Forschungsschwerpunkt

Algorithmen und mathematische Modellierung

Analysis of Width-w Non-Adjacent Forms to Imaginary Quadratic Bases

Clemens Heuberger and Daniel Krenn

Project Area(s):

Analysis of Digital Expansions with Applications in Cryptography

Institut für Optimierung und Diskrete Mathematik (Math B)

Report 2010-10, September 2010

ANALYSIS OF WIDTH-w NON-ADJACENT FORMS TO IMAGINARY QUADRATIC BASES

CLEMENS HEUBERGER AND DANIEL KRENN

Abstract. We consider digital expansions to the base of τ, where τ is an algebraic integer. For a $w \geq 2$, 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-NAF condition, i.e., in an expansion every block of w consecutive digits contains at most one non-zero digit. 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. We give an explicit expression for the expectation and the variance of the occurrence of such a digit in all expansions. Further a central limit theorem is proved.

In the case of an imaginary quadratic τ and the digit set of minimal norm representatives, the analysis is much more refined: We give an asymptotic formula for the number of occurrence of a digit in the w-NAFs of all elements of $\mathbb{Z}[\tau]$ in some region (e.g. a disc). The main term coincides with the full block length analysis, but a periodic fluctuation in the second order term is also exhibited. The proof follows Delange's method.

We also show that in the case of imaginary quadratic τ and $w \geq 2$, the digit set of minimal norm representatives leads to w-NAFs for *all* elements of $\mathbb{Z}[\tau]$. Additionally some properties of fundamental domain are stated.

1. Introduction and Background

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. The motivation comes from elliptic curve cryptography, where those expansions lead to efficient calculation schemes.

Consider the elliptic curve

$$\mathcal{E}_3 \colon Y^2 = X^3 - X - \mu \qquad \text{with } \mu \in \{-1, 1\}$$

defined over $\mathbb{F}_3$. This curve was studied by Koblitz [15]. 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

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

satisfies the relation $\varphi^2 - 3\mu\varphi + 3 = 0$. So φ may be identified with the imaginary quadratic number $\tau = \frac{3}{2}\mu + \frac{1}{2}\sqrt{-3}$, 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 digit set $\mathcal{D}$, then we can compute the action zP as $\sum_{j=0}^{\ell-1} z_j \, \varphi^j(P)$ via a Horner

Key words and phrases. 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.

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

scheme. The resulting Frobenius-and-add method [14, 19, 20] is much faster than the classic double-and-add scalar multiplication.

Another example is the elliptic curve

$$\mathcal{E}_2\colon Y^2 + XY = X^3 + aX^2 + 1 \qquad \text{with } a \in \{0,1\}$$

defined over $\mathbb{F}_2$, cf. Koblitz [14]. There we get the relation $\varphi^2 - \mu\varphi + 2 = 0$ with $\mu = (-1)^{1-a}$ for the Frobenius endomorphism φ, and thus $\tau = \frac{1}{2}\mu + \frac{1}{2}\sqrt{-7}$.

So we are interested in a τ-adic expansion for an element of $\mathbb{Z}[\tau]$ such that the mentioned computation of the action is as efficient as possible.

The fewer non-zero digits there are in an expansion, the faster the main loop of the Horner scheme can be calculated. But usually fewer non-zero coefficients means larger digit sets and thus a higher pre-computation effort. So for optimal performance, a balance between digit set size and number of non-zeros has to be found.

We use the following concept in this paper. Let $w \in \mathbb{N}$ with $w \geq 2$. 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. This was mentioned by Solinas [19, 20]. 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. For the τ corresponding to $\mathcal{E}_3$ and $w \geq 2$ this was shown in Koblitz [15] and Blake, Kumar Murty and Xu [6], for the τ corresponding to $\mathcal{E}_2$ and $w \geq 2$ in Solinas [20] and Blake, Kumar Murty and Xu [5]. Some other τ are handled in Blake, Kumar Murty and Xu [4]. In this paper in Section 6 we show that, for imaginary quadratic τ and $w \geq 2$, every element of $\mathbb{Z}[\tau]$ admits a unique w-NAF, see Theorem 6.1 on page 21. A digit set with this property is called a non-adjacent digit set. Additionally a simple algorithm for calculating those expansions is given. Further in Theorem 6.5 on page 23 we get that every element of $\mathbb{C}$ has a w-NAF-expansion of the form $\xi_{\ell-1} \ldots \xi_1\xi_0\mathbf{.}\xi_{-1}\xi_{-2}\ldots$, where the right hand side of the τ-point is allowed to be of infinite length.

In Section 7 we consider numbers of the form $0\mathbf{.}\xi_{-1}\xi_{-2}\ldots$. The set of all values of such numbers is called the fundamental domain $\mathcal{F}$. It is shown that $\mathcal{F}$ is compact and its boundary has Hausdorff dimension smaller than 2. Further a tiling property with scaled versions of $\mathcal{F}$ is given for the complex plane. Additionally, by using the results of Section 9, we can calculate the Lebesgue measure of the fundamental domain.

The main part of this paper deals with analysing the occurrences of a fixed non-zero digit η. In Section 4 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 4.1 on page 11 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.

A more general question is, what the number of occurrences $Z_{\tau,w,\eta}$ of the non-zero digit η is, when we look at all w-NAFs with absolute value smaller than a given N. For imaginary quadratic τ and a region $U \subseteq \mathbb{C}$ (e.g. the unit disc for the absolute value), the answer is given by Theorem 10.1 on page 36 in Section 10. We prove that $Z_{\tau,w,\eta} \sim e_w N^2\, \lambda(U) \log_{|\tau|} N$. This is not surprising, since intuitively there are about $N^2\, \lambda(U)$ w-NAFs in the region NU, and each of them can be represented as a w-NAF with length $\log_{|\tau|} N$. We even get a more precise result. If the region is "nice", there is a periodic oscillation of order N^2 in the formula.

The structure of the result — main term, oscillation term, smaller error term — is not uncommon in the context of digits counting. For instance, a setting similar to ours can be found in Heuberger and Prodinger [12]. There base 2 and special digit sets are used, and 2-NAFs are

	short description	τ	digit set $\mathcal{D}$
Section 2	Voronoi cells	i-q	——
Lemma 3.3 on page 8	complete residue system	alg	——
Definition 3.5 on page 9	minimal norm representatives digit set	i-q	——
Definition 3.7 on page 9	width-w non-adjacent forms	gen	fin
Proposition 3.8 on page 10	continuity of value	gen	fin
Definition 3.11 on page 11	width-w non-adjacent digit set	gen	fin
Theorem 4.1 on page 11	full block length distribution theorem	alg	RRS
Section 5	bounds for the value	i-q	MNR
Theorem 6.1 on page 21	existence theorem for lattice points	i-q	MNR
Theorem 6.5 on page 23	existence theorem for $\mathbb{C}$	i-q	MNR
Definition 7.1 on page 23	fundamental domain $\mathcal{F}$	gen	fin
Proposition 7.2 on page 23	compactness of the fundamental domain	gen	fin
Corollary 7.4 on page 24	tiling property	i-q	MNR
Remark 7.5 on page 24	iterated function system	gen	fin
Proposition 7.7 on page 25	characterisation of the boundary	i-q	MNR
Proposition 7.8 on page 25	upper bound for the dimension of $\partial\mathcal{F}$	i-q	MNR
Section 8	cell rounding operations	i-q	——
Section 9	characteristic sets	i-q	MNR
Theorem 10.1 on page 36	counting the occurences of a digit	i-q	MNR

Abbreviations for τ (general: $\tau \in \mathbb{C}$ with $\lvert\tau\rvert > 1$)	
gen	$\tau \in \mathbb{C}$
alg	τ algebraic integer
i-q	τ imaginary quadratic algebraic integer

Abbreviations for digit sets (general: $\mathcal{D} \subseteq \mathbb{Z}[\tau]$, $0 \in \mathcal{D}$)	
fin	finite digit set
RRS	reduced residue system digit set
MNR	minimal norm representatives digit set

Table 1.1: Overview of requirements.

considered. The result has the same structure as ours. Another example can be found in Grabner, Heuberger and Prodinger [10] for joint expansions.

The examples followed the ideas of Delange [7] to prove the statements. We will do the same. The proof is given in Section 10. In Section 8 and Section 9 the necessary tools for the proof will be developed and the characteristic sets will be analysed.

At last a short overview of the sections not mentioned until now. In Section 2 Voronoi cells and their basic properties are discussed. Section 3 is dealing with the digit sets, as well as the formal definition of the non-adjacent forms and some basic results. In Section 5 we give bounds for the value of a w-NAF. While the main focus of this paper lies on imaginary quadratic bases and the digit set of minimal norm representatives, some of the results, e.g. the full block length analysis (Theorem 4.1 on page 11), are valid in a more general setting. A more detailed overview on the requirements on τ and digit set $\mathcal{D}$ for the different sections, definitions, theorems, etc. can be found in Table 1.1.

2. Voronoi Cells

Let $\tau \in \mathbb{C}$ be an algebraic integer, imaginary quadratic, i.e., τ is solution of an equation $\tau^2 - p\tau + q = 0$ with $p, q \in \mathbb{Z}$, such that $4q - p^2 > 0$.

We will use the digit set of minimal norm representatives. In order to describe this digit set, we will rewrite the minimality condition in terms of the Voronoi cell for the lattice $\mathbb{Z}[\tau]$, cf. Gordon [9].

Definition 2.1 (Voronoi Cell)**.** We set

$$V := \{z \in \mathbb{C} \mid \forall y \in \mathbb{Z}[\tau] : |z| \leq |z - y|\} .$$

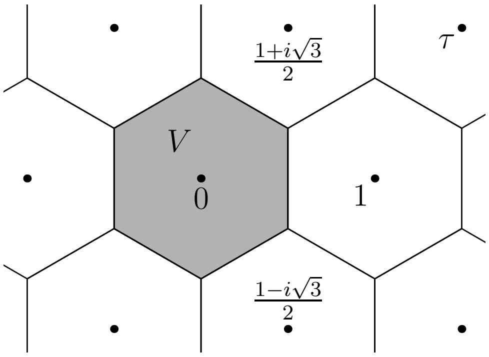


Figure 2.1: Voronoi cell V for 0 corresponding to the set $\mathbb{Z}[\tau]$ with $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$.

V is the *Voronoi cell for* 0 corresponding to the set $\mathbb{Z}[\tau]$. Let $u \in \mathbb{Z}[\tau]$. We define the *Voronoi cell for* u as

$$V_u := u + V = \{u + z \,|\, z \in V\} = \{z \in \mathbb{C} \,|\, \forall y \in \mathbb{Z}[\tau] : |z - u| \leq |z - y|\}\,.$$

The point u is called *centre of the Voronoi cell* or *lattice point corresponding to the Voronoi cell.*

An example of a Voronoi cell in a lattice $\mathbb{Z}[\tau]$ is shown in Figure 2.1. Whenever the word “cells” is used in this paper, these Voronoi cells or scaled Voronoi cells will be meant.

Two neighbouring Voronoi cells have at most a subset of their boundary in common. This can be a problem, when we tile the plane with Voronoi cells and want that each point is in exactly one cell. To fix this problem we define a restricted version of V. This is very similar to the construction used in Avanzi, Heuberger and Prodinger [2].

Definition 2.2 (Restricted Voronoi Cell)**.** Let V_u be a Voronoi cell as above and u its centre. Let $v_0, \ldots, v_{m-1}$ with appropriate $m \in \mathbb{N}$ be the vertices of V_u. We denote the midpoint of the line segment from v_k to v_{k+1} by $v_{k+1/2}$, and we use the convention that the indices are meant modulo m.

The *restricted Voronoi cell* $\widetilde{V}_u$ consists of

- the interior of V_u,
- the line segments from $v_{k+1/2}$ (excluded) to v_{k+1} (excluded) for all k,
- the points $v_{k+1/2}$ for $k \in \left\{0, \ldots, \left\lfloor \frac{m}{2} \right\rfloor - 1\right\}$, and
- the points v_k for $k \in \left\{1, \ldots, \left\lfloor \frac{m}{3} \right\rfloor\right\}$.

Again we set $\widetilde{V} := \widetilde{V}_0$.

In Figure 2.2 on the facing page the restricted Voronoi cell for 0 is shown. The second condition is used, because it benefits symmetries. The third condition is just to make the midpoints unique. Obviously, other rules could have been used to define the restricted Voronoi cell.

As a generalisation of the usual fractional part of elements in $\mathbb{R}$ with respect to the integers, we define the fractional part of an element of $\mathbb{C}$ corresponding to the restricted Voronoi cell $\widetilde{V}$ and thus corresponding to the lattice $\mathbb{Z}[\tau]$.

Definition 2.3 (Fractional Part in $\mathbb{Z}[\tau]$)**.** Let $z \in \mathbb{C}$, $z = u + v$ with $u \in \mathbb{Z}[\tau]$ and $v \in \widetilde{V}$. Then we define the *fractional part corresponding to the lattice* $\mathbb{Z}[\tau]$ by $\{z\}_{\mathbb{Z}[\tau]} := v$.

This definition is valid, because of the construction of the restricted Voronoi cell. The fractional part of a point $z \in \mathbb{C}$ simply means, to search for the nearest lattice point u of $\mathbb{Z}[\tau]$ and returning the difference $z - u$.

Throughout this paper we will use the following notation for discs in the complex plane.

Definition 2.4 (Opened and Closed Discs)**.** Let $z \in \mathbb{C}$ and $r \geq 0$. The *open disc* $\mathcal{B}(z, r)$ *with centre* z *and radius* r is denoted by

$$\mathcal{B}(z, r) := \{y \in \mathbb{C} \,|\, |z - y| < r\}$$

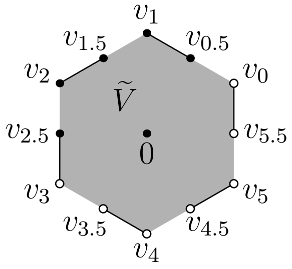


Figure 2.2: Restricted Voronoi cell $\widetilde{V}$ for 0 corresponding to the set $\mathbb{Z}[\tau]$ with $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$.

and the *closed disc* $\overline{\mathcal{B}}(z, r)$ *with centre* z *and radius* r by

$$\overline{\mathcal{B}}(z, r) := \{y \in \mathbb{C} \mid |z - y| \le r\}.$$

The disc $\mathcal{B}(0, 1)$ is called *unit disc.*

We will need suitable bounds for the digits in our digit set. These require precise knowledge on the Voronoi cells, such as the position of the vertices and bounds for the size of V. Such information is derived in the following proposition.

Proposition 2.5 (Properties of Voronoi Cells)**.** *We get the following properties:*

(a) The vertices of V *are given by*

$$\begin{aligned} v_0 &= 1/2 + \frac{i}{2\operatorname{Im}(\tau)}\Big(\operatorname{Im}(\tau)^2 + \{\operatorname{Re}(\tau)\}^2 - \{\operatorname{Re}(\tau)\}\Big), \\ v_1 &= \{\operatorname{Re}(\tau)\} - \frac{1}{2} + \frac{i}{2\operatorname{Im}(\tau)}\Big(\operatorname{Im}(\tau)^2 - \{\operatorname{Re}(\tau)\}^2 + \{\operatorname{Re}(\tau)\}\Big), \\ v_2 &= -1/2 + \frac{i}{2\operatorname{Im}(\tau)}\Big(\operatorname{Im}(\tau)^2 + \{\operatorname{Re}(\tau)\}^2 - \{\operatorname{Re}(\tau)\}\Big) = v_0 - 1, \\ v_3 &= -v_0, \\ v_4 &= -v_1 \end{aligned}$$

and

$$v_5 = -v_2.$$

All vertices have the same absolute value. If $\operatorname{Re}(\tau) \in \mathbb{Z}$*, then* $v_1 = v_2$ *and* $v_4 = v_5$*, i.e., the hexagon degenerates to a rectangle.*

(b) The Voronoi-cell V *is convex.*

(c) We get the bounds

$$\overline{\mathcal{B}}\big(0, \tfrac{1}{2}\big) \subseteq V \subseteq \overline{\mathcal{B}}(0, |\tau|\, c_V)$$

with $c_V = \sqrt{\frac{7}{12}}$.

(d) The Lebesgue measure of V *in the complex plane is*

$$\lambda(V) = |\operatorname{Im}(\tau)|.$$

(e) The inclusion $\tau^{-1}V \subseteq V$ *holds.*

In the proof we will use some properties of Voronoi cells, which can, for example, be found in Aurenhammer [1].

Proof. (a) Since V is point-symmetric with respect to 0, we get $v_0 = -v_3$, $v_1 = -v_4$ and $v_2 = -v_5$. Thus we suppose without loss of generality $\operatorname{Im}(\tau) > 0$. Strict greater holds, because τ is imaginary quadratic. Even more, we get $\operatorname{Im}(\tau) \ge \frac{\sqrt{3}}{2}$, since

$$\tau = \frac{p}{2} \pm \frac{i}{2}\sqrt{4q - p^2}$$

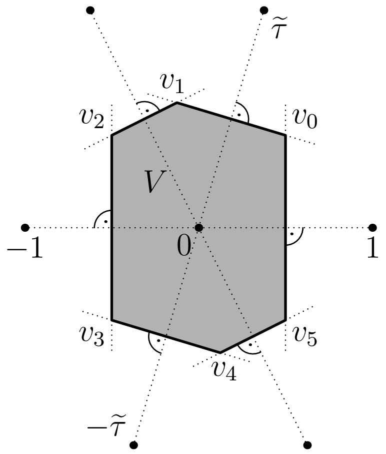


Figure 2.3: Construction of the Voronoi cell V for 0. The picture shows a general situation. Since τ is an imaginary quadratic algebraic integer, we will have $\operatorname{Re}(\widetilde{\tau}) \in \left\{0, \frac{1}{2}\right\}$.

is solution of $\tau^2 - p\tau + q = 0$ for $p, q \in \mathbb{Z}$ and either $4q - p^2 \equiv 0 \pmod 4$ or $4q - p^2 \equiv -1 \pmod 4$.

All elements of the lattice $\mathbb{Z}[\tau]$ can be written as $a + b\tau$, since τ is quadratic. We have to consider the neighbours of 0 in the lattice. The Voronoi cell is the area enclosed by the line segment bisectors of the lines from each neighbour to zero, see Figure 2.3.

Clearly $\operatorname{Re}(v_0) = \frac{1}{2}$ and $\operatorname{Re}(v_2) = -\frac{1}{2}$, since -1 and 1 are neighbours. Set $\widetilde{\tau} = \{\operatorname{Re}(\tau)\} + i \operatorname{Im}(\tau)$. Consider the line from 0 to $\widetilde{\tau}$ with midpoint $\frac{1}{2}\widetilde{\tau}$. We get

$$v_0 = \frac{1}{2}\widetilde{\tau} - x_A i\widetilde{\tau}$$

and

$$v_1 = \frac{1}{2}\widetilde{\tau} + x_B i\widetilde{\tau}$$

for some $x_A \in \mathbb{R}_{\geq 0}$ and $x_B \in \mathbb{R}_{\geq 0}$. Analogously, for the line from 0 to $\widetilde{\tau} - 1$, we have

$$v_1 = \frac{1}{2}\left(\widetilde{\tau} - 1\right) - x_C i \left(\widetilde{\tau} - 1\right)$$

and

$$v_2 = \frac{1}{2}\left(\widetilde{\tau} - 1\right) + x_D i \left(\widetilde{\tau} - 1\right).$$

for some $x_C \in \mathbb{R}_{\geq 0}$ and $x_D \in \mathbb{R}_{\geq 0}$. Solving this system of linear equations leads to the desired result. An easy calculation shows that $|v_0| = |v_1| = |v_2|$.

Until now, we have constructed the Voronoi cell of the points

$$P := \left\{0, 1, -1, \widetilde{\tau}, \widetilde{\tau} - 1, -\widetilde{\tau}, -(\widetilde{\tau} - 1)\right\}.$$

We want to rule out all other points, i.e., make sure, that none of the other points changes the already constructed cell. So let $z = x + iy \in \mathbb{Z}[\tau]$ and consider $\frac{z}{2}$. Because of symmetry reasons, we can assume $x \geq 0$ and $y \geq 0$. Clearly all points $z \in \mathbb{Z}$ with $z \geq 2$ do not change the Voronoi cell, since $\frac{z}{2} > \frac{1}{2}$ and the corresponding line segment bisector is vertical. So we can assume $y > 0$.

Now we will proceed in the following way. A point z can be ruled out, if the absolute value of $\frac{z}{2}$ is larger than

$$R = |v_0| = |v_1| = |v_2|.$$

Let $\tau = a + ib$. If $\{a\} = 0$, then $R^2 = \frac{1}{4}\left(1 + b^2\right)$. We claim that

$$R^2 < \frac{x^2 + y^2}{4} \iff 1 + b^2 < x^2 + y^2.$$

Since $y > 0$, we have $y \geq b$. If $y = b$, then points with $x > 1$ need not be taken into account. But the remaining points are already in P (at least using symmetry and $\widetilde{\tau}+1$ instead of $\widetilde{\tau}-1$). If $y \geq 2b$, then all points except the ones with $x = 0$ can be ruled out, since $1 - b^2 \leq 1 - \frac{3}{4} = \frac{1}{4} < x$. But the points z with $x = 0$ can be ruled out, too, because there is already the point ib in P.

So let $\{a\} = \frac{1}{2}$. Then $R^2 = \frac{1}{4}\left(\frac{1}{2} + b^2 + \frac{1}{16b^2}\right)$ and we claim that

$$R^2 < \frac{x^2+y^2}{4} \iff \frac{1}{2} + b^2 + \frac{1}{16b^2} < x^2 + y^2.$$

If $y = b$, then $x > \sqrt{\frac{7}{12}}$ suffices to rule out a point z, since $b \geq \frac{\sqrt{3}}{2}$. But the only point z with $x \leq \sqrt{\frac{7}{12}}$ is $\frac{1}{2} + ib$, which is already in P. If $y \geq 2b$, then $\frac{1}{2} - b^2 + \frac{1}{16b^2} \leq \frac{1}{2} - \frac{3}{4} + \frac{1}{12} < 0$, so all points can be ruled out.

(b) Follows directly from the fact that all vertices have the same absolute value.

(c) From

$$v_0 = 1/2 + \frac{i}{2\operatorname{Im}(\widetilde{\tau})} \underbrace{\left(\operatorname{Im}(\widetilde{\tau})^2 + \operatorname{Re}(\widetilde{\tau})^2 - \operatorname{Re}(\widetilde{\tau})\right)}_{\leq \operatorname{Im}(\widetilde{\tau})^2}$$

we obtain

$$\frac{|v_0|}{|\widetilde{\tau}|} \leq \frac{|1 + i\operatorname{Im}(\widetilde{\tau})|}{2\,|\widetilde{\tau}|} \leq \frac{\operatorname{Im}(\widetilde{\tau})}{2\,|\widetilde{\tau}|}\sqrt{\frac{1}{\operatorname{Im}(\widetilde{\tau})^2} + 1} \leq \sqrt{\frac{7}{12}} =: c_V$$

since $\frac{\sqrt{3}}{2} \leq \operatorname{Im}(\widetilde{\tau}) \leq |\widetilde{\tau}|$. Therefore $V \subseteq \overline{\mathcal{B}}(0, |\tau|\, c_V)$.

Since $0 \leq \operatorname{Re}(\widetilde{\tau}) \leq 1$, we see that $\operatorname{Im}(v_1) \geq \operatorname{Im}(v_0) = \operatorname{Im}(v_2)$. By construction, the line from 0 to $\widetilde{\tau}$ intersects the line from v_0 to v_1 at $\frac{1}{2}\widetilde{\tau}$, so $\frac{1}{2}\,|\widetilde{\tau}|$ is an upper bound for the largest circle inside V. Analogously we get $\frac{1}{2}\,|\widetilde{\tau}-1|$ as a bound, and from the line from 0 to 1 we get $\frac{1}{2}$. Since $\widetilde{\tau}$ and $\widetilde{\tau}-1$ are lattice points and not zero, their norms are at least 1, so $\overline{\mathcal{B}}\big(0, \frac{1}{2}\big)$ is inside V.

(d) The area of V can be calculated easily, because $\operatorname{Im}(v_0) = \operatorname{Im}(v_2)$. Thus, splitting up the region in a rectangle and a triangle and using symmetry, the result follows.

(e) Let $x \in \tau^{-1}V$. Thus $x = \tau^{-1}z$ for an appropriate $z \in V$. For every $y \in \mathbb{Z}[\tau]$ we obtain

$$|x| = \left|\tau^{-1}\right| |z| \leq \left|\tau^{-1}\right| |z - y| = \left|x - \tau^{-1}y\right|.$$

For an arbitrary $u \in \mathbb{Z}[\tau]$ we can choose $y = \tau u$, and therefore $|x| \leq |x - u|$, i.e., $x \in V$. □

3. Digit Sets and Non-Adjacent Forms

In this section $\tau \in \mathbb{C}$ will be an algebraic integer with $|\tau| > 1$, and let $w \in \mathbb{N}$ with $w \geq 2$. Further let $\mathcal{N}\colon \mathbb{Z}[\tau] \longrightarrow \mathbb{Z}$ denote the norm function. We want to build a numeral system for the elements of $\mathbb{Z}[\tau]$ with base τ. Thus we need a digit set $\mathcal{D}$, which will be a finite subset of $\mathbb{Z}[\tau]$ containing 0.

Definition 3.1 (Reduced Residue Digit Set)**.** Let $\mathcal{D} \subseteq \mathbb{Z}[\tau]$. The set $\mathcal{D}$ is called a *reduced residue digit set modulo* τ^w, if it is consists of 0 and exactly one representative for each residue class of $\mathbb{Z}[\tau]$ modulo τ^w that is not divisible by τ.

From now on suppose $\mathcal{D}$ is a reduced residue digit set modulo τ^w. The following two auxiliary results are well-known; we include a proof for the sake of completeness.

Lemma 3.2. *Let c be a rational integer. Then τ divides c in $\mathbb{Z}[\tau]$ if and only if $\mathcal{N}(\tau)$ divides c in $\mathbb{Z}$.*

Proof. From the minimal polynomial, it is clear that τ divides $\mathcal{N}(\tau)$ in $\mathbb{Z}[\tau]$, so $\mathcal{N}(\tau) \mid c$ implies $\tau \mid c$.

For the converse direction, assume that $\tau \cdot \left(\sum_{j=0}^{d-1} x_j \tau^j\right) = c$ for some rational integers x_j. There d is the degree of τ. Write the minimal polynomial of τ as

$$\tau^d + \sum_{j=0}^{d-1} a_j \tau^j = 0.$$

Thus we obtain

$$c = -x_{d-1}a_0 + \sum_{j=1}^{d-1} (x_{j-1} - x_{d-1}a_j)\tau^j.$$

Comparing coefficients in τ^j yields $c = -x_{d-1}a_0$, which implies that $a_0 = (-1)^d \mathcal{N}(\tau)$ divides c in $\mathbb{Z}$, as required. □

Next, we determine the cardinality of $\mathcal{D}$ by giving an explicit system of representatives of the residue classes.

