# NONADJACENT RADIX-$\tau$ EXPANSIONS OF INTEGERS IN EUCLIDEAN IMAGINARY QUADRATIC NUMBER FIELDS

IAN F. BLAKE, V. KUMAR MURTY, AND GUANGWU XU

Abstract. In the seminal papers [6, 7], Koblitz curves were proposed for cryptographic use. For fast operations on these curves, these papers also initiated a study of the radix-$\tau$ expansion of integers in the number fields $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-7})$. The (window) nonadjacent form of $\tau$-expansion of integers in $\mathbb{Q}(\sqrt{-7})$ was first investigated in [11]. For integers in $\mathbb{Q}(\sqrt{-3})$, the nonadjacent form and the window nonadjacent form of the $\tau$-expansion were studied in [7, 3]. These are used for efficient point multiplications on Koblitz curves. In this paper, we complete the picture by producing the (window) nonadjacent radix-$\tau$ expansions for integers in all Euclidean imaginary quadratic number fields. A wider range of applications is expected.

## 1. Introduction

In many applications, it is convenient to express an integer $n$ in a binary form

$$n = \sum_{i=0}^{t} b_i 2^i, b_i \in \{0, 1\}.$$

The window nonadjacent form (NAF) generalizes the binary expansion and is used to speed up elliptic curve point multiplication. In this form, given a positive integer $w$, every integer $n$ can be represented as

$$n = \sum_{i=0}^{t} b_i 2^i,$$

with

(1) $b_i \in \{-2^{w-1} + 1, -2^{w-1} + 3, \cdots, -1, 1, \cdots, 2^{w-1} - 3, 2^{w-1} - 1\} \cup \{0\}$, for each $i = 0, 1, \cdots, t$, and
(2) any segment of coefficients $\{b_i, b_{i+1}, \ldots, b_{i+w-1}\}$ contains at most one nonzero element.

This is called the nonadjacent from with window width $w$, see [1, 5, 9].

In his seminal paper [6], Koblitz proposed the use of curves

$$y^2 + xy = x^3 + ax^2 + 1,$$

over $\mathbb{F}_{2^m}$ in cryptography, where $a = 0$ or 1. For fast computation on such curves, Koblitz also considered the base-$\tau$ expansion of elements in the ring $\mathbb{Z}[\tau]$ with $\tau = \dfrac{1 + \sqrt{-7}}{2}$. The celebrated window $\tau$ NAF method for $\mathbb{Z}[\tau]$ was proposed by

2000 *Mathematics Subject Classification.* Primary 11A63, 11R04, 11Y16, 11Y40, 14G50.

*Key words and phrases.* Algebraic integer, radix expression, window nonadjacent expansion, algorithm, point multiplication of elliptic curves, cryptography.

Solinas [11] which improves the point multiplication on these curves dramatically. By this method, each $a + b\tau \in \mathbb{Z}[\tau]$ can be written as

$$a + b\tau = \sum_{i=1}^{s} b_i \tau^i,$$

where

(1) each nonzero coefficient $b_i$ is an element with the least norm in the ( mod $\tau^w$ ) class of some odd number $r$ satisfying $|r| < 2^{w-1}$,
(2) any segment of coefficients $\{b_i, b_{i+1}, \ldots, b_{i+w-1}\}$ contains at most one nonzero element.

In [2], we defined a "wider" window $\tau$ NAF, and proved its existence.

In [7], Koblitz introduced another family of elliptic curves, this family being defined over $\mathbb{F}_{3^m}$:

$$y^2 = x^3 - x - (-1)^a$$

with $a = 0$ or 1, and applied them to digital signatures. It is noticed that these curves are also useful in the ID-based cryptosystem, see [4]. The fast point multiplications on these curves using (non-adjacent) base-$\tau$ expansion of elements in the ring $\mathbb{Z}[\tau]$ with $\tau = \dfrac{3 + \sqrt{-3}}{2}$ was also suggested in [7]. The more general window $\tau$ NAF in this case was discussed in [3], and greater efficiency was achieved.

In this paper, the results mentioned above are extended to all Euclidean imaginary quadratic number fields. More specifically, let $R$ be the ring of integers of such a field, and fix a nonunit, nonzero element $\tau \in R$ with the least norm. It is proved that for any integer $w > 2$, a suitable finite set $C \subset R$ can be chosen so that every element $r \in R$ can be *uniquely* written as

$$r = \sum_{i=0}^{t} c_i \tau^i, \tag{1.1}$$

and

(1) $c_i \in C$ for $i = 0, 1, \ldots, t$;
(2) any segment of coefficients $\{c_i, c_{i+1}, \ldots, c_{i+w-1}\}$ contains at most one nonzero element.

Equation (1.1) is the so called radix-$\tau$ width $w$ NAF (nonadjacent form) for $r$.

For the cases that $w = 2$, we still have the desired radix-$\tau$ width 2 NAF and the uniqueness hold for fields $\mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-11})$. In fact, for $\mathbb{Q}(\sqrt{-3})$ the existence and uniqueness of radix-$\tau$ (width 2) NAF for $\mathbb{Q}(\sqrt{-3})$ is a theorem of Koblitz, see[7].

The case of $w = 1$ is also of particular interest. In this case equation (1.1) is simply the usual radix-$\tau$ form of the integer $r$. Our results show that every integer in $R$ has a radix-$\tau$ form with coefficients taken from the set of units. The form is aslo shown to be unique for the field $\mathbb{Q}(\sqrt{-11})$. It is noted for the field $\mathbb{Q}(\sqrt{-7})$, the radix-$\tau$ form was first considered by Koblitz in [6].

We first develop criteria for the divisibility of (algebraic) integers by a power of $\tau$ and these, in turn, will be used to characterize the class of integers modulo $\tau^w$. The set $C$ of coefficients of the above representation will then be easily determined.

