TECHNICAL NOTES AND SHORT PAPERS

On Modular Computation

By Henry B. Mann

It will be assumed that the reader is familiar with the elementary theory of congruences [1].

Let $m_1, m_2, \cdots, m_s$ be s integers relatively prime in pairs and let $M = m_1 m_2 \cdots m_s$. Let $x_1, x_2, \cdots, x_s$ be an ordered set of s integers such that $0 \leqq x_i < m_i$. There exists one and only one residue class x mod M such that $x \equiv x_i \pmod{m_i}$ and we therefore write $x = (x_1, x_2, \cdots, x_s)$. If $x = (x_1, \cdots, x_s)$, $y = (y_1, \cdots, y_s)$ then $x \pm y = (x_1 \pm y_1, \cdots, x_s \pm y_s)$, $xy = (x_1 y_1, \cdots, x_s y_s)$, where the ith coordinates must be reduced mod m_i. The symbols $(x_1, \cdots, x_s)$ are called modular numbers, but it should be kept in mind that $(x_1, \cdots, x_s)$ does not denote a number but a residue class mod M.

The purpose of this note is to describe a simple iterative procedure to determine the least non-negative residue mod M of a given residue class $(x_1, \cdots, x_s)$.

The iteration process described below gives the least non-negative residue in mixed radix representation.

Notation. The moduli are denoted by $m_1, \cdots, m_s$. We put $m_0 = 1$,

$$M_i = (0, \cdots, 0, 1, 0, \cdots, 0); \qquad i = 1, \cdots, s$$

where 1 occurs in the ith position,

$$\pi_i = m_0 m_1 \cdots m_{i-1} \qquad i = 1, \cdots, s,$$

$[x]_M$ denotes the least non-negative residue corresponding to the modular number $x = (x_1, \cdots, x_s)$.

The representation

$$[x]_M = \sum_{i=1}^{s-1} a_i \pi_i, \qquad 0 \leqq a_i < m_i, \quad i = 1, \cdots, (s-1)$$

is the mixed radix representation of $[x]_M$. Because of the condition $0 \leqq a_i < m_i$, the mixed radix representation of a number a can be coded as a modular number $x_a = (a_1, \cdots, a_s)$.

Now proceed as follows:

Find

$$M_i = \sum_j a_{ij} \pi_j, \qquad \pi_i \equiv \sum x_{ij} M_j \pmod{M}.$$

The jth columns of the matrices (a_{ij}) and (x_{ij}) are residues mod m_j, so that the rows of these matrices may be regarded as modular numbers.

In forming $(x_1, \cdots, x_s)(a_{ij})$ we proceed as in ordinary matrix multiplication but compute the inner product $x_1 a_{1j} + \cdots + x_s a_{sj} \bmod m_j$. Similarly, in forming $(a_1, \cdots, a_s)(x_{ij})$ we compute the inner product $a_1 x_{1j} + \cdots + a_s x_{sj} \bmod m_j$. Note

Received June 2, 1960.

that if $[x]_M = \sum_j a_j \pi_j$, then $(a_1, \cdots, a_s)(x_{ij}) = x$, but $x(a_{ij})$ gives in general not the radix representation of x, but of $(x(a_{ij}))(x_{ij})$*.

Given $x = (x_1, \cdots, x_s)$, the iteration proceeds as follows:

x	Δx	Δa	a
$x = (x_1, \cdots, x_s)$			$a^{(1)} = x(a_{ij})$
$x^{(1)} = a^{(1)}(x_{ij})$	$x - x^{(1)}$	$(x - x^{(1)})(a_{ij})$	$a^{(2)} = a^{(1)} + \Delta a^{(1)}$
$x^{(\alpha)} = a^{(\alpha)}(x_{ij})$	$x - x^{(\alpha)}$	$(x - x^{(\alpha)})(a_{ij})$	$a^{(\alpha+1)} = a^{(\alpha)} + \Delta a^{(\alpha)}$

The process ends when $\Delta x = 0$.

The first two coordinates of $x^{(1)}$ will coincide with the first two coordinates of x. Thereafter the first $\alpha + 1$ coordinates of $x^{(\alpha)}$ will coincide with the first $(\alpha + 1)$ coordinates of x so that $x^{(s-1)} = x$ and hence $a^{(s-1)}$ gives the mixed radix representation of $[x]_M$, the coordinates of $a^{(s-1)}$ being the digits of this representation. In many cases, however, less than $(s - 1)$ steps will suffice.

Example 1 (*ascending order*): $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $m_4 = 7$.

$$(a_{ij}) = \begin{matrix} 1 & 1 & 2 & 3 \\ 0 & 2 & 1 & 2 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 4 \end{matrix} \qquad x_{ij} = \begin{matrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 2 \end{matrix}$$

x	Δx	Δa	a
1, 2, 2, 5			1, 2, 1, 0
$x_1 =$ 1, 2, 1, 4	0, 0, 1, 1	0, 0, 1, 1	1, 2, 2, 1
$x_2 =$ 1, 2, 2, 5			

Hence $[x]_{210} = 1 + 2.2 + 2.6 + 1.30 = 47$.