Lemma 3.3. *A complete residue system modulo τ^w is given by*

$$\sum_{j=0}^{w-1} a_j \tau^j \text{ with } a_j \in \{0, \ldots, \mathcal{N}(\tau) - 1\} \text{ for } 0 \leq j < w. \tag{3.1}$$

In particular, there are $\mathcal{N}(\tau)^w$ residue classes modulo τ^w in $\mathbb{Z}[\tau]$.

A representative $\sum_{j=0}^{w-1} a_j \tau^j$ with $a_j \in \{0, \ldots, \mathcal{N}(\tau) - 1\}$ is divisible by τ if and only if $a_0 = 0$. In particular, the cardinality of $\mathcal{D}$ equals $\mathcal{N}(\tau)^{w-1}(\mathcal{N}(\tau) - 1) + 1$.

Proof. Every element z of $\mathbb{Z}[\tau]$ can be written as

$$z = x\tau^w + \sum_{j=0}^{w-1} a_j \tau^j$$

for some $a_j \in \{0, \ldots, \mathcal{N}(\tau) - 1\}$ and an appropriate $x \in \mathbb{Z}[\tau]$: Take the expansion of z with respect to the $\mathbb{Z}$-basis τ^j, $0 \leq j < d$ and subtract appropriate multiples of the minimal polynomial of τ in order to enforce $0 \leq a_j < \mathcal{N}(\tau)$ for $0 \leq j \leq w - 1$. This shows that (3.1) indeed covers all residue classes modulo τ^w.

Assume that $\sum_{j=0}^{w-1} a_j \tau^j \equiv \sum_{j=0}^{w-1} b_j \tau^j \pmod{\tau^w}$ for some a_j, $b_j \in \{0, \ldots, \mathcal{N}(\tau) - 1\}$, but $a_j \neq b_j$ for some j. We choose $0 \leq j_0 \leq w - 1$ minimal such that $a_{j_0} \neq b_{j_0}$. We obtain

$$\sum_{j=j_0}^{w-1} a_j \tau^{j-j_0} \equiv \sum_{j=j_0}^{w-1} b_j \tau^{j-j_0} \pmod{\tau^{w-j_0}},$$

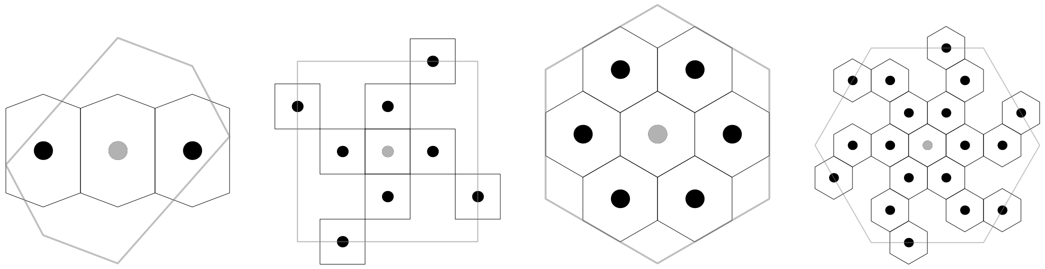
which implies that $a_{j_0} \equiv b_{j_0} \pmod{\tau}$. By Lemma 3.2 on the previous page, this implies that $a_{j_0} = b_{j_0}$, contradiction. Thus (3.1) is indeed a complete system of residues modulo τ^w.

From Lemma 3.2 on the preceding page we also see that exactly the $\mathcal{N}(\tau)^{w-1}$ residue classes $\sum_{j=1}^{w-1} a_j \tau^j$ are divisible by τ. We conclude that $\#\mathcal{D} = \mathcal{N}(\tau)^{w-1}(\mathcal{N}(\tau) - 1) + 1$. □

Since our digit set $\mathcal{D}$ is constructed of residue classes, we want a uniqueness in choosing the representative. We have the following definition, where the restricted Voronoi $\widetilde{V}$ for the point 0 from Definition 2.2 on page 4 is used.

Definition 3.4 (Representatives of Minimal Norm)**.** Let τ be an algebraic integer, imaginary quadratic, and let $\eta \in \mathbb{Z}[\tau]$ be not divisible by τ. Then η is called a *representative of minimal norm of its residue class*, if $\eta \in \tau^w \widetilde{V}$.

With this definition we can define the following digit set, cf. Solinas [19, 20] or Blake, Kumar Murty and Xu [6].



(a) Digit set for $\tau = \frac{1}{2} + \frac{1}{2}\sqrt{-7}$ and $w = 2$.
(b) Digit set for $\tau = 1 + \sqrt{-1}$ and $w = 4$.
(c) Digit set for $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$ and $w = 2$.
(d) Digit set for $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$ and $w = 3$.

Figure 3.1: Minimal norm representatives digit sets modulo τ^w for different τ and w. For each digit η, the corresponding Voronoi cell V_η is drawn. The large scaled Voronoi cell is $\tau^w V$.

Definition 3.5 (Minimal Norm Representatives Digit Set)**.** Let τ be an algebraic integer, imaginary quadratic, and let $\mathcal{D}$ be a reduced residue digit set modulo τ^w consisting of representatives of minimum norm of its residue classes. Then we will call such a digit set *minimal norm representatives digit set modulo* τ^w.

From now on we will suppose that our digit set $\mathcal{D}$ is a minimal norm representatives digit set modulo τ^w. Some examples are shown in Figure 3.1.

The following remark summarises some basic properties of minimal norm representatives and the defined digit sets.

Remark 3.6. Let τ be an algebraic integer, imaginary quadratic. We have the following equivalence. The condition

$$|\eta| \leq |\xi| \text{ for all } \xi \in \mathbb{Z}[\tau] \text{ with } \eta \equiv \xi \pmod{\tau^w}$$

is fulfilled, if and only if $\eta \in \tau^w V$. The advantage of using the restricted Voronoi cell in Definition 3.4 on the preceding page is that also points on the boundary are handled uniquely.

Further we get for all $\eta \in \mathcal{D}$ that $|\eta| \leq |\tau|^{w+1} c_V$. On the other side, if an element of $\mathbb{Z}[\tau]$, which is not divisible by τ, has norm less than $\frac{1}{2}\tau^w$, cf. Proposition 2.5 on page 5, it is a digit. See also Lemma 3.3 on the preceding page.

Since $\mathcal{D} \subseteq \mathbb{Z}[\tau]$, all non-zero elements have norm at least 1.

We can assume that $0 \leq \arg(\tau) \leq \frac{\pi}{2}$. Using any other τ lead to the same digit sets, except some mirroring at the real axis, imaginary axis, or at the origin. By adapting the definition of the boundary of the restricted Voronoi cell, Definition 2.2 on page 4, these mirroring effects can be handled.

Now we are ready to define the numbers built with our digit set $\mathcal{D}$.

Definition 3.7 (Width-w τ-adic Non-Adjacent Forms)**.** Let $\boldsymbol{\eta} = (\eta_j)_{j\in\mathbb{Z}} \in \mathcal{D}^{\mathbb{Z}}$. The sequence $\boldsymbol{\eta}$ is called a *width-w τ-adic non-adjacent form*, or *w-NAF* for short, if each factor $\eta_{j+w-1}\dots\eta_j$, i.e., each block of length w, contains at most one non-zero digit.

Let $J = \{j \in \mathbb{Z} \mid \eta_j \neq 0\}$. We call $\sup(\{0\} \cup (J+1))$ the *left-length of the w-NAF $\boldsymbol{\eta}$* and $-\inf(\{0\} \cup J)$ the *right-length of the w-NAF $\boldsymbol{\eta}$*.

Let λ and ρ be elements of $\mathbb{N}_0 \cup \{\mathsf{fin}, \infty\}$, where fin means finite. We denote the *set of all w-NAFs of left-length at most λ and right-length at most ρ* by $\mathbf{NAF}_w^{\lambda.\rho}$. If $\rho = 0$, then we will simply write $\mathbf{NAF}_w^{\lambda}$. The elements of the set $\mathbf{NAF}_w^{\mathsf{fin}}$ will be called *integer w-NAFs*.

For $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ we call

$$\mathsf{value}(\boldsymbol{\eta}) := \sum_{j\in\mathbb{Z}} \eta_j \tau^j$$

the *value of the w-NAF $\boldsymbol{\eta}$*.

The following notations and conventions are used. A block of zero digits is denoted by $\mathbf{0}$. For a digit η and $k \in \mathbb{N}_0$ we will use

$$\eta^k := \underbrace{\eta \dots \eta}_{k},$$

with the convention $\eta^0 := \varepsilon$, where ε denotes the empty word. A w-NAF $\boldsymbol{\eta} = (\eta_j)_{j\in\mathbb{Z}}$ will be written as $\boldsymbol{\eta}_I\boldsymbol{.}\boldsymbol{\eta}_F$, where $\boldsymbol{\eta}_I$ contains the η_j with $j \geq 0$ and $\boldsymbol{\eta}_F$ contains the η_j with $j < 0$. $\boldsymbol{\eta}_I$ is called *integer part*, $\boldsymbol{\eta}_F$ *fractional part*, and the dot is called *τ-point.* Left-leading zeros in $\boldsymbol{\eta}_I$ can be skipped, except η_0, and right-leading zeros in $\boldsymbol{\eta}_F$ can be skipped as well. If $\boldsymbol{\eta}_F$ is a sequence containing only zeros, the τ-point and this sequence is not drawn.

Further, for a w-NAF $\boldsymbol{\eta}$ (a bold, usually small Greek letter) we will always use η_j (the same letter, but indexed and not bold) for the elements of the sequence.

To see where the values, respectively the fractional values of our w-NAFs lie in the complex plane, have a look at Figure 9.1 on page 32. There some examples are drawn.

The set $\mathbf{NAF}_w^{\mathsf{fin}.\infty}$ can be equipped with a metric. It is defined in the following way. Let $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ and $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$, then

$$\mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}, \boldsymbol{\xi}) := \begin{cases} |\tau|^{\max\{j\in\mathbb{Z} \mid \eta_j \neq \xi_j\}} & \text{if } \boldsymbol{\eta} \neq \boldsymbol{\xi}, \\ 0 & \text{if } \boldsymbol{\eta} = \boldsymbol{\xi}. \end{cases}$$

So the largest index, where the two w-NAFs differ, decides their distance. See for example Edgar [8] for details on such metrics.

We get the following continuity result.

Proposition 3.8. *The value function* value *is Lipschitz continuous on* $\mathbf{NAF}_w^{\mathsf{fin}.\infty}$*.*

Proof. Let $c_{\mathcal{D}}$ be a bound for the absolute value of the digits in the digit set $\mathcal{D}$. Let $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ and $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$, $\boldsymbol{\eta} \neq \boldsymbol{\xi}$, with $\mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}, \boldsymbol{\xi}) = |\tau|^J$. Since $\boldsymbol{\eta}$ and $\boldsymbol{\xi}$ are equal on all digits with index larger than J we obtain

$$|\mathsf{value}(\boldsymbol{\eta}) - \mathsf{value}(\boldsymbol{\xi})| \leq \sum_{j\leq J} |\eta_j - \xi_j|\, |\tau|^j \leq 2c_{\mathcal{D}} \frac{|\tau|^J}{1-|\tau|^{-1}} = \frac{2c_{\mathcal{D}}}{1-|\tau|^{-1}} \mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}, \boldsymbol{\xi}) \,.$$

Thus Lipschitz continuity is proved. □

Furthermore, we get a compactness result on the metric space $\mathbf{NAF}_w^{\ell.\infty} \subseteq \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ in the proposition below. The metric space $\mathbf{NAF}_w^{\mathsf{fin}.\infty}$ is not compact, because if we fix a non-zero digit η, then the sequence $\left(\eta 0^j\right)_{j\in\mathbb{N}_0}$ has no convergent subsequence, but all $\eta 0^j$ are in the set $\mathbf{NAF}_w^{\mathsf{fin}.\infty}$.

Proposition 3.9. *For every $\ell \geq 0$ the metric space $\left(\mathbf{NAF}_w^{\ell.\infty}, \mathrm{d}_{\mathsf{NAF}}\right)$ is compact.*

Proof. Let $(\boldsymbol{\xi}_{0,j})_{j\in\mathbb{N}_0}$ be a sequence with $\boldsymbol{\xi}_{0,j} \in \mathbf{NAF}_w^{\ell.\infty}$. We can assume $\boldsymbol{\xi}_{0,j} \in \mathbf{NAF}_w^{0.\infty}$, therefore each word $\boldsymbol{\xi}_{0,j}$ has digits zero for non-negative index. Now consider the digit with index -1. There is a subsequence $(\boldsymbol{\xi}_{1,j})_{j\in\mathbb{N}_0}$ of $(\boldsymbol{\xi}_{0,j})_{j\in\mathbb{N}_0}$, such that digit -1 is a fixed digit η_{-1}. Next there is a subsequence $(\boldsymbol{\xi}_{2,j})_{j\in\mathbb{N}_0}$ of $(\boldsymbol{\xi}_{1,j})_{j\in\mathbb{N}_0}$, such that digit -2 is a fixed digit η_{-2}. This process can be repeated for each $k \geq 1$ to get sequences $(\boldsymbol{\xi}_{k,j})_{j\in\mathbb{N}_0}$ and digits η_{-k}.

The sequence $(\boldsymbol{\vartheta}_j)_{j\in\mathbb{N}_0}$ with $\boldsymbol{\vartheta}_j := \boldsymbol{\xi}_{j,j}$ converges to $\boldsymbol{\eta}$, since for $\varepsilon > 0$ there is an $J \in \mathbb{N}_0$ such that for all $j \geq J$

$$\mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}, \boldsymbol{\vartheta}_j) \leq |\tau|^{-(J+1)} < \varepsilon.$$

It is clear that $\boldsymbol{\eta}$ is indeed an element of $\mathbf{NAF}_w^{0.\infty}$, as its first k digits coincide with $\boldsymbol{\xi}_{k,k} \in \mathbf{NAF}_w^{0.\infty}$ for all k. So we have found a converging subsequence of $(\boldsymbol{\xi}_{0,j})_{j\in\mathbb{N}_0}$, which proves the compactness. □

Remark 3.10. The compactness of $\left(\mathbf{NAF}_w^{\ell.\infty}, \mathrm{d}_{\mathsf{NAF}}\right)$ can also be deduced from general theory. As a consequence of Tychonoff's Theorem the set $\mathcal{D}^{\mathbb{N}}$ is a compact space, the product topology (of the discrete topology on $\mathcal{D}$) coincides with the topology induced by the obvious generalisation of the metric $\mathrm{d}_{\mathsf{NAF}}$. The subset $\mathbf{NAF}_w^{0.\infty} \subseteq \mathcal{D}^{\mathbb{N}}$ is closed and therefore compact, too.

We want to express all integers in $\mathbb{Z}[\tau]$ by finite w-NAFs. Thus we restrict ourselves to suitable digit sets, cf. Muir and Stinson [17].

Definition 3.11 (Width-w Non-Adjacent Digit Set)**.** A digit set $\mathcal{D}$ is called a *width-w non-adjacent digit set*, or w-NADS for short, when every element $z \in \mathbb{Z}[\tau]$ admits a unique w-NAF $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}}$, i.e., $\mathsf{value}(\boldsymbol{\eta}) = z$. When this is the case, the function

$$\mathsf{value}|_{\mathbf{NAF}_w^{\mathsf{fin}}} \colon \mathbf{NAF}_w^{\mathsf{fin}} \longrightarrow \mathbb{Z}[\tau]$$

is bijective, and we will denote its inverse function by NAF_w.

Later, namely in Section 6, we will see that the digit set of minimal norm representatives is a w-NADS if τ is imaginary quadratic.

4. Full Block Length Analysis of Non-Adjacent Forms

Let $\tau \in \mathbb{C}$ be an algebraic integer, $w \in \mathbb{N}$ with $w \geq 2$, and $\mathcal{D}$ be a reduced residue digit set, cf. Definition 3.1 on page 7. Let $\mathcal{N} \colon \mathbb{Z}[\tau] \longrightarrow \mathbb{Z}$ denote the norm function.

Further, in this section all w-NAFs will be out of the set $\mathbf{NAF}_w^{\mathsf{fin}}$, and with *length* the left-length is meant.

This general setting allows us to analyse digit frequencies under the *full block length modell,*, i.e., we assume that all w-NAFs of given length are equally likely. We will prove the following theorem.

Theorem 4.1 (Full Block Length Distribution Theorem)**.** *We denote the number of w-NAFs of length $n \in \mathbb{N}_0$ by $C_{n,w}$, i.e., $C_{n,w} = \#(\mathbf{NAF}_w^n)$, and we get*

$$C_{n,w} = \frac{1}{(\mathcal{N}(\tau)-1)w+1}\,\mathcal{N}(\tau)^{n+w} + \mathcal{O}((\rho\mathcal{N}(\tau))^n)\,,$$

where $\rho = (1 + \frac{1}{\mathcal{N}(\tau)w^3})^{-1} < 1$.

Further let $0 \neq \eta \in \mathcal{D}$ be a fixed digit and define the random variable $X_{n,w,\eta}$ to be the number of occurrences of the digit η in a random w-NAF of length n, where every w-NAF of length n is assumed to be equally likely.

Then the following explicit expressions hold for the expectation and the variance of $X_{n,w,\eta}$:

$$\mathbb{E}(X_{n,w,\eta}) = e_w n + \frac{(\mathcal{N}(\tau)-1)(w-1)w}{\mathcal{N}(\tau)^{w-1}\,((\mathcal{N}(\tau)-1)w+1)^2} + \mathcal{O}(n\rho^n) \tag{4.1}$$

$$\begin{aligned}\mathbb{V}(X_{n,w,\eta}) = v_w n &\\ &+ \frac{(w-1)w\bigl(-(w-1)^2-\mathcal{N}(\tau)^2w^2+(\mathcal{N}(\tau)-1)\,\mathcal{N}(\tau)^{w-1}((\mathcal{N}(\tau)-1)w+1)^2+2\,\mathcal{N}(\tau)\bigl(w^2-w+1\bigr)\bigr)}{\mathcal{N}(\tau)^{2w-2}\,((\mathcal{N}(\tau)-1)w+1)^4}\\ &+ \mathcal{O}\bigl(n^2\rho^n\bigr)\,,\end{aligned} \tag{4.2}$$

where

$$e_w = \frac{1}{\mathcal{N}(\tau)^{w-1}\,((\mathcal{N}(\tau)-1)w+1)},$$

and

$$v_w = \frac{\mathcal{N}(\tau)^{w-1}\,((\mathcal{N}(\tau)-1)w+1)^2 - \bigl((\mathcal{N}(\tau)-1)w^2+2w-1\bigr)}{\mathcal{N}(\tau)^{2w-2}\,((\mathcal{N}(\tau)-1)w+1)^3}.$$

Furthermore, $X_{n,w,\eta}$ satisfies the central limit theorem

$$\mathbb{P}\biggl(\frac{X_{n,w,\eta}-e_w n}{\sqrt{v_w n}} \leq x\biggr) = \Phi(x) + \mathcal{O}\biggl(\frac{1}{\sqrt{n}}\biggr)\,,$$

uniformly with respect to $x \in \mathbb{R}$, where $\Phi(x) = (2\pi)^{-1/2}\int_{t \leq x} e^{-t^2/2}\,dt$ is the standard normal distribution.

For the proof we need estimates for the zeros of a polynomial which will be needed for estimating the non-dominant roots of our generating function.

Lemma 4.2. *Let $t \geq 2$ and*

$$f(z) = 1 - \frac{1}{t}z - \left(1 - \frac{1}{t}\right) z^w.$$

Then $f(z)$ has exactly one root with $|z| \leq 1 + \frac{1}{tw^3}$, namely $z = 1$.

Proof. It is easily checked that $f(1) = 0$. Assume that $z \neq 1$ is another root of f. As the coefficients of f are reals, it is sufficient to consider z with $\operatorname{Im}(z) \geq 0$. If $|z| < 1$, then

$$1 = \left|\frac{1}{t}z + \left(1 - \frac{1}{t}\right) z^w\right| \leq \frac{1}{t}|z| + \left(1 - \frac{1}{t}\right) |z|^w < \frac{1}{t} + \left(1 - \frac{1}{t}\right) = 1,$$

which is a contradiction. Therefore, we have $|z| \geq 1$. We write $z = re^{i\psi}$ for appropriate $r \geq 1$ and $0 \leq \psi \leq \pi$. For $r > 0$, $f(r)$ is strictly decreasing, so we can assume that $\psi > 0$.

For $\psi < \pi/w$, we have $\sin(w\psi) > 0$ and $\sin(\psi) > 0$, which implies that $\operatorname{Im}\bigl(f(re^{i\psi})\bigr) = -\frac{1}{t}\sin\psi - \bigl(1 - \frac{1}{t}\bigr)\sin(\psi w) < 0$, a contradiction. We conclude that $\psi \geq \pi/w$.

Next, we see that $f(re^{i\psi}) = 0$ implies that

$$1 - \frac{2r}{t}\cos\psi + \frac{r^2}{t^2} = \left|1 - \frac{1}{t}re^{i\psi}\right|^2 = \left(1 - \frac{1}{t}\right)^2 r^{2w}.$$

We have $\cos\psi \leq \cos(\pi/w)$, which implies that

$$\left(1 - \frac{1}{t}\right)^2 r^{2w} \geq 1 - \frac{2r}{t}\cos\frac{\pi}{w} + \frac{r^2}{t^2} = \left(1 - \frac{r}{t}\right)^2 + \left(1 - \cos\frac{\pi}{w}\right)\frac{2r}{t}. \tag{4.3}$$

For $w \geq 4$ and $r < \sqrt{2}$, the right hand side of (4.3) is decreasing and the left hand side is increasing. Thus, for $r \leq 1 + 1/(tw^3)$, (4.3) yields

$$\left(1 - \frac{1}{t}\right)^2 \left(1 + \frac{1}{tw^3}\right)^{2w} \geq \left(1 - \frac{1}{t}\cdot\left(1 + \frac{1}{tw^3}\right)\right)^2 + \left(1 - \cos\frac{\pi}{w}\right)\frac{2}{t}\left(1 + \frac{1}{tw^3}\right).$$

Using the estimates $(1 + \frac{1}{tw^3})^{2w} \leq 1 + \frac{2}{tw^2} + \frac{2}{t^2w^4}$ and $\cos\left(\frac{\pi}{w}\right) \leq 1 - \frac{\pi^2}{2w^2} + \frac{\pi^4}{24w^4}$, we obtain

$$\left(\frac{2 - \pi^2}{t} - \frac{4}{t^2} + \frac{2}{t^3}\right)\frac{1}{w^2} + \left(\frac{2}{t^2} - \frac{2}{t^3}\right)\frac{1}{w^3} + \left(\frac{\pi^4}{12t} + \frac{2}{t^2} - \frac{4}{t^3} + \frac{2}{t^4}\right)\frac{1}{w^4} - \frac{\pi^2}{t^2w^5} - \frac{1}{t^4w^6} + \frac{\pi^4}{12t^2w^7} \geq 0,$$

which is a contradiction for $w \geq 4$ and $t \geq 2$.

For $w = 3$, we easily check that $|z| = \sqrt{\frac{t}{t-1}} \geq 1 + 1/(27t)$; similarly, for $w = 2$, we have $|z| = t/(t-1) > 1 + 1/(4t)$. □

Proof of Theorem 4.1. For simplicity we set $\mathcal{D}^\bullet := \mathcal{D} \setminus \{0\}$. A w-NAF can be described by the regular expression

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

Let a_{mn} be the number of w-NAFs of length n containing exactly m occurrences of the digit η. We consider the generating function $G(Y,Z) = \sum_{m,n} a_{mn}Y^mZ^n$. From the regular expression we see that

$$G(Y,Z) = \frac{1 + (Y + (\#\mathcal{D}^\bullet - 1))\frac{Z^w - Z}{Z-1}}{1 - Z - YZ^w - (\#\mathcal{D}^\bullet - 1)Z^w}.$$

We start with determining the number of w-NAFs of length n. This amounts to extracting the coefficient of Z^n of

$$G(1,Z) = \frac{1 + (\#\mathcal{D}^\bullet - 1)Z - \#\mathcal{D}^\bullet\cdot Z^w}{(1 - Z)(1 - Z - \#\mathcal{D}^\bullet\cdot Z^w)}.$$

This requires finding the dominant root of the denominator. Setting $z = \mathcal{N}(\tau)\, Z$ in the second factor yields

$$1 - \frac{1}{\mathcal{N}(\tau)} z - \left(1 - \frac{1}{\mathcal{N}(\tau)}\right) z^{w}.$$

From Lemma 4.2 on the preceding page, we see that the dominant root of the denominator of $G(1, Z)$ is $Z = 1/\mathcal{N}(\tau)$, and that all other roots satisfy $|Z| \geq 1/\mathcal{N}(\tau) + 1/(\mathcal{N}(\tau)^2\, w^3)$. Extracting the coefficient of Z^n of $G(1, Z)$ then yields the number $C_{n,w}$ of w-NAFs of length n as

$$\frac{1}{(\mathcal{N}(\tau) - 1)w + 1} \mathcal{N}(\tau)^{n+w} + \mathcal{O}((\rho \mathcal{N}(\tau))^n)\,, \tag{4.4}$$

where $\rho = (1 + \frac{1}{\mathcal{N}(\tau) w^3})^{-1}$.

The number of occurrences of the digit μ amongst all w-NAFs of length n is

$$\begin{aligned}[Z^n]\, \frac{\partial G(Y, Z)}{\partial Y}\bigg|_{Y=1} &= \frac{Z}{\left(1 - Z - \left(1 - \frac{1}{\mathcal{N}(\tau)}\right) (\mathcal{N}(\tau)\, Z)^w\right)^2} \\ &= \frac{1}{((\mathcal{N}(\tau) - 1)w + 1)^2} n \mathcal{N}(\tau)^{n+1} + \frac{(\mathcal{N}(\tau) - 1)(w-1)w}{((\mathcal{N}(\tau) - 1)w + 1)^3} \mathcal{N}(\tau)^{n+1} + \mathcal{O}((\rho \mathcal{N}(\tau))^n)\,.\end{aligned}$$

Dividing this by (4.4) yields (4.1).

