BASE CONVERSION IN RESIDUE NUMBER SYSTEMS

Robert Todd Gregory
The University of Tennessee, Knoxville, Tennessee

and

David W. Matula
Southern Methodist University, Dallas, Texas

1. Introduction

We are concerned in this paper with the representation of an integer in a (multiple-modulus) residue number system and, in particular, with an algorithm for changing the base vector of the residue number system. Szabo´ and Tanaka [1, p.47] describe such an algorithm when each modulus of the second base vector is relatively prime to each modulus of the first base vector. However, we show that a much simpler algorithm exists if we allow the moduli of the second base vector to have factors in common with the moduli of the first base vector (even though the moduli of the second base vector are pairwise relatively prime among themselves).

Since the algorithm involves the use of "associated" residue and mixed-radix representations for integers, Section 2 contains an elementary survey of the terminology, notation, and theory behind these two types of representation. Section 3 contains the proofs of the basic theorems upon which our algorithm for residue base conversion is based along with a description of the algorithm. It also contains illustrative examples which demonstrate the power of the algorithm.

In this paper we lay the foundation for a subsequent paper in which we propose procedures for extending single-precision residue arithmetic to multiple-precision residue arithmetic.

2. Associated Residue and Mixed-radix Number Systems

Complete Systems of Residues

Let $\mathbf{R}$ denote the set of real numbers and $\mathbf{I}$ the set of integers. For every $x \in \mathbf{R}$ we use $\lfloor x \rfloor$ to denote the largest integer smaller than or equal to x, and for all $a,b \in \mathbf{I}$ we use (a,b) to denote the greatest common divisor of a and b.

It is well known that each integer is congruent modulo* m to exactly one of the integers in the set $\{0,1,2,\ldots,m-1\}$, and this fact provides $\mathbf{I}$ with exactly m disjoint subsets $\mathbf{S}_0,\mathbf{S}_1,\ldots,\mathbf{S}_{m-1}$ called the residue classes with respect to the modulus m. These residue classes have the following properties:

(i) $$\mathbf{I} = \bigcup_{j=0}^{m-1} \mathbf{S}_j$$

and

(ii) $a,b \in \mathbf{S}_j$ implies $a \equiv b \pmod m$ for $j = 0,1,\ldots,m-1$.

By selecting exactly one integer r_j from each residue class, $\mathbf{S}_j$, we have a set of m different integers $\{r_0,r_1,\ldots,r_{m-1}\}$, called a complete system of residues modulo m. Each r_j "represents" its residue class, and the individual r's are called residues modulo m.

There are infinitely many complete systems of residues for a given modulus m. However, we shall discuss only the two that are most widely used. Suppose $r,s \in \mathbf{I}$ and $r \equiv s \pmod m$. If

$$0 \le r < m, \qquad (2.1)$$

then we use the notation**

$$r = |s|_m, \qquad (2.2)$$

and call $|s|_m$ the residue of s modulo m in the complete system of residues, $\{0,1,2,\ldots,m-1\}$. We call this system the standard complete system of residues modulo m.

If, on the other hand, r lies in the range

$$\left\lfloor -\frac{m}{2} \right\rfloor < r \le \left\lfloor \frac{m}{2} \right\rfloor, \qquad (2.3)$$

then we use the notation

$$r = /s/_m, \qquad (2.4)$$

and call $/s/_m$ the residue of s modulo m in the complete system of residues, $\{r_0,r_1,\ldots,r_{m-1}\}$, with r_i satisfying (2.3) for all i. When m is odd, these residues are symmetric with respect to the origin, but when m is even, perfect symmetry is lost. For this reason, we shall restrict our use of (2.3) and (2.4) to the case where m is odd. A complete system of residues, based on the inequality (2.3) with m odd, is called balanced. (Szabo´ and Tanaka [1, p.113] use the term symmetric but allow m to be both odd and even.)

For the most part we shall discuss standard complete systems of residues in this paper. However, balanced complete systems of residues are also discussed in the literature and so we shall include remarks pertaining to balanced systems as it seems appropriate.

Residue Number Systems

Suppose we have two moduli m_1 and m_2. We call them relatively prime if $(m_1,m_2) = 1$ and redundant if $(m_1,m_2) \ge 2$. Consider the ordered n-tuple

$$\beta = \left[m_1,m_2,\ldots,m_n\right], \qquad (2.5)$$

whose components are the n (distinct) moduli $m_1,m_2,\ldots,m_n$. Assume that the moduli are pairwise relatively prime, that is, that

$$(m_i,m_j) = 1 \qquad i \ne j. \qquad (2.6)$$

If β in (2.5) satisfies (2.6), we call it a base vector for the residue number systems we are about to describe.

Let M_β be the product of the moduli in the base vector β, that is, let

$$M_\beta = \prod_{i=1}^{n} m_i. \qquad (2.7)$$

*We assume $m > 1$ throughout the paper.

**Our notation will generally follow the notation in [1].

For each integer s we call the (unique) n-tuple of residues

$$|s|_\beta = \left[|s|_{m_1}, |s|_{m_2}, \ldots, |s|_{m_n}\right] \qquad (2.8)$$

the standard residue representation of s with respect to the base vector β. The individual residues, $|s|_{m_i}$, are the residue digits of s with respect to β.

THEOREM (2.9)[†] [1, p.13]. Two integers s and t have the same standard residue representation with respect to β, that is, $|s|_\beta = |t|_\beta$, if and only if

$$s \equiv t \pmod{M_\beta}.$$

COROLLARY (2.10)[†]. The integers $|s|_{M_\beta}$ and s have the same standard residue representation with respect to β, that is, if

$$t = |s|_{M_\beta},$$

then $|t|_\beta = |s|_\beta$.

