Journal of Number Theory 133 (2013) 1752–1808

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Analysis of width-w non-adjacent forms to imaginary quadratic bases

Clemens Heuberger[1], Daniel Krenn[*,1]

Institute of Optimisation and Discrete Mathematics (Math B), Graz University of Technology, Steyrergasse 30/II, A-8010 Graz, Austria

ARTICLE INFO

Article history:
Received 11 February 2011
Revised 3 August 2012
Accepted 4 August 2012
Available online 4 January 2013
Communicated by David Goss

Keywords:
τ-adic expansions
Non-adjacent forms
Redundant digit sets
Elliptic curve cryptography
Koblitz curves
Frobenius endomorphism
Scalar multiplication
Hamming weight
Sum of digits
Fractals
Fundamental domain

ABSTRACT

We consider digital expansions to the base of an algebraic integer τ. For a $w \geqslant 2$, the set of admissible digits consists of 0 and one representative of every residue class modulo τ^w which is not divisible by τ. The resulting redundancy is avoided by imposing the width-w non-adjacency condition. Such constructs can be efficiently used in elliptic curve cryptography in conjunction with Koblitz curves. The present work deals with analysing the number of occurrences of a fixed non-zero digit. In the general setting, we study all w-NAFs of given length of the expansion (expectation, variance, central limit theorem). In the case of an imaginary quadratic τ and the digit set of minimal norm representatives, the analysis is much more refined. The proof follows Delange's method. We also show that *each* element of $\mathbb{Z}[\tau]$ has a w-NAF in that setting.

Contents

[*] Corresponding author.
E-mail addresses: clemens.heuberger@tugraz.at (C. Heuberger), math@danielkrenn.at, krenn@math.tugraz.at (D. Krenn).

[1] The authors are supported by the Austrian Science Foundation (FWF): S9606 that is part of the Austrian National Research Network “Analytic Combinatorics and Probabilistic Number Theory”.

0022-314X © 2012 Elsevier Inc. Open access under CC BY-NC-ND license.
http://dx.doi.org/10.1016/j.jnt.2012.08.029

1. Introduction

Let $\tau \in \mathbb{C}$ be an algebraic integer. We consider τ-adic expansions for an element of $\mathbb{Z}[\tau]$ using a redundant digit set $\mathcal{D}$. This means that our expansions need not be unique without any further constraints. However, by applying a width-w non-adjacency property to the digits of a representation, together with choosing an appropriate digit set, we gain uniqueness. The mentioned property simply means that each block of w digits contains at most one non-zero digit.

Such expansions have a low Hamming weight, i.e., a low number of non-zero digits. This is of interest in elliptic curve cryptography: There, scalar multiples of points can be computed by using τ-adic-expansions, where τ corresponds to the Frobenius endomorphism. See Section 2 for a more detailed discussion.

The aim of this paper is to give a precise analysis of the expected number of non-zeros in τ-adic expansions of elements in $\mathbb{Z}[\tau]$, corresponding to the expected number of costly curve operations. Several random models can be considered.

The easiest model is to consider all expansions of given length to be equally likely; this is called the “full block length” model. The result for arbitrary algebraic integers is given in Theorem 5.1. The appropriateness of this random model becomes debatable when looking at the set of complex numbers admitting such an expansion of given length: This is the intersection of the lattice of integers in the number field with a fractal set, a scaled version of the “Fundamental domain”, cf. Fig. 10.1.

A more natural choice seems to be to consider the expansions of all integers in $\mathbb{Z}[\tau]$ whose absolute value is bounded by some N. The main result of this paper (Theorem 11.1) is exactly such a result, where we assume τ to be a imaginary quadratic number. Theorem 11.1 is, in fact, more general: instead of considering all integers within a scaled version of the unit circle, we consider all integers contained in a scaled copy of some set U. Instead of counting the number of non-zeros, we count the number of occurrences of each digit. The full block length analysis result will indeed be needed to prove Theorem 11.1.

For given τ and block length $w \geqslant 2$, several digit sets could be chosen. A rather natural choice was proposed by Solinas [19,20]: Consider the residue classes modulo τ^w in $\mathbb{Z}[\tau]$. As digit set, we use zero and a minimal norm representative from each residue class not divisible by τ. Now let $z \in \mathbb{Z}[\tau]$ with $z = \sum_{j=0}^{\ell-1} z_j \tau^j$. This expansion is a width-w τ-adic non-adjacent form, or w-NAF for short, if each block of w consecutive digits $z_j \ldots z_{j+w-1}$ contains at most one non-zero digit. The name “non-adjacent form” goes back to Reitwiesner [18].

It is commonly known that such expansions, if they exist, are unique, whereas the existence was only known for special cases, see Section 2. In this paper in Section 7 we show that, for imaginary quadratic τ and $w \geqslant 2$, every element of $\mathbb{Z}[\tau]$ admits a unique w-NAF, see Theorem 7.1. Additionally a simple algorithm for calculating those expansions is given.

The full block length analysis is carried out in Section 5: We define a random variable $X_{n,w,\eta}$ for the number of occurrences of η in all w-NAFs of a fixed length n. It is assumed that all those w-NAFs are equally likely. For an arbitrary algebraic integer τ Theorem 5.1 gives explicit expressions for the expectation and the variance of $X_{n,w,\eta}$. Asymptotically we get $\mathbb{E}(X_{n,w,\eta}) \sim e_w n$ and $\mathbb{V}(X_{n,w,\eta}) \sim v_w n$ for constants e_w and v_w depending on w and the norm of τ. The proof uses a regular expression describing the w-NAFs. This will then be translated into a generating function. Further in this theorem it is shown that $X_{n,w,\eta}$ satisfies a central limit theorem.