Example 2 (*descending order*): $m_1 = 7$, $m_2 = 5$, $m_3 = 3$, $m_4 = 2$.

$$a_{ij} = \begin{matrix} 1 & 2 & 0 & 1 \\ 0 & 3 & 0 & 1 \\ 0 & 0 & 2 & 0, \\ 0 & 0 & 0 & 1 \end{matrix} \qquad x_{ij} = \begin{matrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 1 \\ 0 & 0 & 2 & 1. \\ 0 & 0 & 0 & 1 \end{matrix}$$

x	Δx	Δa	a
4, 3, 1, 0			4, 2, 2, 1
4, 3, 1, 1	0, 0, 0, 1	0, 0, 0, 1	4, 2, 2, 0
4, 3, 1, 0			

Hence $[4, 3, 1, 0]_{210} = 4 + 2.7 + 2.35 = 88$.

Remarks: (1) Arranging the modules in ascending order may have an advantage because the matrices (a_{ij}) and (x_{ij}) are half diagonal and if $0 \leqq y_j < m_j$ then also $0 \leqq y_j < m_{j+1}$ so that y_j never has to be converted. However, any arrangement will work.

(2) No conversion to decimals is necessary to decide if $[x^{(1)}]_M > [x^{(2)}]_M$. If $[x^{(1)}]_M = \sum_j a_j^{(1)} \pi_j$, $[x^{(2)}]_M = \sum_j a_j^{(2)} \pi_j$, then $[x^{(1)}]_M > [x^{(2)}]_M$ if and only if $a_s^{(1)} > a_s^{(2)}$ or $a_s^{(1)} = a_s^{(2)}, \cdots, a_{s-j+1}^{(1)} = a_{s-j+1}^{(2)}, a_{s-j}^{(1)} > a_{s-j}^{(2)}$.

* Caution: The matrix multiplication defined above is not associative.

(3) All calculations are mod m_i so that the digits of the mixed radix representation of $[x]_M$ can be obtained using only calculations mod m_i.

(4) The value $x - x^{(a)}$ can be obtained from $x - x^{(a)} = x - x^{(a-1)} + x^{(a-1)} - x^{(a)}$ so that the modular number x need not be remembered during the whole process.

(5) The matrices (a_{ij}) and (x_{ij}) are computed preliminary to the iteration procedure and are not part of it.

Ohio State University
Columbus 10, Ohio

1. B. M. STEWART, *Theory of Numbers*, Macmillan, 1952, p. 111-113 and p. 130.

Generation of Permutations by Transposition

By Mark B. Wells

1. Introduction. As discussed by Tompkins [1], many problems require the generation of all $n!$ permutations of n marks (henceforth called arrangements). This note presents a generation scheme whereby each step consists of merely transposing two of the marks. The bookkeeping is quite simple, thus this scheme is somewhat faster than either the usual dictionary order method or the Tompkins-Paige method [1]. Also, the important property of leaving the $(j + 1)$st position alone until all $j!$ arrangements of the marks in the first j positions have been generated is preserved.

2. Notation. An arrangement of n marks will be given by an n-tuple, $(m_1, m_2, \cdots m_n)$. A permutation, that is, an operation of permuting an arrangement of marks, will be given in cyclic form, with P's modified by subscripts as entries. The subscripts indicate the position of the marks to be moved in the n-tuple on which the permutation is operating. For example, if $a = (1, 2, 5, 4, 3)$ is an arrangement of five marks and $\rho = (P_1P_3P_2)(P_4P_5)$ is a permutation, then $\rho(a) = (2, 5, 1, 3, 4)$.

The bookkeeping for this generation scheme is handled, as in most schemes of this type, by an ordered set of indices t_k, $k = 2, 3, \cdots, n$, where each t_k assumes the values 1 through k and indicates the progress of the subgeneration of the arrangements of marks in positions 1 to k. (This is essentially the "signature" discussed in [1].) Thus there are $n!$ sets of values for the t_k's, one set for each arrangement of the n marks. The set $t_k = 1$ for all k corresponds to the initial arrangement, and successive sets are formed in dictionary order (assuming increasing significance with increasing subscript). An index k' gives at each step the smallest subscript k for which $t_k \neq k$.

3. The Generation Rules. The transposition required at each step depends on the current value of the index k' and on the corresponding value of $t_{k'+1}$ (t_{n+1} is assumed = 1). The rules are:

I. If k' is even, then interchange the marks in positions k' and $k' - 1$.

Received August 12, 1960.