This means, then, that there is a one-to-one correspondence between integers in the range

$$0 \leq s < M_\beta \qquad (2.11)$$

and their standard residue representations with respect to the base vector β. The standard residue number system for the base vector β is the M_β-member set of standard residue representations

$$\mathbf{I}_\beta = \left\{|s|_\beta : s \varepsilon \mathbf{I}\right\}. \qquad (2.12)$$

Obviously, this is a finite number system.

In the residue number system $\mathbf{I}_\beta$ every integer s is represented by a unique n-tuple $|s|_\beta$ and the correspondence is one-to-one for those nonnegative integers less than M_β. This set of integers, $\{0,1,2,\ldots,M_\beta-1\}$, is called the range of $\mathbf{I}_\beta$ and is identical to the standard complete system of residues modulo M_β.

REMARK. If $\beta = [m_1, m_2, \ldots, m_n]$ contains only odd moduli, we can use (2.3) and (2.4) to define the balanced residue number system for β in a similar manner. In this case we represent s by the balanced residue representation

$$/s/_\beta = \left[/s/_{m_1}, /s/_{m_2}, \ldots, /s/_{m_n}\right], \qquad (2.13)$$

and define the balanced residue number system to be the set of balanced residue representations

$$\mathbf{B}_\beta = \left\{/s/_\beta : s \varepsilon \mathbf{I}\right\}. \qquad (2.14)$$

In $\mathbf{B}_\beta$ every integer s is represented by a unique n-tuple of the form (2.13) and the correspondence is one-to-one for those integers in the range

$$-\frac{M_\beta}{2} < s < \frac{M_\beta}{2}. \qquad (2.15)$$

Since $\mathbf{I}_\beta$ and $\mathbf{B}_\beta$, along with their ranges (2.11) and (2.15) respectively, are all M_β-member sets we have a one-to-one correspondence between these two residue number systems. Note that for any $s \varepsilon \mathbf{I}$, conversion from the standard representation $|s|_\beta$ to the balanced representation $/s/_\beta$ is affected by

$$/s/_{m_i} = \begin{cases} |s|_{m_i} & \text{if } 0 \leq |s|_{m_i} < \frac{m_i}{2}, \\ |s|_{m_i} - m_i & \text{otherwise,} \end{cases} \qquad (2.16)$$

for i = 1,2,...,n, and the reverse conversion is similarly evident.

The Associated Mixed-radix Number System

We now introduce a mixed-radix number representation.* Consider the set of positive integers $p_1, p_2, \ldots, p_n$ called radices. Let $P = p_1 \, p_2 \cdots p_n$. It is well known [1, p.41] that any integer s in the range $0 \leq s < P$ can be expressed uniquely in the form

$$s = d_0 + d_1 p_1 + d_2 p_1 p_2 + \cdots + d_{n-1} p_1 p_2 \cdots p_{n-1}, \qquad (2.17)$$

where $d_0, d_1, \ldots, d_{n-1}$ are the standard mixed-radix digits satisfying

$$0 \leq d_i < p_{i+1} \qquad i = 0,1,\ldots,n-1. \qquad (2.18)$$

The digit sequence for s in this mixed-radix representation is denoted by

$$\left\langle s \right\rangle_{[p_1,p_2,\ldots,p_n]} = \left\langle d_0, d_1, \ldots, d_{n-1} \right\rangle_{[p_1,p_2,\ldots,p_n]}. \qquad (2.19)$$

We define the standard mixed-radix number system for the (ordered) radices $p_1, p_2, \ldots, p_n$ to be the set of digit sequences for s, in the range $0 \leq s < P$, of the form (2.19).

A special case occurs if $p_1 = p_2 = \ldots = p_n$, the familiar fixed-radix number system for which the radix ten provides the traditional example. Another special case occurs if $p_i = m_i$, for i = 1,2,...,n, where the integers $m_1, m_2, \ldots, m_n$ are the (ordered) moduli of the base vector β in (2.5). In this case we have the standard mixed-radix number system associated with $\mathbf{I}_\beta$. We call these two number systems associated number systems with respect to β.

REMARK. If we happen to be working with $\mathbf{B}_\beta$ (rather than with $\mathbf{I}_\beta$) we can introduce as its associated mixed-radix system a balanced mixed-radix number system. The only change necessary

[†] The product of the moduli, M_β, should be replaced in this theorem and its corollary, by the least common multiple of the moduli. However, we have assumed that the moduli in β are pairwise relatively prime and so M_β is automatically the least common multiple of the moduli, in this case.

*See, for example, [2, pp.25-27]

to accomplish this is to change the range for the mixed-radix digits to

$$-\frac{m_{i+1}}{2} < d_i < \frac{m_{i+1}}{2}, \qquad i = 0,1,\ldots,n-1. \qquad (2.20)$$

In this balanced system it is easily shown that there exists a unique representation for each integer s in the range

$$-\frac{M_\beta}{2} < s < \frac{M_\beta}{2}. \qquad (2.21)$$

Thus, the ranges for the standard mixed-radix number system and the balanced mixed-radix number system, for the same base vector β, both contain the same number of integers.

By including in the definition of a base vector β the stipulation that the moduli $m_1,m_2,\ldots,m_n$ must be pairwise relatively prime, we guarantee that M_β is the least common multiple of the moduli. This fortunate circumstance causes the ranges of the two residue number systems to be $0 \leq s < M_\beta$ and $-M_\beta/2 < s < M_\beta/2$, respectively. Consequently, in each case the range of the residue number system and the range of its associated mixed-radix number system coincide. (This would not be the case if M_β were not the least common multiple of the moduli.) This is extremely important when we wish to change from one system to the other.

