On Mappings for Modular Arithmetic, I

T. R. N. Rao*

Bell Telephone Laboratories, Inc., Holmdel, New Jersey

AND

N. Zierler†

The MITRE Corp., Bedford, Massachusetts

Abstract. Standard computing machine arithmetic performs the operations of addition, multiplication and division on the integers modulo $m = 2^j$ represented as binary j-tuples. A rather well-known alternative is to represent the integers modulo m as n-tuples $a_1, \cdots, a_n$ where each a_i is treated modulo an integer m_i. An additional operation that must be provided assigns an integer modulo m to each such n-tuple and it is convenient to require that this assignment be additive and onto.

In this note the family of all such mappings is characterized in a simple, explicit way, and it is shown that the number of mappings φ which preserve the multiplicative identity (that is, such that $\varphi(1, 1, \cdots, 1) = 1$) is g.c.d. $(m, m_1) \cdots$ g.c.d. $(m, m_n)/m$ if m divides l.c.m. $\{m_1, \cdots, m_n\}$ and is zero otherwise.

Standard computing machines perform the arithmetic operations on the integers modulo $m = 2^j$ represented as binary j-tuples. An alternative known as modular or residue class arithmetic is to represent integers modulo m as n-tuples $a_1, \cdots, a_n$ where each a_i is treated modulo an integer m_i. The properties and advantages of modular arithmetic are illustrated in earlier work of Garner [1], Svoboda [2] and others [3]. The numbers $m_1, m_2, \cdots, m_n$ are generally called the bases or moduli and m the range of the system.

In this paper, representation of integers modulo m are considered using moduli $m_1, m_2, \cdots, m_n$ which may *not* be pairwise relatively prime. An additional operation that must be provided is one that assigns an integer modulo m to each such n-tuple and it is convenient and natural to require that this assignment be additive, onto and preserve multiplicative identity.

We characterize the family of all such mappings in a simple, explicit way and deduce a formula for their number. The reader who is not familiar with the elementary notions of number theory involved may refer to [4].

Let Z_k denote the ring of residue classes of the integers modulo k.

Let $n, m_1, \cdots, m_n$ and m all be positive integers, let[1] $N = Z_{m_1} x \cdots x Z_{m_n}$, and let φ be a function defined on all of N with values in Z_m.

φ is *additive* if

$$\varphi(x + y) = \varphi(x) + \varphi(y) \quad \text{for all} \quad x, y \text{ in } N. \tag{1}$$

* The work of this author was performed while he was with the Information Systems Laboratory, the University of Michigan, Ann Arbor, Michigan, and was supported by Contract AF33(657)-7811.

† The work of this author was sponsored by the Air Force Electronic Command, under Contract AF19(628)-2290. The author's present address is the Institute for Defense Analysis, Princeton, N. J.

[1] That is, the set of all n-tuples $x_1, \cdots, x_n$ with $x_i \in Z_{m_i}$ $(i = 1, \cdots, n)$.

Journal of the Association for Computing Machinery, Vol. 12, No. 4 (October, 1965), pp. 542–544

φ is *homogeneous* if

$$\varphi(cx) = c\varphi(x) \quad \text{for all} \quad c \in Z, x \in N \tag{2}$$

where $cx = c(x_1, \cdots, x_n) = (cx_1, \cdots, cx_n)$ with $cx_i \in Z_{m_i}$ and $c\varphi(x) \in Z_m$.

For $i = 1, \cdots, n$ let e_i denote the element of N with (the residue class of) 1 as the ith component, and (residue classes) 0 elsewhere; and let $r_i = \varphi(e_i)$.

LEMMA 1. *If φ is additive, then it is homogeneous and $\varphi(0) = 0$.*

PROOF. For any integer c,

$$\varphi(cx) = \varphi((c-1)x + x) = \varphi((c-1)x) + \varphi(x)$$
$$= \varphi((c-2)x + x) + \varphi(x) = \varphi((c-2)x) + 2\varphi(x) = \cdots = c\varphi(x).$$

In particular, $\varphi(0) = \varphi(0x)$ (for every $x \in N$) $= 0\varphi(x) = 0$.

