Conversion of Modular Numbers to their Mixed Radix Representation by a Matrix Formula

By J. Schönheim

Introduction. Let $m_i > 1$, $(i = 1, 2, \cdots, s)$, be integers relatively prime in pairs and denote $m = m_1 m_2 \cdots m_s$. If x_i, $0 \leqq x_i < m_i$, $(i = 1, 2, \cdots, s)$ are integers, the ordered set $(x_1, x_2, \cdots, x_s)$ is called a modular number, with respect to the moduli m_i $(i = 1, 2, \cdots, s)$ and it denotes a unique residue class mod m.

Modular arithmetic has been developed [1], [2], [5], and its use in computers has been suggested [1], [5]. It has also been applied in the solution of various problems [2], [6].

A central question is to determine the least nonnegative residue mod m of a given residue class $(x_1, x_2, \cdots, x_s)$. Denote it by n. In order to work entirely in the given modular system it was suggested [1], [3], [7] and [8] to obtain n in its mixed radix representation with respect precisely to the radices m_i $(i = 1, 2, \cdots, s)$, thus in the form

$$n = b_1 + b_2 m_1 + b_3 m_1 m_2 + \cdots + b_s m_1 m_2 \cdots m_{s-1}$$

where $0 \leqq b_i < m_i$, $(i = 1, \cdots, s)$. In these methods the modular number $(b_1, b_2, \cdots, b_s)$ is obtained from the modular number $(x_1, x_2, \cdots, x_n)$ sequentially or iteratively.

We propose here (see Theorem) a matrix method which consists in precalculating $(s - 1)$ matrices, A_i, $(i = 1, 2, \cdots, s - 1)$, which depend only on the moduli m_i $(i = 1, 2, \cdots, s)$ and in obtaining $(b_1, b_2, \cdots, b_s)$ by postmultiplication of $(x_1, x_2, \cdots, x_s)$ by $A_1, A_2, \cdots, A_{s-1}$ or more precisely, observing the nonassociativity of the used matrix product, computing:

$$(b_1, b_2, b_3, \cdots, b_s) = [\cdots[[(x_1, x_2, x_3, \cdots, x_s)A_1]A_2]\cdots A_{s-2}]A_{s-1}.$$

This method is simpler than Mann's method [3] and concentrates the sequential Svoboda-Lindamood-Shapiro method [1], [4] in a single matricial formula.

Definition 1. Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be matrices of s columns with integer elements, whose rows may be regarded as modular numbers with respect to the moduli m_i $(i = 1, \cdots, s)$. Define, provided B has s rows, $C = AB$ as $C = [c_{ij}]$, $c_{ij} = \sum a_{i\nu} b_{\nu j} \pmod{m_j}$, $0 \leqq c_{ij} < m_j$.

This matrix multiplication is not associative in general, but two exceptions are mentioned in the following lemma.

Lemma 1. *Let $E = E_{i\nu(c_\nu)}$ (fixed i, $\nu = 1, 2, \cdots, h < s$) be $s \times s$ matrices having units in the main diagonal, c_ν as νth element in the ith ($\nu \neq i$) row and zeroes elsewhere. Let D be a diagonal matrix of the same size. Then if X is an arbitrary matrix with s columns and A an arbitrary $s \times s$ matrix, we have:*

$$(XA)D = X(AD), \tag{1}$$

$$(\cdots((XE_1)E_2)\cdots)E_h = X((\cdots((E_1E_2)E_3)\cdots)E_h). \tag{2}$$

Proof. Properties (1) and (2) are immediate consequences of the definitions.

Received May 18, 1966.

Remark 1. The matrices E_ν $(\nu = 1, \cdots, h)$ are generalized elementary matrices.

Notation. Denote $x = (x_1, x_2, \cdots, x_s)$ if x is an arbitrary number of the residue class $(x_1, x_2, \cdots, x_s) \bmod m$ and denote $n \equiv (x_1, x_2, \cdots, x_s)$ if n is the least non-negative residue of the class.