The Order of the Moduli

We have assumed throughout our discussion so far that the moduli $m_1,m_2,\ldots,m_n$ of the base vector β have been kept rigidly ordered when forming the associated mixed-radix number systems. Suppose, on the other hand, we allow permutations of the moduli. Two obvious choices would be the orderings

$$m_{j_1} < m_{j_2} < \ldots < m_{j_n}, \qquad (2.22)$$

and

$$m_{k_1} > m_{k_2} > \ldots > m_{k_n}. \qquad (2.23)$$

In these two examples we use the names ascending associated mixed-radix number system and descending associated mixed-radix number system, respectively. Other permutations are also possible, of course, and each permutation of the moduli in β produces its own associated mixed-radix number system. It is important to note that a permutation of the elements of the base vector β causes simply the same permutation of the residue digits in $|s|_\beta$. However, the mixed-radix digits in $\langle s\rangle_\beta$ can be altered drastically by a permutation of the moduli in β. This apparent anomaly can be utilized to our advantage for certain computations, as we shall show in the next section.

Motivation

One of the motivations for our interest in pairs of associated residue and mixed-radix number systems stems from the fact that addition, subtraction, and multiplication of integers (and even division, under certain circumstances) are extremely simple to perform in a residue number system. On the other hand, the residue representation $|s|_\beta$ does not lend itself to simple algorithms for

(i) magnitude comparison of s with t

(ii) sign detection of s

(iii) recovery of the ordinary decimal (or binary) representation of s from $|s|_\beta$ (called residue-to-radix conversion).

Simple algorithms are available, however, for these three operations if we have the corresponding mixed-radix representation.

Digit Sets

Consider the standard mixed-radix number system and its associated standard residue number system for the base vector $\beta = [m_1,m_2,\ldots,m_n]$. If

$$s = d_0 + d_1m_1 + d_2m_2 + \ldots + d_{n-1}m_1m_2\cdots m_{n-1} \qquad (2.24)$$

has the (unique) digit sequence $\langle s\rangle_\beta = \langle d_0,d_1,\ldots,d_{n-1}\rangle_\beta$ in the former, and if s has the representation

$$|s|_\beta = \left[|s|_{m_1},\ |s|_{m_2},\ldots,\ |s|_{m_n}\right] \qquad (2.25)$$

in the latter, we see from (2.1) and (2.18) that both the residue digits $|s|_{m_i}$, and the mixed-radix digits, d_{i-1}, lie in the same closed interval $[0, m_i-1]$, for $i = 1,2,\ldots,n$.

Similarly, if

$$s = b_0 + b_1m_1 + b_2m_1m_2 + \ldots + b_{n-1}m_1m_2\cdots m_{n-1} \qquad (2.26)$$

has the (unique) digit sequence $\langle s\rangle_\beta = \langle b_0,b_1,\ldots,b_{n-1}\rangle_\beta$ in the balanced mixed-radix number system relative to β (assume all odd moduli) and if

$$/s/_\beta = \left[/s/_{m_i},\ /s/_{m_2},\ldots,\ /s/_{m_n}\right] \qquad (2.27)$$

in the associated balanced residue number system, we see from (2.3) and (2.18) that both $/s/_{m_i}$ and b_{i-1}, for $i = 1,2,\ldots,n$, lie in the same interval $[-m_i/2,\ m_i/2]$.

The integers in the intervals $[0,\ m_i-1]$ for $1 \leqslant i \leqslant n$ are called the digit sets for the standard mixed-radix number system for β. Similarly, the integers in $[-m_i/2,\ m_i/2]$, $1 \leqslant i \leqslant n$ are the digit sets for the balanced mixed-radix system for β. It is no coincidence that the complete systems of residues and their digit sets for the associated standard (respectively balanced) systems are identical. These associated systems were specifically chosen for further investigation with this property in mind. There are advantages with these choices (both esthetic and practical) but it should be pointed out that other choices could have been made. From the point of view of computer architecture it should not go unnoticed that the set of residue digits and the set of associated mixed-radix digits require identical storage and register capacity.

Conversion Between Associated Residue and Mixed-radix Number Systems

Suppose we are given the residue representation $|s|_\beta$ in $\mathbf{I}_\beta$ and we wish to find $\langle s\rangle_\beta$ in the associated mixed-radix number system. In other words, suppose we are given the residue digits $|s|_{m_i}$ and we wish to find the mixed-radix digits d_{i-1} for $i = 1,2,\ldots,n$.

To do this we set $t_1 = s$ and observe that

$$\begin{aligned} |t_1|_{m_1} &= \left|d_0 + m_1(d_1 + d_2m_2 + \ldots + d_{n-1}m_2m_3\ldots m_{n-1})\right|_{m_1} \\ &= \left|d_0 + m_1t_2\right|_{m_1} \\ &= d_0. \qquad (2.28) \end{aligned}$$

We also observe that $|t_1|_{m_1} = |s|_{m_1}$. Thus,

$$d_0 = |s|_{m_1} \qquad (2.29)$$

and so the first mixed-radix digit of s is equal to the first residue digit of s and no computation is necessary.

We continue by writing

$$\begin{aligned} |t_2|_{m_2} &= \left|d_1 + m_2(d_2 + d_3m_3 + \ldots + d_{n-1}m_3m_4\ldots m_{n-1})\right|_{m_2} \\ &= \left|d_1 + m_2t_3\right|_{n_2} \\ &= d_1. \qquad (2.30) \end{aligned}$$

In general, then, $t_1 = s$, $d_0 = |s|_{m_1}$, and

$$\left\{ \begin{aligned} t_{i+1} &= \frac{t_i - d_{i-1}}{m_i} \\ d_i &= \left|t_{i+1}\right|_{m_{i+1}} \end{aligned} \right. \qquad i = 1,2,\ldots,n-1. \qquad (2.31)$$

We should point out that the computations necessary for computing d_i in (2.31) can be carried out using residue arithmetic. (See Szabó and Tanaka [1, p.44] for details.)