LEMMA 2. *φ is additive if and only if both of the following hold:*

$$m_i r_i = 0 \pmod{m} \qquad (i = 1, \cdots, n) \tag{3}$$

$$\varphi(x) = \sum_{i=1}^{n} x_i r_i \quad \textit{for all} \quad x \in N \tag{4}$$

where the equality in (3) as well as (4) means equality in Z_m. (Note that the Equation (4) does not define a function φ if each x_i is an arbitrary member of an equivalence class modulo m_i unless (3) holds.)

PROOF. Suppose φ is additive. Then, by Lemma 1,

$$m_i r_i = m_i \varphi(e_i) = \varphi(m_i e_i) = \varphi(0) = 0,$$

which proves (3). To prove (4), observe that

$$\varphi(x) = \varphi((x_1, \cdots, x_n)) = \varphi(\sum x_i e_i) = \sum x_i \varphi(e_i) = \sum x_i r_i .$$

Conversely, if (3) holds, so that (4) makes sense when each x_i is an arbitrary member of a residue class modulo m_i, and if (4) holds too, then $\varphi(x + y) = \sum (x_i + y_i) r_i$ by definition of addition ($x_i + y_i$ is any member of the appropriate equivalence class) $= \sum x_i r_i + \sum y_i r_i = \varphi(x) + \varphi(y)$, and φ is additive.

LEMMA 3. *Suppose φ is additive. Then φ maps N onto Z_m if and only if $(r_1, \cdots, r_n, m) = 1$.*[2]

PROOF. If φ is onto, there exists x in N with $\varphi(x) = 1$. Hence, for some rational integer a we can write the following equation in rational integers: $\sum x_i r_i = 1 + am$. It follows that any common divisor of $r_1, \cdots, r_n$ and m divides 1; i.e., $(r_1, \cdots, r_n, m) = 1$.

Conversely, if $(r_1, \cdots, r_n, m) = 1$, the Euclidean algorithm assures us that there exist integers $x_0, \cdots, x_n$ such that $x_0 m + \sum x_i r_i = 1$. Then by Lemma 2, $\varphi(x) = \varphi((x_1, \cdots, x_n)) = \sum x_i r_i = 1 - x_0 m = 1$ in Z_m. It follows now that for every integer c, $\varphi(cx) = c\varphi(x) = c1 = c$ in Z_m, so φ is onto, as was to be proved.

Let $u = \text{l.c.m.}\,\{m_1, \cdots, m_n\}$.

LEMMA 4. *Suppose φ is an additive mapping of N on Z_m. Then $m \mid u$.*

PROOF. There exist integers y_i such that $m_i r_i = y_i m$ $(i = 1, \cdots, n)$ by Lemma 2 and integers $x_0, \cdots, x_n$ such that $1 = x_0 m + \sum x_i r_i$ by Lemma 3. Then

$$u = x_0 m u + \sum x_i u r_i = x_0 m u + \sum x_i y_i m u / m_i = m(x_0 u + \sum x_i y_i u / m_i)$$

and, since u/m_i is an integer, $m \mid u$.

[2] $(y_1, y_2, \cdots)$ denotes greatest common divisor of the integers $y_1, y_2, \cdots$ throughout this paper.

Let 1 denote the element $(1, \cdots, 1)$ of N.

