Consiglio Nazionale delle Ricerche

ISTITUTO DI ELABORAZIONE DELLA INFORMAZIONE

PISA

ARITHMETIC PROPERTIES OF A CLASS OF HYBRID NUMBER SYSTEMS

Ferruccio BARSI

Progetto finalizzato

"Materiali e Dispositivi per l'Elettronica a Stato Solido

Nota interna B4-01

Febbraio 1989

ARITHMETIC PROPERTIES OF A CLASS OF HYBRID NUMBER SYSTEMS

Ferruccio BARSI

Progetto finalizzato

"Materiali e Dispositivi per l'Elettronica a Stato Solido

Nota interna B4-01

Febbraio 1989

ARITHMETIC PROPERTIES OF A CLASS OF HYBRID NUMBER SYSTEMS

Ferruccio BARSI

Istituto di Elaborazione dell'Informazione del CNR, Pisa, Italy

Abstract

In attempts to speed-up computer arithmetic, many researchers have investigated the arithmetic properties and practical implementations of non-weighted, residue number systems (RNS). However, RNS's are not successful in those applications, such as division and magnitude comparison, where the result cannot be derived from a separate consideration of operand digits.

In this paper, a class of hybrid number systems, namely, residue number systems with magnitude index (RNS with MI), have been considered under a more general formulation than that previously known. In these systems, numerical information is split into two separate parts, which are given a residue and a weighted representation, respectively. The arithmetic properties of such systems have been investigated in depth and it has been shown that these systems are suitable for fast, general purpose, arithmetic implementations.

Index Terms

Computer Arithmetic, Hybrid Number Systems, Magnitude Index, Number Representation, Residue Number Systems, Weighted Number Systems

---

This research has been supported by the National Program on Solid-State Electronics and Devices of the Italian National Research Council

1 - INTRODUCTION

Since the beginnings of computer science, the ultimate goal of most researchers working in this area has been ever faster information processing. However, in the field of numerical information, conventional weighted number systems soon revealed their limits which are mainly constituded by the mutual dependence of digits.

Efforts to overcome such limits led several authors to reconsider Residue Number Systems ([1], [2], [3]) because of the independence of their digits in representing numbers and in arithmetic operations such as addition, subtraction and multiplication. This independence, together with the possibility of performing modular computations by using table look-up techniques, has stimulated a much research work and has led to many significant designs of digital processors.[4-17].

It was immediately apparent that the needs of Digital Signal Processing arithmetic were almost completely satisfied by processing units constructed in RNS's [18-20] and many RNS-based, digital processors have been successfully designed for digital filtering and FFT implementations, i.e., for applications involving addition, subtraction and multiplication with results expected within a predetermined range.

The advent of VLSI technology and the consequent demand for modular and regular designs has further evidenced the importance of these systems [21-25]; indeed their implementation can easily take advantage of results obtained for conventional binary logic [26].

However, RNS's have been found lacking, in part or completely, in all those applications, such as division and magnitude comparison, in which the results cannot be derived from an independent processing action of operand digits or whenever overflow detection is mandatory to ensure the correctness of the result. In these cases, lengthy intermodular operations, equivalent to a number system conversion process, are necessary.

The principal reason which has led us to investigate hybrid number systems has been the observation that weighted and residue systems may be considered as extreme solutions to the general problem of representing and processing numerical

information. Is it possible to find intermediate solutions suitable for fast, general arithmetic ?

This paper is an attempt to answer the above question by taking advantage of the modular properties of residue systems without completely releasing the explicit knowledge of number magnitude of weighted systems. For this purpose, a class of hybrid number systems, i.e., Residue Number Systems with Magnitude Index [27], [28], has been reconsidered under a more general formulation and its arithmetic properties have been carefully investigated.

The most significant results which have been derived for these systems can be summarized as follows:

i) modular addition and multiplication are possible provided that certain simple conditions are satisfied and results which fall outside the original notation are accepted;

ii) the scaling of numbers by a product of radices of the system has been studied for the most general case and exhibits a complexity which is intermediate between that of residue and weighted systems;

iii) general division is possible and should result in a rather fast procedure as it is seen that the quotient of dividing two integers is, in most cases, exclusively dependent on the weighted parts of the representations of operands.

Finally, it should be noted that architectural aspects of RNS with MI implementations have been intentionally omitted in this paper for the sake of simplicity; however, many simple solutions have been suggested or may be easily inferred from arithmetic results.

2 - THE REPRESENTATION OF NUMBERS

Given an integer X, there are several ways which can be devised for its representation, each corresponding to the definition of a particular number system.

In general, a number system is defined whenever:

i) an ordered set of positive integers $\{m_1, m_2, \ldots, m_n\}$ (*the radices of the system*) is given and

ii) there exists a correspondence law uniquely relating any integer X to the set of digits $\{x_1, x_2, \ldots, x_n\}$ of its representation, i.e., $x_i=f(X,m_1,m_2, \ldots,m_n)$, $i=1,2,\ldots,n$ and, in general, $0 \le x_i < m_i$.

A number system is said to be *non redundant* if the number of different integers which can be represented in this system coincides with the product $M = \Pi_{i=1}^{n} m_i$.

There are two basic classes of correspondence laws relating integers to the digits of their representations: a sequential law (*weighted number systems*) and a parallel or one-step law (*residue number systems*).

To clarify the above assertion, let us recall that any number system, which allows arbitrary integers to be represented by means of sequences of a finite number of symbols, is derived from the application of the following identity :

$$X = \mu \left\lfloor \frac{X}{\mu} \right\rfloor + |X|_\mu \qquad (1)$$

holding for any X. In this identity, μ is a positive integer, $|X|_\mu$ is the *residue of X modulo* μ, i.e., the least non-negative remainder of dividing X by μ and $\left\lfloor \frac{X}{\mu} \right\rfloor$ represents the greatest integer not exceeding $\frac{X}{\mu}$.

The process of defining a number system by using identity (1) will be reconsidered in the following and an interesting extension of conventional systems will be investigated in depth.

2.1 - WEIGHTED NUMBER SYSTEMS

The class of weighted number systems originates from a *sequence* of repeated applications of identity (1). In fact, supposing that an integer X and a set $\{m_1, m_2, \ldots, m_n\}$ of radices are given and letting $\mu = m_1$ in identity (1), we obtain:

$$X = m_1\left\lfloor\frac{X}{m_1}\right\rfloor + |X|_{m_1}$$

and, assuming $x_1 = |X|_{m_1}$ as the first, radix-m_1, digit of X:

$$X = m_1\left\lfloor\frac{X}{m_1}\right\rfloor + x_1 \qquad (1')$$

where x_1 has a weight 1 and $0 \le x_1 < m_1$.

Letting $X_1 = \left\lfloor\frac{X}{m_1}\right\rfloor$ and applying again identity (1), with $\mu = m_2$:

$$X_1 = m_2\left\lfloor\frac{X_1}{m_2}\right\rfloor + |X_1|_{m_2} = m_2\left\lfloor\frac{X}{m_1 m_2}\right\rfloor + |X_1|_{m_2}$$

the second, radix-m_2, digit of X:

$$x_2 = |X_1|_{m_2}$$

is obtained. Combining equalities (1) and (1') gives:

$$X = m_1 m_2\left\lfloor\frac{X}{m_1 m_2}\right\rfloor + x_2 m_1 + x_1 \qquad (1'')$$

and it is seen that x_2 has a weight m_1 with $0 \le x_2 < m_2$.