This is a problem of independent interest, but it is obviously useful in the fast point multiplication for a large family of CM-curves where $\tau$ corresponds to an endomorphism that is efficiently computable. We can derive algorithms for obtaining radix-$\tau$ width $w$ NAF for any integer.

The termination of our methods relies on the norm reducing property and the fact that the ring of integers contains finitely many units. The ring of integers of a Euclidean imaginary quadratic field satisfies these requirements.

It is noted that the minimality of the norm of $\tau$ is not necessary. As we can see in the discussion, the results are easier to establish for $\tau$ with bigger norm.

There are five Euclidean imaginary quadratic number fields:

$$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}),$$

and their corresponding rings of integers are

$$\mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\sqrt{-2}], \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right], \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right], \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]. \tag{1.2}$$

Without loss of generality, we fix a nonunit, nonzero $\tau$ with the least norm for each ring:

| Ring of integers | $\mathbb{Z}[\sqrt{-1}]$ | $\mathbb{Z}[\sqrt{-2}]$ | $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ | $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ | $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ |
|---|---|---|---|---|---|
| $\tau$ | $1+\sqrt{-1}$ | $\sqrt{-2}$ | $\frac{3+\sqrt{-3}}{2}$ | $\frac{1+\sqrt{-7}}{2}$ | $\frac{1+\sqrt{-11}}{2}$ |

The organization of this paper is as follows. In §2, the divisibility of elements by a power of $\tau$ is discussed for each of the rings listed in (1.2). The existence and uniqueness of the radix-$\tau$ NAF for these rings of integers is given in §3. In §4, two algorithms are presented for obtaining the radix-$\tau$ NAF for integers in $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-11})$. An example of fast arithmetic on some Koblitz curves using the radix-$\tau$ NAF is also included. The last section contains some comments and a summary of the paper.

Throughout this paper, for a real number $x$, we denote by $\lfloor x \rfloor$ the largest integer less than or equal to $x$, and $\lceil x \rceil$ the smallest integer greater than or equal to $x$.

## 2. Divisibility by a power of $\tau$

In this section, the problem of $\tau^k | a + b\tau$ is considered. It is translated to properties in terms of $a$ and $b$ and operations in $\mathbb{Z}$. This provides an easier way to determine the congruence classes modulo $\tau^w$.

The first three results are for the rings $\mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, and they are similar in pattern.

**Lemma 2.1.** *Let $\tau = 1 + \sqrt{-1}$. If $k$ is a positive integer and $a + b\tau \in \mathbb{Z}[\tau](= \mathbb{Z}[\sqrt{-1}])$, then*

(1)
$$\tau^k = 2^{\lfloor \frac{k}{2} \rfloor} \exp\left(\frac{\lfloor \frac{k}{2} \rfloor \pi \sqrt{-1}}{2}\right) \tau^{\lceil \frac{k}{2} \rceil - \lfloor \frac{k}{2} \rfloor}$$

(2)
$$\tau^k | a + b\tau \iff 2^{\lceil \frac{k}{2} \rceil} | a \text{ and } 2^{\lfloor \frac{k}{2} \rfloor} | b.$$

*Proof.* (1) This follows since $\tau = \sqrt{2} \exp\left(\frac{\pi}{4}\sqrt{-1}\right)$.

(2) Since $\exp\left(\frac{\lfloor \frac{k}{2} \rfloor \pi \sqrt{-1}}{2}\right)$ is a unit in $\mathbb{Z}[\tau]$, $\tau^k$ is associated to $2^{\lfloor \frac{k}{2} \rfloor} \tau^{\lceil \frac{k}{2} \rceil - \lfloor \frac{k}{2} \rfloor}$. The argument then follows from the facts that

- if $k$ is even,
$$a + b\tau = 2^{\lfloor \frac{k}{2} \rfloor} \left(\frac{a}{2^{\lceil \frac{k}{2} \rceil}} + \frac{b}{2^{\lfloor \frac{k}{2} \rfloor}} \tau\right);$$
- if $k$ is odd,
$$a + b\tau = 2^{\lfloor \frac{k}{2} \rfloor} \tau \left(\frac{a+b}{2^{\lfloor \frac{k}{2} \rfloor}} + \frac{-a}{2^{\lceil \frac{k}{2} \rceil}} \tau\right).$$

□

**Lemma 2.2.** *Let $\tau = \sqrt{-2}$. If $k$ is a positive integer and $a + b\tau \in \mathbb{Z}[\tau]$, then*
$$\tau^k | a + b\tau \iff 2^{\lceil \frac{k}{2} \rceil} | a \text{ and } 2^{\lfloor \frac{k}{2} \rfloor} | b.$$

*Proof.* The proof is straightforward and is omitted. □

**Lemma 2.3.** *Let $\tau = \frac{3+\sqrt{-3}}{2}$. If $k$ is a positive integer and $a + b\tau \in \mathbb{Z}[\tau](= \mathbb{Z}[\frac{1+\sqrt{-3}}{2}])$, then*

(1)
$$\tau^k = 3^{\lfloor \frac{k}{2} \rfloor} \exp\left(\frac{\lfloor \frac{k}{2} \rfloor \pi \sqrt{-1}}{3}\right) \tau^{\lceil \frac{k}{2} \rceil - \lfloor \frac{k}{2} \rfloor}$$

(2)
$$\tau^k | a + b\tau \iff 3^{\lceil \frac{k}{2} \rceil} | a \text{ and } 3^{\lfloor \frac{k}{2} \rfloor} | b.$$

*Proof.* Similar to the proof of lemma 2.1. Also see [3]. □

For the rings $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$, another approach has to be developed. We start with some facts in $p$-adic analysis.