In order to compute the second moment, we compute

$$\begin{aligned}[Z^n]\, \frac{\partial^2 G(Y, Z)}{\partial Y^2}\bigg|_{Y=1} &= \frac{2Z^{w+1}}{\left(1 - Z - \left(1 - \frac{1}{\mathcal{N}(\tau)}\right) (\mathcal{N}(\tau)\, Z)^w\right)^3} \\ &= \frac{1}{((\mathcal{N}(\tau) - 1)w + 1)^3} n^2 \mathcal{N}(\tau)^{n-w+2} + \frac{\left((\mathcal{N}(\tau) - 1)w^2 - 2w \mathcal{N}(\tau) + 1\right)}{((\mathcal{N}(\tau) - 1)w + 1)^4} n \mathcal{N}(\tau)^{n-w+2} \\ &\quad - \frac{(w-1)w \left(w \mathcal{N}(\tau)^2 - 2 \mathcal{N}(\tau) - w + 1\right)}{((\mathcal{N}(\tau) - 1)w + 1)^5} \mathcal{N}(\tau)^{n-w+2} + \mathcal{O}((\rho \mathcal{N}(\tau))^n)\,,\end{aligned}$$

which after division by (4.4) yields

$$\begin{aligned}\mathbb{E}(X_{n,w,\eta}(X_{n,w,\eta} - 1)) &= \frac{1}{\mathcal{N}(\tau)^{2w-2} ((\mathcal{N}(\tau) - 1)w + 1)^2} n^2 + \frac{\left((\mathcal{N}(\tau) - 1)w^2 - 2w \mathcal{N}(\tau) + 1\right)}{\mathcal{N}(\tau)^{2w-2} ((\mathcal{N}(\tau) - 1)w + 1)^3} n \\ &\quad - \frac{(w-1)w \left(w \mathcal{N}(\tau)^2 - 2 \mathcal{N}(\tau) - w + 1\right)}{\mathcal{N}(\tau)^{n-w+2} ((\mathcal{N}(\tau) - 1)w + 1)^4} + \mathcal{O}\big(n^2 \rho^n\big)\,.\end{aligned}$$

Adding $\mathbb{E}(X_{n,w,\eta}) - \mathbb{E}(X_{n,w,\eta})^2$ yields the variance given in (4.2).

The asymptotic normality follows from Hwang's Quasi-Power-Theorem [13]. □

5. Bounds for the Value of Non-Adjacent Forms

Let $\tau \in \mathbb{C}$ be an algebraic integer, imaginary quadratic with minimal polynomial $X^2 - pX + q$ with p, $q \in \mathbb{Z}$ such that $4q - p^2 > 0$. Suppose that $|\tau| > 1$. Let $w \in \mathbb{N}$ with $w \geq 2$. Further let $\mathcal{D}$ be a minimal norm representatives digit set modulo τ^w as in Definition 3.5 on page 9.

In this section the *fractional value* of a w-NAF means the value of a w-NAF of the form $0.\boldsymbol{\eta}$. The term *most significant digit* is used for the digit η_{-1}.

So let us have a closer look at the fractional value of a w-NAF. We want to find upper bounds and if we fix a digit, e.g. the most significant one, a lower bound. We need two different approaches to prove those results. The first one is analytic. The results there are valid for all combinations of τ and w except finitely many. These exceptional cases will be called "problematic values". To handle those, we will use an other idea. We will show an equivalence, which directly leads to a simple procedure to check, whether a condition is fulfilled. If this is the case, the procedure terminates and returns the result. This idea is similar to a proof in Matula [16].

The following proposition deals with three upper bounds, one for the absolute value and two give us regions containing the fractional value.

Proposition 5.1 (Upper Bounds for the Fractional Value)**.** *Let $\boldsymbol{\eta} \in \mathbf{NAF}_w^{0.\infty}$, and let*

$$f_U = \frac{|\tau|^w c_V}{1 - |\tau|^{-w}}.$$

Then the following statements are true:

(a) We get

$$|\mathsf{value}(\boldsymbol{\eta})| \leq f_U.$$

(b) Further we have

$$\mathsf{value}(\boldsymbol{\eta}) \in \bigcup_{z \in \tau^{w-1} V} \overline{\mathcal{B}}\Big(z, |\tau|^{-w} f_U\Big).$$

(c) The following two statements are equivalent:

(1) There is an $\ell \in \mathbb{N}_0$, such that for all $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\ell}$ the condition

$$\overline{\mathcal{B}}\Big(\mathsf{value}(\boldsymbol{\xi}), |\tau|^{-\ell} f_U\Big) \subseteq \tau^{2w-1} \operatorname{int}(V)$$

is fulfilled.

(2) There exists an $\varepsilon > 0$, such that for all $\boldsymbol{\vartheta} \in \mathbf{NAF}_w^{0.\infty}$ the condition

$$\mathcal{B}(\mathsf{value}(\boldsymbol{\vartheta}), \varepsilon) \subseteq \tau^{2w-1} V$$

holds.

(d) We get

$$\mathsf{value}(\boldsymbol{\eta}) \in \tau^{2w-1} V.$$

(e) For $\ell \in \mathbb{N}_0$ we have

$$\mathsf{value}(0.\eta_{-1} \dots \eta_{-\ell}) + \tau^{-\ell} V \subseteq \tau^{2w-1} V.$$

Proof. (a) We have

$$|\mathsf{value}(\boldsymbol{\eta})| = \left| \sum_{j=1}^{\infty} \eta_{-j} \tau^{-j} \right| \leq \sum_{j=1}^{\infty} |\eta_{-j}| \, |\tau|^{-j}.$$

We consider w-NAFs, which have $\eta_{-j} \neq 0$ for $-j \equiv 1 \pmod{w}$. For all other w-NAFs the upper bound is smaller. To see this, assume that there are more than $w-1$ adjacent zeros in a w-NAF or the first digits are zero. Then we could build a larger upper bound by shifting digits to the left, i.e., multiplying parts of the sum by $|\tau|$, since $|\tau| > 1$.

We get

$$\begin{aligned} |\mathsf{value}(\boldsymbol{\eta})| &\leq \sum_{j=1}^{\infty} |\eta_{-j}| \, |\tau|^{-j} = \sum_{j=1}^{\infty} [-j \equiv 1 \pmod{w}] \, |\eta_{-j}| \, |\tau|^{-j} \\ &\leq |\tau|^{-1} \sum_{k=0}^{\infty} \left|\eta_{-(wk+1)}\right| |\tau|^{-wk}, \end{aligned}$$

in which we changed the summation index according to $wk+1 = j$ and the Iversonian notation $[expr] = 1$ if $expr$ is true and $[expr] = 0$ otherwise, cf. Graham, Knuth and Patashnik [11], has been used. Using $\left|\eta_{-(wk+1)}\right| \leq |\tau|^{w+1} c_V$, see Remark 3.6 on page 9, yields

$$|\mathsf{value}(\boldsymbol{\eta})| \leq |\tau|^{-1} |\tau|^{w+1} c_V \frac{1}{1 - |\tau|^{-w}} = \underbrace{\frac{|\tau|^w c_V}{1 - |\tau|^{-w}}}_{=: f_U}.$$

(b) There is nothing to show if the w-NAF $\boldsymbol{\eta}$ is zero, and it is sufficient to prove it for $\eta_{-1} \neq 0$. Otherwise, let $k \in \mathbb{N}$ be minimal, such that $\eta_{-k} \neq 0$. Then

$$\tau^{-(k-1)}\tau^{k-1}\,\mathsf{value}(\boldsymbol{\eta}) \in \tau^{-(k-1)} \bigcup_{z \in \tau^{w-1}V} \overline{\mathcal{B}}\Big(z, |\tau|^{-w} f_U\Big) \subseteq \bigcup_{z \in \tau^{w-1}V} \overline{\mathcal{B}}\Big(z, |\tau|^{-w} f_U\Big),$$

since $|\tau| > 1$ and $\tau^{-1}V \subseteq V$, see Proposition 2.5 on page 5.

Since $\eta_{-1} \in \tau^w V$, see Remark 3.6 on page 9, we obtain $\eta_{-1}\tau^{-1} \in \tau^{w-1}V$. Thus, using (a), yields

$$\left|\tau^w \left(\mathsf{value}(\boldsymbol{\eta}) - \eta_{-1}\tau^{-1}\right)\right| \leq f_U,$$

i.e.,

$$\mathsf{value}(\boldsymbol{\eta}) \in \overline{\mathcal{B}}\Big(\eta_{-1}\tau^{-1}, |\tau|^{-w} f_U\Big),$$

which proves the statement.

(c) *(1) $\Longrightarrow$ (2).* Suppose there exists such an $\ell \in \mathbb{N}$. Then there exists an $\varepsilon > 0$ such that

$$\overline{\mathcal{B}}\Big(\mathsf{value}(\boldsymbol{\xi}), |\tau|^{-\ell} f_U + \varepsilon\Big) \subseteq \tau^{2w-1}V$$

for all $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\ell}$, since there are only finitely many $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\ell}$. Let $\boldsymbol{\vartheta} \in \mathbf{NAF}_w^{0.\infty}$. Then there is a $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\ell}$ such that the digits from index -1 to $-\ell$ of $\boldsymbol{\xi}$ and $\boldsymbol{\vartheta}$ coincide. By using (a) we obtain

$$|\mathsf{value}(\boldsymbol{\vartheta}) - \mathsf{value}(\boldsymbol{\xi})| \leq |\tau|^{-\ell} f_U,$$

and thus

$$\overline{\mathcal{B}}(\mathsf{value}(\boldsymbol{\vartheta}), \varepsilon) \subseteq \overline{\mathcal{B}}\Big(\mathsf{value}(\boldsymbol{\xi}), |\tau|^{-\ell} f_U + \varepsilon\Big) \subseteq \tau^{2w-1}V.$$

(2) $\Longrightarrow$ (1). Now suppose there is such an $\varepsilon > 0$. Since there is an $\ell \in \mathbb{N}$ such that $|\tau|^{-\ell} f_U < \varepsilon$, the statement follows.

(d) We know from Proposition 2.5 on page 5 that $\overline{\mathcal{B}}\Big(0, \frac{1}{2}|\tau|^{2w-1}\Big) \subseteq \tau^{2w-1}V$. Therefore, if the upper bound found in (a) fulfils

$$f_U = \frac{|\tau|^w c_V}{1 - |\tau|^{-w}} \leq \frac{1}{2}|\tau|^{2w-1},$$

the statement follows.

The previous inequality is equivalent to

$$\nu := \frac{1}{2} - \frac{|\tau|\, c_V}{|\tau|^w - 1} \geq 0.$$

The condition is violated for $w = 2$ and $|\tau|$ equal to $\sqrt{2}$, $\sqrt{3}$ or $\sqrt{4}$, and for $w = 3$ and $|\tau| = \sqrt{2}$, see Table 5.1 on the next page. Since ν is monotonic increasing for $|\tau|$ and for w, there are no other "problematic cases".

For those cases we will use (c). For each of the "problematic cases" an ℓ satisfying the condition (1) of equivalences in (c) was found, see Table 5.2 on page 17 for the results. Thus the statement is proved.

(e) Analogously to the proof of (a), except that we use ℓ for the upper bound of the sum, we obtain for $v \in V$

$$\begin{aligned}
\left|\mathsf{value}(0\centerdot\eta_{-1}\ldots\eta_{-\ell}) + \tau^{-\ell}v\right| &\leq |\mathsf{value}(0\centerdot\eta_{-1}\ldots\eta_{-\ell})| + \left|\tau^{-\ell}\right| |\tau|\, c_V \\
&\leq \frac{|\tau|^w c_V}{1 - |\tau|^{-w}} \left(1 - |\tau|^{-w\left\lfloor\frac{\ell-1+w}{w}\right\rfloor}\right) + |\tau|^{-\ell+1} c_V \\
&\leq \frac{|\tau|^w c_V}{1 - |\tau|^{-w}} \left(1 - |\tau|^{-\ell+1-w} + |\tau|^{-\ell+1-w}\left(1 - |\tau|^{-w}\right)\right) \\
&= \frac{|\tau|^w c_V}{1 - |\tau|^{-w}} \left(1 - |\tau|^{-\ell+1-2w}\right).
\end{aligned}$$

	$w=2$	$w=3$	$w=4$
$\lvert\tau\rvert = \sqrt{2}$	-0.58012	-0.09074	0.13996
$\lvert\tau\rvert = \sqrt{3}$	-0.16144	0.18474	0.33464
$\lvert\tau\rvert = \sqrt{4}$	-0.00918	0.28178	0.39816
$\lvert\tau\rvert = \sqrt{5}$	0.07304	0.33224	0.42884

Table 5.1: Values (given five decimal places) of $\nu = \frac{1}{2} - \frac{|\tau| c_V}{|\tau|^w - 1}$ for different $|\tau|$ and w. A negative sign means that this value is a "problematic value".

Since $1 - |\tau|^{-\ell+1-2w} < 1$ we get

$$\left|\mathsf{value}(0.\eta_{-1}\ldots\eta_{-\ell}) + \tau^{-\ell}V\right| \leq \frac{|\tau|^w c_V}{1-|\tau|^{-w}} = f_U$$

for all $\ell \in \mathbb{N}_0$.

Let $z \in \mathbb{C}$. Have again a look at the proof of (d). If $\nu > 0$ there, we get that $|z| \leq f_U$ implies $z \in \tau^{2w-1}V$.

Combining these two results yields the inclusion for $\nu > 0$, i.e., the "problematic cases" are left. Again, each of these cases has to be considered separately.

For each of the problematic cases, we find a $k \in \mathbb{N}_0$ such that

$$\overline{\mathcal{B}}\Big(\mathsf{value}(\boldsymbol{\xi}), 2\,|\tau|^{-k} f_U\Big) \subseteq \tau^{2w-1}V$$

holds for all $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.k}$. These k are listed in Table 5.3 on page 18.

For $\ell > k$ and $v \in V$, we obtain

$$\begin{aligned}\left|\mathsf{value}\big(0.0\ldots0\eta_{-(k+1)}\ldots\eta_{-\ell}\big) + \tau^{-\ell}v\right| &\leq |\tau|^{-k} f_U + |\tau|^{-\ell}|\tau| c_V \\ &\leq |\tau|^{-k} f_U\left(1 + \frac{c_V}{f_U}\right) \\ &= |\tau|^{-k} f_U\left(1 + \frac{1-|\tau|^{-w}}{|\tau|^w}\right) \\ &\leq 2\,|\tau|^{-k} f_U\end{aligned}$$

using (a), Proposition 2.5 on page 5, and $|\tau|^w > 1$. Thus the desired inclusion follows for $\ell > k$.

For the finitely many $\ell \leq k$ we additionally check all possibilities, i.e., whether for all combinations of $\boldsymbol{\vartheta} \in \mathbf{NAF}_w^{0.\ell}$ and vertices of the boundary of $\mathsf{value}(\boldsymbol{\vartheta}) + \tau^{-\ell}V$ the corresponding value is inside $\tau^{2w-1}V$. Convexity of V is used here. All combinations were valid, see last column of Table 5.3 on page 18, thus the inclusion proved. □

Next we want to find a lower bound for the fractional value of a w-NAF. Clearly the w-NAF 0 has fractional value 0, so we are interested in cases, where we have a non-zero digit somewhere.

Proposition 5.2 (Lower Bound for the Fractional Value). *The following is true:*

(a) The following two statements are equivalent:

(1) There is an $\ell \in \mathbb{N}_0$, such that for all $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\ell}$ with non-zero most significant digit the condition

$$|\mathsf{value}(\boldsymbol{\xi})| > |\tau|^{-\ell} f_U$$

is fulfilled.

(2) There exists a $\widetilde{\nu} > 0$, such that for all $\boldsymbol{\vartheta} \in \mathbf{NAF}_w^{0.\infty}$ with non-zero most significant digit the condition

$$|\mathsf{value}(\boldsymbol{\vartheta})| \geq |\tau|^{-1}\widetilde{\nu}.$$

holds.

$q = \lvert\tau\rvert^2$	p	$\mathrm{Re}(\tau)$	$\mathrm{Im}(\tau)$	w	ℓ found?	ℓ	$\lvert\tau\rvert^{-\ell} f_U$	ε
2	-2	-1	1	2	*true*	8	0.1909	0.03003
2	-1	-0.5	1.323	2	*true*	4	0.7638	0.02068
2	0	0	1.414	2	*true*	6	0.3819	0.1484
2	1	0.5	1.323	2	*true*	4	0.7638	0.02068
2	2	1	1	2	*true*	7	0.27	0.08352
2	-2	-1	1	3	*true*	2	1.671	0.4505
2	-1	-0.5	1.323	3	*true*	2	1.671	0.4726
2	0	0	1.414	3	*true*	2	1.671	0.4505
2	1	0.5	1.323	3	*true*	2	1.671	0.4726
2	2	1	1	3	*true*	2	1.671	0.4505
3	-3	-1.5	0.866	2	*true*	1	1.984	0.03641
3	-2	-1	1.414	2	*true*	2	1.146	0.5543
3	-1	-0.5	1.658	2	*true*	2	1.146	0.4581
3	0	0	1.732	2	*true*	1	1.984	0.03641
3	1	0.5	1.658	2	*true*	2	1.146	0.4581
3	2	1	1.414	2	*true*	2	1.146	0.5543
3	3	1.5	0.866	2	*true*	1	1.984	0.03641
4	-3	-1.5	1.323	2	*true*	1	2.037	0.9164
4	-2	-1	1.732	2	*true*	1	2.037	0.4633
4	-1	-0.5	1.936	2	*true*	1	2.037	0.3227
4	0	0	2	2	*true*	1	2.037	0.9633
4	1	0.5	1.936	2	*true*	1	2.037	0.3227
4	2	1	1.732	2	*true*	1	2.037	0.4633
4	3	1.5	1.323	2	*true*	1	2.037	0.9164

Table 5.2: Upper bound inclusion $\mathsf{value}(\boldsymbol{\eta}) \in \tau^{2w-1}V$ checked for “problematic values” of $\lvert\tau\rvert$ and w, cf. (d) of Proposition 5.1 on page 14. The dependence of p, q and τ is given by $\tau^2 - p\tau + q = 0$. We have $p^2 < 4q$, since τ is assumed to be imaginary quadratic.

(b) Let $\boldsymbol{\eta} \in \mathbf{NAF}_w^{0.\infty}$ with non-zero most significant digit. Then

$$\lvert\mathsf{value}(\boldsymbol{\eta})\rvert \geq \lvert\tau\rvert^{-1} f_L$$

with $f_L = \nu$ if $\nu > 0$, where

$$\nu = \frac{1}{2} - \frac{\lvert\tau\rvert\, c_V}{\lvert\tau\rvert^w - 1}.$$

If $\nu \leq 0$, see Table 5.1 on the facing page, then we set $f_L = \widetilde{\nu}$ from Table 5.4 on page 19.

Proof of Proposition 5.2. (a) We have to prove both directions.

(1) $\Longrightarrow$ (2). Suppose there exists such an $\ell \in \mathbb{N}_0$. We set

$$\widetilde{\nu} = \min\left\{ \lvert\tau\rvert \left(\lvert\mathsf{value}(\boldsymbol{\xi})\rvert - \lvert\tau\rvert^{-\ell} f_U \right) \,\middle|\, \boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\ell} \text{ with } \xi_{-1} \neq 0 \right\}.$$

Then clearly $\widetilde{\nu} > 0$. Using (a) of Proposition 5.1 on page 14 with digits shifted ℓ to the right, i.e., multiplication by $\tau^{-\ell}$, the desired result follows by using the triangle inequality.

(2) $\Longrightarrow$ (1). Now suppose there exists such a lower bound $\widetilde{\nu} > 0$. Then there is an $\ell \in \mathbb{N}_0$ such that $\lvert\tau\rvert^{-\ell} f_U < \lvert\tau\rvert^{-1} \widetilde{\nu}$. Since

$$\lvert\mathsf{value}(0.\eta_{-1} \ldots \eta_{-\ell})\rvert \geq \lvert\tau\rvert^{-1} \widetilde{\nu} > \lvert\tau\rvert^{-\ell} f_U$$

for all w-NAFs $0.\eta_{-1} \ldots \eta_{-\ell}$, the statement follows.

$q = \lvert\tau\rvert^2$	p	$\mathrm{Re}(\tau)$	$\mathrm{Im}(\tau)$	w	k found?	k	$2\lvert\tau\rvert^{-k} f_U$	ε	valid for $\ell \leq k$?
2	-2	-1	1	2	*true*	10	0.1909	0.03003	*true*
2	-1	-0.5	1.323	2	*true*	7	0.5401	0.138	*true*
2	0	0	1.414	2	*true*	8	0.3819	0.1484	*true*
2	1	0.5	1.323	2	*true*	7	0.5401	0.138	*true*
2	2	1	1	2	*true*	9	0.27	0.03933	*true*
2	-2	-1	1	3	*true*	4	1.671	0.2737	*true*
2	-1	-0.5	1.323	3	*true*	4	1.671	0.2682	*true*
2	0	0	1.414	3	*true*	4	1.671	0.0969	*true*
2	1	0.5	1.323	3	*true*	4	1.671	0.2682	*true*
2	2	1	1	3	*true*	4	1.671	0.2737	*true*
3	-3	-1.5	0.866	2	*true*	3	1.323	0.5054	*true*
3	-2	-1	1.414	2	*true*	3	1.323	0.04922	*true*
3	-1	-0.5	1.658	2	*true*	4	0.7638	0.4729	*true*
3	0	0	1.732	2	*true*	3	1.323	0.5054	*true*
3	1	0.5	1.658	2	*true*	4	0.7638	0.4729	*true*
3	2	1	1.414	2	*true*	3	1.323	0.04922	*true*
3	3	1.5	0.866	2	*true*	3	1.323	0.5054	*true*
4	-3	-1.5	1.323	2	*true*	2	2.037	0.9164	*true*
4	-2	-1	1.732	2	*true*	2	2.037	0.4633	*true*
4	-1	-0.5	1.936	2	*true*	2	2.037	0.3227	*true*
4	0	0	2	2	*true*	2	2.037	0.9633	*true*
4	1	0.5	1.936	2	*true*	2	2.037	0.3227	*true*
4	2	1	1.732	2	*true*	2	2.037	0.4633	*true*
4	3	1.5	1.323	2	*true*	2	2.037	0.9164	*true*

Table 5.3: Upper bound inclusion $\mathsf{value}(\eta_1 \dots \eta_\ell) + \tau^{-\ell} V \subseteq \tau^{2w-1} V$ checked for "problematic values" of $|\tau|$ and w, cf. (e) of Proposition 5.1 on page 14. The dependence of p, q and τ is given by $\tau^2 - p\tau + q = 0$. We have $p^2 < 4q$, since τ is assumed to be imaginary quadratic.

(b) Set

$$M := \tau^w \,\mathsf{value}(\boldsymbol{\eta}) = \eta_{-1}\tau^{w-1} + \sum_{i=2}^{\ell} \eta_{-i}\tau^{w-i}$$

Since $\eta_{-1} \neq 0$, we can rewrite this to get

$$M = \eta_{-1}\tau^{w-1} + \sum_{i=w+1}^{\ell} \eta_{-i}\tau^{w-i} = \eta_{-1}\tau^{w-1} + \sum_{k=1}^{\ell-w} \eta_{-(w+k)}\tau^{-k}.$$

Now consider the Voronoi cell $V_{\eta_{-1}}$ for η_{-1} and $V_0 = V$ for 0. Since $\eta_{-1} \neq 0$, these two are disjoint, except parts of the boundary, if they are adjacent.

We know from (b) of Proposition 5.1 on page 14, that

$$M - \eta_{-1}\tau^{w-1} = \sum_{k=1}^{\ell-w} \eta_{-(w+k)}\tau^{-k} \in \bigcup_{z \in \tau^{w-1}V} \overline{\mathcal{B}}\Big(z, |\tau|^{-w} f_U\Big),$$

so

$$M \in \bigcup_{z \in \tau^{w-1}V_{\eta_{-1}}} \overline{\mathcal{B}}\Big(z, |\tau|^{-w} f_U\Big).$$

This means that M is in $\tau^{w-1}V_{\eta_{-1}}$ or in a $|\tau|^{-w} f_U$-strip around this cell.

$q = \lvert\tau\rvert^2$	p	$\mathrm{Re}(\tau)$	$\mathrm{Im}(\tau)$	w	ℓ	$\lvert\tau\rvert^{-\ell} f_U$	$\widetilde{\nu}$	$\log_{\lvert\tau\rvert}(f_U/\widetilde{\nu})$
2	−2	−1	1	2	9	0.135	0.004739	18.66
2	−1	−0.5	1.323	2	7	0.27	0.105	9.726
2	0	0	1.414	2	8	0.1909	0.07422	10.73
2	1	0.5	1.323	2	7	0.27	0.105	9.726
2	2	1	1	2	9	0.135	0.04176	12.39
2	−2	−1	1	3	6	0.4177	0.1126	9.782
2	−1	−0.5	1.323	3	6	0.4177	0.04999	12.13
2	0	0	1.414	3	6	0.4177	0.0153	15.54
2	1	0.5	1.323	3	6	0.4177	0.04999	12.13
2	2	1	1	3	6	0.4177	0.1126	9.782
3	−3	−1.5	0.866	2	4	0.3819	0.003019	12.81
3	−2	−1	1.414	2	5	0.2205	0.04402	7.933
3	−1	−0.5	1.658	2	5	0.2205	0.08717	6.689
3	0	0	1.732	2	4	0.3819	0.003019	12.81
3	1	0.5	1.658	2	5	0.2205	0.08717	6.689
3	2	1	1.414	2	5	0.2205	0.04402	7.933
3	3	1.5	0.866	2	4	0.3819	0.003019	12.81
4	−3	−1.5	1.323	2	4	0.2546	0.07613	5.742
4	−2	−1	1.732	2	5	0.1273	0.03807	6.742
4	−1	−0.5	1.936	2	4	0.2546	0.0516	6.303
4	0	0	2	2	5	0.1273	0.07035	5.856
4	1	0.5	1.936	2	4	0.2546	0.0516	6.303
4	2	1	1.732	2	5	0.1273	0.0467	6.447
4	3	1.5	1.323	2	4	0.2546	0.07613	5.742

Table 5.4: Lower bounds for "problematic values" of $|\tau|$ and w, cf. (b) of Proposition 5.2 on page 16. The dependence of p, q and τ is given by $\tau^2 - p\tau + q = 0$. We have $p^2 < 4q$, since τ is assumed to be imaginary quadratic.

Now we are looking at $\tau^{w-1}V_0$ and using Proposition 2.5 on page 5, from which we know that $\overline{\mathcal{B}}\left(0, \frac{1}{2}|\tau|^{w-1}\right)$ is inside such a Voronoi cell. Thus, we get

$$|M| \geq \frac{1}{2}|\tau|^{w-1} - |\tau|^{-w} f_U = \frac{1}{2}|\tau|^{w-1} - \frac{c_V}{1 - |\tau|^{-w}} = |\tau|^{w-1}\nu$$

for our lower bound of M and therefore, by multiplying with τ^{-w} one for $\mathsf{value}(\boldsymbol{\eta})$.

Looking in Table 5.1 on page 16, we see that there are some values where ν is not positive. As in Proposition 5.1 on page 14, this is the case, if $w = 2$ and $|\tau|$ is $\sqrt{2}$, $\sqrt{3}$ or $\sqrt{4}$, and if $w = 3$ and $|\tau| = \sqrt{2}$. Since ν is monotonic increasing with $|\tau|$ and monotonic increasing with w, there are no other non-positive values of ν than the above mentioned.

For those finite many problem cases, we use (a) to find a $\widetilde{\nu}$. The results are listed in Table 5.4 and an example is drawn in Figure 5.1 on the following page. □

Combining the previous two Propositions leads to the following corollary, which gives an upper and a lower bound for the absolute value of a w-NAF by looking at the largest non-zero index.

Corollary 5.3 (Bounds for the Value). *Let $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$, then we get*

$$\mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}, \mathbf{0})\, f_L \leq |\mathsf{value}(\boldsymbol{\eta})| \leq \mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}, \mathbf{0})\, f_U\, |\tau|\,.$$

Proof. Follows directly from Proposition 5.1 on page 14 and Proposition 5.2 on page 16. □

Last in this section, we want to find out, if there are special w-NAFs, for which we know for sure that all their expansions start with a certain finite w-NAF. We will show the following lemma.