This procedure can be iterated and, in general, the i.th digit, of weight

$$P_i = \prod_{k=1}^{i-1} m_k$$

can be derived as:

$$x_i = \left\| \frac{X_{i-1}}{m_{i-1}} \right|_{m_i} = \left\| \frac{X}{\prod_{k=1}^{i-1} m_k} \right\|_{m_i} \qquad (2)$$

$i = 1, 2, \ldots, n$, $X_0 = X$ and $\prod_{k=1}^{0} m_k = 1$

It is worth noting that the representation of X is *consistent*, i.e., X is representable in the given system, if and only if

$$X_n = \left\lfloor \frac{X_{n-1}}{m_n} \right\rfloor = 0$$

or, equivalently, iff $X < M$.

Example 1.

Suppose that a set of radices $m_1 = 7$, $m_2 = 10$, $m_3 = 12$ and $m_4 = 19$ is given and the number $X = 593$ is to be represented in the weighted system. First, observe that X is consistently representable as $593 < m_1 m_2 m_3 m_4 = 15{,}960$. The digits of the representation, as evaluated from equality (2) are:

$$x_1 = |X|_{m_1} = |593|_7 = 5$$

$$x_2 = \left\| \left\lfloor \frac{X}{m_1} \right\rfloor \right\|_{m_2} = \left\| \left\lfloor \frac{593}{7} \right\rfloor \right\|_{10} = 4$$

$$x_3 = \left\| \left\lfloor \frac{X}{m_1 m_2} \right\rfloor \right\|_{m_3} = \left\| \left\lfloor \frac{593}{70} \right\rfloor \right\|_{12} = 8$$

$$x_4 = \left\| \left\lfloor \frac{X}{m_1 m_2 m_3} \right\rfloor \right\|_{m_4} = \left\| \left\lfloor \frac{593}{840} \right\rfloor \right\|_{19} = 0$$

Conversely, consider the representation $\{x_1, \ldots, x_n\}$ of an integer X. It can immediately be seen from (1'), (1") and (2) that the relation between X and the digits of its representation takes the form:

$$X = \sum_{i=1}^{n} x_i \prod_{j=1}^{i-1} m_j \qquad (3)$$

As an example of an application of equality (3) consider, from Example 1, the representation $\{5,4,8,0\}$ in the system of radices $m_1 = 7$, $m_2 = 10$, $m_3 = 12$ and $m_4 = 19$. Then:

$$X = 5 + 4 \times 7 + 8 \times 7 \times 10 + 0 \times 7 \times 10 \times 12 = 593$$

The most familiar weighted systems we deal with correspond to the case in which $m_1 = m_2 = \ldots = m_n = r$ (*fixed radix notation*) whereas the general case we considered in the example will be referred to as a *mixed radix notation.*

Regardless of the particular choice of the set of radices, weighted systems exhibit the following basic features:

i) each digit x_i of the representation is a function of the number X and of radices $m_i, m_{i-1}, ..., m_1$, i.e., $x_i = f(X, m_i, m_{i-1}, ..., m_1)$, and has a weight $P_i = \prod_{j=1}^{i-1} m_j$ which is the product of the subset $m_{i-1}, ..., m_1$ of radices of the system. Because of this, *the ordering of digits cannot be altered without affecting the correctness of the representation.*

ii) in performing arithmetic, each digit of the result depends on all the digits of the operands; this implies that arithmetic operations are inherently sequential processes.

iii) magnitude comparison is also a sequential process and is performed digit-by-digit, starting from the most significant digit x_n; lower order digits are inspected only if higher order digits coincide.

2.2 - RESIDUE NUMBER SYSTEMS

To emphasize the peculiarities of the other class of number systems, let us suppose that the same set of radices $\{m_1, m_2, ... , m_n\}$ that we have already considered for weighted systems is given. When dealing with residue systems, these radices will be referred to as the *moduli* and an additional constraint will be usually assumed to avoid number system redundancy, i.e., it will be supposed that *moduli are pairwise prime numbers*.

For any given integer X, the residue digits of its representation $\{x_1, ... , x_n\}$ are determined from identity (1) by assuming:

$$\begin{array}{lll} \mu = m_1 & X = m_1 \left\lfloor \frac{X}{m_1} \right\rfloor + |X|_{m_1} & x_1 = |X|_{m_1} \\ \mu = m_2 & X = m_2 \left\lfloor \frac{X}{m_2} \right\rfloor + |X|_{m_2} & x_2 = |X|_{m_2} \\ \cdots\cdots & & \\ \cdots\cdots & & \\ \mu = m_n & X = m_n \left\lfloor \frac{X}{m_n} \right\rfloor + |X|_{m_n} & x_n = |X|_{m_r} \end{array} \qquad (4)$$

The correspondence between X and the digits of its representation, as defined by relations (4), justifies the *parallel* or *one-step* attribute of residue systems. In fact, each residue digit is only dependent on the related modulus; as a consequence, the ordering can be arbitrarily altered without affecting the correctness of the representation. Moreover, as in weighted systems, a number X will be consistently representable iff $X<M$, $M = \Pi_{i=1}^{n} m_i$.

The independence of digits has several interesting implications whenever arithmetic operations such as addition, subtraction and multiplication are concerned. In fact, the following property :

$$|X*Y|_{m_i} = \left||X|_{m_i} * |Y|_{m_i}\right|_{m_i} = |x_i * y_i|_{m_i}$$

where the operator * is equivalent to +, -, x, holds for any modulus m_i, i = 1, 2, ..., n.

This provides a carry or borrow-free, fast arithmetic since addition, subtraction and multiplication are carried out digit-by-digit.

However, complications arise in operations implying a number magnitude knowledge such as in comparison, division or overflow detection. In these cases, lengthy intermodular operations are required whose complexity is equivalent to a residue-to-weighted conversion process.

Example 2.

As an example, let us consider the set of moduli $m_1 = 7$, $m_2 = 11$, $m_3 = 12$ and $m_4 = 19$ and the integer $X = 1281$. The application of equalities (4) yields:

$$x_1 = |X|_{m_1} = |1281|_7 = 0$$

$$x_2 = |X|_{m_2} = |1281|_{11} = 5$$

$$x_3 = |X|_{m_3} = |1281|_{12} = 9$$

$$x_4 = |X|_{m_4} = |1281|_{19} = 8$$

In a residue system, a number X is related to its representation $\{x_1, \ldots, x_n\}$ by means of the following equality, also referred to as the *Chinese Remainder Theorem*

$$X = \left|\Sigma_{i=1}^{n} x_i B_i\right|_M \qquad (5)$$

where M is the product of the moduli of the system and

$$B_i = \frac{M}{m_i}\left|\frac{1}{\frac{M}{m_i}}\right|_{m_i} \qquad \left|\frac{M}{m_i}\left|\frac{1}{\frac{M}{m_i}}\right|_{m_i}\right|_{m_i} = 1$$

is the mod M "weight" corresponding to the i.th residue digit.

The Chinese Remainder Theorem can be usefully applied when converting integers from a residue to a weighted representation. However, since all computations are to be performed mod M, a different method (mixed radix conversion) which only permits mod m_i computations to be performed can be employed whenever the conversion process must not alter the modular nature of residue processing.