Let $p$ be a prime in $\mathbb{Z}$ and $m$ an integer such that $p \not| m$. Consider a quadratic polynomial
$$f(x) = x^2 + mx + p.$$
Let $a_0 = 0$, then $f(a_0) \equiv 0 \bmod p$, $f'(a_0) \not\equiv 0 \bmod p$. Using the Hensel procedure, one finds $a_j$ with $0 \leq a_j < p, j = 1, 2, \ldots, k-1$, such that the integer
$$t_k = a_0 + a_1 p + a_2 p^2 + \cdots + a_{k-1} p^{k-1},$$

satisfies

$$f(t_k) \equiv 0 \bmod p^k. \tag{2.1}$$

The $t_k$ is called *the kth p-adic approximation* of a zero of $f(x)$.

The coefficient $a_{k-1}$ can be obtained through (see [8, 10])

$$a_{k-1}m + \frac{f(t_{k-1})}{p^{k-1}} \equiv 0 \bmod p. \tag{2.2}$$

Since $p|t_{k-1}$, (2.2) is equivalent to

$$(m + t_{k-1})(t_{k-1} + a_{k-1}p^{k-1}) + p \equiv 0 \bmod p^k.$$

Therefore, one gets the following relation

$$t_k \equiv -(m + t_{k-1})^{-1}p \bmod p^k \tag{2.3}$$

**Theorem 2.1.** *Let $p$ be a prime in $\mathbb{Z}$, $m$ an integer which is not divisible by $p$. Let $\alpha$ be a root of*

$$x^2 + mx + p = 0.$$

*Then for any positive integer $k$,*

$$\alpha^k | a + b\alpha \text{ in } \mathbb{Z}[\alpha] \iff a + bt_k \equiv 0 \bmod p^k.$$

*Proof.* We proceed by induction. It is obvious that this is a true statement when $k = 1$, i.e.,

$$\alpha | a + b\alpha \text{ in } \mathbb{Z}[\alpha] \iff p|a.$$

Let $k > 1$. Assume that the statement is true for each integer less than $k$. It suffices to consider the case that $p|a$. Observe that

$$\frac{a + b\alpha}{\alpha} = \left(b - \frac{ma}{p}\right) + \left(-\frac{a}{p}\right)\alpha.$$

So

$$\begin{aligned}
\alpha^k | a + b\alpha \text{ in } \mathbb{Z}[\alpha] &\iff \alpha^{k-1} | \left(b - \frac{ma}{p}\right) + \left(-\frac{a}{p}\right)\alpha \text{ in } \mathbb{Z}[\alpha] \\
&\iff b - \frac{ma}{p} - \frac{a}{p}t_{k-1} \equiv 0 \bmod p^{k-1} \\
&\iff bp - am - at_{k-1} \equiv 0 \bmod p^k \\
&\iff a + b(m + t_{k-1})^{-1}(-p) \equiv 0 \bmod p^k \\
&\iff a + bt_k \equiv 0 \bmod p^k.
\end{aligned}$$

□

Since $\tau = \frac{1+\sqrt{-7}}{2}$ is a root of the equation

$$x^2 - x + 2 = 0,$$

applying theorem 2.1, one gets immediately:

**Lemma 2.4.** *Let $\tau = \dfrac{1 + \sqrt{-7}}{2}$ and $k$ a positive integer. Let $t_k$ be the kth 2-adic approximation of $\tau$. Then for $a + b\tau \in \mathbb{Z}[\tau]$,*

$$\tau^k | a + b\tau \iff a + bt_k \equiv 0 \bmod 2^k.$$

**Remark 2.1.** *The above lemma is due to Solinas* [11]*, but the proof there uses Lucas sequences instead of 2-adic analysis.*

Similarly we get the next lemma by considering a root of

$$x^2 - x + 3 = 0.$$

**Lemma 2.5.** *Let* $\tau = \dfrac{1+\sqrt{-11}}{2}$ *and* $k$ *a positive integer. Let* $t_k$ *be the* $k$*th* 3*-adic approximation of* $\tau$*. Then for* $a + b\tau \in \mathbb{Z}[\tau]$*,*

$$\tau^k | a + b\tau \iff a + bt_k \equiv 0 \bmod 3^k.$$

## 3. Window radix-$\tau$ expansion

We begin with a general discussion and come back to each of the individual fields later.

Let $F$ be a Euclidean imaginary quadratic number field and $O_F$ be the ring of integers of $F$. For $k \in F$, as an element of $\mathbb{C}$, the *norm* of $k$ denoted by $N(k)$, is simply the product of $k$ with its complex conjugate. In particular, the norm of a nonzero element is positive.

Let $\alpha \in O_F$ and $N(\alpha) > 1$. Let $C \subset O_F$ and $w$ be a positive integer. An element $k \in O_F$ is said to have a *radix-$\alpha$ width $w$ NAF (nonadjacent form) with respect to $C$* if

$$k = \sum_{i=0}^{n} u_i \alpha^i,$$

where

(1) for each $i = 0, 1, \ldots, n$, $u_i \in C$;
(2) any $w$ consecutive coefficients $u_i, u_{i+1}, \cdots, u_{i+w-1}$ contains at most one nonzero element.

We will call a radix-$\alpha$ width 1 NAF a *radix-$\alpha$ form*.

Now suppose $N(\alpha^w) \geq 12$. Let

$$R = \{k \in O_F : \alpha \not| k\}.$$

Let $C_1, C_2, \ldots, C_t$ be the congruence classes of $R$ modulo $\alpha^w$. It is noted that all units of $O_F$ are in $R$ and no class $C_i$ contains more than two units. For each $1 \leq i \leq t$, if $C_i$ contains a unit, then denote it by $c_i$. If $C_i$ does not contain a unit, fix an element $c_i$ of $C_i$ with $N(c_i) < N(\alpha^w)$ (this can be done since the ring is Euclidean). Set

$$C = \{c_1, c_2, \ldots, c_t\} \cup \{0\}. \tag{3.1}$$

The first result of this section is general.