Suppose, on the other hand, we are given $\langle s\rangle_\beta$ and we wish to determine $|s|_\beta$. In this case we use the relations

$$\left\{ \begin{aligned} |s|_{m_1} &= d_0 \\ |s|_{m_i} &= \left|d_0 + d_1m_1 + \ldots + d_{i-1}m_1m_2\ldots m_{i-1}\right|_{m_i} \end{aligned} \right.$$

$$i = 2,3,\ldots,n \qquad (2.32)$$

where $|s|_{m_i}$ is computed from the relations

$$\left\{ \begin{aligned} P_1 &= \left|d_{i-1}\right|_{m_i} \\ P_2 &= \left|d_{i-2} + P_1m_{i-1}\right|_{m_i} \\ &\cdot \;\; \cdot \;\; \cdot \;\; \cdot \;\; \cdot \;\; \cdot \\ P_i &= \left|d_0 + P_{i-1}m_1\right|_{m_i} \end{aligned} \right. \qquad (2.33)$$

with $|s|_{m_i} = P_i$.

These computations can also be done using residue arithmetic so that converting between residue and mixed-radix systems can be done using residue arithmetic in both directions.

3. Residue Base Conversion

Suppose we are given the base vector β and, for s in the range $0 \leq s < M_\beta$, the standard residue representation $|s|_\beta$, and we wish to find the standard residue representation

$$|s|_{\beta'} = \left[|s|_{m_1'}, |s|_{m_2'}, \ldots, |s|_{m_k'}\right] \qquad (3.1)$$

for some other base vector

$$\beta' = \left[m_1', m_2', \ldots, m_k'\right]. \qquad (3.2)$$

We call the process by which this is accomplished *residue base conversion*.

Carrying out residue base conversion involves the determination of the new residue digits $|s|_{m_i'}$ for $i = 1,2,\ldots,k$, from the old residue digits. Since we shall compute the new residue digits one at a time all we need is an efficient algorithm for determining the residue $|s|_\mu$ for an arbitrary *target modulus* $\mu \geq 2$. For the case where μ is relatively prime to M_β an efficient algorithm is already known. It involves the conversion of $|s|_\beta$ to $\langle s\rangle_\beta$, followed by the evaluation of

$$|s|_\mu = \left|d_0 + d_1m_1 + d_2m_1m_2 + \ldots + d_{n-1}m_1m_2\ldots m_{n-1}\right|_\mu. \qquad (3.3)$$

This algorithm is widely used [1, p.47] if the new base vector $\beta' = [m_1,m_2,\ldots,m_n, \mu]$ is merely an extension of the old base vector β. (In base extension, μ must be relatively prime to M_β.) However, our concern in this paper is not with base extension but with the general problem of residue base conversion and, in particular, with the case where each modulus in β' is *not* relatively prime to M_β even though the moduli in β' are pairwise relatively prime among themselves. It is now shown that this leads to a considerable simplification of the base conversion algorithm mentioned above.

Some Preliminaries

Given the base vector $\beta = [m_1,m_2,\ldots,m_n]$ and the target modulus $\mu \geqslant 2$, we define a set of *β-reduced moduli* $\mu_i(\beta)$, for $i = 0,1,\ldots,n-1$, as follows:

$$\left\{ \begin{aligned} \mu_0(\beta) &= \mu \\ \mu_i(\beta) &= \frac{\mu}{(\mu,\, m_1\, m_2\, \ldots\, m_i)} \qquad i = 1,2,\ldots,n-1. \end{aligned} \right. \qquad (3.4)$$

Since the moduli $m_1,m_2,\ldots,m_n$ are pairwise relatively prime, $\mu_i(\beta)$ can also be written*

$$\mu_i = \frac{\mu}{(\mu,m_1)(\mu,m_2)\dots(\mu,m_i)} \, . \qquad (3.5)$$

Thus, we have the relation

$$\mu_i = \mu_{i+1}(\mu,m_{i+1}) \qquad i = 0,1,\dots,n-2 \qquad (3.6)$$

The following lemma makes use of the β-reduced moduli.

LEMMA (3.7). Let the base vector $\beta = [m_1,m_2,\dots,m_n]$, the target modulus $\mu \geqslant 2$, and the β-reduced moduli $\mu_0,\mu_1,\dots,\mu_{n-1}$ be given. Then, for any integer k,

(i) $$|m_{i+1}k|_{\mu_i} = \left| |m_{i+1}|_{\mu_i} |k|_{\mu_{i+1}} \right|_{\mu_i}$$

$$i = 0,1,\dots,n-2$$

(ii) $$|m_1m_2\dots m_ik|_\mu = \left| |m_1m_2\dots m_i|_\mu |k|_{\mu_i} \right|_\mu$$

$$i = 1,2,\dots,n-1$$

(iii) $$|m_1m_2\dots m_i|_\mu = \left| |m_1|_{\mu_0} |m_2|_{\mu_1} \dots |m_i|_{\mu_{i-1}} \right|_\mu$$

$$i = 1,2,\dots,n-1.$$

Proof: For part (i) we use (3.6) and recall that $|ab|_{am} = a|b|_m$. Then, for $i = 0,1,\dots,n-2$,

$$|m_{i+1}k|_{\mu_i} = |m_{i+1}k|_{\mu_{i+1}(\mu,m_{i+1})}$$

$$= \left| (\mu,m_{i+1}) \frac{m_{i+1}}{(\mu,m_{i+1})} k \right|_{\mu_{i+1}(\mu,m_{i+1})}$$