The Chinese Remainder Theorem, when applied to the representation {0,5,9,8} of Example 2 gives:

$$X = |0.B_1 + 5.B_2 + 9.B_3 + 8.B_4|_M$$

and, since:

$$\frac{M}{m_1} = 11.12.19 = 2508 \qquad \left|\frac{1}{\frac{M}{m_1}}\right|_{m_1} = 4 \qquad B_1 = 10{,}032$$

$$\frac{M}{m_2} = 7.12.19 = 1596 \qquad \left|\frac{1}{\frac{M}{m_2}}\right|_{m_2} = 1 \qquad B_2 = 1{,}596$$

$$\frac{M}{m_3} = 7.11.19 = 1463 \qquad \left|\frac{1}{\frac{M}{m_3}}\right|_{m_3} = 11 \qquad B_3 = 16{,}093$$

$$\frac{M}{m_4} = 7.11.12 = 924 \qquad \left|\frac{1}{\frac{M}{m_4}}\right|_{m_4} = 8 \qquad B_4 = 7{,}392$$

it follows that:

$$X = |5.1596 + 9.16093 + 8.7392|_{17556} = |211{,}953|_{17556} = 1281$$

The equalities (3) and (5) which we have recalled for weighted and residue systems can be given a unified formulation. In fact, an integer represented as:

$X = \{x_1, \ldots, x_n\}$

will always be reconstructed by computing:

$$X = \left| \Sigma_{i=1}^{n} x_i W_i \right|_T \qquad (6)$$

where :

$W_i = P_i$ and $T = \infty$ in weighted systems and
$W_i = B_i$ and $T = M$ in residue systems.

The number systems presented above do not complete the set of possible number systems. In fact, identity (1) suggests that preceding notations could be combined to generate hybrid number systems exhibiting properties which may be exploited in particular applications. Residue number systems with magnitude index represent the most common example of hybrid notation.

2.3 - RESIDUE NUMBER SYSTEMS WITH MAGNITUDE INDEX

The idea of representing integers in a hybrid notation with the aim of taking advantage of favourable features of both weighted and residue systems has been considered in the past by several authors [ ], [ ], [ ], [ ]. We will refer here to the formulation proposed in [28] which is first briefly reviewed for the sake of clarity.

Given an integer X and a set of radices $\{m_1, m_2, \ldots, m_t, m_{t+1}, \ldots, m_n\}$, assume that radices $m_1, m_2, \ldots, m_t$ are pairwise prime numbers and represent X as:

$$X \equiv \{R_X, I_X\} \qquad (7)$$

where:

$$R_X = |X|_\mu \qquad (8)$$

is represented in the residue system of moduli $m_1, m_2, \ldots, m_t$, with $\mu = \Pi_{i=1}^{t} m_i$:

$$R_X \equiv \{x_1, x_2, \ldots, x_t\}$$

and

$$I_X = \left\lfloor \frac{X}{\mu} \right\rfloor \qquad (9)$$

is represented in the weighted system of radices $\{m_{t+1}, \ldots, m_n\}$, $P = \prod_{i=t+1}^{n} m_i$:

$$I_X \equiv \{x_{t+1}, \ldots, x_n\}$$

The number system defined by equalities (7), (8) and (9) will be referred to as a *residue number system with magnitude index (RNS with MI)* . R_X will be called the *residue component* of the representation while I_X, which precisely locates R_X into intervals of width μ, will be called the *weighted* or *magnitude index (MI) component* .

The correspondence law relating X to the set of digits $\{x_1, x_2, \ldots, x_t, x_{t+1}, \ldots, x_n\}$ is immediate as, from identity (1):

$$X = R_X + \mu I_X \qquad (10)$$

and, recalling (3), (5) and (6):

$$X = \left| \sum_{i=1}^{t} x_i W_i \right|_\mu + \sum_{i=t+1}^{n} x_i W_i \qquad (11)$$

where:

$$W_i = \frac{\mu}{m_i} \left| \frac{1}{\frac{\mu}{m_i}} \right|_{m_i} \qquad \text{for} \quad i = 1, 2, \ldots, t$$

:

or

$$W_i = \prod_{j=1}^{i-1} m_j \qquad \text{for } i = t+1, \ldots, n$$

Example 3.

Let us consider the set of radices $m_1 = 7, m_2 = 9, m_3 = 11, m_4 = m_t = 13, m_5 = m_{t+1} = 4, m_6 = m_n = 8$ *and let us suppose that integer* $X = 71812$ *is to be represented. The residue , MI and total system ranges are, respectively:*

$\mu = 7.9.11.13 = 9009$

$P = 4.8 = 32$

$$T = \mu P = 288{,}288$$

From equalities (7), (8) and (9) it can be seen that:

$X \equiv \{R_X, I_X\}$ *with:*

$$R_X = |X|_\mu = |71{,}812|_{9009} = 8749$$

$$I_X = \left\lfloor \frac{X}{\mu} \right\rfloor = \left\lfloor \frac{71812}{9009} \right\rfloor = 7$$

and, from equalities (2) and (4):

$X \equiv \{6,1,4,0,3,1\}$

The correctness of above representation can be verified by means of relation (11). In fact, the weights of system digits are:

$$\frac{\mu}{m_1} = 9.11.13 = 1287 \qquad \left|\frac{1}{\frac{\mu}{m_1}}\right|_{m_1} = \left|\frac{1}{1287}\right|_7 = 6 \qquad W_1 = 7722$$

$$\frac{\mu}{m_2} = 7.11.13 = 1001 \qquad \left|\frac{1}{\frac{\mu}{m_2}}\right|_{m_2} = \left|\frac{1}{1001}\right|_9 = 5 \qquad W_2 = 5005$$

$$\frac{\mu}{m_3} = 7.9.13 = 819 \qquad \left|\frac{1}{\frac{\mu}{m_3}}\right|_{m_3} = \left|\frac{1}{819}\right|_{11} = 9 \qquad W_3 = 7371$$

$$\frac{\mu}{m_4} = 7.9.11 = 693 \qquad \left|\frac{1}{\frac{\mu}{m_4}}\right|_{m_4} = \left|\frac{1}{693}\right|_{13} = 10 \qquad W_4 = 6930$$

$$W_5 = \mu = 9009$$

$$W_6 = \mu m_5 = 36036$$

and the representation {6,1,4,0,3,1} corresponds to the number:

$$X = |6.7722 + 1.5005 + 4.7371 + 0.6930|_{9009} + 3.9009 + 1.36036 =$$

$$= |80821|_{9009} + 63063 = 8749 + 63063 = 71812$$

3 - THE ARITHMETIC PROPERTIES OF RNS WITH MI

The investigation of arithmetic properties of RNS with MI has the ultimate aim of taking advantage of the modular properties of RNS arithmetic and of the explicit knowledge of the number magnitude of weighted systems. In what follows, the fundamental arithmetic operations will be analyzed in detail and observations will be made on the practical applications of these systems. Here, we can only forestall that RNS with MI are very suitable for approximate arithmetic, where they retain the modularity and speed of residue systems.

3.1 - ADDITION

In an RNS with MI of radices $\{m_1, m_2, \ldots, m_t, m_{t+1}, \ldots, m_n\}$, $\mu = \Pi_{i=1}^{t} m_i$ and $P = \Pi_{i=t+1}^{n} m_i$, suppose that two integers $X \equiv \{R_X, I_X\}$ and $Y \equiv \{R_Y, I_Y\}$ are given with:

$$\begin{aligned} X &= R_X + \mu I_X \qquad R_X = |X|_\mu \qquad I_X = \left\lfloor \frac{X}{\mu} \right\rfloor \\ Y &= R_Y + \mu I_Y \qquad R_Y = |Y|_\mu \qquad I_Y = \left\lfloor \frac{Y}{\mu} \right\rfloor \end{aligned} \tag{12}$$

Their sum:

$$S = X + Y = R_X + R_Y + \mu\,(I_X + I_Y) \tag{13}$$

has the RNS representation with MI:

$$S \equiv \{R_S, I_S\} \tag{14}$$

where

$$R_S = |S|_\mu = \left|R_X + R_Y + \mu(I_X + I_Y)\right|_\mu = |R_X + R_Y|_\mu \tag{15}$$

coincides with the modμ sum of residue components of the operands while

$$I_S = \left\lfloor \frac{S}{\mu} \right\rfloor = I_X + I_Y + \left\lfloor \frac{R_X + R_Y}{\mu} \right\rfloor = I_X + I_Y + \frac{R_X + R_Y - |R_X + R_Y|_\mu}{\mu} \tag{16}$$

may differ by "1" from the sum of magnitude indexes of X and Y.