**Theorem 3.1.** *Every element* $k \in O_F$ *has a unique radix-$\alpha$ width $w$ NAF with respect to $C$ defined by (3.1).*

*Proof. Existence:* We prove the existence by induction on the norm.

As $F$ is an imaginary quadratic field, elements of norm 1 are necessarily units, and so they are in $C$ already hence have the width $w$ NAF.

Let $m$ be a positive integer. Assume that all elements of norm less than $m$ have the width $w$ NAF. Let $k \in O_F$ and $N(k) = m$.

There are $q \in O_F$ and $c_{i_0} \in C$ such that

$$k = q\alpha^w + c_{i_0}.$$

It suffices to show that $q$ has a width $w$ NAF. This is true since $N(q) < N(k)$. In fact, $N(k) > 1$ implies that $|k| \geq \sqrt{2}$. So

$$\begin{aligned} \frac{|q|}{|k|} &= \frac{|k - c_{i_0}|}{|\alpha|^w |k|} \\ &\leq \frac{1}{|\alpha|^w} + \frac{1}{|k|} \\ &\leq \frac{1}{2\sqrt{3}} + \frac{1}{\sqrt{2}} \\ &< 1. \end{aligned}$$

*Uniqueness:* Suppose that $k \in O_F$ has two width $w$ NAFs with coefficients in $C$,

$$\begin{aligned} k &= \sum_{i=1}^{n} u_i \alpha^i + u_0 \\ &= \sum_{i=1}^{n'} v_i \alpha^i + v_0. \end{aligned}$$

We may assume that $u_0 \neq 0$. This means that $\alpha \not| k$, so $v_0 \neq 0$. These force that $u_1 = \cdots = u_{w-1} = 0$ and $v_1 = \cdots = v_{w-1} = 0$. Therefore $u_0$ and $v_0$ are in the same class modulo $\alpha^w$ and hence they are equal.

The rest follows from a standard induction argument.

□

It is remarked that the uniqueness of the width $w$ NAF is based on the fact that no distinct coefficients can be in the same class modulo $\alpha^w$. More on this will be seen in the discussion that follows.

Theorem 3.1 can be refined further for each specific Euclidean imaginary quadratic number field.

**Gaussian Integers**

In this case, let $\tau = 1 + \sqrt{-1}$ and consider the radix-$\tau$ window NAF for elements in $\mathbb{Z}[\sqrt{-1}](= \mathbb{Z}[\tau])$.

By lemma 2.1, we can get a simple description of the congruence relation modulo $\tau^w$. Consider the elements of $\mathbb{Z}[\tau]$ that are not divisible by $\tau$. Then the set of representatives of the classes is

$$R = \{x + y\tau : 0 \leq x \leq 2^{\lceil \frac{w}{2} \rceil} - 1, 0 \leq y \leq \ldots, 2^{\lfloor \frac{w}{2} \rfloor} - 1 \text{ and } 2 \not| x\}.$$

Let $w \geq 3$. The units of $\mathbb{Z}[\sqrt{-1}]$ are $1, -1(\equiv 2^{\lceil \frac{w}{2} \rceil} - 1 \bmod \tau^w), \sqrt{-1}(\equiv (2^{\lceil \frac{w}{2} \rceil} - 1) + \tau \bmod \tau^w)$ and $-\sqrt{-1}(\equiv 1 + (2^{\lfloor \frac{w}{2} \rfloor} - 1)\tau \bmod \tau^w)$. They belong to four different

classes modulo $\tau^w$. We choose, for each $x+y\tau \in R$, one element $\tilde{x}+\tilde{y}\tau$ from the class of $x+y\tau$ such that

$$N(\tilde{x}+\tilde{y}\tau) < N(\tau^w) = 2^w.$$

The coefficients of width $w$ NAF consists of zero, units and other $\tilde{x}+\tilde{y}\tau$'s which are not divisible by $\tau$. To be more specific, the set of coefficients is:

$$C = \{0, 1, -1, \sqrt{-1}, -\sqrt{-1}\} \cup \{\tilde{x}+\tilde{y}\tau : x+y\tau \in R, N(\tilde{x}+\tilde{y}\tau) > 1\}. \tag{3.2}$$

**Theorem 3.2.** *If $w > 2$, then every element $a+b\tau \in \mathbb{Z}[\tau]$ has a unique width $w$ NAF with respect to $C$ defined by (3.2).*

*Proof.* If $w > 3$, then $N(\tau^w) > 12$ and it becomes a special case of theorem 3.1.

If $w = 3$. According to the proof of theorem 3.1, we only need to show that if $k \in \mathbb{Z}[\sqrt{-1}] \setminus C$, and if for some $q \in \mathbb{Z}[\sqrt{-1}], c \in C$,

$$k = q\tau^3 + c$$

implies that $N(q) < N(k)$.

If $N(k) = 2$, then $k$ is associated to $\tau$, and the result follows. Otherwise since $\mathbb{Z}[\sqrt{-1}]$ contains no elements of norm 3, so $N(k) \geq 4$. Thus

$$\frac{|q|}{|k|} = \frac{|k-c|}{|\tau|^3|k|} \leq \frac{1}{2^{\frac{3}{2}}} + \frac{1}{|k|} < 1.$$

Since $N(\tau^3) = 8$, distinct units can not be in the same (mod $\tau^3$) class. This also means that distinct elements in $C$ can not be in the same class. Thus the uniqueness follows. □

Theorem 3.2 can not be generalized to the cases of $w \leq 2$. For example, take $w = 2$. If we choose one element from each class of modulo $\tau^2 = 2\sqrt{-1}$, then the set of coefficients would be something like $C = \{0, 1, \sqrt{-1}\}$. But we claim that $-1$ can not have a radix-$\tau$ width 2 NAF with respect to such $C$. If there were width 2 NAF of -1

$$-1 = \sum_{i=0}^{n} u_i \tau^i,$$

then we would have $u_0 = 1, u_1 = 0, u_2 = \sqrt{-1}, u_3 = 0, u_4 = \sqrt{-1}, \cdots$, and $n$ would not be finite.