LEMMA 2. *If $(x_1, x_2, \cdots x_s)$ is a modular number with respect to the moduli m_i $(i = 1, \cdots, s)$ and $n \equiv (x_1, x_2, \cdots, x_s)$ while*

$$\left(\frac{x_2 - x_1}{m_1}, \frac{x_3 - x_1}{m_1}, \cdots, \frac{x_s - x_1}{m_1}\right)$$

means a modular number with respect to the moduli m_i $(i = 2, 3, \cdots, s)$ then

$$\frac{n - x_1}{m_1} \equiv \left(\frac{x_2 - x_1}{m_1}, \frac{x_3 - x_1}{m_1}, \cdots, \frac{x_s - x_1}{m_1}\right).$$

Proof. $n - x_1$ is divisible by m_1 and since $0 \leqq n < m$, it follows that

$$0 \leqq \frac{n - x_1}{m_1} < \frac{m}{m_1}.$$

Definition 2. Let $m_i^{-1} \equiv m_{ij} \pmod{m_j}$, $i < j \leqq s$, $0 < m_{ij} < m_j$ and put $n_{ij} = m_j - m_{ij}$. Let I_k be the identity matrix of rank k. Define, for $1 \leqq k \leqq s - 1$, $s \times s$ matrices,

$$A_k = \left[\begin{array}{c|ccccc} I_{k-1} & & & 0 & & \\ \hline & 1 & n_{k,k+1} & n_{k,k+2} & \cdots & n_{k,s} \\ & 0 & m_{k,k+1} & 0 & \cdots & 0 \\ & 0 & 0 & m_{k,k+2} & \cdots & 0 \\ 0 & & & & & \\ & \vdots & & & & \\ & 0 & 0 & 0 & \cdots & m_{ks} \end{array}\right].$$

LEMMA 3. *If $(y_1, y_2, \cdots, y_s)$ is a modular number with respect to the moduli m_i $(i = 1, \cdots, s)$, then*

$$(3) \qquad (y_1, y_2, \cdots, y_s)\, A_k = \left(y_1, y_2, \cdots, y_k, \frac{y_{k+1} - y_k}{m_k}, \cdots, \frac{y_s - y_k}{m_k}\right).$$

Proof. The matrix A_k is the product of the elementary matrices $E_{k,k+1}(n_{k,k+1}) \cdots E_{ks}(n_{ks})$ multiplied by the diagonal matrix

$$D = \begin{bmatrix} I_k & & & & \\ & m_{k,k+1} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & m_{ks} \end{bmatrix}.$$

By Lemma 1 associativity holds and the effect of postmultiplication by A_k is the same as the effect of successive postmultiplications by $E_{k,k+1}$, $E_{k,k+2}$, $\cdots$, E_{ks} and D, which is precisely the right side of (3).

LEMMA 4. *Let* $n \equiv (x_1, x_2, \cdots, x_s)$ *and let* q_i, r_i $(i = 1, \cdots, s)$ *be the quotients and the remainders in the successive divisions*

$$\begin{aligned} n &= m_1 q_1 + r_1, \\ q_i &= m_{i+1} q_{i+1} + r_{i+1} \qquad (i = 1, \cdots, s-1) \end{aligned} \tag{4}$$

then

$$(\cdots(((x_1, x_2, \cdots, x_s)A_1)A_2)\cdots)A_k = (r_1, r_2, \cdots, r_k, r_{k+1}, y_{k+2}, y_{k+3}, \cdots, y_s)$$

and

$$(r_{k+1}, y_{k+2}, \cdots, y_s) \equiv q_k.$$

Proof. Proceed by induction on k. Let $k = 1$. Then by Lemma 3

$$(x_1, \cdots, x_s)A_1 = \left(x_1, \frac{x_2 - x_1}{m_1}, \cdots, \frac{x_2 - x_1}{m_2}\right),$$

hence $r_1 = x_1$ and by Lemma 2,

$$\left(\frac{x_2 - x_1}{m_1}, \cdots, \frac{x_s - x_1}{n_1}\right) \equiv \frac{n - x_1}{m_1} = q_1.$$

Therefore

$$\frac{x_2 - x_1}{m_1} \equiv r_2 \pmod{m_2} \qquad 0 \leqq r_2 < m_2.$$

Suppose the assertion is true for $1 < k < h \leqq s - 1$, thus

$$(\cdots((x_1, x_2, \cdots, x_s)A_1)\cdots)A_{h-1} = (r_1, r_2, \cdots, r_h, y_{h+1}, y_{h+r}, \cdots, y_s), \tag{5}$$

and

$$q_{h-1} \equiv (r_h, y_{h+1}, \cdots, y_s) \tag{6}$$

with respect to the moduli m_i $(i = h, h+1, \cdots, s)$. Then by Lemma 3 and (5)

$$((\cdots((x_1, x_2, \cdots, x_s)A_1)\cdots)A_{h-1})A_h = \left(r_1, r_2, \cdots, r_h \frac{y_{h+1} - r_h}{m_h}, \cdots, \frac{y_s - r_h}{m_h}\right)$$

and by (6) and Lemma 2

$$\left(\frac{y_{h+1} - r_h}{m_h}, \cdots, \frac{y_s - r_h}{m_h}\right) \equiv \frac{q_{h-1} - r_h}{m_h} = q_h.$$

Therefore

$$\frac{y_{h+1} - r_h}{m_h} = r_{h+1}, \qquad 0 \leqq r_{h+1} < m_{h+1}.$$

Hence the result is true for $k = h$.