Example 4.

In the RNS with MI system of radices $m_1 = 7, m_2 = 9, m_3 = 11, m_4 = m_t = 13, m_5 = m_{t+1} = m_n = 8$ *, let us consider two integers:*

$$X \equiv \{6,1,4,0,3\} = 35,776$$

$$Y \equiv \{1,3,4,7,0\} = 1,632$$

Adding the digits of the representations separately :

$$X + Y \equiv \{0,4,8,7,3\} = 28,399$$

does not provide the correct result as

$$R_X + R_Y \equiv \{6,1,4,0\} + \{1,3,4,7\} = 8749 + 1632 > \mu = 9009$$

In fact, from equality (16):

$$I_S = I_X + I_Y + 1 = 4$$

i.e.,

$$X + Y \equiv \{0,4,8,7,4\} = 37,408$$

Previous properties imply that RNS with MI are not closed under addition, i.e., the representation which is obtained by adding separately the residue and MI components of operands does not coincide with the representation of the sum. To obtain the correct result, it is necessary to evaluate expression (16); this implies converting the residue components to a weighted system representing magnitude index or, alternatively, an extension of the residue range in order to detect overflow occurrences from the range $[0, \mu)$.

However, a "modular" addition can be performed if an appropriate extension of both the residue and the MI ranges is provided. In fact, it is easily seen from equality (13) that adding residues and MI components separately guarantees a correct result; of

course, this result will not be expressed in the original notation, i.e., according to (15) and (16). This solution avoids conversion processes and may prove useful in several applications, as has been extensively treated in [28].

Example 5.

Given the number system of Example 4, let us suppose that an additional modulus $m_0 = 2$ is used to extend the residue range μ=9009. The representations of integers X = 35,776 and Y = 1,632 then become:

$X \equiv \{0,6,1,4,0,3\}$

$Y \equiv \{0,1,3,4,7,0\}$

Adding the representations digit-by-digit yields:

$X + Y \equiv \{0,0,4,8,7,3\} = 37,408$

and the result is obtained according to equality (13).

3.2 - MULTIPLICATION

Let $X \equiv \{R_X, I_X\}$ and $Y \equiv \{R_Y, I_Y\}$ be two integers represented in the RNS with MI of radices $\{m_1, m_2, \ldots, m_t, m_{t+1}, \ldots, m_n\}$, $\mu = \Pi_{i=1}^{t} m_i$ and $P = \Pi_{i=t+1}^{n} m_i$. Then relations (12) hold and, computing their product, we obtaine:

$$XY = \mu^2 I_X I_Y + \mu (I_X R_Y + I_Y R_X) + R_X R_Y \qquad (17)$$

whereas the representation of XY in the same system will take the form:

$$XY = \mu I_{XY} + R_{XY}$$

where:

$$R_{XY} = |XY|_\mu \qquad I_{XY} = \left\lfloor \frac{XY}{\mu} \right\rfloor \qquad (18)$$

and, substituting for XY, as suggested by (17), it follows that:

$$R_{XY} = |R_X R_Y|_\mu \tag{19}$$

$$I_{XY} = \left\lfloor \frac{\mu^2 I_X I_Y + \mu I_X R_Y + \mu I_Y R_X + R_X R_Y}{\mu} \right\rfloor = \mu I_X I_Y + I_X R_Y + I_Y R_X + \left\lfloor \frac{R_X R_Y}{\mu} \right\rfloor \tag{20}$$

As for addition, computing the residue component of the product representation is immediate. Unfortunately, even in the hypothesis of system redundancy, it is much more complicated to obtain the MI component than in addition, and a significant result cannot be obtained without a residue-to-weighted conversion procedure.

Effective solutions which circumvent lengthy intermodular procedures (conversions) can be obtained for certain applications provided that appropriate sets of radices are considered. To give a simple example, we consider the case where:

i) both I_X and I_Y are represented in a weighted range P which does not exceed the smallest residue modulus; this assumption avoids converting the magnitude indexes of operands as:

$$|I_X|_{m_i} = I_X \qquad \text{and} \qquad |I_Y|_{m_i} = I_Y \tag{21}$$

for any i=1,2,.....,t.

ii) both residue and MI ranges are extended to contain products $R_X R_Y$ and $I_X I_Y$, respectively.

In these hypotheses, product XY can be obtained in a slightly more complicated notation starting from equality (17); in fact, $R_X R_Y$ and $I_X I_Y$ can be computed in their original notations and they are assigned weights "1" and "μ^2 " while $I_X R_Y + I_Y R_X$ (of weight μ) is easily computed in the residue range without any conversion (21).

Example 6

In the RNS with MI system of radices $m_1 = 13, m_2 = m_t = 17, m_3 = m_{t+1} = m_n = 12$, *let*

$$X = 1711 \equiv \{R_X = |1711|_{221}, I_X = 7\} = \{8,11,7\}$$

$$Y = 814 \equiv \{R_Y = |814|_{221}, I_Y = 3\} = \{8,15,3\}$$

be two integers represented in the given system. As conditions (21) are satisfied, product XY can be computed by extending the residue range with additional moduli $m_{2+1}= 18$ *and* $m_{2+2}= 19$ *and the single-digit, MI range so that the product* $I_X I_Y$ *can be represented (this is equivalent to substituting* m_n *with a greater radix). In the extended system, the representations of previous numbers X and Y will become:*

$$X = 1711 \equiv \{R_X = |1711|_{221}, I_X = 7\} = \{8,11,1,1,7\}$$

$$Y = 814 \equiv \{R_Y = |814|_{221}, I_Y = 3\} = \{8,15,4,16,3\}$$

and computing terms $R_X R_Y$, $I_X R_Y + I_Y R_X$ *and* $I_X I_Y$ *separately will give:*

i) $R_X R_Y = \{8,11,1,1\}.\{8,15,4,16\} = \{12,12,4,16\} = 24,764$

ii) $I_X R_Y + I_Y R_X = \{7,7,7,7\}.\{8,15,4,16\} + \{3,3,3,3\}.\{8,11,1,1\} = \{2,2,13,1\} = 1549$

iii) $I_X I_Y = 21$

where i), ii) and iii) have weights "1", "μ*" and "*μ^2*", respectively. The correctness of these results is proved from equality (17); in fact:*

$$1711.814 = XY = XY = \mu^2 I_X I_Y + \mu (I_X R_Y + I_Y R_X) + R_X R_Y =$$
$$= \mu^2 .21 + \mu .1549 + 24764 = 1392,754.$$

3.3 - SCALING BY A PRODUCT OF RADICES

Scaling is the process of dividing a number X by a constant K (*the scaling factor*). With integer numbers, it is also assumed that the procedure is complemented with a rounding down estimation of the result, i.e.,

$$X_S = \left\lfloor \frac{X}{K} \right\rfloor$$

represents the result of scaling.

In the following, we will limit our consideration to the case where K=m is a product of one or more radices of the system.

