

Eisenstein Residue Number System with Applications to DSP

V. Dimitrov, G.A. Jullien, W.C. Miller

VLSI Research Group
University of Windsor
Windsor, Ontario, Canada N9B 3P4

I. INTRODUCTION

Logical candidates for residue number system (RNS) implementations are applications which require very high data rates and are numerically intensive. The quadratic residue number system (QRNS) is specifically designed for fast complex arithmetic. In a previous paper by Dubois and Venetsanopoulos the use of Eisenstein complex numbers was proposed for the implementation of a radix-3 fast Fourier transform (FFT). However, since the representation of the cubic root of unity is not error-free, their approach suffered from round-off errors.

In this paper we present a modification to the QRNS, specifically oriented to computations with Eisenstein integers rather than Gaussian integers. Two main advantages accrue from this approach: first, using this RNS we have exact representations of the complex cubic roots of unity; second, it turns out that, in this case, we have a slightly larger dynamic range when the prime moduli are 5-bit integers.

Possible applications of this technique are the error-free implementation of radix-3 FFT algorithms and efficient algorithms for complex multiplication.

II. OVERVIEW OF RADIX-3 FFT ALGORITHMS, QRNS AND THE RING $Z[\mu]$

A. Radix-3 FFT

In [1]-[3] new algorithms for radix-3 FFT have been suggested. The main computational cell, a 3-point butterfly, does not require multiplications. The basic idea of these algorithms is the transformation from the complex field \mathbf{C} to the field of Eisenstein numbers $E(\mu) = \{a + \mu b, a, b \in R\}$, where R is the set of reals, and $\mu = \sqrt[3]{1}$. Therefore,

$\mu = W_3^1 = \exp\left(\frac{-j2\pi}{3}\right)$, hence

$$W_3^1 = -\frac{1}{2} - j\frac{\sqrt{3}}{2} = \mu \quad (1)$$

$$W_3^2 = -\frac{1}{2} + j\frac{\sqrt{3}}{2} = \mu^2 = -1 - \mu$$

From eqn. (1) one easily deduces the forward, eqn. (2),

and inverse, eqn. (3), mappings between traditional complex numbers and Eisenstein numbers:

$$x + jy = \left(x - \frac{y}{\sqrt{3}}\right) - \mu\left(\frac{2y}{\sqrt{3}}\right) \quad (2)$$

$$x + \mu y = \left(x - \frac{y}{2}\right) - j\left(\frac{\sqrt{3}y}{2}\right) \quad (3)$$

The implementation of addition and multiplication in $R(\mu)$ is:

$$\begin{aligned} (x_1 + \mu y_1) + (x_2 + \mu y_2) &= (x_1 + x_2) + \mu(y_1 + y_2) \\ (x_1 + \mu y_1)(x_2 + \mu y_2) &= (x_1 x_2 + y_1 y_2) \\ &\quad + \mu(x_1 y_2 + y_1 x_2 - y_1 y_2) \end{aligned} \quad (4)$$

As an illustration, consider the example of computation of a 9-point Fourier transform. The transformation matrix F_9 can be factorized in the following form:

$$F_9 = Q_9^{(3)} C_9^{-1} (\tilde{F}_3 \otimes I_3) D_9 (I_3 \otimes \tilde{F}_3) C_9 \quad (5)$$

where $Q_9^{(3)}$ is the permutation matrix for digit-reversal in the ternary number system (in the same way that bit-reversal is used in the radix-2 FFT); C_9 and C_9^{-1} are the transformation matrices between \mathbf{C} and $E(\mu)$ (from eqn. (2) and (3)); \tilde{F}_3 is the DFT-matrix in $E(\mu)$; I_3 is a 3x3 unit matrix; $D_9 = I_3 \otimes K_3 \otimes K_3^2$, where $K_3 = \text{diag}(1, W_9^1, W_9^2)$; \otimes denotes the Kronecker matrix product. The general expression of this algorithm (for $N = 3^n$) has the form:

$$F_N = Q_N^{(3)} C_N^{-1} \left[\prod_{i=1}^n (D_{3^i} \otimes I_{3^{n-i}}) (I_{3^{i-1}} \otimes \tilde{F}_3 \otimes I_{3^{n-i}}) \right] C_N \quad (6)$$

B. QRNS

Let $Z_p[j] = (a + jb, a, b \in Z_p)$ be a set of p^2 elements, p - prime, defined in such a manner that the addition is given

by $(a + jb) + (c + jb) = (a + c) + j(b + d)$ and $(a + jb)(c + jb) = (ac - cd) + j(ad + bc)$. The set $Z_p[j]$ is a commutative ring.