If we can take more than one element from each class modulo $\tau^w$, width $w$ NAF can be still produced, even though not necessarily unique. The main ideas of the proof follow along the same lines as that of theorem 3.1 and theorem 3.2, and so will be omitted.

**Theorem 3.3.** (1) *Every element $a+b\tau \in \mathbb{Z}[\tau]$ has a radix-$\tau$ width 2 NAF with respect to $C = \{0, 1, -1, \sqrt{-1}, -\sqrt{-1}\}$.*

(2) *Every element $a+b\tau \in \mathbb{Z}[\tau]$ has a radix-$\tau$ form with respect to $C = \{0, 1, -1\}$.*

*Proof.* (1) The main ideas of the proof of the result can be traced from that of theorem 3.1 and theorem 3.2. The detail will be omitted.

(2) In this part, induction will be used on the norm. Consider a general term $a+b\tau \in \mathbb{Z}[\tau]$.

If $N(a+b\tau) \leq 1$, then the argument is true. In fact, when $a+b\tau \notin \{0,1,-1\}$, $a+b\tau = \pm\sqrt{-1} = \pm(\tau-1)$.

Otherwise, there are several cases to consider.

If $a$ is even, then $a+b\tau$ is divisible by $\tau$ and the argument is reduced to $\dfrac{a+b\tau}{\tau}$ whose norm is smaller.

If $a$ is odd, then $(a\pm 1)+b\tau$ is divisible by $\tau$. Notice that

$$N((a\pm 1)+b\tau) - N(a+b\tau) = 1 \pm 2(a+b).$$

Without loss of generality, we may assume that $a+b \geq 0$. Thus

$$N((a-1)+b\tau) - N(a+b\tau) \leq 1.$$

This implies that

$$N(\frac{(a-1)+b\tau}{\tau}) < N(a+b\tau)$$

since $N(a+b\tau) > 1$. So $\dfrac{(a-1)+b\tau}{\tau}$ has a radix-$\tau$ form with respect to $\{0,1,-1\}$.

Therefore

$$a+b\tau = \left(\frac{(a-1)+b\tau}{\tau}\right)\tau + 1,$$

has a radix-$\tau$ form.

□

As an example, we see that $3 = -\tau^4 - 1 = -\sqrt{-1}\tau^2 + 1$, so the radix-$\tau$ width 2 NAF in the above theorem is not unique.

A counterexample to the uniqueness of part 2 of the above theorem is $\tau^4 + 1 = \tau^3 - \tau - 1$.

**Integers in $\mathbb{Q}(\sqrt{-2})$**

Let $\tau = \sqrt{-2}$. By lemma 2.2, the set of representatives of the classes of elements not divisible by $\tau$ can be

$$R = \{x+y\tau : 0 \leq x \leq 2^{\lceil \frac{w}{2} \rceil} - 1, 0 \leq y \leq \ldots, 2^{\lfloor \frac{w}{2} \rfloor} - 1 \text{ and } 2 \not| x\}.$$

Similar to the previous argument, for each $x+y\tau \in R$, choose $\tilde{x}+\tilde{y}\tau$ from the class of $x+y\tau$ such that

$$N(\tilde{x}+\tilde{y}\tau) < N(\tau^w) = 2^w.$$

Set

$$C = \{0,1,-1\} \cup \{\tilde{x}+\tilde{y}\tau : x+y\tau \in R, N(\tilde{x}+\tilde{y}\tau) > 1\}. \tag{3.3}$$

**Theorem 3.4.** *If $w > 2$, then every element $a+b\tau \in \mathbb{Z}[\tau]$ has a unique width $w$ NAF with respect to $C$ defined by (3.3).*

*Proof.* As in the proof of theorem 3.2, we only consider the case of $w = 3$.

Let $k \in \mathbb{Z}[\sqrt{-2}]$ and $N(k) > 1$.

If $N(k) = 2$, then $k$ is associated to $\tau$.

If $N(k) = 3$, then $k \in \{1+\tau, 1-\tau, -1+\tau, -1-\tau\}$. Notice that $1+\tau \equiv 1-\tau \bmod \tau^3$ and $-1+\tau \equiv -1-\tau \bmod \tau^3$.

It can be checked that there is no other element in the class of $1+\tau$ with norm less than $N(\tau^3)=8$, so one of $1+\tau$ and $1-\tau$ must be in $C$. Without loss of generality we may assume that $1+\tau \in C$. Then

$$1-\tau = (1+\tau)+\tau^3.$$

A similar discussion applies to $-1+\tau$ and $-1-\tau$.

If $N(k) \geq 4$, then the proof is similar to that of theorem 3.2. □

Since $-1$ does have a width 2 NAF with respect to $\{0,1\}$, theorem 3.4 can not be generalized to cases of $w \leq 2$. But we can relax the set of coefficients to get the following theorem.

**Theorem 3.5.** (1) *Every element $a+b\tau \in \mathbb{Z}[\sqrt{-2}]$ has a radix-$\tau$ width 2 NAF with respect to $C=\{0,1,-1,1+\tau\}$.*

(2) *Every element $a+b\tau \in \mathbb{Z}[\sqrt{-2}]$ has a radix-$\tau$ form with respect to $C=\{0,1,-1\}$.*

We omit the proof as its ideas can be found in the proofs of previous results.

Noticed that $3=\tau^4-1=-\tau^2+1$, and we see that the forms satisfying theorem 3.5 are not unique.