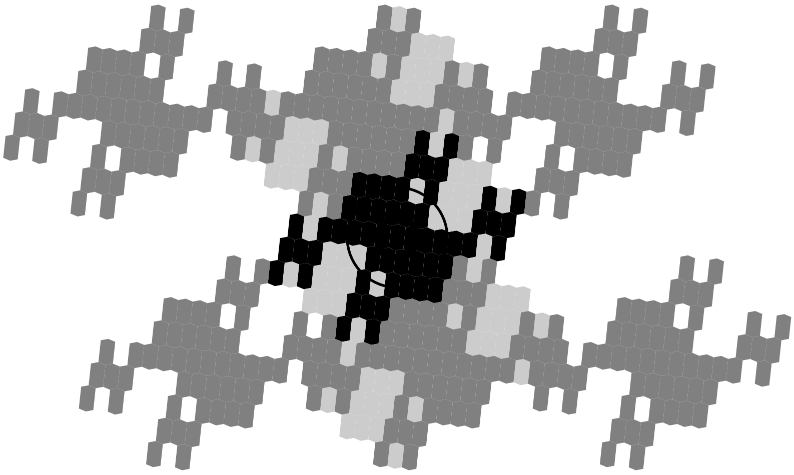


Figure 5.1: Lower bound for $\tau = \frac{1}{2} + \frac{1}{2}\sqrt{-11}$ and $w = 2$. The procedure stopped at $\ell = 6$. The large circle has radius $\left|\tau\right|^{-\ell} f_U$, the small circle is our lower bound with radius $f_L = \widetilde{\nu}$. The dot inside represents zero. The grey region has most significant digit zero, the black ones non-zero.

Lemma 5.4. *Let*

$$k \geq k_0 = \max\left\{19, 2w + 5\right\},$$

let $\boldsymbol{\eta} \in \mathbf{NAF}_w^{0.\infty}$ *start with the word* 0^k, *i.e.*, $\eta_{-1} = 0$, $\dots$, $\eta_{-k} = 0$, *and set* $z = \mathsf{value}(\boldsymbol{\eta})$. *Then we get for all* $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ *that* $z = \mathsf{value}(\boldsymbol{\xi})$ *implies* $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty}$.

Proof. Let $\boldsymbol{\xi}_I.\boldsymbol{\xi}_F \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$. Then $\left|\mathsf{value}(\boldsymbol{\xi}_I.\boldsymbol{\xi}_F)\right| < f_L$ implies $\boldsymbol{\xi}_I = \mathbf{0}$, cf. Proposition 5.2 on page 16. For our $\boldsymbol{\eta}$ we obtain $z = \left|\mathsf{value}(\boldsymbol{\eta})\right| \leq \left|\tau\right|^{-k} f_U$, cf. Proposition 5.1 on page 14. So we have to show that

$$\left|\tau\right|^{-k} f_U < f_L,$$

which is equivalent to

$$k > \log_{\left|\tau\right|} \frac{f_U}{f_L}.$$

For the "non-problematic cases", cf. Propositions 5.1 on page 14 and 5.2 on page 16, we obtain

$$k > 2w - 1 + \log_{\left|\tau\right|} A$$

with

$$A := \frac{1}{\nu} \frac{\left|\tau\right| c_V}{\left|\tau\right|^w - 1} = \left(\frac{\left|\tau\right|^w - 1}{2\left|\tau\right| c_V} - 1\right)^{-1} > 0,$$

where we just inserted the formulas for f_U, f_L and ν, and used $\nu > 0$.

Consider the partial derivation of $\log_{\left|\tau\right|} A$ with respect to $\left|\tau\right|$. We get

$$\frac{\partial \log_{\left|\tau\right|} A}{\partial \left|\tau\right|} = \underbrace{\frac{1}{\log_e \left|\tau\right|}}_{>0} \underbrace{\nu}_{>0} \underbrace{\frac{\left|\tau\right|^w - 1}{\left|\tau\right| c_V}}_{>0} \underbrace{\frac{\partial A}{\partial \left|\tau\right|}}_{<0} < 0,$$

where we used $\left|\tau\right| > 1$, $w \geq 2$, and the fact that the quotient of polynomials $\frac{\left|\tau\right|^w - 1}{2\left|\tau\right| c_V}$ is monotonic increasing with $\left|\tau\right|$. Further we see that A is monotonic decreasing with w, therefore $\log_{\left|\tau\right|} A$, too.

For $\left|\tau\right| = \sqrt{5}$ and $w = 2$ we get $\log_{\left|\tau\right|} A = 5.84522$, for $\left|\tau\right| = \sqrt{3}$ and $w = 3$ we get $\log_{\left|\tau\right|} A = 1.70649$, and for $\left|\tau\right| = \sqrt{2}$ and $w = 4$ we get $\log_{\left|\tau\right|} A = 2.57248$. Using the monotonicity from above yields $k \geq 2w + 5$ for the "non-problematic cases".

For our "problematic cases", the value of $\log_{\left|\tau\right|} \frac{f_U}{f_L}$ is calculated in Table 5.4 on the previous page. Therefore we obtain $k \geq 19$. □

6. Numeral Systems with Non-Adjacent Forms

Let $\tau \in \mathbb{C}$ be an algebraic integer, imaginary quadratic. Suppose that $|\tau| > 1$. Let $w \in \mathbb{N}$ with $w \geq 2$. Further let $\mathcal{D}$ be a minimal norm representatives digit set modulo τ^w as in Definition 3.5 on page 9.

We are now able to show that in this setting, the digit set of minimal norm representatives is indeed a width-w non-adjacent digit set. This is then extended to infinite fractional expansions of elements in $\mathbb{C}$.

Theorem 6.1 (Existence and Uniqueness Theorem concerning Lattice Points)**.** *For each lattice point $z \in \mathbb{Z}[\tau]$ there is a unique element $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}}$, such that $z = \mathsf{value}(\boldsymbol{\xi})$. Thus $\mathcal{D}$ is a width-w non-adjacent digit set. The w-NAF $\boldsymbol{\xi}$ can be calculated using Algorithm 6.1, i.e., this algorithm terminates and is correct.*

The uniqueness result is well known. The existence result is only known for special τ and w. For example in Koblitz [15] the case $\tau = \pm\frac{3}{2} + \frac{1}{2}\sqrt{-3}$ and $w = 2$ was shown. There the digit set $\mathcal{D}$ consists of 0 and powers of primitive sixth roots of unity. Blake, Kumar Murty and Xu [6] generalised that for $w \geq 2$. Another example is given in Solinas [20]. There $\tau = \pm\frac{1}{2} + \frac{1}{2}\sqrt{-7}$ and $w = 2$ is used, and the digit set $\mathcal{D}$ consists of 0 and ± 1. This result was generalised by Blake, Kumar Murty and Xu [5] for $w \geq 2$. The cases $\tau = 1 + \sqrt{-1}$, $\tau = \sqrt{-2}$ and $\tau = \frac{1}{2} + \frac{1}{2}\sqrt{-11}$ were studied in Blake, Kumar Murty and Xu [4].

Algorithm 6.1 Algorithm to calculate a w-NAF $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}}$ for an element $z \in \mathbb{Z}[\tau]$.

```
$\ell \leftarrow 0$
$y \leftarrow z$
while $y \neq 0$ do
    if $\tau \mid y$ then
        $\xi_\ell \leftarrow 0$
    else
        Let $\xi_\ell \in \mathcal{D}$ such that $\xi_\ell \equiv y \pmod{\tau^w}$
    end if
    $y \leftarrow (y - \xi_\ell)/\tau$
    $\ell \leftarrow \ell + 1$
end while
$\boldsymbol{\xi} \leftarrow \xi_{\ell-1}\xi_{\ell-2}\cdots\xi_0$
return $\boldsymbol{\xi}$
```

The proof follows a similar idea as in Section 5 on page 13 and in Matula [16]. There are again two parts, one analytic part for all but finitely many cases, and the other, which proves the remaining by the help of a simple procedure.

Proof. First we show that the algorithm terminates. Let $y \in \mathbb{Z}[\tau]$ and consider Algorithm 6.1 in cycle ℓ. If $\tau \mid y$, then in the next step the norm $|y|^2 \in \mathbb{N}_0$ becomes smaller since $|\tau|^2 > 1$.

Let $\tau \nmid y$. If $|y| < \frac{1}{2}|\tau|^w$, then $y \in \mathcal{D}$, cf. Proposition 2.5 on page 5 and Remark 3.6 on page 9. Thus the algorithm terminates in the next cycle. If

$$|y| > \frac{|\tau|\, c_V}{1 - |\tau|^{-w}} = \frac{|\tau|^{w+1} c_V}{|\tau|^w - 1},$$

we obtain

$$|y|\,|\tau|^w > |y| + |\tau|^{w+1} c_V \geq |y| + |\xi_\ell| \geq |y - \xi_\ell|,$$

which is equivalent to

$$\left|\frac{y - \xi_\ell}{\tau^w}\right| < |y|.$$

So if the condition

$$\frac{|\tau|^{w+1} c_V}{|\tau|^w - 1} < \frac{1}{2} |\tau|^w \iff \nu = \frac{1}{2} - \frac{|\tau| c_V}{|\tau|^w - 1} > 0,$$

with the same ν as in Proposition 5.2 on page 16, is fulfilled, the norm $|y|^2 \in \mathbb{N}_0$ is descending and therefore the algorithm terminating.

Now we consider the case, when $\nu \leq 0$. According to Table 5.1 on page 16 there are the same finitely many combinations of τ and w to check as in Proposition 5.1 on page 14 and Proposition 5.2 on page 16. For each of them, there is only a finite number of elements $y \in \mathbb{Z}[\tau]$ with

$$|y| \leq \frac{|\tau|^{w+1} c_V}{|\tau|^w - 1},$$

so altogether only finitely many $y \in \mathbb{Z}[\tau]$ left to check, whether they admit a w-NAF or not. The results can be found in the table available as online-resource[1]. Every element that was to check, has a w-NAF.

To show the correctness, again let $y \in \mathbb{Z}[\tau]$ and consider Algorithm 6.1 on the preceding page in cycle ℓ. If τ divides y, then we append a digit $\xi_\ell = 0$. Otherwise y is congruent to a non-zero element ξ_ℓ of $\mathcal{D}$ modulo τ^w, since the digit set $\mathcal{D}$ was constructed in that way, cf. Definitions 3.1 and 3.5. The digit ξ_ℓ is appended. Because τ^w divides $y - \xi_\ell$, the next $w-1$ digits will be zero. Therefore a correct w-NAF is produced.

For the uniqueness let $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}}$ be an expansions for the element $z \in \mathbb{Z}[\tau]$. If $\tau \mid z$, then

$$0 \equiv z = \mathsf{value}(\boldsymbol{\xi}) \equiv \xi_0 \pmod{\tau},$$

so $\tau \mid \xi_0 \in \mathcal{D}$. Therefore $\xi_0 = 0$. If $\tau \nmid z$, then $\tau \nmid \xi_0$ and so $\xi_0 \neq 0$. This implies $\xi_1 = 0, \ldots, \xi_{w-1} = 0$. This means ξ_0 lies in the same residue class modulo τ^w as exactly one non-zero digit of $\mathcal{D}$ (per construction of the digit set, cf. Definitions 3.1 and 3.5), hence they are equal. Induction finishes the proof of the uniqueness. □

So we have that all elements of our lattice $\mathbb{Z}[\tau]$ have a unique expansion. Now we want to get a step further and look at all elements of $\mathbb{C}$. We will need the following three lemmata, to prove that every element of $\mathbb{C}$ has a w-NAF-expansion.

Lemma 6.2. *The function* $\mathsf{value}|_{\mathbf{NAF}_w^{\mathsf{fin.fin}}}$ *is injective.*

Proof. Let $\boldsymbol{\eta}$ and $\boldsymbol{\xi}$ be elements of $\mathbf{NAF}_w^{\mathsf{fin.fin}}$ with $\mathsf{value}(\boldsymbol{\eta}) = \mathsf{value}(\boldsymbol{\xi})$. This implies that $\tau^J \mathsf{value}(\boldsymbol{\eta}) = \tau^J \mathsf{value}(\boldsymbol{\xi}) \in \mathbb{Z}[\tau]$ for some $J \in \mathbb{Z}$. By uniqueness of the integer w-NAFs, see Theorem 6.1 on the previous page, we conclude that $\boldsymbol{\eta} = \boldsymbol{\xi}$. □

Lemma 6.3. *We have* $\mathsf{value}\left(\mathbf{NAF}_w^{\mathsf{fin.fin}}\right) = \mathbb{Z}[1/\tau]$.

Proof. Let $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin.fin}}$ and $\eta_j = 0$ for all $|j| > J$ for some $J \geq 1$. Then $\tau^J \mathsf{value}(\boldsymbol{\eta}) \in \mathbb{Z}[\tau]$, which implies that there are some a, $b \in \mathbb{Z}$ such that

$$\mathsf{value}(\boldsymbol{\eta}) = a\tau^{-(J-1)} + b\tau^{-J} \in \mathbb{Z}[1/\tau].$$

Conversely, if

$$z = \sum_{j=0}^{J} \eta_j \tau^{-j} \in \mathbb{Z}[1/\tau],$$

we have $\tau^J z \in \mathbb{Z}[\tau]$. Since every element of $\mathbb{Z}[\tau]$ admits an integer w-NAF, see Theorem 6.1 on the preceding page, there is an $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin.fin}}$ with $\mathsf{value}(\boldsymbol{\xi}) = z$. □

Lemma 6.4. $\mathbb{Z}[1/\tau]$ *is dense in* $\mathbb{C}$.

[1] Table available at `www.danielkrenn.at/goto.php?link=wnaf-analysis`.

Proof. Let $z \in \mathbb{C}$ and $K \geq 0$. Then $\tau^K z = u + v\tau$ for some reals u and v. We have

$$\left| z - \frac{\lfloor u \rfloor + \lfloor v \rfloor \tau}{\tau^K} \right| < \frac{1 + |\tau|}{|\tau|^K},$$

which proves the lemma. □

Now we can prove the following theorem.

Theorem 6.5 (Existence Theorem concerning $\mathbb{C}$)**.** *Let $z \in \mathbb{C}$. Then there is an $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ such that $z = \mathsf{value}(\boldsymbol{\eta})$, i.e., each complex number has a w-NAF-expansion.*

Proof. By Lemma 6.4 on the preceding page, there is a sequence $z_n \in \mathbb{Z}[1/\tau]$ converging to z. By Lemma 6.3 on the facing page, there is a sequence $\boldsymbol{\eta}_n \in \mathbf{NAF}_w^{\mathsf{fin}.\mathsf{fin}}$ with $\mathsf{value}(\boldsymbol{\eta}_n) = z_n$ for all n. By Corollary 5.3 on page 19 the sequence $\mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\eta}_n, 0)$ is bounded from above, so there is an ℓ such that $\boldsymbol{\eta}_n \in \mathbf{NAF}_w^{\ell.\mathsf{fin}} \subseteq \mathbf{NAF}_w^{\ell.\infty}$. By Proposition 3.9 on page 10, we conclude that there is a convergent subsequence $\boldsymbol{\eta}'_n$ of $\boldsymbol{\eta}_n$. Set $\boldsymbol{\eta} := \lim_{n\to\infty} \boldsymbol{\eta}'_n$. By continuity of value, see Proposition 3.8 on page 10, we conclude that $\mathsf{value}(\boldsymbol{\eta}) = z$. □

7. The Fundamental Domain

Let $\tau \in \mathbb{C}$ be an algebraic integer, imaginary quadratic. Suppose that $|\tau| > 1$. Let $w \in \mathbb{N}$ with $w \geq 2$. Further let $\mathcal{D}$ be a minimal norm representatives digit set modulo τ^w as in Definition 3.5 on page 9.

We now derive properties of the *Fundamental Domain*, i.e., the set of complex numbers representable by w-NAFs which vanish left of the τ-point. The boundary of the fundamental domain is shown to correspond to complex numbers which admit more than one w-NAF differing left of the τ-point. Finally, an upper bound for the Hausdorff dimension of the boundary is derived.

Definition 7.1 (Fundamental Domain)**.** The set

$$\mathcal{F} := \mathsf{value}\big(\mathbf{NAF}_w^{0.\infty}\big) = \big\{\mathsf{value}(\boldsymbol{\xi}) \,\big|\, \boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty}\big\}\,.$$

is called *fundamental domain.*

The pictures in Figure 9.1 on page 32 can also be reinterpreted as fundamental domains for the τ and w given there. The definition of the fundamental domain for a general $\tau \in \mathbb{C}$ and a general finite digit set containing zero is meaningful, too. The same is true for following proposition, which is also valid for general $\tau \in \mathbb{C}$ and a general finite digit set including zero.

Proposition 7.2. *The fundamental domain $\mathcal{F}$ is compact.*

Proof. The set $\mathbf{NAF}_w^{0.\infty}$ is compact, cf. Proposition 3.9 on page 10. The compactness of the fundamental domain $\mathcal{F}$ follows, since $\mathcal{F}$ is the image of $\mathbf{NAF}_w^{0.\infty}$ under the continuous function value, cf. Proposition 3.8 on page 10. □

We can also compute the Lebesgue measure of the fundamental domain. This result can be found in Remark 9.3 on page 35. We will need the results of Sections 8 and 9 for calculating $\lambda(\mathcal{F})$.

Next we want to get more properties of the fundamental domain. We will need the following proposition, which will be extended in Proposition 7.7 on page 25.

Proposition 7.3. *Let $z \in \mathcal{F}$. If there exists a w-NAF $\boldsymbol{\xi}_I.\boldsymbol{\xi}_F \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ with $\boldsymbol{\xi}_I \neq \mathbf{0}$ and such that $z = \mathsf{value}(\boldsymbol{\xi}_I.\boldsymbol{\xi}_F)$, then $z \in \partial\mathcal{F}$.*

Proof. Assume that $z \in \operatorname{int}\mathcal{F}$. Then there is an $\varepsilon_z > 0$ such that $\mathcal{B}(z, \varepsilon_z) \subseteq \operatorname{int}\mathcal{F}$. Let ε_z be small enough such that there exists a $y \in \mathcal{B}(z, \varepsilon_z) \cap \mathbb{Z}[1/\tau]$ and a $\boldsymbol{\vartheta} = \boldsymbol{\vartheta}_I.\boldsymbol{\vartheta}_F \in \mathbf{NAF}_w^{\mathsf{fin}.\mathsf{fin}}$ with $y = \mathsf{value}(\boldsymbol{\vartheta})$ and such that $\boldsymbol{\vartheta}_I \neq \mathbf{0}$. Let k be the right-length of $\boldsymbol{\vartheta}$.

Choose $0 < \varepsilon_y < \tau^{-k-w} f_L$ such that $\mathcal{B}(y, \varepsilon_y) \subseteq \operatorname{int}\mathcal{F}$. Since $y \in \mathcal{F}$ there is an $\boldsymbol{\eta} \in \mathbf{NAF}_w^{0.\infty}$ with $y = \mathsf{value}(\boldsymbol{\eta})$. Therefore, there is a $y' \in \mathcal{B}(y, \varepsilon_y) \cap \mathbb{Z}[1/\tau]$ with $y' = \mathsf{value}(\boldsymbol{\eta}')$ for some $\boldsymbol{\eta}' = \boldsymbol{\eta}'_I.\boldsymbol{\eta}'_F \in \mathbf{NAF}_w^{\mathsf{fin}.\mathsf{fin}}$ with $\boldsymbol{\eta}'_I = \mathbf{0}$ (by "cutting" the infinite right side of $\boldsymbol{\eta}$).

As $y' - y \in \mathbb{Z}[1/\tau]$, there is a $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}.\mathsf{fin}}$ with $\mathsf{value}(\boldsymbol{\xi}) = y' - y$. By Corollary 5.3 we obtain $\mathrm{d}_{\mathsf{NAF}}(\boldsymbol{\xi}, \mathbf{0}) < \varepsilon_y / f_L < \tau^{-k-w}$. Thus $\xi_\ell = 0$ for all $\ell \geq -k - (w-1)$.

Now $y' = y + (y' - y)$ and we get a $\boldsymbol{\vartheta}' = \boldsymbol{\vartheta}'_I\boldsymbol{.}\boldsymbol{\vartheta}'_F \in \mathbf{NAF}_w^{\mathsf{fin}.\mathsf{fin}}$ with $\mathsf{value}(\boldsymbol{\vartheta}') = y'$ by digit-wise addition of $\boldsymbol{\vartheta}$ and $\boldsymbol{\xi}$. Note that at each index at most one summand (digit) is non-zero and that the w-NAF-condition is fulfilled. We have $\boldsymbol{\vartheta}'_I \neq \mathbf{0}$, since $\boldsymbol{\vartheta}_I \neq \mathbf{0}$.

So we got two different w-NAFs in $\mathbf{NAF}_w^{\mathsf{fin}.\mathsf{fin}}$ for one element $y' \in \mathbb{Z}[1/\tau]$, which is impossible due to uniqueness, see Lemma 6.2 on page 22. Thus we have a contradiction. □

The complex plane has a tiling property with respect to the fundamental domain. This fact is stated in the following corollary to Theorem 6.1 on page 21 and Theorem 6.5 on the preceding page.

Corollary 7.4 (Tiling Property)**.** *The complex plane can be tiled with scaled versions of the fundamental domain $\mathcal{F}$. Only finitely many different size are needed. More precisely: Let $K \in \mathbb{Z}$, then*

$$\mathbb{C} = \bigcup_{\substack{k \in \{K, K+1, \dots, K+w-1\} \\ \boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}} \\ k \neq K+w-1 \textit{ implies } \boldsymbol{\xi}_0 \neq 0}} \left(\tau^k \,\mathsf{value}(\boldsymbol{\xi}) + \tau^{k-w+1}\mathcal{F}\right),$$

and the intersection of two different $\tau^k \,\mathsf{value}(\boldsymbol{\xi}) + \tau^{k-w+1}\mathcal{F}$ and $\tau^{k'-w+1} \,\mathsf{value}(\boldsymbol{\xi}') + \tau^{k'}\mathcal{F}$ in this union is a subset of the intersection of their boundaries.

Later, after Proposition 7.8 on the next page, we will know that the intersection of the two different sets of the tiling in the previous corollary has Lebesgue measure 0.

Proof of Corollary 7.4. Let $z \in \mathbb{C}$. Then, according to Theorem 6.5 on the preceding page, there is a $\boldsymbol{\eta} \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ with $z = \mathsf{value}(\boldsymbol{\eta})$. We look at the block $\eta_{K+w-1} \dots \eta_{K+1}\eta_K$. If this block is $\mathbf{0}$, then set $k = K + w - 1$, otherwise there is at most one non-zero digit in it, which we call η_k. So the digits $\eta_{k-1}, \dots, \eta_{k-w+1}$ are always zero. We set $\boldsymbol{\xi} = \dots \eta_{k+1}\eta_k\boldsymbol{.}0\dots$, and we obtain

$$z - \tau^k \,\mathsf{value}(\boldsymbol{\xi}) \in \tau^{k-w+1}\mathcal{F}.$$

Now set $F = \tau^k \,\mathsf{value}(\boldsymbol{\xi}) + \tau^{k-w+1}\mathcal{F}$ and $F' = \tau^{k'} \,\mathsf{value}(\boldsymbol{\xi}') + \tau^{k'-w+1}\mathcal{F}$ in a way that both are in the union of the tiling with $(k, \boldsymbol{\xi}) \neq (k', \boldsymbol{\xi}')$ and consider their intersection I. Since every point in there has two different representations per construction, we conclude that $I \subseteq \partial F$ and $I \subseteq \partial F'$ by Proposition 7.3 on the previous page. □

Remark 7.5 (Iterated Function System). Let $\tau \in \mathbb{C}$ and $\mathcal{D}$ be a general finite digit set containing zero. We have two possibilities building the elements $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty}$ from left to right. We can either append 0, what corresponds to a division through τ, so we define $f_0(z) = \frac{z}{\tau}$. Or we can append a non-zero digit $\vartheta \in \mathcal{D}^\bullet$ and then add $w - 1$ zeros. In this case, we define $f_\vartheta(z) = \frac{\vartheta}{\tau} + \frac{z}{\tau^w}$. Thus we get the *iterated function system* $(f_\vartheta)_{\vartheta \in \mathcal{D}}$, cf. Edgar [8] or Barnsley [3]. All f_ϑ are *similarities*, and the iterated function system realizes the *ratio list* $(r_\vartheta)_{\vartheta \in \mathcal{D}}$ with $r_0 = |\tau|^{-1}$ and for $\vartheta \in \mathcal{D}^\bullet$ with $r_\vartheta = |\tau|^{-w}$. So our set can be rewritten as

$$\mathcal{F} = \bigcup_{\vartheta \in \mathcal{D}} f_\vartheta(\mathcal{F}) = \frac{1}{\tau}\mathcal{F} \cup \bigcup_{\vartheta \in \mathcal{D}^\bullet} \left(\frac{\vartheta}{\tau} + \frac{1}{\tau^w}\mathcal{F}\right).$$

Furthermore, if we have an imaginary quadratic algebraic integer τ and a minimal norm representatives digit set, the iterated function system $(f_\vartheta)_{\vartheta \in \mathcal{D}}$ fulfils *Moran's open set condition*[2], cf. Edgar [8] or Barnsley [3]. The *Moran open set* used is $\operatorname{int}\mathcal{F}$. This set satisfies

$$f_\vartheta(\operatorname{int}\mathcal{F}) \cap f_{\vartheta'}(\operatorname{int}\mathcal{F}) = \emptyset$$

for $\vartheta \neq \vartheta' \in \mathcal{D}$ and

$$\operatorname{int}\mathcal{F} \supseteq f_\vartheta(\operatorname{int}\mathcal{F})$$

for all $\vartheta \in \mathcal{D}$. We remark that the first condition follows directly from the tiling property in Corollary 7.4 with $K = -1$. The second condition follows from the fact that f_ϑ is an open mapping.

[2] "Moran's open set condition" is sometimes just called "open set condition"

Now we want to have a look at a special case.

Remark 7.6 (Koch snowflake). Let $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$ and $w = 2$. Then our digit set consists of 0 and powers of primitive sixth roots of unity, i.e., $\mathcal{D} = \{0\} \cup \left\{\zeta^k \,\middle|\, k \in \mathbb{N}_0 \text{ with } 0 \leq k < 6\right\}$ with $\zeta = e^{i\pi/3}$, cf. Koblitz [15].

We get

$$\mathcal{F} = \frac{1}{\tau}\mathcal{F} \cup \bigcup_{0 \leq k < 6} \left(\frac{\zeta^k}{\tau} + \frac{1}{\tau^2}\mathcal{F}\right).$$

Since the digit set is invariant with respect to multiplication by ζ, i.e., rotation by $\frac{\pi}{3}$, the same is true for $\mathcal{F}$. Using this and $\tau = \sqrt{3}e^{i\pi/6}$ yields

$$\mathcal{F} = \frac{e^{i\pi/2}}{\sqrt{3}}\mathcal{F} \cup \bigcup_{0 \leq k < 6} \left(\frac{e^{ik\pi/3 + i\pi/2}}{\sqrt{3}} + \frac{1}{3}\mathcal{F}\right).$$

This is an iterated function system of the *Koch snowflake*[3], it is drawn in Figure 9.1c on page 32.