$$= (\mu,m_{i+1}) \left| \frac{m_{i+1}}{(\mu,m_{i+1})} k \right|_{\mu_{i+1}}$$

$$= (\mu,m_{i+1}) \left| \left| \frac{m_{i+1}}{(\mu,m_{i+1})} \right|_{\mu_{i+1}} |k|_{\mu_{i+1}} \right|_{\mu_{i+1}}$$

$$= \left| (\mu,m_{i+1}) \left| \frac{m_{i+1}}{(\mu,m_{i+1})} \right|_{\mu_{i+1}} |k|_{\mu_{i+1}} \right|_{\mu_{i+1}(\mu,m_{i+1})}$$

$$= \left| \left| (\mu,m_{i+1}) \frac{m_{i+1}}{(\mu,m_{i+1})} \right|_{\mu_{i+1}(\mu,m_{i+1})} |k|_{\mu_{i+1}} \right|_{\mu_i}$$

$$= \left| |m_{i+1}|_{\mu_i} |k|_{\mu_{i+1}} \right|_{\mu_i} .$$

Similarly, for part (ii), using $\mu = \mu_i\ (\mu, m_1m_2\dots m_i)$,

$$|m_1\ m_2\ \dots\ m_ik|_\mu$$

$$= \left| (\mu,m_1m_2\dots m_i) \frac{m_1m_2\dots m_i}{(\mu,m_1m_2\dots m_i)} k \right|_{\mu_i(\mu,m_1m_2\dots m_i)}$$

$$= (\mu,m_1m_2\dots m_i) \left| \frac{m_1m_2\dots m_i}{(\mu,m_1m_2\dots m_i)} k \right|_{\mu_i}$$

$$= \left| |m_1m_2\dots m_i|_\mu |k|_{\mu_i} \right|_\mu .$$

For part (iii), note that applying (ii), with $k = m_i$, yields

$$|m_1m_2\dots m_{i-1}m_i|_\mu = \left| |m_1m_2\dots m_{i-1}|_\mu |m_i|_{\mu_{i-1}} \right|_\mu$$

and applying this result iteratively, for decreasing i, yields

$$|m_1m_2\dots m_i|_\mu = \left| |m_1|_{\mu_0} |m_2|_{\mu_1} \dots |m_{i-1}|_{\mu_{i-2}} |m_i|_{\mu_{i-1}} \right|_\mu .$$

//

The mixed-radix expression $s = d_0 + d_1m_1 + d_2m_1m_2 + \dots + d_{n-1}m_1m_2\dots m_{n-1}$, can be simplified in the sense that the results of Lemma (3.7) can be used to reduce the magnitude of both the mixed-radix digits $d_0,d_1,\dots,d_{n-1}$, and the radices $m_1,m_2,\dots,m_{n-1}$ during the evaluation of $|s|_\mu$.

The Basic Theorem

THEOREM (3.8) (Target Modulus Reduction Theorem). For the base vector β and the target modulus $\mu \geqslant 2$, with β-reduced moduli μ_i, for $i = 0,1,\dots,n-1$, let s have the standard mixed-radix form

$$s = d_0 + d_1m_1 + d_2m_1m_2 + \dots + d_{n-1}m_1m_2\dots m_{n-1}, \qquad (3.9)$$

and let

$$\begin{cases} \bar{d}_i = |d_i|_{\mu_i} \\ \bar{m}_{i+1} = |m_{i+1}|_{\mu_i} \end{cases} \qquad i = 0,1,\dots,n-1. \qquad (3.10)$$

*We write μ_i instead of $\mu_i(\beta)$ when the dependence on β is evident.

Then

$$|s|_\mu = \left|\bar{d}_0 + \bar{d}_1\bar{m}_1 + \bar{d}_2\bar{m}_1\bar{m}_2 + \dots + \bar{d}_{n-1}\bar{m}_1\bar{m}_2\dots\bar{m}_{n-1}\right|_\mu. \tag{3.11}$$

Proof: From results (ii) and (iii) of Lemma (3.7),

$$\begin{aligned}|d_i m_1 m_2 \dots m_i|_\mu &= \left||m_1 m_2 \dots m_i|_\mu |d_i|_{\mu_i}\right|_\mu \\ &= \left||m_1|_{\mu_0}|m_2|_{\mu_1}\dots|m_i|_{\mu_{i-1}}|d_i|_{\mu_i}\right|_\mu \\ &= |\bar{m}_1\bar{m}_2\dots\bar{m}_i\bar{d}_i|_\mu .\end{aligned}$$

Hence,

$$\begin{aligned}|s|_\mu &= \Big||d_0|_\mu + |d_1m_1|_\mu + |d_2m_1m_2|_\mu \\ &\qquad + \dots + |d_{n-1}m_1m_2\dots m_{n-1}|_\mu\Big|_\mu \\ &= \left|\bar{d}_0 + \bar{d}_1\bar{m}_1 + \bar{d}_2\bar{m}_1\bar{m}_2 + \dots + \bar{d}_{n-1}\bar{m}_1\bar{m}_2\dots\bar{m}_{n-1}\right|_\mu .\end{aligned}$$

//

If we are given the base vector β and a target modulus $\mu \geq 2$ along with the β-reduced moduli μ_i from (3.4), we can use (3.10) to introduce the two terms μ-reduced vector

$$\bar{\beta} = [\bar{m}_1, \bar{m}_2, \dots, \bar{m}_n], \tag{3.12}$$

and μ-reduced digit secuence for s

$$\langle s \rangle_{\bar{\beta}} = \langle \bar{d}_0, \bar{d}_1, \dots, \bar{d}_{n-1} \rangle_{\bar{\beta}} . \tag{3.13}$$

REMARK. It should be noted that $\bar{\beta}$ does not necessarily satisfy the definition of a "base vector" since $\bar{m}_i = 0$ or $\bar{m}_i = 1$ might occur for some i. Also, note that the expression

$$\bar{d}_0 + \bar{d}_1\bar{m}_1 + \bar{d}_2\bar{m}_1\bar{m}_2 + \dots + \bar{d}_{n-1}\bar{m}_1\bar{m}_2\dots\bar{m}_{n-1}$$

is not necessarily a standard mixed-radix expression since we cannot guarantee that $\bar{d}_i < \bar{m}_{i+1}$.