In the RNS with MI of radices $\{m_1, m_2, \ldots, m_t, m_{t+1}, \ldots, m_n\}$, $\mu = \Pi_{i=1}^{t} m_i$ and $P = \Pi_{i=t+1}^{n} m_i$, consider an integer $X \equiv \{R_X, I_X\}$, with:

$$X = R_X + \mu I_X \qquad R_X = |X|_\mu \qquad I_X = \left\lfloor \frac{X}{\mu} \right\rfloor$$

and let $X_S \equiv \{R_S, I_S\}$ be the representation in the given number system of the scaled integer $\left\lfloor \frac{X}{m} \right\rfloor$:

$$X_S = \left\lfloor \frac{X}{m} \right\rfloor = R_S + \mu I_S \qquad R_S = \left| \left\lfloor \frac{X}{m} \right\rfloor \right|_\mu \qquad I_S = \left\lfloor \frac{\left\lfloor \frac{X}{m} \right\rfloor}{\mu} \right\rfloor \tag{22}$$

where

$$m = m_R\, m_I$$

$$m_R = \Pi_{i=1}^{v} m_{ki}$$

$$m_{ki} \in \{m_1, m_2, \ldots, m_t\}$$

$$m_I = \Pi_{j=1}^{u} m_{hj}$$

$$m_{hj} \in \{m_{t+1}, \ldots, m_n\}$$

Observing that:

$$\left\lfloor \frac{X}{m} \right\rfloor = \left\lfloor \frac{R_X + \mu I_X}{m} \right\rfloor \tag{23}$$

and comparing equalities (22) and (23), it follows:

$$R_S = \left| \left\lfloor \frac{R_X + \mu I_X}{m} \right\rfloor \right|_\mu \tag{24}$$

$$I_S = \left\lfloor \frac{\left\lfloor \frac{R_X + \mu I_X}{m} \right\rfloor}{\mu} \right\rfloor \qquad (25)$$

Equalities (24) and (25) can be given a different formulation, remembering that the following properties, whose proofs are given in the Appendix, hold.

Property 1

For any integer X and positive integers A, B.

$$\left\lfloor \frac{\left\lfloor \frac{X}{A} \right\rfloor}{B} \right\rfloor = \left\lfloor \frac{X}{AB} \right\rfloor$$

Property 2

For any integer X and positive integers A, B.

$$|A\,X\,|_{AB} = A\,|X\,|_B$$

Property 3

For any integer X , positive integers A, Y and $0 \le B < A$.

$$\left\lfloor \frac{A\,X + B}{A\,Y} \right\rfloor = \left\lfloor \frac{X}{Y} \right\rfloor$$

From equality (24), recalling Properties 1 and 2 and denoting:

$$R_S^* = \left\lfloor \frac{R_X}{m_R} \right\rfloor$$

$$I_S^* = \left\lfloor \frac{I_X}{m_I} \right\rfloor$$

which may be easily computed in the residue and MI ranges, respectively, we derive:

$$R_S = \left|\left\lfloor \frac{R_X+\mu I_X}{m} \right\rfloor\right|_\mu = \left|\left\lfloor \frac{\left|\frac{R_X+\mu I_X}{m_R}\right|}{m_I} \right\rfloor\right|_\mu = \left|\left\lfloor \frac{R_S^*+\frac{\mu}{m_R} I_X}{m_I} \right\rfloor\right|_\mu =$$

$$= \left|\left\lfloor \frac{R_S^*+\frac{\mu}{m_R} m_I I_S^*+\frac{\mu}{m_R}|I_X|_{m_I}}{m_I} \right\rfloor\right|_\mu = \left|\frac{\mu}{m_R} I_S^* + \left\lfloor \frac{R_S^*+\frac{\mu}{m_R}|I_X|_{m_I}}{m_I} \right\rfloor\right|_\mu = \tag{26}$$

$$= \left|\frac{\mu}{m_R}|I_S^*|_{m_R} + \left\lfloor \frac{R_S^*+\frac{\mu}{m_R}|I_X|_{m_I}}{m_I} \right\rfloor\right|_\mu = \frac{\mu}{m_R}|I_S^*|_{m_R} + \left\lfloor \frac{R_S^*+\frac{\mu}{m_R}|I_X|_{m_I}}{m_I} \right\rfloor$$

where the last equality originates from the observation that:

$$\frac{\mu}{m_R}|I_S^*|_{m_R} + \left\lfloor \frac{R_S^*+\frac{\mu}{m_R}|I_X|_{m_I}}{m_I} \right\rfloor \le \frac{\mu}{m_R}(m_R-1) + \left\lfloor \frac{\frac{\mu}{m_R}-1+\frac{\mu}{m_R}(m_I-1)}{m_I} \right\rfloor = \mu - 1$$

Similarly, from Properties 3 and 1:

$$I_S = \left\lfloor \frac{\left\lfloor \frac{R_X+\mu I_X}{m} \right\rfloor}{\mu} \right\rfloor = \left\lfloor \frac{\mu I_X + R_X}{\mu m} \right\rfloor = \left\lfloor \frac{I_X}{m} \right\rfloor = \left\lfloor \frac{I_S^*}{m_R} \right\rfloor \tag{27}$$

There are no problems in computing I_S in the weighted part of the representation. On the contrary, in the hopeful hypothesis that m_I has the multiplicative inverse mod μ, determining R_S means that I_S^* and $|I_X|_{m_I}$ must be converted to the residue notation and several residue multiplicative and additive steps must be performed to obtain R_S. However, Property 1 suggests that the scaling of an integer X can be corrrectly carried out by means of a two step procedure, as follows:

$$X_S = \left\lfloor \frac{X}{m} \right\rfloor = \left\lfloor \frac{X}{m_R m_I} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{X}{m_R} \right\rfloor}{m_I} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{X}{m_I} \right\rfloor}{m_R} \right\rfloor \tag{28}$$

The importance of relation (28) is based upon consistent simplifications in computing R_S; these are possible whenever the scaling factor m identifies with a product of only RNS moduli or MI radices. In fact, from (26) and (27):

the case where:

$m = m_R$ *i.e.,* $m_I = 1$

gives:

$$R_S = \frac{\mu}{m_R}|I_X|_{m_R} + R_S^* \qquad (26')$$

and

$$I_S = \left\lfloor \frac{I_X}{m_R} \right\rfloor \qquad (27')$$

whereas the case:

$m = m_I$, $m_R = 1$

yields:

$$R_S = \left\lfloor \frac{R_X + \mu|I_X|_{m_I}}{m_I} \right\rfloor = \frac{R_X + \mu|I_X|_{m_I} - |R_X + \mu I_X|_{m_I}}{m_I} \qquad (26'')$$

$$I_S = I_S^* \qquad (27'')$$

As a conclusion, for the general case where $m = m_R\, m_I$, letting:

$$X_{S,R} = \left\lfloor \frac{X}{m_R} \right\rfloor = R_{S,R} + \mu I_{S,R} \qquad (29)$$

$$X_{S,I} = \left\lfloor \frac{X}{m_I} \right\rfloor = R_{S,I} + \mu I_{S,I} \qquad (30)$$

where pairs $(R_{S,R}, I_{S,R})$ and $(R_{S,I}, I_{S,I})$ coincide with pairs (R_S, I_S) in (26', 27') and (26", 27"), respectively, relation (28) will take the form:

$$X_S = \left\lfloor \frac{X_{S,R}}{m_I} \right\rfloor = \left\lfloor \frac{X_{S,I}}{m_R} \right\rfloor \qquad (28')$$

Example 7

In the RNS with MI system of radices $m_1 = 7$, $m_2 = 9$, $m_3 = 11$, $m_4 = m_t = 13$, $m_5 = m_{t+1} = 4$, $m_6 = m_n = 8$ *(see Example 3), considering integer* $X = 98{,}711 \equiv$

{4,8,8,2,2,2} and supposing that we wish to scale X by factor m = m1 m3 m6 =616 (m_R=77, m_I=8), we will first compute $X_{S,R} \equiv \{R_{S,R}, I_{S,R}\}$ from (26') and (27'), as follows:

