Canad. J. Math. Vol. **60** (6), 2008 pp. 1267–1282

Nonadjacent Radix-τ Expansions of Integers in Euclidean Imaginary Quadratic Number Fields

Ian F. Blake, V. Kumar Murty, and Guangwu Xu

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

1 Introduction

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

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

The window nonadjacent form (NAF) generalizes the binary expansion and is used in cryptographic computations, especially 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

- $b_i \in \{-2^{w-1}+1, -2^{w-1}+3, \ldots, -1, 1, \ldots, 2^{w-1}-3, 2^{w-1}-1\} \cup \{0\}$, for each $i = 0, 1, \cdots, t$,
- 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 form with window width w [1, 5, 10].

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

$$K(2, a, m) : y^2 + xy = x^3 + ax^2 + 1,$$

Received by the editors December 21, 2005.
AMS subject classification: Primary: 11A63; secondary: 11R04, 11Y16, 11Y40, 14G50.
Keywords: algebraic integer, radix expression, window nonadjacent expansion, algorithm, point multiplication of elliptic curves, cryptography.
©Canadian Mathematical Society 2008.

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

over $\mathbb{F}_{2^m}$, where $a = 0$ or 1. These curves are now known as *Koblitz curves*. For fast computation on such curves, Koblitz also considered the base-τ expansion of elements in the ring $\mathbb{Z}[\tau]$ with τ the Frobenius endomorphism of $K(2, a, 1)$, which can be identified as $\frac{1+\sqrt{-7}}{2}$. Meier and Staffelbach showed how to improve point multiplication on Koblitz curves [9].

Müller [11] considered the Frobenius endomorphisms Φ of elliptic curves over small fields of characterisic two and devloped radix-Φ expansions for elements in $\mathbb{Z}[\Phi]$. Smart generalized these further to small fields of odd characteristic [13]. These radix-Φ expansions were used to obtain more efficient point multiplication algorithms.

The celebrated window τ NAF method for $\mathbb{Z}[\tau]$ which improves the point multiplication on Koblitz curves dramatically was proposed by Solinas [14]. 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

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

Given a point P on a Koblitz curve and an integer n, there is a reduction procedure for getting $a + b\tau$ such that $nP = (a + b\tau)P$. Therefore the point multiplication nP can be done much faster using the above sparse form of $a + b\tau$. In [2] we defined a "wider" window τ NAF, and proved its existence .

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

$$K(3, a, m) : y^2 = x^3 - x - (-1)^a$$

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

In this paper, the results of [2, 3, 6, 14] 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

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

with

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

- $c_i \in C$ for $i = 0, 1, \ldots, t$,
- 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-τ width w NAF (nonadjacent form) for r.

For the cases that $w = 2$, we still have the desired radix-τ 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-τ (width 2) NAF for $\mathbb{Q}(\sqrt{-3})$ is a theorem of Koblitz [7].

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

We first develop criteria for the divisibility of (algebraic) integers by a power of τ and these, in turn, will be used to characterize the class of integers modulo τ^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 τ corresponds to an endomorphism that is efficiently computable. We can derive algorithms for obtaining radix-τ width w NAF for any integer.

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

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

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

Ring of integers	$\mathbb{Z}[\sqrt{-1}]$	$\mathbb{Z}[\sqrt{-2}]$	$\mathbb{Z}\big[\frac{1+\sqrt{-3}}{2}\big]$	$\mathbb{Z}\big[\frac{1+\sqrt{-7}}{2}\big]$	$\mathbb{Z}\big[\frac{1+\sqrt{-11}}{2}\big]$
τ	$1+\sqrt{-1}$	$\sqrt{-2}$	$\frac{3+\sqrt{-3}}{2}$	$\frac{1+\sqrt{-7}}{2}$	$\frac{1+\sqrt{-11}}{2}$

The organization of this paper is as follows. In §2, the divisibility of elements by a power of τ is discussed for each of the rings listed in (1.2). The existence and uniqueness of the radix-τ NAF for these rings of integers is given in §3. In §4, two algorithms are presented for obtaining the radix-τ 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-τ 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.

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

2 Divisibility by a Power of τ

In this section, the problem of $\tau^k \mid a + b\tau$ 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 τ^w. The results in this section will be used later in determining the coefficients of the radix-τ expansions.