THEOREM.[3] *Suppose $m \mid u$. Then the number of additive mappings φ of N on Z_m such that $\varphi(1) = 1$ is $(m, m_1) \cdots (m, m_n)/m$.*

PROOF. If we set $r_i = m/(m, m_i)$ property (3) holds, so the corresponding mapping φ_1 defined by (4) is additive by Lemma 2. If some prime p divides all the r_i, it divides m, and we let p^r denote the largest power of p that does. Then $p^r \mid u$, so for some i, $p^r \mid m_i$. But then $p^r \mid (m, m_i)$ so p does not appear as a factor of r_i and $r = 0$. Thus, $(r_1, \cdots, r_n) = 1$ so, a fortiori, $(r_1, \cdots, r_n, m) = 1$ and φ_1 is onto Z_m by Lemma 3. Let U denote the set of all v in N such that $\varphi_1(v) = 1$. If $v \in U$, clearly $v_i r_i m_i \equiv 0 \bmod m$ for all i and $(v_1 r_1, \cdots, v_n r_n, m) = 1$ since $\sum v_i r_i \equiv 1$ modulo m. Hence the mapping φ_v defined by $\varphi_v(x) = \sum v_i r_i x_i$ is an additive mapping of N on Z_m such that $\varphi_v(1) = 1$. Conversely, if φ is any additive mapping of N on Z_m such that $\varphi(1) = 1$, then by (3) there exist integers z_i such that $m_i \varphi(e_i) = z_i m$. Let $v_i = z_i(m, m_i)/m_i$. Then

$$\varphi_v(e_i) = v_i r_i = v_i m/(m, m_i) = z_i m/m_i = \varphi(e_i),$$

so $\varphi = \varphi_v$. Since

$$\varphi_1(v) = \sum v_i r_i = \sum \varphi(e_i) = \varphi(\sum e_i) = \varphi(1) = 1, \qquad v \in U,$$

and we have shown that every additive mapping of N on Z_m assigning 1 to 1 is of the form φ_v for $v \in U$.

For $y, v \in U$, say $y \sim v$ if $\varphi_y = \varphi_v$. Clearly "$\sim$" is an equivalence relation in U, and the number of distinct mappings φ_v, $v \in U$ is equal to the number of equivalence classes into which U is partitioned by this relation. Now $y \sim v$ if and only if $y_i r_i = v_i r_i$ if and only if $(y_i - v_i)m/(m, m_i) \equiv 0 \bmod m$ if and only if $(m, m_i) \mid (y_i - v_i)$ for $i = 1, \cdots, n$. In other words, $y \sim v$ if and only if there exists w in N with $y = v + w$ and $(m, m_i) \mid w_i$ for $i = 1, \cdots, n$. The number of multiples of (m, m_i) in Z_{m_i} is $m_i/(m, m_i)$ so the number of such w is $\Pi\, m_i/(m, m_i)$, and this is then the number of elements in each equivalence class of U. Similarly, if $\varphi_1(v) = 1$, then $\varphi_1(y) = 1$ if and only if $y = v + w$ with $\varphi_1(w) = 0$, so the number of members of U is equal to the number of members of $\varphi_1^{-1}(0)$. Since this is the kernel of an additive homorphism of N on Z_m, the number of its elements is order N/order $Z_m = \Pi\, m_i/m$. Then the number of distinct mappings φ_v, $v \in U$, is

$$(\Pi\, m_i/m)(\Pi\, m_i/(m, m_i))^{-1} = \Pi(m, m_i)/m$$

as was to be proved.

RECEIVED APRIL, 1963; REVISED APRIL, 1965

REFERENCES

1. GARNER, H. L. The residue number system. *IRE Trans. EC-8*, 2 (June 1959).
2. SVOBODA, A. The numerical system of residual classes in mathematical machines. *Information Processing* (Proc. UNESCO Conf., Paris, June 1959), pp. 419–422; 1960.
3. LOCKHEED MISSILES AND SPACE COMPANY. Modular arithmetic techniques. ASD-TDR,-62-686, Sunnyvale, Calif., Aug. 1962.
4. LEVEQUE, W. J. *Topics in Number Theory, Vol. I*, pp. 1–47. Addison Wesley, 1956.

[3] The authors thank the referee for catching an error in the original form of the theorem.