In (2.32) and (2.33) we demonstrated a recursive procedure for evaluating expressions such as (3.11). However, the following corollary will enable us to reduce the effort in the evaluation, considerably, by using the β-reduced moduli instead of μ.

COROLLARY (3.14). Under the hypotheses of the Target Modulus Reduction Theorem,

$$|s|_\mu = \bar{Q}_n \tag{3.15}$$

where

$$\begin{cases}\bar{Q}_1 = \bar{d}_{n-1} \\ \bar{Q}_j = \left|\bar{d}_{n-j} + \bar{Q}_{j-1}\bar{m}_{n-j+1}\right|_{\mu_{n-j}} \qquad j = 2,3,\dots,n.\end{cases} \tag{3.16}$$

Proof: We can write

$$s = d_0 + d_1m_1 + d_2m_1m_2 + \dots + d_{n-1}m_1m_2\dots m_{n-1}$$

recursively as

$$\begin{cases}Q_1 = d_{n-1} \\ Q_j = d_{n-j} + Q_{j-1}m_{n-j+1} \qquad j = 2,3,\dots,n\end{cases}$$

where $s = Q_n$. Then, from (3.10),

$$\begin{aligned}|Q_1|_{\mu_{n-1}} &= |d_{n-1}|_{\mu_{n-1}} \\ &= \bar{d}_{n-1},\end{aligned}$$

and, for j = 2,3,...,n, using Lemma (3.7) part (i) and (3.10),

$$\begin{aligned}|Q_j|_{\mu_{n-j}} &= \left||d_{n-j}|_{\mu_{n-j}} + |Q_{j-1}m_{n-j+1}|_{\mu_{n-j}}\right|_{\mu_{n-j}} \\ &= \left|\bar{d}_{n-j} + \left||m_{n-j+1}|_{\mu_{n-j}}|Q_{j-1}|_{\mu_{n-j+1}}\right|_{\mu_{n-j}}\right|_{\mu_{n-j}} \\ &= \left|\bar{d}_{n-j} + \bar{m}_{n-j+1}|Q_{j-1}|_{\mu_{n-j+1}}\right|_{\mu_{n-j}} .\end{aligned}$$

If we set

$$\bar{Q}_t = |Q_t|_{\mu_{n-t}}$$

for t = 1,2,...,n, then

$$\begin{cases}\bar{Q}_1 = \bar{d}_{n-1} \\ \bar{Q}_j = \left|\bar{d}_{n-j} + \bar{Q}_{j-1}\bar{m}_{n-j+1}\right|_{\mu_{n-j}} \qquad j = 2,3,\dots,n\end{cases}$$

and (3.16) is satisfied. Since $s = Q_n$ and $\mu_0 = \mu$

$$\begin{aligned}|s|_{\boldsymbol{\mu}} &= |Q_n|_{\mu_0} \\ &= \bar{Q}_n\end{aligned}$$

and the proof is complete.

//

The Effect of Permuting the Moduli

It should be noted that the amount of efficiency achieved by using the smaller β-reduced moduli μ_i, rather than μ, in the process of target modulus conversion depends on the ordering of the $\{m_i\}$ in the base vector $\beta = [m_1, m_2, \dots, m_n]$. Let the base vector π be obtained from β by a permutation of the moduli. Furthermore, let the moduli in

$$\begin{aligned}\pi &= [m_{i_1}, m_{i_2}, \dots, m_{i_n}] \\ &= [p_1, p_2, \dots, p_n]\end{aligned} \tag{3.17}$$

be so ordered that

$$(\mu,p_1) \geq (\mu,p_j) \qquad j = 2,3,\ldots,n. \qquad (3.18)$$

Then certainly

$$\mu_1 = \frac{\mu}{(\mu,p_1)} \qquad (3.19)$$

is minimized over all such permuted orderings.

The effect of permuting the moduli in β to produce π is simply to change the residue representation of an integer s from

$$|s|_\beta = \left[|s|_{m_1}, |s|_{m_2}, \ldots, |s|_{m_n}\right], \qquad (3.20)$$

for the base vector β, to

$$|s|_\pi = \left[|s|_{p_1}, |s|_{p_2}, \ldots, |s|_{p_n}\right] \qquad (3.21)$$

for the base vector π. In other words, the residue digits in $|s|_\beta$ are permuted to produce $|s|_\pi$ in exactly the same way that the moduli in β are permuted to produce π.

Obviously, it is desirable for efficient target modulus conversion first to permute the moduli in the base vector β (producing the base vector π) so that the resulting π-reduced moduli $\mu_i(\pi)$ will be as small as possible. The following theorem shows that a simple ordering procedure for the moduli in a base vector exists which affects a uniformly optimal reduction in the size of $\mu_0,\mu_1,\ldots,\mu_{n-1}$.