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*

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

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

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

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

$$a + b\tau = \begin{cases} 2^{\lfloor \frac{k}{2} \rfloor} \Big(\dfrac{a}{2^{\lceil \frac{k}{2} \rceil}} + \dfrac{b}{2^{\lfloor \frac{k}{2} \rfloor}} \tau \Big) & \text{if } k \text{ is even,} \\ \Big(\dfrac{a+b}{2^{\lfloor \frac{k}{2} \rfloor}} + \dfrac{-a}{2^{\lceil \frac{k}{2} \rceil}} \tau \Big) & \text{if } k \text{ is odd.} \end{cases}$$

■

Lemma 2.2 *Let $\tau = \sqrt{-2}$. If k is a positive integer and $a + b\tau \in \mathbb{Z}[\tau]$, then*

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

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*

(i) $\tau^k = 3^{\lfloor \frac{k}{2} \rfloor} \exp\Big(\dfrac{\lfloor \frac{k}{2} \rfloor \pi \sqrt{-1}}{3} \Big) \tau^{\lceil \frac{k}{2} \rceil - \lfloor \frac{k}{2} \rfloor}$,

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

Proof Similar to the proof of Lemma 2.1. See also [3]. ■

For the rings $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$, another approach must 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 $p \nmid m$. 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 $0 \le a_j < p$, $j = 1, 2, \ldots, k-1$, such that the integer $t_k = a_0 + a_1 p + a_2 p^2 + \cdots + a_{k-1} p^{k-1}$, satisfies

$$f(t_k) \equiv 0 \bmod p^k.$$

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

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

The coefficient a_{k-1} can be obtained through (see [8, 12])

$$a_{k-1}m + \frac{f(t_{k-1})}{p^{k-1}} \equiv 0 \bmod p. \tag{2.1}$$

Since $p \mid t_{k-1}$, (2.1) 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

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

Theorem 2.4 *Let p be a prime in $\mathbb{Z}$, and m an integer which is not divisible by p. Let α be a root of $x^2 + mx + p = 0$. Then for any positive integer k,*

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

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

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

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

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

So

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

■

Since $\tau = \frac{1+\sqrt{-7}}{2}$ is a root of the equation $x^2 - x + 2 = 0$, applying Theorem 2.4 one immediately gets the following.

Lemma 2.5 *Let $\tau = \frac{1+\sqrt{-7}}{2}$ and k a positive integer. Let t_k be the k-th 2-adic approximation of τ. Then for $a + b\tau \in \mathbb{Z}[\tau]$,*

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

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

Remark 2.6. The above lemma is due to Solinas [14], 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 2.7 *Let $\tau = \frac{1+\sqrt{-11}}{2}$ and k a positive integer. Let t_k be the k-th 3-adic approximation of τ. 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-τ 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-α width w NAF (nonadjacent form) with respect to C* if $k = \sum_{i=0}^{n} u_i \alpha^i$, where

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

We will call a radix-α width 1 NAF a *radix-α 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 α^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-α width w NAF with respect to C defined by* (3.1)*, for $N(\alpha^w) \geq 12$.*

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 they have the width w NAF.

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

If $\alpha \,|\, k$, then $N(k\alpha^{-1}) < m$. By induction, $k\alpha^{-1}$ has the width w NAF. Multiplying this NAF by α, we get a width w NAF for k.

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

If $\alpha \nmid k$, by the Euclidean division, there are $q \in O_F$ and non-zero $c_{i_0} \in C$ 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

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

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

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

We may assume that $u_0 \neq 0$. This means that $\alpha \nmid k$, 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 α^w and hence they are equal.

The rest follows from a standard induction argument. ∎

Remark 3.2. (i) Since we consider Euclidean imaginary fields, our choice of coefficient set C is natural, *i.e.,* the elements are remainders with norm less than $N(\alpha^w)$ and all units are included. It is remarked that one should be careful in selecting the coefficient set for radix-α width w NAFs. For example, let α be a root of $x^2 - 3x + 5 = 0$. Let $w = 2$. If we choose

$$C = \left\{ i \in \mathbb{Z} : -\frac{5^2 - 1}{2} \leq i \leq \frac{5^2 - 1}{2}, \text{ and } 5 \nmid i \right\},$$

then it can be easily checked that element $1 + \alpha$ does not have a radix-α width 2 NAF with respect to this C. Some discussions related to this can be found in [2].

