1975), 31–47.
2. N. Koblitz, *CM-curves with good cryptographic properties*, Advances in cryptology—CRYPTO '91 (Santa Barbara, CA, 1991), Lecture Notes in Comput. Sci., vol. 576, Springer, Berlin, 1992, pp. 279–287.
3. ———, *An elliptic curve implementation of the finite field digital signature algorithm*, Advances in cryptology—CRYPTO '98 (Santa Barbara, CA, 1998), Lecture Notes in Comput. Sci., vol. 1462, Springer, Berlin, 1998, pp. 327–337.
4. J. A. Solinas, *An improved algorithm for arithmetic on a family of elliptic curves*, Advances in Cryptology — CRYPTO '97. 17th annual international cryptology conference. Santa Barbara, CA, USA. August 17–21, 1997. Proceedings (B. S. Kaliski, jun., ed.), Lecture Notes in Comput. Sci., vol. 1294, Springer, Berlin, 1997, pp. 357–371.
5. ———, *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249.

Institute of Optimisation and Discrete Mathematics (Math B)
Graz University of Technology
Austria

E-mail address: mail@danielkrenn.at *or* daniel.krenn@tugraz.at