Next we want to have a look at the Hausdorff dimension of the boundary of $\mathcal{F}$. We will need the following characterisation of the boundary, which is an extension to Proposition 7.3 on page 23.

Proposition 7.7 (Characterisation of the Boundary)**.** *Let $z \in \mathcal{F}$. Then $z \in \partial\mathcal{F}$ if and only if there exists a w-NAF $\boldsymbol{\xi}_I\boldsymbol{.}\boldsymbol{\xi}_F \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ with $\boldsymbol{\xi}_I \neq \mathbf{0}$, such that $z = \mathsf{value}(\boldsymbol{\xi}_I\boldsymbol{.}\boldsymbol{\xi}_F)$.*

Proof. Let $z \in \partial\mathcal{F}$. For every $\varepsilon > 0$, there is a $y \in \mathcal{B}(z, \varepsilon)$, such that $y \notin \mathcal{F}$. Thus we have a sequence $(y_j)_{j \geq 1}$ converging to z, where the y_j are not in $\mathcal{F}$. Therefore each y_j has a w-NAF-representation $\boldsymbol{\eta}_j \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ with non-zero integer part. Now we will use the tiling property stated in Corollary 7.4 on the preceding page. The fundamental domain $\mathcal{F}$ can be surrounded by only finitely many scaled versions of $\mathcal{F}$. So there is a subsequence $(\boldsymbol{\vartheta}_j)_{j \in \mathbb{N}_0}$ of $(\boldsymbol{\eta}_j)_{j \in \mathbb{N}_0}$ with fixed integer part $\boldsymbol{\xi}_I \neq \mathbf{0}$. Due to compactness of $\mathcal{F}$, cf. Proposition 7.2 on page 23, we find a $\boldsymbol{\xi} = \boldsymbol{\xi}_I\boldsymbol{.}\boldsymbol{\xi}_F$ with value z as limit of a converging subsequence of $(\boldsymbol{\vartheta}_j)_{j \in \mathbb{N}_0}$.

The other direction is just Proposition 7.3 on page 23, thus the proof is finished. □

The following proposition deals with the Hausdorff dimension of the boundary of $\mathcal{F}$.

Proposition 7.8. *For the Hausdorff dimension of the boundary of the fundamental domain we get* $\dim_H \partial\mathcal{F} < 2$.

The idea of this proof is similar to a proof in Heuberger and Prodinger [12].

Proof. Set $k := k_0 + w - 1$ with k_0 from Lemma 5.4 on page 20. For $j \in \mathbb{N}$ define

$$U_j := \left\{\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.j} \,\middle|\, \xi_{-\ell}\xi_{-(\ell+1)} \dots \xi_{-(\ell+k-1)} \neq 0^k \text{ for all } \ell \text{ with } 1 \leq \ell \leq j - k + 1\right\}.$$

The elements of U_j — more precisely the digits from index -1 to $-j$ — can be described by the regular expression

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

This can be translated to the generating function

$$G(Z) = \sum_{j \in \mathbb{N}} \#U_j Z^j = \left(1 + \#\mathcal{D}^\bullet \sum_{\ell=0}^{w-2} Z^{\ell+1}\right) \frac{1}{1 - \#\mathcal{D}^\bullet \sum_{\ell=w-1}^{k-1} Z^{\ell+1}} \left(\sum_{\ell=0}^{k-1} Z^\ell\right)$$

used for counting the number of elements in U_j. Rewriting yields

$$G(Z) = \frac{1 - Z^k}{1 - Z} \frac{1 + (\#\mathcal{D}^\bullet - 1)Z - \#\mathcal{D}^\bullet Z^w}{1 - Z - \#\mathcal{D}^\bullet Z^w + \#\mathcal{D}^\bullet Z^{k+1}},$$

and we set

$$q(Z) := 1 - Z - \#\mathcal{D}^\bullet Z^w + \#\mathcal{D}^\bullet Z^{k+1}.$$

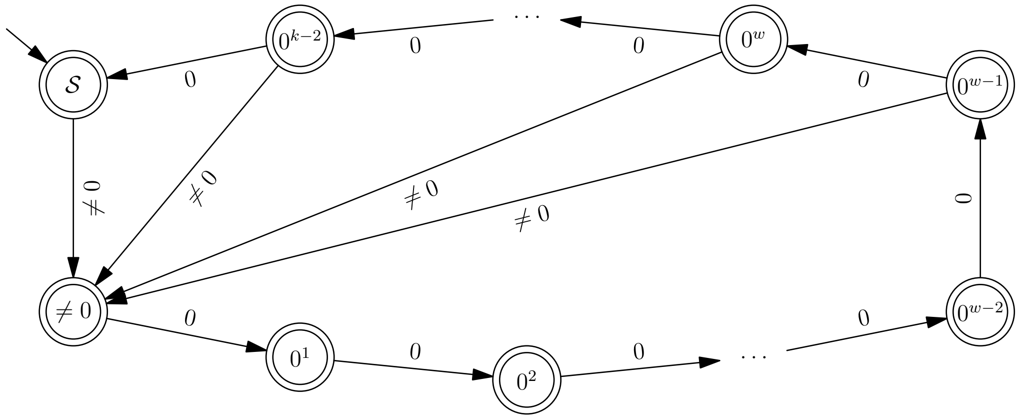


Figure 7.1: Automaton $\mathcal{A}$ recognising $\bigcup_{j\in\mathbb{N}} \widetilde{U}_j$ from right to left, see proof of Proposition 7.8. The state $\mathcal{S}$ is the starting state, all states are valid end states. An edges marked with $\neq 0$ means one edge for each non-zero digit in the digit set $\mathcal{D}$. The state $\neq 0$ means that there was an non-zero digit read, a state 0^ℓ means that ℓ zeros have been read.

Now we define

$$\widetilde{U}_j := \{\boldsymbol{\xi} \in U_j \mid \xi_{-j} \neq 0\}$$

and consider $\widetilde{U} := \bigcup_{j\in\mathbb{N}} \widetilde{U}_j$. The w-NAFs in this set — more precisely the finite strings from index -1 to the index of the largest non-zero digit — will be recognised by the automaton $\mathcal{A}$ which reads its input from right to left, see Figure 7.1. It is easy to see that the underlying directed graph $G_\mathcal{A}$ of the automaton $\mathcal{A}$ is strongly connected, therefore its adjacency matrix $M_\mathcal{A}$ is irreducible. Since there are cycles of length w and $w+1$ in the graph and $\gcd(w, w+1) = 1$, the adjacency matrix is primitive. Thus, using the Perron-Frobenius theorem we obtain

$$\begin{aligned}\#\widetilde{U}_j &= \#(\text{walks in } G_\mathcal{A} \text{ of length } j \text{ from starting state } \mathcal{S} \text{ to some other state})\\ &= \begin{pmatrix}1 & 0 & \dots & 0\end{pmatrix} M_\mathcal{A}^j \begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \widetilde{c}\left(\sigma \left|\tau\right|^2\right)^j \left(1 + \mathcal{O}\left(s^j\right)\right)\end{aligned}$$

for a $\widetilde{c} > 0$, a $\sigma > 0$, and an s with $0 \leq s < 1$. Since the number of w-NAFs of length j is $\mathcal{O}\left(\left|\tau\right|^{2j}\right)$, see Theorem 4.1 on page 11, we get $\sigma \leq 1$.

We clearly have

$$U_j = \biguplus_{\ell=j-k+1}^{j} \widetilde{U}_\ell,$$

so we get

$$\#U_j = \left[Z^j\right] G(Z) = c\left(\sigma \left|\tau\right|^2\right)^j \left(1 + \mathcal{O}\left(s^j\right)\right)$$

for some constant $c > 0$.

To rule out $\sigma = 1$, we insert the "zero" $\left|\tau\right|^{-2}$ in $q(Z)$. We obtain

$$\begin{aligned}q\left(\left|\tau\right|^{-2}\right) &= 1 - \left|\tau\right|^{-2} - \#\mathcal{D}^\bullet \left|\tau\right|^{-2w} + \#\mathcal{D}^\bullet \left|\tau\right|^{-2(k+1)}\\ &= 1 - \left|\tau\right|^{-2} - \left|\tau\right|^{2(w-1)}\left(\left|\tau\right|^2 - 1\right)\left|\tau\right|^{-2w} + \left|\tau\right|^{2(w-1)}\left(\left|\tau\right|^2 - 1\right)\left|\tau\right|^{-2(k+1)}\\ &= \left(\left|\tau\right|^2 - 1\right)\left|\tau\right|^{2(w-k-2)} > 0,\end{aligned}$$

[3] The fact that the Koch snowflake has the mentioned iterated function system seems to be commonly known, although we were not able to find a reference, where this statement is proved. Any hints are welcome.

where we used the cardinality of $\mathcal{D}^\bullet$ from Lemma 3.3 on page 8 and $|\tau| > 1$. Therefore we get $\sigma < 1$.

Define

$$U := \left\{\mathsf{value}(\boldsymbol{\xi}) \,\middle|\, \boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty} \text{ with } \xi_{-\ell}\xi_{-(\ell+1)}\dots\xi_{-(\ell+k-1)} \neq 0^k \text{ for all } \ell \geq 1\right\}.$$

We want to cover U with squares. Let S be the closed paraxial square with centre 0 and width 2. Using Proposition 5.1 on page 14 yields

$$U \subseteq \bigcup_{z\in\mathsf{value}(U_j)} \left(z + f_U \left|\tau\right|^{-j} S\right)$$

for all $j \in \mathbb{N}$, i.e., U can be covered with $\#U_j$ boxes of size $2f_U\left|\tau\right|^{-j}$. Thus we get for the upper box dimension, cf. Edgar [8],

$$\overline{\dim}_B U \leq \lim_{j\to\infty} \frac{\log \#U_j}{-\log(2f_U\left|\tau\right|^{-j})}.$$

Inserting the cardinality $\#U_j$ from above, using the logarithm to base $|\tau|$ and $0 \leq s < 1$ yields

$$\overline{\dim}_B U \leq \lim_{j\to\infty} \frac{\log_{|\tau|} c + j\log_{|\tau|}(\sigma\left|\tau\right|^2) + \log_{|\tau|}(1+\mathcal{O}(s^j))}{j+\mathcal{O}(1)} = 2 + \log_{|\tau|}\sigma.$$

Since $\sigma < 1$, we get $\overline{\dim}_B U < 2$.

Now we will show that $\partial\mathcal{F} \subseteq U$. Clearly $U \subseteq \mathcal{F}$, so the previous inclusion is equivalent to $\mathcal{F}\setminus U \subseteq \operatorname{int}(\mathcal{F})$. So let $z \in \mathcal{F}\setminus U$. Then there is a $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty}$ such that $z = \mathsf{value}(\boldsymbol{\xi})$ and $\boldsymbol{\xi}$ has a block of at least k zeros somewhere on the right hand side of the τ-point. Let ℓ denote the starting index of this block, i.e.,

$$\boldsymbol{\xi} = 0\boldsymbol{.}\underbrace{\xi_{-1}\dots\xi_{-(\ell-1)}}_{=:\boldsymbol{\xi}_A}0^k\xi_{-(\ell+k)}\xi_{-(\ell+k+1)}\dots.$$

Let $\boldsymbol{\vartheta} = \boldsymbol{\vartheta}_I\boldsymbol{.}\boldsymbol{\vartheta}_A\vartheta_{-\ell}\vartheta_{-(\ell+1)}\dots \in \mathbf{NAF}_w^{\mathsf{fin}.\infty}$ with $\mathsf{value}(\boldsymbol{\vartheta}) = z$. We have

$$z = \mathsf{value}(0\boldsymbol{.}\boldsymbol{\xi}_A) + \tau^{-\ell-w}z_\xi = \mathsf{value}(\boldsymbol{\vartheta}_I\boldsymbol{.}\boldsymbol{\vartheta}_A) + \tau^{-\ell-w}z_\vartheta$$

for appropriate z_ξ and z_ϑ. By Lemma 5.4 on page 20, all expansions of z_ξ are in $\mathbf{NAF}_w^{0.\infty}$. Thus all expansions of

$$\mathsf{value}(\boldsymbol{\vartheta}_I\boldsymbol{\vartheta}_A) + \tau^{-(w-1)}z_\vartheta - \mathsf{value}(\boldsymbol{\xi}_A) = \tau^{\ell-1}z - \mathsf{value}(\boldsymbol{\xi}_A) = \tau^{-(w-1)}z_\xi$$

start with 0.0^{w-1}, since our choice of k is k_0+w-1. As the unique NAF of $\mathsf{value}(\boldsymbol{\vartheta}_I\boldsymbol{\vartheta}_A) - \mathsf{value}(\boldsymbol{\xi}_A)$ concatenated with any NAF of $\tau^{-(w-1)}z_\vartheta$ gives rise to such an expansion, we conclude that $\mathsf{value}(\boldsymbol{\vartheta}_I\boldsymbol{\vartheta}_A) - \mathsf{value}(\boldsymbol{\xi}_A) = 0$ and therefore $\boldsymbol{\vartheta}_I = \mathbf{0}$ and $\boldsymbol{\vartheta}_A = \boldsymbol{\xi}_A$. So we conclude that all representations of z as a w-NAF have to be of the form $0\boldsymbol{.}\boldsymbol{\xi}_A0^{w-1}\boldsymbol{\eta}$ for some w-NAF $\boldsymbol{\eta}$. Thus, by using Proposition 7.7 on page 25, we get $z \notin \partial\mathcal{F}$ and therefore $z \in \operatorname{int}(\mathcal{F})$.

Until now we have proved

$$\overline{\dim}_B\partial\mathcal{F} \leq \overline{\dim}_B U < 2.$$

Because the Hausdorff dimension of a set is at most its upper box dimension, cf. Edgar [8] again, the desired result follows. □

8. Cell Rounding Operations

Let $\tau \in \mathbb{C}$ be an algebraic integer, imaginary quadratic. In this section define operators working on subsets (regions) of the complex plane. These will use the lattice $\mathbb{Z}[\tau]$ and the Voronoi cells defined in Section 2. They will be a very useful concept to prove Theorem 10.1 on page 36.

Definition 8.1 (Cell Rounding Operations)**.** Let $B \subseteq \mathbb{C}$ and $j \in \mathbb{R}$. We define the *cell packing of* B ("floor B")

$$\lfloor B\rfloor_{\hexagon} := \bigcup_{\substack{z\in\mathbb{Z}[\tau]\\ V_z\subseteq B}} V_z \qquad\text{and}\qquad \lfloor B\rfloor_{\hexagon,j} := \frac{1}{\tau^j}\left\lfloor \tau^j B\right\rfloor_{\hexagon},$$

the *cell covering of B* ("ceil B")

$$\lceil B \rceil_{\hexagon} := \overline{\lfloor B^C \rfloor_{\hexagon}^C} \qquad\text{and}\qquad \lceil B \rceil_{\hexagon,j} := \frac{1}{\tau^j} \lceil \tau^j B \rceil_{\hexagon},$$

the *fractional cells of B*

$$\{B\}_{\hexagon} := B \setminus \lfloor B \rfloor_{\hexagon} \qquad\text{and}\qquad \{B\}_{\hexagon,j} := \frac{1}{\tau^j} \{\tau^j B\}_{\hexagon},$$

the *cell covering of the boundary of B*

$$\partial(B)_{\hexagon} := \overline{\lceil B \rceil_{\hexagon} \setminus \lfloor B \rfloor_{\hexagon}} \qquad\text{and}\qquad \partial(B)_{\hexagon,j} := \frac{1}{\tau^j} \partial\big(\tau^j B\big)_{\hexagon},$$

the *cell covering of the lattice points inside B*

$$\lfloor B \rceil_{\hexagon} := \bigcup_{z \in B \cap \mathbb{Z}[\tau]} V_z \qquad\text{and}\qquad \lfloor B \rceil_{\hexagon,j} := \frac{1}{\tau^j} \lfloor \tau^j B \rceil_{\hexagon}$$

and the *number of lattice points inside B* as

$$\#(B)_{\hexagon} := \#(B \cap \mathbb{Z}[\tau]) \qquad\text{and}\qquad \#(B)_{\hexagon,j} := \#\big(\tau^j B\big)_{\hexagon}$$

To get a slight feeling what those operators do, have a look at Figure 8.1 on the facing page. There brief examples are given. For the cell covering of a set B an alternative, perhaps more intuitive description can be given by

$$\lceil B \rceil_{\hexagon} := \bigcup_{\substack{z \in \mathbb{Z}[\tau] \\ V_z \cap B \neq \emptyset}} V_z.$$

The following proposition deals with some basic properties that will be helpful, when working with those operators.

Proposition 8.2 (Basic Properties of Cell Rounding Operations)**.** *Let $B \subseteq \mathbb{C}$ and $j \in \mathbb{R}$.*

(a) We have the inclusions

$$\lfloor B \rfloor_{\hexagon,j} \subseteq B \subseteq \overline{B} \subseteq \lceil B \rceil_{\hexagon,j} \tag{8.1a}$$

and

$$\lfloor B \rfloor_{\hexagon,j} \subseteq \lfloor B \rceil_{\hexagon,j} \subseteq \lceil B \rceil_{\hexagon,j}\,. \tag{8.1b}$$

For $B' \subseteq \mathbb{C}$ with $B \subseteq B'$ we get $\lfloor B \rfloor_{\hexagon,j} \subseteq \lfloor B' \rfloor_{\hexagon,j}$, $\lfloor B \rceil_{\hexagon,j} \subseteq \lfloor B' \rceil_{\hexagon,j}$ and $\lceil B \rceil_{\hexagon,j} \subseteq \lceil B' \rceil_{\hexagon,j}$, i.e., monotonicity with respect to inclusion

(b) The inclusion

$$\{B\}_{\hexagon,j} \subseteq \partial(B)_{\hexagon,j} \tag{8.2}$$

holds.

(c) $\partial B \subseteq \partial(B)_{\hexagon,j}$ and for each cell V' in $\partial(B)_{\hexagon,j}$ we have $V' \cap \partial B \neq \emptyset$, so $\partial(B)_{\hexagon,j}$ is the smallest union of cells that contains ∂B.

(d) For $B' \subseteq \mathbb{C}$ with B' disjoint from B, we get

$$\#(B \cup B')_{\hexagon,j} = \#(B)_{\hexagon,j} + \#(B')_{\hexagon,j}\,, \tag{8.3}$$

and therefore the number of lattice points operation is monotonic with respect to inclusion, i.e., for $B'' \subseteq \mathbb{C}$ with $B'' \subseteq B$ we have $\#(B'')_{\hexagon,j} \leq \#(B)_{\hexagon,j}$. Further we get

$$\#(B)_{\hexagon,j} = \#\Big(\lfloor B \rceil_{\hexagon,j}\Big)_{\hexagon,j} = |\tau|^{2j} \frac{\lambda\Big(\lfloor B \rceil_{\hexagon,j}\Big)}{\lambda(V)} \tag{8.4}$$

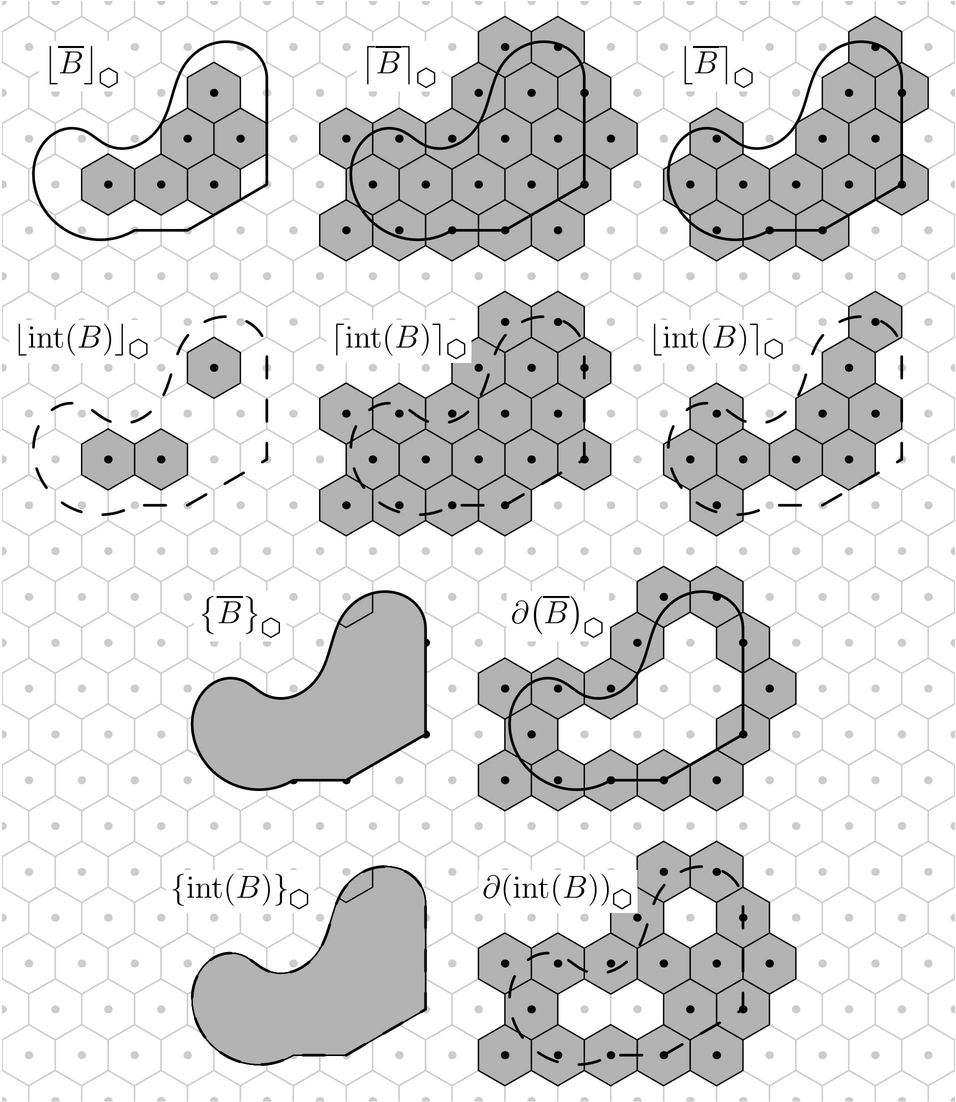

$\lfloor \overline{B} \rfloor_{\hexagon}$
$\lceil \overline{B} \rceil_{\hexagon}$
$\lfloor \overline{B} \rceil_{\hexagon}$
$\lfloor \mathrm{int}(B) \rfloor_{\hexagon}$
$\lceil \mathrm{int}(B) \rceil_{\hexagon}$
$\lfloor \mathrm{int}(B) \rceil_{\hexagon}$
$\{\overline{B}\}_{\hexagon}$
$\partial(\overline{B})_{\hexagon}$
$\{\mathrm{int}(B)\}_{\hexagon}$
$\partial(\mathrm{int}(B))_{\hexagon}$

Figure 8.1: Examples of the cell rounding operators of Definition 8.1 on page 27. As lattice $\mathbb{Z}[\tau]$ with $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$ was used here.

Proof. (a) $\lfloor B \rfloor_{\hexagon,j} \subseteq B$ follows directly from the definition. Since $\lfloor B^C \rfloor_{\hexagon,j} \subseteq B^C$, we get

$$\lceil B \rceil_{\hexagon,j} = \overline{\lfloor B^C \rfloor_{\hexagon,j}^C} \supseteq \overline{(B^C)^C} = \overline{B}.$$

The inclusion $\lfloor B \rfloor_{\hexagon,j} \subseteq \lfloor B \rceil_{\hexagon,j}$ follows directly from the definitions and $\lfloor B \rceil_{\hexagon,j} \subseteq \lceil B \rceil_{\hexagon,j}$ again by considering the complement, because $\overline{\lfloor B^C \rceil_{\hexagon,j}^C} = \lfloor B \rceil_{\hexagon,j}$. Similarly, the monotonicity can be shown.

(b) We have

$$\{B\}_{\hexagon,j} = B \setminus \lfloor B \rfloor_{\hexagon,j} \subseteq \lceil B \rceil_{\hexagon,j} \setminus \lfloor B \rfloor_{\hexagon,j} = \partial(B)_{\hexagon,j}\,.$$

(c) We assume $j = 0$. Using (a) yields $\partial B \subseteq \overline{B} \subseteq \lceil B \rceil_{\hexagon}$. Let $x \in \partial B$. If $x \notin B$, then $\lfloor B \rfloor_{\hexagon} \subseteq B$ implies that $x \notin \lfloor B \rfloor_{\hexagon}$. So we get

$$x \in \lceil B \rceil_{\hexagon} \setminus \lfloor B \rfloor_{\hexagon} \subseteq \overline{\lceil B \rceil_{\hexagon} \setminus \lfloor B \rfloor_{\hexagon}} = \partial(B)_{\hexagon}\,.$$

Now suppose $x \in B$. Consider all Voronoi cells V_i, $i \in I$, for a suitable finite index set I, such that $x \in V_i$. We get $x \in \operatorname{int}\bigl(\bigcup_{i\in I} V_i\bigr)$. If all of the V_i are a subset of $\lfloor B\rfloor_{\hexagon}$, then $x \in \operatorname{int}(B)$, which is a contradiction to $x \in \partial B$. So there is at least one cell V' that is not a subset of $\lfloor B\rfloor_{\hexagon}$. Since

$$\lceil B\rceil_{\hexagon}^C = \overline{\lfloor B^C\rfloor_{\hexagon}^C}^C = \operatorname{int}\left(\bigcup_{\substack{z\in\mathbb{Z}[\tau]\\ V_z\subseteq B^C}} V_z\right)$$

and $x \notin B^C$, V' is not in this union of cells. So V' is in the complement, i.e., $V' \subseteq \lceil B\rceil_{\hexagon}$. And therefore the statement follows.

Now we want to show that there is a subset of the boundary in each V-cell V' of $\partial(B)_{\hexagon}$. Assume $V' \cap \partial B = \emptyset$. If $V' \cap B = \emptyset$, then $V' \subseteq B^C$, so V' is not a subset of $\lceil B\rceil_{\hexagon}$, contradiction. If $V' \cap B \neq \emptyset$, then $V' \subseteq B$, since V' does not contain any boundary. But then, $V' \subseteq \lfloor B\rfloor_{\hexagon}$, again a contradiction.

(d) Since the operator just counts the number of lattice points, the first statement follows.

In the other statement, the first equality follows, because $z \in B \cap \mathbb{Z}[\tau] \iff V_z \subseteq \lfloor B\rceil_{\hexagon}$ holds. Since $\lfloor B\rceil_{\hexagon,j}$ consists of cells each with area $\lambda\bigl(\tau^{-j}V\bigr)$, the second equality is just, after multiplying by $\lambda\bigl(\tau^{-j}V\bigr)$, the equality of the areas. □

We will need some more properties concerning cardinality. We want to know the number of points inside a region after using one of the operators. Especially we are interested in the asymptotic behaviour, i.e., if our region becomes scaled very large. The following proposition provides information about that.

