Modulo multipliers using polynomial rings

D. Radhakrishnan

Indexing terms: Integer multiplication, Polynomial rings, Galois fields

Abstract: The performance of many DSP chips depends to a great extent on their multiply-accumulate (MAC) speed. In this direction, the use of residue arithmetic has been proved to enhance the speed of multiplier units. One approach has been to convert all multiplication operations to addition, thereby speeding up the whole operation. This was made possible by defining a logarithmic transform for the integers in a finite field, more specifically in a prime field \( GF(p) \). The author extends this approach to the case of polynomial rings (quotient rings), thereby providing more choices for the selection of moduli in RNS multipliers.

1 Introduction

Many error-correcting codes are based on polynomial field theory and use primitive polynomials for code generation [1–4], but this area has not been explored so far for integer arithmetic. Recently, many researchers in the area of residue-number-system (RNS) arithmetic have shown a lot of interest in integer multiplication [5–9]. An RNS full adder-based inner product architecture suitable for pipeline applications is given in [5]. This can operate at very high throughput rates and exhibits reduced complexity as compared to ROM-based designs. A modified residue arithmetic, called pseudorNS, is introduced in [6] which uses modified binary processors and exhibits a performance speed comparable with other RNS traditional approaches.

Further speed-up in integer multiplication is possible by exploiting finite-field (Galois field) concepts [7–9]. This is achieved by converting multiplication to addition using logarithms. However, these methods are always restricted to prime fields since, in such fields, a logarithmic transform (index transform) is defined for all nonzero elements of the field. Many times we encounter moduli of the form \( p^m \), where \( p \) is a prime and \( m \) is any integer. They belong to the class of polynomial fields \( GF(p^m) \) where the individual elements themselves are treated as polynomials. When these elements are treated as integers, they form only a quotient ring, called the ring of integers modulo \( p^m \), denoted by \( Z/(p^m) \). An index transform approach for integer multiplication in these rings was not available because of the non-existence of integer generator elements to generate all nonzero elements of the ring \( Z/(p^m) \). In this paper, we have shown that this problem can be overcome by defining an index set rather than a single index value for the elements of the quotient ring.

2 Index generation in Galois fields and quotient rings

An algebraic field is defined with a set of elements together with two operations, + and *, satisfying certain properties [3, 10]. The operators + and * can be conveniently chosen as modulo addition and modulo multiplication, respectively. A field with a finite number of elements is called a finite field or Galois field. Galois fields are classified into two types: prime fields \( GF(p) \), and polynomial fields \( GF(p^m) \), where \( p \) is a prime number and \( m \) is any positive integer. A prime field \( GF(p) \) consists of \( p \) elements from 0 to \( p-1 \). The set of elements \( 1, 2, ..., p-1 \) together with the operand * (multiplication, mod \( p \)) forms a multiplicative group \( G(p) \).

In Galois fields, certain elements exist which generate other elements of the field as its non-negative integer powers. These elements are called primitive roots. In a prime field this is defined mathematically as follows: let \( g \in GF(p) \) and \( (g^m)_p = 1 \), where \( (g^m)_p \) represents the number of non-negative integers less than \( p \) which are prime relative to \( p \). \( \phi(p) \) can be calculated using the general expression:

\[
\phi(n) = n \prod_{q|n} \left( 1 - \frac{1}{q} \right)
\]

where the symbol \( \Pi_{q|n} \) means the product over all primes \( q \) that divide \( n \). When \( p \) is a prime, \( \phi(p) = p - 1 \), and \( g \) generates all elements of the field, thereby forming a complete residue system. The primitive roots for the modulus \( p \), where \( p \) is any integer, can be found using the following general theorem [11].

Theorem 1: Let \( c = \phi(p) \) and let \( p_1, p_2, ..., p_q \) be the different prime divisors of the number \( c \). In order that a number \( g \), which is relatively prime to \( p \), be a primitive root modulo \( p \), it is necessary and sufficient that this \( g \) satisfy none of the congruences:

\[
g^{c/p_1} \equiv 1 \pmod{p}, \quad g^{c/p_2} \equiv 1 \pmod{p}, ..., g^{c/p_q} \equiv 1 \pmod{p}
\]

Using the primitive root \( g \), each and every element of the multiplicative group \( G(p) \) can be uniquely mapped to an index value \( i \) satisfying the following: \( \forall a \in G(p), \exists i \) such that \( g^{i/p} = a \). The following well known theorem is now useful in simplifying the multiplication of two integers.