THEOREM. *If* $m_i, m_i > 1$ $(i = 1, 2, \cdots, s)$ *are integers, relatively prime in pairs*

$m = m_1 \cdots m_s$, and if n is the least nonnegative residue of the class $(x_1, x_2, \cdots, x_s)$ mod m and $b_1, b_2, \cdots, b_s$ are the digits of the mixed radix representation of n with respect to the radices m_i $(i = 1, \cdots, s)$ then with matrix multiplication and matrices A_i $(i = 1, \cdots, s)$ as defined in Definitions 1 and 2

$$(b_1, b_2, \cdots, b_s) = (\cdots(((x_1, x_2, \cdots, x_s)A_1)A_2)\cdots)A_{s-1}.$$

Proof. The digits $b_1, \cdots, b_s$ of the required representation are the remainders of the successive divisions (4) and the theorem is a corollary of Lemma 4 with $k = s - 1$.

Remark 2. The above algorithm requires in general $s - 1$ matrix multiplications, but if $k < s - 1$ and

$$(7) \quad (\cdots(((x_1, x_2, \cdots, x_s)A_1)A_2)\cdots)A_k = (r_1, r_2, \cdots, r_{k+1}, 0, 0, \cdots, 0)$$

then the right side of (7) is the result, and no further multiplications are needed.

Example. Let 2, 3, 5, 7 be the moduli m_1, m_2, m_3, m_4. Then the numbers m_{ij}, $i < j$ are given by

$$\begin{array}{ccc} 2 & 3 & 4 \\ & 2 & 5 \\ & & 3 \end{array}$$

and therefore the numbers n_{ij} are

$$\begin{array}{ccc} 1 & 2 & 3 \\ & 3 & 2 \\ & & 4 \end{array}$$

The matrices A_1, A_2, A_3 are

$$A_1 = \begin{bmatrix} 1 & 1 & 2 & 3 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}; \quad A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 2 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 5 \end{bmatrix}; \quad A_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 3 \end{bmatrix}.$$

Let $(0\,2\,0\,0)$ be a residue class mod 210. Let n be the least nonnegative residue of this class. Then b_1, b_2, b_3, b_4, the digits of the mixed radix representation of n, with respect to the radices 2, 3, 5, 7 are given by

$$(b_1, b_2, b_3, b_4) = (((0\;2\;0\;0)A_1)A_2)A_3 = (0\;1\;3\;4).$$

Indeed $0 + 1\cdot 2 + 3\cdot 2\cdot 3 + 4\cdot 2\cdot 3\cdot 5 = 140$, $140 < 210$ and $140 \equiv 0 \pmod 2$, $2 \pmod 3$, $0 \pmod 5$ and $0 \pmod 7$.

Department of Applied Mathematics
Tel-Aviv University
Ramat-Aviv, Tel-Aviv
Israel

1. M. Valach & A. Svoboda, "Circuit operators," *Stroje na. Zpracovani Informaci Sb.*, v. 111, 1957, pp. 247–297. (Czech)
2. H. S. Shapiro, "Some remarks on modular arithmetic and parallel computation," *Math. Comp.*, v. 16, 1962, pp. 218–222. MR **26** #4511.
3. H. B. Mann, "On modular computation," *Math. Comp.*, v. 15, 1961, pp. 190–192. MR **22** #10944.
4. G. E. Lindamood & G. Shapiro, "Magnitude comparison and overflow detection in modular arithmetic computers," *SIAM Rev.*, v. 5, 1963, pp. 342–350. MR **29** #6662.
5. A. Svoboda, "The numerical system of residual classes in mathematical machines," *Information Processing*, pp. 419–422, UNESCO, Paris, R. Oldenbourg, Munich and Butterworths, London, 1960. MR **28** #5581.
6. J. Borosh & A. S. Fraenkel, "Exact solutions of linear equations with rational coefficients by congruence techniques," *Math. Comp.*, v. 20, 1966, pp. 107–112.
7. V. N. Teĭtel'baum, "Comparison of numbers in the Czech system of numbers," *Dokl. Akad. Nauk SSSR*, v. 121, 1958, pp. 807–810. (Russian) MR **21** #3367.
8. A. S. Fraenkel, *On Size of Modular Numbers*, Proc. ACM 19th National Conference, Philadelphia, Pa., 1964.