Proposition 8.3. *Let $U \subseteq \mathbb{C}$ bounded, measurable, and such that*

$$\#\bigl(\partial(NU)_{\hexagon}\bigr)_{\hexagon} = \mathcal{O}\Bigl(|N|^{\delta}\Bigr) \tag{8.5}$$

for $N \in \mathbb{C}$.

(a) We get

$$\#\bigl(\lfloor NU\rfloor_{\hexagon}\bigr)_{\hexagon} = |N|^2\,\frac{\lambda(U)}{\lambda(V)} + \mathcal{O}\Bigl(|N|^{\delta}\Bigr),$$

$$\#\bigl(\lceil NU\rceil_{\hexagon}\bigr)_{\hexagon} = |N|^2\,\frac{\lambda(U)}{\lambda(V)} + \mathcal{O}\Bigl(|N|^{\delta}\Bigr)$$

and

$$\#(NU)_{\hexagon} = \#\bigl(\lfloor NU\rceil_{\hexagon}\bigr)_{\hexagon} = |N|^2\,\frac{\lambda(U)}{\lambda(V)} + \mathcal{O}\Bigl(|N|^{\delta}\Bigr).$$

(b) We get

$$\#((N+1)U \setminus NU)_{\hexagon} = \mathcal{O}\Bigl(|N|^{\delta}\Bigr).$$

Proof. (a) Considering the areas yields

$$\#\bigl(\lfloor NU\rfloor_{\hexagon}\bigr)_{\hexagon}\,\lambda(V) \le \lambda(NU) = |N|^2\,\lambda(U) \le \#\bigl(\lceil NU\rceil_{\hexagon}\bigr)_{\hexagon}\,\lambda(V),$$

since $\lfloor NU\rfloor_{\hexagon} \subseteq NU \subseteq \lceil NU\rceil_{\hexagon}$, see Proposition 8.2 on page 28. If we use $\lceil NU\rceil_{\hexagon} = \lfloor NU\rfloor_{\hexagon} \cup \partial(NU)_{\hexagon}$, we obtain

$$0 \le |N|^2\,\frac{\lambda(U)}{\lambda(V)} - \#\bigl(\lfloor NU\rfloor_{\hexagon}\bigr)_{\hexagon} \le \#\bigl(\partial(NU)_{\hexagon}\bigr)_{\hexagon}$$

Because $\#\bigl(\partial(NU)_{\hexagon}\bigr)_{\hexagon} = \mathcal{O}\Bigl(|N|^{\delta}\Bigr)$ we get

$$\left| |N|^2\,\frac{\lambda(U)}{\lambda(V)} - \#\bigl(\lfloor NU\rfloor_{\hexagon}\bigr)_{\hexagon} \right| = \mathcal{O}\Bigl(|N|^{\delta}\Bigr),$$

and thus the result follows.

Combining the previous result and Proposition 8.2 on page 28 proves the other two statements.

(b) Let $d \in \mathbb{R}$ such that $U \subseteq \mathcal{B}(0, d)$. Let $y \in (N+1)U \setminus NU$. Obviously, this is equivalent to $y/(N+1) \in U$ and $y/N \notin U$, so there is a $z \in \partial U$ on the line from y/N to $y/(N+1)$. We get

$$\left|z - \frac{y}{N}\right| \leq |y| \cdot \left|\frac{1}{N} - \frac{1}{N+1}\right| = \frac{|y|}{|N+1|} \cdot \frac{1}{|N|} \leq \frac{d}{|N|},$$

and therefore

$$(N+1)U \setminus NU \subseteq \bigcup_{z \in \partial(NU)} \mathcal{B}(z, d)\,.$$

Since the boundary $\partial(NU)$ can be covered by $\mathcal{O}\Bigl(|N|^{\delta}\Bigr)$ cells, cf. (c) of Proposition 8.2 on page 28 and the discs in $\bigcup_{z \in \partial(NU)} \mathcal{B}(z, d)$ have a fixed size, the result follows. □

If the geometry of U is simple, e.g. U is a disc or U is a polygon, then we can check the covering condition (8.5) of Proposition 8.3 on the facing page by means of the following proposition.

Proposition 8.4. *Let $U \subseteq \mathbb{C}$ such that the boundary of U consists of finitely many rectifiable curves. Then we get*

$$\#\bigl(\partial(NU)_{\hexagon}\bigr)_{\hexagon} = \mathcal{O}(|N|)$$

for $N \in \mathbb{C}$.

Proof. Without loss of generality, we may assume that the boundary of U is a rectifiable curve $\gamma\colon\ [0, L] \longrightarrow \mathbb{C}$, which is parametrised by arc length. For any $t \in [1/(2\,|N|), L - 1/(2\,|N|)]$, we have

$$\gamma\biggl(\biggl[t - \frac{1}{2\,|N|}, t + \frac{1}{2\,|N|}\biggr]\biggr) \subseteq \mathcal{B}\biggl(\gamma(t), \frac{1}{2\,|N|}\biggr),$$

as the straight line from $\gamma(t)$ to $\gamma(t')$ is never longer than the arc-length of $\gamma([t, t'])$. Thus ∂U can be covered by $\mathcal{O}(L\,|N|)$ discs of radius $1/(2\,|N|)$ and consequently, $\partial(NU)$ can be covered by $\mathcal{O}(L\,|N|)$ discs of radius $\frac{1}{2}$. As $\mathbb{Z}[\tau]$ is a lattice, each disc with radius $\frac{1}{2}$ is contained in at most 4 Voronoi-cells, cf. Proposition 2.5 on page 5. Therefore, $\mathcal{O}(N)$ cells suffice to cover $\partial(NU)$. □

9. The Characteristic Sets W_η

Let $\tau \in \mathbb{C}$ be an algebraic integer, imaginary quadratic. Suppose that $|\tau| > 1$. Let $w \in \mathbb{N}$ with $w \geq 2$. Further let $\mathcal{D}$ be a minimal norm representatives digit set modulo τ^w as in Definition 3.5 on page 9. We denote the norm function by $\mathcal{N}\colon \mathbb{Z}[\tau] \longrightarrow \mathbb{Z}$, and we simply have $\mathcal{N}(\tau) = |\tau|^2$. Again for simplicity we set $\mathcal{D}^\bullet := \mathcal{D} \setminus \{0\}$.

In this section we define characteristic sets for a digit at a specified position in the w-NAF expansion and prove some basic properties of them. Those will be used in the proof of Theorem 10.1 on page 36.

Definition 9.1 (Characteristic Sets)**.** Let $\eta \in \mathcal{D}^\bullet$. For $j \in \mathbb{N}_0$ define

$$\mathcal{W}_{\eta,j} := \bigl\{\mathsf{value}(\boldsymbol{\xi}) \bigm| \boldsymbol{\xi} \in \mathbf{NAF}_w^{0.j+w} \text{ with } \xi_{-w} = \eta\bigr\}\,.$$

We call $\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}$ the *jth approximation of the characteristic set for* η, and we define

$$W_{\eta,j} := \Bigl\{\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Bigr\}_{\mathbb{Z}[\tau]}\,.$$

Further we define the *characteristic set for* η

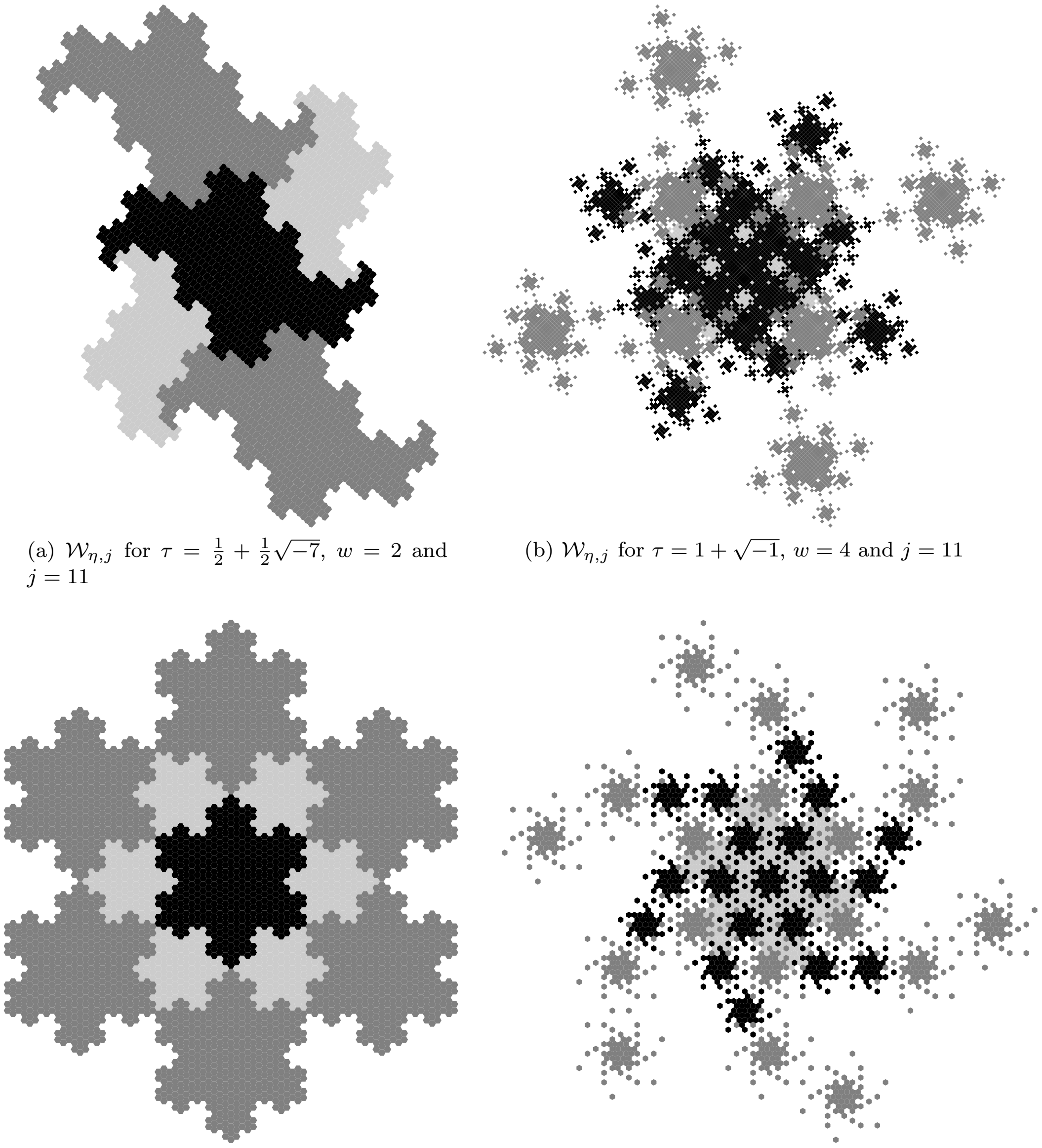
$$\mathcal{W}_{\eta} := \bigl\{\mathsf{value}(\boldsymbol{\xi}) \bigm| \boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty} \text{ with } \xi_{-w} = \eta\bigr\}\,.$$

and

$$W_\eta := \{\mathcal{W}_\eta\}_{\mathbb{Z}[\tau]}\,.$$

For $j \in \mathbb{N}_0$ we set

$$\beta_{\eta,j} := \lambda\Bigl(\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Bigr) - \lambda(\mathcal{W}_\eta)\,.$$



(a) $\mathcal{W}_{\eta,j}$ for $\tau = \frac{1}{2} + \frac{1}{2}\sqrt{-7}$, $w = 2$ and $j = 11$

(b) $\mathcal{W}_{\eta,j}$ for $\tau = 1 + \sqrt{-1}$, $w = 4$ and $j = 11$

(c) $\mathcal{W}_{\eta,j}$ for $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$, $w = 2$ and $j = 7$

(d) $\mathcal{W}_{\eta,j}$ for $\tau = \frac{3}{2} + \frac{1}{2}\sqrt{-3}$, $w = 3$ and $j = 6$

Figure 9.1: Characteristic sets $\mathcal{W}_\eta$. Each figure can either be seen as approximation $\mathcal{W}_{\eta,j}$ for $\mathcal{W}_\eta$, or as values of w-NAFs of length j, where a scales Voronoi cell is drawn for each point. Different colours correspond to the digits 1 and w from the left in the w-NAF. They are "marked" whether they are zero or non-zero.

Note that sometimes the set W_η will also be called *characteristic set for* η, and analogously for the set $W_{\eta,j}$. In Figure 9.1 some of these characteristic sets — more precisely some approximations of the characteristic sets — are shown. The following proposition will deal with some properties of those defined sets,

Proposition 9.2 (Properties of the Characteristic Sets)**.** *Let $\eta \in \mathcal{D}^\bullet$.*

(a) We have

$$\mathcal{W}_\eta = \eta\tau^{-w} + \tau^{-2w+1}\mathcal{F}.$$

(b) The set $\mathcal{W}_\eta$ is compact.

(c) We get

$$\mathcal{W}_\eta = \overline{\bigcup_{j\in\mathbb{N}_0} \mathcal{W}_{\eta,j}} = \overline{\lim_{j\to\infty} \mathcal{W}_{\eta,j}}.$$

(d) The set $\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}$ is indeed an approximation of $\mathcal{W}_\eta$, i.e., we have

$$\mathcal{W}_\eta = \overline{\liminf_{j\in\mathbb{N}_0} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}} = \overline{\limsup_{j\in\mathbb{N}_0} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}}.$$

(e) We have $\operatorname{int} \mathcal{W}_\eta \subseteq \liminf_{j\in\mathbb{N}_0} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}$.

(f) We get $\mathcal{W}_\eta - \eta\tau^{-w} \subseteq V$, and for $j \in \mathbb{N}_0$ we obtain $\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w} - \eta\tau^{-w} \subseteq V$.

(g) For the Lebesgue measure of the characteristic set we obtain $\lambda(\mathcal{W}_\eta) = \lambda(W_\eta)$ and for its approximation $\lambda\Big(\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Big) = \lambda(W_{\eta,j})$.

(h) Let $j \in \mathbb{N}_0$. If $j < w-1$, then the area of $\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}$ is

$$\lambda\Big(\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Big) = |\tau|^{-2(j+w)} \lambda(V).$$

If $j \geq w-1$, then the area of $\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}$ is

$$\lambda\Big(\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Big) = \lambda(V)\, e_w + \mathcal{O}\big(\rho^j\big)$$

with e_w and ρ from Theorem 4.1 on page 11.

(i) The area of W_η is

$$\lambda(W_\eta) = \lambda(V)\, e_w,$$

again with e_w from Theorem 4.1 on page 11.

(j) Let $j \in \mathbb{N}_0$. We get

$$\beta_{\eta,j} = \int_{x\in V} \big(\mathbb{1}_{W_{\eta,j}} - \mathbb{1}_{W_\eta}\big)(x)\, \mathrm{d}x.$$

If $j < w-1$, then its value is

$$\beta_{\eta,j} = \Big(|\tau|^{-2(j+w)} - e_w\Big)\, \lambda(V).$$

If $j \geq w-1$, then we get

$$\beta_{\eta,j} = \mathcal{O}\big(\rho^j\big).$$

Again e_w and ρ can be found in Theorem 4.1 on page 11.

Proof. (a) Is clear, since we have the digit η at index $-w$ and an arbitrary w-NAF starting with index $-2w$. Note that the elements in $\mathbf{NAF}_w^{0.\infty}$ start with index -1.

(b) Follows directly from (a), because $\mathcal{F}$ is compact according to Proposition 7.2 on page 23.

(c) Clearly we have $\mathcal{W}_{\eta,j} \subseteq \mathcal{W}_\eta$. Thus $\bigcup_{j\in\mathbb{N}_0} \mathcal{W}_{\eta,j} \subseteq \mathcal{W}_\eta$, and because $\mathcal{W}_\eta$ is closed, the inclusion $\overline{\bigcup_{j\in\mathbb{N}_0} \mathcal{W}_{\eta,j}} \subseteq \mathcal{W}_\eta$ follows. Now let $z \in \mathcal{W}_\eta$, and let $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty}$, such that $\mathsf{value}(\boldsymbol{\xi}) = z$. Then there is a sequence of w-NAFs $(\boldsymbol{\xi}_\ell)_{\ell\in\mathbb{N}_0}$ with finite right-lengths that converges to $\boldsymbol{\xi}$ and clearly

$$\mathsf{value}(\boldsymbol{\xi}_\ell) \in \bigcup_{k\in\mathbb{N}_0} \mathcal{W}_{\eta,k}.$$

Since evaluating the value is a continuous function, see Proposition 3.8 on page 10, we get

$$z = \mathsf{value}(\boldsymbol{\xi}) = \mathsf{value}\left(\lim_{\ell\to\infty} \boldsymbol{\xi}_\ell\right) = \lim_{\ell\to\infty} \mathsf{value}(\boldsymbol{\xi}_\ell) \in \overline{\bigcup_{k\in\mathbb{N}_0} \mathcal{W}_{\eta,j}}.$$

The equality $\bigcup_{j\in\mathbb{N}_0} \mathcal{W}_{\eta,j} = \lim_{j\to\infty} \mathcal{W}_{\eta,j}$ is obvious, since $\mathcal{W}_{\eta,j}$ is monotonic increasing.

(d) First we show that we have

$$\limsup_{j\to\infty} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w} \subseteq \mathcal{W}_\eta.$$

Let

$$z \in \limsup_{j\to\infty} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w} = \bigcap_{j\in\mathbb{N}_0} \bigcup_{k\geq j} \lfloor \mathcal{W}_{\eta,k} \rceil_{\hexagon,k+w} .$$

Then there is a $j_0 \geq 0$ such that $z \in \lfloor \mathcal{W}_{\eta,j_0} \rceil_{\hexagon,j_0+w}$. Further, for $j_{\ell-1}$ there is a $j_\ell \geq j_{\ell-1}$, such that $z \in \lfloor \mathcal{W}_{\eta,j_\ell} \rceil_{\hexagon,j_\ell+w}$. For each $\ell \in \mathbb{N}_0$ there is a $z_\ell \in \mathcal{W}_{\eta,j_\ell} \subseteq \mathcal{W}_\eta$ with

$$|z - z_\ell| \leq c_V \, |\tau| \, |\tau|^{-j_\ell - w} ,$$

since $\lfloor \mathcal{W}_{\eta,j_\ell} \rceil_{\hexagon,j_\ell+w}$ consists of cells $|\tau|^{-j_\ell-w} V$ with centres out of $\mathcal{W}_{\eta,j_\ell}$. Refer to Proposition 2.5 on page 5 for the constant $c_V \, |\tau|$. Thus we get $z = \lim_{\ell\to\infty} z_\ell \in \mathcal{W}_\eta$, since $|\tau|^{-j_\ell-w}$ tends to 0 for large ℓ and $\mathcal{W}_\eta$ is closed.

Using the closeness property of $\mathcal{W}_\eta$ again yields

$$\overline{\limsup_{j\to\infty} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}} \subseteq \mathcal{W}_\eta .$$

Now we are ready to show the stated equalities. We obtain

$$\mathcal{W}_\eta = \overline{\lim_{j\to\infty} \mathcal{W}_{\eta,j}} = \overline{\liminf_{j\to\infty} \mathcal{W}_{\eta,j}} \subseteq \overline{\liminf_{j\to\infty} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}} \subseteq \overline{\limsup_{j\to\infty} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}} \subseteq \mathcal{W}_\eta,$$

so equality holds everywhere.

(e) Let $z \in \operatorname{int} \mathcal{W}_\eta$. Then there exists an $\varepsilon > 0$ such that $\mathcal{B}(z, \varepsilon) \subseteq \operatorname{int} \mathcal{W}_\eta$. For each $k \in \mathbb{N}_0$ there is a $y \in \tau^{-k-w}\mathbb{Z}[\tau]$ with the property that z is in the corresponding Voronoi cell, i.e., $z \in y + \tau^{-k-w} V$. For this y, there is also an $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}.k+w}$ such that $y = \mathsf{value}(\boldsymbol{\xi})$.

Clearly, if k is large enough, say $k \geq j$, we obtain $y + \tau^{-k-w} V \subseteq \mathcal{B}(z, \varepsilon)$. From Proposition 7.7 on page 25 (combined with (a)) we know that all w-NAFs corresponding to the values in $\operatorname{int} \mathcal{W}_\eta$ must have η at digit $-w$ and integer part $\mathbf{0}$. But this means that $\mathsf{value}(\boldsymbol{\xi}) \in \mathcal{W}_{\eta,k}$ and therefore $z \in \lfloor \mathcal{W}_{\eta,k} \rceil_{\hexagon,k+w}$. So we conclude

$$z \in \bigcup_{j\in\mathbb{N}_0} \bigcap_{k\geq j} \lfloor \mathcal{W}_{\eta,k} \rceil_{\hexagon,k+w} = \liminf_{j\to\infty} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w} .$$

(f) Each w-NAF $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.\infty}$ corresponding to a value in $\mathcal{W}_\eta - \eta\tau^{-w}$ starts with $2w-1$ zeros from the left. Therefore

$$\mathsf{value}(\boldsymbol{\xi}) = \tau^{1-2w} \, \mathsf{value}(\boldsymbol{\vartheta})$$

for an appropriate w-NAF $\boldsymbol{\vartheta} \in \mathbf{NAF}_w^{0.\infty}$. Thus, using $\mathsf{value}(\boldsymbol{\vartheta}) \in \tau^{2w-1} V$ from Proposition 5.1 on page 14, the desired inclusion follows.

The set $\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w} - \eta\tau^{-w} \subseteq V$ consists of cells of type $\tau^{-j-w} V$, where their centres are the fractional value of an element $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.j+w}$. Again the first $2w-1$ digits are zero, so

$$\mathsf{value}(\boldsymbol{\xi}) = \tau^{1-2w} \, \mathsf{value}(\boldsymbol{\vartheta})$$

for an appropriate w-NAF $\boldsymbol{\vartheta} \in \mathbf{NAF}_w^{0.j-w+1}$. Suppose $j \geq w-1$. Using $\mathsf{value}(\boldsymbol{\vartheta}) + \tau^{-(j-w+1)} V \subseteq \tau^{2w-1} V$ again from Proposition 5.1 on page 14, the statement follows. If $j < w-1$, then $\mathsf{value}(\boldsymbol{\vartheta}) = 0$ and it remains to show that $\tau^{-j-w} V \subseteq V$. But this is clearly true, since $\tau^{-1} V \subseteq V$ according to Proposition 2.5 on page 5.

(g) As a shifted version of the sets $\mathcal{W}_\eta$ and $\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}$ is contained in V by (f), so the equality of the Lebesgue measures follows directly.

(h) The set $\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}$ consists of of cells of type $\tau^{-j-w} V$, where their centres are the value of an element $\boldsymbol{\xi} \in \mathbf{NAF}_w^{0.j+w}$. The intersection of two different cells is contained in the boundary of the cells, so a set of Lebesgue measure zero.

Suppose $j \geq w-1$. Since the digit $\xi_{-w} = \eta$ is fixed, the first $2w-1$ digits from the left are fixed, too. The remaining word $\xi_{-2w} \ldots \xi_{-(j+w)}$ can be an arbitrary w-NAF of length $j - w + 1$, so there are $C_{j-w+1,w}$ choices, see Theorem 4.1 on page 11.

Thus we obtain

$$\lambda\Big(\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Big) = C_{j-w+1,w} \, \lambda\Big(\tau^{-(w+j)} V\Big) = C_{j-w+1,w} \, |\tau|^{-2(w+j)} \, \lambda(V) .$$

Inserting the results of Theorem 4.1 on page 11 yields

$$\begin{aligned}\lambda\Big(\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Big) &= \left(\frac{\left|\tau\right|^{2(j-w+1+w)}}{\left(\left|\tau\right|^2-1\right)w+1} + \mathcal{O}\left(\left(\rho\left|\tau\right|^2\right)^{j-w+1}\right)\right)\left|\tau\right|^{-2(w+j)}\lambda(V)\\ &= \lambda(V)\underbrace{\frac{1}{\left|\tau\right|^{2(w-1)}\left(\left(\left|\tau\right|^2-1\right)w+1\right)}}_{=e_w} + \mathcal{O}\big(\rho^j\big)\,.\end{aligned}$$

If $j < w-1$, then $\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}$ consists of only one cell of size $\tau^{-j-w}V$, so the stated result follows directly.

(i) Using (d), (e) and the continuity of the Lebesgue measure yields

$$\begin{aligned}\lambda\Big(\liminf_{j\in\mathbb{N}_0} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Big) &\le \liminf_{j\in\mathbb{N}_0} \lambda\Big(\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Big) \le \limsup_{j\in\mathbb{N}_0} \lambda\Big(\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Big)\\ &\le \lambda\Big(\limsup_{j\in\mathbb{N}_0} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Big) \le \lambda\Big(\overline{\limsup_{j\in\mathbb{N}_0} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}}\Big)\\ &= \lambda(\mathcal{W}_\eta) \le \lambda(\operatorname{int}\mathcal{W}_\eta) + \lambda(\partial\mathcal{W}_\eta)\\ &\le \lambda\Big(\liminf_{j\in\mathbb{N}_0} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Big) + \lambda(\partial\mathcal{W}_\eta)\,.\end{aligned}$$

Since $\lambda(\partial\mathcal{W}_\eta) = 0$, combine (a) and Proposition 7.8 on page 25 to see this, we have equality everywhere, so

$$\lambda(\mathcal{W}_\eta) = \lim_{j\in\mathbb{N}_0} \lambda\Big(\lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}\Big)\,.$$

Thus the desired result follows from (h), because $\rho < 1$.

(j) Using (f) and (g) yields the first statement. The other result follows directly by using (h) and (i). □

Using the results of the previous proposition, we can finally determine the Lebesgue measure of the fundamental domain $\mathcal{F}$ defined in Section 7.

Remark 9.3 (Lebesgue Measure of the Fundamental Domain). We get

$$\lambda(\mathcal{F}) = \left|\tau\right|^{2w-1} e_w\,\lambda(V) = \frac{\left|\tau\right|\left|\operatorname{Im}(\tau)\right|}{(\left|\tau\right|^2-1)w+1},$$

using (a) and (i) from Proposition 9.2 on page 32, e_w from Theorem 4.1 on page 11, and $\lambda(V) = \left|\operatorname{Im}(\tau)\right|$ from Proposition 2.5 on page 5.

The next lemma makes the connection between the w-NAFs of elements of the lattice $\mathbb{Z}[\tau]$ and the characteristic sets $W_{\eta,j}$.

Lemma 9.4. *Let $\eta \in \mathcal{D}^\bullet$, $j \ge 0$. Let $n \in \mathbb{Z}[\tau]$ and let $\mathbf{n} \in \mathbf{NAF}_w^{\mathsf{fin}}$ be its w-NAF. Then the following statements are equivalent:*

(1) The jth digit of $\mathbf{n}$ equals η.