**Eisenstein Integers**

Let $\tau=\dfrac{3+\sqrt{-3}}{2}$, and set

$$R=\{x+y\tau : 0 \leq x \leq 3^{\lceil \frac{w}{2} \rceil}-1, 0 \leq y \leq 3^{\lfloor \frac{w}{2} \rfloor}-1 \text{ and } 3 \not| x\},$$

then $R$ consists of the representatives of the (mod $\tau^w$) classes of those elements not divisible by $\tau$. Once again, we take $\tilde{x}+\tilde{y}\tau$ to be an element in the class of $x+y\tau$ with norm less then $N(\tau^w)=3^w$.

Note that the set of units of $\mathbb{Z}[\tau]$ is $U_6=\{\omega \in \mathbb{C} : \omega^6=1\}$.

Let

$$C=\{0\} \cup U_6 \cup \{\tilde{x}+\tilde{y}\tau : x+y\tau \in R, N(\tilde{x}+\tilde{y}\tau)>1\}. \tag{3.4}$$

The next theorem generalizes a theorem of Koblitz[6] from $w=2$ to any $w>1$ and its existence part was first established in [3]. For the uniqueness part, we need to notice that any two distinct coefficients are not congruent modulo $\tau^w$.

**Theorem 3.6.** *If $w>1$, then every element $a+b\tau \in \mathbb{Z}[\tau]$ has a unique width $w$ NAF with respect to $C$ defined by (3.4).*

In [3], we have already showed that $2-\tau$ can not have a radix-$\tau$ form with respect to $\{0,1,-1\}$. But we have the following

**Theorem 3.7.** *Every element $a+b\tau \in \mathbb{Z}[\tau]$ has a radix-$\tau$ form with respect to $\{0\} \cup U_6$.*

**Integers in $\mathbb{Q}(\sqrt{-7})$**

Let $\tau=\dfrac{1+\sqrt{-7}}{2}$ and $w$ a positive integer. By lemma 2.4, the (mod $\tau^w$) classes of elements not divisible by $\tau$ can be represented by $1,3,\ldots,2^w-1$.. The units of $\mathbb{Z}[\tau]$ are 1 and -1.

Let $c_i \equiv i$ and $N(c_i) < N(\tau^w) = 2^w$. Set

$$C = \{0, 1, -1\} \cup \{c_i : 1 < i < 2^w - 1\}. \tag{3.5}$$

The next theorem generalizes results of Solinas [11] and its existence part was established in [2].

**Theorem 3.8.** *If $w > 1$, then every element $a + b\tau \in \mathbb{Z}[\tau]$ has a unique width $w$ NAF with respect to $C$ defined by (3.5).*

We can verify that $-1$ does not have a radix-$\tau$ form with respect to $\{0, 1\}$. But the following theorem of Koblitz [6] gives the radix-$\tau$ form for every integer in $\mathbb{Q}(\sqrt{-7})$ with -1 added to the coefficient set.

**Theorem 3.9.** *(Koblitz) Every element $a + b\tau \in \mathbb{Z}[\tau]$ has a radix-$\tau$ form with respect to $C = \{0, 1, -1\}$.*

Notice that $\tau - 1 = \tau^2 + 1$, so the radix-$\tau$ form is not unique.

**Integers in $\mathbb{Q}(\sqrt{-11})$**

Let $\tau = \dfrac{1 + \sqrt{-11}}{2}$ and $w$ a positive integer. There are only two units in $\mathbb{Z}[\tau]$: 1, -1. They are not congruent modulo $\tau^w$.

Let $t_w$ be the $w$th 3-adic approximation of $\tau$ defined in section 2, then $3|t_w$. By lemma 2.5, $1, 2, 4, 5, \ldots, 3^w - 1$ are representatives of classes modulo $\tau^w$ of elements in $\mathbb{Z}[\tau]$ which are not divisible by $\tau$.

Let $c_i \equiv i \bmod \tau^w$ and $N(c_i) < N(\tau^w) = 3^w$. Set

$$C = \{0, 1, -1\} \cup \{c_i : 1 < i < 3^w - 1 \text{ and } 3 \not| i\}. \tag{3.6}$$

**Theorem 3.10.** *Let $w$ be any positive integer, then every element $a + b\tau \in \mathbb{Z}[\tau]$ has a unique width $w$ NAF with respect to $C$ defined by (3.6).*

*Proof.* If $w > 2$, then the theorem follows from theorem 3.1. If $w = 2$, consider an element $k \in \mathbb{Z}[\tau]$ with $N(k) > 1$. Since $\mathbb{Z}[\tau]$ contains no element of norm 2, so $N(k) \geq 3$. We will show that if

$$k = q\tau^2 + c$$

for some $q \in \mathbb{Z}[\tau]$ and $c \in C$, then $N(q) < N(k)$ and the induction applies. In fact

$$\frac{|q|}{|k|} = \frac{|k - c|}{|\alpha|^2 |k|} \leq \frac{1}{|\alpha|^2} + \frac{1}{|k|} < 1.$$

Next we consider the case of $w = 1$. In this case, $C = \{0, 1, -1\}$. If $1 < N(k) < 9$, then it is easily checked that $k \in \{\pm(1 - \tau), \pm(-\tau^2 + \tau - 1), \pm(1 + \tau), \pm(-\tau^2 - 1)\}$.

If $N(k) \geq 9$, write

$$k = q\tau + c$$

with $q \in \mathbb{Z}[\tau]$ and $c \in C$, then similar to the argument before, we have $N(q) < N(k)$. The result follows by induction.

Finally the uniqueness for the cases of $w \leq 2$ is due to the fact that no two elements in $C$ are in the same class modulo $\tau^w$.