(ii) A radix-α width w NAF of $k \in \mathbb{Z}[\alpha]$ might not be obtainable by using the results in [11,13] and considering radix-α^w expansion, (*i.e.,* a polynomial in α^w with coefficients from a complete set of reminders modulo $N(\alpha^w)$), since $\mathbb{Z}[\alpha]$ is usually larger than $\mathbb{Z}[\alpha^w]$. The above example also shows that $1 + \alpha$ does not have a radix-α^2 expansion with respect to

$$C = \left\{ i \in \mathbb{Z} : -\frac{5^2 - 1}{2} \leq i \leq \frac{5^2 - 1}{2} \right\}.$$

Theorem 3.1 can be refined further for each specific Euclidean imaginary quadratic number field. The cases of $N(\tau^w) < 12$ are considered.

3.1 Gaussian Integers

In this case, let $\tau = 1 + \sqrt{-1}$ and consider the radix-τ 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 τ^w. Consider the elements of $\mathbb{Z}[\tau]$ that are not divisible by τ. Then the set of representatives of the classes is

$$R = \{x + y\tau : 0 \leq x \leq 2^{\lceil \frac{w}{2} \rceil} - 1, 0 \leq y \leq \ldots, 2^{\lfloor \frac{w}{2} \rfloor} - 1 \text{ and } 2 \nmid x\}.$$

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

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 τ^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 τ. 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 3.3 *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 $w = 3$, then according to the proof of Theorem 3.1, we only need to show that for $k \in \mathbb{Z}[\sqrt{-1}] \setminus C$ the norm decreases during the expansion. This means that if for some $q \in \mathbb{Z}[\sqrt{-1}]$ and $c \in C$ one has $k = q\tau^3 + c$, then this implies that $N(q) < N(k)$.

If $N(k) = 2$, then k is associated to τ, 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 cannot be in the same (mod τ^3) class. This also means that distinct elements in C cannot be in the same class. Thus the uniqueness follows. ∎

Theorem 3.3 cannot 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 cannot have a radix-τ width 2 NAF with respect to such C. If there were a width 2 NAF of -1

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

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

If we can take more than one element from each class modulo τ^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 3.3, and so will be omitted.

Theorem 3.4 (i) *Every element $a + b\tau \in \mathbb{Z}[\tau]$ has a radix-τ width 2 NAF with respect to $C = \{0, 1, -1, \sqrt{-1}, -\sqrt{-1}\}$.*

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

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

Proof (i) The main ideas of the proof of the result can be traced from that of Theorem 3.1 and Theorem 3.3. The details will be omitted.

(ii) 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 $a + b\tau \notin \{0, 1, -1\}$, then $a + b\tau = \pm\sqrt{-1} = \pm(\tau - 1)$.

Otherwise, there are several cases to consider.

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

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

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

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

Therefore

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

has a radix-τ 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.

An example that shows the radix-τ of part (ii) of the theorem need not be unique is $\tau^4 + 1 = \tau^3 - \tau - 1$.

3.2 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 τ can be taken as

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

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 3.5 *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).

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

Proof As in the proof of Theorem 3.3, 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 τ.

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 3.3. ■

Since -1 does not have a width 2 NAF with respect to $\{0, 1\}$, Theorem 3.5 can not be generalized to cases of $w \leq 2$. But we can relax the set of coefficients to get the following theorem.

Theorem 3.6 (i) *Every element $a+b\tau \in \mathbb{Z}[\sqrt{-2}]$ has a radix-τ width 2 NAF with respect to $C = \{0, 1, -1, 1+\tau\}$.*

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

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

Note that $3 = \tau^4 - 1 = -\tau^2 + 1$, and we see that the forms satisfying Theorem 3.6 are not unique.

3.3 Eisenstein Integers

Let $\tau = \frac{3+\sqrt{-3}}{2}$, 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 τ^w) classes of those elements not divisible by τ. 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 τ^w.

Theorem 3.7 *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).

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

Theorem 3.8 *Every element $a+b\tau \in \mathbb{Z}[\tau]$ has a radix-τ form with respect to $\{0\} \cup U_6$.*

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

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

Let $\tau = \frac{1+\sqrt{-7}}{2}$ and w a positive integer. By Lemma 2.5, the (mod τ^w) classes of elements not divisible by τ 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 [14]; its existence part was established in [2].