(2) The condition $\left\{\tau^{-(j+w)}n\right\}_{\mathbb{Z}[\tau]} \in W_{\eta,j}$ holds.

(3) The inclusion $\left\{\tau^{-(j+w)}V_n\right\}_{\mathbb{Z}[\tau]} \subseteq W_{\eta,j}$ holds.

Proof. Define $\mathbf{m}$ by

$$m_k := \begin{cases} n_k & \text{if } k < j+w,\\ 0 & \text{if } k \ge j+w\end{cases}$$

and $m := \mathsf{value}(\mathbf{m})$. Then, by definition, $m \equiv n \pmod{\tau^{j+w}}$,

$$\left\{\tau^{-(j+w)}n\right\}_{\mathbb{Z}[\tau]} = \left\{\tau^{-(j+w)}m\right\}_{\mathbb{Z}[\tau]}$$

and $\tau^{-(j+w)}m \in \mathcal{F}$. As the jth digit of $\mathbf{n}$ only depends on the $j+w$ least significant digits of $\mathbf{n}$, it is sufficient to show the equivalence of the assertions when $\mathbf{n}$ and n are replaced by $\mathbf{m}$ and m, respectively.

By definition, $m_j = \eta$ is equivalent to $\tau^{-(j+w)}m \in \mathcal{W}_{\eta,j}$.

(1) $\Longrightarrow$ *(3).* Assume now that $\tau^{-(j+w)}m \in \mathcal{W}_{\eta,j}$. Then $m \in \tau^{j+w}\mathcal{W}_{\eta,j}$ and

$$\tau^{-(j+w)}V_m \subseteq \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w} .$$

This implies $\left\{\tau^{-(j+w)}V_m\right\}_{\mathbb{Z}[\tau]} \subseteq W_j$.

(3) $\Longrightarrow$ *(2).* This implication holds trivially.

(2) $\Longrightarrow$ *(1).* So now assume that $\left\{\tau^{-(j+w)}m\right\}_{\mathbb{Z}[\tau]} \in W_{\eta,j}$. Thus there is an m' such that

$$\tau^{-(j+w)}m' \in \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}$$

and

$$\tau^{-(j+w)}m - \tau^{-(j+w)}m' \in \mathbb{Z}[\tau].$$

This immediately implies $m' \in \mathbb{Z}[\tau]$ and $m \equiv m' \pmod{\tau^{j+w}}$. We also conclude that $m' \in \tau^{j+w} \lfloor \mathcal{W}_{\eta,j} \rceil_{\hexagon,j+w}$. As $m' \in \mathbb{Z}[\tau]$, this is equivalent to $m' \in \tau^{j+w}\mathcal{W}_{\eta,j}$ and therefore $\tau^{-(j+w)}m' \in \mathcal{W}_{\eta,j}$. By definition of $\mathcal{W}_{\eta,j}$, there is a $0.\mathbf{m}' \in \mathbf{NAF}_w^{0.j+w}$ such that $\tau^{-(j+w)}m' = \mathsf{value}(0.\mathbf{m}')$, i.e., $m' = \mathsf{value}(\mathbf{m}')$, and $m'_j = \eta$. From $m' \equiv m \pmod{\tau^{j+w}}$ we conclude that $m_j = \eta$, too. (In fact, one can now easily show that we have $\mathbf{m}' = \mathbf{m}$, but this is not really needed.) □

10. Counting the Occurrences of a non-zero Digit in a Region

Let $\tau \in \mathbb{C}$ be an algebraic integer, imaginary quadratic. Suppose that $|\tau| > 1$. Let $w \in \mathbb{N}$ with $w \geq 2$. Further let $\mathcal{D}$ be a minimal norm representatives digit set modulo τ^w as in Definition 3.5 on page 9.

We denote the norm function by $\mathcal{N} \colon \mathbb{Z}[\tau] \longrightarrow \mathbb{Z}$, and we simply have $\mathcal{N}(\tau) = |\tau|^2$. We write $\tau = |\tau| e^{i\theta}$ for $\theta \in (-\pi, \pi]$. Further Iverson's notation $[\mathit{expr}] = 1$ if *expr* is true and $[\mathit{expr}] = 0$ otherwise, cf. Graham, Knuth and Patashnik [11], will be used.

In this section we will prove our main result on the asymptototic number of occurrences of a digit in a given region.

Theorem 10.1 (Counting Theorem)**.** *Let $0 \neq \eta \in \mathcal{D}$ and $N \in \mathbb{R}$ with $N \geq 0$. Further let $U \subseteq \mathbb{C}$ be measurable with respect to the Lebesgue measure, $U \subseteq \mathcal{B}(0,d)$ with d finite, i.e., U bounded, and set δ such that $\#\big(\partial(NU)_{\hexagon}\big)_{\hexagon} = \mathcal{O}\big(N^\delta\big)$. Assume $1 \leq \delta < 2$. We denote the number of occurrences of the digit η in all width-w non-adjacent forms with value in the region NU by*

$$Z_{\tau,w,\eta}(N) = \sum_{z \in NU \cap \mathbb{Z}[\tau]} \sum_{j \in \mathbb{N}_0} \left[j\text{th digit of } z \text{ in its } w\text{-NAF-expansion equals } \eta\right].$$

Then we get

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

in which the following expressions are used. The Lebesgue measure is denoted by λ. We have the constant of the expectation

$$e_w = \frac{1}{|\tau|^{2(w-1)}\Big(\Big(|\tau|^2 - 1\Big) w + 1\Big)},$$

cf. Theorem 4.1 on page 11. Then there is the function

$$\psi_\eta(x) = \psi_{\eta,\mathcal{M}}(x) + \psi_{\eta,\mathcal{P}}(x) + \psi_{\eta,\mathcal{Q}}(x),$$

where

$$\psi_{\eta,\mathcal{M}}(x) = \lambda(U)\left(c + 1 - \{x\}\right) e_w,$$

$$\psi_{\eta,\mathcal{P}}(x) = \frac{\left|\tau\right|^{2(c-\{x\})}}{\lambda(V)} \sum_{j=0}^{\infty} \int_{y \in \left\{\left|\tau\right|^{\{x\}-c}\, \widehat{\theta}(\lfloor x \rfloor) U\right\}_{\hexagon, j-w}} \Big(\mathbb{1}_W\Big(\left\{y\tau^{j-w}\right\}_{\mathbb{Z}[\tau]}\Big) - \lambda(W)\Big)\, \mathrm{d}y,$$

with the rotation $\widehat{\theta}(x) = e^{-i\theta x - i\theta c}$, *and*

$$\psi_{\eta,\mathcal{Q}}(x) = \psi_{\eta,\mathcal{Q}} = \frac{\lambda(U)}{\lambda(V)} \sum_{j=0}^{\infty} \frac{\beta_j}{\lambda(V)}.$$

We have $\alpha = 2 + \log_{\left|\tau\right|} \rho < 2$, *with* $\rho = \Big(1 + \frac{1}{\left|\tau\right|^2 w^3}\Big)^{-1} < 1$, *and*

$$c = \Big\lfloor \log_{\left|\tau\right|} d - \log_{\left|\tau\right|} f_L \Big\rfloor + 1$$

with the constant f_L *of Proposition 5.2 on page 16.*

Further, if there is a $p \in \mathbb{N}$, *such that* $e^{2i\theta p} U = U$, *then* ψ_η *is* p*-periodic and continuous.*

Remark 10.2. Consider the main term of our result. When N tends to infinity, we get the asymptotic formula

$$Z_{\tau,w,\eta} \sim e_w N^2\, \lambda(U) \log_{\left|\tau\right|} N.$$

This result is not surprising, since intuitively there are about $N^2\, \lambda(U)$ w-NAFs in the region NU, and each of them can be represented as a w-NAF with length $\log_{\left|\tau\right|} N$. Therefore, using the expectation of Theorem 4.1 on page 11, we get an explanation for this term.

Remark 10.3. Using a disc as region U, e.g. $U = \mathcal{B}(0,1)$, yields that ψ_η is 1-periodic and continuous for all valid τ. The reason is that the condition $e^{i\theta p} U = U$ is then clearly fulfilled for every p, especially for $p = 1$.

The parameter δ is 1 for simple geometries like a disc or a polygon. See Proposition 8.4 on page 31 for details.

Remark 10.4. If $\delta = 2$ in the theorem, then the statement stays true, but degenerates to

$$Z_{\tau,w,\eta}(N) = \mathcal{O}\Big(N^2 \log_{\left|\tau\right|} N\Big).$$

This is a trivial result of Remark 10.2.

The proof of Theorem 10.1 on the preceding page follows the ideas used by Delange [7]. By Remark 10.4 we restrict ourselves to the case $\delta < 2$.

We will use the following abbreviations. We set $Z(N) := Z_{\tau,w,\eta}(N)$, and we set $W := W_\eta$ and $W_j := W_{\eta,j}$ for our fixed η of Theorem 10.1 on the preceding page. Further we set $\beta_j := \beta_{\eta,j}$, cf. Proposition 9.2 on page 32. By log we will denote the logarithm to the base $\left|\tau\right|$, i.e., $\log x = \log_{\left|\tau\right|} x$. These abbreviations will be used throughout the remaining section.

Proof of Theorem 10.1. We know from Theorem 6.1 on page 21 that every element of $\mathbb{Z}[\tau]$ is represented by a unique element of $\mathbf{NAF}_w^{\mathsf{fin}}$. To count the occurrences of the digit η in NU, we sum up 1 over all lattice points $n \in NU \cap \mathbb{Z}[\tau]$ and for each n over all digits in the corresponding w-NAF equal to η. Thus we get

$$Z(N) = \sum_{n \in NU \cap \mathbb{Z}[\tau]} \sum_{j \in \mathbb{N}_0} \left[\varepsilon_j(\mathsf{NAF}_w(n)) = \eta\right],$$

where ε_j denotes the extraction of the jth digit, i.e., for a w-NAF $\boldsymbol{\xi}$ we define $\varepsilon_j(\boldsymbol{\xi}) := \xi_j$. The inner sum over $j \in \mathbb{N}_0$ is finite, we will choose a large enough upper bound J later in Lemma 10.5 on page 39.

Using

$$\left[\varepsilon_j(\mathsf{NAF}_w(n)) = \eta\right] = \mathbb{1}_{W_j}\left(\left\{\frac{n}{\tau^{j+w}}\right\}_{\mathbb{Z}[\tau]}\right)$$

from Lemma 9.4 on page 35 yields

$$Z(N) = \sum_{j=0}^{J} \sum_{n \in NU \cap \mathbb{Z}[\tau]} \mathbb{1}_{W_j}\left(\left\{\frac{n}{\tau^{j+w}}\right\}_{\mathbb{Z}[\tau]}\right),$$

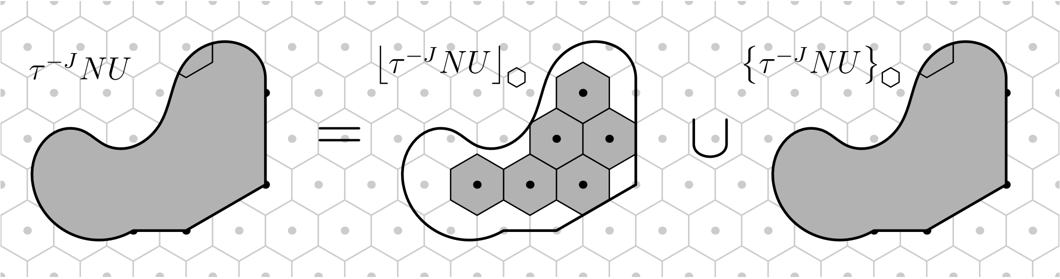

$\tau^{-J}NU$
$=$
$\lfloor \tau^{-J}NU \rceil_{\hexagon}$
$\cup$
$\{\tau^{-J}NU\}_{\hexagon}$

Figure 10.1: Splitting up the region of integration $\tau^{-J}NU$.

where additionally the order of summation was changed. This enables us to rewrite the sum over n as integral

$$\begin{aligned} Z(N) &= \sum_{j=0}^{J} \sum_{n \in NU \cap \mathbb{Z}[\tau]} \frac{1}{\lambda(V_n)} \int_{x \in V_n} \mathbb{1}_{W_j}\left(\left\{ \frac{x}{\tau^{j+w}} \right\}_{\mathbb{Z}[\tau]} \right) \mathrm{d}x \\ &= \frac{1}{\lambda(V)} \sum_{j=0}^{J} \int_{x \in \lfloor NU \rceil_{\hexagon}} \mathbb{1}_{W_j}\left(\left\{ \frac{x}{\tau^{j+w}} \right\}_{\mathbb{Z}[\tau]} \right) \mathrm{d}x. \end{aligned}$$

We split up the integrals into the ones over NU and others over the remaining region and get

$$Z(N) = \frac{1}{\lambda(V)} \sum_{j=0}^{J} \int_{x \in NU} \mathbb{1}_{W_j}\left(\left\{ \frac{x}{\tau^{j+w}} \right\}_{\mathbb{Z}[\tau]} \right) \mathrm{d}x + \mathcal{F}_\eta(N)\,,$$

in which $\mathcal{F}_\eta(N)$ contains all integrals (with appropriate signs) over regions $\lfloor NU \rceil_{\hexagon} \setminus NU$ and $NU \setminus \lfloor NU \rceil_{\hexagon}$.

Substituting $x = \tau^J y,\ \mathrm{d}x = |\tau|^{2J}\, \mathrm{d}y$ we obtain

$$Z(N) = \frac{|\tau|^{2J}}{\lambda(V)} \sum_{j=0}^{J} \int_{y \in \tau^{-J}NU} \mathbb{1}_{W_j}\left(\left\{ y\tau^{J-j-w} \right\}_{\mathbb{Z}[\tau]} \right) \mathrm{d}y + \mathcal{F}_\eta(N)\,.$$

Reversing the order of summation yields

$$Z(N) = \frac{|\tau|^{2J}}{\lambda(V)} \sum_{j=0}^{J} \int_{y \in \tau^{-J}NU} \mathbb{1}_{W_{J-j}}\left(\left\{ y\tau^{j-w} \right\}_{\mathbb{Z}[\tau]} \right) \mathrm{d}y + \mathcal{F}_\eta(N)\,.$$

We rewrite this as

$$\begin{aligned} Z(N) = {} & \frac{|\tau|^{2J}}{\lambda(V)} (J+1)\, \lambda(W) \int_{y \in \tau^{-J}NU} \mathrm{d}y \\ & + \frac{|\tau|^{2J}}{\lambda(V)} \sum_{j=0}^{J} \int_{y \in \tau^{-J}NU} \Big(\mathbb{1}_W\left(\left\{ y\tau^{j-w} \right\}_{\mathbb{Z}[\tau]} \right) - \lambda(W) \Big) \mathrm{d}y \\ & + \frac{|\tau|^{2J}}{\lambda(V)} \sum_{j=0}^{J} \int_{y \in \tau^{-J}NU} \Big(\mathbb{1}_{W_{J-j}}\left(\left\{ y\tau^{j-w} \right\}_{\mathbb{Z}[\tau]} \right) - \mathbb{1}_W\left(\left\{ y\tau^{j-w} \right\}_{\mathbb{Z}[\tau]} \right) \Big) \mathrm{d}y \\ & + \mathcal{F}_\eta(N)\,. \end{aligned}$$

With $\tau^{-J}NU = \lfloor \tau^{-J}NU \rceil_{\hexagon, j-w} \cup \{\tau^{-J}NU\}_{\hexagon, j-w}$, see Figure 10.1, for each integral region we get

$$Z(N) = \mathcal{M}_\eta(N) + \mathcal{Z}_\eta(N) + \mathcal{P}_\eta(N) + \mathcal{Q}_\eta(N) + \mathcal{S}_\eta(N) + \mathcal{F}_\eta(N)\,,$$

in which $\mathcal{M}_\eta$ is *"The Main Part"*, see Lemma 10.8 on the next page,

$$\mathcal{M}_\eta(N) = \frac{|\tau|^{2J}}{\lambda(V)} (J+1)\, \lambda(W) \int_{y \in \tau^{-J} NU} \mathrm{d}y, \tag{10.1a}$$

$\mathcal{Z}_\eta$ is *"The Zero Part"*, see Lemma 10.9 on the following page,

$$\mathcal{Z}_\eta(N) = \frac{|\tau|^{2J}}{\lambda(V)} \sum_{j=0}^{J} \int_{y \in \lfloor \tau^{-J} NU \rceil_{\hexagon, j-w}} \Big(\mathbb{1}_W \Big(\big\{ y \tau^{j-w} \big\}_{\mathbb{Z}[\tau]} \Big) - \lambda(W) \Big) \, \mathrm{d}y, \tag{10.1b}$$

$\mathcal{P}_\eta$ is *"The Periodic Part"*, see Lemma 10.10 on page 41,

$$\mathcal{P}_\eta(N) = \frac{|\tau|^{2J}}{\lambda(V)} \sum_{j=0}^{J} \int_{y \in \{ \tau^{-J} NU \}_{\hexagon, j-w}} \Big(\mathbb{1}_W \Big(\big\{ y \tau^{j-w} \big\}_{\mathbb{Z}[\tau]} \Big) - \lambda(W) \Big) \, \mathrm{d}y, \tag{10.1c}$$

$\mathcal{Q}_\eta$ is *"The Other Part"*, see Lemma 10.11 on page 42,

$$\mathcal{Q}_\eta(N) = \frac{|\tau|^{2J}}{\lambda(V)} \sum_{j=0}^{J} \int_{y \in \lfloor \tau^{-J} NU \rceil_{\hexagon, j-w}} \big(\mathbb{1}_{W_{J-j}} - \mathbb{1}_W \big) \Big(\big\{ y \tau^{j-w} \big\}_{\mathbb{Z}[\tau]} \Big) \, \mathrm{d}y, \tag{10.1d}$$

$\mathcal{S}_\eta$ is *"The Small Part"*, see Lemma 10.12 on page 43,

$$\mathcal{S}_\eta(N) = \frac{|\tau|^{2J}}{\lambda(V)} \sum_{j=0}^{J} \int_{y \in \{ \tau^{-J} NU \}_{\hexagon, j-w}} \big(\mathbb{1}_{W_{J-j}} - \mathbb{1}_W \big) \Big(\big\{ y \tau^{j-w} \big\}_{\mathbb{Z}[\tau]} \Big) \, \mathrm{d}y \tag{10.1e}$$

and $\mathcal{F}_\eta$ is *"The Fractional Cells Part"*, see Lemma 10.13 on page 44,

$$\begin{aligned} \mathcal{F}_\eta(N) = {} & \frac{1}{\lambda(V)} \sum_{j=0}^{J} \int_{x \in \lfloor NU \rceil_{\hexagon} \setminus NU} \mathbb{1}_{W_j} \bigg(\Big\{ \frac{x}{\tau^{j+w}} \Big\}_{\mathbb{Z}[\tau]} \bigg) \, \mathrm{d}x \\ & - \frac{1}{\lambda(V)} \sum_{j=0}^{J} \int_{x \in NU \setminus \lfloor NU \rceil_{\hexagon}} \mathbb{1}_{W_j} \bigg(\Big\{ \frac{x}{\tau^{j+w}} \Big\}_{\mathbb{Z}[\tau]} \bigg) \, \mathrm{d}x. \end{aligned} \tag{10.1f}$$

To complete the proof we have to deal with the choice of J, see Lemma 10.5, as well as with each of the parts in (10.1), see Lemmata 10.8 to 10.13 on pages 40–44. The continuity of ψ_η is checked in Lemma 10.14 on page 44. □

Lemma 10.5 (Choosing J)**.** *Let $N \in \mathbb{R}_{\geq 0}$. Then every w-NAF of $\mathbf{NAF}_w^{\mathsf{fin}}$ with value in NU has at most $J+1$ digits, where*

$$J = \lfloor \log N \rfloor + c$$

with

$$c = \lfloor \log d - \log f_L \rfloor + 1$$

with f_L of Proposition 5.2 on page 16.

Proof. Let $z \in NU$, $z \neq 0$, with its corresponding w-NAF $\boldsymbol{\xi} \in \mathbf{NAF}_w^{\mathsf{fin}}$, and let $j \in \mathbb{N}_0$ be the largest index, such that the digit ξ_j is non-zero. By using Corollary 5.3 on page 19, we conclude that

$$|\tau|^j f_L \leq |z| < Nd.$$

This means

$$j < \log N + \log d - \log f_L,$$

and thus we have

$$j \leq \lfloor \log N + \log d - \log f_L \rfloor \leq \lfloor \log N \rfloor + \lfloor \log d - \log f_L \rfloor + 1.$$

Defining the right hand side of this inequality as J finishes the proof. □

Remark 10.6. For the parameter used in the region of integration in the proof of Theorem 10.1 on page 36 we get

$$\tau^{-J}N = \left|\tau\right|^{\{\log N\}-c}\,\widehat{\theta}(\log N)\,,$$

with the rotation $\widehat{\theta}(x) = e^{-i\theta\lfloor x\rfloor - i\theta c}$. In particular we get $\left|\tau^{-J}N\right| = \mathcal{O}(1)$.

Proof. With $\tau = \left|\tau\right| e^{i\theta}$ and the J of Lemma 10.5 on the preceding page we obtain

$$\tau^{-J}N = \tau^{-\lfloor\log N\rfloor - c}\left|\tau\right|^{\log N} = \left|\tau\right|^{-c-\lfloor\log N\rfloor+\log N} e^{-i\theta(\lfloor\log N\rfloor+c)} = \left|\tau\right|^{\{\log N\}-c}\,\widehat{\theta}(\log N)\,.$$ □

Remark 10.7. Let $\gamma \in \mathbb{R}$ with $\gamma \geq 1$, then

$$\gamma^J = N^{\log\gamma}\gamma^{c-\{\log N\}} = \mathcal{O}\big(N^{\log\gamma}\big)\,.$$

In particular $\left|\tau\right|^{2J} = \mathcal{O}\big(N^2\big)$ and $\left|\tau\right|^{J} = \mathcal{O}(N)$.

Proof. We insert J from Lemma 10.5 on the previous page and obtain

$$\begin{aligned}\gamma^J &= \gamma^{\lfloor\log N\rfloor+c} = \gamma^{\log N}\gamma^{c-\{\log N\}} = \left|\tau\right|^{\log N\log\gamma}\gamma^{c-\{\log N\}}\\ &= N^{\log\gamma}\gamma^{c-\{\log N\}} = \mathcal{O}\big(N^{\log\gamma}\big)\,.\end{aligned}$$ □

Lemma 10.8 (The Main Part)**.** *For* (10.1a) *in the proof of Theorem 10.1 on page 36 we get*

$$\mathcal{M}_\eta(N) = e_w N^2\,\lambda(U)\log N + N^2\,\psi_{\eta,\mathcal{M}}(\log N)$$

with a 1*-periodic function* $\psi_{\eta,\mathcal{M}}$*,*

$$\psi_{\eta,\mathcal{M}}(x) = \lambda(U)\,(c+1-\{x\})\,e_w$$

and

$$e_w = \frac{1}{\left|\tau\right|^{2(w-1)}\Big(\Big(\left|\tau\right|^2-1\Big)\,w+1\Big)}.$$

Proof. We have

$$\mathcal{M}_\eta(N) = \frac{\left|\tau\right|^{2J}}{\lambda(V)}(J+1)\,\lambda(W)\int_{y\in\tau^{-J}NU}\mathrm{d}y.$$

As $\lambda\big(\tau^{-J}NU\big) = \left|\tau\right|^{-2J}N^2\,\lambda(U)$ we obtain

$$\mathcal{M}_\eta(N) = \frac{\lambda(W)}{\lambda(V)}(J+1)N^2\,\lambda(U)\,.$$

By taking $\lambda(W) = \lambda(V)\,e_w$ from (i) of Proposition 9.2 on page 32 and J from Lemma 10.5 on the preceding page we get

$$\mathcal{M}_\eta(N) = N^2\,\lambda(U)\,e_w\,(\lfloor\log N\rfloor + c + 1)\,.$$

Finally, the desired result follows by using $x = \lfloor x\rfloor + \{x\}$. □

Lemma 10.9 (The Zero Part)**.** *For* (10.1b) *in the proof of Theorem 10.1 on page 36 we get*

$$\mathcal{Z}_\eta(N) = 0.$$

Proof. Consider the integral

$$I_j := \int_{y\in\lfloor\tau^{-J}NU\rfloor_{\hexagon,j-w}}\Big(\mathbb{1}_W\Big(\big\{y\tau^{j-w}\big\}_{\mathbb{Z}[\tau]}\Big) - \lambda(W)\Big)\,\mathrm{d}y.$$

We can rewrite the region of integration as

$$\lfloor\tau^{-J}NU\rfloor_{\hexagon,j-w} = \frac{1}{\tau^{j-w}}\,\lfloor\tau^{j-w}\tau^{-J}NU\rfloor_{\hexagon} = \frac{1}{\tau^{j-w}}\bigcup_{z\in T_{j-w}}V_z$$

for some appropriate $T_{j-w}\subseteq\mathbb{Z}[\tau]$. Substituting $x = \tau^{j-w}y,\ \mathrm{d}x = \left|\tau\right|^{2(j-w)}\,\mathrm{d}y$ yields

$$I_j = \frac{1}{\left|\tau\right|^{2(j-w)}}\int_{x\in\bigcup_{z\in T_{j-w}}V_z}\Big(\mathbb{1}_W\Big(\{x\}_{\mathbb{Z}[\tau]}\Big) - \lambda(W)\Big)\,\mathrm{d}x.$$

We split up the integral and eliminate the fractional part $\{x\}_{\mathbb{Z}[\tau]}$ by translation to get

$$I_j = \frac{1}{\left|\tau\right|^{2(j-w)}} \sum_{z \in T_{j-w}} \underbrace{\int_{x \in V} \left(\mathbb{1}_W(x) - \lambda(W)\right) \mathrm{d}x}_{=0}.$$

Thus, for all $j \in \mathbb{N}_0$ we obtain $I_j = 0$, and therefore $\mathcal{Z}_\eta(N) = 0$. □

Lemma 10.10 (The Periodic Part)**.** *For* (10.1c) *in the proof of Theorem 10.1 on page 36 we get*

$$\mathcal{P}_\eta(N) = N^2\, \psi_{\eta,\mathcal{P}}(\log N) + \mathcal{O}\big(N^\delta\big)$$

with a function $\psi_{\eta,\mathcal{P}}$*,*

$$\psi_{\eta,\mathcal{P}}(x) = \frac{\left|\tau\right|^{2(c-\{x\})}}{\lambda(V)} \sum_{j=0}^{\infty} \int_{y \in \left\{\left|\tau\right|^{\{x\}-c}\, \widehat{\theta}(\lfloor x \rfloor) U\right\}_{\hexagon, j-w}} \Big(\mathbb{1}_W\Big(\big\{y\tau^{j-w}\big\}_{\mathbb{Z}[\tau]}\Big) - \lambda(W)\Big)\, \mathrm{d}y,$$

with the rotation $\widehat{\theta}(x) = e^{-i\theta x - i\theta c}$*.*

If there is a $p \in \mathbb{N}$*, such that* $e^{i\theta p} U = U$*, then* $\psi_{\eta,\mathcal{P}}$ *is p-periodic.*

Proof. Consider

$$I_j := \int_{y \in \{\tau^{-J} N U\}_{\hexagon, j-w}} \Big(\mathbb{1}_W\Big(\big\{y\tau^{j-w}\big\}_{\mathbb{Z}[\tau]}\Big) - \lambda(W)\Big)\, \mathrm{d}y.$$

The region of integration satisfies

$$\big\{\tau^{-J} N U\big\}_{\hexagon, j-w} \subseteq \partial\big(\tau^{-J} N U\big)_{\hexagon, j-w} = \frac{1}{\tau^{j-w}} \bigcup_{z \in T_{j-w}} V_z \tag{10.2}$$

for some appropriate $T_{j-w} \subseteq \mathbb{Z}[\tau]$.