□

The next table summarizes the results of this section.

| Fields | $\tau$ | Radix $\tau$ width $w$ NAF | Uniqueness of width $w$ NAF |
|---|---|---|---|
| $\mathbb{Q}(\sqrt{-1})$ | $1+\sqrt{-1}$ | Yes | $w>2$ |
| $\mathbb{Q}(\sqrt{-2})$ | $\sqrt{-2}$ | Yes | $w>2$ |
| $\mathbb{Q}(\sqrt{-3})$ | $\frac{3+\sqrt{-3}}{2}$ | Yes | $w>1$ |
| $\mathbb{Q}(\sqrt{-7})$ | $\frac{1+\sqrt{-7}}{2}$ | Yes | $w>1$ |
| $\mathbb{Q}(\sqrt{-11})$ | $\frac{1+\sqrt{-11}}{2}$ | Yes | all $w$ |

## 4. Algorithms and Applications

In the first part of this section, two algorithms for computing the width $w$ NAF of integers in $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-11})$ are presented. Other cases are similar. One can actually find much of the corresponding algorithms for integers in $\mathbb{Q}(\sqrt{-7})$ in [11] and integers in $\mathbb{Q}(\sqrt{-3})$ in [7, 3].

In the second part of this section, some Koblitz curves over $\mathbb{F}_{5^m}$ are proposed. The width $w$ NAF in $\mathbb{Q}(\sqrt{-11})$ will be used in the fast point multiplication on those curves.

### Algorithms

The first algorithm concerns width $w$ NAF of Gaussian integers. In this case, $\tau = 1+\sqrt{-1}$.

Let $w$ be a positive integer. If $w \geq 3$, then the four units $\pm 1, \pm\sqrt{-1}$ belong to different classes modulo $\tau^w$. The representatives of the (mod $\tau^w$) classes of elements not divisible by $\tau$ are

$$x + y\tau : x = 1, 3, \ldots, 2^{\lceil \frac{w}{2} \rceil} - 1, y = 0, 1, 2, \ldots, 2^{\lfloor \frac{w}{2} \rfloor} - 1. \tag{4.1}$$

If we take, for each $x + y\tau$ in (4.1), one element $\hat{x} + \hat{y}\tau$ from the class of $x + y\tau$ with the least norm and set

$$C = \{\hat{x} + \hat{y}\tau; x + y\tau \text{ as in (4.1)}\},$$

then $C$ contains $\pm 1, \pm\sqrt{-1}$. If $w < 3$, set

$$C = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}.$$

The next algorithm provides an efficient way of producing radix-$\tau$ width $w$ NAF for any element in $\mathbb{Z}[\sqrt{-1}]$ with nonzero coefficients in $C$.

**Algorithm 4.1.** (Radix -$\tau$ width $w$ NAF Method)
`INPUT:` an element $\rho = r_0 + r_1\tau$ of $\mathbb{Z}[\sqrt{-1}]$
`OUTPUT:` S, the array of coefficients of width $w$ NAF for $\rho$.

$S \leftarrow <>$
`While` $N(r_0 + r_1\tau) \geq 1$
  `If` $2 \not| r_0$ `then`
    $x \leftarrow r_0 \bmod 2^{\lceil \frac{w}{2} \rceil}$
    $y \leftarrow r_1 \bmod 2^{\lfloor \frac{w}{2} \rfloor}$
    $r_0 \leftarrow r_0 - \hat{x}$

```
    r1 ← r1 − ŷ
    prepend x̂ + ŷτ to S
  Else
    prepend 0 to S
  Endif
  t ← r0
  r0 ← r0 + r1
  r1 ← −t/2
Endwhile
If  r0 = 0 and r1 = 0  then
  prepend r0 + r1τ to S
Endif

Return S
```

It is noted that when $w = 1$ the above algorithm outputs radix-$\tau$ form with respect to $\{0, 1, -1, \sqrt{-1}, -\sqrt{-1}\}$. One can easily formulate an algorithm for the radix-$\tau$ form of a Gaussian integer with respect to $\{0, 1, -1\}$ based on the proof of part 2 of theorem 3.3.

The second algorithm considers the width $w$ NAF for integers in $\mathbb{Q}(\sqrt{-11})$. In this case, $\tau = \dfrac{1+\sqrt{-11}}{2}$.

Let $w$ be a positive integer and $t_w$ the $w$th $p$-adic approximation of $\tau$. We list the first eight $t_w$s in the next table.

| $w$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $t_w$ | 0 | 3 | 12 | 66 | 228 | 228 | 1686 | 1686 |

Recall that lemma 2.5 claims that for $a + b\tau \in \mathbb{Z}[\tau]$,

$$\tau^w | a + b\tau \iff a + bt_w \equiv 0 \bmod 3^w,$$

therefore $1, 2, 4, 5, \ldots, 3^w - 1$ are representatives of classes modulo $\tau^w$ of elements not divisible by $\tau$.

For each $i$ such that $1 \le i < 3^w$ and $3 \not| i$, let $a_i + b_i\tau$ be an element in the ( mod $\tau^w$ ) class of $i$ with the least norm, and set

$$C = \{a_i + b_i\tau : 1 \le i < 3^w \text{ and } 3 \not| i\}.$$

It is noted that the units of $\mathbb{Z}[\tau]$ are $\pm 1$ and they are both in $C$.