Let p be a prime of the form $4k + 1$ and let h denotes the solution of the congruence $x^2 + 1 \equiv 0 \pmod{p}$. Next we map an element $a + jb$ in $Z_p[j]$ into $a + hb \pmod{p}$. It is easy to show that such a mapping is homomorphic. If one uses both solutions of the congruence $x^2 + 1 \equiv 0 \pmod{p}$, $\pm h$, for mapping an element into $(\Delta, \bar{\Delta})$, where $\Delta = a + hb \pmod{p}$ and $\bar{\Delta} = a - hb \pmod{p}$, then such a mapping is an isomorphic mapping and the set $\{\Delta, \bar{\Delta}\}, \Delta, \bar{\Delta} \in Z_p$ is the direct sum of two copies of Z_p of p^2 elements. The following theorem is very important [5]:

Theorem 1: The direct sum of two copies of Z_p is $S_p = Z_p + Z_p = \{\{\Delta, \bar{\Delta}\}, \Delta, \bar{\Delta} \in Z_p\}$, where $(\Delta, \bar{\Delta}) + (\xi, \bar{\xi}) = (\Delta + \xi, \bar{\Delta} + \bar{\xi})$ and $(\Delta, \bar{\Delta})(\xi, \bar{\xi}) = (\Delta\xi, \bar{\Delta}\bar{\xi})$. S_p is a ring of p^2 elements which is isomorphic to the ring $Z_p[j]$.

If $a + jb \in Z_p[j]$, then the forward (Φ) and the inverse (Φ^{-1}) mappings are given by the following equations:

$$\Phi : \Delta = a + hb \pmod{p}, \bar{\Delta} = a - hb \pmod{p} \quad (7)$$

$$\Phi^{-1} : a = 2^{-1}(\Delta + \bar{\Delta}) \pmod{p}, b = (2h)^{-1}(\Delta - \bar{\Delta}) \pmod{p} \quad (8)$$

where 2^{-1} and h^{-1} are the inverse elements of 2 and h in Z_p , respectively. This is the Quadratic Residue Number System (QRNS) encoding technique. Clearly, the solution of the congruence $x^2 + 1 \equiv 0 \pmod{p}$ mimics the imaginary unit (complex operator) in the complex field. The above theorem shows that if one uses the forward mapping Φ to transform a set of Gaussian integers $\{a, b\}$ into conjugate pairs $(\Delta, \bar{\Delta})$, then in the new domain the complex multiplication is equivalent to two integer modular multiplications.

This property governs the main applications of QRNS. The classical radix-2 FFT requires an extensive use of complex multiplications and the QRNS is a powerful tool to speed-up the computational process. However, the previously mentioned restriction for the moduli to be of the form $4k + 1$ can provide unfortunate hardware limitations.

The aim of this paper is to develop a similar mapping theory for radix-3 FFT algorithms. We include, firstly, the structure of the applicable mappings and, secondly, the conditions for the moduli that can be used in this case.

C. The ring $Z[\mu]$

Consider the set $Z[\mu] = \left\{ a + \mu b \mid a, b \in Z, \mu = \frac{-1 + \sqrt{-3}}{2} \right\}$.

$Z[\mu]$ is closed under addition and multiplication. Moreover, $(a + \mu b)(c + \mu d) = ac + \mu(ad + bc) + \mu^2 bd = (ac - bd) + \mu(ad + bc - bd)$ (9)

Thus $Z[\mu]$ is a ring. We note that $Z[\mu]$ is closed under the complex conjugation.

In fact, since $\sqrt{-3} = \sqrt{3}i = -\sqrt{3}i = -\sqrt{-3}$ we see that $\bar{\mu} = \mu^2$. Thus, if $\alpha = a + \mu b \in Z[\mu]$, then $\bar{\alpha} = a + \bar{\mu}b = a + \mu^2 b = (a - b) - \mu b \in Z\mu$.

The theorem of unique factorization is true in $Z[\mu]$ [4]. G.Eisenstein considered the ring $Z[\mu]$ in connection with his work on cubic reciprocity and this ring is named after him.