Step 1.1:

$$R_{S,R} = \frac{\mu}{m_R} |I_X|_{m_R} + \left\lfloor \frac{R_X}{m_R} \right\rfloor$$

Observing that:

$$\left\lfloor \frac{R_X}{m_R} \right\rfloor = \frac{R_X - |R_X|_{m_R}}{m_R}$$

we have:

$(R_X -$	$\{-,8,-,2\}$
$-\ |R_X|_{m_1 m_2}) \times$	$-\{-,2,-,9\} = \{-,6,-,6\} \times$
$\times \left\lvert \frac{1}{m_1 m_3} \right\rvert_{m_2 m_4} =$	$\times \{-,2,-,12\} =$
$=$	$=\{-,3,-,7\}$

where computations are performed mod μ/m_R. Extending to the original residue range μ will give:

	$\{6,3,1,7\} = 111$
$+\ m_2 m_4 \ |I_X|_{m_R} =$	$\{1,0,4,0\}$
$=$	$\{0,3,5,7\} = 1281$

Step 1.2:

$$I_{S,R} = \left\lfloor \frac{I_X}{m_R} \right\rfloor = 0$$

i.e.,

$$X_{S,R} \equiv \{R_{S,R}, I_{S,R}\} = \{0, 3, 5, 7, 0, 0\}$$

The second (and final) step of the procedure will perform scaling of $X_{S,R}$ by factor $m_I = m_6 = 8$, according to equations (26") and (27").

Step 2.1:

$$R_S = \frac{R_{S,R} + \mu |I_{S,R}|_{m_I} - |R_{S,R} + \mu I_{S,R}|_{m_I}}{m_I}$$

As $(m_I, \mu)=1$, there exists the multiplicative inverse of m_I mod μ and, consequently, computations in the residue range μ are allowed. So, it is obtained:

$$(R_{S,R} + \{0,3,5,7\} +$$

$$+ \mu |I_{S,R}|_{\mu_I} - + \{0,0,0,0\} = \{0,3,5,7\} -$$

$$- |R_{S,R} + \mu I_{S,R}|_{m_I}) = - \{1,1,1,1\} =$$

$$= = \{6,2,4,6\} \times$$

$$\times \left|\frac{1}{m_I}\right|_{\mu} = \times \{1,8,7\ 5\} =$$

$$= = \{6,7,6,4\} = 160$$

Step 2.2

$$I_S = \left\lfloor \frac{I_{S,R}}{m_I} \right\rfloor = 0$$

i.e.,

$$X_S \equiv \{R_S, I_S\} = \{6, 7, 6, 4, 0, 0\} = 160$$

is the correct result of scaling 98,711 by 7.11.8=616.

3.4 - INTEGER DIVISION

We refer again to the RNS with MI of radices $\{m_1, m_2, \ldots, m_t, m_{t+1}, \ldots, m_n\}$, $\mu = \Pi_{i=1}^{t} m_i$ and $P = \Pi_{i=t+1}^{n} m_i$, and suppose that two positive integers $X \equiv \{R_X, I_X\}$ and $Y \equiv \{R_Y, I_Y\} \neq 0$ are given with:

$$X = R_X + \mu I_X \qquad R_X = |X|_\mu \qquad I_X = \left\lfloor \frac{X}{\mu} \right\rfloor$$

$$Y = R_Y + \mu I_Y \qquad R_Y = |Y|_\mu \qquad I_Y = \left\lfloor \frac{Y}{\mu} \right\rfloor$$

For positive integers, dividing X by Y is equivalent to determining the integer quotient:

$$Q = \left\lfloor \frac{X}{Y} \right\rfloor$$

and the remainder

$$R = X - QY$$

For the sake of conciseness, our attention will be limited to the integer quotient Q. This choice is not limiting as, if necessary, the computation of remainder R does not present any real difficulties.

In the number system under consideration, Q will be given the representation $Q \equiv \{R_Q, I_Q\}$ where:

$$Q = R_Q + \mu I_Q \qquad R_Q = |Q|_\mu \qquad I_Q = \left\lfloor \frac{Q}{\mu} \right\rfloor \tag{31}$$

Recalling that:

$$Q = \left\lfloor \frac{X}{Y} \right\rfloor = \left\lfloor \frac{R_X + \mu I_X}{R_Y + \mu I_Y} \right\rfloor \tag{32}$$

and comparing with (31), it is seen :

$$I_Q = \left\lfloor \frac{\lfloor X/Y \rfloor}{\mu} \right\rfloor = \left\lfloor \frac{X}{\mu Y} \right\rfloor = \left\lfloor \frac{\mu I_X + R_X}{\mu(\mu I_Y + R_Y)} \right\rfloor \tag{33}$$

$$R_Q = \left\| \frac{\mu I_X + R_X}{\mu I_Y + R_Y} \right\|_\mu \tag{34}$$

Equalities (33) and (34) show that evaluating the integer quotient is, in the general case, a very time-consuming procedure which implies residue-to-weighted system conversions and vice-versa, as both residue and MI components of the result require a full knowledge of operands.

However, in the hypothesis that $I_Y \neq 0$, it will be shown that good approximations of (33) and (34) can be achieved quickly together with their uncertainty range; in most situations these procedures lead to exact values of I_Q and R_Q. On the contrary, when $I_Y = 0$, significant simplifications are not possible.

In the hypothesis that $I_Y \neq 0$, it can be observed that the fractions appearing in equalities (33) and (34) satisfy the following inequalities, regardless of the actual values of residue components R_X and R_Y:

$$\frac{\mu I_X}{\mu(\mu I_Y + \mu - 1)} \leq \frac{\mu I_X + R_X}{\mu(\mu I_Y + R_Y)} \leq \frac{\mu I_X + \mu - 1}{\mu^2 I_Y}$$

$$\frac{\mu I_X}{\mu I_Y + \mu - 1} \leq \frac{\mu I_X + R_X}{\mu I_Y + R_Y} \leq \frac{\mu I_X + \mu - 1}{\mu I_Y}$$

and, consequently:

$$\left\lfloor \frac{\mu I_X}{\mu(\mu I_Y + \mu - 1)} \right\rfloor \leq \left\lfloor \frac{\mu I_X + R_X}{\mu(\mu I_Y + R_Y)} \right\rfloor \leq \left\lfloor \frac{\mu I_X + \mu - 1}{\mu^2 I_Y} \right\rfloor \tag{35}$$

$$\left\lfloor \frac{\mu I_X}{\mu I_Y + \mu - 1} \right\rfloor \leq \left\lfloor \frac{\mu I_X + R_X}{\mu I_Y + R_Y} \right\rfloor \leq \left\lfloor \frac{\mu I_X + \mu - 1}{\mu I_Y} \right\rfloor \tag{36}$$

Starting from the magnitude indexes of operands only, inequalities (35) and (36) show that it is possible to determine the intervals to which I_Q and R_Q belong; this

enables fast computation of approximate values for I_Q and R_Q with maximum errors Δ_I and Δ_R (mod μ) , respectively, where:

$$\Delta_I = \left\lfloor \frac{\mu I_X + \mu - 1}{\mu^2 I_Y} \right\rfloor - \left\lfloor \frac{\mu I_X}{\mu(\mu I_Y + \mu - 1)} \right\rfloor \tag{37}$$

$$\Delta_R = \left\lfloor \frac{\mu I_X + \mu - 1}{\mu I_Y} \right\rfloor - \left\lfloor \frac{\mu I_X}{\mu I_Y + \mu - 1} \right\rfloor \tag{38}$$

Expressions (35) and (36) can be further simplified by means of the previous Property 3 and the following Property 4, whose proof is also reported in Appendix.