Theorem 2: For a prime integer \( p \), the multiplicative group modulo \( p \) is isomorphic to the additive group modulo \( (p - 1) \).
Using theorem 2, multiplication of two integers can be performed by adding their corresponding indices modulo \((p - 1)\), and then finding the inverse index value [12].

Let us now consider the structure of a polynomial field \(GF(p^m)\). For every prime \(p\) and a positive integer \(m\), there is a Galois field \(GF(p^m)\) with \(p^m\) elements. Unfortunately, the set of integers \(1, 2, ..., (p^m - 1)\) with the operation of multiplication, \(\mod p^m\), does not form a group, because of the nonexistence of multiplicative inverse for each and every element of the set. Instead the set \(\{0, 1, ..., p^m - 1\}\) forms a ring under addition and multiplication, modulo \(p^m\). Primitive roots exist for all integer rings modulo \(p^m\) except when \(p = 2\) and \(m \geq 3\) [10]. However, none of the primitive roots generate all elements of the ring. This poses a problem in using index mapping for multiplication. One solution is to define an index set instead of a single index value in these rings. A procedure for finding an index set for the elements of the ring of integers modulo \(2^m\) is given in [11, 13, 14], and is summarised below.

It turns out that the number 5 plays a central role in finding an index code for the elements of the ring \(Z/(2^m)\). The order of the element 5 in \(Z/(2^m)\) is \(2^{m-2}\) if \(m \geq 3\). Hence the integers \(+5, \pm 5, ..., \pm 2^{m-2}\) form a reduced residue system (RRS) \(\mod 2^m\) for every \(m \geq 3\) [10]. (A reduced residue system, modulo \(m\), is any set of \(\{s_1, s_2, ..., s_k\}\) of \(k\) integers each relatively prime to \(m\), such that each integer \(x\) which is relatively prime to \(m\) is congruent to one and only one of the \(s_i\).) Any odd integer \(x \in \{1, 2^m - 1\}\) can now be uniquely coded in \(\text{RRS}\) as a dual-index code \(\langle \beta, \gamma \rangle\) with the property that \(x = 2^{\beta\gamma} (\gamma^{-1})_{2m}\), where \(\beta \in \{0, 1, ..., (2^{m-2} - 1)\}\) and \(\gamma \in \{0, 1\}\). The even integers in \(Z/(2^m)\) can be included by modifying the above code to a triplet index code \(+\alpha, \beta, \gamma\) using the relationship \(x = 2^{\gamma\beta} (\gamma^{-1})_{2m}\), with \(\alpha \in \{0, 1, ..., m - 1\}\). It may be noted that the triplet codes formed for the even integers are not unique.

Multiplication of two integers can now be carried out as follows: let \(x, y \in Z/(2^m)\), \(x \neq 0, y \neq 0\), and

\[
x = 2^\alpha \left[ 5^{\beta_1} (\gamma_1^{-1})_{2m} \right], \quad y = 2^\alpha \left[ 5^{\beta_2} (\gamma_2^{-1})_{2m} \right]
\]

then the product

\[
|xy|_{2m} = 2^{\alpha+1+\alpha} \left[ 5^{\beta_1+\beta_2} (\gamma_1+\gamma_2^{-1})_{2m} \right]
\]

The indices are added subject to the following constraints: \(\beta_1, \beta_2\) are added \(\mod 2^{m-2}\), \(\gamma_1, \gamma_2\) are added \(\mod 2\), and \(\alpha_1, \alpha_2\) are added in normal binary mode. When \(\alpha_1 + \alpha_2 = m - 1\) the corresponding \(\gamma\) and \(\gamma_2\) are made zero, and when it exceeds \(m\), the final result is made zero.

A unique coding using the triplet index code is given in [14]. This is achieved by modifying the representation of the number to the form \(x = 2^{\gamma} 5^{\beta} (\gamma^{-1})_{2m}\). While using this representation, the index addition on \(\beta\) must be done by \(\mod 2^{m-2}\). Thus, by storing the index and inverse index tables, multiplication of the nonzero elements can be replaced by an index addition.