THEOREM (3.22). Given the base vector $\pi = [p_1p_2\ldots p_n]$ and the target modulus $\mu \geq 2$, where π is so ordered that

$$(\mu,p_1) \geq (\mu,p_2) \geq \ldots \geq (\mu,p_n), \qquad (3.23)$$

let the base vector $\gamma = [p_{t_1}, p_{t_2}, \ldots, p_{t_n}]$ have the same moduli as π but permuted in the order $(t_1t_2\ldots t_n)$. then

$$\mu_j(\pi) \leq \mu_j(\gamma) \qquad j = 0,1,\ldots,n-1 \qquad (3.24)$$

Proof: Suppose the target modulus μ is redundant (not relatively prime) with exactly k of moduli p_i of π. Since the $\{p_i\}$ are pairwise relatively prime and ordered to satisfy (3.23), then

$$(\mu,p_1) > (\mu,p_2) > \ldots > (\mu,p_k) > 1$$

and

$$(\mu,p_{k+1}) = (\mu,p_{k+2}) = \ldots = (\mu,p_n) = 1.$$

Now $\mu_0(\pi) = \mu = \mu_0(\gamma)$, and for $j = 1,2,\ldots,n-1$, consider the j integers $(\mu,p_{t_1}), (\mu,p_{t_2}), \ldots, (\mu,p_{t_j})$. The largest of these is no greater than (μ,p_1), and, in general, the r-th largest of these j numbers is no larger than (μ,p_r) for $r = 1,2,\ldots,j$. Hence

$$(\mu,p_{t_1})(\mu,p_{t_2})\ldots(\mu,p_{t_j}) \leq (\mu,p_1)(\mu,p_2)\ldots(\mu,p_j),$$

so that

$$\begin{aligned}\mu_j(\pi) &= \frac{\mu}{(\mu,p_1p_2\ldots p_j)}\\ &= \frac{\mu}{(\mu,p_1)(\mu,p_2)\ldots(\mu,p_j)}\\ &\leq \frac{\mu}{(\mu,p_{t_1})(\mu,p_{t_2})\ldots(\mu,p_{t_j})}\\ &= \frac{\mu}{(\mu,p_{t_1}p_{t_2}\ldots p_{t_j})}\\ &= \mu_j(\gamma) \qquad j = 1,2,\ldots,n-1.\end{aligned}$$

//

For a set of pairwise relatively prime positive integers $\{m_1,m_2,\ldots,m_n\}$ and $\mu \geq 2$, a redundancy ordering with μ of $\{m_1,m_2,\ldots,m_n\}$ is an ordering $(m_{i_1},m_{i_2},\ldots,m_{i_n})$ such that

$$(\mu,m_{i_1}) \geq (\mu,m_{i_2}) \geq \ldots \geq (\mu,m_{i_n}). \qquad (3.25)$$

The base vector $\pi = [p_1,p_2,\ldots,p_n]$ is μ-redundancy-ordered if $(p_1,p_2,\ldots,p_n)$ is a redundancy ordering with μ of the moduli $\{p_i\}$.

For the purposes of efficient target modulus conversion to modulus μ it is evident from Theorem (3.8), Corollary (3.14), and Theorem (3.22) that the base vector of a residue number system should first be μ-redundancy-ordered. The following examples illustrate target modulus conversion utilizing both a μ-redundancy-ordered base vector π and the subsequent π-reduced moduli $\mu_i(\pi)$ to simplify the computational effort.

Target Modulus Conversion Examples

Let $\beta = [39,41,43,77,80]$ be the base vector of a standard residue number system, where $M_\beta = 423,543,120$. Also, let $\mu = 315$ be the target modulus. We observe that 315 is redundant with 77, 80, and 39 and that

$$\begin{aligned}(315,77) &= 7\\ (315,80) &= 5 \qquad (3.26)\\ (315,39) &= 3.\end{aligned}$$

Thus the permuted base vector $\pi = [77,80,39,41,43]$ is μ-redundancy-ordered (for $\mu = 315$) for the residue number system under consideration. The π-reduced moduli μ_i are

$$\begin{aligned}&\mu_0 = 315 && \mu_3 = \frac{315}{(7)(5)(3)} = 3\\ &\mu_1 = \frac{315}{7} = 45 && \mu_4 = 3 \qquad (3.27)\\ &\mu_2 = \frac{315}{(7)(5)} = 9\end{aligned}$$

and the μ-reduced vector* $\bar{\pi} = [\bar{p}_1,\bar{p}_2,\bar{p}_3,\bar{p}_4,\bar{p}_5]$ has components

$$\begin{aligned} \bar{p}_1 &= |77|_{315} = 77 \\ \bar{p}_2 &= |80|_{45} = 35 \\ \bar{p}_3 &= |39|_{9} = 3 \\ \bar{p}_4 &= |41|_{3} = 2 \\ \bar{p}_5 &= |43|_{3} = 1 \end{aligned} \qquad (3.28)$$

We recall that our objective, in all of this, is the efficient evaluation of $|s|_{315}$. For s in the range

$$0 \leq s < M_\beta = M_\pi \qquad (3.29)$$

the values of $\mu_0,\mu_1,\ldots,\mu_4$ and $\bar{p}_1,\bar{p}_2,\ldots,\bar{p}_5$ are fixed. Therefore, in a practical application, these values can be entered permanently in the computer hardware, microcode, or software implementation of target modulus conversion. The digit reduction procedure indicated in Theorem (3.8) must be carried out, of course, as a particular integer s is being converted.