Property 4

For any positive integers A, Y and X<A:

$$\left\lfloor \frac{AX}{AY + A - 1} \right\rfloor = \left\lfloor \frac{X}{Y+1} \right\rfloor$$

In our case, condition X<A of Property 4 is equivalent to assuming that inequality $I_X < \mu$ is satisfied for any I_X, i.e.,

$$\Pi_{i=1}^{t} m_i > \Pi_{i=t+1}^{n} m_i$$

It is worth noting that this assumption cannot be regarded as a limiting condition since RNS with MI systems have, as a prime goal, the drastic reduction of the weighted portion of number representation. As a conclusion, it is obtained:

$$\left\lfloor \frac{I_X}{\mu I_Y + \mu - 1} \right\rfloor \le I_Q \le \left\lfloor \frac{I_X}{\mu I_Y} \right\rfloor \tag{35'}$$

$$\left\lfloor \frac{I_X}{I_Y + 1} \right\rfloor \le R_Q = \left\| \left\lfloor \frac{\mu I_X + R_X}{\mu I_Y + R_Y} \right\rfloor \right\|_\mu = \left\lfloor \frac{\mu I_X + R_X}{\mu I_Y + R_Y} \right\rfloor \le \left\lfloor \frac{I_X}{I_Y} \right\rfloor \tag{36'}$$

$$\Delta_I = \left\lfloor \frac{I_X}{\mu I_Y} \right\rfloor - \left\lfloor \frac{I_X}{\mu I_Y + \mu - 1} \right\rfloor = 0 \tag{37'}$$

$$\Delta_R = \left\lfloor \frac{I_X}{I_Y} \right\rfloor - \left\lfloor \frac{I_X}{I_Y + 1} \right\rfloor \tag{38'}$$

or, equivalently:

$$I_Q = 0 \qquad R_Q = \left\lfloor \frac{I_X}{I_Y+1} \right\rfloor + k \quad k \varepsilon \{0, \ldots, \Delta_R\} \tag{39}$$

Example 8

In the RNS with MI system of radices $m_1 = 5$ $m_2 = 7$ $m_3 = 8$, $m_4 = m_t = 9$, $m_5 = m_{t+1} = 4$, $m_6 = 8$, $m_7 = m_n = 16$, $\mu = 2520$ and $P=512$, consider integers $X = 978{,}711 \equiv \{R_X=951, I_X=388\} = \{1,6,7,6,0,4,12\}$ and $Y = 105{,}012 \equiv \{R_Y=1692, I_Y=41\}$. As $P<\mu$, computation of their integer quotient:

$$Q = \left\lfloor \frac{X}{Y} \right\rfloor$$

is performed from equalities (39), i.e.,

$$I_Q = 0 \qquad R_Q = \left\lfloor \frac{I_X}{I_Y+1} \right\rfloor = \left\lfloor \frac{388}{42} \right\rfloor = 9 \qquad \text{with} \quad \Delta_R = 0$$

where R_Q is easily computed in weighted notation.

Here, $\Delta_R = 0$ and preceding relations provide the correct value of Q without any approximation error. In order to express the result in the original representation, it is necessary to convert R_Q from weighted to residue notation, thus obtaining:

$$Q = \{4,2,1,0,0,0,0\}$$

The instance which has been reported in the example, where the exact value of Q has been obtained, does not represent a singular occurrence as, from (38'), it can be immediately realized that $\Delta_R = 0$ in most applications.

The case where $I_Y=0$ can be clarified starting from equalities (33) and (34), from which we can derive:

$$\left\lfloor \frac{\mu I_X}{\mu(\mu-1)} \right\rfloor \le \left\lfloor \frac{\mu I_X + R_X}{\mu(\mu I_Y + R_Y)} \right\rfloor \le \left\lfloor \frac{\mu I_X + \mu - 1}{\mu} \right\rfloor = I_X \tag{35"}$$

$$\left\lfloor \frac{\mu I_X}{\mu-1} \right\rfloor \le \left\lfloor \frac{\mu I_X + R_X}{\mu I_Y + R_Y} \right\rfloor \le \left\lfloor \frac{\mu I_X + \mu - 1}{1} \right\rfloor = \mu I_X + \mu - 1 \tag{36"}$$

i.e., I_Q and R_Q may be determined with errors:

$$\Delta_I = I_X - \left\lfloor \frac{I_X}{\mu-1} \right\rfloor \qquad (37")$$

$$\Delta_R = \mu I_X + \mu - 1 - \left\lfloor \frac{\mu I_X}{\mu-1} \right\rfloor \qquad (38")$$

Equalities (37") and (38") preclude any possibility of performing approximate evaluations of integer quotient Q, as Δ_I and Δ_R equal the MI and RNS range of the representation..From a practical point of view, the best solution which could be suggested in this situation consists in:

i) multiplying both operands by a factor A:

$X' = A\,X$

$Y' = A\,Y$

such that $I_Y \neq 0$;

ii) applying (39) to X' and Y' to find approximate value of integer quotient Q as:

$$Q = \left\lfloor \frac{X}{Y} \right\rfloor = \left\lfloor \frac{AX}{AY} \right\rfloor$$

APPENDIX

PROOFS OF PROPERTIES 1-4

Property 1:

$$\left\lfloor \frac{\lfloor \frac{X}{A} \rfloor}{B} \right\rfloor = \left\lfloor \frac{X}{AB} \right\rfloor$$

for any integer X and positive integers A,B.

Proof:

Any number X can be expressed as:

$$X = A\left\lfloor \frac{X}{A} \right\rfloor + |X|_A$$

or, analogously:

$$X = AB\left\lfloor \frac{X}{AB} \right\rfloor + |X|_{AB}$$

where A and AB are positive integers. Comparing the above equalities gives:

$$\frac{\lfloor \frac{X}{A} \rfloor}{B} + \frac{|X|_A}{AB} = \left\lfloor \frac{X}{AB} \right\rfloor + \frac{|X|_{AB}}{AB}$$

and

$$\left\lfloor \frac{\lfloor \frac{X}{A} \rfloor}{B} \right\rfloor = \left\lfloor \left\lfloor \frac{X}{AB} \right\rfloor + \frac{|X|_{AB} - |X|_A}{AB} \right\rfloor = \left\lfloor \frac{X}{AB} \right\rfloor + \left\lfloor \frac{|X|_{AB} - |X|_A}{AB} \right\rfloor$$

Recalling that, for any X:

$$|X|_{AB} \geq |X|_A$$

it follows:

$$0 \leq |X|_{AB} - |X|_A < AB$$

and Property 1 is proved as:

$$\left\lfloor \frac{|X|_{AB} - |X|_A}{AB} \right\rfloor = 0$$

Property 2:

$|A\,X|_{A\,B} = A\,|X|_B$

for any integer X and positive integers A, B.

Proof:

The property is immediately derived from equalities:

$A\,|X|_B = |A\,|X|_B|_{AB} = |A(X+kB)|_{AB} = |AX+kAB|_{AB} = |AX|_{AB}$

where k is an appropriate integer.

Property 3:

$$\left\lfloor \frac{A\,X\,+B}{A\,Y} \right\rfloor = \left\lfloor \frac{X}{Y} \right\rfloor$$

for any integer X, positive integers A, Y and $0 \le B < A$.

Proof:

$$\left\lfloor \frac{A\,X\,+\,B}{A\,Y} \right\rfloor = \left\lfloor \frac{AY\left\lfloor \frac{X}{Y} \right\rfloor + A|X|_Y + B}{AY} \right\rfloor = \left\lfloor \frac{X}{Y} \right\rfloor + \left\lfloor \frac{A|X|_Y + B}{AY} \right\rfloor$$

Observing that:

$0 \le A|X|_Y + B \le A(Y-1) + A-1 = AY - A + A - 1 = AY - 1$

it follows:

$$\left\lfloor \frac{A|X|_Y + B}{AY} \right\rfloor = 0$$

and proof is completed.