The solution to the general problem of finding an index code for each and every element of \(Z/(p^m)\) for odd prime \(p\) has not been available so far. In the following, we give a solution using an index-pair coding, and also show a synthesis procedure to generate the index pairs for each and every element of the quotient ring \(Z/(p^m)\).

3 Index generation for \(Z/(p^m)\), for odd \(p\)

Consider now quotient rings \(Z/(p^m)\) for odd prime \(p\). Let \(g \in Z/(p^m)\) such that

\[
|g^{\phi(p^m)}|_{p^m} \equiv 1
\]

The existence of \(g\) for the case of an odd prime \(p\) is given in [3, 4, 10, 11, 15]. This \(g\) is called the primitive root of \(Z/(p^m)\). Since \(p^m\) is not a prime, \(\phi(p^m) = (p - 1)p^{m-1}\), and hence \(g\) does not generate all elements of \(Z/(p^m)\). However, \(g\) generates all the elements which are relatively prime to the modulus \(p^m\), thereby forming a reduced residue system. The methods for finding the primitive roots for \(Z/(p^m)\), where \(p\) is an odd prime, are given below [11].

Let \(g\) be a primitive root modulo \(p^m\). We can find a \(t\) such that \(u\), which is defined by the equation \((g + pt^{\alpha})^{\beta} = 1 + pu\), is not divisible by \(p\). Then \(g + pt\) is a primitive root modulo \(p^m\) for any \(m > 1\). It may be noted that in many cases the primitive root of \(p^m\) is \(g\) itself.

The following lemma and theorem are proposed to define a logarithmic mapping for the elements of \(Z/(p^m)\).

Lemma 1: For any odd prime \(p\), all integer multiples of \(p\) in the range \(1\) to \((p^m - 1)\) can be expressed as \(r \ast p\) such that \(\gcd(r, p) = 1\) with \(1 \leq r \leq p^{m-1} - 1\) and \(0 \leq i \leq m - 1\).

The proof of this lemma can be easily derived from number theory and hence is omitted here.

Theorem 3: For an odd prime \(p\) and any integer \(m\), all nonzero elements of a quotient ring \(Z/(p^m)\) of integer elements can be generated using the generator pair \(g^p, \gamma\) where \(\gamma\) is a primitive root of the quotient ring, \(\alpha \in \{0, 1, ..., \phi(p^m) - 1\}\), and \(\beta \in \{0, 1, ..., m - 1\}\).

Proof: The proof is shown as a synthesis procedure for generating the elements of the quotient ring \(Z/(p^m)\) for odd prime \(p\). At first the set \(S\) corresponding to the nonzero elements of \(Z/(p^m)\) is partitioned into two sets \(S_1\) and \(S_2\) as follows:

\[
S_1 = \{g^a | \phi(p^m)\} \text{ such that } \forall a \in S_1, (a, p^m) = 1, \quad S_2 = \{k \ast p^i | \phi(p^m)\}, \text{ where } k \in \{1, ..., p^{m-1} - 1\}, S_1 \cup S_2 = S, S_1 \cap S_2 = \emptyset, \text{ the null set.}
\]

Case 1 (generator for the elements of \(S_1\)): The quotient ring \(Z/(p^m)\) has at least one primitive root of order \(\phi(p^m)\). Let \(g\) be that primitive root. Then \(|g^p\phi(p^m)| = 1\), and \(g\) generates all elements \(Z/(p^m)\) which are relatively prime to \(p^m\). There are \(\phi(p^m)\) such elements. Hence all elements of set \(S_1\) are generated by \(g\). Now \(|g^p\phi(p^m)| = \phi(p^m)\) for \(\beta = 0\). Hence \(S_1 = \{g^a | p^i \phi(p^m)\}, \text{ where } i > 0\).

Case 2 (generator for the elements of \(S_2\)): The elements of this set can be enumerated as: \(p, 2p, 3p, ..., (p^m - 1)p\). Here the coefficients of \(p\) include all integers from 1 to \(p^m - 1\). By lemma 1, these elements can be expressed in the form \(r \ast p\phi(p^m), \text{ where } \gcd(r, p) = 1\), but, as \(S_1\) consists of all elements which are relatively prime to \(p^m\), they are also relatively prime to \(p\). Therefore all values of \(r\) are available as elements of the set \(S_1\), and all elements of \(S_2\) can be generated by the product \(g^{ap^i}\).