Theorem 3.9 *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-τ form with respect to $\{0, 1\}$. But the following theorem of Koblitz [6] gives the radix-τ form for every integer in $\mathbb{Q}(\sqrt{-7})$ with -1 added to the coefficient set.

Theorem 3.10 **(Koblitz)** *Every element $a+b\tau \in \mathbb{Z}[\tau]$ has a radix-τ form with respect to $C = \{0, 1, -1\}$.*

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

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

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

Let t_w be the w-th 3-adic approximation of τ defined in §2. Then $3 \mid t_w$. By Lemma 2.7, $1, 2, 4, 5, \ldots, 3^w - 1$ are representatives of classes modulo τ^w of elements in $\mathbb{Z}[\tau]$ which are not divisible by τ.

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

$$C = \{0, 1, -1\} \cup \{c_i : 1 < i < 3^w - 1 \text{ and } 3 \nmid i\}. \tag{3.6}$$

Theorem 3.11 *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 previous argument, 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 τ^w. ■

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

The next table summarizes the results of this section.

Fields	τ	Radix τ 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 find similar corresponding algorithms for integers in $\mathbb{Q}(\sqrt{-7})$ in [14] and integers in $\mathbb{Q}(\sqrt{-3})$ in [3, 7].

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.

4.1 Algorithms

Algorithm 4.1 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 τ^w. The representatives of the (mod τ^w) classes of elements not divisible by τ 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, for each $x + y\tau$ in (4.1), we take 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 $C = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$. This algorithm provides an efficient way of producing radix-τ width w NAF for any element in $\mathbb{Z}[\sqrt{-1}]$ with nonzero coefficients in C.

It is noted that when $w = 1$, the algorithm outputs radix-τ form with respect to $\{0, 1, -1, \sqrt{-1}, -\sqrt{-1}\}$. One can easily formulate an algorithm for the radix-τ form of a Gaussian integer with respect to $\{0, 1, -1\}$ based on the proof of part (ii) of Theorem 3.4.

Algorithm 4.2 considers the width w NAF for integers in $\mathbb{Q}(\sqrt{-11})$. In this case, $\tau = \frac{1+\sqrt{-11}}{2}$.

Let w be a positive integer and t_w the w-th 3-adic approximation of τ. We list the first eight t_w's in the next table.

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

Algorithm 4.1 Radix -τ 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 ρ.

```
S ←<>
While N(r0 + r1τ) ≥ 1
  If 2 ∤ r0 then
    x ← r0 mod 2^⌈w/2⌉
    y ← r1 mod 2^⌊w/2⌋
    r0 ← r0 − x̂
    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
```

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

Recall that Lemma 2.7 shows that for $a + b\tau \in \mathbb{Z}[\tau]$,

$$\tau^w \mid a + b\tau \iff a + bt_w \equiv 0 \bmod 3^w.$$

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

For each i such that $1 \le i < 3^w$ and $3 \nmid i$, let $a_i + b_i\tau$ be an element in the (mod τ^w) class of i with the least norm, and set

$$C = \{a_i + b_i\tau : 1 \le i < 3^w \text{ and } 3 \mid i\}.$$

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

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

We can also derive width w NAF for those τ which are not of minimal norm. For example, let

$$\tau = \frac{3 + \sqrt{-11}}{2}.$$

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

Algorithm 4.2 Radix -τ 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 ρ.

$S \leftarrow <>$
While $r_0 \neq 0$ or $r_1 \neq 0$
  If $3 \nmid r_0$ then
    $u \leftarrow r_0 + r_1 t_w \bmod 3^w$
    $r_0 \leftarrow r_0 - a_u$
    $r_1 \leftarrow r_1 - b_u$
    prepend $a_u + b_u\tau$ to S
  Else
    prepend 0 to S
  Endif
  $t \leftarrow \frac{r_0}{3}$
  $r_0 \leftarrow t + r_1$
  $r_1 \leftarrow -t$
Endwhile

Return S

This τ satisfies $X^2 - 3X + 5 = 0$.

Let w be a positive integer and t_w the w-th 5-adic approximation of τ. The first eight t_ws are:

w	1	2	3	4	5	6	7	8
t_w	0	10	35	410	2910	15410	15410	249785

We have that for $a + b\tau \in \mathbb{Z}[\tau]$,

$$\tau^w \mid a + b\tau \iff a + bt_w \equiv 0 \bmod 5^w.$$

Similar to the discussion of Algorithm 4.2, we can find a set of coefficients and an algorithm for width w NAFs of $\mathbb{Z}[\tau]$.