We use the triangle inequality and substitute $x = \tau^{j-w} y$, $\mathrm{d}x = \left|\tau\right|^{2(j-w)} \mathrm{d}y$ in the integral to get

$$\left|I_j\right| \leq \frac{1}{\left|\tau\right|^{2(j-w)}} \int_{x \in \bigcup_{z \in T_{j-w}} V_z} \underbrace{\left|\mathbb{1}_W\Big(\{x\}_{\mathbb{Z}[\tau]}\Big) - \lambda(W)\right|}_{\leq 1 + \lambda(W)} \mathrm{d}x.$$

After splitting up the integral and using translation to eliminate the fractional part, we get

$$\left|I_j\right| \leq \frac{1 + \lambda(W)}{\left|\tau\right|^{2(j-w)}} \sum_{z \in T_{j-w}} \int_{x \in V} \mathrm{d}x = \frac{1 + \lambda(W)}{\left|\tau\right|^{2(j-w)}} \lambda(V)\, \#(T_{j-w}).$$

Using $\#\big(\partial(NU)_{\hexagon}\big)_{\hexagon} = \mathcal{O}\big(N^\delta\big)$ as assumed and Equation (10.2) we gain

$$\#(T_{j-w}) = \mathcal{O}\Big(\left|\tau\right|^{(j-w)\delta} \left|\tau^{-J} N\right|^\delta\Big) = \mathcal{O}\Big(\left|\tau\right|^{(j-w)\delta}\Big),$$

because $\left|\tau^{-J} N\right| = \mathcal{O}(1)$, see Remark 10.6 on the preceding page, and thus

$$\left|I_j\right| = \mathcal{O}\Big(\left|\tau\right|^{\delta(j-w) - 2(j-w)}\Big) = \mathcal{O}\Big(\left|\tau\right|^{(\delta-2)j}\Big).$$

Now we want to make the summation in $\mathcal{P}_\eta$ independent from J, so we consider

$$I := \frac{\left|\tau\right|^{2J}}{\lambda(V)} \sum_{j=J+1}^{\infty} I_j$$

Again we use triangle inequality and we calculate the sum to obtain

$$|I| = \mathcal{O}\Big(\left|\tau\right|^{2J}\Big) \sum_{j=J+1}^{\infty} \mathcal{O}\Big(\left|\tau\right|^{(\delta-2)j}\Big) = \mathcal{O}\Big(\left|\tau\right|^{2J} \left|\tau\right|^{(\delta-2)J}\Big) = \mathcal{O}\Big(\left|\tau\right|^{\delta J}\Big).$$

Note that $\mathcal{O}\Big(\left|\tau\right|^J\Big) = \mathcal{O}(N)$, see Remark 10.7 on the facing page, so we obtain $|I| = \mathcal{O}\big(N^\delta\big)$.

Let us look at the growth of

$$\mathcal{P}_\eta(N) = \frac{|\tau|^{2J}}{\lambda(V)} \sum_{j=0}^{J} I_j.$$

We get

$$|\mathcal{P}_\eta(N)| = \mathcal{O}\Big(|\tau|^{2J}\Big) \sum_{j=0}^{J} \mathcal{O}\Big(|\tau|^{(\delta-2)j}\Big) = \mathcal{O}\Big(|\tau|^{2J}\Big) = \mathcal{O}\big(N^2\big)\,,$$

using $\delta < 2$, and, to get the last equality, Remark 10.7 on page 40.

Finally, inserting the result of Remark 10.6 on page 40 for the region of integration, rewriting $|\tau|^{2J}$ according to Remark 10.7 on page 40 and extending the sum to infinity, as above described, yields

$$\begin{aligned}\mathcal{P}_\eta(N) &= \frac{|\tau|^{2J}}{\lambda(V)} \sum_{j=0}^{J} \int_{y \in \{\tau^{-J}NU\}_{\hexagon,j-w}} \Big(\mathbb{1}_W\Big(\big\{y\tau^{j-w}\big\}_{\mathbb{Z}[\tau]}\Big) - \lambda(W)\Big)\,\mathrm{d}y \\ &= N^2 \underbrace{\frac{|\tau|^{2(c-\{\log N\})}}{\lambda(V)} \sum_{j=0}^{\infty} \int_{y \in \big\{|\tau|^{\{\log N\}-c}\,\widehat{\theta}(\lfloor \log N \rfloor)U\big\}_{\hexagon,j-w}} \Big(\mathbb{1}_W\Big(\big\{y\tau^{j-w}\big\}_{\mathbb{Z}[\tau]}\Big) - \lambda(W)\Big)\,\mathrm{d}y}_{=:\psi_{\eta,\mathcal{P}}(\log N)} \\ &\qquad + \mathcal{O}\big(N^\delta\big)\,,\end{aligned}$$

with the rotation $\widehat{\theta}(x) = e^{-i\theta x - i\theta c}$.

Now let

$$e^{i\theta p}U = U \iff e^{-i\theta p}U = e^{-i\theta 0}U.$$

Clearly the region of integration in $\psi_{\eta,\mathcal{P}}(x)$ is p-periodic, since x occurs as $\{x\}$ and $\lfloor x \rfloor$. All other occurrences of x are of the form $\{x\}$, i.e., 1-periodic, so period p is obtained. □

Lemma 10.11 (The Other Part)**.** *For* (10.1d) *in the proof of Theorem 10.1 on page 36 we get*

$$\mathcal{Q}_\eta(N) = N^2 \psi_{\eta,\mathcal{Q}} + \mathcal{O}(N^\alpha \log N) + \mathcal{O}\big(N^\delta\big)\,,$$

with

$$\psi_{\eta,\mathcal{Q}} = \frac{\lambda(U)}{\lambda(V)} \sum_{j=0}^{\infty} \frac{\beta_j}{\lambda(V)}$$

and $\alpha = 2 + \log \rho < 2$*, where* $\rho < 1$ *can be found in Theorem 4.1 on page 11.*

Proof. Consider

$$I_{j,\ell} := \int_{y \in \lfloor \tau^{-J}NU \rfloor_{\hexagon,j-w}} \big(\mathbb{1}_{W_{\eta,\ell}} - \mathbb{1}_W\big)\Big(\big\{y\tau^{j-w}\big\}_{\mathbb{Z}[\tau]}\Big)\,\mathrm{d}y.$$

We can rewrite the region of integration and get

$$\big\lfloor \tau^{-J}NU \big\rfloor_{\hexagon,j-w} = \frac{1}{\tau^{j-w}} \big\lfloor \tau^{j-w}\tau^{-J}NU \big\rfloor_{\hexagon} = \frac{1}{\tau^{j-w}} \bigcup_{z \in T_{j-w}} V_z$$

for some appropriate $T_{j-w} \subseteq \mathbb{Z}[\tau]$, as in the proof of Lemma 10.9 on page 40. Substituting $x = \tau^{j-w}y,\ \mathrm{d}x = |\tau|^{2(j-w)}\,\mathrm{d}y$ yields

$$I_{j,\ell} = \frac{1}{|\tau|^{2(j-w)}} \int_{x \in \bigcup_{z \in T_{j-w}} V_z} \big(\mathbb{1}_{W_{\eta,\ell}} - \mathbb{1}_W\big)\Big(\{x\}_{\mathbb{Z}[\tau]}\Big)\,\mathrm{d}x$$

and further

$$I_{j,\ell} = \frac{1}{|\tau|^{2(j-w)}} \sum_{z \in T_{j-w}} \underbrace{\int_{x \in V} \big(\mathbb{1}_{W_{\eta,\ell}} - \mathbb{1}_W\big)(x)\,\mathrm{d}x}_{=\beta_\ell} = \frac{1}{|\tau|^{2(j-w)}}\,\#(T_{j-w})\,\beta_\ell,$$

by splitting up the integral, using translation to eliminate the fractional part and taking β_ℓ according to (j) of Proposition 9.2 on page 32. From Proposition 8.3 on page 30 we obtain

$$\frac{\#(T_{j-w})}{\left|\tau\right|^{2(j-w)}} = \frac{\left|\tau^{j-w}\tau^{-J}N\right|^2}{\left|\tau\right|^{2(j-w)}}\frac{\lambda(U)}{\lambda(V)} + \mathcal{O}\left(\frac{\left|\tau^{j-w}\tau^{-J}N\right|^\delta}{\left|\tau\right|^{2(j-w)}}\right) = \left|\tau^{-J}N\right|^2\frac{\lambda(U)}{\lambda(V)} + \mathcal{O}\Big(\left|\tau\right|^{(\delta-2)j}\Big),$$

because $\left|\tau^{-J}N\right| = \mathcal{O}(1)$, see Remark 10.6 on page 40.

Now let us have a look at

$$\mathcal{Q}_\eta(N) = \frac{\left|\tau\right|^{2J}}{\lambda(V)}\sum_{j=0}^{J} I_{j,J-j}.$$

Inserting the result above and using $\beta_\ell = \mathcal{O}\big(\rho^\ell\big)$, see (j) of Proposition 9.2 on page 32, yields

$$\mathcal{Q}_\eta(N) = \left|\tau\right|^{2J}\left|\tau^{-J}N\right|^2\frac{\lambda(U)}{\lambda(V)}\sum_{j=0}^{J}\frac{\beta_{J-j}}{\lambda(V)} + \left|\tau\right|^{2J}\sum_{j=0}^{J}\mathcal{O}\Big(\left|\tau\right|^{(\delta-2)j}\Big)\,\mathcal{O}\big(\rho^{J-j}\big)$$

We notice that $\left|\tau\right|^{2J}\left|\tau^{-J}N\right|^2 = N^2$.

Therefore, after reversing the order of the first summation, we obtain

$$\mathcal{Q}_\eta(N) = N^2\frac{\lambda(U)}{\lambda(V)}\sum_{j=0}^{J}\frac{\beta_j}{\lambda(V)} + \left|\tau\right|^{2J}\rho^J\sum_{j=0}^{J}\mathcal{O}\Big(\Big(\rho\left|\tau\right|^{2-\delta}\Big)^{-j}\Big).$$

If $\rho\left|\tau\right|^{2-\delta} \geq 1$, then the second sum is $J\,\mathcal{O}(1)$, otherwise the sum is $\mathcal{O}\Big(\rho^{-J}\left|\tau\right|^{(\delta-2)J}\Big)$. So we obtain

$$\mathcal{Q}_\eta(N) = N^2\frac{\lambda(U)}{\lambda(V)}\sum_{j=0}^{J}\frac{\beta_j}{\lambda(V)} + \mathcal{O}\Big(\left|\tau\right|^{2J}\rho^J J\Big) + \mathcal{O}\Big(\left|\tau\right|^{\delta J}\Big).$$

Using $J = \Theta(\log N)$, see Lemma 10.5 on page 39, Remark 10.7 on page 40, and defining $\alpha = 2 + \log\rho$ yields

$$\mathcal{Q}_\eta(N) = N^2\frac{\lambda(U)}{\lambda(V)}\sum_{j=0}^{J}\frac{\beta_j}{\lambda(V)} + \underbrace{\mathcal{O}\big(N^{2+\log\rho}\log N\big)}_{=\mathcal{O}(N^\alpha\log N)} + \mathcal{O}\big(N^\delta\big).$$

Now consider the first sum. Since $\beta_j = \mathcal{O}\big(\rho^j\big)$, see (j) of Proposition 9.2 on page 32, we obtain

$$N^2\sum_{j=J+1}^{\infty}\beta_j = N^2\,\mathcal{O}\big(\rho^J\big) = \mathcal{O}(N^\alpha).$$

Thus the lemma is proved, because we can extend the sum to infinity. □

Lemma 10.12 (The Small Part)**.** *For* (10.1e) *in the proof of Theorem 10.1 on page 36 we get*

$$\mathcal{S}_\eta(N) = \mathcal{O}(N^\alpha\log N) + \mathcal{O}\big(N^\delta\big)$$

with $\alpha = 2 + \log\rho < 2$ *and* $\rho < 1$ *from Theorem 4.1 on page 11.*

Proof. Consider

$$I_{j,\ell} := \int_{y\in\left\{\tau^{-J}NU\right\}_{\text{⬡},j-w}}\left(\mathbb{1}_{W_\ell} - \mathbb{1}_W\right)\Big(\left\{y\tau^{j-w}\right\}_{\mathbb{Z}[\tau]}\Big)\,\mathrm{d}y.$$

Again, as in the proof of Lemma 10.10 on page 41, the region of integration satisfies

$$\left\{\tau^{-J}NU\right\}_{\text{⬡},j-w} \subseteq \partial\big(\tau^{-J}NU\big)_{\text{⬡},j-w} = \frac{1}{\tau^{j-w}}\bigcup_{z\in T_{j-w}} V_z, \tag{10.3}$$

for some appropriate $T_{j-w} \subseteq \mathbb{Z}[\tau]$.

We substitute $x = \tau^{j-w}y$, $\mathrm{d}x = \left|\tau\right|^{2(j-w)}\,\mathrm{d}y$ in the integral to get

$$\left|I_{j,\ell}\right| = \frac{1}{\left|\tau\right|^{2(j-w)}}\left|\int_{x\in\bigcup_{z\in T_{j-w}} V_z}\left(\mathbb{1}_{W_\ell} - \mathbb{1}_W\right)\Big(\left\{x\right\}_{\mathbb{Z}[\tau]}\Big)\,\mathrm{d}x\right|.$$

Again, after splitting up the integral, using translation to eliminate the fractional part and the triangle inequality, we get

$$\left|I_{j,\ell}\right| \leq \frac{1}{\left|\tau\right|^{2(j-w)}} \sum_{z \in T_{j-w}} \underbrace{\left|\int_{x \in V} (\mathbb{1}_{W_\ell} - \mathbb{1}_W)(x) \,\mathrm{d}x\right|}_{=\left|\beta_\ell\right|} = \frac{1}{\left|\tau\right|^{2(j-w)}} \#(T_{j-w}) \left|\beta_\ell\right|,$$

in which $\left|\beta_\ell\right| = \mathcal{O}\bigl(\rho^\ell\bigr)$ is known from (j) of Proposition 9.2 on page 32. Using $\#\bigl(\partial(NU)_{\hexagon}\bigr)_{\hexagon} = \mathcal{O}\bigl(N^\delta\bigr)$, Remark 10.6 on page 40, and Equation (10.3) we get

$$\#(T_{j-w}) = \mathcal{O}\Bigl(\left|\tau\right|^{(j-w)\delta} \left|\tau^{-J} N\right|^\delta\Bigr) = \mathcal{O}\Bigl(\left|\tau\right|^{\delta(j-w)}\Bigr),$$

because $\left|\tau^{-J} N\right| = \mathcal{O}(1)$. Thus

$$\left|I_{j,\ell}\right| = \mathcal{O}\Bigl(\rho^\ell \left|\tau\right|^{(\delta-2)(j-w)}\Bigr) = \mathcal{O}\Bigl(\rho^\ell \left|\tau\right|^{(\delta-2)j}\Bigr)$$

follows by assembling all together.

Now we are ready to analyse

$$\mathcal{S}_\eta(N) = \frac{\left|\tau\right|^{2J}}{\lambda(V)} \sum_{j=0}^{J} I_{j,J-j}.$$

Inserting the result above yields

$$\left|\mathcal{S}_\eta(N)\right| = \frac{\left|\tau\right|^{2J}}{\lambda(V)} \sum_{j=0}^{J} \mathcal{O}\Bigl(\rho^{J-j} \left|\tau\right|^{(\delta-2)j}\Bigr) = \frac{\rho^J \left|\tau\right|^{2J}}{\lambda(V)} \sum_{j=0}^{J} \mathcal{O}\Bigl(\Bigl(\rho \left|\tau\right|^{2-\delta}\Bigr)^{-j}\Bigr)$$

and thus, by the same argument as in the proof of Lemma 10.11 on page 42,

$$\left|\mathcal{S}_\eta(N)\right| = \rho^J \left|\tau\right|^{2J} \mathcal{O}\Bigl(J + \rho^{-J} \left|\tau\right|^{(\delta-2)J}\Bigr) = \mathcal{O}\Bigl(\rho^J \left|\tau\right|^{2J} J\Bigr) + \mathcal{O}\Bigl(\left|\tau\right|^{\delta J}\Bigr),$$

Finally, using Lemma 10.5 on page 39 and Remark 10.7 on page 40, we obtain

$$\left|\mathcal{S}_\eta(N)\right| = \mathcal{O}(N^\alpha \log N) + \mathcal{O}\bigl(N^\delta\bigr)$$

with $\alpha = 2 + \log \rho$. Since $\rho < 1$, we have $\alpha < 2$. □

Lemma 10.13 (The Fractional Cells Part). *For* (10.1f) *in the proof of Theorem 10.1 on page 36 we get*

$$\mathcal{F}_\eta(N) = \mathcal{O}\bigl(N^\delta \log N\bigr)$$

Proof. For the regions of integration in $\mathcal{F}_\eta$ we obtain

$$NU \setminus \lfloor NU \rceil_{\hexagon} \subseteq \lceil NU \rceil_{\hexagon} \setminus \lfloor NU \rfloor_{\hexagon} = \partial(NU)_{\hexagon} = \bigcup_{z \in T} V_z$$

and

$$\lfloor NU \rceil_{\hexagon} \setminus NU \subseteq \lceil NU \rceil_{\hexagon} \setminus \lfloor NU \rfloor_{\hexagon} = \partial(NU)_{\hexagon} = \bigcup_{z \in T} V_z$$

for some appropriate $T \subseteq \mathbb{Z}[\tau]$ using Proposition 8.2 on page 28. Thus we get

$$\left|\mathcal{F}_\eta(N)\right| \leq \frac{2}{\lambda(V)} \sum_{j=0}^{J} \int_{x \in \bigcup_{z \in T} V_z} \mathbb{1}_{W_j}\left(\left\{\frac{x}{\tau^{j+w}}\right\}_{\mathbb{Z}[\tau]}\right) \mathrm{d}x \leq \frac{2}{\lambda(V)} \sum_{j=0}^{J} \sum_{z \in T} \int_{x \in V_z} \mathrm{d}x,$$

in which the indicator function was replaced by 1. Dealing with the sums and the integral, which is $\mathcal{O}(1)$, we obtain

$$\left|\mathcal{F}_\eta(N)\right| = (J+1) \#T \, \mathcal{O}(1).$$

Since $J = \mathcal{O}(\log N)$, see Lemma 10.5 on page 39, and $\#T = \mathcal{O}\bigl(N^\delta\bigr)$, the desired result follows. □

Lemma 10.14. *If the ψ_η from Theorem 10.1 on page 36 is p-periodic, then ψ_η is also continuous.*

Proof. There are two possible parts of ψ_η, where an discontinuity could occur. The first is $\{x\}$ for an $x \in \mathbb{Z}$, the second is building $\{\dots\}_{\hexagon,j-w}$ in the region of integration in $\psi_{\eta,\mathcal{P}}$.

The latter is no problem, i.e., no discontinuity, since

$$\begin{aligned}\int_{y\in\left\{\left|\tau\right|^{\{x\}-c}\,\widehat{\theta}(\lfloor x\rfloor)U\right\}_{\hexagon,j-w}} &\left(\mathbb{1}_W\left(\left\{y\tau^{j-w}\right\}_{\mathbb{Z}[\tau]}\right)-\lambda(W)\right)\,\mathrm{d}y \\ &= \int_{y\in\left|\tau\right|^{\{x\}-c}\,\widehat{\theta}(\lfloor x\rfloor)U} \left(\mathbb{1}_W\left(\left\{y\tau^{j-w}\right\}_{\mathbb{Z}[\tau]}\right)-\lambda(W)\right)\,\mathrm{d}y,\end{aligned}$$

because the integral of the region $\left\lfloor\left|\tau\right|^{\{x\}-c}\,\widehat{\theta}(\lfloor x\rfloor)\,U\right\rfloor_{\hexagon,j-w}$ is zero, see proof of Lemma 10.9 on page 40.

Now we deal with the continuity for $x \in \mathbb{Z}$. Let $m \in x + p\mathbb{Z}$, let $M = \left|\tau\right|^m$, and consider

$$Z_\eta(M) - Z_\eta(M-1)\,.$$

For an appropriate $a \in \mathbb{R}$ we get

$$Z_\eta(M) = aM^2\log M + M^2\,\psi_\eta(\log M) + \mathcal{O}(M^\alpha \log M) + \mathcal{O}\big(M^\delta \log M\big)\,,$$

and thus

$$Z_\eta(M) = aM^2 m + M^2\,\underbrace{\psi_\eta(m)}_{=\psi_\eta(x)} + \mathcal{O}(M^\alpha m) + \mathcal{O}\big(M^\delta m\big)\,.$$

Further we obtain

$$\begin{aligned}Z_\eta(M-1) = a\,(M-1)^2\log(M-1) &+ (M-1)^2\,\psi_\eta(\log(M-1)) \\ &+ \mathcal{O}((M-1)^\alpha \log(M-1)) + \mathcal{O}\Big((M-1)^\delta \log(M-1)\Big)\,,\end{aligned}$$

and thus, using the abbreviation $L = \log\big(1 - M^{-1}\big)$ and $\delta \geq 1$,

$$Z_\eta(M-1) = aM^2 m + M^2\,\underbrace{\psi_\eta(m+L)}_{=\psi_\eta(x+L)} + \mathcal{O}(M^\alpha m) + \mathcal{O}\big(M^\delta m\big)\,.$$

Therefore we obtain

$$\frac{Z_\eta(M) - Z_\eta(M-1)}{M^2} = \psi_\eta(x) - \psi_\eta(x+L) + \mathcal{O}\big(M^{\alpha-2}m\big) + \mathcal{O}\big(M^{\delta-2}m\big)\,.$$

Since $\#(MU \setminus (M-1)\,U)_\hexagon$ is clearly an upper bound for the number of w-NAFs with values in $MU \setminus (M-1)\,U$ and each of these w-NAFs has less than $\lfloor \log M\rfloor + c$ digits, see Lemma 10.5 on page 39, we obtain

$$Z_\eta(M) - Z_\eta(M-1) \leq \#(MU \setminus (M-1)\,U)_\hexagon\,(m+c)\,.$$

Using (b) of Proposition 8.3 on page 30 yields then

$$Z_\eta(M) - Z_\eta(M-1) = \mathcal{O}\big(M^\delta m\big)\,.$$

Therefore we get

$$\psi_\eta(x) - \psi_\eta(x+L) = \mathcal{O}\big(M^{\delta-2}m\big) + \mathcal{O}\big(M^{\alpha-2}m\big) + \mathcal{O}\big(M^{\delta-2}m\big)\,.$$

Taking the limit $m \to \infty$ in steps of p, thus L tends to 0, and using $\alpha < 2$ and $\delta < 2$ yields

$$\psi_\eta(x) - \lim_{\varepsilon\to 0^-}\,\psi_\eta(x+\varepsilon) = 0,$$

i.e., ψ_η is continuous for $x \in \mathbb{Z}$. □

Acknowledgements

We thank Stephan Wagner for contributing the proof of Lemma 4.2 on page 12.

References

[1] F. Aurenhammer, *Voronoi diagrams — a survey of a fundamental geometric data structure*, ACM Comput. Surv. **23** (1991), no. 3, 345–405. (Cited on page 5.)

[2] R. Avanzi, C. Heuberger, and H. Prodinger, *Arithmetic of supersingular koblitz curves in characteristic three*, Tech. Report 2010-8, Graz University of Technology, 2010, `http://www.math.tugraz.at/fosp/pdfs/tugraz_0166.pdf`, also available as Cryptology ePrint Archive, Report 2010/436, `http://eprint.iacr.org/`. (Cited on page 4.)

[3] M. Barnsley, *Fractals everywhere*, Academic Press, Inc, 1988. (Cited on page 24.)

[4] I. Blake, K. Murty, and G. Xu, *Nonadjacent radix-τ expansions of integers in Euclidean imaginary quadratic number fields*, Canad. J. Math. **60** (2008), no. 6, 1267–1282. (Cited on pages 2 and 21.)

[5] I. F. Blake, V. K. Murty, and G. Xu, *A note on window τ-NAF algorithm*, Inform. Process. Lett. **95** (2005), 496–502. (Cited on pages 2 and 21.)

[6] I. F. Blake, V. Kumar Murty, and G. Xu, *Efficient algorithms for Koblitz curves over fields of characteristic three*, J. Discrete Algorithms **3** (2005), no. 1, 113–124. (Cited on pages 2, 8, and 21.)

[7] H. Delange, *Sur la fonction sommatoire de la fonction "somme des chiffres"*, Enseignement Math. (2) **21** (1975), 31–47. (Cited on pages 3 and 37.)

[8] G. A. Edgar, *Measure, topology, and fractal geometry*, second ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2008. (Cited on pages 10, 24, and 27.)

[9] D. M. Gordon, *A survey of fast exponentiation methods*, J. Algorithms **27** (1998), 129–146. (Cited on page 3.)

[10] P. J. Grabner, C. Heuberger, and H. Prodinger, *Distribution results for low-weight binary representations for pairs of integers*, Theoret. Comput. Sci. **319** (2004), 307–331. (Cited on page 3.)

[11] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics. A foundation for computer science*, second ed., Addison-Wesley, 1994. (Cited on pages 14 and 36.)

[12] C. Heuberger and H. Prodinger, *Analysis of alternative digit sets for nonadjacent representations*, Monatsh. Math. **147** (2006), 219–248. (Cited on pages 2 and 25.)

[13] H.-K. Hwang, *On convergence rates in the central limit theorems for combinatorial structures*, European J. Combin. **19** (1998), 329–343. (Cited on page 13.)

[14] 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. (Cited on page 2.)

[15] ———, *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. (Cited on pages 1, 2, 21, and 25.)

[16] D. W. Matula, *Basic digit sets for radix representation*, J. Assoc. Comput. Mach. **29** (1982), no. 4, 1131–1143. (Cited on pages 13 and 21.)

[17] J. A. Muir and D. R. Stinson, *Alternative digit sets for nonadjacent representations*, Selected areas in cryptography, Lecture Notes in Comput. Sci., vol. 3006, Springer, Berlin, 2004, pp. 306–319. (Cited on page 11.)

[18] G. W. Reitwiesner, *Binary arithmetic*, Advances in computers, vol. 1, Academic Press, New York, 1960, pp. 231–308. (Cited on page 2.)

[19] 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. (Cited on pages 2 and 8.)

[20] ———, *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249. (Cited on pages 2, 8, and 21.)

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

E-mail address: `clemens.heuberger@tugraz.at`

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

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