An algorithm that outputs radix-$\tau$ width $w$ NAF for any integer in $\mathbb{Q}(\sqrt{-11})$ with nonzero coefficients in $C$ is as follows:

**Algorithm 4.2.** (Radix -$\tau$ width $w$ NAF Method)
INPUT: an element $\rho = r_0 + r_1\tau$ of $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$
OUTPUT: S, the array of coefficients of width $w$ NAF for $\rho$.

```
S ←<>
While  r0 ≠ 0 or r1 ≠ 0
```

```
  If  3 ∤ r_0  then
    u ← r_0 + r_1 t_w mod 3^w
    r_0 ← r_0 − a_u
    r_1 ← r_1 − b_u
    prepend a_u + b_u τ to S
  Else
    prepend 0 to S
  Endif
  t ← r_0 / 3
  r_0 ← t + r_1
  r_1 ← −t
Endwhile

Return S
```

**Applications**

The radix-$\tau$ width $w$ NAFs in $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-7})$ have been used in the efficient point multiplications of two families of Koblitz curves, namely

$$K(2,a,m): y^2+xy=x^3+ax^2+1/\mathbb{F}_{2^m}, \text{ where } a\in\{0,1\},$$

and

$$K(3,a,m): y^2=x^3-x-(-1)^a/\mathbb{F}_{3^m}, \text{ where } a\in\{0,1\}.$$

See [6, 7, 11, 2, 3].

Here we give an example of using radix-$\tau$ width $w$ NAF in $\mathbb{Q}(\sqrt{-11})$ to the point multiplication of the following Koblitz curves

$$K_1(5,a,m): y^2=x^3+x-(-1)^a/\mathbb{F}_{5^m}, \text{ where } a\in\{0,1\},$$

and

$$K_2(5,a,m): y^2=x^3-x-(-1)^a 2/\mathbb{F}_{5^m}, \text{ where } a\in\{0,1\}.$$

For simplicity, we consider the family of curves

$$K_2(5,1,m): y^2=x^3-x+2/\mathbb{F}_{5^m}.$$

Firstly, it is noted that the Frobenius map

$$\begin{aligned}\tau \quad : \quad & K_2(5,1,1)\to K_2(5,1,1)\\ & (x,y)\mapsto (x^5,y^5)\end{aligned}$$

extends to $K_2(5,1,m)$ for any $m>1$. The characteristic polynomial of $\tau$ is

$$X^2-3X+5.$$

Therefore $\tau$ is identified as $\frac{3+\sqrt{-11}}{2}$. Also note that the operation of $\tau$ can be efficiently implemented.

Secondly, in practice the number $m$ should be chosen so that $\#K_2(5,1,m)$ is a product of a small number and a large prime. As the number $\#K_2(5,1,m)$ can be easily computed using the zeta function, it is checked that $\#K_2(5,1,m)=3p_m$ where $p_m$ is a prime number, for $m=167,227,311$.

Finally, for any $P\in K_2(5,1,m)$ and positive integer $n$, an efficient computation of the point mulitplication $nP$ can be outlined as the follows:

(1) Compute $a+b\tau$ such that $n \equiv a+b\tau \pmod{\tau^m-1}$. Since $(\tau^m-1)P = \mathcal{O}$, we have $nP = (a+b\tau)P$.
(2) Since $N(\tau^w) = 5^w > 12$ if $w > 1$, by theorem 3.1, $a+b\tau$ has a width $w$ radix-$\tau$ NAF:
$$a + b\tau = \sum_{i=0}^{s} c_i \tau^{k_i},$$
with $c_i \in C$ and $k_i - k_{i-1} \geq w$, where $C$ is given by (3.1).
(3) Precompute $Q_c = cP$ for each $c \in C$.
(4) The point multiplication $nP$ is then
$$(a+b\tau)P = \tau^{k_1}(\tau^{k_2-k_1}(\cdots(\tau^{k_s-k_{s-1}}Q_{c_s} + Q_{c_{s-1}}) + \cdots + Q_{c_1}) + Q_{c_0}.$$

## 5. Conclusion

In this paper, the radix-$\tau$ width $w$ NAF is established for every integer in a Euclidean imaginary quadratic number field. These forms are unique provided $w > 2$ (in some fields, this can be true even $w = 2$ or 1). Algorithms for computing these forms are presented, and applications to efficient computation of point multiplication on some Koblitz curves are exemplified. This is a continuation and completion of the work of Koblitz [6, 7], Solinas [11] and ours [2, 3].

## References

1. I. Blake, G. Seroussi and N. Smart, Elliptic Curves in Cryptography, Cambridge University Press, 1999.
2. I. Blake, V. K. Murty and G. Xu, A note on window $\tau$-NAF algorithm, submitted, 2004.
3. I. Blake, V. K. Murty and G. Xu, Efficient algorithms for Koblitz curves over fields of characteristic three, *Journal of Discrete Algorithm*, **3**(2005) 113-124.
4. D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, *Advances in Cryptology, Crypt'01*, LNCS 2139 2001, 213–239.
5. D. Hankerson, A. Menezes and S. Vanstone Guide to Elliptic Curve Cryptography, Springer-Verlag New York, 2003.
6. N. Koblitz, CM-curves with good cryptographic properties, *Advances in Cryptology-CRYPTO '91*, LNCS **576**, 1992, 279-287.
7. N. Koblitz, An elliptic curves implementation of the finite field digital signature algorithm, *Advances in Cryptology-CRYPTO '98*, LNCS **1462**, 1998, 327-337.
8. N. Koblitz, $p$-adic Numbers, $p$-adic Analysis, and Zeta-Functions, GTM 58, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1984.
9. J. A. Muir, D. R. Stinson, Minimality and Other Properties of the Width-w Nonadjacent Form, *preprint*
10. M. R. Murty, Introduction to $p$-Adic Analytic Number Theory, AMS/IP Studies in Advanced Mathematics, 27, American Math. Society, Providence, RI, International Press, 2002.
11. J. Solinas, Efficient arithmetic on Koblitz curves, *Designs, Codes and Cryptography*, **19** (2000), 195-249.

Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada, M5S 3G4
*E-mail address*: ifblake@comm.utoronto.ca

Department of Mathematics, University of Toronto, Toronto, Ontario, Canada, M5S 3G3
*E-mail address*: murty@math.toronto.edu

Ganita Lab, University of Toronto at Mississauga, Mississauga, Ontario, Canada, L5L 1C6
*E-mail address*: gxu@comm.utoronto.ca