The most relevant part of his work to our mapping is this definition of conjunction. Table 1 presents the basic differences between the ring of Gaussian integers and Eisenstein integers:

TABLE I SOME BASIC DIFFERENCES BETWEEN GAUSSIAN AND EISENSTEIN INTEGERS

Ring	Conjunction	Norm	Conditions for GF(p)
$Z_p[j] = a + jb$	$a - jb$	$\sqrt{a^2 + b^2}$	$p = 4k + 1$
$Z_p[\mu] = a + \mu b$	$(a - b) - \mu b$	$\sqrt{a^2 - ab + b^2}$	$p = 3k + 1$

III. RESIDUE COMPUTATIONS WITH EISENSTEIN INTEGERS

Let p be a prime of the form $3k + 1$ and let ω be a solution of the congruence:

$$x^2 + x + 1 \equiv 0 \pmod{p} \quad (10)$$

Let $Z_p[\mu] \{a + \mu b \mid a, b \in Z_p\}$ be a set of p^2 elements,

defined in such a manner that addition and multiplication are given as is defined in eqn. (3) and eqn. (4). The set $Z_p[\mu]$ is a commutative ring.

Now we map an element $a + \mu b$ in $Z_p[\mu]$ into a pair (e, \bar{e}) , where

$$e = (a + \mu b) \bmod p \quad \text{and} \quad \bar{e} = [(a - b) - \mu b] \bmod p \quad (11)$$

The proof of Theorem 1 can be extended straightforwardly to this map, that is, the set (e, \bar{e}) is a direct product of two copies of Z_p of p^2 elements. This means that the multiplication of two Eisenstein integers can be computed using only two modular multiplications. The final reconstruction consists of solving the system of congruences:

$$a + \omega b \equiv e \pmod{p} \quad (12)$$

$$(a - b) - \omega b \equiv \bar{e} \pmod{p} \quad (13)$$

which yields

$$b = (2\omega + 1)^{-1}(e - \bar{e}) \quad \text{and} \quad a = 2^{-1}(b + e + \bar{e}) \quad (14)$$

Based on this, we have the following algorithm for multiplication of Eisenstein integers:

Input: $x = x_1 + \mu x_2$ and $y = y_1 + \mu y_2$ - Eisenstein integers;

Output: $z = xy = z_1 + \mu z_2$

Step 1: Transform x and y as conjugate pairs, according to eqn. (12) and eqn. (13). Let the corresponding pairs be: (x_e, \bar{x}_e) and (y_e, \bar{y}_e) .

Step 2: Compute $z_e = x_e y_e \pmod{p}$ and $\bar{z}_e = \bar{x}_e \bar{y}_e \pmod{p}$.

Step 3: Reconstruct the result based on eqn. (14):

$$z_1 = 2^{-1}(z_2 + z_e + \bar{z}_e) \pmod{p} \quad \text{and}$$

$$z_2 = (2\omega + 1)^{-1}(z_e - \bar{z}_e) \pmod{p}.$$

IV. EISENSTEIN RESIDUE NUMBER SYSTEM

The example presented in the previous section shows us that we are able to perform error-free computations with complex irrational numbers having a special form. However,

the dynamic range conditions force us to use modular arithmetic over very large prime numbers, which reduces the advantages of the approach. Fortunately, the moduli can be selected as arbitrary composite numbers, whose prime divisors are of the form $3k + 1$. Now we recursively apply the residue computations over smaller rings; at the end we use the Chinese Remainder Theorem to reconstruct the result.

Let $M = p_1 p_2 \dots p_L$ be a composite number, $p_i \equiv 1 \pmod{3}$ for $i = 1, \dots, L$, p_i a distinct primes. Then $Z_M \cong Z_{p_1} \otimes Z_{p_2} \otimes \dots \otimes Z_{p_L}$, that is, Z_M is isomorphic to the direct product of the smaller rings Z_{p_i} . A similar result holds for more general number rings, based on the general definition of a prime number. Prime numbers of the form $3k + 1$ are not prime in $Z_{p_i}[\mu]$, thus the further decomposition shown in the previous section is possible.

Now the multiplication algorithm for the Eisenstein Residue Number System (ERNS) becomes:

Input: $x = x_1 + \mu x_2$ and $y = y_1 + \mu y_2$ - Eisenstein integers, $|x_1, x_2, y_1, y_2| < 2^b$; primes $p_i \equiv 1 \pmod{3}$, $i = 1, \dots, L$, such that $\prod_{i=1}^L p_i > 3 \cdot 2^{2b}$.