4.2 Applications

The radix-τ 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 [2, 3, 6, 7, 14].

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

Here we give an example of using radix-τ width w NAF in $\mathbb{Q}(\sqrt{-11})$ for point multiplication on 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 $K_2(5, 1, m) : y^2 = x^3 - x + 2/\mathbb{F}_{5^m}$. First, note that the Frobenius map

$$\tau : K_2(5, 1, 1) \to K_2(5, 1, 1)$$
$$(x, y) \mapsto (x^5, y^5)$$

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

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

Therefore τ is identified as $\frac{3+\sqrt{-11}}{2}$. Also note that the operation of τ 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 $m \in \{167, 227, 311\}$.

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

- Compute $a + b\tau$ such that $n \equiv a + b\tau \pmod{\tau^m - 1}$. Since $(\tau^m - 1)P = \mathcal{O}$, we have $nP = (a + b\tau)P$.
- By the discussion in the previous subsection, we have an algorithm to find a width w radix-τ NAF for $a + b\tau$:

$$a + b\tau = \sum_{i=0}^{s} c_i \tau^{k_i},$$

  with $c_i \in C$ and $k_i - k_{i-1} \geq w$.
- Precompute $Q_c = cP$ for each $c \in C$.
- 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-τ 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 for $w = 2$ or 1). Algorithms for computing these forms are presented, and applications to efficient computation of point multiplication on some Koblitz curves are given. This is a continuation and completion of the work of Koblitz [6,7], Solinas [14] and ours [2,3].

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press

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 τ-NAF algorithm.* Inform. Process. Lett. **95**(2005), no. 5, 496–502.

[3] ———, *Efficient algorithms for Koblitz curves over fields of characteristic three.* J. Discrete Algorithms **3**(2005), no. 1, 113–124.

[4] D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing.* In: Advances in Cryptology–CRYPTO 2001 . Lecture Notes in Computer Science 2139, Springer, Berlin, 2001, pp. 213–239.

[5] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography.* Springer-Verlag, New York, 2004.

[6] N. Koblitz, *CM-curves with good cryptographic properties.*In: Advances in Cryptology–CRYPTO '91. Lecture Notes in Computer Science 576, Springer, Berlin 1992, pp. 279–287.

[7] ———, *An elliptic curves implementation of the finite field digital signature algorithm.* Advances in Cryptology–CRYPTO '98. Lecture Notes in Computer Science 1462, Springer, Berlin, 1998, 327–337.

[8] ———, *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* Second edition. Graduate Texts in Mathematics 58, Springer-Verlag, New York, 1984.

[9] W. Meier and O. Staffelbach, *Efficient multiplication on certain nonsupersingular elliptic curves.* Advances in Cryptology–CRYPTO '92. Lecture Notes in Computer Science 740, Springer, Berlin, 1993, pp. 333–344.

[10] J. A. Muir and D. R. Stinson, *Minimality and other properties of the width-w nonadjacent form.* Math. Comp. **75**(2006), no. 253, 369–384.

[11] V. Müller, *Fast multiplication on elliptic curves over small fields of characteristic two.* J. Cryptology **11**(1998), no. 4, 219–234.

[12] M. R. Murty, *Introduction to p-Adic Analytic Number Theory.* AMS/IP Studies in Advanced Mathematics 27, American Mathematical Society, Providence, RI, 2002.

[13] N. Smart, *Elliptic curve cryptosystems over small fields of odd characteristic.* J. Cryptology **12**(1999), no. 2, 141–151.

[14] J. Solinas, *Efficient arithmetic on Koblitz curves.* Des. Codes Cryptogr. **19**(2000), no. 2-3, 195–249.

Department of Electrical and Computer Engineering, University of Toronto,, Toronto, ON, M5S 3G4
e-mail: ifblake@comm.utoronto.ca

Department of Mathematics, University of Toronto, Toronto, ON, M5S 3G3
e-mail: murty@math.toronto.edu

Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwuakee, WI 53211, U.S.A.
e-mail: gxu4uwm@uwm.edu

https://doi.org/10.4153/CJM-2008-054-1 Published online by Cambridge University Press