For example, s = 228,306,863 has the mixed-radix representation

$$\begin{aligned} s = {} & 15 + 64(77) + 12(77)(80) \\ & + 7(77)(80)(39) + 23(77)(80)(39)(41) \end{aligned} \qquad (3.30)$$

in the standard mixed-radix number system associated with the standard residue number system for $\pi = [77,80,39,41,43]$ under consideration. Then

$$\langle s \rangle_\pi = \langle 15,64,12,7,23 \rangle_\pi . \qquad (3.31)$$

is the digit sequence for s. The μ-reduced digits (for $\mu = 315$) are

$$\begin{aligned} \bar{d}_0 &= |15|_{315} = 15 \\ \bar{d}_1 &= |64|_{45} = 19 \\ \bar{d}_2 &= |12|_{9} = 3 \\ \bar{d}_3 &= |7|_{3} = 1 \\ \bar{d}_4 &= |23|_{3} = 2. \end{aligned} \qquad (3.32)$$

From Theorem (3.8), it follows that

$$\begin{aligned} |s|_{315} = \Big| & 15 + 19(77) + 3(77)(35) \\ & + 1(77)(35)(3) + 2(77)(35)(3)(2) \Big|_{315} \end{aligned} \qquad (3.33)$$

which is a considerable simplification over working with the full mixed-radix form (3.30). If we use Corollary (3.14), we can evaluate (3.33) as follows:

$$\begin{aligned} \bar{Q}_1 &= 2 \\ \bar{Q}_2 &= |1 + (2)(3)|_3 = 2 \\ \bar{Q}_3 &= |3 + (2)(3)|_9 = 0 \\ \bar{Q}_4 &= |19 + (0)(35)|_{45} = 19 \\ \bar{Q}_5 &= |15 + (19)(77)|_{315} = 218 \end{aligned}$$

and so $|s|_{315} = 218$. //

A still more dramatic reduction is possible if the target modulus μ happens to divide M_β. In the example above if we change μ from 315 to the value 105 (which divides 423,543,120) we obtain the results

$$\begin{array}{lll} \mu_0 = 105 & \bar{p}_1 = 77 & \bar{d}_0 = 15 \\ \mu_1 = 15 & \bar{p}_2 = 5 & \bar{d}_1 = 4 \\ \mu_2 = 3 & \bar{p}_3 = 0 & \bar{d}_2 = 0 \\ \mu_3 = 1 & \bar{p}_4 = 0 & \bar{d}_3 = 0 \\ \mu_4 = 1 & \bar{p}_5 = 0 & \bar{d}_4 = 0. \end{array}$$

Hence,

$$\begin{aligned} |s|_{105} &= |15 + 4(77)|_{105} \\ &= 8. \end{aligned} \qquad (3.34)$$

REMARK. Although the theory and examples for target modulus conversion have been derived herein for standard residue number systems, the modifications necessary to establish the same results for balanced residue number systems are straightforward. For reference, the balanced residue system versions of Lemma (3.7), Theorem (3.8), and Corollary (3.14) are given without proof since the proofs follow by simply paralleling the previous proofs in an obvious manner.

LEMMA (3.35). Let the base vector $\beta = [m_1,m_2,\ldots,m_n]$, with all odd moduli, the target modulus $\mu \geq 2$, and the β-reduced moduli $\mu_0,\mu_1,\ldots,\mu_{n-1}$ be given. Then for any integer k,

$$\text{(i)} \quad /m_{i+1}k/_{\mu_i} = \Big/ /m_{i+1}/_{\mu_i} /k/_{\mu_{i+1}} \Big/_{\mu_i}$$

$$i = 0,1,\ldots,n-2$$

$$\text{(ii)} \quad /m_1m_2\ldots m_ik/_\mu = \Big/ /m_1m_2\ldots m_i/_\mu /k/_{\mu_i} \Big/_\mu$$

$$i = 1,2,\ldots,n-1$$

$$\text{(iii)} \quad /m_1m_2\ldots m_i/_\mu = \Big/ /m_1/_{\mu_0} /m_2/_{\mu_1} \ldots /m_i/_{\mu_{i-1}} \Big/_\mu$$

$$i = 1,2,\ldots,n-1$$

THEOREM (3.36) (Target Modulus Reduction Theorem). For the base vector β, with all odd moduli, and the target modulus $\mu \geq 2$, with β-reduced moduli μ_i, for $i = 0,1,\ldots,n-1$, let s have the balanced mixed-radix form

$$s = b_0 + b_1m_1 + b_2m_1m_2 + \ldots + b_{n-1}m_1m_2\ldots m_{n-1},$$

*See (3.12).

and let

$$\begin{cases} \bar{b}_i = /b_i/_{\mu_i} \\ \bar{m}_{i+1} = /m_{i+1}/_{\mu_i} \end{cases} \qquad i = 0,1,\ldots,n-1.$$

Then

$$/s/_{\mu} = /\bar{b}_0 + \bar{b}_1\bar{m}_1 + \bar{b}_2\bar{m}_1\bar{m}_2 + \ldots + \bar{b}_{n-1}\bar{m}_1\bar{m}_2\cdots\bar{m}_{n-1}/_{\mu}.$$

COROLLARY (3.37). Under the hypotheses of the Target Modulus Reduction Theorem,

$$/s/_{\mu} = \bar{Q}_n$$

where

$$\begin{cases} \bar{Q}_1 = \bar{b}_{n-1} \\ \bar{Q}_j = /\bar{b}_{n-j} + \bar{Q}_{j-1}\bar{m}_{n-j+1}/_{\mu_{n-j}} \end{cases} \qquad j = 2,3,\ldots,n.$$

References

1. Szabo´, S., and R. Tanaka, Residue Arithmetic and Its Applications to Computer Technology, New York, McGraw Hill, 1967.

2. Howell, J. A., and R. T. Gregory, "Solving Linear Equations Using Residue Arithmetic - Algorithm II," BIT, v. 10 (1970), pp.23-37.