Output: $z = xy = z_1 + \mu z_2$

Step 1: Find the standard residue representation in RNS with moduli (p_1, p_2, \dots, p_L) for x and y , that is:

$$x = x_1 + \mu x_2 = ((x_1, x_2) \bmod p_1, \dots, (x_1, x_2) \bmod p_L) \\ \rightarrow ((y_{11}, y_{21}), (y_{12}, y_{22}), \dots, (y_{1L}, y_{2L}))$$

$$\text{and } y = y_1 + \mu y_2 = ((y_1, y_2) \bmod p_1, \dots, (y_1, y_2) \bmod p_L)$$

Step 2: Apply the algorithm proposed in the previous section for multiplication of the corresponding pairs (x_{1i}, x_{2i}) and (y_{1i}, y_{2i}) . The resulting pairs are: $((z_{11}, z_{21}), (z_{12}, z_{22}), \dots, (z_{1L}, z_{2L}))$.

Step 3: Component-wise multiplication

Step 4: Inverse maps

Step 5: Final Reconstruction based on the Chinese Remainder Theorem

V. COMPARISON BETWEEN QRNS AND ERNS

Both number systems, QRNS and ERNS, are aimed at processing complex numbers of special form, namely $a + jb$ and $a + \mu b$, a and b - integers. The most visible application of QRNS is the implementation of radix-2 FFT algorithms. Understandably, the Eisenstein Residue Number System is more suitable for radix-3 FFT algorithms, because it allows very efficient processing of numbers of the form $a + \mu b$.

The main comparison figure of merit is the dynamic range condition, which is restricted by the allowable form of the prime moduli in these number systems. The following tables show the applicable primes and the corresponding dynamic ranges:

TABLE II DYNAMIC RANGE COMPARISON BETWEEN QRNS AND ERNS (5-BIT MODULI)

Number System	Applicable primes (5-bit)	Dynamic range
QRNS	5,13,17,29	14.97 bits
ERNS	7,13,19,31	15.71 bits

TABLE III DYNAMIC RANGE COMPARISON BETWEEN QRNS AND ERNS (6-BIT MODULI)

Number System	Applicable primes (6-bit)	Dynamic range
QRNS	5,13,17,29,37,41,53,61	37.19 bits
ERNS	7,13,19,31,37,43,61	32.27 bits

TABLE IV DYNAMIC RANGE COMPARISON BETWEEN QRNS AND ERNS (7-BIT MODULI)

Number System	Applicable primes (7-bit)	Dynamic range
QRNS	5,13,17,29,37,41,53,61,73,89,97,101,109,113	76.71 bits
ERNS	7,13,19,31,37,43,61,67,73,79,97,103,109,127	77.88 bits

One of the main advantage of ERNS versus QRNS is the fact that it allows Mersenne primes (prime numbers of the form $2^n - 1$) as moduli. The specific binary representation of Mersenne primes makes them particularly suitable in implementing the basic modular operations. This could be used to speed-up the performance of radix-3 FFT algorithms, based on ERNS.

VI. CONCLUSIONS

In this paper a new approach for processing complex num-

bers has been proposed. Basically, it is aimed at the implementation of radix-3 FFTs, but it can be used in any situation where the requirement to process Eisenstein integers arises. The comparison between the Quadratic Residue Number System and ERNS provides information on available primes and dynamic ranges for the 2 number systems. This information can be used to decide on which number system is more appropriate for specific processing requirements.

VII. REFERENCES

- [1] E.Dubois and A.Venetsanopoulos, A new algorithm for the radix-3 FFT, IEEE Trans. on ASSP, vol.26, No.2, pp.222-225
- [2] S.Prakash and V.V.Rao, A new radix-6 FFT algorithm, IEEE Trans. on ASSP, vol. 29, No.4, pp.939-941
- [3] Y.Suzuki, T.Sone and K.Kido, A new FFT algorithm of radix 3, 6 and 12, IEEE Trans. on ASSP, vol. 34, No.2, pp.38-383
- [4] K.Ireland and M.Rosen, Elements of number theory, Bogden & Quigley, Inc., New York, 1972
- [5] M.Soderstrand, W.K.Jenkins, G.A.Jullien and F.J.Taylor, Residue number systems: modern applications in digital signal processing. IEEE Press, 1986.