Property 4:

$$\left\lfloor \frac{A\,X}{AY+A-1} \right\rfloor = \left\lfloor \frac{X}{Y+1} \right\rfloor$$

for any positive integers A, Y and $X < A$.

Proof:

$$\left\lfloor \frac{AX}{AY+A-1} \right\rfloor = \left\lfloor \frac{A(Y+1)\left\lfloor \frac{X}{Y+1} \right\rfloor + A|X|_{Y+1}}{AY+A-1} \right\rfloor =$$

$$= \left\lfloor \frac{A(Y+1)\left\lfloor \frac{X}{Y+1} \right\rfloor - \left\lfloor \frac{X}{Y+1} \right\rfloor + \left\lfloor \frac{X}{Y+1} \right\rfloor + A|X|_{Y+1}}{A(Y+1)-1} \right\rfloor = \left\lfloor \frac{X}{Y+1} \right\rfloor + \left\lfloor \frac{A|X|_{Y+1} + \left\lfloor \frac{X}{Y+1} \right\rfloor}{A(Y+1)-1} \right\rfloor$$

As the following inequalities:

$$\frac{A|X|_{Y+1} + \left\lfloor \frac{X}{Y+1} \right\rfloor}{A(Y+1)-1} \leq \frac{AY+A-A+\left\lfloor \frac{X}{Y+1} \right\rfloor}{A(Y+1)-1} =$$

$$= \frac{A(Y+1)-1+1-A+\left\lfloor \frac{X}{Y+1} \right\rfloor}{A(Y+1)-1} = 1 - \frac{A-1-\left\lfloor \frac{X}{Y+1} \right\rfloor}{A(Y+1)-1} < 1$$

are verified, it is concluded that:

$$\left\lfloor \frac{A|X|_{Y+1} + \left\lfloor \frac{X}{Y+1} \right\rfloor}{A(Y+1)-1} \right\rfloor = 0$$

and property is demonstrated.

REFERENCES

[1] H.L. Garner , "The residue number system", IRE Trans. Electronic Computers, vol. EC-8, pp. 140-147, June 1959

[2] N.S. Szabo and R.I. Tanaka, *Residue Arithmetic and its Applications to Computer Technology*, New York, McGraw-Hill, 1967

[3] F.J. Taylor , "Residue Arithmetic: A Tutorial with examples", Computer, vol. 17, n.5, pp. 50-63, May 1984

[4] A. Sasaki, "The Basis for Implementation of Additive Operations in the Residue Number System", IEEE Trans. Comput., vol. C-17, pp. 1066-1073, Nov. 1968

[5] D.K. Banerji, "A Novel Implementation Method for Addition and Subtraction in Residue Number Systems", IEEE Trans. Comput., vol. C-23, pp. 106-109, Jan. 1974

[6] G.A. Jullien, "Residue Number Scaling and Other Operations Using ROM Arrays", IEEE Trans. Comput., vol. C-27, pp. 325-336, Apr. 1978

[7] W.K. Jenkins , "A Comparison of Residue Number Multipliers and 2's Complement Multipliers implemented by Stored Multiplication Tables", Proc. 1978 IEEE Intern. Symp. Circuits Syst., pp. 297-301, May 1978

[8] D.P. Agrawal and T.R.N. Rao , "Modulo (2^n+1) Arithmetic Logic", IEE J. Electronic Circuits and Systems, vol. 2, pp. 186-188, Nov. 1978

[9] D.P. Agarwal , "Modulo 2**n+1 arithmetic Logic", IEE J. Electronic Circuits and Systems, vol. 2. n.6, pp. 186-188, Nov. 1978

[10] G.A. Jullien, "Using ROM arrays to implement computer arithmetic", Proc. 1979 Int. Conf. Micro and Mini Computers, Houston, TX, Nov. 1979

[11] M.A. Soderstrand and C. Vernia, "A High-Speed Low-Cost Modulo P_i Multiplier with RNS Arithmetic Applications", Proc. IEEE, vol. 68, pp. 529-532, Apr. 1980

[12] A.S. Ramnarayan , "Practical realization of Mod p, p prime multiplier", Electron. Lett., vol. 19, n.15, pp. 466-467, June 1980

[13] G.A. Jullien , "Implementation of Multiplication, Modulo a Prime Number, with Applications to Number Theoretic Transforms", IEEE Trans. Comput., vol. C-29, pp. 899-905, Oct. 1980

[14] C.H. Huang, D.G. Peterson, H.E. Rauch, J.W. Teague and D.F. Frasher , "Implementation of fast digital processor using the residue number system", IEEE Trans. Circuits and Systems, vol. CAS-28, pp. 32-38, Jan. 1981

[15] F.J. Taylor and C.H. Huang , "An Autoscale Residue Multiplier", IEEE Trans. Comput., vol. C-31, pp. 321-325, Apr. 1982

[16] M.A. Soderstrand , "A New Hardware Implementation of Modulo Adders for Residue Number System", Proc. of the 26th Midwest symposium on Circuits and Systems, 1983, pp. 412-415

[17] W.K. Jenkins , "A Highly Efficient Residue-Combinatorial Architecture for Digital Filters", Proc. IEEE, vol. 66, pp. 700-702, June 1978

[18] F.J. Taylor , "Large Moduli Multipliers for Signal Processing", IEEE Trans. Circuits Systems, vol. CAS-28, pp. 731-736, July 1981

[19] G.A. Jullien and A. Bayoumi , "RNS modules for VLSI implementation of digital filters", Proc. 26th Midwest Symp. Circuits and Systems, Puebla, Mexico, pp. 403-407, Aug. 1983

[20] F. Barsi and P. Maestrini , "Application of residue arithmetic to recursive digital filters", Proc. 26th Midwest Symp. Circuits and Systems, Puebla, Mexico, Aug. 1983

[21] F.J. Taylor , "A VLSI residue arithmetic multiplier", IEEE trans. Comput., vol. C-31, n.6, pp. 540-546, June 1982

[22] M.A. Bayoumi, G.A. Jullien and W.C. Miller , "The Area-Time Ccomplexity of a VLSI Residue Number System Arithmetic Unit", Proc. 8th Conf. Information Sciences and Systems, Johns Hopkins University, March 1983

[23] G. Alia, F. Barsi and E. Martinelli , "A fast VLSI conversion between binary and residue systems", Inform. Proc. Lett., vol. 18, n. 3, pp. 141-145, March 1984

[24] G. Alia and E. Martinelli , "A VLSI algorithm for direct and reverse conversion from weighted binary number system and residue number system", IEEE Trans. Circuits and Systems, vol. CAS-31, pp. 1033-1039, Dec. 1984

[25] G. Alia and E. Martinelli , "The VLSI residue multiplication and its implication in the direct and reverse positional-to-residue conversion", IEI Internal Report B4-70, Pisa, Italy, Dec. 1986

[26] F. Barsi, "Residue Arithmetic in Binary Systems", IEI Internal Report B4-37, Pisa, Italy, Aug. 1988

[27] F. Barsi and P. Maestrini, "Arithmetic Codes in Residue Number Systems with Magnitude Index", IEEE Trans. Comput., vol. C-27, pp. 1185-1188, Dec. 1978

[28] G. Alia, F. Barsi and E. Martinelli , "Addition and Overflow Handling in a Class of Redundant RNS with Magnitude Index", IEI Internal Report B4-33, Pisa, Italy, Dec. 1987