Using theorem 3, we can define an index pair \((\alpha, \beta)\) for each and every element of \(Z/(p^m)\). Using this index pair the product of two numbers \((x, x_2) \mod p^m\) can be calculated as follows: let \(x_1 = (g^{ap^i} \phi(p^m)) \mod p^m\) and \(x_2 = (g^{ap^i} \phi(p^m)) \mod p^m\), then their product \((x_1, x_2) \mod p^m\) is
given by
\[
|x_1 x_2|_{p^m} = (g^{c_1} p^{\beta_1})(g^{c_2} p^{\beta_2}) \mod p^m
= (g^{c_1+c_2} p^{\beta_1+\beta_2}) \mod p^m.
\]

The indices are added subject to the following constraints: \(c_1\) and \(c_2\) are added mod \(\phi(p^m)\), and \(\beta_1\) and \(\beta_2\) are added mod \(m\).

Thus the multiplication operation is converted to an index addition. The index pair \((\alpha, \beta)\) calculated using theorem 3 is not unique. This results from the fact that the total number of index pairs \(m \cdot \phi(p^m) > (p^m - 1)\). An example to illustrate the generation of index pairs based on theorem 3 is given below.

**Example 1:** Consider the quotient ring \(\mathbb{Z}/(3^2)\). It can be easily verified that 2 is a primary root of \(GF(3)\). It so happens that 2 is also a primitive root of \(\mathbb{Z}/(3^2)\). Hence \(g = 2\). Now \(\phi(3^2) = 18\) and hence \(2^{18} \equiv 1 \mod 3^2\). The integer powers of 2, modulo 3, generate 18 elements which are all relatively prime to the modulus 3. The remaining 8 elements are 3, 6, 9, 12, 15, 18, 21, and 24. By theorem 3, all the nonzero elements are coded as index pairs \((\alpha, \beta)\) using the generator pair \(g^6 p^6\) with the property that \(V x \in \mathbb{Z}/(3^2), \exists \alpha_x \in \{0, 1, \ldots, 17\}, \) and \(\beta_x \in \{0, 1, 2\}\) such that \(|2^x|_{3^2} = x\). The index coding is shown in Table 1.

**Table 1:** Index coding for elements of \(\mathbb{Z}/(3^2)\) with a primitive root of 2

<table>
<thead>
<tr>
<th>(x)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\alpha, \beta)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>(x)</td>
<td>9</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>(\alpha, \beta)</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>(x)</td>
<td>9</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>(\alpha, \beta)</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>8</td>
<td>0</td>
</tr>
</tbody>
</table>

An example to illustrate the multiplication of two integers modulo \(p^m\) using index addition is given below:

**Example 2:** Consider the modulo multiplication of two integers \(X = 12\) and \(Y = 19\) using modulus 27. All the elements now belong to the ring of integers \(\mathbb{Z}/(3^3)\). An index coding for each and every nonzero element of \(\mathbb{Z}/(3^3)\) is given in Table 1. Using Table 1, the index codes for 12 and 19 are (2, 1) and (12, 0), respectively. The indices 2 and 12 are added modulo \(\phi(3^3) = 18\), giving a result of 14, while the indices 1 and 0 are added modulo \(m\), i.e. modulo 3, giving a result of 1. The index addition therefore results in the generation of the index pair (14, 1). This represents the final product \(2^{14} 3^1\) = 12. It can easily be verified that \(12 \cdot 19 = 228\).

**4 Conclusions**

Integer multiplication in the ring of integers modulo \(p^m\) using an index transform approach was not possible earlier because of the non-existence of primitive roots to generate all elements of the ring. In this paper, we have shown a mapping that maps each and every element in the quotient ring \(\mathbb{Z}/(p^m)\) to an index pair for odd \(p\), and to an index triplet for even \(p\). This index coding has properties similar to the logarithm in ordinary arithmetic, thereby simplifying the multiplication operation mod \(p^m\) to an addition of indices in \(\mathbb{Z}/(p^m)\). These techniques can be easily applied to the design of residue number-based multipliers employing moduli of the form \(p^m\) to improve their performance.

**5 References**

12. NAKL, A. (Ed.): 'Decimal arithmetic unit' (Stroje Na Zprocovani, Prague, CSAU Czechoslovakia, 1962)